AX8600R

Troubleshooting Guide

AX86R-T001X

AlaxalA

■ Relevant products

This manual applies to the models in 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.

Please note that the actual product might differ from how it is depicted in output examples and figures.

■ Editions history

August 2013 (Edition 1) AX86R-T001X

■ Copyright

All Rights Reserved, Copyright(C), 2013, ALAXALA Networks, Corp.

Preface

Applicable products

This manual applies to the models in 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 *Manual Corrections*.

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

  Configuration Guide Vol. 1 (AX86R-S001X)
  Configuration Guide Vol. 2 (AX86R-S002X)
  Configuration Guide Vol. 3 (AX86R-S003X)

  ▽ If necessary, see the following references.

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

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

  Operation Command Reference Vol. 1 (AX86R-S007X)
  Operation Command Reference Vol. 2 (AX86R-S008X)
  Operation Command Reference Vol. 3 (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. Troubleshooting Device Failures

This chapter describes the actions to be taken when a device failure occurs.

1.1 Device failure analysis

1.1.1 AX8600R failure analysis

If a failure occurs in the device during operation and you have physical access to the device, troubleshoot the failure by taking appropriate action as described in *1.2 Troubleshooting failures in AX8600R series devices*. Note that even if you do not have physical access to the device, you can still troubleshoot failures in the same way by issuing operation commands from a remote operation terminal to check the status of the LEDs on the device.

The status of the device is displayed on the BCU. *Figure 1-1: Example of the front panel layout* and *Table 1-1: LED display, switches, and connectors* explain the LEDs on the BCU. For details on the LEDs on optional modules other than the BCU (the SFU, PRU, NIF, power supply unit, and fan unit), see the *Hardware Instruction Manual*.

Figure 1-1: Example of the front panel layout

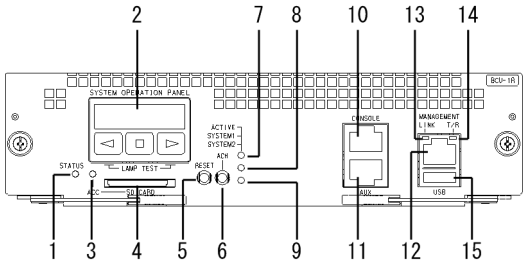


Table 1-1: LED display, switches, and connectors

No.	Name	Type	Information indicated by LED, or type of switch/ connector	Description
1	STATUS	LED: Green or red	Operating status of the BCU	Green: The BCU is available for operation. Blinking green: The BCU is loading software. Red: A failure was detected. Off: The power is off.#1
2	SYSTEM OPERATION PANEL	LCD and operation keys	System operation panel	Displays device information, operating instructions, and failure information. (For details, see the *Configuration Guide*.)
3	ACC	LED: Green	Status of the memory card	Green: The memory card is being accessed. Do not remove it. Off: The memory card is idle. You can insert or remove it.
4	SD CARD	Connector	SD card slot	SD card slot
5	RESET	Button (non-locking)	Manual reset button for the device#2	Press and hold for one second if, for example, a failure occurs with the device.#3 Press and hold for five seconds if the user name or password is forgotten.#4
6	ACH	Button (non-locking)	BCU system-switching switch#2	If redundant BCU modules are in use, pressing this button swaps the active and standby units.#5
7	ACTIVE	LED: Green	Operating status of the BCU	Green: Active Off: Standby

No.	Name	Type	Information indicated by LED, or type of switch/ connector	Description
8	SYSTEM1	LED: Green or red	Status of the device	Green: The device is available for operation. Blinking green: A partial device failure was detected. Red: A device failure was detected.
9	SYSTEM2	LED	Status of the device	This LED is not supported and is always off.
10	CONSOLE	Connector	CONSOLE port	RS232C port for connecting an operation terminal
11	AUX	Connector	AUX port	RS232C port for connecting an operation terminal
12	MANAGEMENT	Connector	Management port	10BASE-T/100BASE-TX/1000BASE-T Ethernet port for connecting an operation terminal
13	LINK	LED: Green or orange	Operating status of the management port	Green: A link has been established. Orange: A failure was detected. Off: Either a link failure occurred[#6] or operation stopped.[#7]
14	T/R	LED: Green	Operating status of the management port	Green: Packets are being transmitted. Off: No packet is being transmitted.
15	USB	Connector	USB port	This port is not supported and cannot be used.

#1: You can turn off the BCU either by using the `inactivate` operation from the system operation panel or by executing a command from the operation terminal.

#2: The button is recessed into the front panel. Use a screwdriver that has a small tip to press the button.

#3: If you hold the button for less than one second, the device might not reset.

#4: After a restart, a login password and administrator password are no longer required. Logging in by using the user name `operator` is permitted. Therefore, be especially careful if you restart the unit by using this method.

#5: The system switches only when the ACH switch of the active BCU is pressed. After the system switches, the new standby BCU restarts.

#6: "Link failure" also includes disconnected cables.

#7: You can stop operation by executing a command.

1.2 Troubleshooting failures in AX8600R series devices

1.2.1 Procedure for handling failures

If a failure occurs in a device, follow the procedure described below.

Table 1-2: Troubleshooting for Device Failure

No.	Problem	Action
1	• Smoke emanates from the device. • An abnormal odor emanates from the device. • An abnormal sound emanates from the device.	Immediately do the following: 1. Turn off the device. 2. If you are using an AC power supply unit, remove the power cable. 3. If you are using a DC power supply unit, turn off the circuit breaker of the power facility. After performing this procedure to stop the device, contact your distributor.
2	The login prompt does not appear.	Perform the following procedure: 1. If a memory card is inserted, remove the card, turn the device off, and then turn the device on again to restart it. 2. If a memory card is not inserted, turn the device off, and then turn the device on again to restart it. 3. If restarting the device does not solve the problem, replace the BCU.
3	All the LEDs on the BCU are off.	Perform the following procedure: 1. Check the LEDs of the power supply unit. - If the ALARM LED of the power supply unit is glowing red, replace the relevant power supply unit. - If both the POWER LED and the ALARM LED of the power supply unit are off, see *Table 1-3: Troubleshooting power supply failures* for the action to be taken for the failure in the power supply unit. If the problem is not resolved, replace the relevant power supply unit and the corresponding power input unit. 2. If the power supply unit is operating properly without any problems, replace the BCU.
4	The SYSTEM1 LED of the BCU is either blinking green or glowing red.	Perform the following procedure: 1. If an error message is displayed on the system operation panel, take appropriate action for the relevant error message as described in the *Message and Log Reference*. 2. If no error message is displayed on the system operation panel, replace the board (BCU, SFU, PRU, or NIF) whose STATUS LED is glowing red.
5	A system message is displayed on the system operation panel.	Take the appropriate action for the relevant message as described in the *Message and Log Reference*.

No.	Problem	Action
6	The STATUS LED of the BCU is glowing red, but all the other LEDs are off, and no system message is displayed on the system operation panel.	Perform the following procedure: 1. Check the BCU configuration. - If you are using a single BCU configuration, perform steps 3 onwards. - If you are using a duplex BCU configuration, perform steps 2 onwards. 2. Check both the active and the standby BCUs. - If a failure occurred in only one of the units, replace the relevant BCU. In such a case, you do not need to perform steps 3 onwards. - If a failure occurred in both the active and standby units, follow steps 3 onwards. 3. Check the LEDs of the power supply unit. - If the ALARM LED of the power supply unit is glowing red, replace the relevant power supply unit. - If both the POWER LED and the ALARM LED of the power supply unit are off, see *Table 1-3: Troubleshooting power supply failures* for the action to be taken for the failure in the power supply unit. If the problem is not resolved, replace the relevant power supply unit. - If all power supply units are operating normally, leave them as they are. 4. Turn off all the circuit breakers on the power input unit that is installed in the device. 5. Wait 30 seconds or more, and then turn on all the circuit breakers on the power input unit that is installed in the device. 6. Replace the BCU in which the failure occurred.

Table 1-3: Troubleshooting power supply failures

No.	Problem	Action
1	The circuit breaker on the power input unit is off.	Turn on the circuit breaker on the power input unit.
2	• The power cable is disconnected. • The power cable is improperly connected.	Perform the following procedure: 1. Turn off the circuit breaker on the power input unit. 2. If you are using a DC power supply unit, turn off the circuit breaker at the power facility. 3. Connect the power cable properly. 4. If you are using a DC power supply unit, turn on the circuit breaker at the power facility. 5. Turn on the circuit breaker on the power input unit.
3	The power input unit is improperly installed (or is unstable).	Perform the following procedure: 1. Turn off the circuit breaker on the power input unit. 2. If you are using a DC power supply unit, turn off the circuit breaker at the power facility. 3. Disconnect the power cables. 4. Remove the power unit, and then insert it again so that it is firmly fixed. 5. Connect the power cables. 6. If you are using a DC power supply unit, turn on the circuit breaker at the power facility. 7. Turn on the circuit breaker on the power input unit.
4	The power supply unit is improperly installed (or is unstable).	Perform the following procedure: 1. Turn off the circuit breaker on the power input unit. 2. Remove the power unit, and then insert it again so that it is firmly fixed. 3. Turn on the circuit breaker on the power input unit.

No.	Problem	Action
5	The measured input power supply is outside the following range:# • For 100 V AC: 90 to 132 V AC • For 200 V AC: 180 to 264 V AC • For -48 V DC: -40.5 to -57 V DC	Ask the person responsible for the facility in which the device is housed to take actions regarding the input power supply.

#: Perform this step only when you are able to measure the input power supply.

1.2.2 Replacing the device and optional modules

For details on how to install or remove optional modules, such as the device and fan unit, power input unit, power supply unit, BCU, SFU, PRU, NIF, memory card, and transceiver, see the *Hardware Instruction Manual*. Install or remove the module by following the procedure described in the *Hardware Instruction Manual*.

Chapter

2. Troubleshooting Operation Management

This chapter describes the actions to be taken when a problem occurs with operation management.

2.1 Login problems

2.1.1 A user forgot the user's login password

If a user forgets his/her password and is unable to log in to the Device, perform either of the following.

(1) If another user exists who can log in or whose input mode can be changed to administrator mode

If a user, other than the user who forgot his/her password, who can log in or whose input mode can be changed to administrator mode exists, that user executes the configuration command `username` to reset the password of the user who forgot his/her password. Execute this command in configuration command mode.

The following figure shows an example of resetting a forgotten password for user1.

Figure 2-1: Example of resetting the password for user1

```
# configure
(config)# username user1 password input
New password:********                          <-1
Retype new password:********                   <-2
!(config)# save
(config)# exit
#
```

1. Type the user's password (the actual characters are not shown).
2. Type the user's password again to confirm it (the actual characters are not shown).

(2) If no other user can log in or can change his/her input mode to administrator mode

Besides the user who forgot his/her password, if no other user can log in or can change his/her input mode to administrator mode, push and hold the RESET button for at least five seconds to perform a default restart. After startup due to the default restart, reset the password. The new password specified at default restart takes effect after the device restarts.

After a default restart, password authentication, authentication when changing to administrator mode (enable command), and command authorization are not performed. Also, login is permitted by using the user name `operator`. Because of this reduction in security, immediately after resetting the password, restart the device.

2.1.2 The administrator forgot the administrator mode password

If you cannot change the input mode to administrator mode because you forgot the password for administrator mode, push and hold the RESET button for at least five seconds to perform a default restart. After startup due to the default restart, reset the password. The new password specified at default restart takes effect after the device restarts.

After a default restart, password authentication, authentication when changing to administrator mode (enable command), and command authorization are not performed. Also, login is permitted by using the user name `operator`. Because of this reduction in security, immediately after resetting the password, restart the device.

2.1.3 A user forgot the user's login name

If a user forgets his/her login user name and is unable to log in to the Device, perform either of the following:

(1) If another user can log in

If a user other than the user who forgot his/her user name can log in, that user executes the `show users` command to check the user name.

(2) If no other user can log in

If no user other than the user who forgot his/her user name can log in, push and hold the RESET button for at least five seconds to perform a default restart. After startup due to the default restart, log in by using the user name `operator`, and then execute the `show users` command to check the user name.

After a default restart, login is permitted by using the user name `operator`. Also, password authentication, authentication when changing to administrator mode (enable command), and command authorization are not performed. Because of this reduction in security, immediately after checking the user name, restart the device.

2.2 Operation terminal problems

2.2.1 Unable to enter information from the console, or the screen image appears incorrectly

If a problem occurs during connection to the console, check the situation according to the following table.

Table 2-1: Problems that occur during connection to the console, and action to take

No.	Problem	Items to be checked
1	Nothing is displayed on the screen.	Perform the following procedure: 1. On the front panel of the device, make sure that the STATUS LED is green. If the STATUS LED is not green, see *1.1 Device failure analysis*. 2. Check whether the cables are connected correctly. For example, check if any cable is incompletely inserted. 3. Check the wire connection of the console. For details, see the *Hardware Instruction Manual*. 4. Make sure that the communication software settings (including the port number, communication speed, data length, parity bit, stop bit, and flow control) are specified as follows: Communication speed: 9600 bit/s (or the specified value if you changed this value) Data length: 8 bits Parity bit: None Stop bit: 1 bit Flow control: None
2	Keyboard input is not accepted.	Perform the following procedure: 1. Data transmission might have been interrupted by XON/XOFF flow control. End the interruption by pressing **Ctrl** + **Q**. If the device still does not accept input from the keyboard, perform steps 2 and 3. 2. Make sure that the communication software settings are correct. 3. The screen might be unresponsive because **Ctrl** + **S** was pressed. Press any key.
3	Unexpected characters are displayed.	Negotiation with the communication software might not have completed correctly. Check the software communication speed by doing the following: 1. If you did not specify the communication speed of CONSOLE (RS232C) by using the `line console 0` configuration command, make sure that the communication speed of the communication software is set to 9600 bit/s. 2. If you set the communication speed of CONSOLE (RS232C) to 1200, 2400, 4800, 9600, or 19200 bit/s by using the `line console 0` configuration command, make sure that the communication speed of the communication software is set correctly. 3. If unexpected characters are displayed even though no problems were found in steps 1 and 2, issue a break signal. Note, however, that depending on the communication speed of the communication software, the break signal might not appear unless you issue it several times.
4	While a user name is being entered, unexpected characters appear.	The communication speed of CONSOLE (RS232C) might have been changed. See step 3.
5	Login is impossible.	Perform the following procedure: 1. Make sure that the login prompt is displayed on the screen. No login prompt on the screen means that the device is starting. Wait a while. 2. Use the `aaa authentication login console` and `aaa authentication login` configuration commands to make sure that RADIUS or TACACS+ authentication is not set. (For details, see *2.2.3 Unable to perform login authentication by using RADIUS or TACACS+*.)

No.	Problem	Items to be checked
6	After login, the communication speed of the communication software is changed. After that, unexpected characters appear, and commands cannot be entered.	Even if you change the communication speed of the communication software after login, correct display is impossible. Restore the original communication speed of the communication software.
7	Item names and the corresponding content are displayed out of alignment.	The displayed information might be greater than the maximum number of characters that can be displayed on one line. Change the screen size setting of the communication software to increase the number of characters that can be displayed on one line.

If a problem occurs during connection to the modem, check the situation according to the following table. Also, see the documentation provided with the modem.

Table 2-2: Problems that occur during connection to the modem, and action to take

No.	Problem	Items to be checked
1	The modem does not answer automatically.	Check the following: • The cables are connected correctly. • The modem is turned on. • The phone number is specified correctly. • The settings for the modem are correct. • If the modem is connected to 2 terminals, a line connection can be established by dialing.
2	Unexpected characters are displayed at login.	Perform the following procedure: 1. Set the communication speed of the modem to 9600 bit/s. 2. If the modem supports V.90, K56flex, x2, or later communication standards, specify V.34 or an earlier communication mode for the connection.
3	After a disconnection, redialing fails due to a busy signal.	After a line disconnects, the modem might not answer for several seconds. See the modem documentation.
4	After a line failure, the connection cannot be re-established.	If a line disconnects due to a line failure, it might take up to 120 seconds before you can reconnect. If you want to reconnect immediately, log in as another user, and then use the `killuser` command to forcibly log out the user that is connected to the AUX port over a dial-up IP connection.
5	After a disconnection, the connection cannot be re-established.	If a dial-up IP connection disconnects, it might take some time before you can reconnect. In such a case, wait approximately 300 seconds before trying to reconnect.

2.2.2 Unable to log in from a remote operation terminal

If a problem occurs during connection to a remote operation terminal, check the situation according to the following table.

Table 2-3: Problems that occur during connection to a remote operation terminal, and action to be taken

No.	Problem	Items to be checked
1	Remote connection is impossible.	Perform the following procedure: 1. From a remote operation terminal, use the `ping` command to make sure that a route for the remote connection has been established. 2. After the "connection established" message is displayed, if it takes time for the prompt to appear, communication with the DNS server might be impossible. (If communication with the DNS server is impossible, the prompt can take up to five minutes to appear. This time is a general estimate and varies depending on the network status.)
2	Login is impossible.	Perform the following procedure: 1. Make sure that the terminal you are using has an IP or IPv6 address that is authorized in the access list that was specified in the configuration command `line vty` mode. Also, make sure that `deny` is not specified for the IPv4 or IPv6 address set in the access list. (For details, see the *Configuration Guide*.) 2. Make sure that the maximum number of users who can log in has not been exceeded. (For details, see the *Configuration Guide*.) If the number of logged-in users has reached the maximum, and if connection from a remote operation terminal to the Device is lost and then restored, no more users are able to log in from a remote operation terminal until the TCP connection times out and the session is disconnected. Although the TCP connection timeout varies depending on the status of the remote operation terminal or the network, the connection usually times out after 10 minutes. 3. Make sure that a protocol via which access to the Device is prohibited is not used in the `transport input` command specified in the configuration command `line vty` mode. (For details, see the *Configuration Command Reference*.) 4. Use the `aaa authentication login` configuration command to make sure that RADIUS or TACACS+ authentication is not set. (For details, see *2.2.3 Unable to perform login authentication by using RADIUS or TACACS+*.)
3	Keyboard input is not accepted.	Perform the following procedure: 1. Data transmission might have been interrupted by XON/XOFF flow control. End the interruption by pressing **Ctrl** + **Q**. If the Device still does not accept input from the keyboard, perform steps 2 and 3. 2. Make sure that the communication software settings are correct. 3. The screen might be unresponsive because **Ctrl** + **S** was pressed. Press any key.
4	The user remains logged in.	Either wait for the user to be automatically logged out, or log in again and then use the `killuser` command to forcibly log out the logged-in user. If the user was editing the configuration at the time, log in to the Device again, enter configuration command mode to save the configuration, and then finish editing.

2.2.3 Unable to perform login authentication by using RADIUS or TACACS+

If login authentication by using RADIUS or TACACS+ is impossible, check the following:

1. Communication with the RADIUS or TACACS+ server

   Use the `ping` command to check if a connection from the Device to the RADIUS or TACACS+ server is established. If no connection is established, see *4.1.1 Unable to communicate, or communication is interrupted*. If the IP address of the loopback interface is specified in the configuration, use the `ping` command from the IP address of the loopback interface to make sure that a connection from the Device to the RADIUS or TACACS+ server is established.

2. Settings for the timeout value and the number of retries

The maximum time period during when the Device cannot communicate with theRADIUS or TACACS+sever is determined depending on the setting of the configuration command.

For RADIUS authentication

<Timeout value set for radius-server timeout (in seconds)> x *<Number of retries set for radius-server retransmit>* x *<Number of RADIUS servers set for radius-server host>*

For TACACS+ authentication

<Timeout value set for tacacs-server timeout (in seconds)> x *<Number of TACACS+ servers set for tacacs-server host>*

If this time is significantly long, an application on a remote operation terminal, such as Telnet, might have terminated due to a timeout. If this happens, change the RADIUS or TACACS+ configuration settings or the timeout setting of the application running on the remote operation terminal.

Also, if Telnet or ftp fails despite a system message being output indicating that RADIUS or TACACS+ authentication was successful, the application on the remote operation terminal might have timed out before connecting to a running RADIUS or /TACACS+ server selected from the RADIUS servers specified in the configuration. In such a case, either set a higher priority for the running RADIUS or TACACS+ server, or decrease the value of *<Timeout value (in seconds)>* x *<Number of retries>*.

3. Action to take when login to the Device is impossible

   If you cannot log in to the Device due to, for example, incorrect settings, log in from the console, and then modify the settings. If login authentication has also been implemented on the console by using the `aaa authentication login console` configuration command, perform a default restart by following *2.1.2 The administrator forgot the administrator mode password*, and then log in and modify the settings.

2.2.4 Unable to authenticate commands by using RADIUS, TACACS+, or local authentication

After RADIUS, TACACS+, or local authentication is successful and you log in to the Device, if command authorization fails or if a command cannot be executed due to an authorization error, check the following:

1. Checking permitted commands and restricted commands

   Use the `show whoami` command on the Device to check the list of operation commands that are permitted or restricted for the current user. Make sure that the command list can be obtained exactly as specified in the settings for the RADIUS or TACACS+ server.

   Also, if local command authorization is used, make sure that the command list has been set as specified in the configuration.

2. Checking the server settings and configuration

   Make sure that the settings related to the command authorization for the Device are correct on the RADIUS or TACACS+ server. Take care with the settings of vendor-specific attributes for RADIUS, and with the service and attribute name settings for TACACS+.

   Also, if local command authorization is used, make sure that the settings in the configuration are correct. For details about RADIUS, TACACS+, and local (configuration) settings, see the *Configuration Guide*.

   Notes on creating a command list

   When you code a command list for command authorization for the Device, note the

handling of space characters. For example, if `show ip` (i.e., `show ip` followed by a space) is specified in the permission command list, the `show ip interface` command is permitted, but the `show ipv6 interface` command is not permitted.

3. Action to take when all commands are restricted

   If all commands are restricted due to, for example, incorrect settings, log in from the console, and then modify the settings. If command authorization has also been implemented on the console by using the `aaa authorization commands console` configuration command, perform a default restart by following *2.1.2 The administrator forgot the administrator mode password*, and then log in and modify the settings.

2.3 Configuration Problems

2.3.1 Unable to return from configuration command mode to administrator mode

If you cannot return to administrator mode from configuration command mode, resolve the problem by using either of the following methods.

(1) When connected to a console

Use the following procedure to forcibly log out the target user:

Example:

1. Use the `show sessions` command to check the login number of the target user.
```
(config)# $show sessions
operator console admin 1 Jan 6 14:16
```
The login number of the target user is underlined.

2. Use the `killuser` command to forcibly log out the target user. For the <*login no.*> parameter, specify the login number you checked in step 1.
```
(config)# $killuser 1
```

(2) When connected to a remote operation terminal

Shut down the remote operation terminal, and then re-connect.

If users are still logged in, see *Table 2-3: Problems that occur during connection to a remote operation terminal, and action to be taken*, and follow instruction 4 to resolve the problem.

2.3.2 Unable to update the configuration

(1) Configuration changes are not applied to the running configuration

If the changes to the configuration are not applied to the running configuration at all, check the commit mode. If the commit mode is set to manual, an edited configuration is not immediately applied to the running configuration.

Example:

1. Execute the `status` configuration command to check the commit mode.
```
(config)# status
File name           : running-config
Commit mode         : Manual commit
Last modified time  : Thu Oct 11 12:00:00 20XX UTC by operator (not modified)
Buffer              : Total     XXXXXXXXXX Bytes
                      Available XXXXXXXXXX Bytes (XXXX%)
                      Fragments XX Bytes (XXXX%)
Login user          : USER  operator  LOGIN  Fri Oct 12 12:00:00 20XX UTC edit
```
If `Commit mode` is `Manual commit`, the manual commit mode is set.

In the manual commit mode, to apply the edited configuration to the running configuration, execute the `commit` configuration command.

(2) Configuration changes are not applied to BGP4 or BGP4+ route learning or advertisement

After the route filtering configuration changes, if the changes are applied to the running configuration but not to the learning or advertisement of BGP4 or BGP4+ routes, specify the `* { in | out | both }` parameter in the `clear ip bgp` or `clear ipv6 bgp command`, and then execute

the command.

2.4 NTP/SNTP Communication Failures

2.4.1 Unable to synchronize the system clock with NTP

If the system clock cannot be synchronized by NTP, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 2-4: Failure-analysis method for NTP

No.	Items to be checked and commands	Action
1	Confirm that the Device is synchronized with the NTP server. • `show ntp associations`	If the Device is synchronized with the NTP server but not with the NTP client, check the settings of the NTP client.
		To synchronize the NTP client with the Device while the Device is not synchronized with the NTP server, set the `ntp master` configuration command.
		If the Device is not synchronized with the NTP server, go to step 2.
2	Confirm that the Device can communicate with the NTP server over IPv4. If an IPv4 address is set for the loopback interface, use the `source` parameter to specify the IPv4 address of the loopback interface. • `ping`	If communication with the NTP server is not possible over IPv4, see *4.1 IPv4 network communication failures*.
		If communication with the NTP server is possible over IPv4, go to step 4.
3	If the NTP configuration permits access, check if NTP packets are being discarded by the filter or by QoS.	For details on how to check the filter and QoS, and the action to take, see *8.1 Checking for discarded packets*.
		If no NTP packets are discarded, go to step 4.
4	Check the time difference between the Device and the NTP server.	If the time difference between the Device and the NTP server is 1000 seconds or more, use the `set clock` command to synchronize the system clock of the Device with the NTP server.
		If the time-zone or summer-time setting of the Device differs from that of the NTP server, set the NTP server and the Device to times that are the same time when converted to UTC.

2.4.2 Unable to synchronize the system clock with SNTP

If the system clock cannot be synchronized by SNTP, isolate the cause of the problem according to the failure-analysis method described in the following table.

Table 2-5: Failure-analysis method for SNTP

No.	Items to be checked and commands	Action
1	Confirm that the Device is synchronized with the SNTP server. • `show sntp status`	If the Device is synchronized with the SNTP server but not with the SNTP client, check the settings of the SNTP client.
		To synchronize the SNTP client with the Device while the Device is not synchronized with the SNTP server, set the `sntp master` configuration command.

