AX3800S, AX3660S, AX3650S

Troubleshooting Guide

AX36S-T002X-50

■ Relevant products

This manual applies to the models in the AX3800S, AX3660S, and AX3650S series of switches.

■ Precautions in exporting

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

■ Trademarks

AMD is a registered trademark of Advanced Micro Device, Inc. in the United States and other countries.
Cisco is a registered trademark of Cisco Systems, Inc. in the United States and other countries.
Ethernet is a registered trademark of Xerox Corporation.
Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and other countries.
IPX is a registered trademark of Novell,Inc.
Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and other countries.
Octpower is a registered trademark of NEC Corporation.
OpenSSL is a registered trademark of OpenSSL Software Foundation in the United States and other countries.
Python is a registered trademark of Python Software Foundation.
RSA and RC4 are registered trademarks of EMC Corporation in the United States and other countries.
sFlow is a registered trademark of InMon Corporation in the United States and other countries.
ssh is a registered trademark of SSH Communications Security, Inc.
UNIX is a registered trademark of The Open Group in the United States and other countries.
VLANaccessController and VLANaccessAgent are trademarks of NEC Corporation.
Windows is a registered trademark or trademark of Microsoft Corporation in the United States and other countries.
Other company and product names in this document are trademarks or registered trademarks of their respective owners.

■ Reading and storing this manual

Before you use the device, carefully read the manual and make sure that you understand all safety precautions.
After reading the manual, keep it in a convenient place for easy reference.

■ Note

Information in this document is subject to change without notice.
Please note that the actual product might differ from how it is depicted in output examples and figures.

■ Editions history

December 2023 (Edition 1) AX36S-T002X-50

■ Copyright

Preface

■ Relevant products

This manual applies to the models in the AX3800S, AX3660S, and AX3650S series of switches.
Before you use the device, carefully read the manual and make sure that you understand all instructions and cautionary notes.
After reading the manual, keep it in a convenient place for easy reference.

■ Corrections to the manual

Descriptions in this manual might be corrected 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 Switch.
Readers must have an understanding of the following:
- The basics of network system management

■ Manual URL

You can view this manual on our website at:
https://www.alaxala.com/en/

■ Reading sequence of the manuals

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

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

Quick Start Guide
(AX36S-Q002X)

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

Hardware Instruction Manual
(AX36S-H002X)

Transceiver
Hardware Instruction Manual
(AX-COM-H001X)

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

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

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

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

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

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

● **To check messages and logs**

Message Log Reference
(AX38S-S017X)

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

Troubleshooting Guide
(AX36S-T002X)

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

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

・AX3660S series switch

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

■ Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point

DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association

MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PMTU	Path Maximum Transmission Unit
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PTP	Precision Time Protocol
QoS	Quality of Service
QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable

RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
Sync-E	Synchronous Ethernet
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLS	Transport Layer Security
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN

VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web

■ Conventions: KB, MB, GB, and TB

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

Contents

1 Troubleshooting of Device Failures

This chapter describes how to take actions when a failure occurs on a device.

1.1 Device failure analysis

1.1.1 Procedure for handling device failures

Use the procedure described below if a failure occurs on a device.

For details about the LED indications of the device, see "Hardware Instruction Manual" of the respective model. Note that even when you cannot look at the actual device, you can still check the LED indications of the device and troubleshoot failures accordingly, just like when you can look at the actual device, by issuing operation commands from a remote operation terminal.

Table 1-1 Troubleshooting device failures

No.	Failure details	Action
1	- Smoke emanates from the device. - An abnormal odor emanates from the device. - An abnormal sound emanates from the device.	Follow the procedures below to stop the supply of all power to the device. - Devices equipped with an AC power supply unit Unplug the power cables connected to all AC power supply units installed in the Switch from the outlets. - Devices equipped with a DC power supply unit Turn off the circuit breakers on all distribution switchboards that supply power to all the DC power supply units installed in the Switch. - Devices equipped with a built-in AC power supply (AX3660S-24T4X) Unplug the power cables connected to all AC power connectors installed in the Switch from the outlets. After completing the above procedure, replace the device.
2	The login prompt does not appear.	1. If a memory card has been inserted, remove the card, and turn the device off and then on again to restart the device. 2. If a memory card has not been inserted, turn the device off and then on again to restart the device. 3. If restarting the device does not solve the problem, replace the device.
3	The PWR LED of the device is off.	Follow the procedure shown below: 1. Follow "Table 1-2 Isolating the cause of power failures". 2. Replace the failed power supply. - For models equipped with a power supply unit Replace the power supply unit. When a failure occurs on a power supply unit, either of the following applies: - For PS-A06, PS-A06R, or PS-D06: (a) The PS OK LED is off. (b) The PS OK LED is lit in orange. - For power supply units other than PS-A06, PS-A06R, and PS-D06 (a) The POWER LED is off. (b) The ALM1 LED is lit in red. (c) The ALM2 LED is lit in red. - For models equipped with a built-in power supply (AX3660S-24T4X) Replace the whole device. 3. If neither step 1 nor 2 above applies, restart the device and check whether there are any abnormalities in the environment. (1) Turn off the power and turn it on again to restart the device.

No.	Failure details	Action
		(2) If the device successfully restarts, execute the "show logging" command to check the failure information. `>show logging | grep ERR` (3) If the failure information contains a high-temperature warning message, the running environment might be the cause of the problem. Ask the system administrator to improve the environment. (4) If you cannot restart the device in step (1) or if failure information cannot be obtained in step (2) or does not contain a high-temperature warning message, a failure has occurred on the device. In this case, replace the device.
4	The ST1 LED of the device is lit in red.	A fatal failure has occurred in the device. Replace the device.
5	- The ST1 LED of the device blinks in red. - The LINK LED of each port on the device blinks in orange or is lit in red.	A partial failure has occurred in the device or a line. Check the error message and take the action against the failure. Execute the "show logging" command to check the failure information and take action. `>show logging | grep ERR`

Table 1-2 Isolating the cause of power failures

No.	Failure details	Action
1	The power switch of the power supply unit is off.#1	Turn the power switch on.
2	The power cable is disconnected or loose.	Perform the following procedure: 1. Turn the power switch off.#1 2. Connect the power cable correctly. 3. Turn the power switch on.#1
3	The power supply unit is not firmly installed and is unstable.#2	Perform the following procedure: 1. Turn the power switch off.#1 2. Install the power supply unit correctly. 3. Turn the power switch on.#1
4	The measured input power supply is outside the following range: For 100 V AC: 90 to 127 V AC For 200 V AC: 180 to 254 V AC For -48 V DC: -40.5 to -57 V DC Note: Take this action only if the input power supply can be measured.	Ask the person responsible for the facility where the device is housed to take action regarding the input power supply.

#1: This step applies when the power supply unit is equipped with a power switch.

#2: This item applies to models equipped with a power supply unit.

1.1.2 Replacing the device and optional modules

The procedures to replace the device and optional modules are described in the "Hardware Instruction Manual". Follow the instructions in the manual.

2 Troubleshooting in Operation Management

This chapter describes what to do if a problem occurs during operation management.

2.1 Login problems

2.1.1 Forgotten login user password

If a user forgets his or her login user password and is unable to log in to the Switch, do the following:

- If another user can log in:
  Ask the user who can log in to execute the "password" command in administrator mode to reset the forgotten login user password. Alternatively, ask the user to use the "clear password" command to delete the password.
  These commands should be executed in administrator mode. Therefore, the user who logs in must know the password for the "enable" command for changing the input mode to administrator mode.
  The following figure shows an example of resetting the forgotten password for user1 in administrator mode.

  Figure 2-1 Example of resetting password for user1

  ```
  # password user1
  Changing local password for user1.
  New password:
  Retype new password:
  #
  ```

- If no users can log in:
  If no users can log in or if a user can log in but does not know the password for the "enable" command, press 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.
  A startup due to the default restart does not perform login authentication by password, authentication when changing to administrator mode ("enable" command), nor command authorization. Therefore, fully exercise caution.
  For details about default restarts, see "Configuration Guide".

The reset password takes effect after the device restarts.

2.1.2 Forgotten administrator mode password

If you cannot change the input mode to administrator mode because you forgot the password for the "enable" command, press 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.

A startup due to the default restart does not perform login authentication by password, authentication when changing to administrator mode ("enable" command), nor command authorization. Therefore, fully exercise caution.

For details about default restarts, see "Configuration Guide".

The reset password takes effect after the device restarts.

2.2 Operation terminal problems

2.2.1 Information cannot be entered from the console or does not appear correctly

If a problem occurs during connection to a console, check the details in accordance with "Table 2-1 Problems occurring during connection to the console and action to take".

If a problem occurs during connection to a modem, check the details in accordance with "Table 2-2 Problems occurring during connection to the modem and action to take". Also, see the documentation provided with the modem.

