AX8600R Software Manual

Message and Log Reference

For Version 12.1

AX86R-S010X

AlaxalA

■ **Relevant products**

This manual applies to the models in the AX8600R series of devices. It also describes the functionality of version 12.1 of the software for the AX8600R series of devices.

■ **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.

IPX is a trademark of Novell, Inc.

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.

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

■ **Reading and storing this manual**

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

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

■ **Notes**

Information in this document is subject to change without notice.

■ **Editions history**

August 2013 (Edition 1) AX86R-S010X

■ **Copyright**

Preface

Applicable products and software versions

This manual applies to the models in the AX8600R series of devices. It also describes the functionality of version 12.1 of the software for the AX8600R series of devices.

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.

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 Device.

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 Device.

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

```
Quick Start Guide


            (AX86R-Q001X)
```

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

```
Hardware Instruction Manual


            (AX86R-H001X)
```
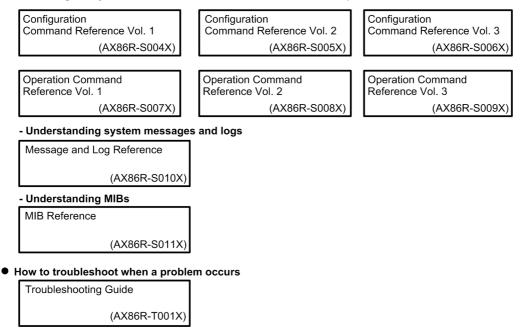
● **Understanding the software functions, configuration settings, and operation commands**
  ▽ First, see the following guides to check the functions or capacity limits.

  - **Capacity limits**   **- Filters and QoS**   **- IP packet forwarding**
  - **Basic operations (e.g. logging in)**   **- Network management**   **- Unicast routing**
  - **Ethernet**   **- Multicast routing**

```
Configuration Guide Vol. 1      Configuration Guide Vol. 2      Configuration Guide Vol. 3


          (AX86R-S001X)                  (AX86R-S002X)                  (AX86R-S003X)
```

  ▽ If necessary, see the following references.
    - **Learning the syntax of commands and the details of command parameters**

```
Configuration                   Configuration                   Configuration
Command Reference Vol. 1        Command Reference Vol. 2        Command Reference Vol. 3
          (AX86R-S004X)                  (AX86R-S005X)                  (AX86R-S006X)
```

```
Operation Command               Operation Command               Operation Command
Reference Vol. 1                Reference Vol. 2                Reference Vol. 3
          (AX86R-S007X)                  (AX86R-S008X)                  (AX86R-S009X)
```

    - **Understanding system messages and logs**

```
Message and Log Reference


          (AX86R-S010X)
```

    - **Understanding MIBs**

```
MIB Reference


          (AX86R-S011X)
```

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

```
Troubleshooting Guide


          (AX86R-T001X)
```

Conventions: The terms "Device" and "device"

The term Device (upper-case "D") is an abbreviation for the following:

AX8600R series device

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

Abbreviations used in the manual

```
AC          Alternating Current
ACK         ACKnowledge
ARP         Address Resolution Protocol
AS          Autonomous System
AUX         Auxiliary
BCU         Basic Control Unit
```

```
BEQ        Best Effort Queueing
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)
BOOTP      Bootstrap Protocol
BPDU       Bridge Protocol Data Unit
CC         Continuity Check
CCM        Continuity Check Message
CFM        Connectivity Fault Management
CFP        C Form-factor Pluggable
CIDR       Classless Inter-Domain Routing
CoS        Class of Service
CRC        Cyclic Redundancy Check
CSMA/CD    Carrier Sense Multiple Access with Collision Detection
DA         Destination Address
DC         Direct Current
DCE        Data Circuit terminating Equipment
DHCP       Dynamic Host Configuration Protocol
DHCPv6     Dynamic Host Configuration Protocol for IPv6
DNS        Domain Name System
DR         Designated Router
DSAP       Destination Service Access Point
DSCP       Differentiated Services Code Point
DTE        Data Terminal Equipment
E-mail     Electronic mail
EAP        Extensible Authentication Protocol
EAPOL      EAP Over LAN
EFM        Ethernet in the First Mile
ETH-AIS    Ethernet Alarm Indicator Signal
ETH-LCK    Ethernet Locked Signal
FAN        Fan Unit
FCS        Frame Check Sequence
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
IEEE       Institute of Electrical and Electronics Engineers, Inc.
IETF       the Internet Engineering Task Force
IGMP       Internet Group Management Protocol
IP         Internet Protocol
IPv4       Internet Protocol version 4
IPv6       Internet Protocol version 6
IPX        Internetwork Packet Exchange
ISO        International Organization for Standardization
ISP        Internet Service Provider
LAN        Local Area Network
LCD        Liquid Crystal Display
LED        Light Emitting Diode
LLC        Logical Link Control
LLDP       Link Layer Discovery Protocol
LLQ        Low Latency Queueing
LSA        Link State Advertisement
MA         Maintenance Association
MAC        Media Access Control
MC         Memory Card
MD5        Message Digest 5
MDI        Medium Dependent Interface
MDI-X      Medium Dependent Interface crossover
MEG        Maintenance Entity Group
MEP        Maintenance association End Point/Maintenance entity group End
           Point
MIB        Management Information Base
MIP        Maintenance domain Intermediate Point
MP         Maintenance Point
```

```
MRU        Maximum Receive Unit
MTU        Maximum Transfer Unit
NAK        Not AcKnowledge
NAS        Network Access Server
NBMA       Non-Broadcast Multiple-Access
NDP        Neighbor Discovery Protocol
NIF        Network Interface
NLA ID     Next-Level Aggregation Identifier
NSAP       Network Service Access Point
NSSA       Not So Stubby Area
NTP        Network Time Protocol
OAM        Operations,Administration,and Maintenance
OSPF       Open Shortest Path First
OUI        Organizationally Unique Identifier
PA         Protocol Accelerator
packet/s   packets per second (can also appear as pps)
PAD        PADding
PC         Personal Computer
PDU        Protocol Data Unit
PID        Protocol IDentifier
PIM        Protocol Independent Multicast
PIM-SM     Protocol Independent Multicast-Sparse Mode
PIM-SSM    Protocol Independent Multicast-Source Specific Multicast
PQ         Priority Queueing
PRU        Packet Routing Unit
PS         Power Supply
PSINPUT    Power Supply Input
QoS        Quality of Service
RA         Router Advertisement
RADIUS     Remote Authentication Dial In User Service
RDI        Remote Defect Indication
RFC        Request For Comments
RIP        Routing Information Protocol
RIPng      Routing Information Protocol next generation
RMON       Remote Network Monitoring MIB
RPF        Reverse Path Forwarding
RR         Round Robin
RQ         ReQuest
SA         Source Address
SD         Secure Digital
SFD        Start Frame Delimiter
SFP        Small Form factor Pluggable
SFP+       Small Form factor Pluggable Plus
SFU        Switch Fabric Unit
SMTP       Simple Mail Transfer Protocol
SNAP       Sub-Network Access Protocol
SNMP       Simple Network Management Protocol
SNPA       Subnetwork Point of Attachment
SOP        System Operational Panel
SPF        Shortest Path First
SSAP       Source Service Access Point
TA         Terminal Adapter
TACACS+    Terminal Access Controller Access Control System Plus
TCP/IP     Transmission Control Protocol/Internet Protocol
TLV        Type, Length, and Value
TOS        Type Of Service
TPID       Tag Protocol Identifier
TTL        Time To Live
UDP        User Datagram Protocol
URL        Uniform Resource Locator
uRPF       unicast Reverse Path Forwarding
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
```

```
WFQ         Weighted Fair Queueing
WWW         World-Wide Web
```

Conventions: KB, MB, GB, and TB

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

Contents

Chapter

1. System Messages

1.1 Format of system messages

The Device outputs information to be reported to the administrator, such as operating status and failure information, to an operation terminal as system messages. The messages are output to operation terminals and are saved on devices as operation logs. Using this log data, you can manage the device operating status.

The following table describes the types of output messages and gives references for those messages.

Table 1-1: Message types and references

Message type	Description	Reference
System messages	Device failure information and event information	This manual
Configuration error messages	Messages output for input of configuration command	*Error Messages Displayed When Editing the Configuration* in the manual *Configuration Command Reference*
Command response messages	Messages output for input of operation command	*Response Messages* section of each command in the manual *Operation Command Reference*

1.1.1 Format of screen output

The following figure shows the format of system messages when output to the screen.

Figure 1-1: Format of screen output

```
yyyy/mm/dd hh:mm:ss zzzz 1-b(c) ee kkkkkkkk [iii...iii] xxxxxxxx
           1                2 3  4  5        6           7

yy yyyyyyyyyyy ttt...ttt
    8           9
```

1. Time: Displays the year, month, day, hour, minute, and second as well as the time zone when the message was output.

2. BCU number: Displays the number of a BCU-installed slot where an event occurred.

3. System status: Displays the status of a BCU in which an event occurred. A is displayed for the active system, and S is displayed for the standby system.

4. Event level (S0 to S7)

5. Message type

6. Message type details. Whether this information is displayed depends on the message type.

7. Message ID: Displays a unique ID for identifying messages.

8. Additional information: Displays event details as codes.

9. Message text (maximum of 316 characters)

1.1.2 Log types

The Device collects two types of log data: operation log data and statistics log data. The operation log collects system messages, command response messages, configuration error messages, and input commands as log entries, in chronological order. The statistics log collects statistics about system messages as log entries.

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

Table 1-2: Features of the operation log and statistics log

Item	Operation log	Statistics log
Log contents	• Acquires messages and input commands in chronological order. [#1]	• For each identical system message[#2], records the statistics for the time of the first and last occurrences, and the total number of occurrences.
The information to be collected	• System messages • Command response messages • Configuration error messages • The input commands	• System messages
The number of acquired entries	• The number of operation log entries to be collected is 200000[#3]. • The minimum number of log entries to be stored is fixed for each message type. You can change the minimum number of log entries to be stored by using the `logging save-count` configuration commands. The default number of entries is 500.	• The number of statistics log entries to be collected is 5000.
Processing for when the maximum number of log entries is exceeded.	• The stored old operation log entries are deleted, excluding the minimum number of operation log entries stored for each message type.	• The statistics logs with the lowest event level are deleted from the stored statistics log entries. If multiple statistics log entries with the lowest event level exist, the statistics log entries with the earliest last-occurrence time among those log entries are deleted.

#1

    If multiple log entries are simultaneously acquired, those log entries might not be displayed in chronological order.

#2

    Messages are regarded as identical if the following details are the same:

    - BCU number

    - System status

    - Event level

    - Message type

    - Message type details

    - Message ID

    - The first 2 digits of the additional information

    However, if the message type details indicate logical sections or numbers such as protocols, the message type details are excluded from the conditions to determine whether the system messages are identical.

#3

    The number of operation log entries to be collected depends on the length of each operation log entry that is actually collected. However, at least 200000 operation log entries can be collected.

1.1.3 Format of operation logs

Each operation log format is shown below.

(1) System messages

The following figure shows the system message format.

Figure 1-2: Format of system messages

```
yyyy/mm/dd hh:mm:ss[.nnn] zzzz 1-b(c) ee kkkkkkkk [iii...iii] xxxxxxxx
          1                       2 3  4     5         6          7

yy yyyyyyyyyyyy ttt...ttt
      8            9
```

1. Time: Displays the year, month, day, hour, minute, and second as well as the time zone when the log entry was acquired.

   If the timezone is displayed by using the `show logging` command, the timezone where the command is executed is displayed. By specifying a parameter for the `show logging` command, you can also display milliseconds.

2. BCU number: Displays the number of a BCU-installed slot where an event occurred.

3. System status: Displays the status of a BCU in which an event occurred. `A` is displayed for the active system, and `s` is displayed for the standby system.

4. Event level (S0 to S7)

5. Message type

6. Message type details. Whether this information is displayed depends on the message type.

7. Message ID: Displays a unique ID for identifying messages.

8. Additional information: Displays event details as codes.

9. Message text (maximum of 316 characters)

(2) Format of input commands, command response messages, and configuration error messages

The following figure shows the format of input commands, command response messages, and configuration error messages.

Figure 1-3: Format of input commands, command response messages, and configuration error messages

```
yyyy/mm/dd hh:mm:ss[.nnn] zzzz 1-b(c) ee kkkkkkkk xxxx(xxxx):xxxx ttt...ttt
          1                       2 3  4     5           6            7
```

1. Time: Displays the year, month, day, hour, minute, and second as well as the time zone when the log entry was acquired.

   If the timezone is displayed by using the `show logging` command, the timezone where the command is executed is displayed. By specifying a parameter for the `show logging` command, you can also display milliseconds.

2. BCU number: Displays the number of a BCU-installed slot where an event occurred.

3. System status: Displays the status of a BCU in which an event occurred. `A` is displayed for the active system, and `s` is displayed for the standby system.

4. Event level (fixed as S6)

5. Message type

6. Account and terminal information (not displayed when they are not acquired)

7. Message text (maximum of 316 characters): Displays entered commands, command response messages, and configuration error messages.

   If the message contains a line feed, it is indicated by `^J`. In addition, a configuration error message might contain the detailed code at the end of the message.

1.1.4 Format of statistics logs

The following figure shows the format of statistics logs.

Figure 1-4: Format of statistics logs

```
1-b(c) ee kkkkkkkk [iii...iii] xxxxxxxx yy yyyyyyyyyyyy
 1 2  3     4          5           6      7

yyyy/mm/dd hh:mm:ss zzzz yyyy/mm/dd hh:mm:ss zzzz cccccccccc
          8                       9                   10
```

1. BCU number: Displays the number of a BCU-installed slot where an event occurred.

2. System status: Displays the status of a BCU in which an event occurred. `A` is displayed for the active system, and `S` is displayed for the standby system.

3. Event level (S0 to S7)

4. Message type

5. Message type details. Whether this information is displayed depends on the message type.

6. Message ID: Displays a unique ID for identifying messages.

7. Additional information: Displays event details as codes.

8. Occurrence date and time of the last event

9. Occurrence date and time of the first event

10. Number of events that occurred

1.2 System message components

1.2.1 Event level

Events that occurred are classified into eight levels according to their severity. The following table describes the event levels and their details.

If an event from the level S0 to S4 occurs, you need to take action. When an event whose event level is S5 occurs, we recommend that you check if any action needs to be taken.

Table 1-3: List of event levels

Event level	Description
S0	The entire device restarts.
S1	This error stops part of the hardware. (The relevant hardware restarts.)
S2	This error stops part of the software.
S3	Minor errors other than S1 and S2.
S4	Warning
S5	Note (part of normal operations is included.)
S6	Record of normal operations
S7	Record of each functionality in detail

1.2.2 Message types

The message type displays the location or functionality in which an event occurred. The following table shows a list of message types.

Table 1-4: List of message types

Message type	Event location or functionality
BCU	BCU
SFU	SFU
PRU	PRU
NIF	NIF
PS	Power supply unit
FAN	Fan
KEY	Input commands
CONFIGERR	Configuration error message
CMDRSP	Command response message
SOFTWARE	Software
CONFIG	Configuration
ACCESS	Access to the device
NTP	NTP, SNTP
SOP-KEY	Operation of system operation panel

Message type	Event location or functionality
SOP-RSP	System operation panel response message
SNMP	SNMP
PORT	Port
ChGr	Link aggregation
CFM	CFM
IP	IPv4, IPv6
PBR	Policy-based routing
DHCP	DHCP/BOOTP relay agent, DHCPv6 relay agent
VRRP	VRRPv4, VRRPv6
RIP	RIP
RIPng	RIPng
OSPF	OSPF
OSPFv3	OSPFv3
BGP4	BGP4
BGP4+	BGP4+
UNICAST	Unicast routing protocol (IPv4, IPv6)
PIM-IPv4	IPv4 PIM
IGMP	IGMP
PIM-IPv6	IPv6 PIM
MLD	MLD
MULTI-IPv4	IPv4 multicast routing protocol
MULTI-IPv6	IPv6 multicast routing protocol
MULTI-INFO	Multicast routing protocol

1.2.3 Message type details

If multiple locations of the same type exist in the device, the details of the location in which an event occurred are displayed. The details are displayed as either physical locations or numbers such as PRU or NIF, or as logical locations or numbers such as protocols. Whether details are displayed depends on the message type.

The following table lists the formats of displayed message type details.

Table 1-5: List of formats of displayed message type details

Formats of displayed message type details	Event location and displayed details
SFU:*<sfu no.>* [*<sfu type>*]	SFU *<sfu no.>*: SFU number *<sfu type>*: Abbreviated model name of SFU[#]

Formats of displayed message type details	Event location and displayed details
PRU:*<pru no.>* [*<pru type>*]	PRU *<pru no.>*: PRU number *<pru type>*: Abbreviated model name of PRU[#]
NIF:*<nif no.>* [*<nif type>*]	NIF *<nif no.>*: NIF number *<nif type>*: Abbreviated model name of NIF[#]
PORT: *<nif no.>*/*<port no.>*	Port *<nif no.>*: NIF number *<port no.>*: Port number
MGMT: 0	Management port
PS:*<ps no.>*	Power supply unit *<ps no.>*: The number of the slot on which the power supply unit is installed.
FAN:*<fan unit no.>*	Fan *<fan unit no.>*: Fan unit number
ChGr:*<channel group number>*	Channel group *<channel group number>*: Channel group number
VRID:*<vrid>*	Virtual router *<vrid>*: Virtual router ID
VRF:*<vrf id>*	VRF *<vrf id>*: VRF ID

#: The system message might omit the abbreviated model name.

Chapter

2. Hardware

2.1 BCU

The following table shows the system messages of the BCU message type.

Table 2-1: System messages of the BCU message type

Message ID	Event level	Message text
		Description and action
00003001	S6	The BCU restarted because the RESET switch was pressed.
		The BCU restarted because the RESET switch was pressed. [Action] None.
00003002	S6	The BCU restarted because of a default restart.
		The BCU restarted because of a default restart. [Action] None.
00003003	S0	The BCU restarted because the software detected a fatal error.
		The software detected a fatal error and restarted the BCU. [Action] Collect dump information, log information, and the configuration. For details about how to collect the information, see the *Troubleshooting Guide*.
00003004	S1	The BCU restarted because the software detected a fatal error.
		The software detected a fatal error and restarted the BCU. [Action] Collect dump information, log information, and the configuration. For details about how to collect the information, see the *Troubleshooting Guide*.
00003005	S6	The BCU restarted because of a user operation.
		The BCU was restarted by the reload command. [Action] None.
00003006	S0	The BCU restarted because the kernel detected a fatal software error.
		The kernel detected a fatal error in the software and restarted the BCU. [Action] Collect dump information, log information, and the configuration. For details about how to collect the information, see the *Troubleshooting Guide*.
00003007	S1	The BCU restarted because the kernel detected a fatal software error.
		The kernel detected a fatal error in the software and restarted the BCU. [Action] Collect dump information, log information, and the configuration. For details about how to collect the information, see the *Troubleshooting Guide*.
00003008	S0	The BCU restarted because of a WDT timeout.
		The BCU restarted because of a WDT (watchdog timer) timeout. [Action] Collect dump information, log information, and the configuration. For details about how to collect the information, see the *Troubleshooting Guide*.

Message ID	Event level	Message text
		Description and action
00003009	S1	The BCU restarted because of a WDT timeout.
	The BCU restarted because of a WDT (watchdog timer) timeout. [Action] Collect dump information, log information, and the configuration. For details about how to collect the information, see the *Troubleshooting Guide*.	
00003010	S0	The BCU restarted because the kernel detected a fatal hardware error.
	The kernel detected a fatal error in the hardware and restarted the BCU. [Action] Replace the BCU.	
00003011	S1	The BCU restarted because the kernel detected a fatal hardware error.
	The kernel detected a fatal error in the hardware and restarted the BCU. [Action] Replace the BCU.	
00003012	S0	The BCU restarted because the hardware detected a fatal hardware error.
	The BCU restarted because the hardware detected a fatal hardware error. [Action] Replace the BCU.	
00003013	S1	The BCU restarted because the hardware detected a fatal hardware error.
	The BCU restarted because the hardware detected a fatal hardware error. [Action] Replace the BCU.	
00003014	S6	The BCU restarted because of an auto restart by software.
	The BCU restarted because of an auto restart of the software. [Action] None.	
00003015	S6	The BCU restarted because the ACH switch was pressed.
	The BCU restarted because the ACH switch was pressed. [Action] None.	
00200100	S3	An access error was detected on the internal flash memory.
	An access error was detected on the internal flash memory. [Action] An access error was detected in the BCU-internal flash disk. Replace the BCU.	
01101001	S6	Initialization is complete.
	Initialization is complete. [Action] None.	

Message ID	Event level	Message text
		Description and action
01101002	S3	Initialization failed because the BCU is unknown.
		The BCU board cannot be initialized because the board is unknown. [Action] 1. Make sure that the BCU board is inserted properly. 2. The software version does not support the BCU board. Check the type of the BCU board and the version of the software, and replace the BCU board or update the software. 3. The Device does not support the BCU board. Replace the BCU board.
01101003	S6	The BCU will be restarted because of the user operation.
		A user operation will now restart the BCU. [Action] None.
01101004	S6	The BCU will be restarted because the RESET switch was pressed.
		The BCU will be restarted because the RESET switch was pressed. [Action] None.
01101005	S5	The BCU redundancy status changed from duplex to simplex.
		The BCU redundancy status changed from duplex to simplex. [Action] None.
01101006	S6	The BCU redundancy status changed from simplex to duplex.
		The BCU redundancy status changed from simplex to duplex. [Action] None.
01101007	S6	The other BCU went down.
		The BCU of the other system went down. [Action] None.
01101008	S6	The time was synchronized with the time of the active BCU.
		The time was matched to the time of the active system. This message appears only at the standby system. [Action] None.
01101009	S6	The standby BCU will be inactivated by a command operation.
		A command operation will now stop the standby BCU. [Action] None.
0110100a	S6	The standby BCU will be activated by a command operation.
		A command operation will now start the standby BCU. [Action] None.

Message ID	Event level	Message text
		Description and action
0110100b	S6	The standby BCU will be inactivated by an operation from the system operation panel.
	An operation from the system operation panel will now stop the standby BCU. [Action] None.	
0110100c	S6	The standby BCU will be activated by an operation from the system operation panel.
	An operation from the system operation panel will now start the standby BCU. [Action] None.	
0110100d	S5	The BCU was switched over from standby to active.
	The BCU was switched over from the standby to the active system. [Action] 1. There is no problem if a user operation caused the switchover. 2. In other cases, execute the `show logging` command or `show logging standby` command, check the error message, and then take action accordingly. If the new standby system has not yet started, wait a while, and then check the message.	
0110100e	S5	The BCU was switched over from active to standby.
	The BCU was switched over from the active to the standby system. [Action] 1. There is no problem if a user operation caused the switchover. 2. In other cases, execute the `show logging` command or `show logging standby` command, check the error message, and then take action accordingly. If the new standby system has not yet started, wait a while, and then check the message.	
0110100f	S6	The BCU will be restarted because of a BCU switchover occurred.
	The BCU will restart because the system switchover occurred while the system was not in a redundant configuration. This message appears in the new active system. [Action] None.	
01101010	S6	The BCU will be switched over from active to standby and restart, because the ACH switch was pressed.
	The BCU will be switched over from active to standby and restart, because the ACH switch was pressed. [Action] None.	
01101011	S3	A fatal error was detected on the other BCU.
	A fatal error occurred in the BCU of the other system. [Action] After the BCU of the other system restarts, execute the `show logging` command or `show logging standby` command, check the error details, and then take action accordingly.	

Message ID	Event level	Message text
		Description and action
01101012	S3	An error was detected by the health check between the active BCU and the standby BCU.
	An error was detected during a health check between BCUs. [Action] 1. The BCU board might not be inserted properly. If this message appears immediately after the board was replaced, check that it is properly inserted. 2. Restart the BCU that is thought to be the cause of the failure. After the restart, if the same failure does not occur, no further action is required. 3. After the restart, if the same failure occurs, replace the BCU of the restarted system. 4. If the above action does not resolve the above problem, replace the BCU of the other system. 5. If the above action does not resolve the above problem, replace the chassis.	
01101013	S3	An error was detected by a health check of the BCU.
	An error was detected by a health check of the BCU. [Action] 1. The BCU board might not be inserted properly. If this message appears immediately after the board was replaced, check that it is properly inserted. 2. Restart the BCU that is thought to be the cause of the failure. After the restart, if the same failure does not occur, no further action is required. 3. After the restart, if the same failure occurs, replace the BCU of the restarted system.	
01101014	S1	The BCU will be restarted because a hardware error was detected.
	The BCU will restart because a hardware failure was detected. [Action] Replace the BCU.	
01101015	S5	The BCU has been extracted.
	Removal of a BCU was detected. [Action] The BCU might have been removed or might not be inserted properly. Make sure that the BCU is inserted properly.	
01101016	S5	The BCU has been inserted.
	Insertion of a BCU was detected. [Action] None.	
01211001	S4	The inlet temperature of the device dropped to 2 degrees C or less, and a low temperature warning was detected.
	The intake temperature of the device dropped to 2 degrees Celsius or less, and a low-temperature warning was detected. [Action] Check and improve the environment around the device (for example, the room temperature).	
01211002	S6	The low temperature warning was cleared because the inlet temperature of the device rose to 5 degrees C or more.
	The intake temperature of the device rose to 5 degrees Celsius or more, so the device has recovered from the low-temperature warning. [Action] None.	

Message ID	Event level	Message text
		Description and action
01211003	S4	The inlet temperature of the device rose to 43 degrees C or more, and a high temperature warning was detected.
		The intake temperature of the device rose to 43 degrees Celsius or more, and a high-temperature warning was detected. [Action] 1. Check and improve the environment around the device (for example, the ventilation and heat sources). 2. Check the fans. If you find a failure, replace the fan unit containing the faulty fan.
01211004	S6	The high temperature warning was cleared because the inlet temperature of the device dropped to 40 degrees C or less.
		The intake temperature of the device dropped to 40 degrees Celsius or less, so the device has recovered from the high-temperature warning. [Action] None.
01211005	S4	The inlet temperature of the device rose to 53 degrees C or more, and is approaching a high temperature that might affect device operation.
		The intake temperature of the device rose to 53 degrees Celsius or more, nearing the temperature that could affect the device operation. [Action] 1. A malfunction might occur in the device. Immediately check and improve the environment around the device (for example, the ventilation and heat sources). 2. Check the fans. If you find a failure, replace the fan unit containing the faulty fan.
01211006	S6	The inlet temperature of the device has been restored to 50 degrees C or less from a temperature that could have affected device operation. Care must still be taken because the temperature is still over the recommended maximum.
		The intake temperature of the device has dropped to 50 degrees Celsius or less from a temperature that affects device operation. However, care must be taken because the temperature is still higher than the allowable range. [Action] 1. Check and improve the environment around the device (for example, the ventilation and heat sources). 2. Check the fans. If you find a failure, replace the fan unit containing the faulty fan.
01211007	S3	The inlet temperature of the device rose to 65 degrees C or more, and has reached a temperature that might severely damage the device.
		The intake temperature of the device rose to 65 degrees Celsius or more, and has reached a temperature that might severely damage the device. [Action] 1. Immediately check and improve the environment around the device (for example, the ventilation and heat sources). 2. Check the fans. If you find a failure, replace the fan unit containing the faulty fan.
01211008	S1	The BCU will stop because of a hardware failure.
		The BCU will stop because a hardware failure was detected. [Action] Replace the BCU.

Message ID	Event level	Message text
		Description and action
01211009	S6	The inlet temperature of the device rose to greater than or equal to the temperature set by the 'system temperature-warning-level' configuration command.(temperature = <*temperature*> degrees C)
	The intake temperature of the device rose to greater than or equal to the temperature that is set by using the `system temperature-warning-level` configuration command. • <*temperature*>: Temperature of the device (in Celsius). [Action] The temperature of the device has reached the specified temperature. Check the environment surrounding the device (for example, the condition of the fan, ventilation, and existence of the heat sources).	
0121100a	S6	The inlet temperature of the device dropped 3 degrees C or more from the temperature set by the 'system temperature-warning-level' configuration command.
	The intake temperature of the device dropped by 3 degrees Celsius or more from the temperature set by using the `system temperature-warning-level` configuration command. [Action] None.	
0121100b	S6	The mean inlet temperature of the device rose to greater than or equal to temperature set by the 'system temperature-warning-level average' configuration command.(temperature = <*average temperature*> degrees C)
	The average intake temperature of the device rose to greater than or equal to the temperature that is set by using the `system temperature-warning-level average` configuration command. • <*average temperature*>Temperature of the device (in Celsius). [Action] The average intake temperature of the device has reached the specified temperature. Check the environment surrounding the device (for example, the condition of the fan, ventilation, and existence of the heat sources).	
0122100c	S3	Access to the BCU statistics failed.
	Access to the total operating time for the BCU failed. [Action] This event does not affect communication and usual operation. However, you cannot use the total operating time management function. If you want to use this function, replace the BCU.	
0122100d	S6	Access to the BCU statistics finished successfully.
	Access to the total operating time for the BCU is complete. [Action] None.	
0122100e	S4	The BCU-CPU memory usage exceeded 98%.
	The BCU-CPU memory usage exceeded 98%. [Action] 1. If many users are logged in, log out all but the most essential users. 2. If there is a lot of use from ftp, disconnect all but the most essential connections. 3. If there is too much access from the network management device, limit the amount of access to the minimum necessary. 4. If the above actions do not recover the system, the capacity limit of the Device might not be satisfied. Revise the network configuration.	
0122100f	S6	The BCU-CPU memory usage fell below 95%.
	The BCU-CPU memory usage fell below 95%. [Action] None.	