No.	Items to be checked and commands	Action
		If the Device is not synchronized with the SNTP server, go to step 2.
2	Confirm that the Device can communicate with the SNTP server over IPv4 or IPv6. If an IPv4 or IPv6 address is set for the loopback interface, use the `source` parameter to specify the IPv4 or IPv6 address of the loopback interface. • `ping` • `ping ipv6`	If communication with the SNTP server is not possible over IPv4 or IPv6, see *4.1 IPv4 network communication failures* or *4.2 IPv6 network communication failures*.
		If communication with the SNTP server is possible over IPv4 or IPv6, go to step 3.
3	If the SNTP configuration permits access, check if SNTP packets are being discarded by the filter or by QoS.	For details about how to check the filter and QoS, and the action to take, see *8.1 Checking for discarded packets*.
		If no SNTP packets are discarded, go to step 4.
4	Check the time difference between the Device and the SNTP server.	If the time difference between the Device and the SNTP server is 1000 seconds or more, use the `set clock` command to synchronize the system clock of the Device with the SNTP server.
		If the time-zone or summer-time setting of the Device differs from that of the SNTP server, set the SNTP server and the Device to times that are the same time when converted to UTC.

2.5 Memory Card Problems

2.5.1 Unable to display the status of the memory card

If the `show system` or `show mc` command displays `--------` for `MC`, check the situation and take action according to the following table.

Table 2-6: Action to take when -------- is displayed for MC

No.	Items to be checked and commands	Action
1	Check the ACC LED.	If the ACC LED is green, another process might be accessing the memory card. After the ACC LED turns off, execute the command again.
		If the ACC LED is not green, go to step 2.
2	Remove the memory card, and then re-insert it.	After removing and re-inserting the memory card, execute the command again. Before inserting the memory card, check the memory card and the memory card slot of the Device for dust. If there is dust, wipe it off with a dry cloth, and then insert the memory card.
		If you remove and re-insert the memory card several times but the problem is not resolved, go to step 3.
3	Replace the memory card.	After replacing the memory card, execute the command again. If replacing the memory card does not resolve the problem, the memory card slot might have failed. Replace the BCU.

2.5.2 An error occurs when accessing the memory card

When a command that accesses the memory card is executed, if `The memory card was not found.` is displayed, check the situation and take action according to the following table.

Table 2-7: How to troubleshoot failures when "The memory card was not found." is displayed

No.	Items to be checked and commands	Action
1	Check the ACC LED.	If the ACC LED is green, another process might be accessing the memory card. After the ACC LED turns off, execute the command again.
		If the ACC LED is not green, go to step 2.
2	Remove the memory card, and then re-insert it.	After removing and re-inserting the memory card, execute the command again. Before inserting the memory card, check the memory card and the memory card slot of the Device for dust. If there is dust, wipe it off with a dry cloth, and then insert the memory card.
		If you remove and re-insert the memory card several times but the problem is not resolved, go to step 3.
3	Replace the memory card.	After replacing the memory card, execute the command again. If replacing the memory card does not resolve the problem, the memory card slot might have failed. Replace the BCU.

2.6 Problems with the duplex configuration of the BCU

2.6.1 Unable to switch from the active BCU

If switching between the active and standby BCUs is impossible, check the situation and take action according to the following table.

Table 2-8: Problems that occur during switchover of the active BCU, and action to take

No.	Cause of the problem	Items to be checked	
1	The standby BCU is not running. Check the STATUS LED on the standby BCU.	Red	A fault has occurred in the standby BCU. Replace the standby BCU board.
		Off	The standby BCU is not running. Execute the `inactivate bcu standby` and the `activate bcu standby` commands from the active BCU to start the standby BCU.
		Blinking green	The standby BCU is running. Wait a while until the STATUS LED turns solid green.
		Solid green	The standby BCU has started. The problem in switching is probably due to another cause. See the other items to be checked.
2	The standby BCU is not ready for switching. Log in to the active BCU, and then execute the `show system command` to check the status of the standby BCU.	`fault`	A fault has occurred in the standby BCU. Replace the standby BCU board.
		`inactive`	Startup of the standby BCU has been suppressed. Execute the `activate bcu standby` command to start up the standby BCU.
		`notconnect`	A standby BCU is not installed. Install a standby BCU, and then execute the `activate bcu standby` command to start the standby BCU.
		`initialize`	The standby BCU is starting. Wait a while until startup is complete.
		`standby(configuration discord)`	The configuration of the active BCU does not match the configuration of the standby BCU. Use the `save` or `synchronize` command to harmonize the configuration between the BCUs.
		`notsupport`	An unsupported BCU is installed. Replace the standby BCU board.
		`standby`	The problem in switching is probably due to another cause. See the other items to be checked.
3	A configuration operation is being performed. During this time, if an operation command is executed to switch the active system, the command fails. Check whether a configuration operation is being performed.	During configuration operations, switching the active system by using an operation command is not allowed. From the active BCU, execute the `status` configuration command. Log out all the users who are performing configuration operations, and then execute the operation command to switch the active system.	

2.7 SNMP communication failures

2.7.1 The SNMP manager cannot acquire MIBs

Check the configuration setting as follows:

(1) When using SNMPv1 or SNMPv2C

Execute the `show ip access-list` configuration command, and check whether the IP address of the SNMP manager has been set in the access list. If the IP address of the SNMP manager is not set in the access list, add the IP address.

After that, execute the `show snmp-server` configuration command, and check whether the community name and access list have been set correctly. If the community name and access list have not been correctly set, execute the `snmp-server community` configuration command to set the information about the SNMP manager.

Example:

```
(config)# show ip access-list
 ip access-list standard ACL
 10 permit 20.1.1.1
 !
(config)# show snmp-server
 snmp-server community "event-monitor" ro ACL
 !
(config)#
```

(2) When using SNMPv3

Execute the `show snmp-server` configuration command, and check whether the SNMP information has been set correctly in the configuration of the Device. If the information has not been correctly set, execute the following configuration commands to set the SNMP information.

- `snmp-server engineID local`
- `snmp-server group`
- `snmp-server user`
- `snmp-server view`

Example:

```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv read "view1" write "view1"
  snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/
+6789"
  snmp-server view "view1" 1.3.6.1.2.1.1 included
  !
(config)#
```

2.7.2 The SNMP manager cannot receive traps

Check the configuration setting as follows:

Some SNMP manager systems might not be able to receive OSPF and BGP traps issued over SNMPv2C or SNMPv3. In such a case, check the trap reception setting for the SNMP manager based on the object ID of each type of trap described in the *MIB Reference*.

(1) When using SNMPv1 or SNMPv2C

Execute the `show snmp-server` configuration command, and check whether the information about the SNMP manager and traps has been set in the configuration of the Device. If the information has not been set, execute the `snmp-server host` configuration command to set the information

about the SNMP manager and traps.

Example:

```
(config)# show snmp-server
 snmp-server host    192.0.2.0 traps "event-monitor" snmp
 !
(config)#
```

(2) When using SNMPv3

Execute the `show snmp-server` configuration command, and check whether the information about the SNMP and traps has been set in the configuration of the Device. If the information has not been correctly set, execute the following configuration commands to set the information about the SNMP and traps.

- `snmp-server engineID local`
- `snmp-server group`
- `snmp-server host`
- `snmp-server user`
- `snmp-server view`

Example:

```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv notify "view1"
  snmp-server host    192.0.2.0 traps "v3user" version 3 priv snmp
  snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/
+6789"
  snmp-server view "view1" 1.3.6.1 included
  !
(config)#
```

2.7.3 The SNMP manager cannot receive informs

Execute the `show snmp-server` configuration command, and check whether the information about the SNMP manager and informs has been set in the configuration of the Device. If the information has not been set, execute the `snmp-server host` configuration command to set the information about the SNMP manager and informs.

Example:

```
(config)# show snmp-server
  snmp-server host 192.0.2.0 informs "event-monitor" snmp
 !
(config)#
```

Some SNMP manager systems might not be able to receive OSPF and BGP informs issued over SNMPv2C or SNMPv3. In such a case, check the inform reception settings for the SNMP manager based on the object ID of each type of inform described in the *MIB Reference*.

Chapter

3. Troubleshooting Network Interfaces

This chapter describes the actions to be taken when a problem occurs with a network interface.

3.1 Ethernet communication failure

3.1.1 Unable to connect to an Ethernet port

If it is possible that the Ethernet port caused the communication failure, check the status of the NIF, the status of the port, and the statistics of the port, in that order.

(1) Checking the status of the NIF

1. Checking the log

   For details about the contents of the log and the action to be taken, see the *Message and Log Reference*.

2. Isolating the cause of the problem by checking the NIF status

   Use the `show interfaces` command to check the NIF status, and then isolate the cause of the problem according to the following table.

   Table 3-1: Checking the NIF status, and action to be taken

No.	NIF status	Cause	Action
1	`active`	The target NIF is operating normally.	Check the status of the port according to *Table 3-2: Checking the port status, and action to be taken*
2	`notconnect`	The target NIF is not installed.	Install the NIF.
3	`inactive`	The `inactivate` command has been set.	Use the `activate` command to activate the target NIF.
		The NIF is not running.	Use the `show system` command to check the operating status of the PRU, and then activate the PRU.
4	`fault`	A failure has occurred in the target NIF.	Based on the log entry for the target NIF displayed by the `show logging` command, take the action described in the *Message and Log Reference*.
5	`initialize`	The target NIF is being initialized.	Wait until the initialization is complete.
6	`disable`	`no power enable` has been set by a configuration command.	Make sure that the NIF to be used is installed, and then use the `power enable` configuration command to activate the target NIF.
7	`power shortage`	Operation stopped due to a power shortage.	Use the `show environment` command to check the information on the power and surplus power of the device. • If the power supply is in the `fault` status, replace the power supply unit. • If the power supply is in the `active` status, check the surplus power of the device, and add a power supply unit if necessary.
8	`notsupport`	A NIF that the Device does not support is installed.	Replace the NIF.
		A NIF that the software version does not support is installed.	Check the NIF type and the software version, and then either replace the NIF or update the software.

(2) Checking the port status

1. Checking the log

   For details about the contents of the log and the action to be taken, see the *Message and Log Reference*.

2. Isolating the cause of the problem by checking the port status

   Use the `show interfaces` command to check the port status, and then isolate the cause of the problem according to the following table.

   Table 3-2: Checking the port status, and action to be taken

No.	Port status	Cause	Action
1	`active up`	The target port is operating normally.	None
2	`active down`	A line failure has occurred on the target port.	Based on the log entry for the target port displayed by the `show logging` command, take the action described in the *Message and Log Reference*.
3	`inactive`	The `inactivate` command has been set.	To change the status to `active up`, make sure that the cable is connected to the target port, and then use the `activate` command to activate the target port.
4	`fault`	A failure has occurred in the hardware of the target port.	Based on the log entry for the target port displayed by the `show logging` command, take the action described in the *Message and Log Reference*.
5	`initialize`	The target port is being initialized.	Wait until initialization is complete.
6	`disable`	The `shutdown` configuration command has been set.	To change the status to `active up`, make sure that the cable is connected to the target port, and then use the `no shutdown` configuration command to activate the target port.
7	`standby`	The port has been put into the standby status by the link aggregation standby-link function.	Because the port has been put into the `standby` status by the link aggregation standby-link function, operation is normal. Use the `show channel-group` command with the `detail` parameter to check the standby link functionality.
8	`suspend`	The port cannot be started due to either of the following causes: • An insufficient number of SFU units are operating. • The PRU is being initialized.	Use the `show system` command to check the status of the SFU and the PRU. • Check the number of SFU units that are in the `active` status. • If the PRU is in the `initialize` status, wait for the PRU initialization to finish.
9	`unused`	No configuration has been generated.	Wait for the configuration of the port that corresponds to the installed NIF to be generated.
10	`mismatch`	The Ethernet type recorded in the installed NIF does not match the Ethernet type of the running configuration.	• Check the type of the installed NIF. If the type of the installed NIF is incorrect, replace the NIF. • Use the `show running-config` command to check the running configuration. If the running configuration is incorrect, delete the pre-installation configuration of the port. For details about deleting the configuration, see the *Configuration Guide*.

(3) Checking statistics

You can use the `show port statistics` command to check the number of sent and received packets and the number of discarded packets for all ports on the Device.

Figure 3-1: Example of displaying port statistics

```
> show port statistics
Date 20XX/04/01 12:00:00 UTC
Port Counts: 12
Port  Name           Status   Packets                 Tx                   Rx
```

```
 1/1   geth1/1         down      Ucast                    0                    0
                                 Mcast                    0                    0
                                 Bcast                    0                    0
                                 Discard                  0                    0
 1/2   geth1/2         down      Ucast                    0                    0
                                 Mcast                    0                    0
                                 Bcast                    0                    0
                                 Discard                  0                    0
 1/3   geth1/3         down      Ucast                    0                    0
                                 Mcast                    0                    0
                                 Bcast                    0                    0
                                 Discard                  0                    0
         :
>
```

Note that if a value of `Discard` is greater than 0, it indicates that a failure has occurred and packets have been discarded. Use the `show interfaces` command to check the detailed information about the target port.

3.1.2 SFU/PRU problems

If it is possible that the SFU or PRU unit caused the communication failure, perform the check procedure described below.

(1) Checking the status of the SFU

1. Checking the log

   For details about the contents of the log and the action to be taken, see the *Message and Log Reference*.

2. Isolating the cause of the problem by checking the SFU status

   Use the `show system` command to check the SFU status, and then isolate the cause of the problem according to the following table.

   Table 3-3: Checking the SFU status, and action to be taken

No.	SFU status	Cause	Action
1	`active`	The target SFU is operating normally as an active unit.	See *3.1.1 Unable to connect to an Ethernet port*. If an insufficient number of SFU units is in the `active` status, the bandwidth may decrease.
2	`fault`	A failure has occurred in the target SFU.	Based on the log entry for the target SFU displayed by the `show logging` command, take the action described in the *Message and Log Reference*.
3	`initialize`	The target SFU is being initialized.	Wait until initialization is complete.
4	`inactive`	The `inactivate sfu` command has been set.	Use the `activate sfu` command to activate the target SFU.
5	`notsupport`	An SFU that the Device does not support is installed.	Replace the SFU.
6	`disable`	`no power enable` has been set by a configuration command.	Make sure that the SFU to be used is installed, and then use the `power enable` configuration command to activate the target SFU.
7	`notconnect`	The target SFU is not installed.	Install the SFU.

(2) Checking the status of the PRU

1. Checking the log

   For details about the contents of the log and the action be to taken, see the *Message and Log*

Reference.

2. Isolating the cause of the problem by checking the PRU status

   Use the `show system` command to check the PRU status, and then isolate the cause of the problem according to the following table.

   Table 3-4: Checking the PRU status, and action to be taken

No.	PRU status	Cause	Action
1	`active`	The target PRU is operating normally.	See *3.1.1 Unable to connect to an Ethernet port*.
2	`fault`	A failure has occurred in the target PRU.	Based on the log entry for the target PRU displayed by the `show logging` command, take the action described in the *Message and Log Reference*.
3	`initialize`	The target PRU is being initialized.	Wait until initialization is complete.
4	`inactive`	The `inactivate pru` command has been set.	Use the `activate pru` command to activate the target PRU.
5	`notsupport`	A PRU that the Device does not support is installed.	Replace the PRU.
6	`power shortage`	Operation stopped due to a power shortage.	Use the `show environment` command to check the information on the power and surplus power of the device. • If the power supply is in the `fault` status, replace the power supply unit. • If the power supply is in the `active` status, check the surplus power of the device, and add a power supply unit if necessary.
7	`disable`	`no power enable` has been set by a configuration command.	Make sure that the PRU to be used is implemented, and then use the `power enable` configuration command to activate the target PRU.
8	`notconnect`	The target PRU is not installed.	Install the PRU.

3.1.3 10BASE-T, 100BASE-TX, or 1000BASE-T problems

If a 10BASE-T, 100BASE-TX, or 1000BASE-T problem occurs, use the following procedure to isolate the failure:

1. Checking the log

   For details about the contents of the log and the action to be taken, see the *Message and Log Reference*.

2. Isolating the cause of the problem by using the failure-analysis method

   Isolate the cause of the problem by using the failure-analysis method described in the following table.

   Table 3-5: Failure-analysis method for 10BASE-T, 100BASE-TX, and 1000BASE-T problems

No.	Items to be checked and commands	Cause	Action
1	Use the failure statistics of the target port to check whether there is a count for `Link down`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The line quality is degraded.	Check whether the cable types are correct. For details on the cable types, see the *Hardware Instruction Manual*.

No.	Items to be checked and commands	Cause	Action
			If the Device is set in one of the following ways, make sure that the pin mapping is the MDI-X pin mapping: • A fixed connection is set for the target port. • On the target port, auto-negotiation is enabled and the automatic MDI/MDIX functionality is disabled.
			Check the cable length. For details on the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly.
			Replace the interface with a connection interface that the Device supports. For details about the connection interfaces that the Device supports, see the *Configuration Guide*.
2	Use the failure statistics for the receiving side of the target port to check whether there is a count for `CRC errors` or `Symbol errors`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The line quality is degraded.	Check whether the cable types are correct. For details on the cable types, see the *Hardware Instruction Manual*.
			If the Device is set in one of the following ways, make sure that the pin mapping is the MDI-X pin mapping: • A fixed connection is set for the target port. • On the target port, auto-negotiation is enabled and the automatic MDI/MDIX functionality is disabled.
			Check the cable length. For details on the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly.
			Replace the interface with a connection interface that the Device supports. For details about the connection interfaces that the Device supports, see the *Configuration Guide*.
3	Use the failure statistics of the target port to check whether there is a count for `MDI cross over changed`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The pin mapping of the cable is incorrect.	Correct the pin mapping. For details about the pin mapping, see the *Configuration Guide*.
4	Use the port information of the target port to check whether the line type and speed are correct. If the line type or speed is incorrect, see the *Cause* and *Action* columns. • `show interfaces`	The cable is incompatible.	Check whether the cable types are correct. For details on the cable types, see the *Hardware Instruction Manual*.
		The line speed and `duplex` settings do not match the settings of the remote device.	For the `speed` and `duplex` configuration commands, specify the same values that are set on the remote device.
		Other than the above	To use a specific speed in auto-negotiation, set the line speed for auto-negotiation. For details, see the *Configuration Guide*.

No.	Items to be checked and commands	Cause	Action
5	Use the failure statistics for the receiving side of the target port to check whether there is a count for `Long frames`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	Packets that exceed the maximum allowed frame length were received.	Adjust the jumbo frame settings to match those on the remote device.

3.1.4 1000BASE-X problems

If a 1000BASE-X problem occurs, use the following procedure to isolate the failure:

1. Checking the log

   For details about the contents of the log and the action to be taken, see the *Message and Log Reference*.

2. Isolating the cause of the problem by using the failure analysis method

   Isolate the cause of the problem by using the failure-analysis method described in the following table.

   Table 3-6: Failure-analysis method for 1000BASE-X problems

No.	Items to be checked and commands	Cause	Action
1	Use the failure statistics of the target port to check whether there is a count for `Link down` or `Signal detect errors`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The line quality on the receiving side is degraded.	Check the type of the optical fiber. For details on the type of optical fiber, see the *Hardware Instruction Manual.*
			If an optical attenuator is in use, check the attenuation value. For details on the optical level, see the *Hardware Instruction Manual*.
			Check the cable length. For details on the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly. Make sure that the ends of the cables are clean. If they are dirty, clean them.
			Check whether the transceiver is connected correctly.
			For the `speed` and `duplex` configuration commands, specify the same values that are set on the remote device.
			Comply with the segment standards of the remote device.
			Check whether the optical level is correct. For details on the optical level, see the *Hardware Instruction Manual*.
2	Use the failure statistics for the receiving side of the target port to check whether there is a count for `CRC errors` or `Symbol errors`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The line quality on the receiving side is degraded.	Check the type of the optical fiber. For details on the cable types, see the *Hardware Instruction Manual*.

No.	Items to be checked and commands	Cause	Action
			If an optical attenuator is in use, check the attenuation value. For details on the optical level, see the *Hardware Instruction Manual*.
			Check the cable length. For details on the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly. Make sure that the ends of the cables are clean. If they are dirty, clean them.
			Check whether the transceiver is connected correctly.
			For the `speed` and `duplex` configuration commands, specify the same values that are set on the remote device.
			Comply with the segment standards of the remote device.
			Check whether the optical level is correct. For details on the optical level, see the *Hardware Instruction Manual*.
3	If a single-core optical fiber cable such as 1000BASE-BX is in use, make sure that the transceiver of the Device is suitable for use with the remote transceiver.	The combination of the transceivers is incorrect.	If 1000BASE-BX is in use, one side must use a U-type transceiver and the other side must use a D-type transceiver. Check whether the transceiver types are correct.
4	Use the failure statistics for the receiving side of the target port to check whether there is a count for `Long frames`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	Packets that exceed the maximum allowed frame length were received.	Adjust the jumbo frame settings to match those on the remote device.

3.1.5 10GBASE-R and 100GBASE-R problems

If a 10GBASE-R or 100GBASE-R problem occurs, use the following procedure to isolate the failure:

1. Checking the log

   For details about the contents of the log and the action to be taken, see the *Message and Log Reference*.

2. Isolating the cause of the problem by using the failure-analysis method

   Isolate the cause of the problem by using the failure-analysis method described in the following table.

   Table 3-7: Failure-analysis method for 10GBASE-R and 100GBASE-R problems

No.	Items to be checked and commands	Cause	Action
1	Use the failure statistics of the target port to check whether there is a count for `Signal detect errors`, `LOS of sync`, `HI_BER`, or `LF`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The line quality on the receiving side is degraded.	Check the type of the optical fiber. For details on the types of optical fiber, see the *Hardware Instruction Manual*.

No.	Items to be checked and commands	Cause	Action
			If an optical attenuator is in use, check the attenuation value. For details on the optical level, see the *Hardware Instruction Manual*.
			Check the cable length. For details on the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly. Make sure that the ends of the cables are clean. If they are dirty, clean them.
			Check whether the transceiver is connected correctly.
			Adjust the transceiver to comply with the segment standards of the remote device.
			Check whether the optical level is correct. For details on the optical level, see the *Hardware Instruction Manual*.
2	Use the failure statistics for the receiving side of the target port to check whether there is a count for `CRC errors` or `Symbol errors`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The line quality on the receiving side is degraded.	Check the type of the optical fiber. For details on the types of optical fiber, see the *Hardware Instruction Manual*.
			If an optical attenuator is in use, check the attenuation value. For details on the optical level, see the *Hardware Instruction Manual*.
			Check the cable length. For details on the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly. Make sure that the ends of the cables are clean. If they are dirty, clean them.
			Check whether the transceiver is connected correctly.
			Adjust the transceiver to comply with the segment standards of the remote device.
			Check whether the optical level is correct. For details on the optical level, see the *Hardware Instruction Manual*.
3	Use the failure statistics of the target port to check whether there is a count for `RF`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	The line quality on the sending side is degraded.	Check the type of the optical fiber. For details on the types of optical fiber, see the *Hardware Instruction Manual*.
			If an optical attenuator is in use, check the attenuation value. For details on the optical level, see the *Hardware Instruction Manual*.
			Check the cable length. For details on the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly (for example, make sure the connectors are fully inserted). Make sure that the ends of the cables are clean. If they are dirty, clean them.
			Check whether the transceiver is connected correctly.

No.	Items to be checked and commands	Cause	Action
			Adjust the transceiver to comply with the segment standards of the remote device.
			Check whether the optical level is correct. For details on the optical level, see the *Hardware Instruction Manual*.
4	Use the failure statistics for the receiving side of the target port to check whether there is a count for `Long frames`. If there is, see the *Cause* and *Action* columns. • `show interfaces`	Packets that exceed the maximum allowed frame length were received.	Adjust the jumbo frame settings to match those on the remote device.

3.2 Communication failure when using link aggregation

When link aggregation is in use, if communication is impossible or operation is degraded, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 3-8: Communication failure-analysis method when link aggregation is used

No.	Items to be checked and commands	Action
1	Check that the mode of the aggregated link that has failed matches the mode of the remote device. • `show channel-group detail`	If the modes are different, change the link aggregation mode to match the mode for the remote device.
		If the modes are the same and LACP link aggregation is in use, check that the LACP start method of each port is not `passive` on both the Device and the remote device. If the LACP start method on both devices is `passive`, change the method of either the Device or the remote device to `active`. If the method is set to `active` on either (but not both) the Device or the remote device, go to step 2.
		If the modes are the same, and static link aggregation is in use, go to step 3.
2	Use the statistics of the aggregated link that has failed to check if the values of `TxLACPDUs` and `RxLACPDUs` increase. • `show channel-group statistics lacp`	If the value of either TxLACPDUs or RxLACPDUs does not increase, see *3. Troubleshooting Network Interfaces* to check the line status. If the line status has no problem, check if LACPDUs are not being discarded by the filter or QoS. For details on how to check this, see *8.1 Checking for discarded packets*.
		If the values of both TxLACPDUs and RxLACPDUs increase, go to step 3.
3	Use `Status` to check the status of the port that caused the communication failure. • `show channel-group detail`	If all ports of the channel group go down, the channel group also goes down. For the port that went down, take one of the following actions according to the reason displayed: • `Standby` The port of the channel group of the Device is in the standby status. To cancel the standby status, delete the `channel-group max-active-port` setting from the configuration of the port channel interface. • `CH Disabled` The link channel group is in the `Disable` status, and therefore down. To cancel the `Disable` status, delete the `shutdown` setting from the configuration of the port channel interface. • `Port Down` The port link is down. See *3. Troubleshooting Network Interfaces*. • `Port Speed Unmatch` The line speed of the port is different from that of the other ports in the channel group, and degradation has occurred. To resolve the degradation, specify the same speed for all ports in the channel group. • `Duplex Half` The duplex mode is `Half` and degradation has occurred. To resolve the degradation, set the duplex mode to `Full`.