Table 2-1 Problems occurring during connection to the console and action to take

No.	Failure details	Items to check
1	Nothing is displayed on the screen.	Perform the following procedure: 1. Make sure the ST1 LED on the front panel of the device is lit in green. If it is not lit in green, see "Hardware Instruction Manual". 2. Check whether the cables are connected correctly. 3. Make sure that an RS232C crossover cable is used. 4. Make sure that the communication software settings (including port number, communication speed, data length, parity bit, stop bit, and flow control) are specified as follows: Communication speed: 9600 bit/s (or the set value if you have changed this value) Data length: 8 bits Parity bit: None Stop bit: 1 bit Flow control: None
2	Key entry is not accepted.	Perform the following procedure: 1. Data transmission might have been interrupted by XON/XOFF flow control. End the interruption of data transmission (by simultaneously pressing the [Ctrl] + [Q] keys). If the device still does not accept entry from the keys after this operation, perform steps 2 and 3. 2. Make sure that the communication software settings are correct. 3. The screen might not respond because the [Ctrl] + [S] keys were simultaneously pressed. Press any key.
3	Unexpected characters are displayed.	Negotiation with the communication software might not have been performed correctly. Check the software communication speed by doing the following: 1. If the communication speed of CONSOLE (RS232C) was not specified 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 the communication speed of CONSOLE (RS232C) has been set 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.
4	Unexpected characters are displayed when a user name is being entered.	The communication speed of CONSOLE (RS232C) might have been changed. See No. 3.
5	Login is not possible.	1. Make sure that the login prompt is displayed on the screen. If it is not, the device is starting up. Wait a while. 2. If you log in using local authentication, check whether you are trying to log in using an account that does not exist on the device. 3. Use the "aaa authentication login console" and "aaa authentication login" configuration commands to make sure that the RADIUS/TACACS+

No.	Failure details	Items to check
		authentication is not set. (For details, see "2.2.3 Login authentication using RADIUS/TACACS+ is not possible".)
6	When the communication speed of the communication software is changed after login, unexpected characters are displayed and no commands can be entered.	Despite changing the communication speed of the communication software after login, correct display is not possible. Restore the original communication speed of the communication software.
7	A user wants to use Tera Term Pro to log in, but unexpected characters are displayed during login.	Negotiation with the communication software might not have been performed correctly. See No. 3. Issue a break signal by simultaneously pressing the [Alt] + [B] keys. Note, however, that the login page might not be displayed unless the break signal is issued several times, depending on the communication speed of Tera Term Pro.
8	Item names and the corresponding contents 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.

Table 2-2 Problems occurring during connection to the modem and action to take

No.	Failure details	Items to check
1	The modem does not answer automatically.	Check the following: - The cables are connected correctly. - The power of the modem is turned on. - The phone number is correctly specified. - The settings for the modem are correct. - If the modem is connected to two 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 the V.90, K56flex, x2, or later communication standards, specify the V.34 or earlier communication mode to connect to the line.
3	After a line disconnection, redialing fails to connect due to a busy line.	After a line is disconnected, the modem might not answer for some seconds. See the documentation for the modem.
4	After a line failure, the connection cannot be re-established.	If a line is disconnected due to a line failure, it might take up to 120 seconds before you can reconnect. If you want to reconnect immediately, log in by another method, and use the "killuser" command to forcibly log out the user connected to the AUX port with a dial-up IP connection.
5	After a line disconnection, the connection cannot be re-established.	If a dial-up IP connection is disconnected, it might take some time before you can reconnect. In such case, wait 300 seconds or so before trying to reconnect.

2.2.2 Login from a remote operation terminal is not possible

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

Table 2-3 Problems occurring during connection to a remote operation terminal and action to take

No.	Symptom	Action or location to check
1	Remote connection is not possible.	Perform the following procedure: 1. Use the "ping" command from a PC or WS to make sure that a route for remote connection has been established.

No.	Symptom	Action or location to check
		2. After the connection established message is displayed, if it takes time before the prompt appears, communication with the DNS server might not be possible. (If communication with the DNS server is not possible, it takes about five minutes before the prompt appears. This time is a general estimate and varies depending on the network status.)
2	Login is not possible.	Perform the following procedure: 1. Make sure that the terminal you are using has an IP or IPv6 address that is permitted in the access list for the configuration command "line vty" mode. Also, make sure that deny is not specified for the IP or IPv6 address set in the configuration command access list. (For details, see "Configuration Guide".) 2. If you log in using local authentication, check whether you are trying to log in using an account that does not exist on the device. 3. Make sure that the maximum number of users who can log in has not been exceeded. (For details, see "Configuration Guide".) If the number of login users has reached the maximum and if connection from a remote operation terminal to the Switch is lost and then restored, no more users will be able to log in from a remote operation terminal until the TCP protocol of the session times out and the session is disconnected. Although the timeout period of the TCP protocol varies depending on the status of a remote operation terminal or the network, the protocol usually times out after 10 minutes. 4. Execute the "transport input" command in the configuration command "line vty" mode to make sure that a protocol for which access to the Switch is prohibited is not used. (For details, see "Configuration Command Reference".) 5. Check whether the RADIUS/TACACS+ authentication is set using the "aaa authentication login" configuration command. (For details, see "2.2.3 Login authentication using RADIUS/TACACS+ is not possible".)
3	Key entry is not accepted.	Perform the following procedure: 1. Data transmission might have been interrupted by XON/XOFF flow control. End the interruption of data transmission (by simultaneously pressing the [Ctrl] + [Q] keys). If the device still does not accept entry from the keys after this operation, perform steps 2 and 3. 2. Make sure that the communication software settings are correct. 3. The screen might not respond because the [Ctrl] + [S] keys were simultaneously pressed. Press any key.
4	A user remains logged in.	Either wait for the user to be automatically logged out, or log in again and delete the login user by using the "killuser" command. If the user was editing the configuration, the editing has not been finished and the configuration might have not been saved. Log in to the device again and enter configuration command mode to save the configuration, and then finish editing.

2.2.3 Login authentication using RADIUS/TACACS+ is not possible

If a login cannot be authenticated by using RADIUS/TACACS+, check the following:

1. Communication with the RADIUS/TACACS+ server
   Use the "ping" command to check if a connection from the Switch to the RADIUS/TACACS+ server has been established. If the connection has not been established, see "7.1.1 Communication is not possible or is disconnected". If a local address is specified in the configuration, use the "ping" command from the local address to make sure that a connection from the Switch to the RADIUS/TACACS+ server has been established.
2. Settings for the timeout value and the number of retries
   For RADIUS authentication, depending on the "radius-server host", "radius-server retransmit", and "radius-server timeout" configuration command settings, the maximum length of time required by the Switch to determine that

the Switch is unable to connect to the RADIUS server is calculated as follows: <Specified timeout value (in seconds)> x <Specified number of retries> x <Specified number of RADIUS servers>.
For TACACS+ authentication, depending on the "tacacs-server host" and "tacacs-server timeout" configuration command settings, the maximum length of time required by the Switch to determine that the Switch is unable to connect to the TACACS+ server is calculated as follows: <Specified timeout value (in seconds)> x <Specified number of TACACS+ servers>. If the time increases significantly, an application on a remote operation terminal, such as Telnet, might have terminated due to a timeout. If this happens, change the RADIUS/TACACS+ configuration settings or the timeout setting of an application running on a remote operation terminal. In addition, Telnet or FTP might have failed even when a message indicating successful RADIUS/TACACS+ authentication is output to the operation log. In this case, an application running on a remote operation terminal might time out before the application can connect to a running RADIUS/TACACS+ server among the RADIUS servers you specified in the configuration. Change the settings so that a running RADIUS/TACACS+ server takes priority, or decrease the value of <Timeout value (in seconds)> x <Number of retries>.

3. Action to take when a login to the Switch is not possible
   If you cannot log in to the Switch due to, for example, incorrect settings, log in from the console and modify the settings. If login authentication has also been implemented on the console by the "aaa authentication login console" configuration command, perform a default restart and then log in.

   Default restart

   Press and hold the RESET button for at least five seconds.

   A startup due to the default restart does not perform authentication by password, authentication when changing to administrator mode ("enable" command), nor command authorization. Therefore, fully exercise caution when performing a default restart. The specified password takes effect after the device restarts.

2.2.4 RADIUS/TACACS+/local command authorization is not possible

After RADIUS, TACACS+, or local authentication is successful and you log in to the Switch, if command authorization fails or if an authorization error message appears indicating that the executed command fails, check the following:

1. Checking with the "show whoami" command
   Use the "show whoami" command for the Switch to display and check the list of operation commands that are permitted or restricted for the current user. Make sure that the command list can be obtained as specified in the settings for the RADIUS/TACACS+ server. Also, if the 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 Switch are correct on the RADIUS/TACACS+ server. Take care with the settings of the vendor-specific attributes for RADIUS, or the service and attribute name settings for TACACS+. Also, if the local command authorization is used, make sure that the settings in the configuration are correct. For details about the RADIUS, TACACS+, and local (configuration) settings, see "Configuration Guide".