Message ID	Event level	Message text
		Description and action
09200001	S1	The BCU will restart because a configuration software error occurred.
	The BCU will restart because a configuration software error occurred. [Action] Check the log by executing the `show logging` command. If the log indicates that another failure occurred, take appropriate action according to the error message.	
09300001	S1	The BCU will restart because a configuration software error occurred.
	The BCU will restart because a configuration software error occurred. [Action] Check the log by executing the `show logging` command. If the log indicates that another failure occurred, take appropriate action according to the error message.	
09400001	S1	The BCU will restart because a configuration software error occurred.
	The BCU will restart because a configuration software error occurred. [Action] Check the log by executing the `show logging` command. If the log indicates that another failure occurred, take appropriate action according to the error message.	
09500001	S1	The BCU will restart because a configuration software error occurred.
	The BCU will restart because a configuration software error occurred. [Action] Check the log by executing the `show logging` command. If the log indicates that another failure occurred, take appropriate action according to the error message.	
09600001	S1	The BCU will restart because a configuration software error occurred.
	The BCU will restart because a configuration software error occurred. [Action] Check the log by executing the `show logging` command. If the log indicates that another failure occurred, take appropriate action according to the error message.	
25011001	S6	The port status is Up.
	The port status is Up. [Action] None.	
25011002	S6	The port was inactivated by configuration.
	The port was inactivated by the `shutdown` configuration command. [Action] None.	
25011003	S6	The port was activated by configuration.
	The port was activated by the `no shutdown` configuration command. [Action] None.	
25011004	S6	The port was inactivated by an operation command.
	The port was inactivated by the `inactivate` command. [Action] None.	

Message ID	Event level	Message text
		Description and action
25011005	S6	The port was activated by an operation command.
	The port was activated by the `activate` command. [Action] None.	
25011201	S5	An error was detected on the port.
	An error was detected on the port. [Action] 1. Make sure that the specified cables are properly connected. 2. Make sure that the remote device is running.	
35000101	S6	Past event information was initialized because the BCU was switched over from active to standby.
	Past event information was initialized because the Device was switched from the active BCU to the standby BCU. This message appears only for at standby BCU. [Action] None.	
35010001	S1	The BCU will restart because a hardware error was detected.
	The BCU will restart because a hardware failure was detected. [Action] Replace the BCU.	
35020401	S4	The PA memory usage exceeded 98%.
	The PA memory usage exceeded 98%. [Action] If the PA memory usage does not drop for a long time, restart the BCU.	
35020402	S6	The PA memory usage fell below 95%.
	The PA memory usage fell below 95%. [Action] None.	
350d0101	S6	The HDC on the BCU will be updated. Do not remove the BCU.
	The HDC (Hardware Dependent Code) will be updated. [Action] Do not remove the BCU.	
350d0102	S6	The BCU will restart because its HDC was updated.
	The BCU will restart because its HDC (Hardware Dependent Code) was updated. [Action] None.	
350d0103	S3	The HDC update was unsuccessful on the BCU.
	The HDC (Hardware Dependent Code) update failed. [Action] 1. Update the HDC again by using the `update software` command. 2. If the update fails again, the BCU might be the cause of the failure. Replace the BCU.	

Message ID	Event level	Message text
		Description and action
350e0201	S6	The PA online dump command was executed.
	Collection of the memory dump, initiated by executing the PA dump (without a BCU restart) command, is complete. [Action] None.	
350e0203	S6	Collection of the PA dump was canceled.
	Collection of the dump was canceled. [Action] None.	

2.2 SFU

The following table shows the system messages of the SFU message type.

Table 2-2: System messages of the SFU message type

Message ID	Event level	Message text
		Description and action
35050001	S6	The SFU was activated by a configuration command.
	The SFU was activated by the `power enable` configuration command. [Action] None.	
35050002	S6	The SFU was inactivated by a configuration command.
	The SFU was inactivated by the `no power enable` configuration command. [Action] None.	
35050003	S5	The SFU has been extracted.
	Removal of an SFU was detected. [Action] The SFU might have been removed or might not be inserted properly. Make sure that the SFU is inserted properly.	
35050004	S5	The SFU has been inserted.
	Insertion of a SFU was detected. [Action] None.	
35050101	S6	The SFU initialization is complete.
	The SFU initialization is complete. [Action] None.	
35050102	S6	The SFU termination is complete.
	The SFU termination is complete. [Action] None.	
35050103	S3	The SFU could not be initialized because the SFU was unknown.
	The SFU could not be initialized because the SFU was unknown. [Action] 1. Make sure that the SFU is inserted properly. 2. The software version does not support the SFU. Check the type of the SFU and the software version, and replace the SFU or update the software. 3. The Device does not support the SFU. Replace the SFU.	
35050201	S1	The SFU will stop because of a hardware failure.
	A hardware failure has been detected in the SFU. The SFU will now stop. [Action] Replace the SFU.	

Message ID	Event level	Message text
		Description and action
35050202	S1	A hardware failure was detected during SFU self-diagnosis. The SFU will restart.
	A failure was detected during SFU self-diagnosis. The SFU will restart. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the SFU.		
35050203	S6	The SFU recovered from a hardware failure detected during self-diagnosis.
	The SFU recovered from a failure detected during self-diagnosis. [Action] None.		
35050204	S1	The SFU will restart because of a hardware failure.
	The SFU will restart because a hardware failure occurred. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the SFU.		
35050205	S6	The SFU recovered from a hardware failure.
	The SFU recovered from a hardware failure. [Action] None.		
35050206	S1	The SFU restarted, but has not recovered from a hardware failure.
	The SFU restarted, but has not recovered from the hardware failure or the failure detected during self-diagnosis. [Action] Replace the SFU.		
35050301	S6	The HDC on the SFU will be updated. Do not remove the SFU.
	The HDC (Hardware Dependent Code) will be updated. [Action] Do not remove the SFU until either of the following messages is displayed: • Message type: SFU Message ID: 35050302 • Message type: SFU Message ID: 35050304		
35050302	S6	The SFU will restart because its HDC was updated.
	The SFU will restart because its HDC (Hardware Dependent Code) was updated. [Action] None.		
35050303	S3	The HDC update was unsuccessful on the SFU.
	The HDC (Hardware Dependent Code) update failed. [Action] 1. Update the HDC again by using the update software command. 2. If the update fails again, the SFU might be the cause of the failure. Replace the SFU.		
35050304	S5	The HDC on the SFU was updated, and will be applied after restarting the SFU.
	The HDC (Hardware Dependent Code) was updated, but has not been applied to operations. [Action] Restart the SFU.		

Message ID	Event level	Message text
		Description and action
35050501	S3	Access to the SFU statistics failed.
		Access to the total operating time for the SFU failed. [Action] This event does not affect communication and usual operation. However, you cannot use the total operating time management function. If you want to use this function, replace the SFU.
35050502	S6	Access to the SFU statistics finished successfully.
		Access to the total operating time for the SFU is complete. [Action] None.
350e0501	S6	The SFU online dump command was executed.
		Collection of the memory dump, initiated by executing the SFU dump (without an SFU restart) command, is complete [Action] None.
350e0502	S6	The SFU offline dump command was executed.
		Collection of the memory dump, initiated by executing the SFU dump (with an SFU restart) command, is complete. [Action] None.
350e0503	S6	Collection of the SFU dump was canceled.
		Collection of the dump was canceled. [Action] None.
35400501	S6	The SFU was inactivated by an operation command.
		The SFU was inactivated by the `inactivate` command. [Action] None.
35400502	S6	The SFU was activated by an operation command.
		The SFU was activated by the `activate` command. [Action] None.

2.3 PRU

The following table shows the system messages of the PRU message type.

Table 2-3: System messages of the PRU message type

Message ID	Event level	Message text
		Description and action
35060001	S6	The PRU was activated by a configuration command.
	The PRU was activated by the `power enable` configuration command. [Action] None.	
35060002	S6	The PRU was inactivated by a configuration command.
	The PRU was inactivated by the `no power enable` configuration command. [Action] None.	
35060003	S5	The PRU has been extracted.
	Removal of a PRU was detected. [Action] The PRU might have been removed or might not be inserted properly. Make sure that the PRU is inserted properly.	
35060004	S5	The PRU has been inserted.
	Insertion of a PRU was detected. [Action] None.	
35060101	S6	The PRU initialization is complete.
	The PRU initialization is complete. [Action] None.	
35060102	S6	The PRU termination is complete.
	The PRU termination is complete. [Action] None.	
35060103	S3	The PRU could not be initialized because the PRU was unknown.
	The PRU could not be initialized because the PRU was unknown. [Action] 1. Make sure that the PRU is inserted properly. 2. The software version does not support the PRU. Check the type of the PRU and the software version, and replace the PRU or update the software. 3. The Device does not support the PRU. Replace the PRU.	

Message ID	Event level	Message text
		Description and action
35060104	S3	The PRU could not be initialized because the power supply was insufficient.
	The PRU could not be initialized because the power supply was insufficient. [Action] 1. Check the implementation and operation status of the power supply unit. If the power supply units that are running normally are insufficient, add new power supply units. For details about how to add power supply units, see the *Hardware Instruction Manual*. 2. After adding the power supply units, restart the PRU by using the `activate pru` command.	
35060201	S1	The PRU will stop because of a hardware failure.
	A hardware failure was detected in the PRU. The PRU will now stop. [Action] Replace the PRU.	
35060202	S1	A hardware failure was detected during PRU self-diagnosis. The PRU will restart.
	A failure was detected during PRU self-diagnosis. The PRU will now restart. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the PRU.	
35060203	S6	The PRU recovered from a hardware failure detected during self-diagnosis.
	The PRU recovered from a failure detected during self-diagnosis. [Action] None.	
35060204	S1	The PRU will restart because of a hardware failure.
	The PRU will restart because a hardware failure occurred. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the PRU.	
35060205	S6	The PRU recovered from a hardware failure.
	The PRU recovered from a hardware failure. [Action] None.	
35060206	S1	The PRU restarted, but has not recovered from a hardware failure.
	The PRU restarted, but has not recovered from a hardware failure or a failure detected during self-diagnosis. [Action] Replace the PRU.	
35060208	S1	The PRU will restart because of a software failure.
	The PRU will restart because a software failure occurred. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the PRU.	
35060209	S6	The PRU recovered from a software failure.
	The PRU recovered from a software failure. [Action] None.	

Message ID	Event level	Message text
		Description and action
3506020a	S1	The PRU restarted, but has not recovered from a software failure.
		The PRU restarted, but has not recovered from a software failure. [Action] Replace the PRU.
35060301	S6	The HDC on the PRU will be updated. Do not remove the PRU.
		The HDC (Hardware Dependent Code) will be updated. [Action] Do not remove the PRU until either of the following messages is displayed: • Message type: PRU Message ID: 35060302 • Message type: PRU Message ID: 35060304
35060302	S6	The PRU will restart because its HDC was updated.
		The PRU will restart because its HDC (Hardware Dependent Code) was updated. [Action] None.
35060303	S3	The HDC update was unsuccessful on the PRU.
		The HDC (Hardware Dependent Code) update failed. [Action] 1. Update the HDC again by using the update software command. 2. If the update fails again, the PRU might be the cause of the failure. Replace the PRU.
35060304	S5	The HDC on the PRU was updated, and will be applied after restarting the PRU.
		The HDC (Hardware Dependent Code) was updated, but has not been applied to operations. [Action] Restart the PRU.
35060401	S4	The PRU memory usage exceeded 98%.
		The PRU memory usage exceeded 98%. [Action] If the PRU memory usage does not drop for a long time, restart the PRU.
35060402	S6	The PRU memory usage fell below 95%.
		The PRU memory usage fell below 95%. [Action] None.
35060501	S3	Access to the PRU statistics failed.
		Access to the total operating time for the PRU failed. [Action] This event does not affect communication and usual operation. However, you cannot use the total operating time management function. If you want to use this function, replace the PRU.
35060502	S6	Access to the PRU statistics finished successfully.
		Access to the total operating time for the PRU is complete. [Action] None.

Message ID	Event level	Message text
		Description and action
350e0601	S6	The PRU online dump command was executed.
	Collection of the memory dump, initiated by executing the PRU dump (without a PRU restart) command, is complete. [Action] None.	
350e0602	S6	The PRU offline dump command was executed.
	Collection of the memory dump, initiated by executing the PRU dump (with a PRU restart) command, is complete. [Action] None.	
350e0603	S6	Collection of the PRU dump was canceled.
	Collection of the dump was canceled. [Action] None.	
35400601	S6	The PRU was inactivated by an operation command.
	The PRU was inactivated by the `inactivate` command. [Action] None.	
35400602	S6	The PRU was activated by an operation command.
	The PRU was activated by the `activate` command. [Action] None.	
3f000001	S4	The number of shared resources exceeded the *<percent>*% of the PRU capacity.
	The usage amount for resources on the input side exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] Make sure that the amount of usage of resources on the input side does not exceed the capacity limit.	
3f000002	S3	The number of shared resources has reached the capacity of the PRU.
	The amount of usage of resources on the input side has reached the capacity limit. [Action] Review the system configuration. For details about the action to be taken when the usage exceeds the capacity limit, see the *Troubleshooting Guide*.	
3f000003	S6	The number of shared resources has fell below the *<percent>*% of the PRU capacity.
	The amount of usage of resources on the input side has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.	

Message ID	Event level	Message text
		Description and action
3f000004	S4	The number of outbound forwarding resources exceeded the *<percent>*% of the PRU capacity.
		The number of entries being used in the Outbound forwarding resources table exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] Make sure that the number of entries being used in the Outbound forwarding resources table does not exceed the capacity limit.
3f000005	S3	The number of outbound forwarding resources has reached the capacity of the PRU.
		The number of entries being used in the Outbound forwarding resources table has reached the capacity limit. [Action] Review the system configuration. For details about the action to be taken when the number of entries exceeds the capacity limit, see the *Troubleshooting Guide*.
3f000006	S6	The number of outbound forwarding resources has fell below the *<percent>*% of the PRU capacity.
		The number of entries used in the Outbound forwarding resources table fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.
3f000007	S4	The number of destination resources exceeded the *<percent>*% of the PRU capacity.
		The number of destination resources in use exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] Make sure that the number of destination resources does not exceed the capacity limit.
3f000008	S3	The number of destination resources has reached the capacity of the PRU.
		The number of destination resources in use reached the capacity limit. [Action] Review the system configuration. For details about the action to be taken when the usage exceeds the capacity limit, see the *Troubleshooting Guide*.
3f000009	S6	The number of destination resources has fell below the *<percent>*% of the PRU capacity.
		The number of destination resources in use has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.

Message ID	Event level	Message text
		Description and action
40100001	S4	Some advance access-lists cannot be set.
	An advance access-list could not be applied to a PRU interface. [Action] Either restart the PRU and then apply the flow detection mode, or delete the advance access-list that is applied to the interface.	
40100002	S4	The number of filter entries exceeded *\<percent>*% of the PRU capacity.
	The number of filter entries exceeded *\<percent>*% of the capacity limit. • *\<percent>*: percent 80, 85, 90, 95 [Action] To add more filter entries, make sure that the number of entries does not exceed the PRU capacity limit.	
40100003	S3	The number of filter entries has reached the capacity of the PRU.
	The number of filter entries has reached the capacity limit. [Action] Review the system configuration because entries added after the capacity limit is reached are not set.	
40100004	S3	The number of filter entries exceeded the PRU capacity.
	The number of filter entries exceeded the capacity limit. [Action] Restart the PRU, and then apply the flow detection mode and flow distribution pattern.	
40100005	S6	The number of filter entries has fell below the *\<percent>*% of the PRU capacity.
	The number of filter entries has fallen below *\<percent>*% of the capacity limit. • *\<percent>*: percent 75, 80, 85, 90, 95 [Action] None.	
40200001	S4	Some advance qos-flow-lists cannot be set.
	A `advance qos-flow-lists` could not be applied to a PRU interface. [Action] Either restart the PRU and then apply the flow detection mode, or delete the `advance qos-flow-list` that is applied to the interface.	
40200002	S4	The number of QoS entries exceeded *\<percent>*% of the PRU capacity.
	The number of QoS entries exceeded *\<percent>*% of the capacity limit. • *\<percent>*: percent 80, 85, 90, 95 [Action] To add more QoS entries, make sure that the number of entries does not exceed the PRU capacity limit.	
40200003	S3	The number of QoS entries has reached the capacity of the PRU.
	The number of QoS entries has reached the capacity limit. [Action] Review the system configuration because entries added after the capacity limit is reached are not set.	
40200004	S3	The number of QoS entries exceeded the PRU capacity.
	The number of QoS entries exceeded the capacity limit. [Action] Restart the PRU, and then apply the flow detection mode and flow distribution pattern.	

Message ID	Event level	Message text
		Description and action
40200005	S6	The number of QoS entries has fell below the *<percent>*% of the PRU capacity.
		The number of QoS entries has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.
41011001	S4	The number of IPv4 unicast routing entries exceeded *<percent>*% of the PRU capacity.
		The number of IPv4 unicast routing entries exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] When adding more IPv4 unicast routing entries, make sure that the number of entries does not exceed the PRU capacity.
41011002	S4	The number of IPv4 unicast routing entries has reached the capacity of the PRU.
		The number of IPv4 unicast routing entries has reached the capacity limit. [Action] Review the system configuration because entries added after the capacity limit is reached are not set. For details about the action to be taken when the number of entries exceeds the capacity limit, see the *Troubleshooting Guide*.
41011003	S6	The number of IPv4 unicast routing entries has fell below the *<percent>*% of the PRU capacity.
		The number of IPv4 unicast routing entries has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.
41012001	S4	The number of IPv6 unicast routing entries exceeded *<percent>*% of the PRU capacity.
		The number of IPv6 unicast routing entries exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] When adding more IPv6 unicast routing entries, make sure that the number of entries does not exceed the PRU capacity.
41012002	S4	The number of IPv6 unicast routing entries has reached the capacity of the PRU.
		The number of IPv6 unicast routing entries has reached the capacity limit. [Action] Review the system configuration because entries added after the capacity limit is reached are not set. For details about the action to be taken when the number of entries exceeds the capacity limit, see the *Troubleshooting Guide*.

Message ID	Event level	Message text
		Description and action
41012003	S6	The number of IPv6 unicast routing entries has fell below the *<percent>*% of the PRU capacity.
	The number of IPv6 unicast routing entries has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.	
41021001	S4	The number of IPv4 multicast routing entries exceeded *<percent>*% of the PRU capacity.
	The number of IPv4 multicast routing entries exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] When adding more IPv4 multicast routing entries, make sure that the number of entries does not exceed the PRU capacity.	
41021002	S4	The number of IPv4 multicast routing entries has reached the capacity of the PRU.
	The number of IPv4 multicast routing entries has reached the capacity limit. [Action] Review the system configuration because entries added after the capacity limit is reached are not set. For details about the action to be taken when the number of entries exceeds the capacity limit, see the *Troubleshooting Guide*.	
41021003	S6	The number of IPv4 multicast routing entries has fell below the *<percent>*% of the PRU capacity.
	The number of IPv4 multicast routing entries has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.	
41022001	S4	The number of IPv6 multicast routing entries exceeded *<percent>*% of the PRU capacity.
	The number of IPv6 multicast routing entries exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] When adding more IPv6 multicast routing entries, make sure that the number of entries does not exceed the PRU capacity.	
41022002	S4	The number of IPv6 multicast routing entries has reached the capacity of the PRU.
	The number of IPv6 multicast routing entries has reached the capacity limit. [Action] Review the system configuration because entries added after the capacity limit is reached are not set. For details about the action to be taken when the number of entries exceeds the capacity limit, see the *Troubleshooting Guide*.	

Message ID	Event level	Message text
		Description and action
41022003	S6	The number of IPv6 multicast routing entries has fell below the *<percent>*% of the PRU capacity.
	The number of IPv6 multicast routing entries has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.	
41023001	S4	The total number of outgoing interfaces of multicast forwarding entries exceeded *<percent>*% of PRU capacities.
	The total number of downstream interfaces of multicast forwarding entries exceeded *<percent>*% of the capacity limit. • *<percent>*: percent 80, 85, 90, 95 [Action] When adding more downstream interfaces to multicast forwarding entries, make sure that the number of the interfaces does not exceed the PRU capacity.	
41023002	S4	The total number of outgoing interfaces of multicast forwarding entries has reached the capacity of the PRU.
	The total number of downstream interfaces of multicast forwarding entries has reached the capacity limit. [Action] Review the system configuration because downstream interfaces added after the capacity limit is reached are not set. For details about the action to be taken when the number of downstream interfaces exceeds the capacity limit, see the *Troubleshooting Guide*.	
41023003	S6	The total number of outgoing interfaces of multicast forwarding entries has fell below the *<percent>*% of the PRU capacity.
	The total number of downstream interfaces of multicast forwarding entries has fallen below *<percent>*% of the capacity limit. • *<percent>*: percent 75, 80, 85, 90, 95 [Action] None.	

2.4 NIF

The following table shows the system messages of the `NIF` message type.

Table 2-4: System messages of the NIF message type

Message ID	Event level	Message text
		Description and action
25010008	S6	The port recovered from a hardware failure.
	The port recovered from a hardware failure. [Action] None.	
25010009	S1	The port restarted but has not recovered from a hardware failure.
	The port restarted but has not recovered from a hardware failure. [Action] Replace the NIF.	
25010109	S1	The port will restart because of a hardware failure.
	The port will restart because hardware failure occurred. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the NIF.	
35070001	S6	The NIF was activated by a configuration command.
	The NIF was activated by the `power enable` configuration command. [Action] None.	
35070002	S6	The NIF was inactivated by a configuration command.
	The NIF was inactivated by the `no power enable` configuration command. [Action] None.	
35070003	S5	The NIF has been extracted.
	Removal of a NIF was detected. [Action] The NIF might have been removed or might not be inserted properly. Make sure that the NIF is inserted properly.	
35070004	S5	The NIF has been inserted.
	Insertion of a NIF was detected. [Action] None.	
35070101	S6	The NIF initialization is complete.
	The NIF initialization is complete. [Action] None.	

Message ID	Event level	Message text
		Description and action
35070102	S6	The NIF termination is complete.
	The NIF termination is complete. [Action] None.	
35070103	S3	The NIF could not be initialized because the NIF was unknown.
	The The NIF could not be initialized because the NIF was unknown. [Action] 1. Make sure that the NIF is inserted properly. 2. The software version does not support the NIF. Check the type of the NIF and the software version, and replace the NIF or update the software. 3. The Device does not support the NIF. Replace the NIF.	
35070104	S3	The NIF could not be initialized because the power supply was insufficient.

	The NIF could not be initialized because the power supply was insufficient
	[Action]
	1. Check the implementation and operation status of the power supply unit.
	    If the power supply units that are running normally are insufficient, add new power supply units.
	    For details about how to add power supply units, see the *Hardware Instruction Manual*.
	2. After adding the power supply units, restart the NIF by using the `activate nif` command.	

35070201	S1	The NIF will stop because of a hardware failure.
	A hardware failure was detected in the NIF. The NIF will now stop. [Action] Replace the NIF.	
35070202	S1	A hardware failure was detected during NIF self-diagnosis. The NIF will restart.
	A failure was detected during NIF self-diagnosis. The NIF will restart. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the NIF.	
35070203	S6	The NIF recovered from a hardware failure detected during self-diagnosis.
	The NIF recovered from a failure detected during self-diagnosis. [Action] None.	
35070204	S1	The NIF will restart because of a hardware failure.
	The NIF will restart because a hardware failure occurred. [Action] After the restart, check the messages and make sure the recovery from the failure was successful. If the recovery was successful, operations can resume. If the recovery failed, replace the NIF.	
35070205	S6	The NIF recovered from a hardware failure.
	The NIF recovered from the hardware failure. [Action] None.	

Message ID	Event level	Message text
		Description and action
35070206	S1	The NIF restarted, but has not recovered from a hardware failure.
	The NIF restarted, but has not recovered from a hardware failure or a failure detected during self-diagnosis. [Action] Replace the NIF.	
35070301	S6	The HDC on the NIF will be updated. Do not remove the NIF.
	The HDC (Hardware Dependent Code) will be updated. [Action] Do not remove the NIF until either of the following messages is displayed: • Message type: NIF Message ID: 35070302 • Message type: NIF Message ID: 35070304	
35070302	S6	The NIF will restart because its HDC was updated.
	The NIF will restart because its HDC (Hardware Dependent Code) was updated. [Action] None.	
35070303	S3	The HDC update was unsuccessful on the NIF.
	The HDC (Hardware Dependent Code) update failed. [Action] 1. Update the HDC again by using the update software command. 2. If the update fails again, the NIF might be the cause of the failure. Replace the NIF.	
35070304	S5	The HDC on the NIF was updated, and to be applied after restarting the NIF.
	The HDC (Hardware Dependent Code) was updated, but has not been applied to operations. [Action] Restart the NIF.	
35070501	S3	Access to the NIF statistics failed.
	Access to the total operating time for the NIF failed. [Action] This event does not affect communication and usual operation. However, you cannot use the total operating time management function. If you want to use this function, replace the NIF.	
35070502	S6	Access to the NIF statistics finished successfully.
	Access to the total operating time for the NIF is complete. [Action] None.	
350e0701	S6	The NIF online dump command was executed.
	Collection of the memory dump, initiated by executing the NIF dump (without a NIF restart) command, is complete [Action] None.	
350e0702	S6	The NIF offline dump command was executed.
	Collection of the memory dump, initiated by executing the NIF dump (with a NIF restart) command, is complete [Action] None.	

Message ID	Event level	Message text
		Description and action
350e0703	S6	Collection of the NIF dump was canceled.
	Collection of the dump was canceled. [Action] None.	
35400701	S6	The NIF was inactivated by an operation command.
	The NIF was inactivated by the `inactivate` command. [Action] None.	
35400702	S6	The NIF was activated by an operation command.
	The NIF was activated by the `activate` command. [Action] None.	

2.5 PS

The following table shows the system messages of the PS message type.

Table 2-5: System messages of the PS message type

Message ID	Event level	Message text
		Description and action
01202001	S6	The power supply unit is normal.
	The power supply unit is normal. [Action] None.	
01202002	S1	A fatal error was detected in the power supply unit.
	A failure was detected in the power supply unit. [Action] Replace the power supply unit.	
01202003	S3	The power supply unit is not supported.
	The mounted power supply unit is not supported. [Action] Replace the current power supply unit with a supported model.	
01202004	S6	The power supply unit is not connected.
	A power supply unit is not mounted. [Action] None.	
01202005	S6	The power supply unit is powered off.
	The power supply unit has stopped supplying power. [Action] None.	
01202006	S3	A mix of AC and DC power supply units are mounted.
	A mix of AC and DC power supply units are mounted. [Action] Mount power supply units that are either all for AC power or all for DC power.	
01202007	S3	A mix of AC 100 V and AC 200 V power supply units are mounted.
	A mix of AC 100 V and AC 200 V power supply units are mounted. [Action] Mount power supply units that are either all AC 100 V AC or all AC 200 V.	
01202008	S6	The combination of power supply units is correct.
	The combination of mounted power supply units is correct. [Action] None.	
01202009	S3	The power supply is insufficient.
	The power supply is insufficient. [Action] Mount power supply units so that sufficient power supply is available for use.	

Message ID	Event level	Message text
		Description and action
0120200a	S6	The power supply is now sufficient.
		The power supply is now sufficient. [Action] None.
0120200b	S5	The power supply units are not in a redundant configuration.
		The power supply units are not in a redundant configuration. This message is output when the `power redundancy-mode` configuration command is set. [Action] When a redundant power supply unit is required, check if the power supply status of the device is normal by using the `show environment` command.
0120200c	S6	The power supply units are in a redundant configuration.
		The power supply units are in a redundant configuration. This message is output when the `power redundancy-mode` configuration command is set. [Action] None.
0120200d	S5	The power available is insufficient from input source A.
		The power available is insufficient from input source A. This message is output when 2 (redundant power supply unit and redundant power feed) is specified by using the `power redundancy-mode` configuration command. [Action] When the redundant power feed is required, check if the power supply status of the device is normal by using the `show environment` command.
0120200e	S6	The power available is now sufficient from input source A.
		The power available is now sufficient from input source A. This message is output if 2 (redundant power supply unit and redundant power feed) is specified by using the `power redundancy-mode` configuration command. [Action] None.
0120200f	S5	The power available is insufficient from input source B.
		The power available is insufficient from input source B. This message is output if 2 (redundant power supply unit and redundant power feed) is specified by using the `power redundancy-mode` configuration command. [Action] If the redundant power feed is required, check if the power supply status of the device is normal by using the `show environment` command.
01202010	S6	The power available is now sufficient from input source B.
		The power available is now sufficient from input source B. This message is output if 2 (redundant power supply unit and redundant power feed) is specified by using the `power redundancy-mode` configuration command. [Action] None.
01222011	S3	Access to the power supply unit statistics failed.
		Access to the total operating time for the power supply unit failed. [Action] This event does not affect communication and usual operation. However, you cannot use the total operating time management function. If you want to use this function, replace the power supply unit.

Message ID	Event level	Message text
		Description and action
01222012	S6	Access to the power supply unit statistics finished successfully.
	Access to the total operating time for the power supply unit is complete. [Action] None.	

2.6 FAN

The following table shows the system messages of the FAN message type.

Table 2-6: System messages of the FAN message type

Message ID	Event level	Message text
		Description and action
01213001	S6	The fan unit is normal.
	The fan unit is now operating normally. [Action] None.	
01213002	S3	A problem occurred in a fan.
	A problem occurred in a fan. Replace the fan unit. [Action] Replace the fan unit.	
01213003	S1	The fan unit is not working.
	The fan has stopped. Replace the fan unit immediately. [Action] Replace the fan unit immediately.	
01213004	S1	The fan unit is not connected.
	The fan unit is not mounted. [Action] 1. If you are replacing the fan unit, continue with the replacement. 2. If you are not performing the replacement, check the mounting status. If the fan unit is not mounted, mount it. 3. Make sure that the fan unit is inserted properly. 4. If (3) above does not start the recovery, replace the fan unit.	
01213005	S3	The fan unit is not supported.
	The mounted fan unit is not supported. [Action] Replace the fan unit with a model that is supported by the device.	
01213006	S4	The fan speed was changed to high.
	The fan speed was changed to high because of a fan failure. [Action] None.	
01213007	S6	The fan speed has returned to normal.
	High-speed operation of the fan was canceled. [Action] None.	
01213008	S3	The fan speed failed to change.
	The fan speed failed to change. [Action] Replace the fan unit.	