No.	Items to be checked and commands	Action
		• `Port Selecting` A port aggregation condition check is being performed, and degradation has occurred. Wait a while. If the problem is not resolved, check the operating status and settings of the remote device. • `Waiting Partner Synchronization` The port aggregation condition check finished, but degradation has occurred because the system is waiting for the partner port to synchronize. Wait a while. If the problem is not resolved, check the operating status and settings of the remote device. • `Partner System ID Unmatch` The `Partner System ID` received from the partner port is different from the `Partner System ID` of the group, and degradation has occurred. To resolve the degradation, check the operating status and wiring of the remote device. • `LACPDU Expired` The validity period of the LACPDU from the partner port expired, and the target port is in a degraded state. Use the `show channel-group statistics` command with the `lacp` parameter to check the statistics for the LACPDU. Also, check the operating status and settings of the remote device. • `Partner Key Unmatch` The key received from the partner port is different from the `Partner Key` of the group, and degradation has occurred. To resolve the degradation, check the operating status and wiring of the remote device. • `Partner Aggregation Individual` A "link aggregation impossible" message was received from the partner port, and degradation has occurred. To resolve the degradation, check the operating status and settings of the remote device. • `Partner Synchronization OUT_OF_SYNC` A "synchronization impossible" message was received from the partner port, and degradation has occurred. (This state occurs if the link aggregation changes or if the line is deactivated on the remote device.) • `Port Moved` The connected port was moved to another port. Check the wiring. • `Operation of Detach Port Limit` The port detachment restriction functionality is activated, and the channel group is down.

Chapter

4. Troubleshooting IP and Routing

This chapter describes the action to be taken when a problem occurs with communication or routing on an IP network.

4.1 IPv4 network communication failures

4.1.1 Unable to communicate, or communication is interrupted

There are three probable causes of problems that occur during communication on an IPv4 network on which the Device is in use:

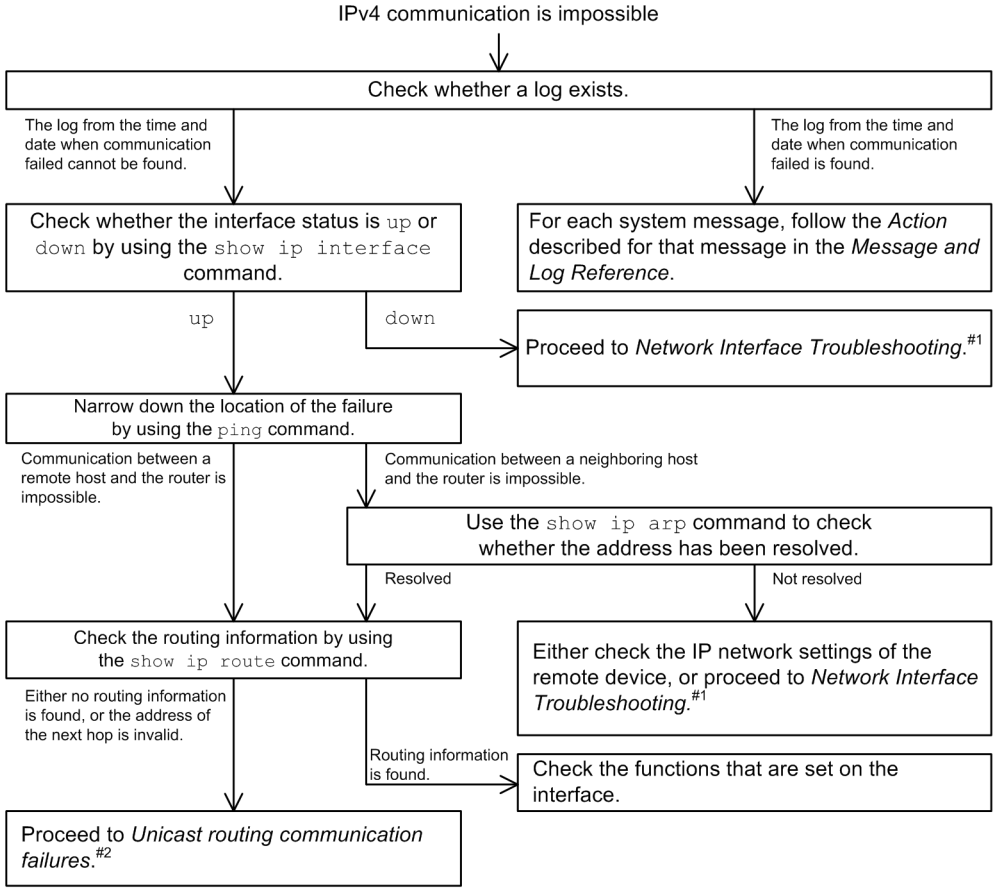
1. A setting related to IPv4 communication was changed.
2. The network configuration was changed.
3. A network device failed.

For causes 1 and 2, check the differences between the Device configuration and network configuration before and after the change to uncover any issue that could disable communication.

This subsection describes the procedure for isolating the fault location to determine the cause of a problem, and applies mainly to failures due to cause 3. For example, IPv4 communication might be impossible even if the Device configuration and network configuration are correct, or even for operations that hitherto were normal.

Use the following flowchart to isolate the fault location and identify the cause of the problem.

Figure 4-1: Failure-analysis flow when IPv4 communication is disabled



#1: See *3. Troubleshooting Network Interfaces*.

#2: See *4.5 Unicast routing communication failures*.

(1) Checking the log

Display the log to check for a system message that indicates the occurrence of a failure. If

communication is disabled due to a line failure (or line damage) or another cause, a system message is displayed. To check the log, do the following:

1. Log in to the Device.
2. Execute the `show logging` command to display the log.
3. Each entry in the log indicates the date and time that a failure occurred. Check whether a log entry was displayed for the date and time when communication was disabled.
4. For details about the failure and corrective action for the log entry described above, follow the instructions given in the *Message and Log Reference*.
5. If a log entry was not displayed for the date and time when communication was disabled, see *(2) Checking the interface status*.

(2) Checking the interface status

Even if the hardware of the Device is operating normally, a fault might have occurred in the hardware of a neighboring device that is connected to the Device.

To check the status of the interface between the Device and the neighboring device, do the following:

1. Log in to the Device.
2. Use the `show ip interface` command to check whether the status of the interface with the target neighboring device is `Up` or `Down`.
3. If the status of the target interface is `Down`, see *3. Troubleshooting Network Interfaces*.
4. If the target interface is `Up`, see *(3) Narrowing down the location of the failure (from the Device)*.

(3) Narrowing down the location of the failure (from the Device)

If the failure did not occur on the Device, the failure might have occurred somewhere on the route between the Device and the remote devices. To narrow down the location of the failure, do the following:

1. Log in to the Device.
2. Use the `ping` command to check the communication with the two remote devices that are unable to communicate. For examples of using the `ping` command and details about how to interpret the execution result, see the *Operation Command Reference*.
3. If communication with the remote devices cannot be verified by using the `ping` command, execute the command again to check communication with each of the devices up to the remote device, beginning with the device closest to the Device.
4. If the execution result of the `ping` command indicates that the failure occurred on the neighboring device, see *(5) Checking the status of ARP resolution with a neighboring device*. If the execution result indicates a failure on the remote device, see *(6) Checking the unicast routing information*.

(4) Narrowing down the location of the failure (from a customer's terminal)

In an environment in which logging in to the Device is impossible, to use a customer's terminal to narrow down the location of the failure, do the following:

1. Make sure that the customer's terminal has the `ping` functionality.
2. Use the `ping` functionality to check whether communication between the customer's terminal and the remote device is possible.
3. If communication with the remote device cannot be verified by using the `ping` functionality, use the `ping` command to check communication with each of the devices up to the remote device, beginning with the device closest to the customer's terminal.

4. If you are able to narrow down the location of the failure by using the `ping` functionality, and it appears likely that the failure lies in the Device, log in to the Device, and then investigate the cause of the failure by using the failure-analysis flowchart.

(5) Checking the status of ARP resolution with a neighboring device

If the result of the `ping` command indicates that communication with a neighboring device is disabled, ARP might not have resolved the address. To check the status of address resolution between the Device and the neighboring device, do the following:

1. Log in to the Device.
2. Use the `show ip arp` command to check the status of address resolution (whether ARP entry information exists) between the Device and the neighboring device.
3. If the address of the neighboring device has been resolved (ARP entry information exists), see *(6) Checking the unicast routing information*.
4. If the address has not been resolved (no ARP entry information exists), check whether the IP network settings on the neighboring device and on the Device are identical.

(6) Checking the unicast routing information

You need to check the routing information obtained by the Device in the following cases: communication is still disabled after address resolution with the neighboring device completes, communication is disabled on the route to the remote device during IPv4 unicast communication, or the route to the remote device has a problem. The procedure for checking the routing information is as follows:

1. Log in to the Device.
2. Execute the `show logging` command to check for a message that indicates that the number of IPv4 unicast routes has reached the limit (message type: PRU, message identifier: 41011002).

   If such a system message is displayed, the number of IPv4 unicast routes has reached the limit. In that case, no more IPv4 unicast routes can be registered. We recommend that you review the network configuration and operate within the limits.

   After reviewing the network configuration, use the `clear ip route` command with the `vrf all *` parameter specified to re-register the IPv4 unicast routes.
3. Execute the `show ip route` command to check the routing information obtained by the Device.
4. Check whether packets are being discarded at the null interface. In the routing information, if `null0` is displayed for the sending interface that caused the communication failure, packets are being discarded at the null interface. Review the static routing configuration.
5. If the routing information obtained by the Device either does not contain the routing information about the interface that caused the communication failure or contains an incorrect address of the interface's next hop, see *4.5 Unicast routing communication failures*.
6. If the routing information obtained by the Device contains routing information about the interface that caused the communication failure, the interface might have a problem with one of the functions shown below. Check that function.
   - DHCP/BOOTP relay agent

     See *(7) Checking the configuration of DHCP/BOOTP relay agent*.
   - Filter, QoS, or uRPF

     See *(8) Checking for discarded packets*.
   - Policy-based routing

     See *4.3.1 Checking for policy-based routing communication failures*.

(7) Checking the configuration of DHCP/BOOTP relay agent

If IP addresses are assigned to neighboring devices by the DHCP/BOOTP relay agent on the Device, the IP addresses might have not been properly assigned.

Check the configuration of the DHCP/BOOTP relay agent. For the procedure, see *4.1.2 The DHCP/BOOTP relay agent cannot allocate IP addresses*.

(8) Checking for discarded packets

Packets might have been discarded by filters, QoS, or uRPF. For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.

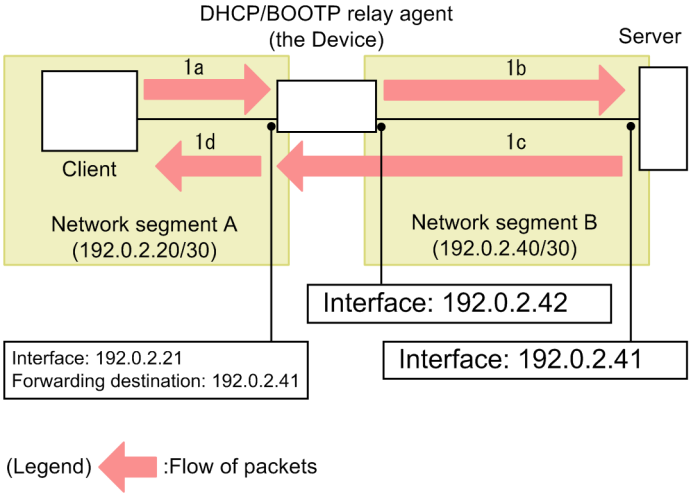
4.1.2 The DHCP/BOOTP relay agent cannot allocate IP addresses

The following shows the four possible causes of a communication problem with the DHCP/BOOTP relay agent:

- The configuration of the DHCP/BOOTP relay agent
- The configuration of the DHCP or BOOTP server (hereinafter, the server)
- The configuration of the DHCP or BOOTP client (hereinafter, the client)
- An IPv4 network communication failure

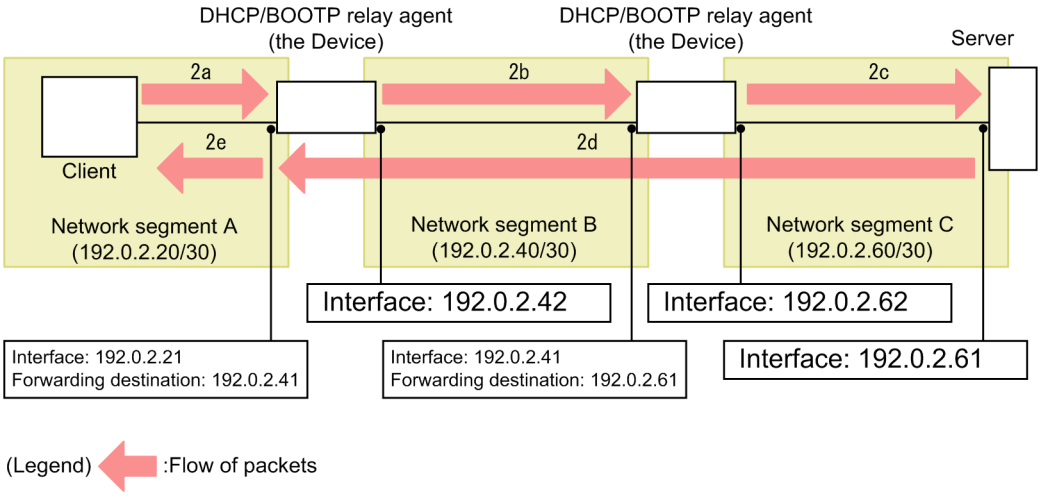
This section uses the following network configuration as an example to explain the procedure for isolating the fault location and cause of the failure.

Figure 4-2: Example network configuration for the DHCP/BOOTP relay agent (single layer)



Items to be checked (Indication in the figure)	Value in the packet			
	Destination IP address	Source IP address	Destination UDP port number	Source UDP port number
1a	255.255.255.255	0.0.0.0	67	Optional
1b	192.0.2.41	192.0.2.42	67	68
1c	192.0.2.21	192.0.2.41	67	Optional
1d	Address assigned by DHCP	192.0.2.21	68	67

Figure 4-3: Example network configuration for the DHCP/BOOTP relay agent (multiple layers)



Items to be checked (Indication in the figure)	Value in the packet			
	Destination IP address	Source IP address	Destination UDP port number	Source UDP port number
2a	255.255.255.255	0.0.0.0	67	Optional
2b	192.0.2.41	192.0.2.42	67	68
2c	192.0.2.61	192.0.2.62	67	68
2d	192.0.2.21	192.0.2.61	67	Optional
2e	Address assigned by DHCP	192.0.2.21	68	67

Before checking items marked 1a and 1d or 2a and 2e in the figure, temporarily set a fixed IP address for the client instead of the assigned DHCP address.

(1) Checking the status and statistics of the DHCP/BOOTP relay agent

Check the status and statistics of the DHCP/BOOTP relay agent and isolate the cause by following the failure-analysis method described in the following table.

Table 4-1: DHCP/BOOTP relay agent failure-analysis method

No.	Items to be checked and commands	Action
1	Check whether there is a count for the number of packets received from the client at the interface on the client side (`Receive Packets` under `DHCP/BOOTP Request Packets Count`). • `show ip dhcp relay statistics`	If there is, go to step 2.

No.	Items to be checked and commands	Action
		Otherwise, check the following: • See *(2) Checking the configuration of the DHCP/BOOTP relay agent* to check the forwarding destination of the DHCP or BOOTP packets. • Check the network segment on the client side of the Device (items marked 1a, or 2a and 2b in the figure). For the procedure, see *4.1.1 Unable to communicate, or communication is interrupted*. • Follow the procedure for isolating the cause of a failure on the target client to check the configuration.
2	Check whether there is a count for the number of packets discarded because the number of hops exceeded the maximum number (`Hops Over` under `DHCP/BOOTP Error Packets Count`). • `show ip dhcp relay statistics`	If there is, see *(2) Checking the configuration of the DHCP/BOOTP relay agent* to check the maximum number of hops of the DHCP or BOOTP packets.
		Otherwise, go to step 3.
3	Check if there is a count for the number of packets successfully sent to the server (forwarding destination) at the interface on the client side (`Send Packets` under `DHCP/BOOTP Request Packets Count`). • `show ip dhcp relay statistics`	If there is, go to step 4.
		Otherwise, check the following: • See *(2) Checking the configuration of the DHCP/BOOTP relay agent* to check the IP address of the DHCP/BOOTP relay agent. • Check the items marked 1b, or 2b and 2c in the figure. For the procedure, see *4.1.1 Unable to communicate, or communication is interrupted*.
4	Check whether there is a count for the number of packets received from the server (`Receive Packets` under `DHCP/BOOTP Reply Packets Count`). • `show ip dhcp relay statistics`	If there is, go to step 5.
		Otherwise, check the following: • See *(2) Checking the configuration of the DHCP/BOOTP relay agent* to check the IP address of the DHCP/BOOTP relay agent. • Check the items marked 1c, or 2c and 2d in the figure. For the procedure, see *4.1.1 Unable to communicate, or communication is interrupted*. • Follow the procedure for isolating the cause of the failure on the target server to check the configuration, and check if the network segment is the same.
5	Check whether there is a count for the number of packets successfully sent to the client (`Send Packets` of `DHCP/BOOTP Reply Packets Count`). • `show ip dhcp relay statistics`	If there is, check the following: • Follow the procedure for isolating the cause of the failure on the target server to check if there are enough IP addresses to assign. • Follow the procedure for isolating the cause of the failure on the target client to check the configuration.

No.	Items to be checked and commands	Action
		If there is no such count, check the following: • See *(2) Checking the configuration of the DHCP/BOOTP relay agent* to check the IP address of the DHCP/BOOTP relay agent. • Check the network segment on the client side of the Device (items marked 1d or 2e in the figure). For the procedure, see *4.1.1 Unable to communicate, or communication is interrupted*. • Follow the procedure for isolating the cause of the failure on the target client to check the configuration.

(2) Checking the configuration of the DHCP/BOOTP relay agent

It is possible that IP addresses cannot be assigned to clients because the resources on the DHCP/BOOTP relay agent are configured incorrectly. The following describes the procedure for checking the configuration of the DHCP/BOOTP relay agent.

1. Check whether the forwarding destination of DHCP and BOOTP packets is set (`ip helper-address` configuration command) for the client IP interface.
2. Check whether the maximum number of hops of DHCP and BOOTP packets is set (`ip dhcp relay maximum-hop-count` configuration command) to a value larger than the number of DHCP/BOOTP relay agents between the Device and the clients.
3. For a multihomed configuration, check whether the IP address that matches the network segment of the client is set (`ip dhcp relay gateway` configuration command) for the IP address (`giaddr`) of the DHCP/BOOTP relay agent.

   You can also check the configuration in the interface information of the DHCP/BOOTP relay agent displayed by the `show ip dhcp relay interface` command.

(3) Procedure for when DHCP/BOOTP relay agent and VRRP are operated on the same IP interface

To set the DHCP/BOOTP relay agent and the VRRP on the same IP interface, make sure that the gateway from the client to the server remains the same even if the gateway is switched to other device by VRRP. For example, on the server side, make sure that the virtual router address is set as the default router (router option) and is assigned to the client.

4.2 IPv6 network communication failures

4.2.1 Unable to communicate, or communication is interrupted

There are three probable causes of problems that occur during communication on an IPv6 network on which the Device is in use:

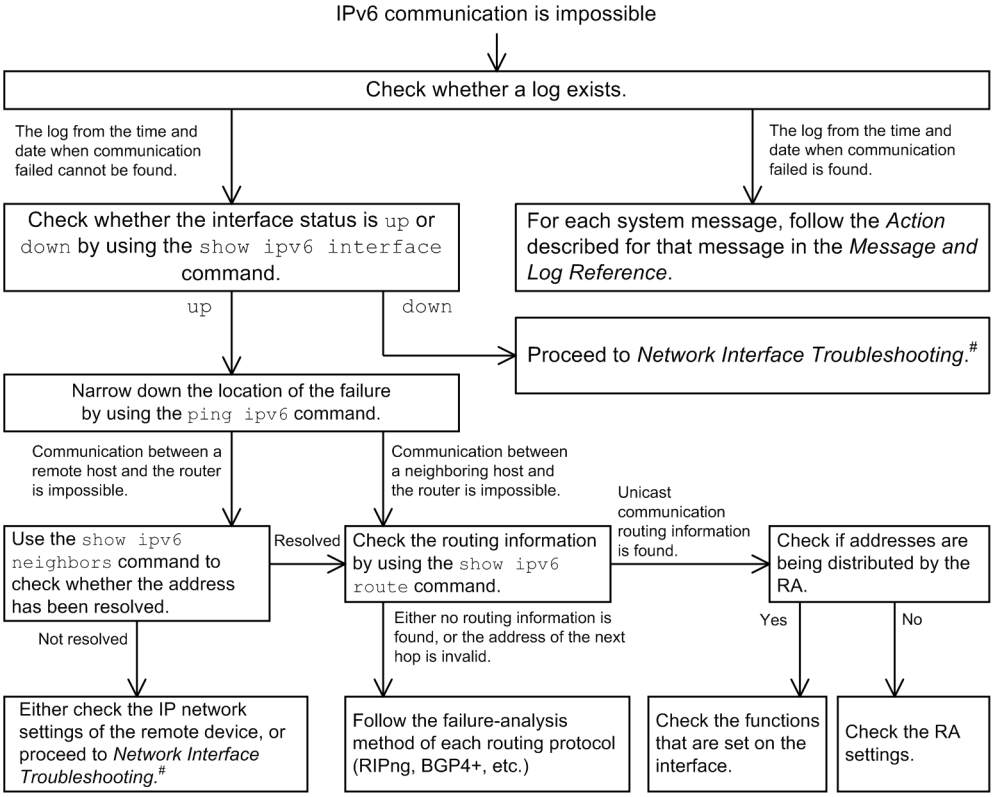
1. A setting related to IPv6 communication was changed.
2. The network configuration was changed.
3. A network device failed.

For causes 1 and 2, check the differences between the Device configuration and network configuration before and after the change to uncover any issue that could disable communication.

This subsection describes the procedure for isolating the fault location to determine the cause of a problem, and applies mainly to failures due to cause 3. For example, IPv6 communication might be impossible even if the configuration and network configuration are correct, or even for operations that hitherto were normal.

Use the following flowchart to isolate the fault location and identify the cause of the problem.

Figure 4-4: Failure-analysis flow when IPv6 communication is disabled



#: See *3. Troubleshooting Network Interfaces*.

(1) Checking the log

Display the log to check for a system message that indicates the occurrence of a failure. If communication is disabled due to a line failure (or line damage) or another cause, a system message is displayed. To check the log, do the following:

1. Log in to the Device.

2. Execute the `show logging` command to display the log.
3. Each entry in the log indicates the date and time that a failure occurred. Check whether a log entry was displayed for the date and time when communication was disabled.
4. For details about the failure and corrective action for the log entry described above, follow the instructions given in the *Message and Log Reference*.
5. If a log entry was not displayed for the date and time when communication was disabled, see *(2) Checking interface status*.

(2) Checking interface status

Even if the hardware of the Device is operating normally, a fault might have occurred in the hardware of a neighboring device that is connected to the Device.

To check the status of the interface between the Device and the neighboring device, do the following:

1. Log in to the Device.
2. Use the `show ipv6 interface` command to check whether the status of the interface with the target neighboring device is `Up` or `Down`.
3. If the status of the target interface is `Down`, see *3. Troubleshooting Network Interfaces*.
4. If the target interface is `Up`, see *(3) Narrowing down the location of the failure (from the Device)*.

(3) Narrowing down the location of the failure (from the Device)

If the failure did not occur on the Device, the failure might have occurred somewhere on the route between the Device and the remote devices. To narrow down the location of the failure in order, do the following:

1. Log in to the Device.
2. Use the `ping ipv6` command to check the communication with the two remote devices that are unable to communicate. For examples of using the `ping ipv6` command and details about how to interpret the execution result, see the *Operation Command Reference*.
3. If communication with the remote devices cannot be verified by using the `ping ipv6` command, execute the command again to check communication with each of the devices up to the remote device, beginning with the device closest to the Device.
4. If the execution result of the `ping ipv6` command indicates that the failure occurred on the neighboring device, see *(5) Checking the status of NDP resolution with a neighboring device*. If the execution result indicates a failure on the remote device, see *(6) Checking the unicast routing information*.

(4) Narrowing down the location of the failure (from a customer's terminal)

In an environment in which logging in to the Device is impossible, to use a customer's terminal to narrow down the location of the failure, do the following:

1. Make sure that the customer's terminal has the `ping ipv6` functionality.
2. Use the `ping ipv6` functionality to check whether communication between the customer's terminal and the remote device is possible.
3. If communication with the remote device cannot be verified by using the `ping ipv6` functionality, use the `ping` command to check communication with each of the devices up to the remote device, beginning with the device closest to the customer's terminal.
4. If you are able to narrow down the location of the failure by using the `ping ipv6` functionality, and it appears likely that the failure lies in the Device, log in to the Device, and then investigate the cause of the failure by using the failure-analysis flowchart.

(5) Checking the status of NDP resolution with a neighboring device

If the result of the `ping ipv6` command indicates that communication with a neighboring device is disabled, NDP might not have resolved the address. To check the status of address resolution between the Device and the neighboring device, do the following:

1. Log in to the Device.
2. Use the `show ipv6 neighbors` command to check the status of address resolution (whether NDP entry information exists) between the Device and the neighboring device.
3. If the address of the neighboring device has been resolved (NDP entry information exists), see *(6) Checking the unicast routing information*.
4. If the address has not been resolved (no NDP entry information exists), check whether the IP network settings on the neighboring device and on the Device are identical.

(6) Checking the unicast routing information

You need to check the routing information obtained by the Device in the following cases: communication is still disabled after address resolution with the neighboring device completes, communication is disabled on the route to the remote device during IPv6 unicast communication, or the route to the remote device has a problem. The procedure for checking the routing information is as follows:

1. Log in to the Device.
2. Execute the `show logging` command to check for a message that indicates that the number of IPv6 unicast routes has reached the limit (message type: PRU, message identifier: 41012002).

   If such a system message is displayed, the number of IPv6 unicast routes has reached the limit. In that case, no more IPv6 unicast routes can be registered. We recommend that you review the network configuration and operate within the limits.