   Notes on coding a command list

   Note the handling of space characters when you code a command list for command authorization for the Switch. For example, if "show ip " (i.e., show ip followed by a space) is specified in the authorized command list, the show ip interface is permitted, but the "show ipv6 interface" command is restricted.

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 modify the settings. If command authorization has also been implemented on the console by the "aaa authorization commands console" configuration command, perform a default restart and then log in.

Default restart

Press and hold the RESET button for at least five seconds.

A startup due to the default restart does not perform authentication by password, authentication when changing to administrator mode ("enable" command), nor command authorization. Therefore, fully exercise caution when performing a default restart. The specified password takes effect after the device restarts.

2.3 SSH problems

2.3.1 Unable to connect to the Switch using SSH

If you are unable to connect to the Switch using SSH (ssh, scp, and sftp) from an SSH client on another device, follow the steps below to check the problem.

(1) Check the establishment of the remote connection path

The communication path may not be established between the Switch and the operation terminal. Execute the "ping" command to check the communication path.

(2) Check the SSH server configuration

If the SSH server configuration has not been set, you will not be able to connect to the Switch using SSH. Additionally, if the authentication method does not match between the SSH server settings of the Switch and the SSH client settings of another device, the connection cannot be established.

Make sure that the SSH server information is set correctly in the configuration. If you have specified an access list for remote access control, check that you are connecting from a terminal with a permitted address.

(3) Check whether the correct user public key is registered in the Switch

If you log in to the Switch using public key authentication, check again whether the user public key registered in the configuration of the Switch is the correct one.

Figure 2-2 Example of checking the user public key on the Switch

```
(config)# show ip ssh
ip ssh
ip ssh authkey staff1 key1 "xxxxxx"                    <-1
!


(config)#
```

1. Check whether the correct public key is registered with the correct user name.

(4) Check that the password for the login account has been set

With SSH, if you omit the password during authentication, you will not be able to log in. Set a password for the login account.

(5) Check the number of login users

Execute the "show logging" command to check whether the operation log shown in the following figure is output due to the number of users who try to log in to the Switch has exceeded the maximum number of users that can log in.

Figure 2-3 Example where the maximum number of login users on the Switch has been exceeded

```
> show logging
EVT 04/13 18:03:54 E3 ACCESS 00000003 0207:000000000000 Login refused for too many users logged
in.
```

(6) Check for unauthorized access to the Switch

To prevent unauthorized access, the SSH server function of the Switch not only limits the number of login users, but also limits the number of accesses during the authentication stage before logging in and limits the time required to complete login (2 minutes). Therefore, if you cannot establish the connection using SSH even though the number of

login users on the Switch displayed by the "show sessions" command is small, it is possible that there are still sessions that are connected but not logged in. Check the following:

1. Execute the "show ssh logging" command on the Switch and check the SSH server trace log.
   The following figure shows an example where the connection is denied because too many sessions are connected to the SSH server. The contents in this example will be displayed when there are sessions that are connected but not logged in.

   Figure 2-4 Example where the connection is denied because too many sessions are connected to the SSH server

   ```
   > show ssh logging
   Date 20XX/04/14 19:00:00 UTC
   20XX/04/14 18:50:04 sshd[662] fatal: Login refused for too many sessions.
   20XX/04/14 18:49:50 sshd[638] fatal: Login refused for too many sessions.
   20XX/04/14 18:49:00 sshd[670] fatal: Login refused for too many sessions.
   ```

2. Look into the connection source of an unauthorized session that is connected but not logged in, and take measures such as restricting remote access.
   Note that unauthorized sessions that are connected but not logged in will be released after 2 minutes, and then you will be able to log in again using SSH. For urgent cases, you can forcefully disconnect and release the TCP session using the "clear tcp" command.

(7) Regenerate the host key pair

On the AX3800S and AX3650S series switches, when the device sleep function is used, the host key pair may become invalid, disabling the users to connect to the Switch using SSH from the SSH client of another device. This symptom may occur if you execute the "set ssh hostkey" command immediately before or after the operation message "E3 SOFTWARE 01910405 1001:000000000000 System is going to sleep soon." is output when the Switch goes to sleep.

To recover from this state, execute the "set ssh hostkey" command after cancelling the device sleep and regenerate the host key pair.

2.3.2 Unable to remotely execute commands to the Switch

(1) Check the SSH client specification options

If you execute an operation command (remotely execute a command) from an SSH client of another device to the Switch without logging in using SSH, an error may be displayed without displaying the command execution results. The following figure shows an example where remote execution of a command to the Switch has failed.

Figure 2-5 Example where remote execution of a command to the Switch has failed

```
client-host> ssh operator@myhost show ip arp
operator@myhost's password: ******
Not tty allocation error.
client-host>
```

If you want to remotely execute commands to the Switch without logging in using SSH, you must allocate a virtual terminal using the -t parameter. The following figure shows an example where remote execution of a command to the Switch has succeeded.

Figure 2-6 Example of where remote execution of a command to the Switch has succeeded

```
client-host> ssh -t operator@myhost show ip arp
operator@myhost's password: ******
Date 20XX/04/17 16:59:12 UTC
Total: 2 entries
```

```
 IP Address      Linklayer Address  Netif           Expire    Type
 192.168.0.1     0000.0000.0001    VLAN0001        3h55m56s   arpa
 192.168.0.2     0000.0000.0002    VLAN0001        3h58m56s   arpa
Connection to myhost closed.
client-host>
```

(2) Check the input mode of the command to be executed

The only commands that can be executed remotely to the Switch without logging in using SSH are commands in user mode. An error occurs if a command in administrator mode is executed.

To execute a command in administrator mode, log in to the Switch using SSH and change the mode to administrator mode before executing it.

(3) Check if the command requires y/n entry

Commands that prompt you to enter "(y/n)" in response to a confirmation message, such as the "reload" command, cannot be remotely executed to the Switch. To execute such a command, log in to the Switch using SSH or specify a parameter that forcibly executes the command without outputting the confirmation message (if such a parameter is available).

2.3.3 Unable to execute secure copy to the Switch

Some SSH clients log into an interactive session (CLI) without allocating a virtual terminal, and then transfer files after logging in. The Switch does not support logging into the CLI. Check the trace log on the client side to see if the message shown in the following figure has been sent from the Switch. Secure copy to the Switch cannot be performed from such an SSH client.

Figure 2-7 Trace log on the client side where secure copy to the Switch fails

```
Not tty allocation error.
```

Note that even such an SSH client can transfer files if it supports and uses the secure FTP.

2.3.4 Forgotten the passphrase for public key authentication

If the user has forgotten the passphrase to be entered for logging in to the Switch using SSH public key authentication, the user key pair (user public key and user private key) cannot be used. Take action by following the steps below.

(1) Delete the user public key from the SSH configuration of the Switch

Use the "ip ssh authkey" configuration command of the Switch to delete the user public key of a user who has forgotten their passphrase. The following figure shows an example of deleting a user public key from the SSH configuration of the Switch.

Figure 2-8 Example of deleting a user public key from the SSH configuration of the Switch

```
(config)# show ip ssh
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff1 key1 "xxxxxxxxxx"
ip ssh authkey staff1 key2 "xxxxxxxxxx"
!

(config)# no ip ssh authkey staff1 key1
```

```
(config)# show ip ssh
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff1 key2 "xxxxxxxxxx"
!
```

(2) Delete the user key pair on the SSH client side terminal

On the SSH client side terminal, delete the user key pair (user public key and user private key) of a user who has forgotten the passphrase, and also cancel the registration. To use public key authentication again, recreate the user key pair on the SSH client to be used, and then register the user public key again in the SSH configuration of the Switch.

2.3.5 Warning about a change of the host public key is displayed at connection attempt

When connecting to the Switch from another device using SSH and the message "@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @" is displayed, the host public key on the Switch side has been changed since the previous connection.

If this message is displayed, there is a risk that a malicious third party is impersonating the Switch. Therefore, follow the steps below and check the situation carefully before connecting using SSH.

(1) Contact the device administrator of the Switch

Contact the device administrator to ask the following information.

- Has the host key pair intentionally been changed using the "set ssh hostkey" command?
- Has any change been made to the device configuration?

If the device administrator has not changed the host key pair for the Switch, there is a risk of an impersonation attack or a connection to another host. Interrupt the SSH connection and contact the network administrator. The following figure shows an example of interrupting the SSH connection.