Message ID	Event level	Message text
		Description and action
01223009	S3	Access to the fan unit statistics failed.
	Access to the total operating time for the fan unit failed. [Action] Cooling functionality of the fan is not affected. However, you cannot use the total operating time management function. If you want to use this function, replace the fan unit.	
0122300a	S6	Access to the fan unit statistics finished successfully.
	Access to the total operating time for the fan unit is complete. [Action] None.	

Chapter

3. Operation Management

3.1 SOFTWARE

The following table shows the system messages of the SOFTWARE message type.

Table 3-1: System messages of the SOFTWARE message type

Message ID	Event level	Message text
		Description and action
01100001	S1	The BCU will be restarted because a software error occurred.
		The BCU will restart because a software error occurred. [Action] Check the log by executing the show logging command. If other failures are indicated in the log, take appropriate action according to the error message.
01100002	S5	The software versions of the active BCU and the standby BCU are different.
		The software versions of the active system and the standby system are different. [Action] 1. There is no problem if the software is being updated. 2. In other cases, update the software so that the software versions of the active system and the standby system match. For details about how to update the software, see the *Software Installation Guide*.
01100003	S6	The mismatch of software versions recovered.
		The inconsistency between the software versions of the active system and the standby system has been resolved. This message is displayed if, while the software versions do not match. the BCU of the other system goes down. [Action] None.
01200002	S1	The BCU will be restarted because a software error occurred.
		The BCU will restart because a software error occurred. [Action] Check the log by executing the show logging command. If other failures are indicated in the log, take appropriate action according to the error message.
01220001	S3	Writing of temperature log data failed.
		Writing of the temperature log failed. [Action] 1. Check the user area of the internal flash memory. 2. If the free space is lacking, delete unnecessary files to ensure free space (approximately 8 KB).
01300001	S5	The CPU usage statistics were initialized because a change in the system time of 5 seconds or more was detected.
		The statistics table that holds the CPU usage was initialized because a time change of 5 seconds or more was detected. [Action] None.
01400001	S6	The software started.
		The software has started. [Action] None.

Message ID	Event level	Message text
		Description and action
01400002	S7	Reference logs will now be acquired.
	The system started collecting statistics logs. [Action] None.	
01400003	S1	The BCU will be restarted because a software error occurred.
	The BCU will restart because a software error occurred. [Action] Check the log by executing the show logging command. If other failures are indicated in the log, take appropriate action according to the error message.	
01400004	S6	All operation logs have been cleared.
	All operation log entries were deleted. [Action] None.	
01400005	S6	Operation logs of the specified message type were cleared. (message type = *<message type>*)
	Operation logs of the *<message type>* message type were deleted. • *<message type>*: Message type [Action] None.	
01400006	S2	The log control program (logCtl) restarted.
	The log control program (logCtl) has restarted. The device outputs this message after the log control program is forcibly terminated and then automatically restarted. [Action] Collect the core file (logCtl.core file under /usr/var/core), log information, and the configuration of the log control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
01400007	S2	The SYSLOG control program (logSyslogCtl) restarted.
	The syslog transmission-control program (logSyslogCtl) has restarted. The device outputs this message when the syslog transmission-control program automatically restarts. [Action] Collect the core file (logSyslogctl.core file under /usr/var/core), log information, and the configuration of the syslog transmission-control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
01400008	S2	The Email control program (logEmailCtl) restarted.
	The email transmission-control program (logEmailCtl) has restarted. The device outputs this message when the email transmission-control program automatically restarts. [Action] Collect the core file (logEmailctl.core file under /usr/var/core), log information, and the configuration of the e-mail transmission-control program. For details about how to collect the information, see the *Troubleshooting Guide*.	

Message ID	Event level	Message text
		Description and action
01400009	S2	The sysmsg control program (logSysMsgCtl) restarted.
	The system message output-control program (logSysMsgCtl) has restarted. The device outputs this message when the system message output-control program automatically restarts. [Action] Collect the core file (`logSysMsgctl.core` file under `/usr/var/core`), log information, and the configuration of the system message output-control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
01500001	S2	The SOP control program (sopd) restarted.
	The SOP control program (sopd) has restarted. The device outputs this message after the SOP control program is forcibly terminated and is then restarted automatically. [Action] Collect the core file (`sopd.core` file under `/usr/var/core`), log information, and the configuration of the SOP control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
01600001	S1	The BCU will be restarted because a software error occurred.
	The BCU will restart because a software error occurred. [Action] Check the log by executing the `show logging` command. If other failures are indicated in the log, take appropriate action according to the error message.	
0200ff02	S2	The SNMP agent program (snmpd) restarted.
	The SNMP agent program (snmpd) has restarted. The device outputs this message after the SNMP agent program is forcibly terminated and is then restarted automatically. [Action] Collect the core file (`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 will restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
0201ff00	S2	The RMON program (rmon) restarted.
	The RMON program (rmon) has restarted. The device outputs this message after the RMON program is forcibly terminated and is then restarted automatically. [Action] Collect the core file (`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 will restart automatically. If it does not restart or if restarts occur frequently, restart the device.	

Message ID	Event level	Message text
		Description and action
05000001	S2	The unicast routing program (rtm) was forced to stop. [(error = *<error string>*)]
	The unicast routing program (rtm) was forcibly terminated. • *<error string>*: Error cause Cannot allocate memory: The program was forcibly terminated because of lack of memory. Blank: The program was forcibly terminated because of other causes. [Action] 1. Collect the core file (`rtm.core` file under `/usr/var/core`), log information, and the configuration of the IP unicast routing program. For details about how to collect the information, see the *Troubleshooting Guide*. 2. If the cause of the error is `The program was forcibly terminated because of lack of memory`, the error occurred because the memory area was full. Check if the capacity limit has not been exceeded. If the capacity limit has not been exceeded, take action according to steps 3 and 4. 3. If the cause of the error is `The program was forcibly terminated because of other causes`, check whether other log messages related to the unicast routing protocol (message type: `UNICAST`) have been issued. If such log messages have been issued, take action accordingly. 4. When the cause of the error is `The program was forcibly terminated because of other causes`, the unicast routing program restarts automatically. If the program does not restart or if restarts occur frequently, restart the device.	
05000002	S6	The unicast routing program (rtm) restarted.
	The unicast routing program (rtm) has restarted. The device outputs this message when the unicast routing program automatically restarts, or a restart is requested by the `restart unicast` command. [Action] None.	
05000003	S1	The BCU will restart because a software error occurred.
	The BCU will restart because a software error occurred. [Action] Check the log by executing the `show logging` command. If other failures are indicated in the log, take appropriate action according to the error message.	
0b000001	S2	The software update control program (upctld) restarted.
	The update control program (upctld) has restarted. The device outputs this message when the update control program automatically restarts. [Action] Collect the core file (`upctld.core` file under `/usr/var/core`) of the update control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
0b000002	S2	The syslogd program (syslogd) restarted.
	The syslog transmission program (syslogd) has restarted. The device outputs this message when the syslog transmission program automatically restarts. [Action] Collect the core file (`syslogd.core` file under `/usr/var/core`) of the syslog transmission program. For details about how to collect the information, see the *Troubleshooting Guide*.	
0b000003	S2	The dualization file copy program (dupcopyd) restarted.
	The program for managing file copying between BCUs (dupcopyd) has restarted. The device outputs this message when the program for managing file copying between BCUs automatically restarts. [Action] Collect the core file (`dupcopyd.core` file under `/usr/var/core`) of the program for managing file copying between BCUs. For details about how to collect the information, see the *Troubleshooting Guide*.	

Message ID	Event level	Message text
		Description and action
0b000004	S2	The log control program (krclogd) restarted.
		The program for transferring device information (krclogd) has restarted. The device outputs this message when the program for transferring device information automatically restarts. [Action] Collect the core file (`krclogd.core` file under `/usr/var/core`) of the program for transferring device information. For details about how to collect the information, see the *Troubleshooting Guide*.
0d00b001	S2	The DHCP/BOOTP relay agent program (dhcpd) restarted.
		The DHCP/BOOTP relay agent program (dhcpd) has restarted. The device outputs this message when the DHCP/BOOTP relay agent program automatically restarts. [Action] None.
0e008014	S2	The VRRP program (vrrpd) restarted.
		The VRRP program (vrrpd) has restarted. The device outputs this message when the VRRP program automatically restarts. [Action] Collect the core file (`vrrpd.core` file under `/usr/var/core`) of the VRRP program. For details about how to collect the information, see the *Troubleshooting Guide*.
0f010001	S2	The IPv4 multicast routing program (pimd) restarted.
		The IPv4 multicast routing program (pimd) has restarted. The device outputs this message when the IPv4 multicast routing program automatically restarts. [Action] 1. Check whether other log messages related to the IPv4 multicast routing program (message type: `IPv4-PIM`, `IGMP`) have been issued. If such log messages have been issued, take action accordingly. 2. The IPv4 multicast routing program will restart automatically. If it does not restart or if restarts occur frequently, restart the device. 3. Collect the core file (`pimd.core` file under `/usr/var/core`), log information, and the configuration of the IPv4 multicast routing program. For details about how to collect the information, see the *Troubleshooting Guide*.
0f010002	S6	The IPv4 multicast routing program (pimd) restarted.
		The IPv4 multicast routing program (pimd) has restarted. The device outputs this message when a restart is requested by the `restart ipv4-multicast` command. [Action] None.
11110001	S2	The policy-based routing program (policyd) restarted.
		The policy-based routing control program (policyd) has restarted. The device outputs this message when the policy-based routing control program automatically restarts. [Action] Collect the core file (`policyd.core` file under `/usr/var/core`) of the policy-based routing control program. For details about how to collect the information, see the *Troubleshooting Guide*.
11110002	S6	The policy-based routing program (policyd) restarted.
		The policy-based routing control program (policyd) has restarted. The device outputs this message when a restart is requested by the `restart policy-based-routing` command. [Action] None.

Message ID	Event level	Message text
		Description and action
19010001	S2	The IPv6 multicast routing program (pim6sd) restarted.
	The IPv6 multicast routing program (pim6sd) has restarted. The device outputs this message when the IPv6 multicast routing program automatically restarts. [Action] 1. Check whether other log messages related to the IPv6 multicast routing program (message type: `IPv6-PIM`, `MLD`) have been issued. If such log messages have been issued, take action accordingly. 2. The IPv6 multicast routing program will restart automatically. If it does not restart or if restarts occur frequently, restart the device. 3. Collect the core file (`pim6sd.core` file under `/usr/var/core`), log information, and the configuration of the IPv6 multicast routing program. For details about how to collect the information, see the *Troubleshooting Guide*.	
19010002	S6	The IPv6 multicast routing program (pim6sd) restarted.
	The IPv6 multicast routing program (pim6sd) has restarted. The device outputs this message when a restart is requested by the `restart ipv6-multicast` command. [Action] None.	
1e001000	S2	The flow statistics program (flowd) restarted.
	The flow statistics agent program (flowd) was forcibly terminated. [Action] 1. Collect core files (`flowd.core` file under `/usr/var/core`). 2. The flow statistics agent program will restart automatically. If restarts occur frequently, restart the device.	
1e001001	S6	The flow statistics program (flowd) restarted.
	The flow statistics agent program (flowd) has restarted. The device outputs this message when a restart is requested by the `restart sflow` command. [Action] None.	
1f01b021	S2	The DHCPv6 relay agent program (dhcp6_relay) restarted.
	The DHCPv6 relay agent program (dhcp6_relay) has restarted. The device outputs this message when the DHCPv6 relay agent program automatically restarts. [Action] None.	
1f01b022	S6	The DHCPv6 relay agent program (dhcp6_relay) restarted.
	The DHCPv6 relay agent program (dhcp6_relay) has restarted. The device outputs this message when a restart is requested by the `restart ipv6-dhcp relay` command. [Action] None.	
20120000	S2	The LACP program (lacpd) restarted.
	The LACP program (lacpd) has restarted. The device outputs this message when the LACP program automatically restarts. [Action] Collect the core file (`lacpd.core` file under `/usr/var/core`), log information, and the configuration of the LACP program. For details about how to collect the information, see the *Troubleshooting Guide*.	

Message ID	Event level	Message text
		Description and action
20120001	S6	The LACP program (lacpd) restarted.
		The LACP program (lacpd) has restarted. The device outputs this message when a restart is requested by the `restart lacp` command. [Action] None.
20140001	S2	The LLDP program (lldpd) restarted.
		The LLDP program (lldpd) has restarted. The device outputs this message when the LLDP program automatically restarts. [Action] Collect the core file (`lldpd.core` file under `/usr/var/core`), log information, and the configuration of the LLDP program. For details about how to collect the information, see the *Troubleshooting Guide*.
20140002	S6	The LLDP program (lldpd) restarted.
		The LLDP program (lldpd) has restarted. The device outputs this message when a restart is requested by the `restart lldp` command. [Action] None.
20900001	S2	The CFM program (cfmd) restarted.
		The CFM program (cfmd) has restarted. The device outputs this message when the CFM program automatically restarts. [Action] Collect the core file (`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*.
20900002	S6	The CFM program (cdmd) restarted.
		The CFM program (cfmd) has restarted. The device outputs this message when a restart is requested by the `restart cfm` command. [Action] None.
25000001	S6	The network interface management program (nimd) restarted.
		The network interface manager program (nimd) has restarted. The device outputs this message when a restart is requested by the `restart interface-manager` command. [Action] None.
25000002	S2	The network interface management program (nimd) restarted.
		The network interface manager program (nimd) has restarted. The device outputs this message when the network interface manager program automatically restarts. [Action] Collect the core file (`nimd.core` file under `/usr/var/core`) of the network interface manager program. For details about how to collect the information, see the *Troubleshooting Guide*.
27000001	S2	The accounting program (acctd) restarted.
		The accounting program (acctd) has restarted. The device outputs this message when the accounting program automatically restarts, or a restart is requested by the `restart accounting` command. [Action] None.

Message ID	Event level	Message text
		Description and action
27000002	S2	The accounting program (acctd) was forced to stop.
	The accounting program (acctd) was forcibly terminated. [Action] 1. Collect the core file (`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*. 2. Delete the accounting settings from the configuration, and then make the settings again. For details about how to make the settings, see *Configuration Guide Vol. 1 For Version 12.1*. 3. After you perform step 2, if the accounting program is still forced to stop, restart the device.	
35000001	S1	The BCU will restart because a software error occurred.
	The BCU will restart because a software error occurred. [Action] Check the log by executing the `show logging` command. If other failures are indicated in the log, take appropriate action according to the error message.	
35020001	S1	The BCU will restart because a PA software error occurred.
	The BCU will restart because a PA software error occurred. [Action] Check the log by executing the `show logging` command. If other failures are indicated in the log, take appropriate action according to the error message.	
37110001	S2	The queue control program (quectld) restarted.
	The queue control program (quectld) has restarted. The device outputs this message when the queue control program automatically restarts. [Action] Collect the core file (`quectld.core` file under `/usr/var/core`) of the queue control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
37110002	S6	The queue control program (quectld) restarted.
	The queue control program (quectld) has restarted. The device outputs this message when a restart is requested by the `restart queue-control` command. [Action] None.	
37410001	S2	The queue statistics program (queinfod) restarted.
	The queue statistics control program (queinfod) has restarted. The device outputs this message when the queue statistics control program automatically restarts. [Action] Collect the core file (`queinfod.core` file under `/usr/var/core`) of the queue statistics control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
37410002	S6	The queue statistics program (queinfod) restarted.
	The queue statistics control program (queinfod) has restarted. The device outputs this message when a restart is requested by the maintenance command. [Action] None.	
38000001	S2	The synchronization management program(dupctld) restarted.
	The program for managing the information synchronized between BCUs (dupctld) was forced to restart. [Action] Collect the core file (`dupctld.core` file under `/usr/var/core`) of the program. For details about how to collect the information, see the *Troubleshooting Guide*.	

Message ID	Event level	Message text
		Description and action
38000002	S6	The synchronization management program(dupctld) restarted.
	The program for managing the information synchronized between BCUs (dupctld) has restarted. [Action] None.	
3a110001	S2	The filter and qosflow program (flowctld) restarted.
	The filter and QoS flow program (flowctld) has restarted. The device outputs this message when the filter and QoS flow program is forcibly terminated. [Action] Collect the core file (`flowctld.core` file under `/usr/var/core`), log information, and the configuration of the filter and QoS flow program. For details about how to collect the information, see the *Troubleshooting Guide*.	
3a110002	S6	The filter and qosflow program (flowctld) restarted.
	The filter and QoS flow program (flowctld) has restarted. The device outputs this message when a restart is requested by the `restart filter-qosflow` command. [Action] None.	
3a510001	S2	The filter-qosflow statistics program (flowinfod) restarted.
	The filter and QoS flow statistics control program (flowinfod) has restarted. The device outputs this message when the filter and QoS flow statistics control program automatically restarts. [Action] Collect the core file (`flowinfod.core` file under `/usr/var/core`) of the filter and QoS flow statistics control program. For details about how to collect the information, see the *Troubleshooting Guide*.	
3a510002	S6	The filter-qosflow statistics program (flowinfod) restarted.
	The filter and QoS flow statistics control program (flowinfod) has restarted. The device outputs this message when a restart is requested by the maintenance command. [Action] None.	
3b000001	S2	The command-driver-interface-program (cmddrvif) restarted.
	The command driver interface program has restarted. [Action] 1. If an operation command exists that,during execution, displayed an error message and then terminated, re-execute the command. 2. Collect the core file (`cmddrvifd.core` file under `/usr/var/core`) of the command driver interface program. For details about how to collect the information, see the *Troubleshooting Guide*.	
3d008605	S2	The NTP program (ntpd) restarted.
	The NTP program (ntpd) has restarted. The device outputs this message when the NTP program automatically restarts. [Action] Collect the core file (`ntpd.core` file under `/usr/var/core`) of the NTP program. For details about how to collect the information, see the *Troubleshooting Guide*.	

Message ID	Event level	Message text
		Description and action
3d008615	S2	The SNTP program (sntpd) restarted.
	The SNTP program (sntpd) has restarted. The device outputs this message when the SNTP program automatically restarts. [Action] Collect the core file (`sntpd.core` file under `/usr/var/core`) of the SNTP program. For details about how to collect the information, see the *Troubleshooting Guide*.	

3.2 CONFIG

The following table shows the system messages of the CONFIG message type.

Table 3-2: System messages of the CONFIG message type

Message ID	Event level	Message text
		Description and action
09200003	S3	Synchronization of the configuration files failed.
	At the beginning of the redundant operation, the synchronization of running configuration and configuration being edited between the active BCU and standby BCU failed. [Action] If the versions of software for the active system and the standby system match, restart the standby BCU so that its running configuration and configuration being edited match those of the active BCU.	
09200004	S6	Configuration files were successfully synchronized between the active and standby systems.
	At the beginning of the redundant operation, synchronization of running configuration and configuration being edited between the active BCU and standby BCU succeeded. [Action] None.	
09200005	S3	The active and standby configurations are different.
	The active BCU configuration differs from the standby BCU configuration. If system switching occurs in this state due to a fatal error, clicking of the Reset button, pressing of the ACH switch, or execution of the redundancy force-switchover command or reload active command, the new active BCU will restart after the system switchover. This message appears if any of the following conditions are met: • If the running configuration or configuration being edited was inconsistent between the active BCU and the standby BCU: • If the running configuration or configuration being edited has become inconsistent between the active BCU and the standby BCU: • If the running configuration or configuration being edited has become inconsistent after the start up of the BCU of the other system: [Action] 1. If the versions of software for the active system and the standby system match, restart the standby BCU so that its running configuration and configuration being edited match those of the active BCU. (Running configuration and configuration being edited of the standby BCU will be the same as those of the active BCU.) 2. If the versions of software are inconsistent between the active BCU and the standby BCU, match the software version of the active BCU to that of the standby BCU, and then restart the BCUs of both systems.	
09200006	S6	The mismatch of configurations recovered.
	A configuration mismatch between the active BCU and the standby BCU has been solved. This message appears if either of the following conditions is met: • Configurations of the active BCU and the standby BCU are now consistent. • Configurations of the active BCU and the standby BCU are inconsistent, and a BCU went done. [Action] None.	

Message ID	Event level	Message text
		Description and action
09300003	S3	This system started with the default configuration file because the startup configuration file was corrupted or not found.
		This system started with the default configuration file because the startup configuration file was corrupted or not found. [Action] 1. If you have saved the configuration file, apply the saved configuration file to the startup configuration file by using the `copy` command. 2. If you have not saved the configuration file, create a new configuration file.
09300005	S3	The startup configuration file has a command syntax error. (line = *<line number>*, syntax = *<error syntax>*)
		Application to the running configuration was skipped because a syntax error was detected in the startup configuration file. • *<line number>*: Line number of the target configuration command • *<error syntax>*: Syntax of the target configuration command [Action] Review the syntax of the target configuration command.
09300006	S3	An attempt to change the interface configuration failed. (NIF = *<nif no.>*)
		The setting of the configuration of an Ethernet interface for a NIF failed. • *<nif no.>*: NIF number [Action] Remove the NIF, and then insert it again.
09300007	S6	The interface configuration changed because a NIF was connected. (NIF/port = *<nif no.>*/*<port no.>*)
		The configuration of the Ethernet interface was changed because NIF was installed. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] None.
09300008	S3	An automatic configuration command failed. (command = *<command>*)
		Automatic setting of the configuration command failed. • *<command>*: Command name [Action] Manually set the corresponding command.
09300009	S6	The configuration will now be rebuilt to update version.
		The configuration will be reconfigured for the new version because software was updated. [Action] None.
0930000b	S3	The command cannot be set because the maximum number of entries was exceeded. (entry = *<value1>*, maximum number = *<value2>*)
		The command cannot be set because the maximum number of entries was exceeded. (entry = *<value1>*, maximum number = *<value2>*) • *<value1>*: Entry name • *<value2>*: Maximum value [Action] Restore the software version to the version from before the update, and then modify the configuration.

Message ID	Event level	Message text
		Description and action
0930000c	S4	The ifIndex of the MIB was re-set.
		Because MIB ifIndex could not be read from the startup configuration file, it was set again and applied to the running configuration. [Action] Check the MIB ifIndex value.
0930000d	S3	The interface type is different from a port of the NIF. (NIF/port = *<nif no.>*/*<port no.>*)
		The line type of the Ethernet interface differs between the NIF and the configuration. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Delete the configuration of the Ethernet interface where inconsistency was found. The configuration of an Ethernet interface for a NIF is automatically generated.
0930000e	S6	The NIF recovered from a mismatch with the interface configuration.
		The configurations of the installed NIF and Ethernet interface are now consistent. [Action] None.
09400003	S6	The configuration commit mode was changed. (mode = *<mode>*)

		The configuration commit mode was changed.
		 • *<mode>*: Configuration commit mode after the change
		    Auto commit: Auto-applied commit mode
		    Manual commit: Manual commit mode
		 [Action]
		 None.

09600003	S5	A lock on the configuration was released because access by a process took too long. (process = *<process name>*, pid = *<process id>*, time = *<time>*)
		A lock on the configuration was released and the device was automatically recovered because a process was taking a long time to access the configuration. • *<process name>*: Occurrence process name • *<process id>*: Occurrence process ID • *<time>*: Occurrence time (year/month/day hour:minute:second time zone) [Action] None.
3a110003	S6	A flow table allocation configuration was changed. Restart all the PRUs.
		Restart all the PRUs to apply the configuration of the flow distribution pattern. If you have changed the configuration, make sure that you restart the PRU regardless of the details of the distribution pattern. [Action] Restart all the PRUs.
3a110004	S6	A flow detection mode configuration was changed. Restart all the PRUs.
		Restart all the PRUs to apply the configuration of the flow detection pattern. If you have changed the configuration, make sure that you restart the PRU regardless of the details of the flow detection pattern. [Action] Restart all the PRUs.

Message ID	Event level	Message text
		Description and action
3f000001	S6	A forwarding table allocation configuration was changed. Restart all the PRUs.
	Restart all the PRUs to apply the configuration of the route allocation pattern. If you have changed the configuration, make sure that you restart the PRU regardless of the details of the distribution pattern. [Action] Restart all the PRUs to apply the configuration of the route allocation pattern. If you have changed the configuration, make sure that you restart the PRU regardless of the details of the distribution pattern.	

3.3 ACCESS

The following table shows the system messages for the ACCESS message type.

Table 3-3: System messages of the ACCESS message type

Message ID	Event level	Message text
		Description and action
06000001	S5	Login was refused because the host address is unknown. (address = *<ip address>*, kind = *<kind>*)
	An attempt to connect via a remote operation terminal from *<ip address>* was rejected. • *<ip address>*: IPv4 address or IPv6 address • *<kind>*: Connection type [Action] 1. There might have been an unauthorized access (an access from a remote host other than one permitted by the configuration) to the Device. 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 in 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 in the configuration.	
06000002	S5	Login failed. (user name = *<user name>*, address = *<ip address>*, kind = *<kind>*)
	An attempt to log in from *<ip address>* by using the *<user name>* account was made, but the login was not allowed. • *<user name>*: User name • *<ip address>*: IPv4 address or IPv6 address • *<kind>*: Connection type [Action] 1. There might have been an unauthorized access (account authentication or password authentication failed) to the Device from a remote host permitted at the console or by the configuration. Check the operating status of the remote host that is permitted at the console or the configuration. 2. This log data is collected even when a legitimate user executes an incorrect operation during login. Therefore, even if this log data is collected, the operating status of the remote host might be normal. 3. Check if the account is registered by using the username configuration command. (How to check: Use the show users command to find out if the user account exists.)	
06000003	S5	Login was refused because too many users already logged in. (kind = *<kind>*)
	An attempt to connect via a remote operation terminal was rejected because the maximum number of login users was exceeded. • *<kind>*: Connection type [Action] 1. Check the number of users who are currently logged in. 2. If necessary, increase the upper limit for the number of users who can log in by the configuration.	

Message ID	Event level	Message text
		Description and action
06005002	S6	A user logged in. (user = *<user name>*, host = *<host>*, terminal = *<term>*, kind = *<kind>*)
	A user logged in. • *<user name>*: User name • *<host>*: Host ID IPv4 address, IPv6 address, or host name: Remote operation terminal `Console`: Console terminal `aux`: AUX terminal • *<term>*: Terminal name `ttyp0` or larger : Remote operation terminal `tty00`: Console terminal `tty01`: AUX terminal • *<kind>*: Connection type [Action] None.	
06005003	S6	A user logged out. (user = *<user name>*, host = *<host>*, terminal = *<term>*, kind = *<kind>*)
	A user logged out. • *<user name>*: User name • *<host>*: Host ID IPv4 address, IPv6 address, or host name: Remote operation terminal `Console`: Console terminal `aux`: AUX terminal • *<term>*: Terminal name `ttyp0` or larger : Remote operation terminal `tty00`: Console terminal `tty01`: AUX terminal • *<kind>*: Connection type [Action] None.	
06020001	S5	Login via the AUX port failed. (user = *<user name>*)
	An attempt to establish a PPP link via the AUX port by using the *<user name>* account was rejected. • *<user name>*: User name [Action] 1. There might have been an unauthorized access (account authentication or password authentication failed) during a PPP access for the AUX port. 2. This log data is collected even when a legitimate user executes an incorrect operation during login. Therefore, even if this log data is collected, the operating status might be normal.	
06030001	S6	Local authentication succeeded. (kind = *<kind>*)
	Local authentication was performed and was successful for a user login request or request to change to the administrator mode (`enable` command). • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] None.	

Message ID	Event level	Message text
		Description and action
06030002	S5	Local authentication failed. (kind = *<kind>*)
		Local authentication was performed and was unsuccessful for a user login request or a request to change to the administrator mode (`enable` command). • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] 1. There might have been an unauthorized access to the Device 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 during login. Therefore, even if this log data is collected, the operating status of the remote host might be normal.
06030003	S6	The RADIUS server approved the authentication request. (host = *<host>*, kind = *<kind>*)
		RADIUS authentication was performed successfully for a user login request or request to change to the administrator mode (`enable` command). • *<host>*: IP address or host name of the RADIUS server • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] None.
06030004	S5	The RADIUS server rejected the authentication request. (host = *<host>*, message from server = *<message>*, kind = *<kind>*)
		RADIUS authentication was attempted for a user login request or request to change to the administrator mode (`enable` command), but the RADIUS server denied it. • *<host>*: IP address or host name of the RADIUS server • *<message>*: RADIUS server response message • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] 1. There might have been an unauthorized access to the Device 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 during login. Therefore, even if this log data is collected, the operating status of the remote host might be normal. 3. Check the RADIUS server setting.
06030005	S5	The RADIUS server did not respond to the authentication request. (host = *<host>*, kind = *<kind>*)
		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. • *<host>*: IP address or host name of the RADIUS server • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] 1. Check the configuration to make sure that the RADIUS server IP address is correct. 2. Check the configuration to make sure that the RADIUS server port number is correct.

Message ID	Event level	Message text
		Description and action
06030006	S3	The RADIUS server configuration is not defined. (kind = *\<kind\>*)
	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. • *\<kind\>*: Connection type `enable`: Change to the administrator mode [Action] 1. Check that a RADIUS configuration is set up. 2. Make sure that `acct only` is specified for the RADIUS configuration and that authentication is not limited.		
06030007	S5	An invalid response was received from the authentication server. (host = *\<host\>*, kind = *\<kind\>*)
	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. • *\<host\>*: IP address or host name of RADIUS or TACACS+ server • *\<kind\>*: Connection type `enable`: Change to the administrator mode [Action] Make sure that the same RADIUS or TACACS+ key is specified for the Device and the RADIUS or TACACS+ server.		
06030008	S5	RADIUS authentication failed. (kind = *\<kind\>*)
	RADIUS authentication was performed and was unsuccessful for a user login request or request to change to the administrator mode (`enable` command). • *\<kind\>*: Connection type `enable`: Change to the administrator mode [Action] If any other operation log messages for RADIUS authentication were output, refer to them.		
0603000a	S5	Communication with the RADIUS server failed. (host = *\<host\>*, kind = *\<kind\>*)
	Communication with the RADIUS server failed. • *\<host\>*: IP address or host name of the RADIUS server • *\<kind\>*: Connection type `enable`: Change to the administrator mode [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.		
0603000b	S5	No command lists were successfully acquired from the RADIUS server. (kind = *\<kind\>*)
	RADIUS command authorization was performed, but a command list was not properly obtained from the RADIUS server. • *\<kind\>*: Connection type [Action] Make sure that `Class`, `Alaxala-Allow-Commands`, and `Alaxala-Deny-Commands` are properly set in the RADIUS server settings (vendor-specific settings for the Device).		