   After reviewing the network configuration, use the `clear ipv6 route` command with the `vrf all *` parameter specified to re-register the IPv6 unicast routes.
3. Execute the `show ipv6 route` command to check the routing information obtained by the Device.
4. Check whether packets are being discarded at the null interface. In the routing information, if `null0` is displayed for the sending interface that caused the communication failure, packets are being discarded at the null interface. Review the static routing configuration.
5. If the routing information obtained by the Device either does not contain the routing information about the interface that caused the communication failure or contains an incorrect address of the interface's next hop, see *4.5 Unicast routing communication failures*.

(7) Checking the setting of IPv6 address distribution information

If communication between the Device and a terminal that is directly connected to the Device is impossible, address information might not have been correctly distributed by RA or the DHCPv6 relay agent.

- RA

  The following shows the procedure for checking whether the RA configuration is correct.

  1. Log in to the Device.
  2. Execute the `show ipv6 routers` command to check the RA information for the Device. For details about the information distributed by the RA, see the *Configuration Guide*.

- DHCPv6 relay agent

  If you are using a DHCPv6 relay agent, see *4.2.2 The DHCPv6 relay agent cannot allocate IPv6 addresses*.

(8) Checking for discarded packets

Packets might have been discarded by filters, QoS, uRPF, or policy-based routing

- Filter, QoS, or uRPF

  For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.

- Policy-based routing

  For details about how to check this situation and the action to be taken, see *4.3.1 Checking for policy-based routing communication failures*.

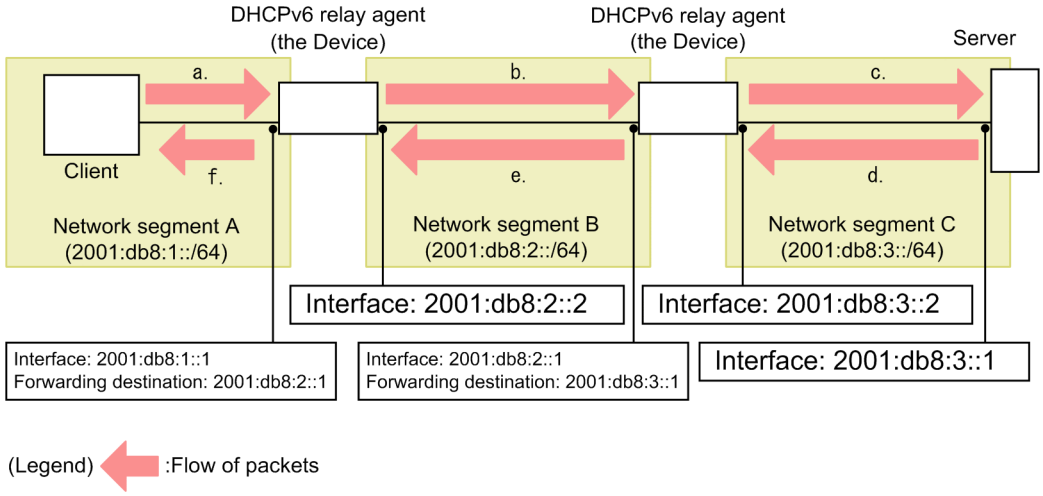
4.2.2 The DHCPv6 relay agent cannot allocate IPv6 addresses

The following shows the five possible causes of a communication problem with the DHCPv6 relay agent:

- The configuration of the DHCPv6 relay agent
- The configuration of the DHCPv6 server (hereinafter, the server)
- The configuration of the DHCPv6 client (hereinafter, the client)
- The RA configuration
- An IPv6 network communication failure

This section uses the following network configuration as an example to explain the procedure for isolating the fault location and cause of the failure.

Figure 4-5: Example network configuration for the DHCPv6 relay agent



Items to be checked (Indication in the figure)	Value in the packet			
	Destination IPv6 address	Source IPv6 address	Destination UDP port number	Source UDP port number
a.	ff02::1:2	Client link-local address	547	Optional
b.	2001:db8:2::1	2001:db8:2::2	547	546
c.	2001:db8:3::1	2001:db8:3::2	547	546
d.	2001:db8:3::2	2001:db8:3::1	547	Optional

Items to be checked (Indication in the figure)	Value in the packet			
	Destination IPv6 address	Source IPv6 address	Destination UDP port number	Source UDP port number
e.	2001:db8:2::2	2001:db8:2::1	547	547
f.	Client link-local address	2001:db8:1::1	546	547

(1) Checking the status and statistics of the DHCPv6 relay agent

Check the status and statistics of the DHCPv6 relay agent and isolate the cause by following the failure-analysis method described in the following table.

Table 4-2: DHCPv6 relay agent failure-analysis method

No.	Items to be checked and commands	Action
1	Check whether there is a count for the number of packets received from the client at the interface on the client side (`Receive Packets` under `DHCPv6 Request Packets Count`). • `show ipv6 dhcp relay statistics`	If there is a count, go to step 2.
		Otherwise, check the following: • See *(2) Checking the configuration of the DHCPv6 relay agent* to check the forwarding destination of the DHCPv6 packets. • If the client is directly connected, check the RA setting. For the procedure, see *(3) Checking the RA settings*. • Check the network segment on the client side of the Device (the item marked *a* in the figure). For the procedure, see *4.2.1 Unable to communicate, or communication is interrupted*. • Follow the procedure for isolating the cause of a failure on the target client to check the configuration.
2	Check whether there is a count for the number of packets discarded because the number of hops exceeded the maximum number (`Hops Over` under `DHCPv6 Error Packets Count`). • `show ipv6 dhcp relay statistics`	If there is, see *(2) Checking the configuration of the DHCPv6 relay agent* to check the maximum number of hops of the DHCPv6 packets.
		Otherwise, go to step 3.
3	Check if there is a count for the number of packets successfully sent to the server (forwarding destination) at the interface on the client side (`Send Packets` under `DHCPv6 Request Packets Count`). • `show ipv6 dhcp relay statistics`	If there is, go to step 4.
		Otherwise, check the following: • See *(2) Checking the configuration of the DHCPv6 relay agent* to check whether the forwarding destination of the DHCPv6 packets is correct. • Check the items marked *b* and *c* in the figure. For the procedure, see *4.2.1 Unable to communicate, or communication is interrupted*.

No.	Items to be checked and commands	Action
4	Check whether there is a count for the number of packets received from the server (`Receive Packets` of `DHCPv6 Reply Packets Count`). • `show ipv6 dhcp relay statistics`	If there is, go to step 5.
		Otherwise, check the following: • See *(2) Checking the configuration of the DHCPv6 relay agent* to check whether the forwarding destination of the DHCPv6 packets is correct. • Check the items marked *d* and *e* in the figure. For the procedure, see *4.2.1 Unable to communicate, or communication is interrupted*. • Follow the procedure for isolating the cause of the failure on the target server to check the configuration, and check if the network segment is the same.
5	Check whether there is a count for the number of packets successfully sent to the client (`Send Packets` under `DHCPv6 Reply Packets Count`). • `show ipv6 dhcp relay statistics`	If there is, check the following: • If the client is directly connected, check the RA setting. For the procedure, see *(3) Checking the RA settings*. • Follow the procedure for isolating the cause of the failure on the target server to check if there are enough IPv6 addresses to assign. • Follow the procedure for isolating the cause of the failure on the target client to check the configuration.
		If there is no such count, go to step 6.
6	Check whether there is a count for the number of packets discarded because the number of binding (IA_PD) entries exceeded the maximum (`Lease Prefix Over` of `DHCPv6 Error Packets Count`). • `show ipv6 dhcp relay statistics`	If there is, review the network configuration so that the number of addresses to be assigned (IA_PD) does not exceed the maximum number for the Device.
		Otherwise, check the following: • Check the client network segment of the Device (the item marked *f* in the figure). For the procedure, see *4.2.1 Unable to communicate, or communication is interrupted*. • Follow the procedure for isolating the cause of the failure in the target client to check the configuration.

(2) Checking the configuration of the DHCPv6 relay agent

It is possible that IP addresses cannot be assigned to clients because the resources on the DHCPv6 relay agents are configured incorrectly. The following describes the procedure for checking the configuration of the DHCPv6 relay agent.

1. Make sure that the forwarding destination of DHCPv6 packets is set (`ipv6 dhcp relay destination` configuration command) for the client IPv6 interface.
2. Make sure that the network configuration matches the IPv6 address or IPv6 interface of the server or DHCPv6 relay agent that is set (`ipv6 dhcp relay destination` configuration command) as the forwarding destination of DHCPv6 packets.
3. Check whether the maximum number of hops of DHCPv6 packets is set (`ipv6 dhcp relay maximum-hop-count` configuration command) to a value larger than the number of DHCPv6 relay agents between the Device and the clients.

(3) Checking the RA settings

If clients are directly connected, it is possible that IPv6 addresses cannot be assigned to clients because the resources on the RA are configured incorrectly. The procedure for checking the RA

configuration is as follows:

1. Check whether the client IPv6 interface has been set so that the automatic address management flag is enabled (`ipv6 nd managed-config-flag` configuration command). The automatic address management setting flag indicates that an IPv6 address on a terminal is to be automatically set by a method other than the automatic address setting by RA. This method can include DHCPv6.

   To acquire by DHCPv6 information other than the IPv6 address, make sure that the configuration mentioned above is not set.

2. Check whether the client IPv6 interface is set so that non-address information setting flag is enabled (`ipv6 nd other-config-flag` configuration command). The non-address information setting flag indicates that a terminal is to automatically acquire information, except for the IPv6 address, by a method other than the RA. This method can include DHCPv6.

   To assign by DHCPv6 only the IPv6 address, make sure that the configuration mentioned above is not set.

(4) Checking when DHCPv6 relay agent and IPv6 multicast are concurrently operated

For the Device to concurrently use DHCPv6 relay agents and IPv6 multicast, make sure that each server is individually set as the forwarding destination of the DHCPv6 relay agents. If all servers are specified as the forwarding destination of DHCPv6 packets, check the following:

- Whether the partner router of the Device has been set so the Device becomes the DR of the IPv6 multicast, by setting the maximum value to the link-local address of the IPv6 interface to which the Device is connected

  For details about the configuration, see the router documentation.

- Whether IPv6 multicasting is set on the Device and the partner router so that the partner router becomes the rendezvous point

4.3 Policy-based routing communication failures

4.3.1 Checking for policy-based routing communication failures

One of the possible causes of a communication problem on a network on which the Device is used is packets not being relayed as expected or being discarded due to policy-based routing.

The following describes how to check whether packets have been relayed to another interface or discarded by the policy-based routing:

1. Execute the `show access-filter` command to check the filter condition of the access list specified for the policy-based routing, and the number of packets that meet the filter criteria.
2. If the number of packets checked in step 1 matches the number of packets that could not be transmitted, the packets might not have been relayed as expected or might have been discarded due to the policy-based routing list that is set as the filter condition.
3. Check whether the policy-based routing configuration is correct.

4.3.2 Policy-based routing problems

When policy-based routing is in use, if packets are not relayed to the next specified hop, isolate the cause by following the failure-analysis method described in the table below.

Also, a problem might have occurred due to the filter that is specified for the policy-based routing list. In addition to the following procedures, see *6.1.1 Filter problems*.

Table 4-3: Failure-analysis method for policy-based routing

No.	Items to be checked and commands	Action
1	Use `Matched packets` to check the number of packets that meet the conditions of the filter that is specified for the policy-based routing list. • `show access-filter`	If the number of packets that could not be transmitted differs from the value of `Matched packets`, either of the following may be the cause: The packets are not subject to policy-based routing For details about packets that are the target of policy-based routing, see the *Configuration Guide*. The detection condition of the filter is incorrect Revise the filter settings.
		If the number of packets that could not be transmitted is the same as the value of `Matched packets`, go to step 2.
2	Check the next hop that is currently in use for policy-based routing and for which `*>` is displayed. • `show ip cache policy` • `show ipv6 cache policy`	If `*>` is not displayed, the next hop selection may be suppressed. Go to step 3.
		If `*>` is displayed for the default operation, go to step 4.
		If `*>` is displayed for an unexpected next hop, go to step 4.
		If `*>` is displayed for the expected next hop, go to step 5.
3	Check the start and end dates and times for the suppression of the next hop selection of the policy-based routing. • `show ip cache policy` • `show ipv6 cache policy`	If `-` is displayed for only `End Time`, one of the following operations might be in effect to suppress the next hop selection. • Relay to an unexpected next hop • Relay according to the routing protocol • Discard Wait for suppression of next hop selection to finish.
		If `Start Time` and `End Time` are both `-`, or the date and time are displayed, go to step 6.

No.	Items to be checked and commands	Action
4	Check the interface status of the sending destination for the policy-based routing. • `show ip interface` • `show ipv6 interface`	If the status of the sending destination interface of the expected next hop is not `Up`, one of the following operations might be in effect: • Relay to an unexpected next hop • Relay according to the routing protocol • Discard Put the sending destination interface in the `Up` status.
		If the status of the sending destination interface of the expected next hop is `Up`, go to step 5.
5	Check whether a network communication failure has occurred at the sending destination interface of the expected next hop.	A communication failure might have occurred. For details about how to check this situation, see *4.1 IPv4 network communication failures* and *4.2 IPv6 network communication failures*. If a communication failure has occurred, follow the instructions in the sections referenced above. If the instructions in the referenced sections do not solve the problem, go to step 6.
		If a communication failure has not occurred, go to step 6.

6	Check whether policy-based routing has not been set up due to a resource shortage.
	• Check the system message output (message type: PRU, message identifier: 3f000002).
	`show logging`
	• Check the number of entries being used and the maximum possible number of entries.
	`show pru resources`
		If the system message mentioned above has been output, or if `Shared resources Used/Max` shows that the number of entries in use matches the maximum possible number of entries, policy-based routing might not have been set up. Follow the instruction in *5.1 When a resource shortage occurs in shared memory*.
		If the instruction in the referenced section does not solve the problem, go to step 7.

		If the system message mentioned above has not been output, or if `Shared resources Used/Max` shows that the number of entries in use is less than the maximum possible number of entries, go to step 7.
7	Check whether packets are being discarded by uRPF.	uRPF might be discarding packets. For details about how to check this situation and the action to be taken, see *8.1.3 Checking for packets discarded by uRPF*.
		If no packets are being discarded by uRPF, go to step 8.
8	Check whether frames are being discarded by QoS.	QoS might be discarding frames. For details about how to check this situation and the action to be taken, see *8.1.2 Checking for packets discarded by QoS*.

4.4 VRRP communication failures

4.4.1 Unable to communicate in a VRRP configuration

If communication is impossible in a VRRP configuration, isolate the cause of the problem by following the failure-analysis method described in the following table.

Table 4-4: Failure-analysis method for VRRF

No.	Items to be checked and commands	Action
1	On the Device and the remote devices that make up the virtual router, check the status of the virtual router, and make sure that only one device is the master router and that the others are backup routers. • `show vrrpstatus`	If the status of the virtual router is correct, go to step 2.
		If the status of the virtual router is incorrect, go to step 3.
2	If terminals are connected directly to the virtual router (not via other routers), make sure that the virtual IP address of the virtual router is set as the default gateway in the network settings of the terminals.	• Check the routing information of the devices on the communication path that includes the Device. • In the network setting of each terminal that is connected directly to the virtual router, if the virtual IP address of the virtual router is not set as the default gateway, set it as the default gateway.
		If no problem exists with the routing information of the devices on the communication path, go to step 5.
3	Make sure that the status of the virtual router is not `INITIAL`. • `show vrrpstatus detail`	If the status of the virtual router is `INITIAL`, check the following: • If the current priority is not 0, resolve the cause of the virtual router being disabled, which is displayed in `Admin State`. (For details about the cause of the virtual router being disabled, see the *Operation Command Reference*.)
		If the status of the virtual router is not `INITIAL`, go to step 4.
4	Make sure that the interface on which the virtual router is set is operating. • `show port` • `show channel-group`	If the status of the interface is `down`, see *3. Troubleshooting Network Interfaces*.
		If the status of the interface is `up`, go to step 5.
5	Make sure that Group Switching is set. • `show vrrpstatus detail`	If Group Switching is set, go to step 6.
		If Group Switching is not set, go to step 7.
6	Make sure that both the VRID for the primary virtual router in use and the TPID of the VLAN Tag are the same among the devices that make up the virtual routers. • `show vrrpstatus` • `show ip interface`	If the VRID for the primary virtual router and the TPID of the VLAN Tag differ among the devices that make up the virtual routers, more than one router will become a master router. Among the devices that make up the virtual routers, use the same settings.
		If the VRID for the primary virtual router and the TPID of the VLAN Tag are the same among the devices that make up the virtual routers, go to step 7. Note that items 7 and onward apply only to the primary virtual router.

No.	Items to be checked and commands	Action
7	Check communication between the routers that make up the virtual router by using the actual IPv4 or IPv6 addresses. • `ping` • `ping ipv6`	If communication between the routers that make up the virtual router by using the actual IPv4 or IPv6 addresses is impossible, see *4.1 IPv4 network communication failures* or *4.2 IPv6 network communication failures*.
		If communication between the routers that make up the virtual router by using the actual IPv4 or IPv6 addresses is possible, go to step 8.
8	Check whether advertisement packets are being discarded by the filters or QoS.	For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*. If no such filters or QoS setting is applied, check the operating status of the remote devices that make up the same virtual router.
		If no advertisement packets are being discarded, go to step 9.
9	After the advertisement packet sending interval, execute the following command to check whether the statistics of the advertisement packets increase. • `show vrrpstatus statistics`	• In the statistics, if the value of <*number of packets*> `with bad advertisement interval` increases, make sure that the setting for the advertisement packet sending interval is the same on the Device and on the remote devices. • In the statistics, if the value of <*number of packets*> `with authentication failed` increases, make sure that the authentication password settings are the same on the Device and on the remote device. • In the statistics, if the value of <*number of packets*> `with bad ip ttl` increases, make sure that no other router exists between the Device and the remote device. • In the statistics, if the value of <*number of packets*> `with bad ipv6 hoplimit` increases, make sure that no other router exists between the Device and the remote device. • In the statistics, if the value of <*number of packets*> `with bad ip address list` increases, make sure that the virtual IP address settings are the same. • In the statistics, if the value of <*number of packets*> `with bad ipv6 address` increases, make sure that the virtual IP address settings and the VRRP operating mode are the same. • In the statistics, if the value of <*number of packets*> `with bad authentication type` increases, check whether an authentication password is set on the Device and on the remote device. • In the statistics, if the value of <*number of packets*> `with packet length error` increases, make sure that the setting of the VRRP operating mode is the same on the Device and on the remote device. • In the statistics, if the value of <*number of packets*> `with invalid type` increases, make sure that the setting of the VRRP operating mode is the same on the Device and on the remote device.
		If advertisement packets are received correctly, check the remote device. If advertisement packets are not received, go to step 10.

No.	Items to be checked and commands	Action

10	Check the load on the Ethernet network and on the device.
	• Check the statistics for the Ethernet network to which the remote devices that make up the same virtual router are connected.
	`show interfaces`
	• Check the CPU usage.
	`show cpu bcu`
		For the Ethernet network to which the remote devices that make up the same virtual router are connected, you might find that the `Input rate` and `Output rate` values are large and that the line load is high. In addition, the CPU usage displayed might be high. In such a case, take the following action:
		• If a network loop has occurred, revise the loop configuration.
		• Use the `vrrp timers advertise` configuration command to set a longer sending interval for advertisement packets.
		• Use the `vrrp preempt delay` configuration command to set the automatic switchback suppression time.

		If the load of the Ethernet network is low, check the operating status of the remote devices that make up the same virtual router.

4.5 Unicast routing communication failures

4.5.1 No static routing information exists

(1) No static routing information exists

If the routing information obtained by the Device does not include static routing information, isolate the cause of the problem by following the failure-analysis method described in the table below.

If IPv6 static routing information automatically generated by a DHCPv6 relay agent does not exist, follow the failure-analysis method in *(2) No IPv6 static routing information automatically generated by a DHCPv6 relay agent exists*.

If VRF is in use, and the `maximum routes` or `ipv6 maximum routes` configuration command is used to set the upper limit of the routes, first follow *4.5.5 No unicast routing information in VRF exists*.

Table 4-5: Failure-analysis method for static routing

No.	Items to be checked and commands	Action
1	Check the configuration to see if the static route settings are correct.	If the configuration is correct, go to step 2.
		If the configuration is incorrect, revise it.
2	Check whether routing information that resolves the next hop address of the static route exists. • `show ip route` • `show ipv6 route`	If routing information that resolves the next hop address exists and the dynamic monitoring functionality is in use, go to step 3.
		If no routing information that resolves the next hop address exists, perform the failure analysis for the protocol used for learning the routing information.
3	Check static route gateway information. • `show ip static gateway` • `show ipv6 static gateway`	If there is a count for consecutive successful pollings, wait for reachability to the gateway to become stable.
		If the count for consecutive successful polling commands remains 0, go to step 4.
4	Check whether ICMP or ICMPv6 packets are being discarded by the filters or QoS.	For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.

(2) No IPv6 static routing information automatically generated by a DHCPv6 relay agent exists

If the routing information obtained by the Device does not include static routing information automatically generated by a DHCPv6 relay agent, isolate the cause of the problem by following the failure-analysis method described in the following table.

Table 4-6: Failure-analysis method for DHCPv6 relay agent

No.	Items to be checked and commands	Action
1	Check the binding (IA_PD) of the DHCPv6 relay agent. • `show ipv6 dhcp relay binding`	If the binding (IA_PD) has been learned, go to step 2.
		If the binding (IA_PD) has not been learned, see *4.2.2 The DHCPv6 relay agent cannot allocate IPv6 addresses*.

No.	Items to be checked and commands	Action
2	Check the configuration to see if the DHCPv6 relay agent settings (`ipv6 dhcp relay static-route-setting`) are correct.	If no setting to automatically generate an IPv6 static route by a DHCPv6 relay agent exists, revise the configuration.

4.5.2 No RIP or RIPng routing information exists

If the routing information obtained by the Device does not include RIP or RIPng routing information, isolate the cause of the problem by following the failure-analysis method described in the table below.

If VRF is in use, and the `maximum routes` or `ipv6 maximum routes` configuration command is used to set the upper limit of the routes, first follow *4.5.5 No unicast routing information in VRF exists*.

Table 4-7: Failure-analysis method for RIP or RIPng

No.	Items to be checked and commands	Action
1	Check the RIP or RIPng neighbor information. • `show ip rip neighbor` • `show ipv6 rip neighbor`	If the interface of the neighboring router is not displayed, go to step 2.
		If the interface of the neighboring router is displayed, go to step 3.
2	Check the configuration to see if the RIP or RIPng settings for the operating interface or network and for the RIP version are correct.	If the configuration is correct, go to step 3.
		If the configuration is incorrect, revise it.
3	Check whether RIP or RIPng packets are being discarded by the filters or QoS.	For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.
		If no packets are being discarded, check whether the neighboring router is advertising the RIP or RIPng route.

4.5.3 No OSPF or OSPFv3 routing information exists

If the routing information obtained by the Device does not include OSPF or OSPFv3 routing information, isolate the cause of the problem by following the failure-analysis method described in the table below.

If VRF is in use, and the `maximum routes` or `ipv6 maximum routes` configuration command is used to set the upper limit of the routes, first follow *4.5.5 No unicast routing information in VRF exists*.

Table 4-8: Failure-analysis method for OSPF or OSPFv3

No.	Items to be checked and commands	Action
1	Check the interface status of OSPF or OSPFv3. • `show ip ospf interface` <*ip address*> • `show ipv6 ospf interface` <*interface type*> <*interface number*>	If the interface status is `BackupDR` or `DR Other`, go to step 2.
		If the interface status is `DR` or `P to P`, go to step 3.
2	Check the status of the neighboring router that has the `DR` status in `Neighbor List`.	If the status of that neighboring router is other than `Full`, go to step 4.
		If the status of that neighboring router is `Full`, go to step 5.

No.	Items to be checked and commands	Action
3	Check the status of every neighboring router in `Neighbor List`.	If the status of any neighboring router is other than `Full`, go to step 4.
		If the status of every neighboring router is `Full`, go to step 5.
4	Check the configuration to see if the OSPF or OSPFv3 settings for the area, intervals, and OSPF authentication are correct.	If the configuration is correct, go to step 5.
		If the configuration is incorrect, revise it.
5	Check the route that has learned the OSPF or OSPFv3 route. • `show ip route all-routes` • `show ipv6 route all-routes`	If the route is `InActive`, go to step 6.
		If the route does not exist, check whether a neighboring router is advertising the OSPF or OSPFv3 route.
6	Check whether OSPF or OSPFv3 packets are being discarded by the filters or QoS.	For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.
		If no packets are being discarded, check whether a neighboring router is advertising the OSPF or OSPFv3 route.

4.5.4 No BGP4 or BGP4+ routing information exists

If the routing information obtained by the Device does not include BGP4 or BGP4+ routing information, isolate the cause of the problem by following the failure-analysis method described in the table below.

If VRF is in use, and the `maximum routes` or `ipv6 maximum routes` configuration command is used to set the upper limit of the routes, first follow *4.5.5 No unicast routing information in VRF exists*.

Table 4-9: Failure-analysis method for BGP4 or BGP4+

No.	Items to be checked and commands	Action
1	Check the BGP4 or BGP4+ peer status. • `show ip bgp neighbors` • `show ipv6 bgp neighbors`	If the peer status is other than `Established`, go to step 2.
		If the peer status is `Established`, go to step 3.
2	Check the configuration to see if the BGP4 or BGP4+ settings for the AS number, peer address, and authentication are correct.	If the configuration is correct, go to step 3.
		If the configuration is incorrect, revise it.
3	Check whether a BGP4 or BGP4+ route has been learned. • `show ip bgp received-routes` • `show ipv6 bgp received-routes`	If such a route exists but its status is not `active`, go to step 4.
		If no such route exists, go to step 5.
4	Check whether routing information that resolves the next hop address of the BGP4 or BGP4+ route exists. • `show ip route` • `show ipv6 route`	If routing information that resolves the next hop address exists, go to step 5.