Figure 2-9 Example of interrupting SSH connection

```
client-host> ssh operator@myhost
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
   :
(omitted)
   :
Are you sure you want to continue connecting (yes/no)? no  <-1
Host key verification failed.
client-host>
```

1. Enter "no" here to disable connection.

If there is no risk of impersonation and the host public key of the Switch has been changed, follow the steps below to re-establish the connection.

(2) Re-establish the connection if host public key changes

Use the SSHv2 protocol from an SSH client to connect to the SSH server of the Switch whose host key pair has been changed. To connect more securely, follow the steps below to use the key fingerprint and confirm that the SSH server of the Switch you are trying to connect is the correct connection target host.

1. Check the key fingerprint in advance
   Log in to the Switch in advance and check the key fingerprint using the "show ssh hostkey" command. You can check the key fingerprint more securely by a secure method other than via the network, such as a console connection.
2. Notify the client user of the key fingerprint
   Notify the SSH client user of the checked key fingerprint. You can notify of the key fingerprint more securely by a secure method other than via the network, such as by a postal mail or telephone.
3. Check the key fingerprint and connect using SSH
   On the client, confirm that the key fingerprint displayed when an SSH connection to the SSH server of the Switch is established is the same as the key fingerprint notified in step 2, and then establish the connection.
   Depending on the client, the key fingerprint may be displayed in the HEX format or in bubblebabble format. Also, some SSHv1 protocols do not support key fingerprints. Check the key fingerprint in the format applicable to the client.

(3) Register or delete the host public key database of the user

Depending on the SSH client in use, the host public key of the SSH server for the Switch, which is registered in the host public key database of the user, is not automatically deleted. As the result, the warning may be displayed each time the user tries to establish the connection or the user may not be able to establish the connection. In this case, manually edit or delete the file and re-establish the connection.

2.4 Configuration problems

2.4.1 Returning to administrator mode from configuration command mode is not possible

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:

1. Use the "show sessions" command to check the login number of the target user.

   Example:

   ```
   (config)# $show sessions
   operator console admin 1 Jan 6 14:16
   ```

   The underlined part indicates the login number of the target user.

2. Use the "killuser" command to forcibly log out the target user.
   Specify the login number you checked in step 1 to the <login no.> parameter.

   Example:

   ```
   (config)# $killuser 1
   ```

(2) When connected to a remote operation terminal

Temporarily shut down the remote operation terminal, and then re-establish the connection.

If any user remains logging in, follow No. 4 of "Table 2-3 Problems occurring during connection to a remote operation terminal and action to take" and take measures.

2.5 Stack configuration problems

2.5.1 Stack configuration is not possible

If you cannot configure a stack successfully, check the following in order: the status of member switches, the information about the software licenses and optional licenses, and the status of the stack port.

1. Checking the log
   For details about the log, see "Message Log Reference".
2. Isolating the cause of the problem, from possible causes such as the status of member switches, the information about the software licenses and optional licenses, and the status of the stack port
   Isolate the cause according to the following table.

Table 2-4 Action to take when you cannot configure a stack

No.	Items to check and commands	Action
1	Execute the following command on each member switch to check the state of the switch: show switch detail	If the stack status is Disable, the member switch is running standalone. After setting the "stack enable" configuration command and saving the change to the startup configuration, restart the device and execute the stack function.
		If multiple member switches share the same switch number, you cannot configure a stack. Use the "set switch" command to change the switch number, and make sure that no member switches share the same switch number. To enable the use of the "set switch" command to change switch numbers, you must restart the member switches.
		For other cases, go to No. 2.
2	Execute the following command on each member switch to check the information about the software licenses and optional licenses of the member switch: show license	If there is inconsistency in the functions enabled by the software licenses and optional licenses set for each member switch, you cannot configure a stack. Use the "set license" command or the "erase license" command to ensure consistency in the functions enabled by the software licenses and optional licenses between member switches. To enable license keys applied by using these commands, you must restart the member switches.
		For other cases, go to No. 3.
3	Execute the following commands on each member switch to check the state of the stack ports: show port show switch detail	If Status is not up in the results of executing the "show port" command, see "3.1.1 Ethernet port cannot be connected " and check the Ethernet port status.
		If Status is up in the results of executing the "show port" command, but Status is Down in the results of executing the "show switch" command with the detail parameter specified, there might be a mistake in the configuration of the member switches connected via stack port. Check the configuration as follows: - Switch number and device model settings: Make sure that the switch numbers and device models set by using the "switch provision" configuration command are consistent with the switch numbers and device models of the member switches that are actually connected. - Stack port settings Make sure that the stack ports set by using the stack parameter of the "switchport mode" configuration command are consistent with the ports that are actually connected.

2.5.2 Stack configuration cannot be edited

If you can configure a stack but cannot edit the configuration, check the software information.

Execute the "show version" command on the master switch to check the software information of all member switches in the stack configuration. Even if you already have a stack configuration, the following software information must be consistent when you can edit the configuration:

- Software type (OS-L3M, OS-L3SA, or OS-L3SL)
- Software version

If the above are not consistent, make sure that the software information is consistent for all member switches in the stack configuration.

2.5.3 How to configure a stack with a specific member switch as the master switch

Even if you set a high master selection priority for a member switch you want to make the master switch, and start (or restart) all the member switches in the stack configuration simultaneously, a member switch with a high master selection priority might not become the master switch. This is because the time taken to start up can change due to the following causes, upsetting the synchronization of the startup of member switches:

- The switch is being restarted
- The software type or software version is different
- The startup configuration is different
- The software was updated or upgraded before startup

If you want to fix the member switch that becomes the master switch, configure the stack by using either of the following methods:

- Start up the member switch that you want to make the master switch first. After confirming that this member switch has started and become the master switch, start the remaining member switches.
- Set a value of 2 or greater for the master selection priority of the member switch you want to make the master switch, and set 1 for the master selection priority of the remaining member switches. Afterward, start all the member switches.

2.6 Power saving function problems

2.6.1 Scheduling is disabled

If scheduling is disabled, perform the check procedure described below.

1. Execute the "show power-control schedule" command to check whether the displayed schedule contains the current time, and isolate the cause of the problem according to the following table.

Table 2-5
Power saving function problems that occur when scheduling is used and action to take

No.	Resulting display	Items to check	Cause	Action
1	The current time is not contained.	Check the setting of the "schedule-power-control time-range" configuration command.	The "schedule-power-control time-range" configuration command has not been set correctly.	- Specify an entry that contains the current time if such an entry is not specified. - If "action" for an entry that contains the current time has been set to "disable", delete the entry for which "disable" has been set.
2	The current time is contained.	Check whether the function specified with the "schedule-power-control" configuration does not match the function specified to be used during a normal time range. If they match each other, see the Cause and Action columns.	The function is running as set with the "schedule-power-control" configuration.	Check the setting of the "schedule-power-control" configuration.
3		Execute the "show logging" command to display the log. Confirm that the system time was not changed within 30 minutes before the start time or end time of the schedule. If the system time was changed, see the Cause and Action columns.	A time error has occurred in the schedule due to the change of the system time.	Wait a while. The schedule will automatically start within 30 minutes. For notes on changing the time, see "Configuration Guide".

2.7 NTP communication failures

2.7.1 Unable to synchronize time using NTP

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

Table 2-6 Failure analysis method for NTP

No.	Items to check and commands	Action
1	Use the "show clock" command to make sure that the time zone is set.	If the time zone is set in the information displayed by the command, go to No. 2.
		If the time zone is not set in the information displayed by the command, set the time zone.
2	Check the time difference between the Switch and the NTP server.	If the time difference between the Switch and the NTP server is less than 1000 seconds, go to No. 3.
		If the time difference between the Switch and the NTP server is 1000 seconds or more, use the "set clock" command to match the system clock of the Switch with the NTP server.
3	Check communication with the NTP server via IPv4.	Use the "ping" command to check whether communication is possible via IPv4 between the NTP server and the Switch.
		Make sure that there is no setting for discarding any packets at the UDP port number 123 in the settings of the NTP server or the Switch.

2.8 Memory card problems

2.8.1 Memory card status is not displayed

If the "show system" or "show mc" command displays "MC : --------", check the problem according to the following table.

Table 2-7 Action to take when "MC : --------" is displayed

No.	Items to check and commands	Action
1	Check the ACC LED.	If the ACC LED is lit in 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 lit in green, go to No. 2.
2	Remove the memory card and insert it again.	After removing and inserting the memory card, execute the command again. Before inserting the memory card, check the memory card and memory card slot of the device for dust. If there is dust, wipe it off with a dry cloth and insert the memory card. If you remove and insert the memory card several times but the problem is not resolved, go to No. 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 device.

2.8.2 Error occurs when accessing a memory card

If MC not found. is displayed when a command that accesses the memory card is executed, check the problem and take action according to the following table.