Message ID	Event level	Message text
		Description and action
06030013	S6	The TACACS+ server approved the authentication request. (host = *<host>*, kind = *<kind>*)
	TACACS+ authentication was successfully performed for a user login request or request to change to the administrator mode (`enable` command). • *<host>*: IP address or host name of the TACACS+ server • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] None.	
06030014	S5	The TACACS+ server rejected the authentication request. (host = *<host>*, kind = *<kind>*)
	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. • *<host>*: IP address or host name of the TACACS+ server • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] 1. There might have been an unauthorized access to the Device 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 during login. Therefore, even if this log data is collected, the operating status of the remote host might be normal. 3. Check the TACACS+ server setting.	
06030015	S5	The TACACS+ server did not respond to the authentication request. (host = *<host>*, kind = *<kind>*)
	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. • *<host>*: IP address or host name of the TACACS+ server • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] Check the configuration to make sure that the TACACS+ server IP address is correct.	
06030016	S3	The TACACS+ server configuration is not defined. (kind = *<kind>*)
	TACACS+ authentication was attempted for a user login request or request to change to the administrator mode (`enable` command), but a TACACS+ server configuration has not been set up. • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] 1. Make sure that a TACACS+ configuration is set up. 2. Make sure that `acct-only` is specified for the TACACS+ configuration and the authentication is not limited.	
06030018	S5	TACACS+ authentication failed. (kind = *<kind>*)
	TACACS+ authentication was performed and was unsuccessful for a user login request or request to change to the administrator mode (`enable` command). • *<kind>*: Connection type `enable`: Change to the administrator mode [Action] If any other operation log messages for TACACS+ authentication were output, refer to them.	

Message ID	Event level	Message text
		Description and action
0603001a	S5	Communication with the TACACS+ server failed. (host = *<host>*, kind = *<kind>*)
	Communication with the TACACS+ server failed. • *<host>*: IP address or host name of the TACACS+ server • *<kind>*: Connection type enable: Change to the administrator mode [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. Make sure that the TACACS+ server is turned on by using the port number set for the TACACS+ configuration. 4. Make sure that the IP address of the Device is registered for the client IP address on the TACACS+ server side.	
0603001b	S5	No command lists were successfully acquired from the TACACS+ server. (kind = *<kind>*)
	TACACS+ command authorization was performed, but a command list was not properly obtained from the TACACS+ server. • *<kind>*: Connection type [Action] Make sure that class, allow-commands, deny-commands are properly set in the TACACS+ server settings (vendor-specific setting for the Device).	
0603001c	S5	TACACS+ command authorization was rejected by the TACACS+ server. (host = *<host>*, kind = *<kind>*)
	TACACS+ command authorization was attempted, but was denied by the TACACS+ server. • *<host>*: IP address or host name of the TACACS+ server • *<kind>*: Connection type [Action] 1. Make sure that the service name is correct in the TACACS+ server settings (vendor-specific settings for the Device). 2. Check other settings on the TACACS+ server side.	
0603001d	S3	A local authorization response had no content. (kind = *<kind>*)
	Local command authorization was performed, but there is no user name and corresponding command class or command list settings. • *<kind>*: Connection type [Action] Make sure that settings for the command class (username view-class) and the command list (username view, parser view, commands exec) are set correctly for users authenticated using local login.	

Message ID	Event level	Message text
		Description and action
27000011	S5	Accounting was temporarily stopped because too many accounting events caused some congestion.
		Accounting event transmission is congested, and accounting of the login, logout, and commands was stopped temporarily. [Action] 1. Using the `show accounting` command, make sure that the RADIUS server or TACACS+ server is not issuing errors. 2. Check the configuration for the RADIUS server or TACACS+ server that is issuing errors. Additionally, make sure that the settings on the RADIUS server or TACACS+ server side are correct. The congested state will be resolved when any of the following occur: • 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. • When the `restart accounting` command was executed • When the following accounting-related configuration is changed: - aaa accounting exec - aaa accounting commands - radius-server - tacacs-server - ip address of interface loopback mode
27000012	S6	Accounting was restarted because the congestion caused by the accounting events was cleared up.
		The accounting event transmission has recovered from congestion, and accounting of login, logout, and commands resumed. [Action] None.
27000013	S5	Accounting failed. (number of failures = <*number*>)
		Accounting for the login, logout, and commands failed. This message appears at intervals when accounting fails. If accounting succeeds even once or no failure occurs for one hour, the failure count is cleared. • <*number*>: The number 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.

3.4 NTP

The following table shows the system messages of the NTP message type.

Table 3-4: System messages of the NTP message type

Message ID	Event level	Message text
		Description and action
3d008601	S5	Synchronization with an NTP server was lost. (NTP server = *<ip address>*)
		Synchronization with an NTP server was lost. • *<ip address>*: IPv4 address of NTP server [Action] Use the `show ntp associations` command to check the NTP status. If the non-synchronized state continues, check the NTP configuration, NTP server operation status, and availability of communication.
3d008602	S5	An invalid packet from an NTP server was detected. (NTP server = *<ip address>*)
		An invalid packet from an NTP server was detected. • *<ip address>*: IPv4 address of NTP server [Action] Check the NTP server.
3d008603	S5	The NTP server to synchronize with was not found.
		An NTP server to synchronize with was not found. [Action] Check the NTP configuration, NTP server operation status, and availability of communication.
3d008604	S6	It synchronized with the NTP server. (NTP server = *<ip address>*)
		Synchronization with the NTP server was successful. • *<ip address>*: IPv4 address of NTP server [Action] None.
3d008611	S5	Synchronization with an SNTP server was lost. (SNTP server = *<ip address>*)
		Synchronization with an SNTP server was lost. • *<ip address>*: IPv4 address or IPv6 address of the SNTP server [Action] Check the SNTP server.
3d008612	S5	An invalid packet from an SNTP server was detected. (SNTP server = *<ip address>*)
		An invalid packet from an SNTP server was detected. • *<ip address>*: IPv4 address or IPv6 address of the SNTP server [Action] Check the SNTP server.
3d008613	S5	The SNTP server to synchronize with was not found.
		An SNTP server to synchronize with was not found. [Action] Check the SNTP configuration, NTP server operation status, and availability of communication.

Message ID	Event level	Message text
		Description and action
3d008614	S6	It synchronized with the SNTP server. (SNTP server = *\<ip address\>*)
	Synchronization with the SNTP server was successful. • *\<ip address\>*: IPv4 address or IPv6 address of the SNTP server [Action] None.	

3.5 SOP-KEY

The following table shows the system messages of the SOP-KEY message type.

Table 3-5: System messages of the SOP-KEY message type

Message ID	Event level	Message text
		Description and action
01504000	S6	An inactivate operation for the board was selected. (board = *<board>*)
		An inactivate instruction for *<board>* was selected. This message appears only for the active BCU. • *<board>*: Board type Standby BCU: Standby BCU SFU*<sfu no.>*: SFU number PRU*<pru no.>*: PRU number NIF*<nif no.>*: NIF number [Action] None.
01504001	S6	The inactivate operation was canceled.
		NO was selected for the inactivate instruction. This message appears only for the active BCU. [Action] None.
01504002	S6	The inactivate operation was confirmed.
		YES was selected for the inactivate instruction. This message appears only for the active BCU. [Action] None.
01504010	S6	An activate operation for the board was selected. (board = *<board>*)
		An activate instruction for *<board>* was selected. This message appears only for the active BCU. • *<board>*: Board type Standby BCU: Standby BCU SFU*<sfu no.>*: SFU number PRU*<pru no.>*: PRU number NIF*<nif no.>*: NIF number [Action] None.
01504011	S6	The activate operation was canceled.
		NO was selected for the activate instruction. This message appears only for the active BCU. [Action] None.
01504012	S6	The activate operation has been confirmed.
		YES was selected for the activate instruction. This message appears only for the active BCU. [Action] None.
01504020	S6	The shutdown operation was canceled.
		NO was selected for the shutdown instruction. [Action] None.

Message ID	Event level	Message text
		Description and action
01504121	S6	The shutdown operation was confirmed.
		YES was selected for the shutdown instruction. [Action] None.

3.6 SOP-RSP

The following table shows the system messages of the SOP-RSP message type.

Table 3-6: System messages of the SOP-RSP message type

Message ID	Event level	Message text
		Description and action
01505000	S6	No board exists that can be inactivated.
	There is no board for which the inactivate operation can be performed. This message appears only for the active BCU. [Action] None.	
01505001	S6	No board exists that can be activated.
	There is no board for which the activate operation can be performed. This message appears only for the active BCU. [Action] None.	
01505002	S6	The port information cannot be displayed because no NIF is active.
	The port information is not displayed because no NIF is active. This message appears only for the active BCU. [Action] None.	
01505003	S6	The operation cannot be executed on the standby BCU.
	The operation cannot be executed on the standby BCU. This message appears only for the standby BCU. [Action] None.	
01505004	S6	You will be returned to the Main Menu because the information could not be obtained.
	You will be returned to the Main Menu because the information could not be obtained. [Action] None.	
01505010	S6	The activate operation cannot be executed on the standby BCU.
	The board activate operation cannot be executed on the standby BCU. [Action] None.	
01505011	S6	The inactivate operation cannot be executed on the standby BCU.
	The board inactivate operation cannot be executed on the standby BCU. [Action] None.	
01505012	S6	The activate operation cannot be executed. Try again.
	The board activate operation cannot be executed. Re-execute the command. [Action] None.	

Message ID	Event level	Message text
		Description and action
01505013	S6	The inactivate operation cannot be executed. Try again.
		The board inactivate operation cannot be executed. Re-execute the command. [Action] None.
01505014	S6	The specified board is already active. (board = <*board*>)

		The specified board is already active.
		• <*board*>: Board type
		  Standby BCU: Standby BCU
		  SFU<*sfu no.*>: SFU number
		  PRU<*pru no.*>: PRU number
		  NIF<*nif no.*>: NIF number
		[Action]
		If you specified the board correctly, you do not need to execute the command.

01505015	S6	The specified board is already inactive.(board = <*board*>)

		The specified board is already inactive.
		• <*board*>: Board type
		  Standby BCU: Standby BCU
		  SFU<*sfu no.*>: SFU number
		  PRU<*pru no.*>: PRU number
		  NIF<*nif no.*>: NIF number
		[Action]
		If you specified the board correctly, you do not need to execute the command.

01505016	S6	The specified board is already being initialized.(board = <*board*>)

		The specified board is already being initialized.
		• <*board*>: Board type
		  SFU<*sfu no.*>: SFU number
		  PRU<*pru no.*>: PRU number
		  NIF<*nif no.*>: NIF number
		[Action]
		If you specified the board correctly, you do not need to execute the command.

01505017	S6	The specified board is disabled. (board = <*board*>)

		The specified port is in the disable status due to the configuration.
		• <*board*>: Board type
		  SFU<*sfu no.*>: SFU number
		  PRU<*pru no.*>: PRU number
		  NIF<*nif no.*>: NIF number
		[Action]
		None.

01505018	S6	The specified board failed. (board = <*board*>)

		The specified board failed.
		• <*board*>: Board type
		  SFU<*sfu no.*>: SFU number
		  PRU<*pru no.*>: PRU number
		  NIF<*nif no.*>: NIF number
		[Action]
		None.

Message ID	Event level	Message text
		Description and action
01505019	S6	The specified board is not connected.(board = <*board*>)

	The specified board is not mounted or is not used.
	• <*board*>: Board type
	  Standby BCU: Standby BCU
	  SFU<*sfu no.*>: SFU number
	  PRU<*pru no.*>: PRU number
	  NIF<*nif no.*>: NIF number
	[Action]
	None.	

0150501a	S6	There is not enough power supply for the specified board.(board = <*board*>)

	There is not enough power for the specified board.
	• <*board*>: Board type
	  PRU<*pru no.*>: PRU number
	  NIF<*nif no.*>: NIF number
	[Action]
	None.	

0150501b	S6	The specified board is not supported. (board = <*board*>)

	The specified board is not supported.
	• <*board*>: Board type
	  SFU<*sfu no.*>: SFU number
	  PRU<*pru no.*>: PRU number
	  NIF<*nif no.*>: NIF number
	[Action]
	None.	

0150501c	S6	The PRU that controls the specified NIF is not active. (NIF = <*nif no.*>)
	The PRU that controls the specified NIF is not active. • <*nif no.*>: NIF number [Action] Activate the PRU.	
01505020	S6	The board will be stopped because of the shutdown operation.(board = <*board*>)

	The board will be stopped because a shutdown was requested.
	• <*board*>: Board type
	  Active BCU: Active BCU
	  Both systems: Active BCU and standby BCU
	[Action]
	None.	

01505021	S6	The shutdown operation cannot be executed on the standby BCU.
	The shutdown operation cannot be executed on the standby BCU. [Action] None.	
01505022	S6	The shutdown operation cannot be executed. Try again.
	The shutdown operation cannot be executed. Re-execute the command. [Action] None.	

Message ID	Event level	Message text
		Description and action
01505023	S6	The shutdown operation cannot be executed because the standby BCU is inactivated or not connected.
		The shutdown operation cannot be executed because the standby BCU has stopped or is not connected. [Action] None.
01505024	S6	The shutdown operation cannot be executed because the standby BCU is booting or fault.
		The shutdown operation cannot be executed because the standby BCU is starting or has failed. [Action] None.

3.7 SNMP

The following table shows the system messages of the SNMP message type.

Table 3-7: System messages of the SNMP message type

Message ID	Event level	Message text
		Description and action
02000300	S5	An incorrect instance value was specified.
		An incorrect instance value (set when specifying MIB settings) was specified. [Action] Check and set the instance value.
02000301	S5	A specified MIB value is outside the valid range.
		A specified MIB value (set when specifying MIB settings) is outside the valid range. [Action] For details about the range of MIB values, see *13. SNMP* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.
02000302	S5	The data length of the MIB value is too long.
		The data length of an MIB value (set when specifying MIB settings) is too long. [Action] For details about the number of characters that can be set for a MIB value, see *13. SNMP* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.
02000303	S5	One or more invalid characters were used in a MIB setting.
		You attempted to set up the MIB by using invalid characters. [Action] Check the character code list in *1. Reading the Manual* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*, and set up the MIB.
02000304	S3	A MIB value was not set because an error occurred during editing of the configuration.
		A MIB value was not set because an error occurred during editing of the configuration (when specifying the MIB settings). [Action] For details on configuration errors, see *Error Messages Displayed When Editing the Configuration* in the *Configuration Command Reference*.
02000305	S6	A request set an object for a MIB value. (object = *<object name>*, MIB value = *<mib value>*, source SNMP manager = *<ip address>*)
		<object name> was set to *<mib value>* because of a request from the SNMP manager *<ip address>*. • *<object name>*: MIB object mnemonic • *<mib value>*: MIB value • *<ip address>*: IPv4 or IPv6 address of the SNMP manager [Action] None.

Message ID	Event level	Message text
		Description and action
0200ff00	S5	The SNMP agent program received a packet with an unexpected community name. (source SNMP manager = *<ip address>*, community name = *<community name>*)
	The SNMP agent received a packet that had the unexpected community name *<community name>* from the SNMP manager *<ip address>*. • *<ip address>*: IPv4 or IPv6 address of the SNMP manager • *<community name>*: Community name [Action] An SNMP manager that the configuration does not authorize to access the Device attempted to access the Device. 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 that is authorized by the configuration. 1. Check the configuration to make sure that the IP address and the community name of the SNMP manager that is attempting to access the Device are identical to *<ip address>* and *<community name>*. 2. If they do not match, unauthorized access might be taking place. Contact the administrator of the SNMP manager at *<ip address>* to prevent the SNMP manager from accessing the Device. The Device suppresses repeated output to the operation log of access from an unauthorized IP address or community. A maximum of 16 unauthorized IP addresses are saved and, for each saved IP address, 1 out of every 128 unauthorized access attempts is output to the log.	
0200ff01	S5	The specified MIB does not exist, or does not have the read/write attribute.
	Either the specified MIB does not exist, or the MIB does not have read and write attributes. [Action] See the manual *MIB Reference For Version 12.1*, and make sure that the specified MIB has read and write attributes.	

Chapter

4. Network Interfaces

4.1 PORT

The following table shows the system messages of the `PORT` message type.

Table 4-1: System messages of the PORT message type

Message ID	Event level	Message text
		Description and action
25010001	S6	The port status is Up.
	The port is up. [Action] None.	
25010002	S5	Reception of frames at a port failed many times because of problems with the port.
	Frame reception at the corresponding port failed multiple times because of errors such as from noise. [Action] 1. Make sure that the cables have no problem. 2. If the cables are normal, check the connected devices.	
25010003	S5	Sending of frames to a port failed many times because of problems with the port.
	Frame transmission at the corresponding port failed multiple times because of errors such as from noise. [Action] 1. Make sure that the cables have no problem. 2. If the cables are normal, check the connected devices.	
25010004	S6	The port was inactivated by configuration.
	The port was stopped by the `shutdown` configuration command. [Action] None.	
25010005	S6	The port was activated by configuration.
	The port was started by the `no shutdown` configuration command. [Action] None.	
25010006	S6	The port was inactivated by an operation command.
	The port was stopped by the `inactivate` command. [Action] None.	
25010007	S6	The port was activated by an operation command.
	The port was started by the `activate` command. [Action] None.	

Message ID	Event level	Message text
		Description and action
25010101	S5	An error was detected on the port.
	Errors were detected at the ports. [Action] For 10BASE-T, 100BASE-TX, or 1000BASE-T: 1. Make sure that the specified cables are properly connected. 2. Make sure that the partner device has finished starting up. 3. Execute the `test interfaces` command, and make sure that the devices and cables have no problem. For 1000BASE-X, 10GBASE-R, or 100GBASE-R: 1. Make sure that the specified cables are properly connected. Make sure that the end sections of the cables are clean. If they are dirty, clean them. 2. If an optical attenuator is used, check the attenuation value. 3. Make sure that the partner device has finished starting up. 4. Execute the `test interfaces` command, and make sure that the devices and cables have no problem.	
25010102	S5	The transceiver is not inserted properly.
	A transceiver removal was detected. [Action] The transceiver might have been removed or might not have been properly inserted. Make sure that the transceiver is properly inserted into the device.	
25010103	S5	Auto-negotiation failed.
	Auto-negotiation failed. [Action] 1. Check the auto-negotiation settings. 2. Make sure that the cables have no problem. 3. If the cables are normal, check the connected devices.	
25010104	S5	The unsupported transceiver was detected.
	An unsupported transceiver was detected. [Action] Insert a supported transceiver.	
25010105	S5	The inserted transceiver was detected.
	Insertion of a transceiver was detected. [Action] None.	
25010106	S1	The transceiver stopped because of a failure in its hardware.
	A transceiver failure was detected. The transceiver will be stopped. [Action] Replace the transceiver.	
35050208	S5	All ports were stopped, because there are not enough active SFUs.
	All the ports stopped because packet forwarding via the Device became impossible due to insufficient active SFUs. [Action] Use the `show system` command to check the SFU status.	

Message ID	Event level	Message text
		Description and action
35050209	S6	All ports were started, because there are enough active SFUs.
	All the ports started because packet forwarding via the Device became possible after an increase in active SFUs. [Action] None.	

4.2 ChGr

The following table shows the system messages of the ChGr message type.

Table 4-2: System messages of the ChGr message type

Message ID	Event level	Message text
		Description and action
20120002	S6	The status of channel group is Up.
		The channel group status was changed to Up. [Action] None.
20120003	S5	The channel group is Down because all ports were detached.
		The channel group status was changed to Down because all ports in the channel group are detached. [Action] None.
20120004	S5	The channel group is Down because the number of detached ports exceeded the configured number.
		The channel group status was changed to Down because the number of detached ports in the channel group exceeded the set limit. [Action] Check the line connection status of the partner device.
20120005	S6	A command disabled the channel group.
		The channel group was disabled by the shutdown configuration of the channel group. [Action] None.
20120006	S6	A command enabled the channel group.
		The channel group was released from the disabled state by the no shutdown configuration of the channel group. [Action] None.
20120007	S5	The port was detached from the channel group because different partner system ID were detected. (NIF/port = *<nif no.>*/*<port no.>*)
		The port was detached from the channel group because the no matches for the system ID of a partner device were found among the ports for LACP mode link aggregation. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Make sure that the connection with and the system ID for the partner device are correct.
20120008	S5	The port was detached from the channel group because the partner key do not match. (NIF/port = *<nif no.>*/*<port no.>*)
		The key of a partner device does not match between the ports for LACP mode link aggregation, and the port was detached from the channel group. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Make sure that the connection with and the key for the partner device are correct.

Message ID	Event level	Message text
		Description and action
20120009	S6	The port was removed from the channel group. (NIF/port = *<nif no.>*/*<port no.>*)
	A port was detached from the channel group because a configuration link was deleted. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] None.	
20120010	S5	The port was detached from the channel group because the port status is Down. (NIF/port = *<nif no.>*/*<port no.>*)
	The status of a line changed to down. The port was detached from the channel group. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Check the line connection status for problems such as physical disconnection.	
20120011	S5	The port was detached from the channel group because other ports have faster data speeds. (NIF/port = *<nif no.>*/*<port no.>*)
	Lines that have different data rates exist in the channel group. Lines that have low data rates were detached from the channel group. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Check the line connection status, such as physical disconnection, and line rates of the Device and the partner device.	
20120012	S5	The port was detached from the channel group because the port is half duplex. (NIF/port = *<nif no.>*/*<port no.>*)
	Lines operating in half-duplex mode were detached from the channel group. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Check the line connection status of the Device and the partner device for problems such as physical disconnection.	
20120013	S5	The port was detached from the channel group because connection was denied by the LACP partner. (NIF/port = *<nif no.>*/*<port no.>*)
	In LACP mode link aggregation, a connection from the partner device was denied due to LACP, and the port was detached from the channel group. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Check the status of the partner device.	
20120014	S5	The port was detached from the channel group because of an LACPDU timeout. (NIF/port = *<nif no.>*/*<port no.>*)
	In LACP mode link aggregation, the port did not receive an LACPDU from the partner device, and the port was detached from the channel group because of a timeout. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Check the status of the partner device.	

Message ID	Event level	Message text
		Description and action
20120015	S6	The port was detached from the channel group because of a configuration change. (NIF/port = <*nif no.*>/<*port no.*>)
		A port was detached from the channel group because of a configuration change. • <*nif no.*>: NIF number • <*port no.*>: Port number [Action] None.
20120016	S5	The port was detached from the channel group because the port was moved. (NIF/port = <*nif no.*>/<*port no.*>)
		A port was detached from the channel group because the port was moved in the channel group. • <*nif no.*>: NIF number • <*port no.*>: Port number [Action] None.
20120017	S5	The port was detached from the channel group because the partner aggregation bit is FALSE. (NIF/port = <*nif no.*>/<*port no.*>)
		The application bit of the partner device in the LACP mode was false, and the port was detached from the channel group. • <*nif no.*>: NIF number • <*port no.*>: Port number [Action] None.
20120018	S5	The port was detached from the channel group because the partner port number was changed. (NIF/port = <*nif no.*>/<*port no.*>)
		The port number of the partner device was changed, and the port was detached from the channel group. • <*nif no.*>: NIF number • <*port no.*>: Port number [Action] None.
20120019	S5	The port was detached from the channel group because the partner port priority was changed. (NIF/port = <*nif no.*>/<*port no.*>)
		The port priority of the partner device was changed, and the port was detached from the channel group. • <*nif no.*>: NIF number • <*port no.*>: Port number [Action] None.
20120020	S5	The port was detached from the channel group because of a detach port limit operation. (NIF/port = <*nif no.*>/<*port no.*>)
		A port was detached from the channel group by the port-detachment restriction functionality. • <*nif no.*>: NIF number • <*port no.*>: Port number [Action] None.

Message ID	Event level	Message text
		Description and action
20120021	S6	The port was added to the channel group. (NIF/port = *<nif no.>*/*<port no.>*)
	A port was added to the channel group. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] None.	
20120022	S6	The port was attached to the channel group. (NIF/port = *<nif no.>*/*<port no.>*)
	A port was aggregated to the channel group. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] None.	
20120023	S6	The standby port became active. (NIF/port = *<nif no.>*/*<port no.>*)
	Operation by a standby link has started. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] None.	
20120024	S6	The port detached from the channel group became the standby port. (NIF/port = *<nif no.>*/*<port no.>*)
	Operation by a standby link has stopped. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] None.	
20120025	S6	The port cannot attach because of non-revertive function. (NIF/port = *<nif no.>*/*<port no.>*)
	A port was not aggregated because Reversion Suppression activated. • *<nif no.>*: NIF number • *<port no.>*: Port number [Action] Execute the `clear channel-group non-revertive` command to aggregate lines.	

Chapter

5. Network Management

5.1 CFM

5.1 CFM

The following table shows the system messages of the CFM message type.

Table 5-1: System messages of the CFM message type

Message ID	Event level	Message text
		Description and action
20900003	S3	The number of Remote MEP entries exceeded the total Remote MEP capacity.
		The number of remote MEPs exceeds the capacity limit. [Action] Make sure that the number of remote MEPs does not exceed the capacity limit.
20900004	S5	An OtherCCM failure was detected in MEP. (Domain Level = *<level>*, MA = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (OtherCCM). • *<level>*: Domain level • *<no.>*: MA identification number • *<mepid>*: MEP ID [Action] A partner device is not recognized as the same MA. Check that the domain level, MA ID, domain name, and MA name match the partner devices.
20900005	S5	An ErrorCCM failure was detected in MEP. (Domain Level = *<level>*, MA = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (ErrorCCM). • *<level>*: Domain level • *<no.>*: MA identification number • *<mepid>*: MEP ID [Action] A partner device and the configuration do not match. Check whether the MEP ID is different from the partner device, and make sure the send interval (`interval`) matches that of the partner device.
20900006	S5	A Timeout failure was detected in MEP. (Domain Level = *<level>*, MA = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (Timeout). • *<level>*: Domain level • *<no.>*: MA identification number • *<mepid>*: MEP ID [Action] A timeout occurred while receiving a CCM from the partner device. Check the network status.
20900007	S5	A PortState failure was detected in MEP. (Domain Level = *<level>*, MA = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (PortState). • *<level>*: Domain level • *<no.>*: MA identification number • *<mepid>*: MEP ID [Action] A timeout occurred while receiving a CCM from the partner device. Check the network status.

Message ID	Event level	Message text
		Description and action
20900008	S5	An RDI failure was detected in MEP. (Domain Level = *<level>*, MA = *<no.>*, MEP = *<mepid>)*
		The relevant MEP detected a fault (RDI). • *<level>*: Domain level • *<no.>*: MA identification number • *<mepid>*: MEP ID [Action] A fault was detected in a partner device. Check the status of the partner device.
20900009	S5	A Mismerge failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (Mismerge). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] A partner device is not recognized as the same MEG. Check that the MEG level, MEG identification number, and MEG ID match the partner devices.
20900010	S5	An UnexpectedMEGLevel failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (UnexpectedMEGLevel). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] The Device received a CCM of a level lower than the MEG level configured for the Device. Check the settings of the Device and the partner device.
20900011	S5	An UnexpectedMEP failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (UnexpectedMEP). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] The CCM received from the partner device and the MEP ID set for the Device are the same. Change the MEP ID of either the Device or the partner device.
20900012	S5	An UnexpectedPeriod failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
		The relevant MEP detected a fault (UnexpectedPeriod). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] The CCM-sending intervals of the partner device and the Device are not the same. Make sure that the CCM-sending intervals of the devices are the same.

Message ID	Event level	Message text
		Description and action
20900013	S5	An UnexpectedPriority failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
	The relevant MEP detected a fault (UnexpectedPriority). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] The CoS values of the partner device and the Device are not the same. Make sure that the CoS values of the devices are the same.	
20900014	S5	An LOC failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
	The relevant MEP detected a fault (LOC). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] A timeout occurred while receiving a CCM from the partner device. Check the network status.	
20900015	S5	An RDI failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
	The relevant MEP detected a fault (RDI). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] A fault was detected in a partner device. Check the status of the partner device.	
20900016	S5	An AIS failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
	The relevant MEP detected a fault (AIS). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] The AIS status occurred. Check the network status.	
20900017	S5	An LCK failure was detected in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
	The relevant MEP detected a fault (LCK). • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] The LCK status occurred after an LCK was received from the partner device. Check the network status.	

Message ID	Event level	Message text
		Description and action
20900018	S6	An AIS failure was cleared in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
	The AIS failure for the MEP was cleared. • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] None.	
20900019	S6	An LCK failure was cleared in MEP. (MEL = *<level>*, MEG = *<no.>*, MEP = *<mepid>*)
	The LCK failure for the MEP was cleared. • *<level>*: MEG level • *<no.>*: MEG identification number • *<mepid>*: MEP ID [Action] None.	

Chapter

6. IP Packet Forwarding

6.1 IP

The following table shows the system messages of the IP message type.

Table 6-1: System messages of the IP message type

Message ID	Event level	Message text
		Description and action
00400100	S5	Duplication of IPv4 address with the node was detected. (IPv4 address = *<ipv4 address>*, node MAC address = *<mac address>*)
	The IPv4 address *<ipv4 address>* is being used by the device that has the MAC address *<mac address>*. • *<ipv4 address>*: IPv4 address that is registered for the interface for the Device • *<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. If you changed the IPv4 address of the other device while Address Conflict Detection is in use, on the Device, execute the `clear ip duplicate-address` command. 2. When using VRRP, this message might be issued frequently when the CPU load is heavy. In such a case, increase the value of the `vrrp timers advertise` configuration command for the devices comprising the VRRP. 3. If Address Conflict Detection is in use, check the network configuration, and then execute the `clear ip duplicate-address` command.	
00400101	S3	The number of ARP entries exceeded the maximum, causing old entries to be deleted in order to add new entries.
	The number of ARP entries exceeded the capacity limit of the Device. Old entries were deleted, and new entries were added. [Action] If this message is issued frequently, take the following action: 1. Delete unnecessary information from the settings of the `arp` configuration command. 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 entries can be reduced.	
00400102	S3	The number of ARP entries exceeded the maximum allowed for the global network, causing old entries to be deleted in order to add new entries.
	The number of ARP entries exceeded the maximum value for the global network. Old entries were deleted, and new entries were added. [Action] If this message is issued frequently, take the following action: 1. Delete unnecessary information from the settings of the `arp` configuration command. 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 entries can be reduced.	