No.	Items to be checked and commands	Action
		If no routing information that resolves the next hop address exists, perform the failure analysis for the protocol used for learning the routing information.
5	Check whether BGP4 or BGP4+ packets are being discarded by the filters or QoS.	For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.
		If no packets are being discarded, check whether a neighboring router is advertising the BGP4 or BGP4+ route.

4.5.5 No unicast routing information in VRF exists

If the routing information of each protocol cannot be found in the routing information obtained by the Device, isolate the cause of the problem by following the failure-analysis method described in the following table.

Table 4-10: Failure-analysis method for VRF

No.	Items to be checked and commands	Action
1	Check whether the number of routes in VRF is equal to or larger than the maximum value specified in the configuration. • `show ip vrf` • `show ipv6 vrf`	If the number of routes is equal to or larger than the maximum value, go to step 2.
		If the number of routes is less than the maximum value, perform the failure analysis for the protocol used for the route that does not exist. • RIP or RIPng *4.5.2 No RIP or RIPng routing information exists* • OSPF or OSPFv3 *4.5.3 No OSPF or OSPFv3 routing information exists* • BGP4 or BGP4+ *4.5.4 No BGP4 or BGP4+ routing information exists*
2	Check the maximum number of routes in VRF specified in the configuration.	Either increase the maximum number, or reduce the number of specified routes by, for example, aggregating routes.

4.6 Multicast routing communication failures

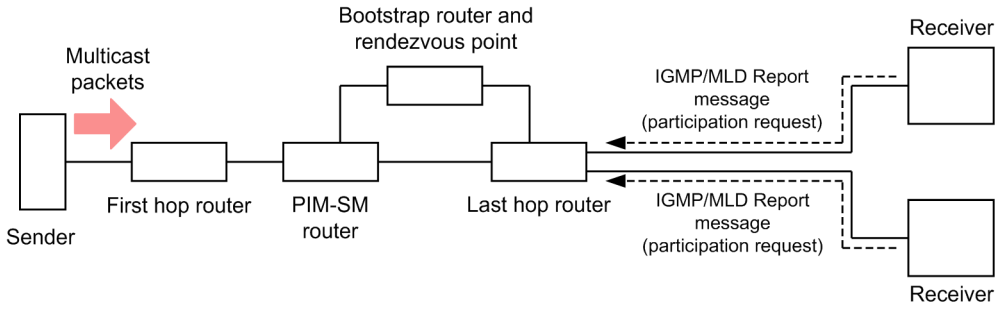
This section describes the action to be taken when an IPv4 or IPv6 multicast communication failure occurs on the Device.

4.6.1 Unable to perform multicast communication on a PIM-SM network

If multicast forwarding is impossible in a PIM-SM network configuration, isolate the cause of the problem by following the failure-analysis method described below.

The following figure shows an example of a PIM-SM network.

Figure 4-6: PIM-SM network example



The role of each router in the figure is as follows:

- Bootstrap router: The router that sends the information about the rendezvous point
- Rendezvous point: The router that relays a multicast packet that has no relay destination determined toward the receiving side
- First hop router: The router that connects directly to the sending side
- Last hop router: The router that connects directly to the receiving side
- PIM-SM router: A router other than one described above where PIM-SM is operating

(1) Common items to be checked

The following table shows the items to be checked for all Devices in a PIM-SM network configuration in common.

Table 4-11: Common items to be checked

No.	Items to be checked and commands	Action
1	Make sure that the IPv4 or IPv6 multicast routing program is running. • `show ip pim interface` • `show ipv6 pim interface`	If the IPv4 or IPv6 multicast routing program is not running, go to step 2.
		If the IPv4 or IPv6 multicast routing program is running, go to step 6.
2	Check the configuration to confirm that the setting that enables the multicast routing functionality (`ip multicast routing` or `ipv6 multicast routing`) has been made. • `show running-config`	If the IPv4 multicast routing functionality is enabled, go to step 3.
		If the IPv6 multicast routing functionality is enabled, go to step 4.

No.	Items to be checked and commands	Action
		If no multicast routing functionality is enabled, revise the configuration.
3	When using IPv4 multicast, check the configuration to confirm that multihoming is not set for the target interface. • `show running-config`	If multihoming is not set, go to step 5.
		Multihoming is not supported. If multihoming is set, revise the configuration.
4	When using IPv6 multicast, check the configuration to confirm that an IPv6 address is set for the loopback interface. • `show running-config`	If an IPv6 address is set for the loopback interface, go to step 5.
		If no IPv6 address is set for the loopback interface, revise the configuration.
5	Make sure that PIM-SM is running on 1 or more interfaces. • `show ip pim interface` • `show ipv6 pim interface`	If PIM-SM is running, go to step 6.
		If PIM-SM is not running, revise the configuration so that PIM-SM runs on at least 1 interface.
6	Check the configuration to see if the route distribution pattern for which multicast is available is set. • `show running-config`	If the route distribution pattern for which multicast is available is set, go to step 7.
		If the route distribution pattern for which multicast is available is not set, revise the configuration. For details about how to change the route distribution pattern, see the *Configuration Command Reference*. After changing the route distribution pattern, go to step 22.
7	Check whether protocol or multicast packets are being discarded by the filters or QoS at the interface on which PIM-SM, IGMP, and MLD are running.	For details about how to check this situation and the action to be taken see *8.1 Checking for discarded packets*.
		If no packets are being discarded, go to step 8.
8	Check whether a unicast route to the sender, rendezvous point, and bootstrap router exists. • `show ip route` • `show ipv6 route`	If a unicast route exists, go to step 9.
		If no unicast route exists, see *4.5 Unicast routing communication failures*.
9	Make sure that PIM-SM is running on the interface that is connected to the next hop address for the sending side, rendezvous point, and bootstrap router. • `show ip pim interface` • `show ipv6 pim interface`	If PIM-SM is running, go to step 10.
		If PIM-SM is not running, revise the configuration so that PIM-SM runs on the interface that is connected to the next hop address for the sending side, rendezvous point, and bootstrap router.

No.	Items to be checked and commands	Action
10	Check the PIM-SM neighbor information. • `show ip pim neighbor` • `show ipv6 pim neighbor`	If the next hops of the routes checked in step 8 are all displayed as neighboring routers, go to step 11.
		If any of the next hops of the routes checked in step 8 is not displayed as a neighboring router, check the configuration of the neighboring router that is not displayed.
11	Check the configuration to make sure that the address range used for PIM-SSM does not include the forwarding target group address. • `show running-config`	If the address range used for PIM-SSM does not include the forwarding target group address, go to step 12.
		If the address range used for PIM-SSM includes the forwarding target group address, revise the configuration.
12	If the rendezvous point for the forwarding target group address is not a static rendezvous point, make sure that the bootstrap router has been determined. • `show ip pim bsr` • `show ipv6 pim bsr`	If the bootstrap router has been determined, go to step 13.
		If no bootstrap router has been determined, check whether a unicast route to the bootstrap router exists. If no unicast route exists, see *4.5 Unicast routing communication failures*. If a unicast route exists, check the bootstrap router settings. If the Device is being used as the bootstrap router, see *(2) Items to be checked for the bootstrap router*.
13	Make sure that the rendezvous point has been determined. • `show ip pim rp-mapping` • `show ipv6 pim rp-mapping`	If the rendezvous point has been determined, go to step 14.
		If no rendezvous point has been determined, check whether a unicast route to the rendezvous point exists. If no unicast route exists, see *4.5 Unicast routing communication failures*. If a unicast route exists, check the rendezvous point settings. If the Device is being used as the rendezvous point, see *(3) Items to be checked for the rendezvous point*.
14	Make sure that the rendezvous point group addresses contain the forwarding target group address. • `show ip pim rp-mapping` • `show ipv6 pim rp-mapping`	If the rendezvous point group addresses contain the forwarding target group address, go to step 15.
		If the rendezvous point group addresses do not contain the forwarding target group address, check the rendezvous point router settings. If the Device is being used as the rendezvous point, see *(3) Items to be checked for the rendezvous point*.
15	Check whether the rendezvous points for the forwarding target group addresses are the same for all Devices in the network. • `show ip pim rp-hash` • `show ipv6 pim rp-hash`	If the rendezvous points are the same, go to step 16.
		If the rendezvous points differ, check the rendezvous point settings.

No.	Items to be checked and commands	Action
16	Check whether the rendezvous point selection algorithms are the same for all Devices in the network. • `show running-config`	If the rendezvous point selection algorithms are the same, go to step 17.
		If rendezvous point selection algorithms differ, revise the configuration.
17	Make sure that multicast forwarding entries exist. • `show ip mcache` • `show ipv6 mcache`	If multicast forwarding entries exist, go to step 18.
		If no multicast forwarding entries exist, make sure that multicast packets have reached the upstream interface. If multicast packets have not reached the upstream interface, check the settings of the sender or the upstream router.
18	Check whether the number of multicast relay entries has reached the maximum (the value of `ip pim mcache-limit` or `ipv6 pim mcache-limit`). • `show ip mcache` • `show ipv6 mcache`	If no warning is displayed, go to step 19.
		If a warning is displayed, the number of multicast relay entries has reached the maximum. Revise the network configuration and operate within the limits. If more negative cache entries than were expected are generated, check whether a terminal is sending unnecessary multicast packets.
19	Make sure that multicast routing information exists. • `show ip mroute` • `show ipv6 mroute`	If multicast routing information exists, go to step 20.
		If no multicast routing information exists, check the downstream router settings.
20	Check whether the number of multicast routing information items has reached the maximum (the value of `ip pim mroute-limit` or `ipv6 pim mroute-limit`). • `show ip mroute` • `show ipv6 mroute`	If no warning is displayed, go to step 21.
		If a warning is displayed, the number of multicast routing information items has reached the maximum. Revise the network configuration and operate within the limits.
21	Check whether a multicast packet is received that has a TTL value of 1 (when IPv4 multicast is in use) or a hop limit value of 1 (when IPv6 multicast is in use). • `show tcpdump`	If the TTL value or the hop limit value is not 1, go to step 22.
		If the TTL value or the hop limit value is 1, the Device does not relay the multicast packet. Revise the settings of the sender.
22	Check for a system message# that indicates that the number of multicast relay entries has reached the limit. • `show logging`	If no such system message is displayed, go to step 23.

No.	Items to be checked and commands	Action
		If such a system message is displayed, the number of multicast relay entries has reached the limit. After the limit is reached, no multicast relay entry can be set. We recommend that you not operate while the limit has been reached. Revise the network configuration and operate within the limits. After reviewing the network configuration, execute either the `restart ipv4-multicast` command or the `restart ipv6-multicast` command to reset the multicast relay entries.
23	Check for a system message that indicates that the total number of downstream interfaces of the multicast relay entries has reached the limit (message type: PRU, message identifier: 41023002). • `show logging`	If such a system message is displayed, the total number of downstream interfaces of the multicast relay entries has reached the limit. After the limit is reached, no downstream interface can be set. We recommend that you not operate while the limit has been reached. Revise the network configuration and operate within the limits. Note that the total number of downstream interfaces is the total of both the IPv4 multicast entries and the IPv6 multicast entries. After reviewing the network configuration, execute both the `restart ipv4-multicast` command and the `restart ipv6-multicast` command to reset the multicast relay entries.

#

When the number of IPv4 multicast relay entries reaches the limit, a system message with message type PRU and message identifier 41021002 is displayed, and when the number of IPv6 multicast relay entries reaches the limit, a system message with message type PRU and message identifier 41022002 is displayed.

(2) Items to be checked for the bootstrap router

The following table shows the items to be checked if the Device is being used as a bootstrap router in a PIM-SM network configuration.

Table 4-12: Items to be checked for the bootstrap router

No.	Items to be checked and commands	Action
1	Make sure that the Device is a bootstrap router candidate. • `show ip pim bsr` • `show ipv6 pim bsr`	If the Device is not a bootstrap router candidate, go to step 2.
		If the Device is a bootstrap router candidate, go to step 4.
2	Check the configuration to see if an IPv4 address (if IPv4 multicast is in use) or an IPv6 address (if IPv6 multicast is in use) is set for the loopback interface. • `show running-config`	If an IPv4 or IPv6 address is set for the loopback interface, go to step 3.
		If neither an IPv4 address nor an IPv6 address is set for the loopback interface, revise the configuration.
3	Check the configuration to see if either the loopback interface number (when using IPv4 multicast) or the IPv6 address of the loopback interface (when using IPv6 multicast) is specified as a bootstrap router candidate. • `show running-config`	If the bootstrap router candidate setting is correct, go to step 4.
		If the bootstrap router candidate setting is incorrect, revise the configuration.

No.	Items to be checked and commands	Action
4	Make sure that the Device is a bootstrap router. • `show ip pim bsr` • `show ipv6 pim bsr`	If the Device is not a bootstrap router, check the priority of each other bootstrap router candidate. A larger value represents a higher priority. If priorities are the same, the bootstrap router candidate with the highest IPv4 or IPv6 address is used as the bootstrap router.

(3) Items to be checked for the rendezvous point

The following table shows the items to be checked when the Device is in use as a rendezvous point in a PIM-SM network configuration.

Table 4-13: Items to be checked for the rendezvous point

No.	Items to be checked and commands	Action
1	Make sure that the Device is a rendezvous point candidate for the forwarding target group address. • `show ip pim rp-mapping` • `show ipv6 pim rp-mapping`	If the Device is not a rendezvous point candidate, go to step 2.
		If the Device is a rendezvous point candidate, go to step 4.
2	Check the configuration to see if an IPv4 address (if IPv4 multicast is in use) or an IPv6 address (if IPv6 multicast is in use) is set for the loopback interface. • `show running-config`	If an IPv4 or IPv6 address is set for the loopback interface, go to step 3.
		If neither an IPv4 address nor an IPv6 address is set for the loopback interface, revise the configuration.
3	Check the configuration to see if either the loopback interface number (when using IPv4 multicast) or the IPv6 address of the loopback interface (when using IPv6 multicast) is specified as a rendezvous point candidate. • `show running-config`	If the rendezvous point candidate setting is correct, go to step 4.
		If the rendezvous point candidate setting is incorrect, revise the configuration.
4	Make sure that the Device is the rendezvous point for the forwarding target group address. • `show ip pim rp-hash` • `show ipv6 pim rp-hash`	If the Device is not the rendezvous point, check the priority of each other rendezvous point candidate. A smaller value represents a higher priority. If the priorities of more than one rendezvous point candidate are the same, the candidates are distributed by group address according to the protocol specification, and thus the Device may not operate as the rendezvous point for the target multicast group. If you want to use the Device as the rendezvous point, set a higher priority for the Device than the other rendezvous point candidates.

(4) Items to be checked for the last hop router

The following table shows the items to be checked when the Device is used as a last hop router in a PIM-SM network configuration.

Table 4-14: Items to be checked for the last hop router

No.	Items to be checked and commands	Action
1	Make sure that IGMP or MLD is running on the interface connected to the receiver. • `show ip igmp interface` • `show ipv6 mld interface`	If IGMP or MLD is not running, revise the configuration so that IGMP or MLD runs.
2	Make sure that the receivers are participating in the forwarding target multicast group via IGMP or MLD. • `show ip igmp group` • `show ipv6 mld group`	If a receiver is not participating in the forwarding target multicast group, check the receiver settings.
3	If an interface is participating in the forwarding target multicast group, make sure that the Device is the DR. • `show ip pim interface` • `show ipv6 pim interface`	If the Device is not the DR, check the DR of the forwarding target interface.
4	If an interface is using the static group participation functionality, make sure that the Device is the DR. • `show ip pim interface` • `show ipv6 pim interface`	If the Device is not the DR, enable the static group participation functionality for the device that is the DR of the forwarding target interface.
5	Check whether any anomaly has been detected on any interface. • `show ip igmp interface` • `show ipv6 mld interface`	Make sure that no warning information is displayed for `Notice`. If warning information is displayed, check the following: • `L`: The maximum number of multicast groups (the setting of `ip igmp group-limit` or `ipv6 mld group-limit`) or the maximum number of sources (the setting of `ip igmp source-limit` or `ipv6 mld source-limit`) has been reached, so IGMP Report messages or MLD Report messages are being discarded. Check the number of receivers. • `Q`: The IGMP or MLD version is different from the version on the neighboring routers. Use the same IGMP or MLD version on all routers. • `R`: At least one receiver has sent an IGMP Report message or an MLD Report message that cannot be received under the current settings. Either change the IGMP or MLD version on the Device, or check the settings of the receiver. • `S`: Some of the participation information has been discarded because the number of sources stored in a message exceeds the maximum number for IGMPv3 or MLDv2. Check the settings of the receiver.

(5) Items to be checked for the first hop router

The following table shows the items to be checked when the Device is used as a first hop router in a PIM-SM network configuration.

Table 4-15: Items to be checked for the first hop router

No.	Items to be checked and commands	Action
1	Make sure that the Device is directly connected to the sender and that multicast packets from the sender have reached the Device. • `show interface`	If multicast packets have not reached the Device, check the settings of the network configuration and of the sender.

No.	Items to be checked and commands	Action
2	Make sure that PIM-SM, IGMP or MLD is running on the interface that is connected to the sender. • `show ip pim interface` • `show ip igmp interface` • `show ipv6 pim interface` • `show ipv6 mld interface`	If PIM-SM, IGMP or MLD is not running, revise the configuration so that PIM-SM, IGMP or MLD runs.
3	Check whether multicast routing information exists. • `show ip mroute` • `show ipv6 mroute`	If no multicast routing information exists, make sure that the source address of the multicast packets is the network address of the interface that is directly connected to the sender.

4.6.2 Multicast packets are forwarded twice in a PIM-SM network

In a PIM-SM network configuration, if multicast packets are forwarded twice, check the settings of each router, and revise the settings so that PIM-SM runs on any interface that belongs to a network in which multiple routers exist.

The following table shows the items to be checked when data continues to be forwarded twice even after you have checked and revised the settings as described above.

Table 4-16: Items to be checked when data continues to be forwarded twice

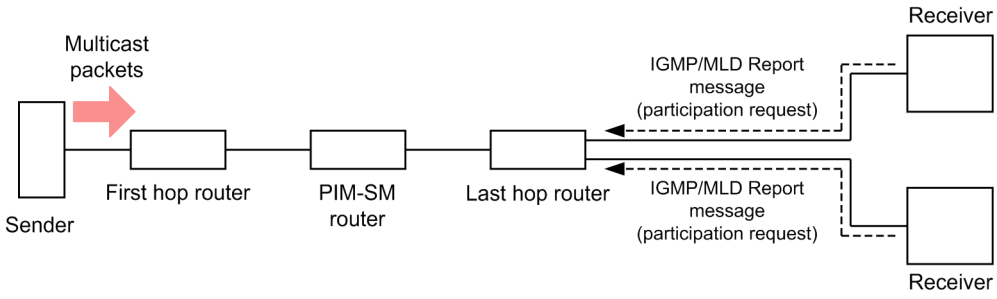
No.	Items to be checked and commands	Action
1	Check the PIM-SM neighbor information of the interface that belongs to the network in which multiple routers exist. • `show ip pim neighbor` • `show ipv6 pim neighbor`	If no neighboring routers are displayed, check the following: • Use the `show ip pim interface` or `show ipv6 pim interface` command to make sure that PIM-SM is running on the interface that is connected to the neighboring routers. • Check whether protocol packets are being discarded by the filters or QoS. For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*. • Check the settings of the neighboring routers.

4.6.3 Unable to perform multicast communication on a PIM-SSM network

If multicast forwarding is not possible in a PIM-SSM network configuration, isolate the cause of the problem by following the failure-analysis method described below.

The following figure shows an example of a PIM-SSM network.

Figure 4-7: PIM-SSM network example



The role of each router in the figure is as follows:

- First hop router: The router that connects directly to the sending side
- Last hop router: The router that connects directly to the receiving side

- PIM-SM router: A router, other than either of the above, on which PIM-SM is running

(1) Common items to be checked

The following table shows the items to be checked for all Devices in a PIM-SSM network configuration in common.

Table 4-17: Common items to be checked

No.	Items to be checked and commands	Action
1	Make sure that the IPv4 or IPv6 multicast routing program is running. • `show ip pim interface` • `show ipv6 pim interface`	If the IPv4 or IPv6 multicast routing program is not running, go to step 2.
		If the IPv4 or IPv6 multicast routing program is running, go to step 6.
2	Check the configuration to confirm that the multicast routing functionality is enabled (`ip multicast routing` or `ipv6 multicast routing`). • `show running-config`	If the IPv4 multicast routing functionality is enabled, go to step 3.
		If the IPv6 multicast routing functionality is enabled, go to step 4.
		If no multicast routing functionality is enabled, revise the configuration.
3	When using IPv4 multicast, check the configuration to confirm that multihoming is not set for the target interface. • `show running-config`	If multihoming is not set, go to step 5.
		Multihoming is not supported. If multihoming is set, revise the configuration.
4	When using IPv6 multicast, check the configuration to confirm that an IPv6 address is set for the loopback interface. • `show running-config`	If an IPv6 address is set for the loopback interface, go to step 5.
		If no IPv6 address is set for the loopback interface, revise the configuration.
5	Make sure that PIM-SM is running on 1 or more interfaces. • `show ip pim interface` • `show ipv6 pim interface`	If PIM-SM is running, go to step 6.
		If PIM-SM is not running, revise the configuration so that PIM-SM runs on at least 1 interface.
6	Check the configuration to see if a route distribution pattern for which multicast is available has been set. • `show running-config`	If a route distribution pattern for which multicast is available has been set, go to step 7.
		If no route distribution pattern for which multicast is available has been set, revise the configuration. For details about how to change the route distribution pattern, see the *Configuration Command Reference*. After changing the route distribution pattern, go to step 17.

No.	Items to be checked and commands	Action
7	Check whether protocol or multicast packets are being discarded by filters or QoS on the interface where PIM-SM, IGMP, and MLD are running.	For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.
		If no packets are being discarded, go to step 8.
8	Check whether a unicast route to the sender exists. • `show ip route` • `show ipv6 route`	If a unicast route exists, go to step 9.
		If no unicast route exists, see *4.5 Unicast routing communication failures*.
9	Make sure that PIM-SM is running on the interface that is connected to the next hop to the sender. • `show ip pim interface` • `show ipv6 pim interface`	If PIM-SM is running, go to step 10.
		If PIM-SM is not running, revise the configuration so that PIM-SM runs on the interface that is connected to the next hop to the sender.
10	Check the PIM-SM neighbor information. • `show ip pim neighbor` • `show ipv6 pim neighbor`	If the next hops of the routes that you checked in step 8 are all displayed as neighboring routers, go to step 11.
		If any of the next hops of the routes that you checked in step 8 is not displayed as a neighboring router, check the configuration of the neighboring router that is not displayed.
11	Check the configuration to make sure that the address range used for PIM-SSM includes the forwarding target group address. • `show running-config`	If the address range used for PIM-SSM includes the forwarding target group address, go to step 12.
		If the address range used for PIM-SSM does not include the forwarding target group address, revise the configuration.
12	Make sure that multicast forwarding entries exist. • `show ip mcache` • `show ipv6 mcache`	If multicast forwarding entries exist, go to step 13.
		If no multicast forwarding entries exist, make sure that multicast packets have reached the upstream interface. If no multicast packets have reached the upstream interface, check the settings of the sender or of the upstream router.
13	Check whether the number of multicast relay entries has reached the maximum (the setting of `ip pim mcache-limit` or `ipv6 pim mcache-limit`). • `show ip mcache` • `show ipv6 mcache`	If no warning is displayed, go to step 14.
		If a warning is displayed, the number of multicast relay entries has reached the maximum. Revise the network configuration and operate within the limits. If more negative cache entries are generated than expected, check whether a terminal is sending unnecessary multicast packets.

No.	Items to be checked and commands	Action
14	Make sure that multicast routing information exists. • `show ip mroute` • `show ipv6 mroute`	If multicast routing information exists, go to step 15.
		If no multicast routing information exists, check the downstream router settings.
15	Check whether the number of multicast routing information items has reached the maximum (the setting of `ip pim mroute-limit` or `ipv6 pim mroute-limit`). • `show ip mroute` • `show ipv6 mroute`	If no warning is displayed, go to step 16.
		If a warning is displayed, the number of multicast routing information items has reached the maximum. Revise the network configuration and operate within the limits.
16	Check whether a multicast packet is received that has a TTL value of 1 (when IPv4 multicast is in use) or a hop limit value of 1 (when IPv6 multicast is in use). • `show tcpdump`	If the TTL value or the hop limit value is not 1, go to step 17.
		If the TTL value or the hop limit value is 1, the Device does not relay the multicast packet. Revise the settings of the sender.
17	Check for a system message# that indicates that the number of multicast relay entries has reached the limit. • `show logging`	If no such system message is displayed, go to step 18.
		If such a system message is displayed, the number of multicast relay entries has reached the limit. After the limit is reached, no multicast relay entry can be set. We recommend that you not operate while the limit has been reached. Revise the network configuration and operate within the limits. After reviewing the network configuration, execute either the `restart ipv4-multicast` command or the `restart ipv6-multicast` command to reset the multicast relay entries.
18	Check for a system message that indicates that the total number of downstream interfaces of the multicast relay entries has reached the limit (message type: PRU, message identifier: 41023002). • `show logging`	If such a system message is displayed, the total number of downstream interfaces of the multicast relay entries has reached the limit. After the limit is reached, no downstream interface can be set. We recommend that you not operate while the limit has been reached. Revise the network configuration and operate within the limits. Note that the total number of downstream interfaces is the total of both the IPv4 multicast entries and the IPv6 multicast entries. After reviewing the network configuration, execute both the `restart ipv4-multicast` command and the `restart ipv6-multicast` command to reset the multicast relay entries.

#

When the number of IPv4 multicast relay entries reaches the limit, a system message with message type PRU and message identifier 41021002 is displayed, and when the number of IPv6 multicast relay entries reaches the limit, a system message with message type PRU and message identifier 41022002 is displayed.

(2) Items to be checked for the last hop router

The following table shows the items to be checked when the Device is used as a last hop router in a PIM-SSM network configuration.