Table 2-8 Action to take when "MC not found." is displayed

No.	Items to check and commands	Action
1	Check the ACC LED.	If the ACC LED is lit in 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 lit in green, go to No. 2.
2	Remove the memory card and insert it again.	After removing and inserting the memory card, execute the command again. Before inserting the memory card, check the memory card and memory card slot of the device for dust. If there is dust, wipe it off with a dry cloth and insert the memory card. If you remove and insert the memory card several times but the problem is not resolved, go to No. 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 device.

2.8.3 Memory card cannot be accessed

If execution of a command to access the memory card fails, check the problem according to the following table.

Table 2-9 Action to take when "MC not found." is displayed

No.	Items to check and commands	Action
1	Check whether the target memory card is one recommended by ALAXALA.	If the memory card is not one recommended by ALAXALA, you may not be able to correctly access the memory card. If the memory card is recommended by ALAXALA, go to No. 2.
2	Check whether the memory card has been formatted on the Switch.	If the memory card recommended by ALAXALA is formatted on another device (such as a PC), you may not be able to correctly access the memory card. Insert the memory card into the Switch and format the memory card by executing the "format mc" command. If the symptom does not improve even after the memory card is formatted on the Switch, go to No. 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 device.

2.9 SNMP communication failures

2.9.1 MIBs cannot be obtained from the SNMP manager

Make sure that the configuration has been set correctly.

When using SNMPv1 or SNMPv2C

Execute the "show access-list" configuration command, and check whether the IP address of the SNMP manager has been set in the access list in the configuration. 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 set, execute the "snmp-server community" configuration command to set information about the SNMP manager.

```
(config)# show access-list
 access-list 1 permit ip 20.1.1.1 0.0.0.255
 !
(config)# show snmp-server
 snmp-server community "event-monitor" ro 1
 !
(config)#
```

When using SNMPv3

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

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

```
(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)#
```

2.9.2 Traps cannot be received by the SNMP manager

Make sure that the configuration has been set correctly.

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 Switch.

If the information has not been set, execute the "snmp-server host" configuration command to set the information about the SNMP manager and traps.

```
(config)# show snmp-server
 snmp-server host    20.1.1.1 traps "event-monitor" snmp
 !
(config)#
```

When using SNMPv3

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

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

```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv notify "view1"
  snmp-server host  20.1.1.1 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)#
```

Some SNMP manager systems might not be able to receive ospf and bgp traps issued under SNMPv2C or SNMPv3. If so, check the trap reception setting for the SNMP manager based on the object ID of each type of traps described in the "MIB Reference".

2.9.3 Inform requests cannot be received by the SNMP manager

Execute the "show snmp-server" configuration command, and check whether the information about the SNMP manager and inform requests has been set in the configuration of the Switch. If the information has not been set, execute the "snmp-server host" configuration command to set the information about the SNMP manager and inform requests.

```
 (config)# show snmp-server
  snmp-server host 20.1.1.1 informs "event-monitor" snmp
 !
(config)#
```

Some SNMP manager systems might not be able to receive ospf and bgp inform requests issued under SNMPv2C or SNMPv3. If so, check the inform request reception setting for the SNMP manager based on the object ID of each type of inform requests described in the "MIB Reference".

3 Troubleshooting of Network Interfaces

This chapter describes what to do when a failure occurs in network interfaces.

3.1 Ethernet communication failures

3.1.1 Ethernet port cannot be connected

If the Ethernet port is suspected as the cause of the communication failure, check the port status and then the port statistics.

(1) Checking the port status

1. Checking the log
   For details about the log, see "Message 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 isolate the cause of the problem according to the following table.

Table 3-1 Checking the port status and action to take

No.	Port status	Cause	Action
1	active up	The target port is running 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, see the relevant descriptions of the "Message Log Reference" and take the action described in Action.
3	inactive	The port is in inactive status due to one of the following reasons: - "inactivate" command - Inactive due to the standby link function of link aggregation - BPDU guard function of a Spanning Tree Protocol - Port resetting function of GSRP - Failure detection in the IEEE 802.3ah/UDLD function - The port is deactivated by the L2 loop detection function - The port is deactivated by the storm control function.	- If the port is deactivated by the standby link function of the link aggregation, this is the normal behavior. Do not activate the port by using the "activate" command. Use the "show channel-group" command with the detail parameter to check the standby link function. - If the port is deactivated by the BPDU guard function of a Spanning Tree Protocol, check the settings of the partner switch, modify the configuration so that the Switch does not receive BPDUs, and use the "activate" command to activate the target port. Use the "show spanning-tree" command with the detail parameter to check the BPDU guard function. - If the port is deactivated by the port resetting function of GSRP, the port will automatically return to the active status. This inactive status of the port is normal. Do not activate the port by using the "activate" command. - If the port is deactivated due to the unidirectional link failure detection or L2 loop detection in the IEEE 802.3ah/UDLD function, see "8.4 IEEE 802.3ah/UDLD function problems". After restoration from the failure, use the "activate" command to activate the target port. - If the port is deactivated by the L2 loop detection function, modify the configuration in which the loop occurs, and then use the "activate" command to activate the target port. Also, if the "loop-detection auto-restore-time" configuration command is specified, the port will automatically return to the active status. - If the port is deactivated by the storm control function, after the LAN is restored from the storm, use the "activate" command to activate the target port. - If any of the reasons described above does not apply and

No.	Port status	Cause	Action
			you want to activate the port, make sure that the cable is connected to the target port, and then use the "activate" command to activate the target port.
4	test	A line test is being performed at the port by the "test interfaces" command.	To resume the communication, use the "no test interfaces" command to stop the line test, and then use the "activate" command to activate the target port.
5	fault	A failure has occurred on the hardware of the target port.	Based on the log entry for the target port displayed by the "show logging" command, see the relevant descriptions of the "Message Log Reference" and take the action described in Action.
6	initialize	The target port is being initialized.	Wait until the initialization is complete.
7	disable or locked	The "shutdown" configuration command is set.	Make sure that the cable is connected to the target port, and set the "no shutdown" configuration command to activate the target port.

(2) Checking statistics

You can use the "show port statistics" command to check the number of sent and received packets and the number of discarded send and receive packets for all ports on the Switch.

Figure 3-1 Display example of port running status check

```
> show port statistics
20XX/03/23 12:00:00
Port Counts:48
Port  Name      Status  T/R   Unicast   Multicast   Broadcast    Discard
0/ 1  geth1/0/1  up     Tx          0           0           0          0
                        Rx          0           0           0          0
0/ 2  geth1/0/2  down   Tx          0           0           0          0
                        Rx          0           0           0          0
0/ 3  geth1/0/3  down   Tx          0           0           0          0
                        Rx          0           0           0          0
       :
>
```

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

3.1.2 Problems in 10BASE-T/100BASE-TX/1000BASE-T/10GBASE-T

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

1. Checking the log
   For details about the log, see "Message Log Reference".
2. Isolating the cause of the problem according to the failure analysis method
   Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-2 Failure analysis method for 10BASE-T/100BASE-TX/1000BASE-T/10GBASE-T problems

No.	Items to check	Cause	Action
1	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - Link down	Line quality is degraded.	Check whether the cable types are correct. For the types, see "Hardware Instruction Manual".
			If the Switch is set as follows, make sure that the pin mapping is for MDI-X. - A fixed connection is set for the target port. - Auto-negotiation is enabled and the AUTO-MDI/MDI-X is disabled for the target port.
			Check the cable length. For the cable length, see "Hardware Instruction Manual".
			Check whether the cables are connected correctly.
			Replace with the connection interface supported by the Switch. For details about the connection interfaces supported by the Switch, see "Configuration Guide".
			Perform a line test on the Switch and make sure that the function of the receiving side has no problem. Check the results of the "no test interfaces" (Ethernet) command, and take the action described in Action. For the test type to be specified, see "10.1 Line test".
2	Use the "show interfaces" command to display the receive error statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - CRC errors - Symbol errors	Line quality is degraded.	Check whether the cable types are correct. For the types, see "Hardware Instruction Manual".
			If the Switch is set as follows, make sure that the pin mapping is for MDI-X. - A fixed connection is set for the target port. - Auto-negotiation is enabled and the AUTO-MDI/MDI-X is disabled for the target port.
			Check the cable length. For the cable length, see "Hardware Instruction Manual".
			Check whether the cables are connected correctly.
			Replace with the connection interface supported by the Switch. For details about the connection interfaces supported by the Switch, see "Configuration Guide".
			Perform a line test on the Switch and make sure that the function of the receiving side has no problem. Check the results of the "no test interfaces" command, and take the action described in Action. For the test type to be specified, see "10.1 Line test".
3	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - MDI cross over changed	The pin mapping of the cable is not correct.	Modify the pin mapping correctly. For details about the pin mapping, see "Configuration Guide".
4	Execute the "show interfaces" command and check the line type and line speed in the detail information	The cable is not compatible.	Check whether the cable types are correct. For the types, see "Hardware Instruction Manual".