Message ID	Event level	Message text
		Description and action
00400103	S3	The number of ARP entries exceeded the maximum allowed for each VRF, causing old entries to be deleted in order to add new entries.
	The number of ARP entries exceeded the maximum value for each VRF. Old entries were deleted, and new entries were added. [Action] If this message is issued frequently, take the following action: 1. Delete unnecessary information from the settings of the `arp` configuration command. 2. If unnecessary entries have been generated dynamically, delete them by using the `clear arp-cache` command. 3. Change the network configuration so that the the number of ARP entries can be reduced.	
00400104	S3	The number of ARP entries of the interface exceeded the maximum. (interface = *<interface name>*)
	The maximum number of ARP entries for each interface was exceeded in the interface *<interface name>*. • *<interface name>*: Interface name [Action] Display the ARP entries for the interface by using the `show ip arp interface` command, and then check if the maximum number of ARP entries has been exceeded. If the maximum number was exceeded, take the following actions: 1. Delete unnecessary information from the settings of the `arp` configuration command. 2. If unnecessary entries have been generated dynamically, delete them by using the `clear arp-cache` command. 3. Change the network configuration so that the the number of ARP entries can be reduced.	
00600100	S5	Duplication of IPv6 address with the node was detected. (IPv6 address = *<ipv6 address>*, node MAC address = *<mac address>*)
	The IPv6 address *<ipv6 address>* is being used by the device that has the MAC address *<mac address>*. • *<ipv6 address>*: IPv6 address of the Device interface that has become unavailable because of address duplication detection • *<mac address>*: MAC address of a device for which address duplication detection was detected [Action] 1. If *<ipv6 address>* set in the Device is incorrect, change *<ipv6 address>* of the device. 2. If *<ipv6 address>* on the other device is incorrect, change *<ipv6 address>* of the conflicting device. After that, either delete *<ipv6 address>* of the Device and then re-set it, or execute the `clear ipv6 duplicate-address` command. 3. When using VRRP, this message might be issued frequently when the CPU load is heavy. In such a case, increase the value of the `vrrp timers advertise` configuration command for the devices comprising the VRRP.	
00600101	S3	The number of NDP entries exceeded the maximum, causing old entries to be deleted in order to add new entries.
	The number of NDP entries has exceeded the capacity limit of the Device. Old entries are deleted, and new entries are added. [Action] If this message is issued frequently, take the following action: 1. Delete unnecessary information from the settings of the `ipv6 neighbor` configuration command. 2. If unnecessary entries have been generated dynamically, delete them by executing the `clear ipv6 neighbors` command. 3. Change the network configuration so that the the number of NDP entries can be reduced.	

Message ID	Event level	Message text
		Description and action
00600102	S3	The number of NDP entries exceeded the maximum allowed for the global network, causing old entries to be deleted in order to add new entries.
	The number of NDP entries exceeded the maximum value for the global network. Old entries were deleted, and new entries were added. [Action] If this message is issued frequently, take the following action: 1. Delete unnecessary information from the settings of the `ipv6 neighbor` configuration command. 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 entries can be reduced.	
00600103	S3	The number of NDP entries exceeded the maximum allowed for each VRF, causing old entries to be deleted in order to add new entries.
	The number of NDP entries exceeded the maximum value for each VRF. Old entries were deleted, and new entries were added. [Action] If this message is issued frequently, take the following action: 1. Delete unnecessary information from the settings of the `ipv6 neighbor` configuration command. 2. If unnecessary entries have been generated dynamically, delete them by executing the `clear ipv6 neighbors` command. 3. Change the network configuration so that the the number of NDP entries can be reduced.	
00600104	S3	The number of the NDP entries of the interface exceeded the maximum. (interface = *\<interface name\>*)
	The maximum number of NDP entries for each interface was exceeded in the interface *\<interface name\>*. • *\<interface name\>*: Interface name [Action] Display NDP entries for the interface by using the `show ipv6 neighbors interface` command, and then check if the maximum number of NDP entries was exceeded. If the maximum number was exceeded, take the following actions: 1. Delete unnecessary information from the settings of the `ipv6 neighbor` configuration command. 2. If unnecessary entries have been generated dynamically, delete them by executing the `clear ipv6 neighbors` command. 3. Change the network configuration so that the the number of NDP entries can be reduced.	
00600110	S4	The number of the NDP entries of the interface exceeded the threshold. (threshold = *\<higher count\>*, interface = *\<interface name\>*)
	The number of NDP entries for each interface exceeded the threshold value in the interface *\<interface name\>*. • *\<interface name\>*: Interface name • *\<higher count\>*: Warning threshold value for the number of NDP entries per interface [Action] 1. Delete unnecessary information from the settings of the `ipv6 neighbor` configuration command. 2. If unnecessary entries have been generated dynamically, delete them by executing the `clear ipv6 neighbors` command. 3. Change the network configuration so that the the number of NDP entries can be reduced.	

Message ID	Event level	Message text
		Description and action
00600111	S6	The number of the NDP entries of the interface recovered from the threshold. (threshold = *<lower count>*, interface = *<interface name>*)
		The number of NDP entries for each interface decreased to the threshold value in the interface *<interface name>*. • *<interface name>*: Interface name • *<lower count>*: Recovery threshold value for the number of NDP entries per interface undefined is displayed immediately after the configuration is deleted. [Action] None.
05100100	S5	A received message was ignored because the option length in the message was 0. (type = *<type>*)
		A received message was ignored because the length of the option was 0. • *<type>*: Received option type [Action] Check the settings of the terminal that sends a router solicitation.
05100200	S5	A Router Solicitation message was ignored because the received interface was not found. (source = *<address1>*, destination = *<address2>*)
		A router solicitation was ignored because the interface that received the solicitation was not found. • *<address1>*: Router solicitation sender address • *<address2>*: Router solicitation destination address [Action] If this error occurs frequently, check the status of the interface.
05100201	S5	A Router Solicitation message from the unspecified address (::) was ignored because the message had a source link-layer address option. (interface = *<interface name>*)
		The router solicitation was ignored because the source link-layer address option has been set for router solicitation from unspecified address (::). • *<interface name>*: Name of interface for receiving router solicitation [Action] Check the settings of the terminal that sends a router solicitation.
05100202	S5	A Router Solicitation message was ignored because it was received on a non-advertising interface. (interface = *<interface name>*)
		The router solicitation was ignored because the router solicitation was received by the interface that does not advertise routers. • *<interface name>*: Name of interface for receiving router solicitation [Action] If it is necessary to respond to the router solicitation, enable router advertisement in the interface.
05100203	S5	A Router Solicitation message was ignored because of an invalid hoplimit. (received hoplimit = *<hoplimit>*, source = *<address>*, interface = *<interface name>*)
		A router solicitation was ignored because the hop limit of the received router solicitation message is not the correct value (255). • *<hoplimit>*: Hop limit value of the received router solicitation message • *<address>*: Router solicitation sender address • *<interface name>*: Name of interface for receiving router solicitation [Action] Check the settings of the terminal that sends a router solicitation.

Message ID	Event level	Message text
		Description and action
05100204	S5	A Router Solicitation message was ignored because of an invalid code. (code = *<code>*, source = *<address>*, interface = *<interface name>*)
		A router solicitation was ignored because the code of the received router solicitation message is not the correct value (0). • *<code>:* ICMP6 code value of the received router solicitation message • *<address>*: Router solicitation sender address • *<interface name>*: Name of interface for receiving router solicitation [Action] Check the settings of the terminal that sends a router solicitation.
05100205	S5	A Router Solicitation message was ignored because the packet length was too short. (source = *<address>*, interface = *<interface name>*, length = *<length>*)
		The router solicitation was ignored because the received router solicitation packet is short. • *<address>*: Router solicitation sender address • *<interface name>*: Name of interface for receiving router solicitation • *<length>*: Received router solicitation packet length [Action] Check the settings of the terminal that sends a router solicitation.
05100400	S4	A Router Advertisement message could not be sent from an interface because there was no valid link-local address on the interface. (interface = *<interface name>*)
		Router advertisements cannot be sent because there is no valid link-local address in the relevant interface. • *<interface name>*: Name of the router advertisement sending interface [Action] If this error occurs frequently, check the status of the interface.
05100402	S3	A Router Advertisement message could not be sent from an interface. (interface = *<interface name>*, error = *<error string>*)
		Router advertisements cannot be sent from the relevant interface. • *<interface name>*: Name of the router advertisement sending interface • *<error string>*: Error cause [Action] If this error occurs frequently, check the status of the interface.
05104101	S3	A Router Advertisement message could not be sent from an interface because the MTU option value exceeded the interface MTU. (interface = *<interface name>*, MTU option = *<configured value>*, MTU = *<interface mtu>*)
		Router advertisements cannot be sent from the interface because the MTU option value exceeds the MTU of the physical interface. • *<interface name>*: Name of the router advertisement sending interface • *<configured value>*: MTU option value of the router advertisement • *<interface mtu>*: Physical MTU of the interface [Action] Check the settings of the Device.

6.2 PBR

The following table shows the system messages of the PBR message type.

Table 6-2: System messages of the PBR message type

Message ID	Event level	Message text
		Description and action
11210011	S6	There is a change in the nexthop of an IPv4 policy-based routing list. (policy-list = *<policy list name>*, new priority = *<priority>*)
		A IPv4 policy-based routing list selected the next hop with the priority *<priority>*. • *<policy list name>*: Name of the policy-based routing list • *<priority>*: Priority of the next hop [Action] None.
11210012	S6	There is a change in an IPv4 policy-based routing list based on the default rule. (policy-list = *<policy list name>*)
		The IPv4 policy-based routing list *<policy list name>* selected the default action. • *<policy list name>*: Name of the policy-based routing list [Action] None.
11310011	S6	There is a change in the nexthop of an IPv6 policy-based routing list. (policy-list = *<policy list name>*, new priority = *<priority>*)
		The IPv6 policy-based routing list *<policy list name>* selected the next hop with the priority *<priority>*. • *<policy list name>*: Name of the policy-based routing list • *<priority>*: Priority of the next hop [Action] None.
11310012	S6	There is a change in an IPv6 policy-based routing list based on the default rule. (policy-list = *<policy list name>*)
		The IPv6 policy-based routing list *<policy list name>* selected the default action. • *<policy list name>*: Name of the policy-based routing list [Action] None.

6.3 DHCP

The following table shows the system messages of the DHCP message type.

Table 6-3: System messages of the DHCP message type

Message ID	Event level	Message text
		Description and action
1f01b024	S3	A DHCPv6 packet was discarded by a DHCPv6 relay agent because the number of binding(IA_PD) exceeded the maximum.
		DHCPv6 packets were discarded by the DHCPv6 relay agent because the the maximum number of addresses that can be assigned (IA_PD) was exceeded. After this message is issued, the same system message is not issued until 5 minutes elapses. [Action] 1. Check if the number of addresses that can be assigned (IA_PD) is more than the expected number by using the `show ipv6 dhcp relay binding` command. In addition, check the number of discarded DHCPv6 packets by using the `show ipv6 dhcp relay statistics` command. 2. Check the settings of the DHCPv6 relay agent (the `ipv6 dhcp relay destination` configuration command). 3. Check the network configuration and reconsider the configuration of the Device.

6.4 VRRP

The following table shows the system messages of the VRRP message type.

Table 6-4: System messages of the VRRP message type

Message ID	Event level	Message text
		Description and action
0e008001	S6	The status of a virtual router changed from active to "*<state>*". (interface = *<interface name>*)
		The status of the virtual router changed. • *<state>*: Virtual router state • *<interface name>*: Name of interface on which VRRP is configured [Action] None.
0e008002	S5	A virtual router received a VRRP packet with an IP TTL not equal to 255. (interface = *<interface name>*)
		The virtual router received a VRRP advertisement packet whose TTL (Time-to-Live) in the IP header was not 255. • *<interface name>*: Name of interface on which VRRP is configured [Action] Check the remote devices that make up the same virtual router.
0e008003	S5	A virtual router received a VRRP packet shorter than the VRRP header. (interface = *<interface name>*)
		The virtual router received a VRRP advertisement packet that had an invalid length. • *<interface name>*: Name of interface on which VRRP is configured [Action] Check the remote devices that make up the same virtual router.
0e008004	S5	A virtual router received a VRRP packet that did not pass the authentication check. (interface *<interface name>*)
		Authentication of a received VRRP advertisement packet failed. • *<interface name>*: Name of interface on which VRRP is configured [Action] Check the password settings for the Device and the remote devices that make up the same virtual router.
0e008005	S5	A virtual router received a VRRP packet whose address list differs from the one set for the virtual router. (interface *<interface name>*)
		The IP address of a virtual router specified in a received VRRP advertisement packet does not match the settings of the Device. • *<interface name>*: Name of interface on which VRRP is configured [Action] Check the IP address settings of virtual routers for the Device and for the remote devices that make up the same virtual router.
0e008006	S5	A virtual router received a VRRP packet whose advertisement interval differs from the one set for the local virtual router. (interface *<interface name>*)
		The sending interval specified in a received VRRP advertisement packet does not match the settings of the Device. • *<interface name>*: Name of interface on which VRRP is configured [Action] Check the sending intervals for the Device and the remote devices that make up the same virtual router.

Message ID	Event level	Message text
		Description and action
0e008007	S5	A received VRRP packet has an unsupported VRRP version number.
		The VRRP version specified in a received VRRP advertisement packet does not match the VRRP version of the Device. [Action] When constructing the Device with a virtual router, match the VRRP version of the remote device with the VRRP version of the Device.
0e008012	S6	A virtual router ended. (interface = <*interface name*>)
		The virtual router ended. • <*interface name*>: Name of interface on which VRRP is configured [Action] None.
0e008015	S5	A virtual router received a VRRP packet with an IP hop limit not equal to 255. (interface = <*interface name*>)
		The virtual router received a VRRP advertisement packet whose hop limit in the IP header was not 255. • <*interface name*>: Name of interface on which VRRP is configured [Action] Check the remote devices that make up the same virtual router.
0e008022	S5	An unsupported value is set for the send interval of Advertisement packets. The default value will be used. (interface = <*interface name*>)
		An unsupported value is specified for the interval for sending advertisement packets. The default value is used for `Advertisement Interval`. • <*interface name*>: Name of interface on which VRRP is configured [Action] 1. If the VRRP operation mode is set 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.
0e008023	S5	A virtual router was disabled because the primary virtual router is not running.(interface = <*interface name*>)
		The follower virtual router is disabled because no primary virtual router is configured. • <*interface name*>: Name of interface on which VRRP is configured [Action] Configure a primary virtual router.
0e008024	S6	A virtual router was enabled because the primary virtual router started.(interface = <*interface name*>)
		The follower virtual router was enabled because a primary virtual router was configured. • <*interface name*>: Name of interface on which VRRP is configured [Action] None.

Chapter

7. Unicast Routing

7.1 RIP

The following table shows the system messages of the RIP message type.

Table 7-1: System messages of the RIP message type

Message ID	Event level	Message text
		Description and action
05020100	S5	A received RIP packet was ignored because a version field was 0. (message type = *<rip command>*, source = *<source address>*)
	A received RIP packet was ignored because the version field is 0. • *<rip command>*: Received message type 　Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry • *<source address>*: Source gateway [Action] Check the unicast routing program (RIP) for the source gateway.		
05020101	S5	A received RIP packet was ignored because a reserved field was not 0. (message type = *<rip command>*, source = *<source address>*)
	A received RIP packet was ignored because the reserved field is not 0. • *<rip command>*: Received message type 　Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry • *<source address>*: Source gateway [Action] Check the unicast routing program (RIP) for the source gateway.		
05020201	S5	A received RIP packet was ignored because of an authentication error. (message type = *<rip command>*, source = *<source address>*[, key ID = *<key id>*])
	A received RIP packet was ignored because of an authentication error. This system message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above numbers indicate the total number of times the following messages are output. 　Message type: RIP Message ID: 05020201 　Message type: RIP Message ID: 05020202 　Message type: RIP Message ID: 05020203 　Message type: RIP Message ID: 05020204 • *<rip command>*: Received message type 　Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry • *<source address>*: Source gateway • *<key id>*: Key identifier [Action] 1. Check whether the authentication key for the local device RIP matches the authentication key for the remote device RIP. 2. If they do not match, specify the authentication keys so that they do match.		

Message ID	Event level	Message text
		Description and action
05020202	S5	A received RIP packet was ignored because the authentication type was invalid. (message type = *<rip command>*, source = *<source address>*)
	A received RIP packet was ignored because the authentication type of authentication information is invalid. This system message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above numbers indicate the total number of times the following messages are output. Message type: `RIP` Message ID: 05020201 Message type: `RIP` Message ID: 05020202 Message type: `RIP` Message ID: 05020203 Message type: `RIP` Message ID: 05020204 • *<rip command>*: Received message type `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry` • *<source address>*: Source gateway [Action] Check the unicast routing program (RIP) for the source gateway.	
05020203	S5	A received RIP packet was ignored because the authentication key ID was invalid. (message type = *<rip command>*, source = *<source address>*, key ID = *<key id>*)
	A received RIP packet was ignored because the key identifier of authentication information was invalid. This system message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above numbers indicate the total number of times the following messages are output. Message type: `RIP` Message ID: 05020201 Message type: `RIP` Message ID: 05020202 Message type: `RIP` Message ID: 05020203 Message type: `RIP` Message ID: 05020204 • *<rip command>*: Received message type `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry` • *<source address>*: Source gateway • *<key id>*: Key identifier [Action] 1. 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. 2. If they do not match, specify the key identifier of authentication information so that they do match.	

Message ID	Event level	Message text
		Description and action
05020204	S5	A received RIP packet was ignored because an authentication sequence number was invalid. (message type = *<rip command>*, source = *<source address>*, key ID = *<key id>*)
		A received RIP packet was ignored because the sequence number of authentication information is invalid. This system message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above numbers indicate the total number of times the following messages are output. Message type: `RIP` Message ID: 05020201 Message type: `RIP` Message ID: 05020202 Message type: `RIP` Message ID: 05020203 Message type: `RIP` Message ID: 05020204 • *<rip command>*: Received message type `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry` • *<source address>*: Source gateway • *<key id>*: Key identifier [Action] Check the unicast routing program (RIP) for the source gateway.
05020400	S5	A received route information was ignored because of an invalid metric value. (metric = *<metric>*, destination = *<destination address>*, source = *<source address>*)
		The routing information was ignored because routing information that has an invalid metric value (0, or 17 or larger) was received. • *<metric>*: Metric value of the routing information • *<destination address>*: Routing information destination address • *<source address>*: Source gateway [Action] Check the unicast routing program (RIP) for the source gateway.
05020401	S5	A received route information was ignored because of an invalid network mask. (mask = *<mask>*, source = *<source address>*, destination = *<destination address>*)
		The routing information was ignored because routing information that has an invalid network mask was received. • *<mask>*: Routing information network mask • *<source address>*: Source gateway • *<destination address>*: Routing information destination address [Action] Check the unicast routing program (RIP) for the source gateway.
05020500	S3	The total number of RIP targets exceeded the permitted maximum.
		The total number of RIP targets (neighboring) exceeded the maximum number permitted. [Action] Review the RIP settings so that the maximum number of neighboring routers does not exceed the capacity limit.

7.2 RIPng

The following table shows the system messages of the RIPng message type.

Table 7-2: System messages of the RIPng message type

Message ID	Event level	Message text
		Description and action
05030100	S5	A received RIPng packet was ignored because its packet length was too short. (source = <*source address*>, packet length = <*size*>)
		A received packet was ignored because the packet length was shorter than the RIPng header. • <*source address*>: Source gateway • <*size*>: Packet length [Action] Check the unicast routing program (RIPng) for the source gateway.
05030101	S5	A received RIPng packet was ignored because of an invalid version field value. (message type = <*ripng command*>, source = <*source address*>)
		A received RIPng packet was ignored because the version field was invalid. • <*ripng command*>: Received message type Request, Response • <*source address*>: Source gateway address [Action] Check the unicast routing program (RIPng) for the source gateway.
05030102	S5	A received RIPng packet was ignored because of an invalid hoplimit. (hoplimit = <*hoplimit*>)
		A received RIPng packet was ignored because the hop limit was invalid. • <*hoplimit*>: Received hop limit [Action] Check the unicast routing program (RIPng) for the source gateway.
05030300	S5	A received RIPng packet was ignored because of the invalid length of a route information. (source = <*source address*>)
		A received RIPng packet was ignored because routing information of invalid length was included. • <*source address*>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
05030400	S5	A received RIPng packet was ignored because the source address was not a link-local address. (message type = <*ripng command*>, source = <*source address*>)
		A received RIPng packet was ignored because the source address was not a link-local address. • <*ripng command*>: Received message type • <*source address*>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
05030401	S5	A received RIPng packet was ignored because of the invalid source UDP port number. (message type = <*ripng command*>, source = <*source address*>)
		A received RIPng packet was ignored because the source port was invalid. • <*ripng command*>: Received message type • <*source address*>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.

Message ID	Event level	Message text
		Description and action
05030402	S5	A route information was ignored because of its invalid length. (source = *<source address>*)
		The routing information of the received RIPng packet was ignored because its length was invalid. • *<source address>*: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
05030403	S5	A received route information was ignored because of an invalid metric value. (metric = *<metric>*, prefix = *<prefix>*, source = *<source address>*)
		The routing information was ignored because routing information that has an invalid metric value (0, or 17 or larger) was received. • *<metric>*: Metric value of the routing information • *<prefix>*: Routing information destination prefix • *<source address>*: Source gateway address [Action] Check the unicast routing program (RIPng) for the source gateway.
05030404	S5	A received route information was ignored because of an invalid prefix length. (prefix length = *<prefixlen>*, destination = *<prefix>*, source = *<source address>*)
		The routing information was ignored because routing information that has an invalid prefix length was received. • *<prefixlen >*: Prefix length of the routing information • *<prefix>*: Routing information destination • *<source address>*: Source gateway address [Action] Check the unicast routing program (RIPng) for the source gateway.
05030500	S3	The total number of RIPng targets exceeded the permitted maximum.
		The total number of RIPng targets (neighboring) exceeded the maximum number permitted. [Action] Review the RIPng settings so that the maximum number of neighboring routers does not exceed the capacity limit.

7.3 OSPF

The following table shows the system messages of the OSPF message type.

Table 7-3: System messages of the OSPF message type

Message ID	Event level	Message text
		Description and action
05040000	S6	The adjacency has been established. (router ID = *<router id>*, address = *<address>*, interface = *<interface name>*)
	A connection with the OSPF neighboring router was successfully established. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<interface name>*: Interface name [Action] None.	
05040001	S6	The system finished advertising my own router-LSA as a stub router. (domain = *<domain id>*)
	Router LSA advertising for a stub router has ended. • *<domain id>*: OSPF domain ID [Action] None.	
05040002	S6	A graceful restart succeeded. (domain = *<domain id>*)
	A graceful restart succeeded. • *<domain id>*: OSPF domain ID [Action] None.	
05040100	S4	Sending of an OSPF packet failed. (source = *<source address>*, destination = *<destination address>*, error = *<error string>*)
	An attempt to send an OSPF packet failed. • *<source address>*: Source IPv4 address • *<destination address>*: Destination IPv4 address • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.	

Message ID	Event level	Message text
		Description and action
05040200	S5	A received OSPF packet was ignored because the packet was invalid. (source = <*source address*>, destination = <*destination address*>[, area ID = <*area id*>], log = <*log type*>)
		A received OSPF packet was ignored because it was invalid. • <*source address*>: Source IPv4 address • <*destination address*>: Destination IPv4 address • <*area id*>: Area ID • <*log type*>: One of the following log types: OSPF: invalid checksum OSPF: unknown neighbor OSPF: area mismatch OSPF: invalid virtual link OSPF: authentication type mismatch OSPF: authentication failure HELLO: netmask mismatch HELLO: hello timer mismatch HELLO: dead timer mismatch HELLO: unknown neighbor on NBMA network HELLO: extern option mismatch DD: extern option mismatch HELLO: router id confusion DD: router id confusion [Action] The action to be taken depends on the type of the log. • OSPF: invalid checksum The OSPF checksum is invalid. Check the neighboring routers. • OSPF: unknown neighbor Non-Hello packets were received from the neighboring router that is not recognized by Hello packets, but no action is required. • OSPF: area mismatch • OSPF: invalid virtual link If packets are received from the new neighboring router, review the area settings. In other cases, no action is required. • OSPF: authentication type mismatch • OSPF: authentication failure Review the authentication settings. • HELLO: netmask mismatch • HELLO: hello timer mismatch • HELLO: dead timer mismatch • HELLO: unknown neighbor on NBMA network Review the OSPF interface settings. • HELLO: extern option mismatch • DD: extern option mismatch Review the stub area settings. • HELLO: router id confusion • DD: router id confusion Review the router ID settings.

Message ID	Event level	Message text
		Description and action
05040201	S5	The system stopped forming the adjacency to a neighbor because a received DD packet had invalid LS Type. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*), invalid LS Type = *<lsid> <advertised router id> <ls type>*)
		Adjacency established with the neighboring router was suspended because an invalid LS type is included in the received Database Description packet. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<interface name>*: Interface name • *<lsid>*: LSID of LSA • *<advertised router id>*: LSA advertising router ID • *<ls type>*: LSA LS type code [Action] Check the LSA advertised by the neighboring router.
05040202	S5	The system stopped forming the adjacency to a neighbor stopped because a received LSA differed from a requested LSA. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*), LSA infomation= *<lsid> <advertised router id> <ls type>*)
		Adjacency established with the neighboring router was suspended because an LSA that is different from the requested LSA was received. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<interface name>*: Interface name • *<lsid>*: LSID of LSA • *<advertised router id>*: LSA advertising router ID • *<ls type>*: LSA LS type code [Action] None.
05040203	S5	The adjacency to a neighbor was lost because a received DD packet had an unexpected sequence or optional code. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*), sequence number 1, 2 = *<sequence1>*, *<sequence2>*)
		Adjacency was terminated because the sequence (or the option) of the received Database Description packet did not match. This message is output when the neighboring router is restarted or Database Description packets sent by the Device are not properly received by the neighboring router. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<interface name>*: Interface name • *<sequence1>*: Sequence number in control data • *<sequence2>*: Sequence number in the DD message [Action] None.

Message ID	Event level	Message text
		Description and action
05040204	S5	The adjacency to a neighbor was lost because a requested LSA was not exist in LSDB. (router ID = *<router id>*, address = *<address>*, interface = *<interface name>*, invalid LS request = *<lsid>* *<advertised router id>* *<ls type>*)
	Adjacency was terminated due to a request from the LSA that does not exist in the database. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<interface name>*: Interface name • *<lsid>*: LSID of LSA • *<advertised router id>*: LSA advertising router ID • *<ls type>*: LSA LS type code [Action] Check the unicast routing program (OSPF) of the neighboring router.	
05040300	S5	The adjacency to a neighbor was lost because the adjacency timed out. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*)
	Adjacency was terminated because Hello packets were not received during a given interval after the last Hello packet was received from the neighboring router. This message is output when the neighboring router is deactivated, or if a problem occurs in communication between the Device and the neighboring router. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<interface name>*: Interface name [Action] If this error occurs frequently, shorten the interval for sending Hello packets (hello-interval) or extend the length of time that adjacency is to be maintained (dead-interval).	
05040301	S5	The adjacency to a neighbor was lost because a neighbor did not receive a Hello packet recently. (router ID = *<router id>*, address = *<address>*, interface = *<interface name>*)
	Adjacency was terminated because the neighboring router no longer recognizes the Device. This message is output when the neighboring router is restarted or Hello packets sent by the Device are not properly received by the neighboring router. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<interface name>*: Interface name [Action] If this error occurs frequently, shorten the interval for sending Hello packets (hello-interval) or extend the length of time that adjacency is to be maintained (dead-interval).	
05040400	S5	A graceful restart failed because a neighbor was not running as a helper. (router ID = *<router id>*, address = *<address>*, domain = *<domain id>*)
	A graceful restart failed because the neighboring router is not operating as a helper. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<domain id>*: OSPF domain ID [Action] Check the configuration of a graceful restart of the neighboring router.	

Message ID	Event level	Message text
		Description and action
05040401	S5	A graceful restart failed because a neighbor stopped working as a helper. (router ID = *<router id>*, address = *<address>*, domain = *<domain id>*)
	A graceful restart failed because the neighboring router stopped operating as a helper. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address • *<domain id>*: OSPF domain ID [Action] If this error occurs frequently, check the OSPF status of the neighboring router and the cause of termination of the helper operation.	
05040402	S5	A graceful restart failed because the system failed in LSA synchronization between all the neighbors. (domain = *<domain id>*)
	A graceful restart failed because reconnection and LSA synchronization with all of the neighboring routers connected before the restart could not be performed within the restart time. • *<domain id>*: OSPF domain ID [Action] Check the configuration of the restart time.	
05040500	S5	The system stopped acting as a helper because the network topology changed. (router ID = *<router id>*, address = *<address>*)
	The helper operation stopped because the topology was changed. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address [Action] None.	
05040501	S5	The system stopped acting as a helper because the restart timed out. (router ID = *<router id>*, address = *<address>*)
	The helper operation stopped because the waiting time for restart elapsed. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's IPv4 address [Action] 1. Check if the neighboring router has stopped the restart operation. 2. If it has not stopped, review the restart time of the neighboring router.	

7.4 OSPFv3

The following table shows the system messages of the `OSPFv3` message type.