Table 4-18: Items to be checked for the last hop router

No.	Items to be checked and commands	Action
1	Make sure that IGMP or MLD is running on the interface connected to the receiver. • `show ip igmp interface` • `show ipv6 mld interface`	If IGMP or MLD is not running, revise the configuration so that IGMP or MLD runs.
2	If the receiver uses IGMPv1, IGMPv2, IGMPv3 (EXCLUDE mode), MLDv1, or MLDv2 (EXCLUDE mode), make sure that the configuration (`ip igmp ssm-map enable` or `ipv6 mld ssm-map enable`) enables the IGMP/MLD PIM-SSM linkage functionality. • `show running-config`	If the configuration does not enable the IGMP/MLD PIM-SSM linkage functionality, revise the configuration.
3	If the receiver uses IGMPv1, IGMPv2, IGMPv3 (EXCLUDE mode), MLDv1, or MLDv2 (EXCLUDE mode), make sure that in the configuration, the group address and the sender address that are relayed via PIM-SSM are specified in the IGMP/MLD PIM-SSM linkage functionality (`ip igmp ssm-map static` or `ipv6 mld ssm-map static`). • `show running-config`	If the group address and the sender address relayed via PIM-SSM are not specified, revise the configuration.
4	Make sure that the receivers are participating in the forwarding target multicast group via IGMP or MLD. • `show ip igmp group` • `show ipv6 mld group`	If a receiver is not participating in the forwarding target multicast group, check the receiver settings.
5	If the IGMP/MLD PIM-SSM linkage functionality is in use, make sure that the sender address is displayed for the source address of the target multicast group. • `show ip igmp group` • `show ipv6 mld group`	If the sender address is not displayed for the source address, the settings of the IGMP/MLD PIM-SSM linkage functionality are invalid. Revise the configuration.
6	If an interface is participating in the forwarding target multicast group, make sure that the Device is the DR. • `show ip pim interface` • `show ipv6 pim interface`	If the Device is not the DR, check the DR of the forwarding target interface.
7	If an interface is using the static group participation functionality, make sure that the Device is the DR. • `show ip pim interface` • `show ipv6 pim interface`	If the Device is not the DR, enable the static group participation functionality for the device that is the DR of the forwarding target interface.

No.	Items to be checked and commands	Action
8	Check whether any anomaly has been detected on any interface. • `show ip igmp interface` • `show ipv6 mld interface`	Make sure that no warning information is displayed for `Notice`. If warning information is displayed, check the following: • `L`: The maximum number of multicast groups (the setting of `ip igmp group-limit` or `ipv6 mld group-limit`) or the maximum number of sources (the setting of `ip igmp source-limit` or `ipv6 mld source-limit`) has been reached, so IGMP Report messages or MLD Report messages are being discarded. Check the number of receivers. • `Q`: The IGMP or MLD version is different from the version on the neighboring routers. Use the same IGMP or MLD version on all routers. • `R`: At least one receiver has sent an IGMP Report message or an MLD Report message that cannot be received under the current settings. Either change the IGMP or MLD version on the Device, or check the settings of the receiver. • `S`: Some of the participation information has been discarded because the number of sources stored in a message exceeds the maximum number for IGMPv3 or MLDv2. Check the settings of the receiver.

(3) Items to be checked for the first hop router

The following table shows the items to be checked when the Device is in use as a first hop router in a PIM-SSM network configuration.

Table 4-19: Items to be checked for the first hop router

No.	Items to be checked and commands	Action
1	Make sure that the Device is directly connected to the sender and that multicast packets from the sender have reached the Device. • `show interface`	If no multicast packets have reached the Device, check the settings of the network configuration and of the sender.
2	Make sure that PIM-SM, IGMP or MLD is running on the interface that is connected to the sender. • `show ip pim interface` • `show ip igmp interface` • `show ipv6 pim interface` • `show ipv6 mld interface`	If PIM-SM, IGMP or MLD is not running, revise the configuration so that PIM-SM, IGMP or MLD runs.
3	Check whether the group address and source address are the same in the multicast packets and in the multicast routing information. • `show ip mroute` • `show ipv6 mroute`	If a different group address and source address are used, check the settings of the sender and of the last hop router.

4.6.4 Multicast packets are forwarded twice in a PIM-SSM network

In a PIM-SSM network configuration, if multicast packets are forwarded twice, check the settings of each router, and revise the settings so that PIM-SM runs on any interface that belongs to a network in which multiple routers exist.

The following table shows the items to be checked when data continues to be forwarded twice even after you have checked and revised the settings as described above.

Table 4-20: Items to be checked when data continues to be forwarded twice

No.	Items to be checked and commands	Action
1	Check the PIM-SM neighbor information of the interface that belongs to the network in which multiple routers exist. • `show ip pim neighbor` • `show ipv6 pim neighbor`	If no neighboring routers are displayed, check the following: • Use the `show ip pim interface` or `show ipv6 pim interface` command to make sure that PIM-SM is running on the interface that is connected to the neighboring routers. • Check whether protocol packets are being discarded by filters or QoS. For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*. • Check the settings of the neighboring routers.

4.6.5 Unable to perform multicast communication for a VRF

The following table describes the items to be checked when multicast communication is impossible for a VRF.

Table 4-21: Items to be checked for a VRF

No.	Items to be checked and commands	Action
1	If you are using the Device as a rendezvous point or a bootstrap router, check the configuration to see if an IPv4 address (if IPv4 multicast is in use) or an IPv6 address (if IPv6 multicast is in use) is set for the loopback interface of the target VRF. • `show running-config`	If an IPv4 or IPv6 address is set for the loopback interface of the target VRF, go to step 2.
		If you are not using the Device as a rendezvous point or a bootstrap router, go to step 6.
		If neither an IPv4 address nor an IPv6 address is set for the loopback interface of the target VRF, revise the configuration.
2	Make sure that the Device is operating as a rendezvous point candidate on the target VRF. • `show ip pim vrf all rp-mapping` • `show ipv6 pim vrf all rp-mapping`	If the Device is not operating as a rendezvous point candidate, go to step 3.
		If the Device is operating as a rendezvous point candidate, go to step 4.
3	Check the configuration to see if either the loopback interface number of the target VRF (when using IPv4 multicast) or the IPv6 address of the loopback interface of the target VRF (when using IPv6 multicast) is specified as a rendezvous point candidate. • `show running-config`	If the rendezvous point candidate setting is correct, go to step 4.
		If the rendezvous point candidate setting is incorrect, revise the configuration.
4	Make sure that the Device is operating as a bootstrap router candidate on the target VRF. • `show ip pim vrf all bsr` • `show ipv6 pim vrf all bsr`	If the Device is not operating as a bootstrap router candidate, go to step 5.
		If the Device is operating as a bootstrap router candidate, go to step 6.

No.	Items to be checked and commands	Action
5	Check the configuration to see if either the loopback interface number of the target VRF (when using IPv4 multicast) or the IPv6 address of the loopback interface of the target VRF (when using IPv6 multicast) is specified as a bootstrap router candidate. • `show running-config`	If the bootstrap router candidate setting is correct, go to step 6.
		If the bootstrap router candidate setting is incorrect, revise the configuration.
6	If multiple VRFs are in use, check whether a global network or a specific VRF is occupying an unexpectedly large number of multicast forwarding entries. • `show ip mcache vrf all` • `show ipv6 mcache vrf all`	If no global network or VRF is occupying more multicast forwarding entries than expected from the network design, go to step 7.
		If a global network or specific VRF is occupying more multicast forwarding entries than expected from the network design, check whether any unexpected multicast forwarding entries are being generated. If you find many negative cache entries, check whether a terminal is sending unnecessary multicast packets. To prevent one global network or a specific VRF from incorrectly occupying multicast forwarding entries, we recommend that you use the following configuration to set the maximum number of multicast forwarding entries for each VRF. • `ip pim vrf` <*vrf id*> `mcache-limit` <*number*> • `ipv6 pim vrf` <*vrf id*> `mcache-limit` <*number*>
7	For each VRF, check the details described in *4.6.1 Unable to perform multicast communication on a PIM-SM network* through *4.6.4 Multicast packets are forwarded twice in a PIM-SSM network*.	To check the information, you must specify VRF for each command. For how to specify VRF, see the *Operation Command Reference*.

4.6.6 Unable to perform multicast communication in an extranet

If multicast communication is impossible in an extranet, first, check the items described in *4.6.5 Unable to perform multicast communication for a VRF*, and make sure that multicast communication is possible in each VRF. After that, check the items described in the following table.

Table 4-22: Items to be checked for an extranet

No.	Items to be checked and commands	Action
1	Make sure that the unicast route from the destination VRF to the source address traverses the expected VRF or global network. • `show ip rpf vrf` <*vrf id*> • `show ipv6 rpf vrf` <*vrf id*>	If it does not, revise the settings of the unicast extranet.
2	For the upstream VRF, make sure that the unicast route to the source address does not traverse another VRF. • `show ip rpf vrf` <*vrf id*> • `show ipv6 rpf vrf` <*vrf id*>	If the unicast route to the source address traverses another VRF, multi-tier VRF relay within the device becomes necessary. Multi-tier VRF relay is not supported. Revise the network configuration.

No.	Items to be checked and commands	Action
3	In the (S, G) multicast routing information, check if `(denied)` is displayed for `incoming`. • `show ip mroute vrf all` • `show ipv6 mroute vrf all`	If (denied) is displayed for `incoming`, in the multicast route filtering of the upstream VRF, set the group address and the relay destination VRF that are used for extranet communication. If neither the group address nor the relay destination VRF is set in the multicast route filtering, all group addresses and VRFs are permitted as relay destinations.
4	Make sure that for `extranet filter` of the target VRF, the expected number of filters is displayed. • `show ip multicast resources` • `show ipv6 multicast resources`	If the value differs from the expected number of filters, the multicast route filtering settings are invalid. Revise the multicast route filtering settings.

Chapter

5. Troubleshooting Communication Failures Due to a Resource Shortage

This chapter describes the actions to be taken for communication failures that are due to a resource shortage.

5.1 When a resource shortage occurs in shared memory

5.1.1 Checking the resource usage of shared memory

When the usage of shared memory exceeds 80% of the capacity, exceeds 85% of the capacity, exceeds 90% of the capacity, exceeds 95% of the capacity, or reaches 100% of the capacity, the Device outputs the following system messages:

- Message type: PRU, Message identifier: 3f000001
- Message type: PRU, Message identifier: 3f000002
- Message type: PRU, Message identifier: 3f000004
- Message type: PRU, Message identifier: 3f000005
- Message type: PRU, Message identifier: 3f000007
- Message type: PRU, Message identifier: 3f000008

Merely exceeding 80%, 85%, 90%, or 95% of the capacity does not immediately affect communications. However, if the usage of shared memory continuously increases, the limit will be reached, and a resource shortage might occur. A resource shortage might, for example, prevent a route from being registered. To avoid the limit being reached, check the set value and the capacity ahead of time.

You can check the usage of the shared memory by using the `show pru resources` command. For details, see the *Operation Command Reference*.

5.1.2 Action to be taken if a resource shortage occurs in shared memory

If the usage of shared memory reaches 100%, do the following:

- Refer to the capacity described in the *Configuration Guide*, and check the settings and capacity of the route distribution pattern. To change the settings of the route distribution pattern, you need to restart the PRU.
- Revise the network configuration. If revising the network does not resolve the problem, restart the target PRU.

Chapter

6. Troubleshooting Each Functionality

This chapter describes the actions to be taken when a failure occurs in AX8600R functionality.

6.1 Problems with filters or QoS

6.1.1 Filter problems

If a frame of a kind specified in the filter is not passed or discarded, isolate the cause by using the failure-analysis method described in the following table.

Table 6-1: Failure-analysis method when a frame is not passed or discarded by the filter

No.	Items to be checked and commands	Action
1	Make sure that the filter that specifies the frames to be passed or discarded is set in the configuration. • `show running-config`	If the filter specifying the frames to be passed or discarded is not set, revise the configuration.
		If the filter specifying the frames to be passed or discarded is set, go to step 2.
2	Check whether `(restart required)` is displayed for the PRU update status. • `show system` • `show pru resources`	If `(restart required)` is displayed for the PRU update status, restart the PRU.
		If `(restart required)` is not displayed for the PRU update status, go to step 3.
3	For the filter entry that specifies the frames to be passed or discarded, check whether `Unset` is displayed for `Matched packets` for each PRU. • `show access-filter`	For the target filter entry, if `Unset` is displayed for `Matched packets` for each PRU, the filter entry is in the process of being applied to the Device. Wait until `Unset` disappears.
		For the target filter entry, if `Unset` is not displayed for `Matched packets` of each PRU, go to step 4.
4	Use the value of `Matched packets` to check the number of packets that match the filter criteria. • `show access-filter`	If the number of frames to be passed or discarded differs from the value of `Matched packets`, the filter detection conditions might be incorrect, which would cause frames to be silently discarded. Revise the filter entry settings.
		If the value of `Matched packets` is smaller than the number of frames to be passed or discarded, go to step 5.
5	Check whether packets are being discarded by uRPF.	uRPF might be discarding packets. For details about how to check this situation and the action to be taken, see *8.1.3 Checking for packets discarded by uRPF*.

6.1.2 QoS problems

(1) When the policer does not operate

If the policer does not operate, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 6-2: Failure-analysis method when the policer does not operate

No.	Items to be checked and commands	Action
1	In the configuration, check whether the QoS flow and the policer that specify the frames to be monitored are set. • `show running-config`	If the QoS flow and the policer that specify the frames to be monitored are not set, revise the configuration.

No.	Items to be checked and commands	Action
		If the QoS flow and the policer that specify the frames to be monitored are set, go to step 2.
2	Check whether `(restart required)` is displayed for the PRU update status. • `show system` • `show pru resources`	If `(restart required)` is displayed for the PRU update status, restart the PRU.
		If `(restart required)` is not displayed for the PRU update status, go to step 3.
3	For the QoS flow entry that specifies the frame to be monitored, check whether `Unset` is displayed for `Matched packets` of each PRU. • `show qos-flow`	For the target QoS flow entry, if `Unset` is displayed for `Matched packets` of each PRU, the QoS flow entry is in the process of being applied to the Device. Wait until `Unset` disappears.
		For the target QoS flow entry, if `Unset` is not displayed for `Matched packets` of each PRU, go to step 4.
4	For the policer entry specified in the QoS flow entry that specifies the frame to be monitored, check whether `Unset` is displayed for the number of packets of each PRU. • `show policer`	For the target policer entry, if `Unset` is displayed for the number of packets of each PRU, the policer entry is in the process of being applied to the Device. Wait until `Unset` disappears.
		For the target policer entry, if `Unset` is not displayed for the number of packets of each PRU, go to step 5.
5	Use the values of `Max-rate over`, `Max-rate under`, `Min-rate over`, and `Min-rate under` to check the number of compliant frames and the number of non-compliant frames. • `show policer`	If the number of frames to be monitored differs from the value displayed by the `show policer` command, the frames might not be a detection target of the QoS flow. For details, see the *Configuration Guide*.
		If the number of frames to be monitored differs from the value displayed by the `show policer` command, the detection conditions for QoS flow might be incorrect. Revise the QoS flow entry settings.
		If the number of compliant frames and the number of non-compliant frames displayed by the `show policer` command is inappropriate for the number of frames to be monitored, the monitoring bandwidth or the burst size of the policer might be incorrect. Revise the policer settings.
		If the value displayed by the `show policer` command is smaller than the number of frames to be monitored, go to step 6.
6	Check whether packets are being discarded by uRPF.	uRPF might be discarding packets. For details about how to check this situation and the action to be taken, see *8.1.3 Checking for packets discarded by uRPF*.
		If no packets are being discarded by uRPF, go to step 7.
7	Check whether frames are being discarded by the filter.	The filter might be discarding frames. For details about how to check this situation and the action to be taken, see *8.1.1 Checking for packets discarded by a filter*.

(2) When the marker and the priority change do not operate

If the marker and the priority change do not operate, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 6-3: Failure-analysis method when the marker and the priority change do not operate

No.	Items to be checked and commands	Action
1	In the configuration, make sure that the QoS flow that specifies the frames for which markers and priority changes are to be applied is set. • `show running-config`	If the QoS flow that specifies the frames for which markers and priority changes are to be applied is not set, revise the configuration.
		If the QoS flow that specifies the frames for which markers and priority changes are to be applied is set, go to step 2.
2	Check whether `(restart required)` is displayed for the PRU update status. • `show system` • `show pru resources`	If `(restart required)` is displayed for the PRU update status, restart the PRU.
		If `(restart required)` is not displayed for the PRU update status, restart the PRU, go to step 3.
3	For the QoS flow entry that specifies the frames for which markers and priority changes are to be applied, check whether `Unset` is displayed for the `Matched packets` item for each PRU. • `show qos-flow`	For the target QoS flow entry, if `Unset` is displayed for the `Matched packets` item for each PRU, the QoS flow entry is in the process of being applied to the Device. Wait until `Unset` disappears.
		For the target QoS flow entry, if `Unset` is not displayed for the `Matched packets` item for each PRU, go to step 4.
4	Use the value of `Matched packets` to check the number of packets that match the QoS flow conditions. • `show qos-flow`	If the number of frames for which markers and priority changes are to be applied differs from the value of `Matched packets`, the frames might not be a detection target of the QoS flow. For details, see the *Configuration Guide*.
		If the number of frames for which markers and priority changes are to be applied differs from the value of `Matched packets`, the QoS flow detection condition might be incorrect. Revise the QoS flow entry settings.
		If the value of `Matched packets` is smaller than the number of frames for which markers and priority changes are to be applied, go to step 5.
5	Check whether packets are being discarded by uRPF.	uRPF might be discarding packets. For details about how to check this situation and the action to be taken, see *8.1.3 Checking for packets discarded by uRPF*.
		If no packets are being discarded by uRPF, go to step 6.
6	Check whether frames are discarded by the filter.	Frames might have been discarded by the filter. For details about how to check this situation and the action to be taken, see *8.1.1 Checking for packets discarded by a filter*.

(3) When the port shaper does not operate

If the port shaper do not operate, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 6-4: Failure-analysis method when the port shaper does not operate

No.	Items to be checked and commands	Action
1	Use `Schedule-mode`, `Port-rate-limit`, `Active-rate`, `Qlen`, `Peak-Qlen`, `Limit-Qlen`, and `Drop-mode` to check the operating status of the target Ethernet interface. • `show qos queueing port`	If the status is `-`, the port shaper settings might not take effect. Make the Ethernet interface being in normal operation.
		If the status is not `-`, go to step 2.
2	Check whether packets are being discarded by uRPF.	uRPF might be discarding packets. For details about how to check this situation and the action to be taken, see *8.1.3 Checking for packets discarded by uRPF*.
		If no packets are being discarded by uRPF, go to step 3.
3	Check whether frames are being discarded by the filter.	The filter might be discarding packets. For details about how to check this situation and the action to be taken, see *8.1.1 Checking for packets discarded by a filter*.

6.2 Problems with sFlow statistics (flow statistics) functionality

This chapter describes the action to take when the following failures occur in the sFlow functionality of the Device:

- sFlow packets do not reach the collector.
- Flow samples do not reach the collector.
- Counter samples do not reach the collector.

6.2.1 sFlow packets do not reach the collector

The troubleshooting procedure for when sFlow packets do not reach the collector on the Device is as follows:

1. Check the operating status by using an operation command.
2. Check the contents of the configuration.
3. Check the route to the collector.
4. Check any other failures.

(1) Using operation commands to check the operating status

Execute the `show sflow` command a few times to display the sFlow statistics. Check whether the sFlow statistics functionality is running. If the values that are indicated by underlined text in the table below do not increase, see *(2) Checking the configuration* and *(3) Checking the route to the collector*. If the values increase, see *(3) Checking the route to the collector* and *(4) Checking the settings on the collector* to check whether the network is correctly connected to the collector.

Figure 6-1: Example of show sflow command output

```
> show sflow
Date 20XX/07/19 12:00:00 UTC
sFlow service status: enable
Elapsed time from the last statistics clearance:  8:00:05
sFlow agent data :
  sFlow service version  : 4
  CounterSample interval rate: 60 seconds
  Received sFlow samples : 37269  Dropped sFlow samples     : 2093
  Exported sFlow samples : 37269  Non-exported sFlow Samples:    0
sFlow collector data :
  Collector IP address: 192.168.1.20  UDP:6343  Source IP address: 192.168.1.1
   Send FlowSample UDP packets   : 12077  Send failed packets:     0
   Send CounterSample UDP packets:   621  Send failed packets:     0
sFlow sampling data :
  Configured rate(actual rate)  : 1 per 2048 packets(1 per 2048 packets)
   Configured sFlow ingress ports: 1/2
>
```

Note: Check whether the values indicated by underlined text increase.

(2) Checking the configuration

In the active configuration, check the following items.

- In the configuration, make sure that the IP address and UDP port number of the collector to which sFlow packets are sent have been correctly set.

```
(config)# show sflow
sflow destination 192.168.1.20 6343   <-1
sflow sample 2048
!
(config)#
```

1. Make sure the collector information is correctly set.

- Make sure that the sampling interval has been set.

  If the sampling interval is not set, a large default value is used. This value is too large, and almost no flow samples are sent to the collector. Therefore, set an appropriate value for the sampling interval.

  The following shows an example of the configuration output:

```
(config)# show sflow
sflow destination 192.168.1.20 6343
sflow sample 2048      <-1
!
(config)#
```

  1. Make sure that an appropriate sampling interval has been set.

  The following shows an example of executing the operation command:

```
> show sflow
Date 20XX/07/19 12:00:00 UTC
sFlow service status: enable
Elapsed time from the last statistics clearance:  16:00:05
sFlow agent data :
  sFlow service version  : 4
  CounterSample interval rate: 60 seconds
  Received sFlow samples : 37269  Dropped sFlow samples     : 2093
  Exported sFlow samples : 37269  Non-exported sFlow Samples:    0
                           :
sFlow sampling data :
  Configured rate(actual rate)  : 1 per 2048 packets(1 per 2048 packets)
   Configured sFlow ingress ports: 1/2
>
```

  Note: Make sure that the part indicated by underlined text displays an appropriate sampling interval.

- Make sure that `sflow forward ingress` has been set for the physical port at which the sFlow statistics are recorded.

```
(config)# show interfaces tengigabitethernet 1/2
interface tengigabitethernet 1/2
  sflow forward ingress           <-1
!
(config)#
```

  1. Make sure that `sflow forward ingress` has been set here.

- Make sure that sFlow packets are not discarded by the filter or QoS on the physical port where the sFlow statistics are recorded. For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.

- If the `sflow source` configuration command was used to specify the source (agent) IP address of the sFlow packet, make sure that the IP address is set for the interface of the Device.

```
(config)# show sflow
sflow destination 192.168.1.20 6343
sflow sample 2048
sflow source 192.168.1.1     <-1
!
(config)#
```

  1. Make sure that this is the IP address set for the interface of the Device.

(3) Checking the route to the collector

Refer to *4.1.1 Unable to communicate, or communication is interrupted* and *4.2.1 Unable to communicate, or communication is interrupted*, and make sure that the network is correctly connected to the collector. If the maximum size of an sFlow packet (`sflow max-packet-size`) was changed in the configuration, check whether connecting to the collector by using the specified

packet size is possible.

(4) Checking the settings on the collector

Make sure that the collector currently in use is correctly configured.

6.2.2 Flow samples do not reach the collector

If you took the action described in *6.2.1 sFlow packets do not reach the collector*, but the problem is not resolved, check the following items.

(1) Checking whether packets are forwarded

Execute the `show interfaces` command, and check whether packets are forwarded.

Figure 6-2: Example of port status output

```
>show interfaces tengigabitethernet 1/2
Date 20XX/07/19 12:00:00 UTC
NIF1: active 6-port 10GBASE-R(SFP+) retry:0
        Average:7000Mbps/120Gbps Peak:7500Mbps at 08:10:30
Port2: active up 10GBASE-LR 0012.e240.0a04
        SFP+ connect
        Time-since-last-status-change:10:30:30
        Bandwidth:10000000kbps Average out:3500Mbps Average in:3500Mbps
        Peak out:3800Mbps at 08:10:30 Peak in:3700Mbps at 08:10:30
        Output rate:2900.0Mbps 3400pps
        Input rate:2900.0Mbps 3400pps      <-1
        Flow control send :on
        Flow control receive:on
        TPID:8100
                              :
>
```

1. Make sure that packets are relayed at the physical port where flow samples are collected.

6.2.3 Counter samples do not reach the collector

If you took the the action described in *6.2.1 sFlow packets do not reach the collector*, but the problem is not resolved, check the following.

(1) Checking the sending interval of counter samples

In the configuration of the Device, make sure that the sending interval of counter samples is not 0. If the value is 0, counter samples cannot be sent to the collector.

Figure 6-3: Example of configuration output

```
(config)# show sflow
sflow destination 192.168.1.20 6343
sflow sample 2048
sflow polling-interval 60      <-1
!
(config)#
```

1. Make sure that a value of 0 is not set here.

6.3 CFM problems

6.3.1 CFM does not operate

If CFM does not operate, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 6-5: Failure-analysis method for CFM

No.	Items to be checked and commands	Action
1	Check the remote MEP information. • `show cfm remote-mep`	If the remote MEP information is displayed, go to step 2.
		If the remote MEP information is not displayed, go to step 4.
2	Check the MEP status. • `show cfm`	If the MEP status is `Up`, go to step 3.
		If the MEP status is not `Up`, check the CFM configuration and the line status. For details about how to check the line status, see *3. Troubleshooting Network Interfaces*.
3	Check the operation status of the CC.	If the operation status of the CC is `Enable`, go to step 4.
		If the operation status of the CC is not `Enable`, revise the CFM configuration.
4	Check the reception statistics of CFM. • `show cfm statistics`	If the reception statistics do not increase, check the settings of the remote MEP. If you find no problem with the remote MEP settings, check whether CFM PDUs are not being discarded by the filter or QoS. For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.

6.3.2 CC detected a fault

If a failure is detected when CC is in use, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 6-6: Failure-analysis method when a failure is detected in CC

No.	Items to be checked and commands	Action
1	Identify the location in the CFM where the failure was detected. • `show cfm fault detail`	If the level displayed is `MD`, go to step 2.
		If the level displayed is `MEL`, go to step 3.