No.	Items to check	Cause	Action
	displayed for the target port. If the line type or speed is invalid, see the Cause and Action columns.	The values specified for the "speed" and "duplex" configuration commands are different from those on the remote device.	For the "speed" and "duplex" configuration commands, specify the same values that are 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 "Configuration Guide".
5	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - Long frames	Packets exceeding the maximum allowed frame length are received.	Adjust the jumbo frame settings to those on the remote device.
6	Use the "show qos queueing" command to check whether any of the following statistics items is counted. If any item is counted, see the Cause and Action columns. - discard_pkt	Packets are discarded.	Check whether drop control and the shaper are being used appropriately in the system configuration.

3.1.3 Problems in 100BASE-FX/1000BASE-X

If a 100BASE-FX/1000BASE-X problem occurs, use the procedure below to isolate the failure.

1. Checking the log
   For details about the log, see "Message Log Reference".
2. Isolating the cause of the problem according to the failure analysis method
   Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-3 Failure analysis method for 100BASE-FX/1000BASE-X problems

No.	Items to check	Cause	Action
1	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - Link down - Signal detect errors	Line quality on the receiving side is degraded.	Check the type of the optical fiber. For the types, see "Hardware Instruction Manual".
			If an optical attenuator is used, check the attenuation value. For the optical level, see "Hardware Instruction Manual".
			Check the cable length. For the cable length, see "Hardware Instruction Manual".
			Check whether the cables are connected correctly. Make sure that the end sections 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 on the remote device.

No.	Items to check	Cause	Action
			Comply with the segment standard of the remote device.
			Check whether the optical level is correct. For the optical level, see "Hardware Instruction Manual".
			Perform a line test on the Switch and make sure that the function of the receiving side has no problem. Check the results of the "no test interfaces" command, and take the action described in Action. For the test type to be specified, see "10.1 Line test".
2	Use the "show interfaces" command to display the receive error statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - CRC errors - Symbol errors	Line quality on the receiving side is degraded.	Check the type of the optical fiber. For the mode, see "Hardware Instruction Manual".
			If an optical attenuator is used, check the attenuation value. For the optical level, see "Hardware Instruction Manual".
			Check the cable length. For the cable length, see "Hardware Instruction Manual".
			Check whether the cables are connected correctly. Make sure that the end sections 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 on the remote device.
			Comply with the segment standard of the remote device.
			Check whether the optical level is correct. For the optical level, see "Hardware Instruction Manual".
			Perform a line test on the Switch and make sure that the function of the receiving side has no problem. Check the results of the "no test interfaces" command, and take the action described in Action. For the test type to be specified, see "10.1 Line test".
3	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - TX fault	The transceiver has failed.	Replace the transceiver.
4	If a single-core optical fiber cable such as 1000BASE-BX is used, make sure that the transceiver of the Switch is suitable to use with the remote transceiver.	The combination of the transceivers is incorrect.	If 1000BASE-BX is used, 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.
5	If 100BASE-FX is used, execute the "show interfaces" command and check the line type and line speed in the detail information displayed for the target port. If the line type or speed is invalid, see the Cause and Action columns.	The values specified for the "speed" and "duplex" configuration commands are different from those on the remote device.	For the "speed" and "duplex" configuration commands, specify the same values that are on the remote device.

No.	Items to check	Cause	Action
6	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - Long frames	Packets exceeding the maximum allowed frame length are received.	Adjust the jumbo frame settings to those on the remote device.
7	Use the "show qos queueing" command to check whether any of the following statistics items is counted. If any item is counted, see the Cause and Action columns. - discard_pkt	Packets are discarded.	Check whether drop control and the shaper are being used appropriately in the system configuration.

3.1.4 Problems in 10GBASE-R/40GBASE-R/100GBASE-R

If a 10GBASE-R/40GBASE-R/100GBASE-R problem occurs, use the following procedure to isolate the failure:

1. Checking the log
   For details about the log, see "Message Log Reference".
2. Isolating the cause of the problem according to the failure analysis method
   Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-4 Failure analysis method for 10GBASE-R/40GBASE-R/100GBASE-R problems

No.	Items to check	Cause	Action
1	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - Signal detect errors	Line quality on the receiving side is degraded.	Check the type of the optical fiber. For the types, see "Hardware Instruction Manual".
			If an optical attenuator is used, check the attenuation value. For the optical level, see "Hardware Instruction Manual".
			Check the cable length. For the cable length, see "Hardware Instruction Manual".
			Check whether the cables are connected correctly. Make sure that the end sections 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 standard of the remote device.
			Check whether the optical level is correct. For the optical level, see "Hardware Instruction Manual".
			Perform a line test on the Switch and make sure that the function of the receiving side has no problem. Check the results of the "no test interfaces" command, and take the action described in Action. For the test type to be specified, see "10.1 Line test".
2	Use the "show interfaces" command to display the receive error statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns.	Line quality on the receiving side is degraded.	Check the type of the optical fiber. For the types, see "Hardware Instruction Manual".
			If an optical attenuator is used, check the attenuation value. For the optical level, see "Hardware Instruction Manual".
			Check the cable length. For the cable length, see "Hardware Instruction Manual".

No.	Items to check	Cause	Action
	- CRC errors - Symbol errors		Check whether the cables are connected correctly. Make sure that the end sections 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 standard of the remote device.
			Check whether the optical level is correct. For the optical level, see "Hardware Instruction Manual".
			Perform a line test on the Switch and make sure that the function of the receiving side has no problem. Check the results of the "no test interfaces" command, and take the action described in Action. For the test type to be specified, see "10.1 Line test".
3	Use the "show interfaces" command to display the failure statistics, and check whether any of the following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - Long frames	Packets exceeding the maximum allowed frame length are received.	Adjust the jumbo frame settings to those on the remote device.
4	Use the "show qos queueing" command to check whether any of the following statistics items is counted. If any item is counted, see the Cause and Action columns. - discard_pkt	Packets are discarded.	Check whether drop control and the shaper are being used appropriately in the system configuration.

3.2 Communication failures occurring when the link aggregation is used

If communication is not possible or if degraded operation is in effect when link aggregation is used, isolate the cause of the problem according to the failure analysis method in the following table.

Table 3-5 Communication failure analysis method when link aggregation is used

No.	Items to check and commands	Action
1	Use the "show channel-group" command with the detail parameter specified to check the link aggregation setting that caused the communication failure.	Make sure the link aggregation mode is the same as the mode for the remote device. If the modes are different, modify the link aggregation mode so that it will be the same as the mode for the remote device.
		If the link aggregation modes match, check whether the LACP start method is set to passive for both ports. If passive is set for both ports, change the setting of one of the ports to active.
2	Use the "show channel-group" command with the detail parameter specified to check the running status of the port that caused the communication failure.	Check the status of each port displayed for Status. If all ports of the channel group have gone Down, the channel group also goes Down. Based on the value displayed for Reason, take one of the actions described below on ports that have gone Down. - CH Disabled The link channel group is disabled and DOWN. - Port Down The status of the port is link down. See "3.1 Ethernet communication failures". - 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 avoid the degradation, specify the same speed for all ports in the channel group. - Duplex Half The mode is Half and degradation has occurred. To avoid the degradation, set Duplex mode to Full. - Port Selecting The port aggregation condition check is being performed, and degradation has occurred. Wait for a while, and if the problem is not resolved, check the running status and the settings of the remote device. - Waiting Partner Synchronization The port aggregation condition check has been finished, but degradation has occurred because the system is waiting for the partner port to be synched. Wait for a while, and if the problem is not resolved, check the running status and the 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 avoid the degradation, check the running status of the remote device and also check the wiring. - LACPDU Expired The valid time of the LACPDU from the partner port has expired, and the target port is in a degraded state. Use the "show channel-group statistics" command with the lacp parameter specified to check the statistics for the LACPDU. Also, check the running status of the remote device. - Partner Key Unmatch

No.	Items to check and commands	Action
		The key received from the partner port is different from the Partner Key of the group, and degradation has occurred. To avoid the degradation, check the running status of the remote device and also check the wiring. - Partner Aggregation Individual A "link aggregation impossible" message is received from the partner port, and degradation has occurred. To avoid degradation, check the running status and the settings of the remote device. - Partner Synchronization OUT_OF_SYNC A "synchronization impossible" message is received from the partner port, and degradation has occurred. (This state occurs if the configuration is changed on the Switch or if the line is deactivated on the remote device.) - Port Moved The connected port has been connected to another port. Check the wiring. - Operation of Detach Port Limit The port detachment restriction function is activated, and the channel group is Down.