Table 7-4: System messages of the OSPFv3 message type

Message ID	Event level	Message text
		Description and action
05050000	S6	The adjacency has been established. (router ID = *<router id>*, interface = *<interface name>*)
	A connection with the OSPFv3 neighboring router was successfully established. • *<router id>*: Neighboring router's router ID • *<interface name>*: Interface name [Action] None.	
05050001	S6	The system finished advertising my own router-LSA as a stub router. (domain = *<domain id>*
	Router LSA advertising for a stub router has ended. • *<domain id>*: OSPFv3 domain ID [Action] None.	
05050002	S6	A graceful restart succeeded. (domain = *<domain id>*)
	A graceful restart succeeded. • *<domain id>*: OSPFv3 domain ID [Action] None.	
05050100	S4	Sending of an OSPFv3 packet failed. (source = *<source address>* (*<interface name>*), destination = *<destination address>*, error = *<error string>*)
	An attempt to send an OSPFv3 packet failed. • *<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.	

Message ID	Event level	Message text
		Description and action
05050200	S5	A received OSPFv3 packet was ignored because the packet was invalid. ([area = *<area id>*,]router ID = *<router id>*[(*<interface name>*)], destination = *<destination address>*, log = *<log type>*)
		A received OSPFv3 packet was ignored because it was invalid. • *<area id>*: Area ID • *<router id>*: Neighboring router's router ID • *<interface name>*: Interface name • *<destination address>*: Destination IPv6 address • *<log type>*: One of the following log types: invalid checksum unknown neighbor area mismatch invalid virtual link HELLO: hello timer mismatch HELLO: dead timer mismatch HELLO: extern option mismatch DD: extern option mismatch HELLO: router id confusion DD: router id confusion [Action] The action to be taken depends on the type of the log. • invalid checksum The OSPFv3 header checksum is invalid. Check the neighboring routers. • unknown neighbor Non-Hello packets were received from the neighboring router that is not recognized by Hello packets, but no action is required. • area mismatch • invalid virtual link If packets are received from the new neighboring router, review the area settings. In other cases, no action is required. • HELLO: hello timer mismatch • HELLO: dead timer mismatch Review the OSPFv3 interface settings. • HELLO: extern option mismatch • DD: extern option mismatch Review the stub area settings. • HELLO: router id confusion • DD: router id confusion Review the router ID settings.
05050201	S5	The system stopped forming the adjacency to a neighbor because a received DD packet had invalid LS Type. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*), invalid LS Type = *<lsid>* *<advertised router id>* *<ls type>*
		Adjacency established with the neighboring router was suspended because an invalid LS type is included in the received Database Description packet. This message is output when the scope value of LS Type is invalid. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's address • *<interface name>*: Interface name • *<lsid>*: LSID of LSA • *<advertised router id>*: LSA advertising router ID • *<ls type>*: LSA LS type code [Action] Check the LSA advertised by the neighboring router.

Message ID	Event level	Message text
		Description and action
05050202	S5	The system stopped forming the adjacency to a neighbor because a received LSA differed from a requested LSA. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*), LSA info.= *<lsid> <advertised router id> <ls type>*
	Adjacency established with the neighboring router was suspended because an LSA that is different from the requested LSA was received. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's address • *<interface name>*: Interface name • *<lsid>*: LSID of LSA • *<advertised router id>*: LSA advertising router ID • *<ls type>*: LSA LS type code [Action] None.		
05050203	S5	The adjacency to a neighbor was lost because a received DD packet had an unexpected sequence number or optional code. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*), sequence number 1, 2 = *<sequence1>*, *<sequence2>*)
	Adjacency was terminated because the sequence or option of the received Database Description packet did not match. This message is output when the neighboring router is restarted or Database Description packets sent by the Device are not properly received by the neighboring router. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's address • *<interface name>*: Interface name • *<sequence1>*: Sequence number in control data • *<sequence2>*: Sequence number in the DD message [Action] None.		
05050204	S5	The adjacency to a neighbor was lost because a requested LSA was not exist in LSDB. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*), invalid LS request = *<lsid> <advertised router id> <ls type>*)
	Adjacency was terminated due to a request from the LSA that does not exist in the database. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's address • *<interface name>*: Interface name • *<lsid>*: LSID of LSA • *<advertised router id>*: LSA advertising router ID • *<ls type>*: LSA LS type code [Action] Check the unicast routing program (OSPFv3) of the neighboring router.		
05050300	S5	The adjacency to a neighbor was lost because the adjacency timed out. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*))
	Adjacency was terminated because Hello packets were not received during a given interval after the last Hello packet was received from the neighboring router. This message is output when the neighboring router is deactivated, or if a problem occurs in communication between the Device and the neighboring router. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's address • *<interface name>*: Interface name [Action] If this error occurs frequently, shorten the interval for sending Hello packets (hello-interval) or extend the length of time that adjacency is to be maintained (dead-interval).		

Message ID	Event level	Message text
		Description and action
05050301	S5	The adjacency to a neighbor was lost because a neighbor did not receive a Hello packet recently. (router ID = *<router id>*, address (name) = *<address>* (*<interface name>*)
		Adjacency was terminated because the neighboring router no longer recognizes the Device. This message is output when the neighboring router is restarted or Hello packets sent by the Device are not properly received by the neighboring router. • *<router id>*: Neighboring router's router ID • *<address>*: Neighboring router's address • *<interface name>*: Interface name [Action] If this error occurs frequently, shorten the interval for sending Hello packets (hello-interval) or extend the length of time that adjacency is to be maintained (dead-interval).
05050400	S5	A graceful restart failed because a neighbor was not running as a helper. (domain = *<domain id>*, router ID = *<router id>*)
		A graceful restart failed because the neighboring router is not operating as a helper. • *<domain id>*: OSPFv3 domain ID • *<router id>*: Neighboring router's router ID [Action] Check the configuration of a graceful restart of the neighboring router.
05050401	S5	A graceful restart failed because a neighbor stopped working as a helper. (domain = *<domain id>*, router ID = *<router id>*)
		A graceful restart failed because the neighboring router stopped operating as a helper. • *<domain id>*: OSPFv3 domain ID • *<router id>*: Neighboring router's router ID [Action] If this error occurs frequently, check the OSPF status of the neighboring router and the cause of termination of the helper operation.
05050402	S5	A graceful restart failed because the system failed in LSA synchronization between all the neighbors. (domain = *<domain id>*)
		A graceful restart failed because reconnection and LSA synchronization with all of the neighboring routers connected before the restart could not be performed within the restart time. • *<domain id>*: OSPFv3 domain ID [Action] Check the configuration of the restart time.
05050500	S5	The system stopped acting as a helper because the network topology changed. (router ID = *<router id>*)
		The helper operation stopped because the topology was changed. • *<router id>*: Neighboring router's router ID [Action] None.
05050501	S5	The system stopped acting as a helper because the restart timed out. (router ID = *<router id>*)
		The helper operation stopped because the waiting time for restart elapsed. • *<router id>*: Neighboring router's router ID [Action] 1. Check if the neighboring router has stopped the restart operation. 2. If it has not stopped, review the restart time of the neighboring router.

7.5 BGP4

The following table shows the system messages of the BGP4 message type.

Table 7-5: System messages of the BGP4 message type

Message ID	Event level	Message text
		Description and action
05070000	S5	A peer connection has been established. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was established. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05070001	S5	A peer connection closed because of a change in the interface state. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected due to a change in the interface state. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] Check the cause of the change in the interface state.
05070003	S6	A peer connection closed because the peer configuration was deleted. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected due to a change (deletion or change of the peer information) in the configuration. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05070004	S6	A peer connection closed because of a configuration change. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected due to a change in the configuration. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05070005	S6	A peer connection closed because of the execution of 'clear ip bgp' command. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected by executing the `clear ip bgp` command. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05070006	S6	A peer connection has been reestablished in a graceful restart. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was reestablished. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.

Message ID	Event level	Message text
		Description and action
05070007	S6	An End-Of-RIB marker was received. (source = *<bgp name>*[(*<description>*)])
		End-Of-RIB was received. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] None.
05070008	S6	An End-Of-RIB marker was sent. (destination peer = *<bgp name>*[(*<description>*)])
		End-Of-RIB was sent. • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer [Action] None.
05070009	S6	Learning of a route information from receiving routers has finished.
		Route learning from receiving routers has finished. [Action] None.
05070010	S5	The system has stopped route learning from at least one receive router and started route advertisement.
		Route learning from some of the receiving routers will be stopped, and route advertisement will start. [Action] None.
05070100	S4	A connection to a peer failed because the local address was unusable. (peer = *<bgp name>*[(*<description>*)], address = *<ipv4 address>*)
		An attempt to establish a connection failed because the address used for establishing a connection with the relevant peer could not be used. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer • *<ipv4 address>*: Address used for peering [Action] If this error occurs frequently, check the cause of the error.
05070101	S3	The peer remains in idle state because the interface to be used to the peer connection was not found. (peer = *<bgp name>*[(*<description>*)])
		The peer remains in an idle state because the interface connected to the relevant peer cannot be found. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] 1. Check the configuration. 2. If the configuration is correct, check the state of the interface to be connected with the relevant peer.

Message ID	Event level	Message text
		Description and action
05070102	S3	The peer remains in idle state because the local address to be used to the peer connection was not on the same network as the peer. (peer = *<bgp name>*[(*<description>*)], address = *<ipv4 address>*)
	The peer remains in an idle state because the address used for connecting with the relevant peer does not exist in the same network. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer • *<ipv4 address>*: Address used for establish a connection [Action] Check the configuration.	
05070103	S3	The peer remains in idle state because the interface for the local address to be used to the peer connection was not found. (peer = *<bgp name>*[(*<description>*)], local address = *<ipv4 address>*)
	The peer remains in an idle state because the interface for the device used for connecting with the relevant peer cannot be found. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer • *<ipv4 address>*: Address used for establish a connection [Action] Check the configuration.	
05070200	S4	A connection request was ignored because an acceptance of a connection failed. (socket = *<socket>*, error = *<error string>*)
	The connection request was ignored because acceptance of the connection failed. • *<socket>*: Socket descriptor number • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.	
05070201	S4	The connection will be closed because a fetching of the address to be used to connection failed.
	The connection will be disconnected because extraction of the address used for establishing a connection failed. [Action] If this error occurs frequently, check the unicast routing program (BGP4) in the peer.	

Message ID	Event level	Message text
		Description and action
05070202	S5	A connection request was ignored because no MD5 digest was attached to the received TCP segment. (source IPv4 + TCP port = *<source ipv4>* + *<TCP port no.>*, destination IPv4 + TCP port = *<destination ipv4>* + *<TCP port no.>*)

		The connection request was ignored because the MD5 authentication option is not set for the received TCP segment. This system message is output according to the following conditions:
		 1. The messages from the first to the 16th event are output.
		 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs.
		 3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above.
		 Note that the above numbers indicate the total number of times the following messages are output.
		  Message type: BGP4 Message ID: 05070202
		  Message type: BGP4 Message ID: 05070203
		 • *<source ipv4>*: Source IPv4 address
		 • *<TCP port no.>*: TCP port number
		 • *<destination ipv4>*: Destination IPv4 address
		 [Action]
		 1. Check whether the MD5 authentication is set in BGP4 of the remote device.
		 2. If it is not set, set the MD5 authentication so that it matches.
		 3. If the setting matches, check whether TCP segments are sent from a peer other than the source BGP4 peer.

05070203	S5	A connection request was ignored because an invalid MD5 digest was attached. (source IPv4 + TCP port = *<source ipv4>* + *<TCP port no.>*, destination IPv4 + TCP port = *<destination ipv4>* + *<TCP port no.>*)

		The connection request was ignored because the MD5 authentication option for the received TCP segment is invalid. This system message is output according to the following conditions:
		 1. The messages from the first to the 16th event are output.
		 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs.
		 3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above.
		 Note that the above numbers indicate the total number of times the following messages are output.
		  Message type: BGP4 Message ID: 05070202
		  Message type: BGP4 Message ID: 05070203
		 • *<source ipv4>*: Source IPv4 address
		 • *<TCP port no.>*: TCP port number
		 • *<destination ipv4>*: Destination IPv4 address
		 [Action]
		 1. Check if the MD5 authentication keys match in BGP4 of the local and remote devices.
		 2. If the MD5 authentication keys do not match, set them so that they do match.
		 3. If the MD5 authentication keys match, check if TCP segments are sent from a peer other than the source BGP4 peer.

05070300	S4	A peer connection closed because a message could not be sent to the peer owing to the lack of space in socket buffer. (send request message length = *<length>* bytes, destination peer = *<bgp name>*[(*<description>*)], error = *<error string>*)
		An attempt to send a message to the relevant peer failed because the socket buffer became full. The connection with the relevant peer was disconnected. • *<length>*: Send request message length • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.

Message ID	Event level	Message text
		Description and action
05070301	S4	A peer connection closed because a message could not be sent to the peer. (message length = *\<length\>* bytes, destination peer = *\<bgp name\>*[(*\<description\>*)], error = *\<error string\>*)
		The connection with the relevant peer was disconnected because an attempt to send a message to that peer failed. • *\<length\>*: Send request message length • *\<bgp name\>*: Target peer name • *\<description\>*: Description name of the destination peer • *\<error string\>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05070302	S5	A message could not be sent to a peer because the connection closed. (send request = *\<length\>* bytes, destination peer = *\<bgp name\>*[(*\<description\>*)])
		An attempt to send the message to the relevant peer failed because the connection was disconnected. • *\<length\>*: Send request message length • *\<bgp name\>*: Target peer name • *\<description\>*: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.
05070303	S4	A peer connection closed because the system had repeatedly failed in sending a message to the peer. (destination peer = *\<bgp name\>*[(*\<description\>*)], error = *\<error string\>*)
		The connection with the relevant peer was disconnected because the system had repeatedly failed in sending a message to the peer. • *\<bgp name\>*: Target peer name • *\<description\>*: Description name of the destination peer • *\<error string\>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05070304	S4	A peer connection closed because the system failed in sending a message to the peer. (send request = *\<length1\>* bytes, sent data = *\<length2\>* bytes, destination peer = *\<bgp name\>*[(*\<description\>*)], error = *\<error string\>*)
		The connection with the relevant peer was disconnected because an attempt to send a message to that peer failed. • *\<length1\>*: Send request data length • *\<length2\>*: Sent data length • *\<bgp name\>*: Target peer name • *\<description\>*: Description name of the destination peer • *\<error string\>*: Error cause [Action] If this error occurs frequently, check the cause of the error.

Message ID	Event level	Message text
		Description and action
05070305	S5	A message was not sent to a peer because the peer connection closed. (send request = *<length1>* bytes, sent data = *<length2>* bytes, destination peer = *<bgp name>*[(*<description>*)])
		An attempt to send the message to the relevant peer failed because the connection was disconnected. • *<length1>*: Send request data length • *<length2>*: Sent data length • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.
05070306	S5	A peer connection closed because the system had repeatedly failed in sending a message to the peer. (destination peer = *<bgp name>*[(*<description>*)], sent data = *<length1>*, remaining = *<length2>*, error = *<error string>*)
		The connection with the relevant peer was disconnected because the system had repeatedly failed in sending a message to the peer. • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<length1>*: Sent data length • *<length2>*: Length of the data that remains unsent • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05070307	S4	A peer connection closed because the system had repeatedly failed in sending KEEPALIVE messages to the peer. (destination peer = *<bgp name>*[(*<description>*)], error = *<error string>*)
		The connection with the relevant peer was disconnected because the system had repeatedly failed in sending KEEPALIVE messages to the peer. • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.

Message ID	Event level	Message text
		Description and action
05070308	S5	A NOTIFICATION message was sent to a peer. (destination peer = *<bgp name>*[(*<description>*)], code = *<code>* (*<code string>*)[, sub code = *<sub code>* (*<sub code string>*)][, value = *<value>*][, data = *<data>*])

	A NOTIFICATION message was sent to the relevant peer.
	• *<bgp name>*: Target peer name
	• *<description>*: Description name of the destination peer
	• *<code>* (*<code string>*): Error code
	• *<sub code>* (*<sub code string>*): Error subcode
	  Error code 1 (Message Header Error)
	   - Error subcode 1 (lost connection synchronization)
	   - Error subcode 2 (bad length)
	   - Error subcode 3 (bad message type)
	  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 code 3 (UPDATE Message Error)
	   - Error subcode 1 (invalid attribute list)
	   - Error subcode 2 (unknown well known attribute)
	   - Error subcode 3 (missing well known attribute)
	   - Error subcode 4 (attribute flags error)
	   - Error subcode 5 (bad attribute length)
	   - Error subcode 6 (bad ORIGIN attribute)
	   - Error subcode 9 (error with optional attribute)
	   - Error subcode 10 (bad address or prefix field)
	   - Error subcode 11 (AS path attribute problem)
	  Error code 4 (Hold Timer Expired Error)
	  Error code 5 (Finite State Machine Error)
	  Error code 6 (Cease)
	  invalid: *<code string>* for invalid *<code>*
	  unknown: *<sub code string>* for invalid *<sub code>*
	• *<value>*: Information in the data field of the NOTIFICATION message (Decimal representation)
	• *<data>*: Information in the data field of the NOTIFICATION message (Hexadecimal representation)
	[Action]
	1. Check the network configuration and peer configuration.
	2. If there is no problem with them, check the unicast routing program (BGP4) in the peer.	

05070400	S5	A peer connection closed because a header marker in the received message was invalid. (peer = *<bgp name>* [(*<description>*)])
	The connection with the relevant peer was disconnected because a header marker in the received message was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.	

Message ID	Event level	Message text
		Description and action
05070401	S5	A NOTIFICATION message from a peer was truncated. (peer = *<bgp name>*[(*<description>*)], length = *<length>*)
		The length of the NOTIFICATION message received from the relevant peer was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Received data length [Action] Check the unicast routing program (BGP4) in the peer.
05070402	S5	A peer connection closed because there was an error in an UPDATE message from the peer. (error = *<code>* (*<error string>*), peer = *<bgp name>*[(*<description>*)], *<length>* bytes error data, first 5 bytes = *<error data>*)
		The connection with the relevant peer was disconnected because there was an error in an UPDATE message from the peer. • *<code>* (*<error string>*): Error cause • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Error data length • *<error data>*: First 5 bytes of error data [Action] Check the unicast routing program (BGP4) in the peer.
05070403	S4	A peer connection closed because the system failed in receiving a message from the peer. (source = *<bgp name>*[(*<description>*)], error = *<error string>*)
		The connection with the relevant peer was disconnected because the system failed in receiving a message from the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05070404	S5	A peer connection closed because the system failed in receiving a message from the peer owing to an unexpected EOF. (source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the system failed in receiving a message from the peer owing to an unexpected EOF. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] If this error occurs frequently, check the cause of the disconnection.
05070405	S5	A peer connection closed because of an invalid message length. (source = *<bgp name>*[(*<description>*)], message type = *<message type>*, length = *<length>*)
		The connection with the relevant peer was disconnected because an invalid-length message was received from that peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<message type>*: Received message type invalid, OPEN, UPDATE, NOTIFICATION, KEEPALIVE • *<length>*: Received data length [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070406	S5	A peer connection closed because of a reception of an unexpected message type. (source = *<bgp name>*[(*<description>*)], received type = *<message type1>*, expected type = *<message type2>*[or *<message type 2>*])

	The connection with the relevant peer was disconnected because a message whose message type is inappropriate for the current state was received from that peer.
	• *<bgp name>*: Source peer name
	• *<description>*: Description name of the source peer
	• *<message type1>*: Received message type
	  invalid, OPEN, UPDATE, NOTIFICATION, KEEPALIVE
	• *<message type2>*: Message type appropriate for the current state
	  invalid, OPEN, UPDATE, NOTIFICATION, KEEPALIVE
	[Action]
	Check the unicast routing program (BGP4) in the peer.	

05070407	S5	A peer connection closed because an OPEN message from the peer was too short. (source = *<bgp name>*[(*<description>*)], BGP version in message = *<version>*, message length = *<length>* octets)
	The connection with the relevant peer was disconnected because an OPEN message from the peer was too short. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<version>*: BGP version number in the received message • *<length>*: Received data length [Action] Check the unicast routing program (BGP4) in the peer.	
05070408	S5	A peer connection closed because an OPEN message from a peer had an unsupported BGP version. (version = *<version>*, peer = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because an OPEN message that has an unsupported BGP version number was received from that peer. • *<version>*: BGP version number of received messages • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Make sure that the peer supports BGP4.	
05070409	S5	A peer connection closed because the holdtime in an OPEN message from the peer was too small. (source = *<bgp name>*[(*<description>*)], holdtime = *<holdtime>*)
	The connection with the relevant peer was disconnected because an OPEN message whose hold time is less than three seconds was received from that peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<holdtime>*: Hold time in the received message [Action] Check the peer configuration.	

Message ID	Event level	Message text
		Description and action
05070410	S5	A peer connection closed because the BGP identifier in an OPEN message from the peer was invalid. (source = *<bgp name>*[(*<description>*)], invalid ID = *<router id>*)
	The connection with the relevant peer was disconnected because an OPEN message that has an invalid BGP identifier was received from that peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<router id>*: BGP identifier in the received message [Action] Check the unicast routing program (BGP4) in the peer.	
05070411	S5	A peer connection closed because an OPEN message from the peer had an invalid option code. (source = *<bgp name>*[(*<description>*)], option code = *<option>*)
	The connection with the relevant peer was disconnected because an OPEN message from the peer had an invalid option code. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<option>*: Option code in the received message [Action] Check the unicast routing program (BGP4) in the peer.	
05070412	S3	A peer connection closed because an OPEN message from the peer had an AS number different from the configured one. (source = *<bgp name>*[(*<description>*)], message AS. = *<as1>*, configured AS. = *<as2>*)
	The connection with the relevant peer was disconnected because an OPEN message from the peer had an AS number different from the configured one. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<as1>*: AS number of the received message • *<as2>*: AS number of the peer in the configuration [Action] Check the configuration.	
05070413	S5	A peer connection closed because the BGP version in a KEEPALIVE message from the peer was not supported by the system. (source = *<bgp name>*[(*<description>*)], source version = *<version1>*, this system's version = *<version2>*)
	The connection with the relevant peer was disconnected because a KEEPALIVE message that has a mismatched BGP version number was received from that peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<version1>*: Remote BGP version number • *<version2>*: Local BGP version number [Action] Make sure that the peer supports BGP4.	
05070414	S3	A peer connection closed because the peer sending an OPEN message was not configured in the system. (source = *<bgp name>*)
	The connection with the relevant peer was disconnected because the peer sending an OPEN message was not configured in the system. • *<bgp name>*: Source peer name [Action] Check the configuration.	

Message ID	Event level	Message text
		Description and action
05070415	S5	A peer connection closed because an OPEN message was sent from the peer in an unexpected state. (source = *<bgp name>*[(*<description>*)], state = *<state>*)
		The connection with the relevant peer was disconnected because an OPEN message was received from that peer during the Idle, OpenConfirm, or Established state. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<state>*: Peer state Idle, OpenConfirm, Established [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
05070416	S5	A peer connection closed because of an unsupported BGP version in an OPEN message. (received version = *<version>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an OPEN message that has an unsupported BGP version number was received from that peer. • *<version>*: BGP version number of received messages • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the BGP version supported by the peer.
05070417	S5	An OPEN message was ignored because of an unexpected extra data. (source = *<bgp name>*[(*<description>*)])
		The OPEN message was ignored because unnecessary data is appended to the message from the relevant peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070418	S3	The configured Capabilities for the system did not match with the received Capabilities from a peer. Only a set of matched capabilities has been enabled for the peer. (source = *<bgp name>*[(*<description>*)])
		The capability settings of the Device do not match with the capability received from the peer. Only the matched capability is enabled. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the configuration.
05070419	S5	A peer connection closed because the message length in a message from the peer was invalid. (source = *<bgp name>*[(*<description>*)], length in header = *<length>*)
		The connection with the relevant peer was disconnected because the message length in a message from the peer was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Message length of the received message header [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070420	S5	A peer connection closed because a message type in a message from the peer was invalid. (source = *<bgp name>*[(*<description>*)], type = *<type>*)
		The connection with the relevant peer was disconnected because the message type of a message received from that peer is invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<type>*: Message type [Action] Check the unicast routing program (BGP4) in the peer.
05070421	S5	A peer connection closed because an OPEN message was received from the peer in the Established state. (source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an OPEN message was received from the peer in the ESTABLISHEDstate. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
05070422	S5	A peer connection closed because of a too short UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)], message length = *<length>*)
		The connection with the relevant peer was disconnected because of a too short UPDATE message from the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Received data length [Action] Check the unicast routing program (BGP4) in the peer.
05070423	S5	A peer connection closed because an unreachable prefix length of an UPDATE message from the peer exceeded the message length. (prefix length = *<length1>*, message length = *<length2>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an unreachable prefix length of an UPDATE message from the peer exceeded the message length. • *<length1>*: Prefix length of unreachable routing information in the received message • *<length2>*: Received data length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070424	S5	An UPDATE message was ignored because a path attribute length of the UPDATE message from a peer was 0, but there was a data in the path attribute. (source = *<bgp name>*[(*<description>*)], data length = *<length>* bytes)
		The attribute length of the UPDATE message from the relevant peer is 0 even though actual data exists. The UPDATE message was ignored. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Actual data length [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070425	S5	A peer connection closed because a path attribute length of an UPDATE message from the peer exceeded the actual path attribute length. (received attribute lengths = *<length1>*, actual length = *<length2>*, source = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because a path attribute length of an UPDATE message from the peer exceeded the actual path attribute length. • *<length1>*: Path attribute length of the received message • *<length2>*: Entity data length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.	
05070426	S5	A peer connection closed because there was no nexthop attribute in an UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because there was no nexthop attribute in an UPDATE message from the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.	
05070427	S5	The LOCALPREF attribute in an UPDATE message was ignored because the UPDATE message was sent from an external peer. (source = *<bgp name>*[(*<description>*)])
	The LOCALPREF attribute is included in the UPDATE message from the external peer. The LOCALPREF attribute was ignored. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.	
05070428	S5	A peer connection closed because there was no LOCALPREF attribute in a received UPDATE message from the internal peer. (source = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because there was no LOCALPREF attribute in a received UPDATE message from the internal peer. • *<bgp name>*: Source peer number • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.	
05070429	S5	The UPDATE message was ignored because a received UPDATE message from a peer had no reachable prefixes in a path attribute. (source = *<bgp name>*[(*<description>*)])
	The UPDATE message was ignored because the UPDATE message from the relevant peer has path attributes but does not have the corresponding routing information. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.	

Message ID	Event level	Message text
		Description and action
05070430	S5	A peer connection closed because an UPDATE message from the peer had an invalid prefix length in the unreachable route information. (source = *<bgp name>*[(*<description>*)], prefix length = *<length>*)
		The connection with the relevant peer was disconnected because the prefix length of unreachable routing information of the UPDATE message received from that peer is invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Prefix length in received messages [Action] Check the unicast routing program (BGP4) in the peer.
05070431	S5	A peer connection closed because a prefix length in an UPDATE message from the peer exceeded the remaining unreachable prefix data. (received prefix length = *<length1>*, actual length = *<length2>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the prefix length of unreachable routing information of the UPDATE message received from that peer exceeds the prefix data of unreachable routing information. • *<length1>*: Prefix length in received messages • *<length2>*: Entity data length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070434	S5	A route information was ignored because an UPDATE message from a peer had an invalid unreachable route. (route = *<ipv4 address>*/*<mask>*, source = *<bgp name>*[(*<description>*)], location = *<length1>* of *<length2>*)
		Invalid routes of unreachable routing information of the UPDATE message received from the relevant peer are ignored. • *<ipv4 address>*: Destination address of unreachable routing information • *<mask>*: Network mask of unreachable routing information • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length1>* of *<length2>*: The location of invalid information in the message [Action] Check the unicast routing program (BGP4) in the peer.
05070435	S5	A peer connection closed because an UPDATE message from the peer in AS *<as1>* had an AS-path with the first-hop AS *<as2>*. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an UPDATE message from the peer in AS *<as1>* had an AS-path with the first-hop AS *<as2>*. • *<as1>*: AS number of the source peer • *<as2>*: Next-hop AS number in the received message • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070436	S5	A peer connection closed because of an invalid prefix length in an UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)], prefix length = *<length>*)
	The connection with the relevant peer was disconnected because the prefix length of the UPDATE message received from that peer is invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Prefix length in received messages [Action] Check the unicast routing program (BGP4) in the peer.	
05070437	S5	A peer connection closed because a prefix length in an UPDATE message from the peer exceeded the actual prefix length. (received prefix length = *<length1>*, actual length = *<length2>*, source = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because the prefix length of the UPDATE message received from that peer exceeds the actual prefix length. • *<length1>*: Prefix length in received messages • *<length2>*: Actual prefix length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.	
05070440	S5	An invalid route information was ignored in an UPDATE message from a peer. (source = *<bgp name>*[(*<description>*)], address = *<ipv4 address>*/*<mask>*, location = *<length1>* of *<length2>*)
	The route was ignored because the UPDATE message received from the peer includes invalid routes. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<ipv4 address>*: Destination address • *<mask>*: Network mask • *<length1>* of *<length2>*: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.	
05070441	S5	A network 0 route from a peer was ignored. (destination address = *<ipv4 address>*/*<mask>*, peer = *<bgp name>*[(*<description>*)], invalid info. in message = *<length1>* of *<length2>*)
	Routes addressed to network 0 from the relevant peer are ignored. • *<ipv4 address>*: Destination address • *<mask>*: Network mask • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length1>* of *<length2>*: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.	
05070442	S5	A loopback route from a peer was ignored. (source = *<bgp name>*[(*<description>*)], location = *<length1>* of *<length2>*)
	Loopback routes from the relevant peer are ignored. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length1>* of *<length2>*: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.	