No.	Items to be checked and commands	Action
2	In the target IEEE 802.1ag MEP, check the failure detected in CC.	Identify the item where the failure is `On`, and then depending on the detected failure, perform one of the following: • `OtherCCM` Check whether the settings prevent the domain from being configured. For details about whether or not the domain can be configured, see the *Configuration Guide*. • `ErrorCCM` Check whether the MEP ID is specified more than once, and make sure the CCM sending intervals match each other. • `Timeout` A failure might have occurred in the layer 2 network. Revise the network configuration. • `PortState` Check the line status of the target remote MEP. • `RDI` A failure occurred in the remote MEP of the source of the notification. Check the target device.
3	In the target ITU-T Y.1731 MEP, check the failure detected in CC.	Identify the item where the failure is `On`, and then depending on the detected failure, perform one of the following: • `UnexpMEL` Check whether the settings prevent the domain from being configured. For details about whether or not the domain can be configured, see the *Configuration Guide*. • `Mismerge` Check whether the settings prevent the MEG from being configured. • `UnexpMEP` Check whether the same MEP ID has been specified more than once in the same MEG. • `UnexpPeriod` Make sure that the CC sending intervals match each other in the MEG. • `UnexpPriority` Check whether the CoS values of CC match each other in the MEG. • `LOC` A failure might have occurred in the layer 2 network. Revise the network configuration. • `RDI` A failure occurred in the remote MEP of the source of the notification. Check the target device. • `AIS` A failure occurred in a lower level. Check the CC failure status in the lower levels. • `LCK` Check if ETH-LCK is in use in a lower level to stop communications.

6.4 LLDP problems

6.4.1 Unable to obtain neighboring device information by using LLDP

If neighboring device information cannot be correctly obtained by using LLDP, isolate the cause of the problem by using the failure-analysis method described in the following table.

Table 6-7: Failure-analysis method when LLDP is in use

No.	Items to be checked and commands	Action
1	Check the LLDP operation status. • `show lldp`	If `Status` is `Enabled`, go to step 2.
		If `Status` is not `Enabled`, LLDP is disabled. Enable LLDP.
2	Check the port information. • `show lldp detail`	If information for the port to which the neighboring device is connected is displayed, go to step 3.
		If information for the port to which the neighboring device is connected is not displayed, LLDP is disabled for the target port. Enable LLDP for the target port.
3	Check the link status of the port to which the neighboring device is connected. • `show lldp detail`	If `Up` is displayed for `Link`, go to step 4.
		If `Down` is displayed for `Link`, check the line status. For details about how to check the line status, see *3. Troubleshooting Network Interfaces*.
4	On the neighboring device side, check the transmission statistics of the LLDP frames.	If the LLDP frame count does not increase on the neighboring device, check the settings of the neighboring device.
		If the LLDP frame count does increase on the neighboring device, the connection between the devices might be incorrect. Check the connection. Also, check whether LLDP frames are being discarded by the filter or QoS. For details about how to check this situation and the action to be taken, see *8.1 Checking for discarded packets*.

Chapter

7. Obtaining Failure Information

This chapter mainly describes how to obtain failure information.

7.1 Collect maintenance information

During operation, when a failure occurs with the device, log and dump information is automatically collected. You can also use operation commands to capture dump information.

7.1.1 Maintenance information

The table below describes the maintenance information of the Device.

Table 7-1: Maintenance information

Item	Path and file name	FTP transfer mode	Delete after transfer
The dump file created when the device restarts	On the system that failed: `/dump0/bcu**.000` `**`: BCU number of the BCU that failed	Binary mode	Y
The dump file created when the PA fails	On the system that failed: `/usr/var/hardware/pa**.***` `**`: BCU number of the BCU that failed `***`: A serial number assigned in sequence from when dump data was collected. Up to 2 files (the oldest file and the most recent file) are stored.	Binary mode	Y
The PA dump file created when the `dump pa` command is executed	On the system on which the command was executed: `/usr/var/hardware/pa**.cmd` `**`: BCU number of the BCU that executed the command	Binary mode	Y
The dump file created when the SFU fails	On the system that failed: `usr/var/hardware/sfu**.***` `**`: SFU number of the SFU that failed `***`: A serial number assigned in sequence from when dump data was collected up to 2 files (the oldest file and the most recent file) are stored.	Binary mode	Y
The SFU dump file created when the `dump sfu` command is executed	On the system on which the command was executed: `/usr/var/hardware/sfu**.cmd` `**`: SFU number of the specified SFU	Binary mode	Y
The dump file created when the PRU fails	On the system that failed: `/usr/var/hardware/pru**.***` `**`: PRU number of the PRU that failed `***`: A serial number assigned in sequence from when dump data was collected Up to 2 files (the oldest file and the most recent file) are stored.	Binary mode	Y
The PRU dump file created when the `dump pru` command is executed	On the system on which the command was executed: `/usr/var/hardware/pru**.cmd` `**`: PRU number of the specified PRU	Binary mode	Y
The dump file created when the NIF fails	On the system that failed: `/usr/var/hardware/nif**.***` `**`: NIF number of the NIF that failed `***`: A serial number assigned in sequence from when dump data was collected up to 2 files (the oldest file and the most recent file) are stored.	Binary mode	Y

Item	Path and file name	FTP transfer mode	Delete after transfer
The NIF dump file created when the `dump nif` command is executed	On the system on which the command was executed: `/usr/var/hardware/nif**.cmd` `**`: NIF number of the specified NIF	Binary mode	Y
The dump file created when the PS fails	On the system that failed: `/usr/var/hardware/ps**.000` `**`: PS number of the PS that failed	Binary mode	Y
The dump file created when the fan unit fails	On the system that failed: `/usr/var/hardware/fan**.000` `**`: Fan unit number of the fan unit that failed	Binary mode	Y
Log	Files are stored in the acquired-log directory with the following names: Operation log: `log.txt` Statistics log: `log_ref.txt`	ASCII mode	Y
Information from when the configuration file encounters an error	In administrator mode, execute the following commands to copy 2 files to the home directory. After that, transfer the files. • `cp /config/cnf/system.cnf system.cnf` • `cp /config/cnf/system.txt system.txt`	Binary mode	Y#
Error-recovery information	`/usr/var/core/*.core`	Binary mode	Y

Legend: Y: The user must delete the file.

#: Delete the files that were created as a result of the copy operation.

7.1.2 Collecting failure information by using the dump command

You can use operation commands on the Device to capture dump information from the board or other components of the device.

If a communication failure occurs, execute all of the following commands on the active BCU to capture memory dumps.

1. For all SFUs in the `active` status, execute the `dump sfu` command.
2. For the PRU on which the failed port is located, execute the `dump pru` command.
3. For the NIF on which the failed port is located, execute the `dump nif` command.

The captured memory dumps are stored as memory dump files on the system on which the commands were executed, in /usr/var/hardware. After capturing the memory dumps, you need to delete the memory dump files.

Example:

The following is an example of a communication failure on port number 1 of NIF number 1.

1. Log in to the active BCU, and then execute the `dump sfu` command for all SFUs in the `active` status. If a system message is displayed, execute the following `dump sfu` command:

```
> dump sfu 1
The dump-collection command was accepted.
>
20XX/01/01 08:18:23 UTC 1-1(A) S6 SFU SFU:1 350e0501 00 000000000000 The SFU
online dump command was executed.
>
> dump sfu 2
The dump-collection command was accepted.
```

```
>
20XX/01/01 08:28:23 UTC 1-1(A) S6 SFU SFU:2 350e0501 00 000000000000 The SFU
online dump command was executed.
>
> dump sfu 3
The dump-collection command was accepted.
>
20XX/01/01 08:38:23 UTC 1-1(A) S6 SFU SFU:3 350e0501 00 000000000000 The SFU
online dump command was executed.
>
> dump sfu 4
The dump-collection command was accepted.
>
20XX/01/01 08:48:23 UTC 1-1(A) S6 SFU SFU:4 350e0501 00 000000000000 The SFU
online dump command was executed.
>
```

2. After the last SFU system message is displayed, execute the `dump pru` command for the PRU on which the failed port (port number 1) is located.

```
> dump pru 1
The dump-collection command was accepted.
>
20XX/01/01 08:58:52 UTC 1-1(A) S6 PRU PRU:1 350e0601 00 000000000000 The PRU
online dump command was executed.
>
```

3. After the PRU system message is displayed, execute the `dump nif` command for the NIF (NIF number 1) on which the failed port (port number 1) is located.

```
> dump nif 1
The dump-collection command was accepted.
>
20XX/01/01 09:04:14 UTC 1-1(A) S6 NIF NIF:1 350e0701 00 000000000000 The NIF
online dump command was executed.
>
```

7.2 Transferring maintenance information by using the ftp command

The `ftp` command available on the Device allows you to transfer files that contain maintenance information such as logs or dump files to a remote operation terminal or remote host.

7.2.1 Transferring a dump file to a remote operation terminal

The following shows the procedure for using the `ftp` command to transfer a collected dump file to a remote operation terminal.

Figure 7-1: Transferring a dump file to a remote operation terminal

```
> cd /dump0                                          <---1
> ftp 192.168.0.1                                    <---2
Connected to 192.168.0.1.
220 192.168.0.1 FTP server ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary                                         <---3
200 Type set to I.
ftp> cd /usr/home/staff1                            <---4
250 CWD command successful.
ftp> put bcu01.000                                  <---5
local: bcu01.000 remote: bcu01.000
200 EPRT command successful.
150 Opening BINARY mode data connection for 'bcu01.000'.
100% |************************|  2780 KiB    1.55 MiB/s    00:00 ETA
226 Transfer complete.
2846953 bytes sent in 00:01 (1.55 MiB/s)
ftp> bye
221 Thank you for using the FTP service on 192.168.0.1.
>
```

1. Specify the source directory.
2. Specify the address of the destination terminal.
3. Specify binary mode.#
4. Specify the destination directory.
5. Transfer the dump file.

#

Make sure that you use binary mode to transfer dump files. If you transfer dump files in ASCII mode, you cannot obtain correct dump information.

7.2.2 Transferring logs to a remote operation terminal

The following shows the procedure for using the `ftp` command to transfer collected logs to a remote operation terminal.

Figure 7-2: Transferring log files to a remote operation terminal

```
> show logging > log.txt
> show logging reference > log_ref.txt
> ftp 192.168.0.1                                    <---1
Connected to 192.168.0.1.
220 192.168.0.1 FTP server ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
```

```
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii                                          <---2
200 Type set to A.
ftp> cd /usr/home/staff1                            <---3
250 CWD command successful.
ftp> put log.txt                                    <---4
local: log.txt remote: log.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log.txt'.
100% |************************|   251 KiB   11.13 MiB/s    --:-- ETA
226 Transfer complete.
257490 bytes sent in 00:00 (1.21 MiB/s)
ftp>
ftp> put log_ref.txt                                <---4
local: log_ref.txt remote: log_ref.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log_ref.txt'.
100% |************************| 33165        7.48 MiB/s    --:-- ETA
226 Transfer complete.
33165 bytes sent in 00:00 (160.98 KiB/s)
ftp> bye
221 Thank you for using the FTP service on 192.168.0.1.
>
```

1. Specify the address of the destination terminal.
2. Specify ASCII mode.
3. Specify the destination directory.
4. Transfer the log file.

7.2.3 Transferring core files to a remote operation terminal

The following shows the procedure for using the `ftp` command to transfer collected core files to a remote operation terminal.

Figure 7-3: Transferring core files to a remote operation terminal

```
> cd /usr/var/core/
> ls                                                <---1
configManager.core snmpd.core
> ftp 192.168.0.1                                   <---2
Connected to 192.168.0.1.
220 192.168.0.1 FTP server ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt                                         <---3
Interactive mode off.
ftp> binary                                         <---4
200 Type set to I.
ftp> cd /usr/home/staff1                            <---5
250 CWD command successful.
ftp> mput *.core                                    <---6
local: configManager.core remote: configManager.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'configManager.core'.
100% |************************|  6740 KiB    0.98 MiB/s    00:00 ETA
226 Transfer complete.
6902471 bytes sent in 00:06 (0.98 MiB/s)
local: snmpd.core remote: snmpd.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'snmpd.core'.
```

```
100% |************************|   843 KiB   12.83 MiB/s    00:00 ETA
226 Transfer complete.
863812 bytes sent in 00:00 (4.10 MiB/s)
ftp> bye
221 Thank you for using the FTP service on 192.168.0.1.
>
```

1. Make sure that the core file exists.

   If the file does not exist, exit the procedure without doing anything.

2. Specifies the destination terminal address.
3. Change the interactive mode.
4. Specify binary mode.#
5. Specify the destination directory.
6. Transfer the core file.

#

Make sure that you use binary mode to transfer core files. If you transfer core files in ASCII mode, you cannot obtain correct error-recovery information.

7.3 Collecting information and transferring files by using the show tech-support command

You can use the `show tech-support` command to collect information when a failure occurs in a batch operation. Also, by specifying the `ftp` parameter, you can transfer the collected information to a remote operation terminal or remote host.

The following shows the procedure for using the `show tech-support` command to collect maintenance information and transfer it to a remote operation terminal.

Figure 7-4: Transferring a maintenance information file to a remote operation terminal

```
> show tech-support ftp                                                    <-1
Enter the host name of the FTP server.           : 192.168.0.1           <-2
Enter the user ID for the FTP server connection. : staff1                 <-3
Enter the password for the FTP server connection. :                       <-4
Enter the path name of the FTP server.           : /usr/home/staff1       <-5
Enter the file names for the log and dump files.  : support               <-6
Do you want to check and extract dump files on a standby system? (y/n): y  <-7
Mon Dec 31 12:00:00 UTC 20XX
Transferred support.txt .
Executing.............................
File transfer ended successfully.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 4568
-rwxrwxrwx  1 root  wheel  4677464 Dec 18 21:16:16 20XX bcu01.000
***** ls -l /usr/var/hardware *****
total 1368
-rwxrwxrwx  1 root  wheel  1002811 Dec 27 11:56:16 20XX nif05.000
***** ls -l /standby/dump0 *****
***** ls -l /standby/usr/var/hardware/ *****
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /usr/var/core *****
***** ls -l /standby/usr/var/core *****
No Core files
########## End of Core files' Information ##########
Transferred support.tgz .
Executing...
File transfer ended successfully.
>
```

1. Execute the command.
2. Specifies the remote host name.
3. Specify the user name.
4. Enter a password.
5. Specify the destination directory.
6. Specifies the file name.
7. Choose to collect dump files from the standby system.

7.4 Collecting information from a remote operation terminal and transferring files by using the ftp command

You can use the `ftp` command on a remote operation terminal or remote server to connect to the Device, and then specify a file name to obtain failure or maintenance information.

(1) Collecting "show tech-support" information

The procedures below describe how to connect a remote operation terminal, as a client, to the Device by using the `ftp` command, and how to collect information by specifying the name of a file that contains the required `show tech-support` information.

Figure 7-5: Obtaining the "show tech-support" information

```
client-host> telnet 192.168.0.21                    <---1
Trying 192.168.0.21...
Connected to 192.168.0.21
Escape character is '^]'.

login: staff1
Password:

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.

>show tech-support > show-tech.txt                  <---2
>exit
Connection closed by foreign host.
client-host> ftp 192.168.0.21                       <---3
Connected to 192.168.0.21.
220 192.168.0.21 FTP server ready.
Name (192.168.0.21:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get show-tech.txt                              <---4
local: show-tech.txt remote: show-tech.txt
200 EPRT command successful.
150 Opening BINARY mode data connection for 'show-tech.txt' (3784076 bytes).
100% |**********************************|  3695 KiB    1.02 MiB/s    00:00 ETA
226 Transfer complete.
3784076 bytes received in 00:03 (1.02 MiB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.21.
client-host>
```

1. Use `telnet` to connect to the Device from the client.
2. Save the `show tech-support` information to a file on the Device (Specify the file name `show-tech.txt`).
3. Use `ftp` to connect to the Device from the client.
4. Transfer the `show-tech.txt` file to the client.

Notes

Depending on the load on the device or the state of the communication path, the client might close the connection due to a network timeout. If this occurs, you must set a longer client timeout period.

(2) Collecting a dump file and a core file

Connect a remote operation terminal, as a client, to the Device by using the `ftp` command, and then specify the necessary file names to obtain the dump file and the core file. By specifying

special file names for the `get` subcommand of the `ftp` command, you can obtain multiple files at once. When you obtain core files, you can specify each file individually.

The following table shows the special file names used for the `get` subcommand, and the corresponding files.

Table 7-2: Files you can obtain by using the get subcommand of the ftp command

Special file names to specify for the get subcommand	Obtained files
`.dump`	The files in `/dump0`, `/usr/var/hardware`, and `/usr/var/core` (these files will be compressed)
`.dump0`	The files in `/dump0` (these files will be compressed)
`.hardware`	The files in `/usr/var/hardware` (these files will be compressed)
`.core`	The files in `/usr/var/core` (these files will be compressed)

The following shows the procedure for specifying the `get` subcommand of the `ftp` command to collectively obtain dump files.

Figure 7-6: Obtaining dump files from a remote operation terminal

```
client-host> ftp 192.168.0.60                              <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary                                                <---2
200 Type set to I.
ftp> get .dump dump.tgz                                    <---3
local: dump.tgz remote: .dump
200 EPRT command successful.
150 Opening BINARY mode data connection for '/etc/ftpdump'.
 16539 KiB  816.40 KiB/s
226 Transfer complete.
16936547 bytes received in 00:20 (813.99 KiB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. Use `ftp` to connect to the Device from the client.
2. Specify binary mode.

   Make sure that you use binary mode to transfer dump files and core files. You cannot transfer correct information in ASCII mode.
3. Transfer the `.dump` files to the client. (Specify the file name `dump.tgz`.)

Notes

- Some `ftp` commands, such as `ls`, do not display the special file names to be specified for the `get` subcommand that are shown in *Table 7-2: Files you can obtain by using the get subcommand of the ftp command*. For this reason, you cannot check the size of the files to be collectively obtained.
- Depending on the load on the device or the state of the communication path, the client might close the connection due to a network timeout. If this occurs, you must set a longer client timeout period.

- The current directory might contain a file that has the same name as one of the special file names shown in *Table 7-2: Files you can obtain by using the get subcommand of the ftp command*. In such a case, the actual file that has that name is obtained, and therefore dump files cannot be collectively obtained. To collectively obtain dump files, either delete the file that has the that name, or move the file to a different directory by using `cd` or another commands. After that, obtain the dump files.

7.5 Writing to a memory card

You can write failure and maintenance information to a memory card. Note, however, that memory cards have limited capacity.

7.5.1 Writing data to a memory card on an operation terminal

The following shows the procedure for writing device information to a memory card on an operation terminal.

Example:

1. Into the Device, insert a memory card to which information is to be written.
2. Use the `ls` command to check the size of the source file (`tech.log`).
```
> ls -l tech.log
-rw-r--r--  1 operator  users  234803 Nov 15 15:52 tech.log
```
3. Use the `show mc` command to check the space available on the memory card.
```
> show mc
Date 20XX/04/01 07:20:11 UTC
BCU1 MC: enabled
     CID: 00c7000910d06b224734304653415001
     used:        189,792KB
     free:      3,680,928KB
     total:     3,870,720KB
BCU2 MC: --------
>
```
   The figure indicated with underlined text indicates the available space.
4. Use the `cp` command to copy the source file to the memory card by using the destination file name `tech-1.log`.
```
> cp tech.log mc-file tech-1.log
```
5. Use the `ls` command to make sure that the file was written to the memory card.
```
> ls mc-dir
Name             Size
tech-1.log              234803
>
```

Chapter

8. Analysis of Communication Failures

This chapter describes the actions to be taken when a communication failure occurs.

8.1 Checking for discarded packets

8.1.1 Checking for packets discarded by a filter

One possible cause of a communication failure on a network that uses the Device is that specific frames are being discarded by a filter. The following shows how to check if frames are being discarded by a filter.

If policy-based routing is specified for the filter operation, in addition to the following check method, see also *4.3.1 Checking for policy-based routing communication failures*.

(1) How to check whether packets have been discarded by a filter

1. Execute the `show access-filter` command. In the access list that is applied to the interface, check the filter criteria, the number of packets that match the filter criteria, and the number of packets that were discarded by a silent-discard filter entry.
2. To determine whether the target frames were discarded, compare the filter criteria that you checked in step 1 with the contents of the frames that cannot be forwarded. If the contents of the frames that cannot be forwarded match none of the applied filter criteria, the frames might have been discarded by the silent-discard filter entry.
3. If the frames were discarded by filters, check if the filter configuration is appropriate.

8.1.2 Checking for packets discarded by QoS

One possible cause of a communication failure on a network that uses the Device is that frames are being discarded or accumulated by a QoS policy, the port shaper, or an internal queue in the device. The following shows how to identify if and where frames are being discarded or accumulated in the Device because of QoS.

(1) How to check whether packets are being discarded by the policer

1. Execute the `show qos-flow` or `show policer` command to check the flow detection conditions and the operating specification of the policer that is applied to the interface, and the policer statistics.
2. To determine whether the target frames were discarded, compare the flow detection conditions you checked in step 1 with the contents of the frames that cannot be forwarded.

   If a frame violates the maximum-bandwidth monitoring conditions, the frame is discarded and the `Matched packets(Max-rate over)` statistics item increases. An increase in this statistics item means that frames were discarded by the policer that is applied to the interface.
3. If frames were discarded by the policer, check if the QoS configuration settings and the policer settings are appropriate.

(2) Checking for frames discarded and accumulated by the port shaper

1. Execute the `show qos queueing port` command. In the statistics of the port send queue of the output interface that is being used for communication, check the `Discard packets`, `Send packets`, and `Qlen` items.
2. If the `Discard packets` item that you checked in step 1 increases, the frames were discarded by discard control.
3. If the `Send packets` item that you checked in step 1 does not increase, but the `Qlen` item increases, the frames are being queued by scheduling.
4. If frames were discarded or queued, make sure that the port shaper configuration is appropriate.

(3) How to check for frames that are discarded and queued by an internal queue in the device

1. Execute the `show qos queueing` command to check the `Discard packets`, `Send packets`, and `Qlen` items of the following queues.

   For unicast frames:

   - Port receive queue
   - PRU-FE SSW send (relay) queue
   - PRU-SSW FE receive (unicast) queue
   - PRU-SSW FE send (unicast) queue
   - PRU-FE SSW receive (relay) queue
   - Port send queue

   For multicast frames:

   - Port receive queue
   - PRU-FE SSW send (relay) queue
   - PRU-SSW FE receive (multicast) queue
   - PRU-SSW FE send (multicast) queue
   - PRU-FE SSW receive (relay) queue
   - Port send queue

   For frames through BCU:

   - Port receive queue
   - PRU-FE CPU send queue
   - BCU-PA PRU receive queue
   - BCU-CPU PA receive queue
   - BCU-CPU send queue
   - PRU-FE SSW send (control) queue
   - PRU-SSW FE receive queue
   - PRU-SSW FE send queue
   - PRU-FE SSW receive (control) queue
   - Port send queue

2. If the `Discard packets` item that you checked in step 1 increases, the frames were discarded by an internal queue in the device.
3. If the `Send packets` item does not increase but the `Qlen` item increases, the frames are being queued by an internal queue in the device.
4. If frames were discarded or accumulated, revise the flow volume of the target frames.

8.1.3 Checking for packets discarded by uRPF

One possible cause of a communication failure on a network that uses the Device is that specific packets are being discarded by uRPF. The following shows how to check whether packets are being discarded by uRPF.

1. Execute the `show ip urpf statistics` or `show ipv6 urpf statistics` command with the `interface` parameter specified, and check the `Discarded IPv4 packets` item and the

`Discarded IPv6 packets` item.

2. If the `Discarded IPv4 packets` item or the `Discarded IPv6 packets` item that you checked in step 1 increases, the packets were discarded by uRPF.
3. If packets were discarded by uRPF, revise the network configuration so that the packets to be discarded by uRPF are not sent to the Device.

8.2 Layer 2 network failure analysis

8.2.1 Layer 2 network failure analysis by using CFM

The following shows how to check the situation if layer 2 communication is unavailable while CFM is in operation.

1. Execute the `l2ping` command to check the following:
   - Whether or not communication with a remote MEP is possible
   - The response time
2. Execute the `l2traceroute` command to check the devices in the layer 2 network with which communication is possible.

(1) Checking communication by using the l2ping command

Executing the `l2ping` command sends a Loopback Message to a remote MEP. By checking the response to this message, you can check the availability of layer 2 communication and the response time.

Example:

1. Execute the `show cfm remote-mep` command to check the destination remote MEP.

```
> show cfm remote-mep
Date 20XX/04/01 12:00:00 UTC
Total RMEP Counts:      6
Domain Level:3   MA:  100
  Domain Name(str ): ProviderDomain_3
  MA     Name(str ): Kanagawa_to_Nagoya
  MEP ID: 101  (Up  )  Port:ChGr: 16        Tag: 100  Status: -
    RMEP Information  Counts:  2
    ID:   3  MAC:0012.e220.1224  Status:-            20XX/04/01 07:55:20 UTC
    ID:  15  MAC:0012.e200.005a  Status:-            20XX/04/01 08:04:54 UTC
```

   The value indicated by underlined text is the MEP information of the Device. This example uses `ID:3` under `RMEP Information` as the destination remote MEP.

2. Execute the `l2ping` command for the destination remote MEP that you checked in step 1, and check the response.

```
> l2ping remote-mep 3 domain-level 3 ma 100 mep 101
L2ping to MP:3(0012.e220.1224) on Level:3 MA:100 MEP:101
Time:20XX/04/01 12:00:00 UTC
1: L2ping Reply from 0012.e220.1224 64bytes Time= 25 ms
2: L2ping Reply from 0012.e220.1224 64bytes Time= 22 ms
3: L2ping Reply from 0012.e220.1224 64bytes Time= 23 ms
4: L2ping Reply from 0012.e220.1224 64bytes Time= 22 ms
5: L2ping Reply from 0012.e220.1224 64bytes Time= 23 ms
--- L2ping Statistics ---
Tx L2ping Request : 3 Rx L2ping Reply : 5 Lost Frame : 0%
Round-trip Min/Avg/Max : 22/23/25 ms
```

   Check whether a response is returned and whether the response time is appropriate.

If no response to the `l2ping` command is returned or if the response time is inappropriate, revise the network configuration between the MEP of the Device and the target remote MEP.

(2) Checking communication by using the l2traceroute command

Executing the `l2traceroute` command sends a Linktrace Message to a remote MEP to collect responses to the message as routing information. From this routing information, you can check the devices with which layer 2 communication is possible.

Example:

1. Execute the `show cfm remote-mep` command to check the destination remote MEP.