4 Troubleshooting of Layer 2 Switching

This chapter describes what to do when a failure occurs in layer 2 switching.

4.1 VLAN communication failures

If Layer 2 communication is not possible when VLANs are used, isolate the cause of the problem according to the failure analysis method described in the table below.

(1) Checking the VLAN state

Execute the "show vlan" command or the "show vlan" command with the detail parameter specified to check the status of the VLAN. The following describes the items that must be checked for each VLAN type.

(a) Items checked in common for all VLAN types

- Check whether the VLAN is set up correctly on the port.
- Check whether the correct mode is set for the port. If the expected port does not belong to the default VLAN (VLAN ID 1), check whether:
  - A port VLAN other than VLAN ID 1 is specified for the access VLAN or native VLAN.
  - The default VLAN setting is omitted in "allowed vlan" for trunk ports.
  - The port is specified as a mirror port.
- Check whether IEEE 802.1X VLAN-based authentication (static), Web authentication (fixed VLAN mode), or MAC-based authentication is set only for some of the VLANs set up for trunk ports.

(b) Item checked for protocol VLANs

When you are using a protocol VLAN, execute the "show vlan" command and make sure that the protocol has been set correctly.

```
> show vlan
      :
VLAN ID:100   Type:Protocol based  Status:Up
  Protocol VLAN Information  Name:ipv4
    EtherType:0800,0806  LLC:  Snap-EtherType:
  Learning:On   Uplink-VLAN:      Uplink-Block:    Tag-Translation:
      :
```

(c) Item checked for MAC VLANs

- When you are using a MAC VLAN, execute the "show vlan mac-vlan" command and make sure that the MAC addresses allowed for communication that uses the VLAN have been set correctly. In the example below, the value enclosed in parentheses indicates the function used to register the MAC address.

  [Function used for registration]

  static: The MAC address is set in the configuration.
  dot1x: The MAC address is set by the IEEE 802.1X function.
  wa: The MAC address is set by Web authentication.
  vaa: The MAC address is set by an authentication VLAN.
  macauth: The MAC address is set by MAC-based authentication.

```
> show vlan mac-vlan
      :
VLAN ID:100    MAC Counts:4
   0012.e200.0001 (static)       0012.e200.0002 (static)
   0012.e200.0003 (static)       0012.e200.0004 (dot1x)
```

- Execute the "show vlan mac-vlan" command and make sure that the MAC address set for a VLAN by using the Layer 2 authentication function has not been set for another VLAN in the configuration. In the example below, the

MAC address indicated with an asterisk (*) is disabled because the address has also been set in the configuration.

```
> show vlan mac-vlan
      :
VLAN ID:500    MAC Counts:4
   0012.e200.aa01 (static)       0012.e200.aa02 (static)
   0012.e200.aa03 (static)       0012.e200.aa04 (dot1x)
VLAN ID:600    MAC Counts:1
  * 0012.e200.aa01 (dot1x)
```

(2) Checking the port status

- Execute the "show vlan" command with the detail parameter specified and make sure that the port status is Up. If the port status is Down, see "3.1 Ethernet communication failures".
- Make sure the port status is Forwarding. If it is Blocking, the cause is indicated in parentheses. Check the status of the function that caused the problem.

[Cause]

VLAN: Suspend is specified for the VLAN.

CH: Transfer has been suspended by the link aggregation function.

STP: Transfer has been suspended by the Spanning Tree function.

GSRP: Transfer has been suspended by GSRP.

dot1x: Transfer has been suspended by the IEEE 802.1X function.

CNF: Transfer has been suspended because the configuration cannot be set.

AXRP: Transfer has been suspended by Ring Protocol.

```
> show vlan detail
      :
VLAN ID:100  Type:Protocol based  Status:Up
      :
  Port Information
   1/0/1        Up   Forwarding     Untagged
   1/0/2        Up   Forwarding     Tagged
```

(3) Checking the MAC address table

(a) Checking the status of MAC address learning

- Execute the "show mac-address-table" command and check the information about the destination MAC address that caused the communication failure.

```
> show mac-address-table
Date 20XX/10/29 11:33:50 UTC
MAC address       VLAN   Type     Port-list
0012.e22c.650c      10   Dynamic  1/0/1
0012.e22c.650b       1   Dynamic  1/0/2
       :
```

- Take one of the actions described below according to the value displayed for Type.

[When Dynamic is displayed for Type]

The MAC address learning information might not have been updated. Use the "clear mac-address-table" command to clear the old information. Information can also be updated by sending frames from the destination device.

[When Static is displayed for Type]

Use the "mac-address-table static" configuration command to check the destination port for the transfer.

[When Snoop is displayed for Type]

See "4.5 IGMP snooping communication failures" and "4.6 MLD snooping communication failures".

[When Dot1x is displayed for Type]

See "5.1 Communication failures occurring when IEEE 802.1X is used".

[When Wa is displayed for Type]

See "5.2 Communication failures occurring when Web authentication is used".

[When Macauth is displayed for Type]

See "5.3 Communication failures occurring when MAC-based authentication is used".

- If the target MAC address is not displayed, flooding is performed.
  If the MAC address is not displayed, but communication is still disabled, check whether inter-port relay suppression has been set. Also, check whether a threshold that is too low is set for the storm control function.

(4) Checking frame discarding

Frames might have been discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets".

4.2 VXLAN communication failures

If communication is not possible due to a VXLAN tunnel when the VXLAN function is used, isolate the cause of the problem according to the failure analysis method described in the table below.

Table 4-1 Failure analysis method for VXLAN

No.	Items to check and commands	Action
1	Execute the "show ip arp" command, and check whether the ARP of the next hop is resolved.	If the ARP is resolved, go to No. 2.
		If the ARP is not resolved, check whether the IP network settings between the neighboring device and the Switch are identical.
2	Execute the "show vxlan peers" command, and check the status.	If Up is displayed for Status, go to No. 3.
		If Down is displayed for Status, execute the "show ip route" command and check that the IP address of the VTEP of the partner VXLAN Gateway is registered as a host address in the routing table. If the gateway is not registered, review the routing-related settings. To change Status to Up, the IP address of the VTEP of the partner VXLAN Gateway must be registered as a host address.
3	Execute the "show vxlan statistics" command and check the Encap counter value.	If the Encap value counts up, go to No. 4.
		If the Encap value does not count up, go to No. 5.
4	Execute the "show vxlan statistics" command on the partner VXLAN Gateway and check the Decap counter value.	If the Decap value counts up, perform analysis starting from No. 5 with the partner VXLAN Gateway.
		If the Decap value does not count up, check the settings of the network devices between the VXLAN Gateways.
5	Execute the "show ip interface" command and check the MTU length of the VXLAN Network port.	If the MTU length is set in consideration of the VXLAN header, go to No. 7.
		If the MTU length is not set in consideration of the VXLAN header, review the MTU length setting or use the VXLAN PMTU function. If the VXLAN PMTU function is already used, go to No. 6. Note that the default MTU length is 1500.
6	Execute the "show vxlan" command and check the contents of the VXLAN PMTU function. - Check that the VXLAN PMTU value matches the PMTU threshold. - Make sure that the Port value matches the VXLAN PMTU enabled port.	If the displayed contents and network configuration match, go to No. 7. Note that, depending on the connected terminal, the problem may not be resolved even if the VXLAN PMTU function is used. In that case, delete the VXLAN PMTU function settings and set the MTU length taking into account the VXLAN header.
		If the displayed contents and the network configuration do not match, review the VXLAN PMTU settings.
7	Execute the "show vxlan" command and check the VTEP information. - Make sure that the Source IP value matches the IP address of the VTEP. - Make sure that the Destination IP value matches the IP address of the VTEP of the partner VXLAN Gateway. - Make sure that the VNI value matches the VNI of the partner VXLAN Gateway.	If the displayed contents and network configuration match, go to No. 8.
		If the displayed contents and the network configuration do not match, review the settings for the VXLAN interface. Also, if the displayed contents of Source IP do not match the settings, review the settings for the "interface loopback" command as well.
8	Execute the "show vxlan peers" command and check the display contents shown below. - Make sure that the Source IP value matches the IP address of the VTEP.	If the displayed contents and network configuration match, go to No. 9.
		If the displayed contents and the network configuration do not match, review the settings.