Message ID	Event level	Message text
		Description and action
05070443	S5	A peer connection closed because of an invalid MP_UNREACH_NLRI attribute length in an UPDATE message. (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the length of the MP_UNREACH_NLRI attribute for the UPDATE message from that peer was invalid. • *<length>*: Received MP_UNREACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070444	S5	The MP_UNREACH_NLRI attribute was ignored because of an invalid address family in the MP_UNREACH_NLRI attribute in an UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)], address family = *<address family>*)
		The MP_UNREACH_NLRI attribute was ignored because the address family of the MP_UNREACH_NLRI attribute for the UPDATE message received from the peer is invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<address family>*: Address family information of the received MP_UNREACH_NLRI attribute [Action] Check the unicast routing program (BGP4) in the peer.
05070445	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message from the peer (no address family length). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. No address family exists. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070446	S5	The MP_REACH_NLRI attribute was ignored because of an invalid address family in the MP_REACH_NLRI attribute in an UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)], address family = *<address family>*)
		The MP_REACH_NLRI attribute was ignored because the address family of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<address family>*: Address family information of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) in the peer.
05070447	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message from the peer (no nexthop length field). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. The length of the next-hop attribute has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070448	S5	A peer connection closed because of an invalid nexthop length in the MP_REACH_NLRI attribute in a UPDATE message from the peer. (nexthop length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because of an invalid nexthop length in the MP_REACH_NLRI attribute in a UPDATE message from the peer. • *<length>*: Next-hop length of the received MP_REACH_NLRI attribute • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070449	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute in an UPDATE message from the peer (no nexthop). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. The next hop has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070450	S5	A peer connection closed because of an invalid nexthop route distinguisher (RD) in the MP_REACH_NLRI attribute of an UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)], nexthop RD = *<rd1>*:*<rd2>*)
		The connection with the relevant peer was disconnected because the next-hop route identifier (RD) of the MP_REACH_NLRI attribute for the UPDATE message received from that peer was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<rd1>*:*<rd2>*: Next-hop RD of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) in the peer.
05070451	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message from the peer (no reserved field attribute length). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. The length of the reserved field attribute has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070452	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message from the peer (no SNPA length). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. The length of the SNPA attribute has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
05070453	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute in an UPDATE message from the peer (no SNPA). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. SNPA has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070454	S5	A peer connection closed because a NOTIFICATION message was received from a peer. (source = *<bgp name>*[(*<description>*)], code = *<code>* (*<code string>*)[, sub code = *<sub code>* (*<sub code string>*)][, value = *<value>*][, data = *<data>*])

		The connection with the relevant peer was disconnected because a NOTIFICATION message was received from a peer.
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		• *<code>* (*<code string>*): Error code
		• *<sub code>* (*<sub code string>*): Error subcode
		  Error code 1 (Message Header Error)
		   - Error subcode 1 (lost connection synchronization)
		   - Error subcode 2 (bad length)
		   - Error subcode 3 (bad message type)
		  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)
		  Error code 3 (UPDATE Message Error)
		   - Error subcode 1 (invalid attribute list)
		   - Error subcode 2 (unknown well known attribute)
		   - Error subcode 3 (missing well known attribute)
		   - Error subcode 4 (attribute flags error)
		   - Error subcode 5 (bad attribute length)
		   - Error subcode 6 (bad ORIGIN attribute)
		   - Error subcode 7 (AS loop detected)
		   - Error subcode 8 (invalid NEXT_HOP)
		   - Error subcode 9 (error with optional attribute)
		   - Error subcode 10 (bad address or prefix field)
		   - Error subcode 11 (AS path attribute problem)
		  Error code 4 (Hold Timer Expired Error)
		  Error code 5 (Finite State Machine Error)
		  Error code 6 (Cease)
		  `invalid`: *<code string>* for invalid *<code>*
		  `unknown`: *<sub code string>* for invalid *<sub code>*
		• *<value>*: Information in the data field of the NOTIFICATION message (Decimal representation)
		• *<data>*: Information in the data field of the NOTIFICATION message (Hexadecimal representation)
		[Action]
		Check the network configuration and peer configuration.

05070455	S5	All routes learned from a peer will be deleted because the peer in a graceful restart could not retain the forwarding routes. (peer =*<bgp name>*)
		All routes learned from a peer will be deleted because the peer in a graceful restart could not retain the forwarding routes. • *<bgp name>*: Connection target peer name [Action] Check the unicast routing program (BGP4) in the peer.

Message ID	Event level	Message text
		Description and action
05070456	S4	The number of prefixes received from a peer exceeded the threshold. (source = *<bgp name>*[(*<description>*)], routes from peer = *<routes1>*, max. routes from peer = *<routes2>*)
	The number of paths (active paths and inactive paths) learned from the relevant peer exceeded the threshold. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<routes1>*: Number of paths learned from peers • *<routes2>*: Maximum number of paths learned from peers [Action] If the number of paths learned from the relevant peer further increases, check the number of the paths advertised by the peer.	
05070457	S3	The number of prefixes received from a peer exceeded the limit. If a 'warning-only' command is not set, the peer connection will be closed. (source = *<bgp name>*[(*<description>*)], routes from peer = *<routes1>*, max. routes from peer = *<routes2>*)
	The number of paths (active paths and inactive paths) learned from the relevant peer exceeded the maximum value. If `warning-only` is not specified in the configuration, disconnect the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<routes1>*: Number of paths learned from peers • *<routes2>*: Maximum number of paths learned from peers [Action] Check the number of the paths advertised by the relevant peer.	
05070458	S5	A peer connection closed because the number of prefixes received from the peer had exceeded the limit. (peer = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because the the maximum number of learned paths was exceeded. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] 1. Check the number of the paths advertised by the relevant peer. 2. 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.	
05070459	S5	A peer acting as a receiving router could not retain the forwarding routes. A message sent to the peer might be discarded. (peer = *<bgp name>*)
	The peer operating as a receiving router cannot save the forwarding routes. Messages that are transferred to the relevant peer might be discarded. • *<bgp name>*: Connection target peer name [Action] The negotiation of the graceful restart functionality has notified that the forwarding is not possible. Check if a failure has occurred on the peer router.	

Message ID	Event level	Message text
		Description and action
05070460	S5	A received path attribute was ignored because an UPDATE message from a peer had a path attribute with type code 0. (source = *<bgp name>*[(*<description>*)][, AS path = *<as number>*: *<aspath>*])

		The path attribute was ignored because the UPDATE message including the path attribute of type code 0 was received from the relevant peer. This system message is not output again on the same peer for an hour after the previous output.
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		• *<as number>*: Number of AS numbers
		• *<aspath>*: AS paths[#], in the following format:
		  AS sequential number: AS_SEQ
		  {*AS sequential number*}: AS_SET
		  (*AS sequential number*): AS_CONFED_SEQUENCE
		[Action]
		Check the unicast routing program (BGP4) in the peer.

05070500	S5	A peer connection closed because the holdtime for the peer timed out. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the holdtime for the peer timed out. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] Check the unicast routing program (BGP4) in the peer.
05070501	S5	A peer connection closed because no OPEN message received from the peer before the expiry of its holdtime. (peer = *<bgp name>*)
		The connection with the relevant peer was disconnected because the timer for waiting for an OPEN message from that peer timed out. • *<bgp name>*: Connection target peer name [Action] Check the unicast routing program (BGP4) in the peer.
05070502	S5	A graceful restart was failed because a peer connection was not reestablished within 'restart-time'. All routes learned from the peer will be deleted. (peer = *<bgp name>*[(*<description>*)])
		A graceful restart failed. A connection to the peer router cannot be established within the restart-time specified by the peer router. All the paths learned from the relevant peer will be deleted. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] 1. Check if a communication can be established with the peer router. 2. Check if BGP4 is running on the peer router. 3. 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.

Message ID	Event level	Message text
		Description and action
05070503	S5	A graceful restart was failed because no End-Of-RIB marker received from a restarting router. All routes learned from the peer will be deleted. (peer = *<bgp name>*[(*<description>*)])
		A graceful restart failed. End-Of-RIB cannot be received from the peer router. All the paths learned from the relevant peer will be deleted. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] 1. Check if BGP4 is running on the relevant peer router. 2. If it is running, increase the stalepath-time value.

#: Note that, the entire AS path might not be output (only part of the AS sequential number is output) because there is a limit to the number of characters that can be output in a system message.

7.6 BGP4+

The following table shows the system messages of the `BGP4+` message type.

Table 7-6: System messages of the BGP4+ message type

Message ID	Event level	Message text
		Description and action
05080000	S5	A peer connection has been established. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was established. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05080001	S5	A peer connection closed because of a change in the interface state. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected due to a change in the interface state. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] Check the cause of the change in the interface state.
05080003	S6	A peer connection closed because the peer configuration was deleted. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected due to a change (deletion of the peer information) in the configuration. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05080004	S6	A peer connection closed because of a configuration change. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected due to a change in the configuration. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05080005	S6	A peer connection closed because of the execution of 'clear ipv6 bgp' command. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected by executing the `clear ipv6 bgp` command. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.
05080006	S6	A peer connection has been reestablished in a graceful restart. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was reestablished. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] None.

Message ID	Event level	Message text
		Description and action
05080007	S6	An End-Of-RIB marker was received. (source = *<bgp name>*[(*<description>*)])
		End-Of-RIB was received. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] None.
05080008	S6	An End-Of-RIB marker was sent. (destination peer = *<bgp name>*[(*<description>*)])
		End-Of-RIB was sent. • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer [Action] None.
05080009	S5	A peer connection closed because the number of prefixes received from the peer had exceeded the limit. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the the maximum number of learned paths was exceeded. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] 1. Check the number of the paths advertised by the relevant peer. 2. 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.
05080010	S6	Learning of a route information from receiving routers has finished.
		Route learning from receiving routers has finished. [Action] None.
05080011	S5	The system has stopped route learning from at least one receive router and started route advertisement.
		Route learning from some of the receiving routers will be stopped, and route advertisement will start. [Action] None.
05080100	S4	A connection to a peer failed because the local address was unusable. (peer = *<bgp name>*[(*<description>*)], address = *<ipv6 address>*)
		An attempt to establish a connection failed because the address used for establishing a connection with the relevant peer could not be used. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer • *<ipv6 address>*: Address used for peering [Action] If this error occurs frequently, check the cause of the error.

Message ID	Event level	Message text
		Description and action
05080101	S3	The peer remains in idle state because the interface to be used to the peer connection was not found. (peer = *\<bgp name>*[(*\<description>*)])
		The peer remains in an idle state because the interface connected to the relevant peer cannot be found. • *\<bgp name>*: Connection target peer name • *\<description>*: Description name of the connection target peer [Action] 1. Check the configuration. 2. If the configuration is correct, check the state of the interface to be connected with the relevant peer.
05080102	S3	The peer remains in idle state because the local address to be used to the peer connection was not on the same network as the peer. (peer = *\<bgp name>*[(*\<description>*)], address = *\<ipv6 address>*)
		The peer remains in an idle state because the address used for connecting with the relevant peer does not exist in the same network. • *\<bgp name>*: Connection target peer name • *\<description>*: Description name of the connection target peer • *\<ipv6 address>*: Address used for establish a connection [Action] Check the configuration.
05080103	S3	The peer remains in idle state because the interface for the local address to be used to the peer connection was not found. (peer = *\<bgp name>*[(*\<description>*)], address = *\<ipv6 address>*)
		The peer remains in an idle state because the interface for the device used for connecting with the relevant peer cannot be found. • *\<bgp name>*: Connection target peer name • *\<description>*: Description name of the connection target peer • *\<ipv6 address>*: Address used for establish a connection [Action] Check the configuration.
05080200	S4	A connection request was ignored because an acceptance of a connection failed. (socket = *\<socket>*, error = *\<error string>*)
		The connection request was ignored because acceptance of the connection failed. • *\<socket>*: Socket descriptor number • *\<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05080201	S4	The connection will be closed because a fetching of the link-local address to be used to connection failed. (peer = *\<bgp name>*[(*\<description>*)], error = *\<error string>*)
		The connection will be disconnected because extraction of the link-local address used for establishing a connection failed. • *\<bgp name>*: Connection target peer name • *\<description>*: Description name of the connection target peer • *\<error string>*: Error cause [Action] If this error occurs frequently, check the unicast routing program (BGP4+) in the peer.

Message ID	Event level	Message text
		Description and action
05080202	S4	The connection will be closed because a fetching of the address to be used to connection failed.
		The connection will be disconnected because extraction of the address used for establishing a connection failed. [Action] If this error occurs frequently, check the unicast routing program (BGP4+) in the peer.
05080203	S5	A connection request was ignored because no MD5 digest was attached to the received TCP segment. (source IPv6 + TCP port = *<source ipv6>* + *<TCP port no.>*, destination IPv6 + TCP port = *<destination ipv6>* + *<TCP port no.>*)

		The connection request was ignored because the MD5 authentication option is not set for the received TCP segment. This system message is output according to the following conditions:
		1. The messages from the first to the 16th event are output.
		2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs.
		3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above.
		Note that the above numbers indicate the total number of times the following messages are output.
		  Message type: `BGP4+` Message ID: 05080203
		  Message type: `BGP4+` Message ID: 05080204
		• *<source ipv6>*: Source IPv6 address
		• *<TCP port no.>*: TCP port number
		• *<destination ipv6>*: Destination IPv6 address
		[Action]
		1. Check whether the MD5 authentication is set in BGP4+ of the remote device.
		2. If it is not set, set the MD5 authentication so that it matches.
		3. If the setting matches, check whether TCP segments are sent from a peer other than the source BGP4+ peer.

05080204	S5	A connection request was ignored because an invalid MD5 digest was attached. (source IPv6 + TCP port = *<source ipv6>* + *<TCP port no.>*, destination IPv6 + TCP port = *<destination ipv6>* + *<TCP port no.>*)

		The connection request was ignored because the MD5 authentication option for the received TCP segment is invalid. This system message is output according to the following conditions:
		1. The messages from the first to the 16th event are output.
		2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs.
		3. If an event occurs three minutes or more after the last event occurred, this message is output depending on 1 and 2 above.
		Note that the above numbers indicate the total number of times the following messages are output.
		  Message type: `BGP4+` Message ID: 05080203
		  Message type: `BGP4+` Message ID: 05080204
		• *<source ipv6>*: Source IPv6 address
		• *<TCP port no.>*: TCP port number
		• *<destination ipv6>*: Destination IPv6 address
		[Action]
		1. Check if the MD5 authentication keys match in BGP4+ of the local and remote devices.
		2. If the MD5 authentication keys do not match, set them so that they do match.
		3. If the MD5 authentication keys match, check if TCP segments are sent from a peer other than the source BGP4+ peer.

Message ID	Event level	Message text
		Description and action
05080300	S4	A peer connection closed because a message could not be sent to the peer owing to the lack of space in socket buffer. (send request message length = *<length>* bytes, destination peer = *<bgp name>*[(*<description>*)], error = *<error string>*)
	An attempt to send a message to the relevant peer failed because the socket buffer became full. The connection with the relevant peer was disconnected. • *<length>*: Send request message length • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.	
05080301	S4	A peer connection closed because a message could not be sent to the peer. (message length = *<length>* bytes, destination peer = *<bgp name>*[(*<description>*)], error = *<error string>*)
	The connection with the relevant peer was disconnected because an attempt to send a message to the that peer failed. • *<length>*: Send request message length • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.	
05080302	S5	A message could not be sent to a peer because the connection closed. (send request = *<length>* bytes, destination peer = *<bgp name>*[(*<description>*)])
	An attempt to send the message to the relevant peer failed because the connection was disconnected. • *<length>*: Send request message length • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.	
05080303	S4	A peer connection closed because the system had repeatedly failed in sending a message to the peer. (destination peer = *<bgp name>*[(*<description>*)], error = *<error string>*)
	The connection with the relevant peer was disconnected because the system had repeatedly failed in sending a message to the peer. • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.	

Message ID	Event level	Message text
		Description and action
05080304	S4	A peer connection closed because the system failed in sending a message to the peer. (send request = *<length1>* bytes, sent data = *<length2>* bytes, destination peer = *<bgp name>*[(*<description>*)], error = *<error string>*)
		The connection with the relevant peer was disconnected because the system failed in sending a message to the peer. • *<length1>*: Send request data length • *<length2>*: Sent data length • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05080305	S5	A message was not sent to a peer because the peer connection closed. (send request = *<length1>* bytes, sent data = *<length2>* bytes, destination peer = *<bgp name>*[(*<description>*)])
		An attempt to send the message to the relevant peer failed because the connection was disconnected. • *<length1>*: Send request data length • *<length2>*: Sent data length • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.
05080306	S5	A peer connection closed because the system had repeatedly failed in sending a message to the peer. (destination peer = *<bgp name>*[(*<description>*)], sent data = *<length1>*, remaining = *<length2>*, error = *<error string>*)
		The connection with the relevant peer was disconnected because the system had repeatedly failed in sending a message to the peer. • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<length1>*: Sent data length • *<length2>*: Length of the data that remains unsent • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05080307	S4	A peer connection closed because the system had repeatedly failed in sending KEEPALIVE messages to the peer. (destination peer = *<bgp name>*[(*<description>*)], error = *<error string>*)
		The connection with the relevant peer was disconnected because the system had repeatedly failed in sending KEEPALIVE messages to the peer. • *<bgp name>*: Target peer name • *<description>*: Description name of the destination peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.

Message ID	Event level	Message text
		Description and action
05080308	S5	A NOTIFICATION message was sent to a peer. (destination peer = *<bgp name>*[(*<description>*)], code = *<code>* (*<code string>*)[, sub code = *<sub code>* (*<sub code string>*)][, value = *<value>*][, data = *<data>*])

	A NOTIFICATION message was sent to the relevant peer.
	• *<bgp name>*: Target peer name
	• *<description>*: Description name of the destination peer
	• *<code>* (*<code string>*): Error code
	• *<sub code>* (*<sub code string>*): Error subcode
	  Error code 1 (Message Header Error)
	   - Error subcode 1 (lost connection synchronization)
	   - Error subcode 2 (bad length)
	   - Error subcode 3 (bad message type)
	  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 code 3 (UPDATE Message Error)
	   - Error subcode 1 (invalid attribute list)
	   - Error subcode 2 (unknown well known attribute)
	   - Error subcode 3 (missing well known attribute)
	   - Error subcode 4 (attribute flags error)
	   - Error subcode 5 (bad attribute length)
	   - Error subcode 6 (bad ORIGIN attribute)
	   - Error subcode 9 (error with optional attribute)
	   - Error subcode 10 (bad address or prefix field)
	   - Error subcode 11 (AS path attribute problem)
	  Error code 4 (Hold Timer Expired Error)
	  Error code 5 (Finite State Machine Error)
	  Error code 6 (Cease)
	  invalid: *<code string>* for invalid *<code>*
	  unknown: *<subcode string>* for invalid *<subcode>*
	• *<value>*: Information in the data field of the NOTIFICATION message (Decimal representation)
	• *<data>*: Information in the data field of the NOTIFICATION message (Hexadecimal representation)
	[Action]
	1. Check the network configuration and peer configuration.
	2. If there is no problem with them, check the unicast routing program (BGP4+) in the peer.	

05080400	S5	A peer connection closed because a header marker in the received message was invalid. (peer = *<bgp name>* [(*<description>*)])
	The connection with the relevant peer was disconnected because a header marker in the received message was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.	

Message ID	Event level	Message text
		Description and action
05080401	S5	A NOTIFICATION message from a peer was truncated. (peer = *<bgp name>*[(*<description>*)], length = *<length>*)
		The length of the NOTIFICATION message received from the relevant peer was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.
05080402	S5	A peer connection closed because there was an error in an UPDATE message from the peer. (error = *<code>* (*<error string>*), peer = *<bgp name>*[(*<description>*)], *<length>* bytes error data, first 5 bytes = *<error data>*)
		The connection with the relevant peer was disconnected because there was an error in an UPDATE message from the peer. • *<code>* (*<error string>*): Error cause • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Error data length • *<error data>*: First 5 bytes of error data [Action] Check the unicast routing program (BGP4+) in the peer.
05080403	S5	A peer connection closed because the system failed in receiving a message from the peer. (source = *<bgp name>*[(*<description>*)], error = *<error string>*)
		The connection with the relevant peer was disconnected because the system failed in receiving a message from the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
05080404	S5	A peer connection closed because the system failed in receiving a message from the peer owing to an unexpected EOF. (source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the system failed in receiving a message from the peer owing to an unexpected EOF. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] If this error occurs frequently, check the cause of the disconnection.
05080405	S5	A peer connection closed because of an invalid message length. (source = *<bgp name>*[(*<description>*)], message type = *<message type>*, length = *<length>*)
		The connection with the relevant peer was disconnected because an invalid-length message was received from that peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<message type>*: Received message type invalid, OPEN, UPDATE, NOTIFICATION, KEEPALIVE • *<length>*: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.

Message ID	Event level	Message text
		Description and action
05080406	S5	A peer connection closed because of a reception of an unexpected message type. (source = <*bgp name*>[(<*description*>)], received type = <*message type1*>, expected type = <*message type2*>[or <*message type 2*>])

	The connection with the relevant peer was disconnected because a message whose message type is inappropriate for the current state was received from that peer.
	• <*bgp name*>: Source peer name
	• <*description*>: Description name of the source peer
	• <*message type1*>: Received message type
	  invalid, OPEN, UPDATE, NOTIFICATION, KEEPALIVE
	• <*message type2*>: Message type appropriate for the current state
	  invalid, OPEN, UPDATE, NOTIFICATION, KEEPALIVE
	[Action]
	Check the unicast routing program (BGP4+) in the peer.	

05080407	S5	A peer connection closed because an OPEN message from the peer was too short. (source = <*bgp name*>[(<*description*>)], BGP version in message = <*version*>, message length = <*length*> octets)
	The connection with the relevant peer was disconnected because an OPEN message from the peer was too short. • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer • <*version*>: BGP version number in the received message • <*length*>: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.	
05080408	S5	A peer connection closed because an OPEN message from a peer had an unsupported BGP version. (version = <*version*>, peer = <*bgp name*>[(<*description*>)])
	The connection with the relevant peer was disconnected because an OPEN message that has an unsupported BGP version number was received from that peer. • <*version*>: BGP version number of received messages • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer [Action] Make sure that the peer supports BGP4+.	
05080409	S5	A peer connection closed because the holdtime in an OPEN message from the peer was too small. (source = <*bgp name*>[(<*description*>)], holdtime = <*holdtime*>)
	The connection with the relevant peer was disconnected because an OPEN message whose hold time is less than three seconds was received from that peer. • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer • <*holdtime*>: Hold time in the received message [Action] Check the peer configuration.	

Message ID	Event level	Message text
		Description and action
05080410	S5	A peer connection closed because the BGP4+ identifier in an OPEN message from the peer was invalid. (source = *<bgp name>*[(*<description>*)], invalid ID = *<router id>*)
	The connection with the relevant peer was disconnected because the BGP4+ identifier in an OPEN message from the peer was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<router id>*: BGP4+ identifier in the received message [Action] Check the unicast routing program (BGP4+) in the peer.	
05080411	S5	A peer connection closed because an OPEN message from the peer had an invalid option code. (source = *<bgp name>*[(*<description>*)], option code = *<option>*)
	The connection with the relevant peer was disconnected because an OPEN message from the peer had an invalid option code. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<option>*: Option code in the received message [Action] Check the unicast routing program (BGP4+) in the peer.	
05080412	S3	A peer connection closed because an OPEN message from the peer had an AS number different from the configured one. (source = *<bgp name>*[(*<description>*)], message AS. = *<as1>*, configured AS. = *<as2>*)
	The connection with the relevant peer was disconnected because an OPEN message from the peer had an AS number different from the configured one. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<as1>*: AS number of the received message • *<as2>*: AS number of the peer in the configuration [Action] Check the configuration.	
05080413	S5	A peer connection closed because the BGP version in a KEEPALIVE message from the peer was not supported by the system. (source = *<bgp name>*[(*<description>*)], source version = *<version1>*, this system's version = *<version2>*)
	The connection with the relevant peer was disconnected because a KEEPALIVE message that has a mismatched BGP version number was received from that peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<version1>*: Remote BGP version number • *<version2>*: Local BGP version number [Action] Make sure that the peer supports BGP4+.	
05080414	S3	A peer connection closed because the peer sending an OPEN message was not configured in the system. (source = *<bgp name>*)
	The connection with the relevant peer was disconnected because the peer sending an OPEN message was not configured in the system. • *<bgp name>*: Source peer name [Action] Check the configuration.	

Message ID	Event level	Message text
		Description and action
05080415	S5	A peer connection closed because an OPEN message was sent from the peer in an unexpected state. (source = *<bgp name>*[(*<description>*)], state = *<state>*)
		The connection with the relevant peer was disconnected because an OPEN message was received from that peer during the Idle, OpenConfirm, or Established state. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<state>*: Peer state Idle, OpenConfirm, Established [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
05080416	S5	A peer connection closed because of an unsupported BGP version in an OPEN message. (received version = *<version>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an OPEN message that has an unsupported BGP version number was received from that peer. • *<version>*: BGP version number of received messages • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the BGP version supported by the peer.
05080417	S5	An OPEN message was ignored because of an unexpected extra data. (source = *<bgp name>*[(*<description>*)])
		The OPEN message was ignored because unnecessary data is appended to the message from the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080418	S3	The configured Capabilities for the system did not match with the received Capabilities from a peer. Only a set of matched capabilities has been enabled for the peer. (source = *<bgp name>*[(*<description>*)])
		The capability settings of the Device do not match with the capability received from the peer. Only the matched capability is enabled. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the configuration.
05080419	S5	A peer connection closed because the message length in a message from the peer was invalid. (source = *<bgp name>*[(*<description>*)], length in header = *<length>*)
		The connection with the relevant peer was disconnected because the message length in a message from the peer was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Message length of the received message header [Action] Check the unicast routing program (BGP4+) in the peer.

Message ID	Event level	Message text
		Description and action
05080420	S5	A peer connection closed because a message type in a message from the peer was invalid. (source = *<bgp name>*[(*<description>*)], type = *<type>*)
		The connection with the relevant peer was disconnected because a message type in a message from the peer was invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<type>*: Message type [Action] Check the unicast routing program (BGP4+) in the peer.
05080421	S5	A peer connection closed because an OPEN message was received from the peer in the Established state. (source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an OPEN message was received from the peer in the ESTABLISHEDstate. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
05080422	S5	A peer connection closed because of a too short UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)], message length = *<length>*)
		The connection with the relevant peer was disconnected because of a too short UPDATE message from the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.
05080423	S5	A peer connection closed because an unreachable prefix length of an UPDATE message from the peer exceeded the message length. (prefix length = *<length1>*, message length = *<length2>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an unreachable prefix length of an UPDATE message from the peer exceeded the message length. • *<length1>*: Prefix length of unreachable routing information in the received message • *<length2>*: Received data length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080424	S5	A peer connection closed because an unreachable prefix length of an UPDATE message from the peer was too long. (prefix length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because an unreachable prefix length of an UPDATE message from the peer was too long. • *<length>*: Prefix length in received messages • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.

Message ID	Event level	Message text
		Description and action
05080425	S5	A peer connection closed because a prefix length in an UPDATE message from the peer exceeded the remaining unreachable prefix data. (received prefix length = *<length1>*, actual length = *<length2>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the prefix length of unreachable routing information of the UPDATE message from that peer exceeds the prefix data of unreachable routing information.
		• *<length1>*: Prefix length in received messages
		• *<length2>*: Entity data length
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		[Action]
		Check the unicast routing program (BGP4+) in the peer.
05080426	S5	An UPDATE message was ignored because a path attribute length of the UPDATE message from a peer was 0, but there was a data in the path attribute. (source = *<bgp name>*[(*<description>*)], data length = *<length>* bytes)
		The attribute length of the UPDATE message from the relevant peer is 0 even though actual data exists. The UPDATE message was ignored.
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		• *<length>*: Entity data length
		[Action]
		Check the unicast routing program (BGP4+) in the peer.
05080427	S5	A peer connection closed because a path attribute length of an UPDATE message from the peer exceeded the actual path attribute length. (received attribute lengths = *<length1>*, actual length = *<length2>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because a path attribute length of an UPDATE message from the peer exceeded the actual path attribute length.
		• *<length1>*: Path attribute length of the received message
		• *<length2>*: Entity data length
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		[Action]
		Check the unicast routing program (BGP4+) in the peer.
05080428	S5	A peer connection closed because there was no nexthop attribute in an UPDATE message from the peer. (source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because there was no nexthop attribute in an UPDATE message from the peer.
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		[Action]
		Check the unicast routing program (BGP4+) in the peer.
05080429	S5	The LOCALPREF attribute in an UPDATE message was ignored because the UPDATE message was sent from an external peer. (source = *<bgp name>*[(*<description>*)])
		The LOCALPREF attribute is included in the UPDATE message from the external peer. The LOCALPREF attribute was ignored.
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		[Action]
		Check the unicast routing program (BGP4+) in the peer.

Message ID	Event level	Message text
		Description and action
05080430	S5	A peer connection closed because there was no LOCALPREF attribute in a received UPDATE message from the internal peer. (source = <*bgp name*>[(<*description*>)])
		The connection with the relevant peer was disconnected because there was no LOCALPREF attribute in a received UPDATE message from the internal peer. • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080431	S5	The UPDATE message was ignored because a received UPDATE message from a peer had no reachable prefixes in a path attribute. (source = <*bgp name*>[(<*description*>)])
		The UPDATE message was ignored because the UPDATE message from the relevant peer has path attributes but does not have the corresponding routing information. • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080432	S5	A peer connection closed because an UPDATE message from the peer in AS <*as1*> had an AS-path with the first-hop AS <*as2*>. (peer = <*bgp name*>[(<*description*>)])
		The connection with the relevant peer was disconnected because an UPDATE message from the peer in AS <*as1*> had an AS-path with the first-hop AS <*as2*>. • <*as1*>: AS number of the source peer • <*as2*>: Next-hop AS number in the received message • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080433	S5	A routing information in the NLRI field as described in RFC 1771 was ignored. (source = <*bgp name*>[(<*description*>)])
		Routing information in a format that complies with RFC 1771 was ignored. • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080434	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message. (attribute length = <*length*>, source = <*bgp name*>[(<*description*>)])
		The connection with the relevant peer was disconnected because of an invalid MP_REACH_NLRI attribute length in an UPDATE message. • <*length*>: Received MP_REACH_NLRI attribute length • <*bgp name*>: Source peer name • <*description*>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.