```
> show cfm remote-mep
Date 20XX/04/01 12:00:00 UTC
Total RMEP Counts:      6
Domain Level:3   MA:  100
  Domain Name(str ): ProviderDomain_3
  MA     Name(str ): Kanagawa_to_Nagoya
  MEP ID: 101  (Up  )  Port:ChGr: 16        Tag: 100  Status: -
    RMEP Information  Counts:  2
    ID:   3  MAC:0012.e220.1224  Status:-            20XX/04/01 07:55:20 UTC
    ID:  15  MAC:0012.e200.005a  Status:-            20XX/04/01 08:04:54 UTC
```

   The value indicated by underlined text is the MEP information of the Device. This example uses `ID:3` under `RMEP Information` as the destination remote MEP.

2. Execute the `l2traceroute` command for the destination remote MEP that you checked in step 1, and check the routing information.

```
> l2traceroute remote-mep 3 domain-level 3 ma 100 mep 101 ttl 255
L2traceroute to MP:3(0012.e220.1224) on Level:3 MA:100 MEP:101
Time:20XX/04/01 12:00:00 UTC
254 0012.e220.00c2 Forwarded
253 0012.e210.000d Forwarded
252 0012.e220.1224 NotForwarded Hit
```

   Check whether `Hit` (indicated by underlined text) is displayed.

If `Hit` is not displayed in the routing information, revise the network configuration between the device indicated by the MAC address contained in the last response and the remote MEP.

Chapter 9. Restarting a Device

This chapter mainly describes how to restart a device.

9.1 Restarting a device

9.1 Restarting a device

9.1.1 Restarting a device

You can use the `reload` command on the active BCU to restart a device. For details on the syntax and parameters of the command, see the *Operation Command Reference*.

(1) Collecting a memory dump and restarting a BCU

The following shows procedures for collecting a memory dump and restarting a BCU.

Example 1

The standby BCU restarts and a memory dump is collected.

1. Execute the `reload` command shown below. Note that you can omit the `dump-image` parameter.
```
> reload -f dump-image standby
>
```

Example 2

The active BCU restarts and a memory dump is collected. When the active BCU restarts, the system is switched.

1. Execute the `reload` command shown below. Note that you can omit the `dump-image` parameter.
```
> reload -f dump-image active
>
```

Example 3

Both the standby BCU and the active BCU restart and memory dumps are collected.

1. Execute the `reload` command shown below. Note that you can omit the `dump-image` parameter.
```
> reload -f dump-image
>
```

(2) Restarting a BCU without collecting a memory dump

The following shows procedures for restarting a BCU without collecting a memory dump.

Example 1

The standby BCU restarts but a memory dump is not collected.

1. Execute the `reload` command shown below.
```
> reload -f no-dump-image standby
>
```

Example 2

The active BCU restarts but a memory dump is not collected. When the active BCU restarts, the system is switched.

1. Execute the `reload` command shown below.
```
> reload -f no-dump-image active
>
```

Example 3

Both the standby BCU and the active BCU restart but memory dumps are not collected.

1. Execute the `reload` command shown below.
```
> reload -f no-dump-image
>
```

(3) Stopping a device

The following shows procedures for stopping the BCU and the device. When stopping the BCU or the device, no memory dump is collected.

Example 1

The standby BCU stops.

1. Execute the `reload` command shown below.

```
> reload -f stop standby
>
```

Example 2

The active BCU stops. When the active BCU stops, the system is switched.

1. Execute the `reload` command shown below.

```
> reload -f stop active
>
```

Example 3

The device stops.

1. Execute the `reload` command shown below.

```
> reload -f stop
>
```

Appendix

A. Detailed Display Contents of the "show tech-support" Command

A. Detailed Display Contents of the "show tech-support" Command

A.1 Detailed display contents of the "show tech-support" command

The following tables list descriptions of the content that is displayed when protocol parameters are used with the `show tech-support` command. For the details of the display contents, see the *Operation Command Reference*.

Note

The *Operation Command Reference* does not cover some of the information that the `show tech-support` command displays. Such information is not disclosed to the public because it contains internal information of the device.

Note also that depending on the software version, some information might not appear.

Table A-1: Command details

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
1	`show version`	Software version and hardware information of the Device	Y	Y	Y	Y
2	`show system`	Operating information of the Device	Y	Y	N	N
3	`show process cpu bcu`	CPU usage per BCU process	Y	Y	Y	Y
4	`show cpu bcu detail`	BCU-CPU usage	Y	Y	Y	Y
5	`show process memory bcu`	Memory usage per BCU process	Y	Y	Y	Y
6	`/usr/local/diag/statShow`	Counter information of OS resources	Y	Y	Y	Y
7	`show memory`	BCU memory information	Y	Y	Y	Y
8	`show processes cpu pa`	CPU usage information of PA processes	Y	Y	Y	Y
9	`show cpu pa detail`	CPU usage information of the PA	Y	Y	Y	Y
10	`show processes memory pa`	Memory usage information of PA processes	Y	Y	Y	Y
11	`show memory pa`	Memory usage information of the PA	Y	Y	Y	Y
12	`show processes cpu pru`	CPU usage information of PRU-CPU processes	Y	Y	Y	Y
13	`show cpu pru detail`	CPU usage information of the PRU-CPU	Y	Y	Y	Y

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
14	show processes memory pru	Memory usage information of PRU-CPU processes	Y	Y	Y	Y
15	show memory pru	Memory usage information of the PRU-CPU	Y	Y	Y	Y
16	fstat	Usage information of BCU-internal device file descriptors	Y	Y	Y	Y
17	/usr/local/diag/rtsystat	Counters for OS-internal routing information and internal control information	Y	Y	Y	Y
18	/usr/local/diag/rtastat	Counters for OS-internal routing information and internal control information	Y	Y	Y	Y
19	netstat -An	BCU internal communication information	Y	Y	Y	Y
20	show netstat interface	BCU-internal communication information	Y	Y	Y	Y
21	show netstat statistics	BCU-internal communication information	Y	Y	N	N
22	pstat -f	Descriptor information	Y	Y	Y	Y
23	/sbin/dmesg	OS trace information	Y	Y	Y	Y
24	cat /var/run/dmesg.boot	BCU OS boot log	Y	Y	Y	Y
25	cat /var/log/messages.old	BCU OS operation log	Y	Y	Y	Y
26	cat /var/log/messages	BCU OS operation logs	Y	Y	Y	Y
27	cat /standby/var/run/dmesg.boot	OS trace information	Y	Y	N	N
28	cat /standby/var/log/messages.old	OS trace information	Y	Y	N	N
29	cat /standby/var/log/messages	OS trace information	Y	Y	N	N
30	cat /var/log/clitrace1	CLI-internal error information	Y	Y	Y	Y
31	cat /var/log/clitrace2	Log of the commands executed in the CLI	Y	Y	Y	Y
32	cat /var/log/clitrace3	Device information from CLI startup	Y	Y	Y	Y
33	cat /standby/var/log/clitrace1	Error information from the standby CLI	Y	Y	Y	Y
34	cat /standby/var/log/clitrace2	Log of the commands executed in the standby CLI	Y	Y	Y	Y

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
35	`cat /standby/var/log/clitrace3`	Device information from startup of the standby CLI	Y	Y	Y	Y
36	`cat /var/log/mmitrace`	Operation command trace information	Y	Y	Y	Y
37	`show pru resources`	PRU resource Information	Y	Y	N	N
38	`show dumpfile`	Information about captured dump files	Y	Y	N	N
39	`df -ik`	Usage of the BCU internal disk	Y	Y	Y	Y
40	`show environment`	Environment information of the Device	Y	Y	N	N
41	`du -Pk /`	Usage of the BCU internal disk	Y	Y	Y	Y
42	`ls -lTiR /dump0`	Usage of the BCU internal disk	Y	Y	Y	Y
43	`ls -lTiR /dump1`	Usage of the BCU internal disk	Y	Y	Y	Y
44	`ls -lTiR /log`	Usage of the BCU internal disk	Y	Y	Y	Y
45	`ls -lTiR /tmp`	Usage of the BCU internal disk	Y	Y	Y	Y
46	`ls -lTiR /config`	Usage of the BCU internal disk	Y	Y	Y	Y
47	`ls -lTiR /standby/dump0`	Usage of the BCU internal disk	Y	Y	N	N
48	`ls -lTiR /var`	Usage of the BCU internal disk	Y	Y	N	N
49	`ls -lTiR /standby/config`	Usage of the BCU internal disk	Y	Y	N	N
50	`ls -lTiR /standby/log`	Usage of the BCU internal disk	Y	Y	N	N
51	`ls -lTiR /standby/dump1`	Usage of the BCU internal disk	Y	Y	N	N
52	`ls -lTiR /standby/var`	Usage of the BCU internal disk	Y	Y	N	N
53	`ls -lTiR /standby/tmp`	Usage of the BCU internal disk	Y	Y	N	N
54	`show sessions`	Login session information	Y	Y	Y	Y
55	`stty -a -f /dev/tty00`	Console terminal information	Y	Y	Y	Y
56	`show accounting`	Accounting information	Y	Y	Y	Y
57	`show users`	Login user-account information set in the Device	Y	Y	Y	Y
58	`/usr/sbin/pstat -t`	Terminal information	Y	Y	Y	Y
59	`show ntp associations`	Operating status of the connected NTP server	Y	Y	Y	Y
60	`show logging count 10000`	Active operation log information	Y	Y	Y	Y

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
61	`show logging reference`	Active statistics log information	Y	Y	Y	Y
62	`show logging count 10000 standby`	Standby operation log information	Y	Y	Y	Y
63	`show logging reference standby`	Standby statistics log information	Y	Y	Y	Y
64	`cat /var/log/kern.log.old`	Usage of the BCU internal disk	Y	Y	Y	Y
65	`cat /var/log/kern.log`	Usage of the BCU internal disk	Y	Y	Y	Y
66	`cat /var/log/daemon.log.old`	Usage of the BCU internal disk	Y	Y	Y	Y
67	`cat /var/log/daemon.log`	Usage of the BCU internal disk	Y	Y	Y	Y
68	`cat /var/log/fixsb.log`	Usage of the BCU internal disk	Y	Y	Y	Y
69	`cat /standby/var/log/kern.log.old`	Usage of the BCU internal disk	Y	Y	N	N
70	`cat /standby/var/log/kern.log`	Usage of the BCU internal disk	Y	Y	N	N
71	`cat /standby/var/log/daemon.log.old`	Usage of the BCU internal disk	Y	Y	N	N
72	`cat /standby/var/log/daemon.log`	Usage of the BCU internal disk	Y	Y	N	N
73	`cat /standby/var/log/fixsb.log`	fsck information of BCU internal disk	Y	Y	N	N
74	`cat /var/tmp/gen/trace/mng.trc`	Configuration command trace information 1 (Trace information of ConfigManager)	Y	Y	Y	Y
75	`cat /var/tmp/gen/trace/mng_sub.trc`	Configuration command trace information 2 (Event trace information of ConfigManager)	Y	Y	Y	Y
76	`cat /var/tmp/gen/trace/api.trc`	Configuration command trace information 3 (Trace information of ConfigAPI)	Y	Y	Y	Y
77	`cat /var/tmp/gen/trace/ctl.trc`	Configuration command trace information 4 (Trace information of ConfigControl)	Y	Y	Y	Y
78	`/usr/local/diag/inci_info -T -c nodeProc`	nodeProc debug information	Y	Y	Y	Y
79	`/usr/local/diag/inci_info -T -c nodeCtl`	nodeCtl debug information	Y	Y	Y	Y

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
80	/usr/local/diag/inci_info -T -c nodeDev	nodeDev debug information	Y	Y	Y	Y
81	/usr/local/diag/inci_info -T -c logCtl	logCtl debug information	Y	Y	Y	Y
82	cat /var/tmp/logctl/trace/logCtl.log	logCtl trace information	Y	Y	Y	Y
83	cat /var/tmp/logctl/trace/logSysMsgCtl.log	logSysMsgCtl trace information	Y	Y	Y	Y
84	cat /var/tmp/logctl/trace/logSyslogCtl.log	logSyslogCtl trace information	Y	Y	Y	Y
85	cat /var/tmp/logctl/trace/logEmailCtl.log	logEmailCtl trace information	Y	Y	Y	Y
86	cat /var/tmp/logctl/trace/logMateSend.log	logMateSend trace information	Y	Y	Y	Y
87	cat /var/tmp/logctl/trace/logSave-l.log	logSave trace information	Y	Y	Y	Y
88	cat /var/log/quectl/quectld.log	Log information of the queue control program	Y	Y	Y	Y
89	cat /var/log/queinfo/queinfod.log	Log information of the queue statistics control program	Y	Y	Y	Y
90	cat /usr/var/pplog/ppupdate.log	Update log information	Y	Y	Y	Y
91	cat /usr/var/pplog/ppupdate2.log	Update log information	Y	Y	Y	Y
92	cat /var/log/authlog	Authentication trace information	Y	Y	Y	Y
93	cat /var/log/xferlog	FTP trace information	Y	Y	Y	Y
94	cat /var/log/policy/policyd.log	Log information of the policy-based routing control program	Y	N	Y	N
95	cat /var/log/ssh.log	SSH log information	Y	Y	Y	Y
96	/usr/local/diag/mqlib_trace -w 0	List of tje message queues in use	Y	N	Y	N
97	/usr/local/diag/genbintrns -s	Information about access to the change list and configuration	Y	Y	Y	Y
98	cat /var/log/flowctl/flowctld.log	Log information of the filter and QoS control program	Y	N	Y	N
99	cat /var/log/flowinfo/flowinfod.log	Log information of the filter and QoS statistics control program	Y	N	Y	N

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
100	/usr/local/diag/padctrl -l tech	Information of the diag command (for use by show tech of PAD and the PA	N	Y	N	Y
101	/usr/local/diag/padctrl -l techd	Information of the diag command (for use by show tech detail) of PAD and the PA	Y	N	Y	N
102	/usr/local/diag/qosdiag policy tech	Internal information of the policy-based routing control program	Y	N	Y	N
103	/usr/local/diag/ppuapinfo filter all tech	Detailed information of the filter control	Y	Y	N	N
104	/usr/local/diag/ppuapinfo qos all tech	Detailed information of the QoS control	Y	Y	N	N
105	/usr/local/diag/bpifc tech	Information about the distribution of control data in the device	Y	Y	Y	Y
106	/usr/local/diag/cswdiag tech	Detailed SFU information	Y	Y	Y	Y
107	/usr/local/diag/iswdiag	ISW device information	Y	Y	Y	Y
108	/usr/local/diag/showdev -s	Detailed status of the device	Y	Y	Y	Y
109	/usr/local/diag/qosdiag quectl tech	Internal information of the queue control program	Y	Y	Y	Y
110	/usr/local/diag/qosdiag queinfo tech	Internal information of the queue statistics control program	Y	Y	Y	Y
111	/usr/local/diag/ppuapinfo ssw all tech	Detailed SSW information	Y	Y	Y	Y
112	/usr/local/diag/ppuapinfo isw all tech	PPU-ISW device information and driver application information	Y	Y	Y	Y
113	/usr/local/diag/ppuapinfo rctl all tech	Detailed information of the RCTL control	Y	Y	N	N
114	/usr/local/diag/ppuapinfo rctlcom all tech	Detailed information common to the RCTLs	Y	Y	N	N
115	/usr/local/diag/ppuapinfo rctlstat all tech	Detailed information of RCTL statistics	Y	Y	N	N
116	/usr/local/diag/cmddrvif show stat	Internal statistics related to hardware control by operation commands and to information acquisition	Y	N	Y	N
117	/usr/local/diag/flowctl tech	Internal information of the filter and QoS control program	Y	N	Y	N

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
118	/usr/local/diag/qosdiag flowinfo tech	Internal information of the filter and QoS statistics control program	Y	N	Y	N
119	/usr/local/diag/dupctl tech	Carry over status information and statistics information managed by the redundant control	Y	N	Y	N
120	show port	Port information	Y	Y	N	N
121	show port statistics	Port statistics	Y	Y	N	N
122	show port transceiver debug	Transceiver details for ports	Y	Y	N	N
123	show interfaces nif XXX_NIF line XXX_LINE debug	Detailed statistics for ports	Y	Y	N	N
124	show channel-group detail	Link aggregation details	Y	N	N	N
125	show channel-group statistics lacp	LACPDU send and receive statistics for link aggregation	Y	N	N	N
126	show lldp detail	Configuration and neighboring device information for LLDP.	Y	N	N	N
127	show lldp statistics	LLDP statistics	Y	N	N	N
128	show cfm detail	Detailed CFM information and failure detection information of the Device	Y	N	N	N
129	show vrrpstatus detail statistics	VRRP virtual-routers status and statistics	Y	N	N	N
130	show vrrpstatus group	VRRP virtual routers grouping information	Y	N	N	N
131	show sflow detail	Configuration setting status and operating status of sFlow statistics.	Y	N	N	N
132	show snmp	SNMP information	Y	N	N	N
133	/usr/local/diag/snmp_dp -mem	Memory counter for SNMP functionality	Y	N	N	N
134	/usr/local/diag/snmp_dp -resource	Resource counter for SNMP functionality	Y	N	N	N
135	show environment temperature-logging	Temperature history of the Device	Y	Y	N	N
136	show running-config	Operating configuration	Y	Y	Y	Y
137	show qos queueing	Device-internal queue information	Y	Y	Y	Y
138	show qos queueing tech-support	Device-internal control queue information in the device	Y	Y	Y	Y
139	show access-filter	Filtering statistics	Y	N	N	N

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
140	show qos-flow	QoS flow statistics	Y	N	N	N
141	show policer	Policer statistics	Y	N	N	N
142	show ip cache policy	Destination routing information and status of the IPv4 policy-based routing list	Y	N	N	N
143	show ipv6 cache policy	Destination routing information and status of the IPv6 policy-based routing list	Y	N	N	N
144	show netstat routing-table numeric	BCU OS routing information	Y	Y	Y	Y
145	show processes memory unicast	Amount of available memory for and memory usage of the unicast routing program	Y	N	Y	N
146	show processes cpu minutes unicast	CPU usage of the unicast routing program	Y	N	Y	N
147	show graceful-restart unicast	Operating status of restart routers that perform graceful restarts in the unicast routing protocol	Y	N	N	N
148	show ip interface ipv4-unicast	Interface information of the Devices that the unicast routing program recognizes	Y	N	Y	N
149	show ip route vrf all summary	Number of active and inactive routes maintained by the routing protocol for each VRF	Y	N	N	N
150	show ip vrf all	Number of routes learned for each VRF	Y	N	N	N
151	show ip dhcp relay statistics	DHCP/BOOTP relay agent statistics	Y	N	N	N
152	show ip rip vrf all statistics	RIP statistics for each VRF	Y	N	Y	N
153	show ip rip vrf all advertised-routes summary	Number of routes advertised by RIP for each VRF	Y	N	N	N
154	/usr/local/diag/ppuapinfo uni all tech	Control management information of the unicast driver of the PPU (Information related to IPv4/IPv6 unicast routing, ARP, and NDP)	Y	N	N	N
155	show ip rip vrf all received-routes summary	Number of routes learned by RIP for each VRF	Y	N	N	N

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
156	`/usr/local/diag/ppuapinfo mlt all tech`	Control management information of the multicast driver of the PPU (Information related to IPv4/IPv6 multicast routing)	Y	N	N	N
157	`show ip ospf discard-packets`	Information on packets discarded by OSPF	Y	N	Y	N
158	`show ip ospf vrf all statistics`	Statistics on sent and received packets collected by OSPF for each VRF	Y	N	Y	N
159	`show ip ospf vrf all neighbor detail`	Details of OSPF neighboring routers for each VRF	Y	N	N	N
160	`show ip ospf vrf all virtual-links detail`	Details of OSPF virtual links for each VRF	Y	N	N	N
161	`show ip ospf vrf all database database-summary`	Number of LSAs per OSPF LS type for each VRF	Y	N	N	N
162	`show ip vrf all ospf`	OSPF global information for each VRF	Y	N	N	N
163	`show ip bgp vrf all neighbor detail`	BGP4 peering information for each VRF	Y	N	N	N
164	`show ip bgp vrf all notification-factor`	Messages that caused the disconnection of BGP4 connections for each VRF	Y	N	Y	N
165	`show ip bgp vrf all received-routes summary`	Number of routes received from BGP4 peers for each VRF	Y	N	N	N
166	`show ip bgp vrf all advertised-routes summary`	Number of routes advertised to BGP4 peers for each VRF	Y	N	N	N
167	`show ipv6 interface ipv6-unicast`	Interface information of the Devices that the unicast routing program recognizes	Y	N	Y	N
168	`show ipv6 route vrf all summary`	Number of active and inactive routes maintained by the unicast routing program for each VRF	Y	N	N	N
169	`show ipv6 vrf all`	Number of routes learned for each VRF	Y	N	N	N
170	`show ipv6 dhcp relay statistics`	DHCPv6 relay agent statistics	Y	N	N	N
171	`show ipv6 rip vrf all advertised-routes summary`	Number of routes advertised by RIPng for each VRF	Y	N	N	N
172	`show ipv6 rip vrf all received-routes summary`	Number of routes learned by RIPng for each VRF	Y	N	N	N

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
173	`show ipv6 rip vrf all statistics`	RIPng Sstatistics on RIPng for each VRF	Y	N	Y	N
174	`show ipv6 ospf discard-packets`	Information on packets discarded by OSPFv3	Y	N	Y	N
175	`show ipv6 ospf vrf all statistics`	Statistics on packets collected by OSPFv3 for each VRF	Y	N	Y	N
176	`show ipv6 ospf vrf all neighbor detail`	OSPFv3 neighboring router status for each VRF	Y	N	N	N
177	`show ipv6 ospf vrf all virtual-links detail`	OSPFv3 virtual link information for each VRF	Y	N	N	N
178	`show ipv6 ospf vrf all database database-summary`	Number of LS-Databases for OSPFv3	Y	N	N	N
179	`show ipv6 ospf vrf all`	OSPFv3 global information for each VRF	Y	N	N	N
180	`show ipv6 bgp vrf all neighbor detail`	BGP4+ peering information for each VRF	Y	N	N	N
181	`show ipv6 bgp vrf all received-routes summary`	Number of routes received from BGP4+ peers for each VRF	Y	N	N	N
182	`show ipv6 bgp vrf all advertised-routes summary`	Number of routes advertised to BGP4+ peers for each VRF	Y	N	N	N
183	`show ipv6 bgp vrf all notification-factor`	Packets that caused the disconnection of BGP4+ connections for each VRF	Y	N	Y	N
184	`show netstat multicast numeric`	BCU OS multicast statistics	Y	Y	Y	Y
185	`show ip multicast vrf all statistics`	IPv4 multicast statistics (first)	Y	N	Y	N
186	`show ipv6 multicast vrf all statistics`	IPv6 multicast statistics (first)	Y	N	Y	N
187	`show ip multicast vrf all resources`	Entries used in the IPv4 multicast routing functionality	Y	N	Y	N
188	`show ip igmp vrf all interface detail`	IGMP interface information	Y	N	Y	N
189	`show ip igmp vrf all group`	IGMP multicast group information	Y	N	Y	N
190	`show ip pim vrf all interface detail`	IPv4 PIM interface information	Y	N	Y	N
191	`show ip pim vrf all neighbor detail`	Neighboring information of the IPv4 multicast interface	Y	N	Y	N

No.	Command (displayed)	Description	Execution on an active system		Execution on a standby system	
			No parameter specified	Basic	No parameter specified	Basic
192	`show ip pim vrf all bsr`	IPv4 PIM-SM bootstrap router information	Y	N	Y	N
193	`show ip pim vrf all rp-mapping`	IPv4 PIM-SM rendezvous point information	Y	N	Y	N
194	`show ip mroute vrf all`	IPv4 multicast routing information	Y	N	Y	N
195	`show ip mcache vrf all`	IPv4 multicast relay entry information	Y	N	Y	N
196	`show ipv6 multicast vrf all resources`	Entries used in the IPv6 multicast routing functionality	Y	N	Y	N
197	`show ipv6 mld vrf all interface`	MLD interface information	Y	N	Y	N
198	`show ipv6 mld vrf all group`	MLD multicast group information	Y	N	Y	N
199	`show ipv6 pim vrf all interface detail`	IPv6PIM interface information	Y	N	Y	N
200	`show ipv6 pim vrf all neighbor detail`	Neighboring information of the IPv6 multicast interface	Y	N	Y	N
201	`show ipv6 pim vrf all bsr`	IPv6 PIM-SM bootstrap router information	Y	N	Y	N
202	`show ipv6 pim vrf all rp-mapping`	IPv6 PIM-SM rendezvous point information	Y	N	Y	N
203	`show ipv6 mroute vrf all`	IPv6 multicast routing information	Y	N	Y	N
204	`show ipv6 mcache vrf all`	IPv6 multicast relay entry information	Y	N	Y	N
205	`show ip multicast vrf all statistics`	IPv4 multicast statistics (second)	Y	N	Y	N
206	`show ipv6 multicast vrf all statistics`	IPv6 multicast statistics (second)	Y	N	Y	N
207	`show qos queueing tech-support`	Information on device-internal control queues (second)	Y	Y	Y	Y
208	`show qos queueing`	Device-internal queue information (second)	Y	Y	Y	Y
209	`show access-filter`	Filtering statistics (second)	Y	N	N	N
210	`show qos-flow`	QoS flow statistics (second)	Y	N	N	N
211	`show policer`	Policer statistics (second)	Y	N	N	N

Legend: Y: Displayed, N: Not displayed

Index

S

T

U

V

W