Message ID	Event level	Message text
		Description and action
05080435	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message from the peer (no nexthop length field). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
	The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. The length of the next-hop attribute has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.	
05080436	S5	A peer connection closed because of an invalid nexthop length in the MP_REACH_NLRI attribute in a UPDATE message from the peer. (nexthop length = *<length>*, source = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because of an invalid nexthop length in the MP_REACH_NLRI attribute in a UPDATE message from the peer. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.	
05080437	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message from the peer (no reserved field attribute length). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
	The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. The length of the reserved field attribute has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.	
05080438	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute length in an UPDATE message from the peer (no SNPA length). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
	The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. The length of the SNPA attribute has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.	

Message ID	Event level	Message text
		Description and action
05080439	S5	A peer connection closed because of an invalid MP_REACH_NLRI attribute in an UPDATE message from the peer (no SNPA). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. SNPA has not been configured. The connection with the relevant peer was disconnected. • *<length>*: Received MP_REACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080440	S5	A peer connection closed because a multi-protocol prefix length in an UPDATE message from a peer exceeded the remaining prefix data. (prefix length = *<length1>*, remaining data length = *<length2>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because a multi-protocol prefix length in an UPDATE message from a peer exceeded the remaining prefix data. • *<length1>*: Prefix length in received messages • *<length2>*: Entity data length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080441	S5	A peer connection closed because a multi-protocol prefix length in an UPDATE message from a peer was too long. (prefix length = *<length>*, source = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the prefix length of the route for the UPDATE message from that peer exceeds the maximum length. • *<length>*: Received data length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080442	S5	A peer connection closed because a nexthop address length was invalid. (source = *<bgp name>*[(*<description>*)], length = *<length>*)
		The connection with the relevant peer was disconnected because the next-hop address length of the route from that peer is invalid. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<length>*: Next-hop address length [Action] Check the unicast routing program (BGP4+) in the peer.
05080443	S5	A route information was ignored because there was no nexthop address on the same network as the peer. (source = *<bgp name>*[(*<description>*)], nexthop = *<ipv6 address>*)
		A route information was ignored because there was no nexthop address on the same network as the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<ipv6 address>*: Next-hop address [Action] Check the unicast routing program (BGP4+) in the peer.

Message ID	Event level	Message text
		Description and action
05080444	S5	A peer connection closed because the received route information from a peer was not an IPv6 unicast address. (source = *<bgp name>*[(*<description>*)], family/sub family = *<family>*/*<sub family>*)
	The connection with the relevant peer was disconnected because the received route information from a peer was not an IPv6 unicast address. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<family>*: Address family • *<sub family>*: Sub address family [Action] Check the unicast routing program (BGP4+) in the peer.		
05080445	S5	A peer connection closed because of an invalid MP_UNREACH_NLRI attribute length in an Update message from the peer (no address family). (attribute length = *<length>*, source = *<bgp name>*[(*<description>*)])
	The length of the MP_UNREACH_NLRI attribute for the UPDATE message from the relevant peer is invalid. No address family exists. The connection with the relevant peer was disconnected. • *<length>*: Received MP_UNREACH_NLRI attribute length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.		
05080446	S5	A peer connection closed because a prefix length in an UPDATE message from a peer exceeded the remaining unreachable multi-protocol prefix data. (prefix length = *<length1>*, remaining data = *<length2>*, source = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because a prefix length in an UPDATE message from a peer exceeded the remaining unreachable multi-protocol prefix data. • *<length>*: Next-hop address length • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.		
05080447	S5	A peer connection closed because an unreachable multi-protocol prefix length in an UPDATE message from a peer was too long. (prefix length = *<length>*, source = *<bgp name>*[(*<description>*)])
	The connection with the relevant peer was disconnected because the prefix length of unreachable routing information of the UPDATE message from that peer exceeds 128 bits. • *<length>*: Prefix length in received messages • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.		

Message ID	Event level	Message text
		Description and action
05080448	S5	The route information was ignored because an unreachable muti-protocol prefix was not an IPv6 unicast address. (source = *<bgp name>*[(*<description>*)], family/sub family = *<family>*/*<sub family>*)
		The route information was ignored because an unreachable multi-protocol prefix was not an IPv6 unicast address. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<family>*: Address family • *<sub family>*: Sub address family [Action] Check the unicast routing program (BGP4+) in the peer.
05080449	S5	A peer connection closed because a NOTIFICATION message was received from a peer. (source = *<bgp name>*[(*<description>*)], code = *<code>* (*<code string>*)[, sub code = *<sub code>* (*<sub code string>*)][, value = *<value>*][, data = *<data>*])

		The connection with the relevant peer was disconnected because a NOTIFICATION message was received from a peer.
		 • *<bgp name>*: Source peer name
		 • *<description>*: Description name of the source peer
		 • *<code>* (*<code string>*): Error code
		 • *<sub code>* (*<sub code string>*): Error subcode
		  Error code 1 (Message Header Error)
		   - Error subcode 1 (lost connection synchronization)
		   - Error subcode 2 (bad length)
		   - Error subcode 3 (bad message type)
		  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)
		  Error code 3 (UPDATE Message Error)
		   - Error subcode 1 (invalid attribute list)
		   - Error subcode 2 (unknown well known attribute)
		   - Error subcode 3 (missing well known attribute)
		   - Error subcode 4 (attribute flags error)
		   - Error subcode 5 (bad attribute length)
		   - Error subcode 6 (bad ORIGIN attribute)
		   - Error subcode 7 (AS loop detected)
		   - Error subcode 8 (invalid NEXT_HOP)
		   - Error subcode 9 (error with optional attribute)
		   - Error subcode 10 (bad address or prefix field)
		   - Error subcode 11 (AS path attribute problem)
		  Error code 4 (Hold Timer Expired Error)
		  Error code 5 (Finite State Machine Error)
		  Error code 6 (Cease)
		  invalid: *<code string>* for invalid *<code>*
		  unknown: *<subcode string>* for invalid *<subcode>*
		 • *<value>*: Information in the data field of the NOTIFICATION message (Decimal representation)
		 • *<data>*: Information in the data field of the Notification message (Hexadecimal representation)
		 [Action]
		 Check the network configuration and peer configuration.

Message ID	Event level	Message text
		Description and action
05080450	S5	All routes learned from a peer will be deleted because the peer in a graceful restart could not retain the forwarding routes. (peer =*<bgp name>*)
		All routes learned from a peer will be deleted because the peer in a graceful restart could not retain the forwarding routes. • *<bgp name>*: Connection target peer name [Action] Check the unicast routing program (BGP4+) in the peer.
05080451	S5	A graceful restart was failed because a peer connection was not reestablished within 'restart-time'. All routes learned from the peer will be deleted. (peer = *<bgp name>*[(*<description>*)])
		A graceful restart failed. A connection to the peer router cannot be established within the restart-time specified by the peer router. All the paths learned from the relevant peer will be deleted. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] 1. Check if a communication can be established with the peer router. 2. Check if BGP4+ is running on the peer router. 3. 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.
05080452	S5	A graceful restart was failed because no End-Of-RIB marker received from a restarting router. All routes learned from the peer will be deleted. (peer = *<bgp name>*[(*<description>*)])
		A graceful restart failed. End-Of-RIB cannot be received from the peer router. All the paths learned from the relevant peer will be deleted. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] 1. Check if BGP4+ is running on the relevant peer router. 2. If it is running, increase the stalepath-time value.
05080453	S4	The number of prefixes received from a peer exceeded the threshold. (source = *<bgp name>*[(*<description>*)], routes from peer = *<routes1>*, threshold routes from peer = *<routes2>*)
		The number of paths (active paths and inactive paths) learned from the relevant peer exceeded the threshold. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<routes1>*: Number of paths learned from peers • *<routes2>*: Maximum number of paths learned from peers [Action] If the number of paths learned from the relevant peer increases further , check the number of the paths advertised by the peer.

Message ID	Event level	Message text
		Description and action
05080454	S3	The number of prefixes received from a peer exceeded the limit. If a 'warning-only' command is not set, the peer connection will be closed. (source = *<bgp name>*[(*<description>*)], routes from peer = *<routes1>*, max. routes from peer = *<routes2>*)
		The number of paths (active paths and inactive paths) learned from the relevant peer exceeded the maximum value. If `warning-only` is not specified in the configuration, disconnect the peer. • *<bgp name>*: Source peer name • *<description>*: Description name of the source peer • *<routes1>*: Number of paths learned from peers • *<routes2>*: Maximum number of paths learned from peers [Action] Check the number of the paths advertised by the relevant peer.
05080455	S5	A peer acting as a receiving router could not retain the forwarding routes. A message sent to the peer might be discarded. (peer = *<bgp name>*)
		The peer operating as a receiving router cannot save the forwarding routes. Messages that are transferred to the relevant peer might be discarded. • *<bgp name>*: Connection target peer name [Action] The negotiation of the graceful restart functionality has notified that the forwarding is not possible. Check if a failure has occurred on the peer router.
05080456	S5	A received path attribute was ignored because an UPDATE message from a peer had a path attribute with type code 0. (source = *<bgp name>*[(*<description>*)][, AS path = *<as number>*: *<aspath>*])

		A received path attribute was ignored because an UPDATE message from a peer had a path attribute with type code 0. This system message is not output again on the same peer for an hour after the previous output.
		• *<bgp name>*: Source peer name
		• *<description>*: Description name of the source peer
		• *<as number>*: Number of AS numbers
		• *<aspath>*: AS paths[#], in the following format:
		   AS sequential number: AS_SEQ
		   {*AS sequential number*}: AS_SET
		   (*AS sequential number*): AS_CONFED_SEQUENCE
		[Action]
		Check the unicast routing program (BGP4+) in the peer.

05080500	S5	A peer connection closed because the holdtime for the peer timed out. (peer = *<bgp name>*[(*<description>*)])
		The connection with the relevant peer was disconnected because the holdtime for the peer timed out. • *<bgp name>*: Connection target peer name • *<description>*: Description name of the connection target peer [Action] Check the unicast routing program (BGP4+) in the peer.
05080501	S5	A peer connection closed because no OPEN message received from the peer before the expiry of its holdtime. (peer = *<bgp name>*)
		The connection with the relevant peer was disconnected because the timer for waiting for an OPEN message from that peer timed out. • *<bgp name>*: Connection target peer name [Action] Check the unicast routing program (BGP4+) in the peer.

#: Note that, the entire AS path might not be output (only part of the AS sequential number is

output) because there is a limit to the number of characters that can be output in a system message.

7.7 UNICAST

The following table shows the system messages of the UNICAST message type.

Table 7-7: System messages of the UNICAST message type

Message ID	Event level	Message text
		Description and action
05010000	S4	The dump collection was canceled because of a lack of memory.
		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. [Action] There is not enough memory to execute the command. Review the capacity limit.
05010100	S4	The number of IPv4 unicast routes on the global network exceeded the warning threshold.
		The number of IPv4 unicast routes on the global network has exceeded the warning threshold value. [Action] When adding routes, make sure that the maximum number of routes is not exceeded.
05010101	S4	The number of IPv4 unicast routes on a VRF exceeded the warning threshold.
		The number of IPv4 unicast routes on VRF *<vrf id>* has exceeded the warning threshold value. [Action] When adding routes, make sure that the number of added routes does not exceed the maximum.
05010102	S3	The number of IPv4 unicast routes on the global network exceeded the limit.
		The number of IPv4 unicast routes on the global network has exceeded the maximum. [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.
05010103	S3	The number of IPv4 unicast routes on a VRF exceeded the limit.
		The number of IPv4 unicast routes on VRF *<vrf id>* has exceeded the maximum. [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.
05010104	S4	The number of IPv6 unicast routes on the global network exceeded the warning threshold.
		The number of IPv6 unicast routes on the global network has exceeded the warning threshold value. [Action] When adding routes, make sure that the number of added routes does not exceed the maximum.
05010105	S4	The number of IPv6 unicast routes on a VRF exceeded the warning threshold.
		The number of IPv6 unicast routes on VRF *<vrf id>* has exceeded the warning threshold value. [Action] When adding routes, make sure that the number of added routes does not exceed the maximum.

Message ID	Event level	Message text
		Description and action
05010106	S3	The number of IPv6 unicast routes on the global network exceeded the limit.
	The number of IPv6 unicast routes on the global network has exceeded the maximum. [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.	
05010107	S3	The number of IPv6 unicast routes on a VRF exceeded the limit.
	The number of IPv6 unicast routes on VRF *<vrf id>* has exceeded the maximum. [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.	
05010200	S4	A graceful restart was failed.
	A graceful restart failed. [Action] Check if another system switchover has occurred or the unicast routing program restarted during a graceful restart.	

Chapter

8. Multicast Routing

8.1 PIM-IPv4

The following table shows the system messages of the PIM-IPv4 message type.

Table 8-1: System messages of the PIM-IPv4 message type

Message ID	Event level	Message text
		Description and action
0f040001	S5	A received Bootstrap message was ignored because a unicast route to the BSR was not found. (source = *<source address>*, BSR address = *<ip address>*)
	A received PIM message was ignored because the unicast route to the bootstrap router address in the PIM Bootstrap message was not found. • *<source address>*: Source IPv4 address • *<ip address>*: Bootstrap router address [Action] Check whether the route to the bootstrap router address in the Bootstrap packet exists.	
0f040002	S5	BSR information was cleared because Rendezvous Point advertisements from the Bootstrap router were lost.
	Bootstrap router information was cleared because advertisements from the Bootstrap router were lost. [Action] Check the reason why advertisements from the Bootstrap router were lost.	
0f040003	S6	BSR address has been changed. (new BSR address = *<ip address>*)
	The Bootstrap router address was updated to *<ip address>*. • *<ip address>*: Bootstrap router address If the Bootstrap router address is the Device, (this system) is displayed after the IPv4 address. [Action] None.	
0f040004	S5	Deleted a neighbor because no Hello message has been advertised from the neighbor recently. (neighbor = *<neighbor address>*, interface = *<interface name>*, Generation ID = *<generation id>*)
	Adjacency was deleted because a PIM Hello message was not received from the neighboring router during a given interval • *<neighbor address>*: Neighboring router's address • *<interface name>*: Interface name • *<generation id>*: Generation ID NONE: Generation ID is not supported [Action] 1. If the neighboring router stops operation, make sure there is no communication failure between the Device and the neighboring router. 2. If there is no problem, use the show cpu command to check whether the CPU load of the Device has increased.	

Message ID	Event level	Message text
		Description and action
0f040005	S5	Deleted a neighbor because a Hello message with holdtime 0 has been advertised from the neighbor. (neighbor = *<neighbor address>*, interface = *<interface name>*, Generation ID = *<generation id>*)
		Adjacency was deleted because a PIM Hello message whose holdtime value is 0 was received from the neighboring router. • *<neighbor address>*: Neighboring router's address • *<interface name>*: Interface name • *<generation id>*: Generation ID NONE: Generation ID is not supported [Action] None.
0f040006	S6	Added a neighbor. (neighbor = *<neighbor address>*, interface = *<interface name>*, Generation ID = *<generation id>*)
		A new neighboring router was detected. • *<neighbor address>*: Neighboring router's address • *<interface name>*: Interface name • *<generation id>*: Generation ID NONE: Generation ID is not supported [Action] None.
0f040008	S5	Refreshed a neighbor because of a change of Generation ID. (neighbor = *<neighbor address>*, interface = *<interface name>*, old Generation ID = *<old generation id>*, new Generation ID = *<new generation id>*)

		The Generation ID of a neighboring router has changed.
		• *<neighbor address>*: Neighboring router's address
		• *<interface name>*: Interface name
		• *<old generation id>*: Generation ID before the change
		  NONE: The neighboring router is not supported.
		• *<new generation id>*: Generation ID after the change
		  NONE: The neighboring router is not supported.
		[Action]
		None.

0f040009	S6	Updated a DR address. (interface = *<interface name>*, old DR address = *<old ip address>*, new DR address = *<ip address>*)
		The DR address was updated to *<ip address>* on the interface *<interface name>*. • *<interface name>*: Interface name • *<old ip address>*: Previous DR address • *<ip address>*: DR address [Action] None.

8.2 IGMP

The following table shows the system messages of the IGMP message type.

Table 8-2: System messages of the IGMP message type

Message ID	Event level	Message text
		Description and action
0f030001	S6	Updated a querier address. (interface = *<interface name>*, new querier = *<ip address>*, old querier = *<old ip address>*)

		The querier was updated to *<ip address>* on the interface *<interface name>*.
		• *<interface name>*: Interface name
		• *<ip address>*: Querier IPv4 address
		  (this system): Displayed if the querier IPv4 address is the Device address.
		• *<old ip address>*: Previous querier IPv4 address
		  (this system): Displayed if the previous querier IPv4 address is the Device address.
		[Action]
		None.

8.3 PIM-IPv6

The following table shows the system messages of the PIM-IPv6 message type.

Table 8-3: System messages of the PIM-IPv6 message type

Message ID	Event level	Message text
		Description and action
19040001	S5	A received Bootstrap message was ignored because a unicast route to the BSR was not found. (source = *<source address>*, BSR address = *<ipv6 address>*)
		A received PIM message was ignored because the unicast route to the bootstrap router address in the PIM Bootstrap message was not found. • *<source address>*: Source IPv6 address • *<ipv6 address>*: Bootstrap router address [Action] Check whether the route to the bootstrap router address in the Bootstrap packet exists.
19040002	S5	BSR information was cleared because Rendezvous Point advertisements from the Bootstrap router were lost.
		Bootstrap router information was cleared because advertisements from the Bootstrap router were lost. [Action] Check the reason why advertisements from the Bootstrap router were lost.
19040003	S6	BSR address has been changed. (new BSR address = *<ipv6 address>*)
		The Bootstrap router address was updated to *<ipv6 address>*. • *<ipv6 address>*: Bootstrap router address If the Bootstrap router address is the Device, (this system) is displayed after the IPv6 address. [Action] None.
19040004	S5	Deleted a neighbor because no Hello message has been advertised from the neighbor recently. (neighbor = *<neighbor address>*, interface = *<interface name>*, Generation ID = *<generation id>*)
		Adjacency was deleted because a PIM Hello message was not received from the neighboring router during a given interval • *<neighbor address>*: Neighboring router's address • *<interface name>*: Interface name • *<generation id>*: Generation ID NONE: Generation ID is not supported [Action] 1. If the neighboring router stops operation, make sure there is no communication failure between the Device and the neighboring router. 2. If there is no problem, use the show cpu command to check whether the CPU load of the Device has increased.

Message ID	Event level	Message text
		Description and action
19040005	S5	Deleted a neighbor because a Hello message with holdtime 0 has been advertised from the neighbor. (neighbor = *<neighbor address>*, interface = *<interface name>*, Generation ID = *<generation id>*)
	Adjacency was deleted because a PIM Hello message whose holdtime value is 0 was received from the neighboring router. • *<neighbor address>*: Neighboring router's address • *<interface name>*: Interface name • *<generation id>*: Generation ID NONE: Generation ID is not supported [Action] None.	
19040006	S6	Added a neighbor. (neighbor = *<neighbor address>*, interface = *<interface name>*, Generation ID = *<generation id>*)
	A new neighboring router was detected. • *<neighbor address>*: Neighboring router's address • *<interface name>*: Interface name • *<generation id>*: Generation ID NONE: Generation ID is not supported [Action] None.	
19040008	S5	Refreshed a neighbor because of a change of Generation ID. (neighbor = *<neighbor address>*, interface = *<interface name>*, old Generation ID = *<old generation id>*, new Generation ID = *<new generation id>*)

	The Generation ID of a neighboring router has changed.
	• *<neighbor address>*: Neighboring router's address
	• *<interface name>*: Interface name
	• *<old generation id>*: Generation ID before the change
	  NONE: The neighboring router is not supported.
	• *<new generation id>*: Generation ID after the change
	  NONE: The neighboring router is not supported.
	[Action]
	None.	

19040009	S6	Updated a DR address. (interface = *<interface name>*, old DR address = *<old ipv6 address>*, new DR address = *<ipv6 address>*)
	The DR address has been updated to *<ipv6 address>* on the interface *<interface name>*. • *<interface name>*: Interface name • *<old ipv6 address>*: Previous DR address • *<ipv6 address>*: DR address [Action] None.	

8.4 MLD

The following table shows the system messages of the MLD message type.

Table 8-4: System messages of the MLD message type

Message ID	Event level	Message text
		Description and action
19030001	S6	Updated a querier address. (interface = *\<interface name\>*, new querier = *\<ipv6 address\>*, old querier = *\<old ipv6 address\>*)

		The querier was updated to *\<ipv6 address\>* on the interface *\<interface name\>*.
		• *\<interface name\>*: Interface name
		• *\<ipv6 address\>*: Querier IPv6 address
		  (this system): Displayed if the querier IPv6 address is the Device address.
		• *\<old ipv6 address\>*: Previous querier IPv6 address
		  (this system): Displayed if the previous querier IPv6 address is the Device address.
		[Action]
		None.

8.5 MULTI-IPv4

The following table shows the system messages of the MULTI-IPv4 message type.

Table 8-5: System messages of the MULTI-IPv4 message type

Message ID	Event level	Message text
		Description and action
0f020001	S6	The IPv4 multicast routing program (pimd) restarted because the IPv4 multicast (PIM) max-interfaces configuration was changed.
		The IPv4 multicast routing program restarted because the IPv4 multicast (PIM) information of the running configuration was changed by the `ip pim max-interface` configuration command. [Action] None.
0f020002	S3	Suspended learning IPv4 multicast routing entries because the number of routing entries exceeded the maximum. (number = <*number*>)
		One or more entries were discarded because the number of IPv4 multicast routing entries exceeded the maximum value of <*number*>. • <*number*>: Maximum number of IPv4 multicast routing entries [Action] 1. Check whether more than the expected number of requests to add multicast routing entries were generated. The number of multicast routing entries exceeds the maximum value. 2. Check the settings of the `ip pim mroute-limit` configuration command. 3. Check the network configuration and reconsider the configuration of the Device.
0f020003	S6	Resumed learning IPv4 multicast routing entries because the number of routing entries fell below the maximum. (number = <*number*>)
		The system has recovered from the state in which requests to add IPv4 multicast routing entries were discarded. • <*number*>: Maximum number of IPv4 multicast routing entries [Action] None.
0f020004	S3	Suspended creating IPv4 multicast forwarding entries because the number of forwarding entries exceeded the maximum. (number = <*number*>)
		One or more IPv4 multicast forwarding entries were discarded because the number of entries exceeded the maximum value of <*number*>. • <*number*>: Maximum number of IPv4 multicast forwarding entries [Action] 1. Check whether more than the expected number of requests to add multicast forwarding entries were generated. The number of multicast forwarding entries exceeds the maximum value. 2. Check whether a negative cache was generated due to reception of multicast packets that were not forwarded. 3. Check the settings of the `ip pim mcache-limit` configuration command. 4. Check the network configuration and reconsider the configuration of the Device.
0f020005	S6	Resumed creating IPv4 multicast forwarding entries because the number of forwarding entries fell below the maximum. (number = <*number*>)
		IPv4 multicast forwarding entries have recovered from the state in which requests to add entries were discarded. • <*number*>: Maximum number of IPv4 multicast forwarding entries [Action] None.

Message ID	Event level	Message text
		Description and action
0f020006	S3	Suspended receiving IGMP requests because the number of IGMP groups exceeded the limit number at interface. (number = *<number>*, interface = *<interface name>*)
	One or more requests were discarded because the interface *<interface name>* received a request that exceeded the IGMP multicast group limit value of *<number>*. • *<number>*: IGMP multicast group limit • *<interface name>*: Interface name [Action] 1. Check whether more than the expected number of requests to add IGMP multicast groups were generated. 2. Check the settings of the `ip igmp group-limit` configuration command. 3. Check the network configuration and reconsider the configuration of the Device.	
0f020007	S6	Resumed receiving IGMP requests because the number of IGMP groups fell below the limit number at interface. (number = *<number>*, interface = *<interface name>*)
	The interface *<interface name>* recovered from the state in which requests to add IGMP multicast groups were discarded. • *<number>*: IGMP multicast group limit • *<interface name>*: Interface name [Action] None.	
0f020008	S3	Suspended receiving IGMP requests because the number of IGMP sources exceeded the limit number at interface. (number = *<number>*, interface = *<interface name>*)
	A request was discarded because the interface *<interface name>* received a request that exceeded the limit value of *<number>* for the source that belongs to IGMP multicast group. • *<number>*: Limit on sources that belong to the IGMP multicast group • *<interface name>*: Interface name [Action] 1. Check whether more than the expected number of requests to add sources that belong to the IGMP multicast group were generated. 2. Check the settings of the `ip igmp source-limit` configuration command. 3. Check the network configuration and reconsider the configuration of the Device.	
0f020009	S6	Resumed receiving IGMP requests because the number of IGMP sources fell below the limit number at interface. (number = *<number>*, interface = *<interface name>*)
	The interface *<interface name>* has recovered from the state in which requests to add sources that belong to the IGMP multicast group were discarded. • *<number>*: Limit on sources that belong to the IGMP multicast group • *<interface name>*: Interface name [Action] None.	

8.6 MULTI-IPv6

The following table shows the system messages of the `MULTI-IPv6` message type.

Table 8-6: System messages of the MULTI-Pv6 message type

Message ID	Event level	Message text
		Description and action
19020001	S6	The IPv6 multicast routing program (pim6sd) restarted because the IPv6 multicast (PIM6) max-interfaces configuration was changed.
		The IPv6 multicast routing program restarted because the IPv6 multicast (PIM6) information of the running configuration was changed by the `ipv6 pim max-interface` configuration command. [Action] None.
19020002	S3	Suspended learning IPv6 multicast routing entries because the number of routing entries exceeded the maximum. (number = <*number*>)
		One or more entries were discarded because the number of IPv6 multicast routing entries exceeded the maximum value of <*number*>. • <*number*>: Maximum number of IPv6 multicast routing entries [Action] 1. Check whether more than the expected number of requests to add multicast routing entries were generated. The number of multicast routing entries exceeds the maximum value. 2. Check the settings of the `ipv6 pim mroute-limit` configuration command. 3. Check the network configuration and reconsider the configuration of the Device.
19020003	S6	Resumed learning IPv6 multicast routing entries because the number of routing entries fell below the maximum. (number = <*number*>)
		The system has recovered from the state in which requests to add IPv6 multicast routing entries were discarded. • <*number*>: Maximum number of IPv6 multicast routing entries [Action] None.
19020004	S3	Suspended creating IPv6 multicast forwarding entries because the number of forwarding entries exceeded the maximum. (number = <*number*>)
		One or more entries were discarded because the number of IPv6 multicast forwarding entries exceeded the maximum value of <*number*>. • <*number*>: Maximum number of IPv6 multicast forwarding entries [Action] 1. Check whether more than the expected number of requests to add multicast forwarding entries were generated. The number of multicast forwarding entries exceeds the maximum value. 2. Check whether a negative cache was generated due to reception of multicast packets that were not forwarded. 3. Check the settings of the `ipv6 pim mcache-limit` configuration command. 4. Check the network configuration and reconsider the configuration of the Device.
19020005	S6	Resumed creating IPv6 multicast forwarding entries because the number of forwarding entries fell below the maximum. (number = <*number*>)
		The system has recovered from the state in which requests to add IPv6 multicast forwarding entries were discarded. • <*number*>: Maximum number of IPv6 multicast forwarding entries [Action] None.

Message ID	Event level	Message text
		Description and action
19020006	S3	Suspended receiving MLD requests because the number of MLD groups exceeded the limit number at interface. (number = *\<number\>*, interface = *\<interface name\>*)
	A request was discarded because the interface *\<interface name\>* received a request that exceeded the MLD multicast group limit value of *\<number\>*. • *\<number\>*: MLD multicast group limit • *\<interface name\>*: Interface name [Action] 1. Check whether more than the expected number of requests to add MLD multicast groups were generated. 2. Check the settings of the `ipv6 mld group-limit` configuration command. 3. Check the network configuration and reconsider the configuration of the Device.	
19020007	S6	Resumed receiving MLD requests because the number of MLD groups fell below the limit number at interface. (number = *\<number\>*, interface = *\<interface name\>*)
	The interface *\<interface name\>* has recovered from the state in which requests to add MLD multicast groups were discarded. • *\<number\>*: MLD multicast group limit • *\<interface name\>*: Interface name [Action] None.	
19020008	S3	Suspended receiving MLD requests because the number of MLD sources exceeded the limit number at interface. (number = *\<number\>*, interface = *\<interface name\>*)
	A request was discarded because the interface *\<interface name\>* received a request that exceeded the limit value of *\<number\>* for the source that belongs to MLD multicast group. • *\<number\>*: Limit on sources that belong to the MLD multicast group • *\<interface name\>*: Interface name [Action] 1. Check whether more than the expected number of requests to add sources that belong to an MLD multicast group were generated. 2. Check the settings of the `ipv6 mld source-limit` configuration command. 3. Check the network configuration and reconsider the configuration of the Device.	
19020009	S6	Resumed receiving MLD requests because the number of MLD sources fell below the limit number at interface. (number = *\<number\>*, interface = *\<interface name\>*)
	The interface *\<interface name\>* has recovered from the state in which requests to add sources that belong to the MLD multicast group were discarded. • *\<number\>*: Limit on sources that belong to the MLD multicast group • *\<interface name\>*: Interface name [Action] None.	

8.7 MULTI-INFO

The following table shows the system messages of the `MULTI-INFO` message type.

Table 8-7: System messages of the MULTI-INFO message type

Message ID	Event level	Message text
		Description and action
19050001	S6	An interface was added from the output interface list of IPv6 multicast forwarding entries. (interface = *<interface name>*, source = *<source address>*, group = *<group address>*)
	The interface *<interface name>* was added to the output interface list of IPv6 multicast forwarding entries. This message is output when the `ipv6 multicast join-prune-event logging enable` configuration command is specified. • *<interface name>*: Interface name • *<source address>*: Source IPv6 address • *<group address>*: IPv6 group address [Action] None.	
19050002	S6	An interface was deleted from the output interface list of IPv6 multicast forwarding entries. (interface = *<interface name>*, source = *<source address>*, group = *<group address>*)
	The interface *<interface name>* was removed from the output interface list of IPv6 multicast forwarding entries. This message is output when the `ipv6 multicast join-prune-event logging enable` configuration command is specified. • *<interface name>*: Interface name • *<source address>*: Source IPv6 address • *<group address>*: IPv6 group address [Action] None.	

Index