No.	Items to check and commands	Action
	- Make sure that the Destination IP value matches the IP address of the VTEP of the partner VXLAN Gateway. - Make sure that the Nexthop value matches the IP address of the next hop. - Make sure that the VRF value matches the VRF ID set in the "interface loopback" command and set for the VXLAN Network port.	
9	Execute the "show vxlan vni" command, and check the status of the target VNI.	If enable is displayed for Status, go to No. 10.
		If disable is displayed for Status, review the following settings in the VXLAN interface. - source-interface loopback - member vni - destination-ip If the above commands are set, go to No. 10.
10	Execute the "show vxlan vni" command and check the VNI mapping status. - Make sure that the Port value matches the port for a VLAN that is mapped to the VNI. - Make sure that the VLAN value matches the value of a VLAN that is mapped to the VNI.	If the displayed contents and network configuration match, go to No. 11.
		If the VNI, Port, and VLAN mappings do not match the network configuration, review the VNI mapping settings. - VLAN mapping Check the settings for the "vxlan-vni" command in the VLAN. Check the port to which the above VLAN belongs. - Subinterface mapping Check the settings for the "encapslation dot1q" and "vxlan-vni" commands settings in the subinterface. When performing subinterface mapping, make sure that the partner port of the VXLAN Access port is a trunk port.
11	Execute the "show vxlan mac-address-table" command and check the display contents listed below for the destination MAC address that caused the communication failure. If Access is displayed for Port - Make sure that the Connect value matches the VXLAN Access port. - Make sure that the VLAN value matches the VLAN of the VXLAN Access port. - Make sure that the VNI value matches the VNI mapped to the VLAN. If Network is displayed for Port - Make sure that the Connect value matches the IP address of the VTEP of the partner VXLAN Gateway. - Make sure that the VNI value matches the VNI of the partner VXLAN Gateway.	Check that the displayed contents match the network configuration. If they do not match, review the settings. The MAC address learning information might not have been updated. Use the "clear vxlan mac-address-table" command to clear the old information. Information can also be updated by sending frames from the destination device.

4.3 Spanning Tree communication failures

If Layer 2 communication fails or the running status of the Spanning Tree Protocol does not conform to the network configuration when the Spanning Tree function is used, use the analysis method described in the following table and isolate the cause of the problem. For Multiple Spanning Tree, perform the check for each CIST or each MST instance. When checking a root bridge, for example, replace the word "root bridge" with CIST root bridge or root bridge for each MST instance.

Table 4-2 Failure analysis method for Spanning Tree Protocols

No.	Items to check and commands	Action
1	Execute the "show spanning-tree" command for the Spanning Tree Protocol that caused the failure, and then check the running status of the protocol of the Spanning Tree Protocol.	If the displayed status is Enable, go to No. 2.
		If Ring Protocol and PVST+ are used together, but the tree information of the target VLAN is not displayed, go to No. 7.
		If the displayed status is Disable, the Spanning Tree Protocol has stopped. Check the configuration.
		If Ring Protocol and Multiple Spanning Tree are used together, go to No. 8.
		Check whether the number of the PVST+ instances is within the capacity limit.
2	Execute the "show spanning-tree" command for the Spanning Tree Protocol that caused the failure, and then check the bridge ID of the root bridge for the Spanning Tree Protocol.	If the bridge ID of the root bridge indicates the root bridge defined in the network configuration, go to No. 3.
		If the bridge ID of the root bridge does not indicate the root bridge defined in the network configuration, check the network configuration and other configurations.
3	Execute the "show spanning-tree" command for the Spanning Tree Protocol that caused the failure, and then check the port status and port role for the Spanning Tree Protocol.	If the port status and port role for the Spanning Tree Protocol are the same as those defined in the network configuration, go to No. 4.
		If the port status and port role for the Spanning Tree Protocol are different from the network configuration, check the status of neighboring devices and their configurations.
4	Execute the "show spanning-tree statistics" command for the Spanning Tree Protocol that caused the failure, and then check whether BPDUs were sent and received on the failed port.	If the target port is the root port and the BPDU receiving counter counts up, go to No. 5.
		If the target port is the root port and the BPDU receiving counter does not count up, check whether BPDUs are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets". If you do not find any problems, check the neighboring devices.
		If the target port is the designated port and the BPDU sending counter counts up, go to No. 5.
		If the target port is the designated port and the BPDU sending counter does not count up, see "3 Troubleshooting of Network Interfaces".
5	Execute the "show spanning-tree" command with the detail parameter specified for the Spanning Tree Protocol that caused the failure, and then check the bridge ID for the received BPDUs.	Make sure that the root bridge ID and sending bridge identifier for the received BPDUs are the same as those defined in the network configuration. If they are different from the network configuration, check the status of the neighboring devices.
6	Check whether the value for the maximum number of Spanning Tree Protocols, one of which caused the failure, is within the capacity limit.	Set a value within the capacity limit. For details about capacity limits, see "Configuration Guide".

No.	Items to check and commands	Action
7	Make sure that only one VLAN intended to be used in PVST+ mode is set in vlan-mapping for Ring Protocol.	Set the target VLAN in vlan-mapping for Ring Protocol if not set. If multiple VLANs are set in vlan-mapping, specify only one VLAN in the vlan-mapping setting.
8	Make sure that VLANs intended to be used in an MST instance are consistent with those set in vlan-mapping for Ring Protocol.	If any of the target VLANs are not set in vlan-mapping for Ring Protocol, set them to be consistent with the VLANs for Multiple Spanning Tree.

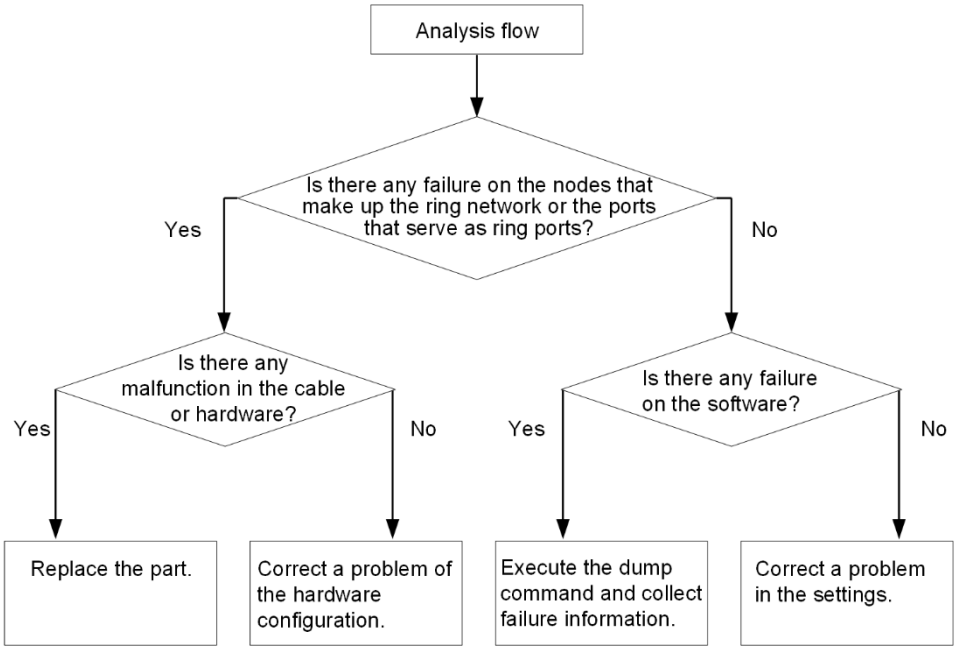
4.4 Ring Protocol communication failures

This section describes failures occurring in the Autonomous Extensible Ring Protocol.

The Autonomous Extensible Ring Protocol (abbreviated hereafter to Ring Protocol) is a Layer 2 network redundancy protocol for ring topologies.

If communication is not possible when the Ring Protocol is used, use the following analysis flowchart to determine the problem and isolate the cause.

Figure 4-1 Analysis flowchart



If the Ring Protocol is used but does not run normally or a ring network failure is detected, use the failure analysis method described in the table below to isolate the cause of the problem for all nodes in the target ring network.

Table 4-3 Failure analysis method for the Ring Protocol

No.	Items to check and commands	Action
1	Use the "show axrp" command and check the running status of the Ring Protocol.	If "enable" is displayed for "Oper State", go to No. 3.
		If a hyphen (-) is displayed for "Oper State", required items for using the Ring Protocol have not been configured. Check the configuration.
		If "disable" is displayed for "Oper State", the Ring Protocol is disabled. Check the configuration.
		If "Not Operating" is displayed for "Oper State", the Ring Protocol function is not running. Check the configuration for any conflict (for example, an incorrect combination of the attribute and ring port for the running mode of the Switch). If the configuration is correct, go to No. 2.
2	Use the "show axrp" command and check the running mode and attribute.	If the running mode and attribute defined in the network configuration are displayed for "Mode" and "Attribute", go to No. 3.
		If any other information is displayed, check the configuration.
3	Use the "show axrp" command and check the ring port and its status for each VLAN group.	If the information about the port and status defined in the network configuration is displayed for "Ring Port" and "Role/State", go to No. 4.
		If any other information is displayed, check the configuration.

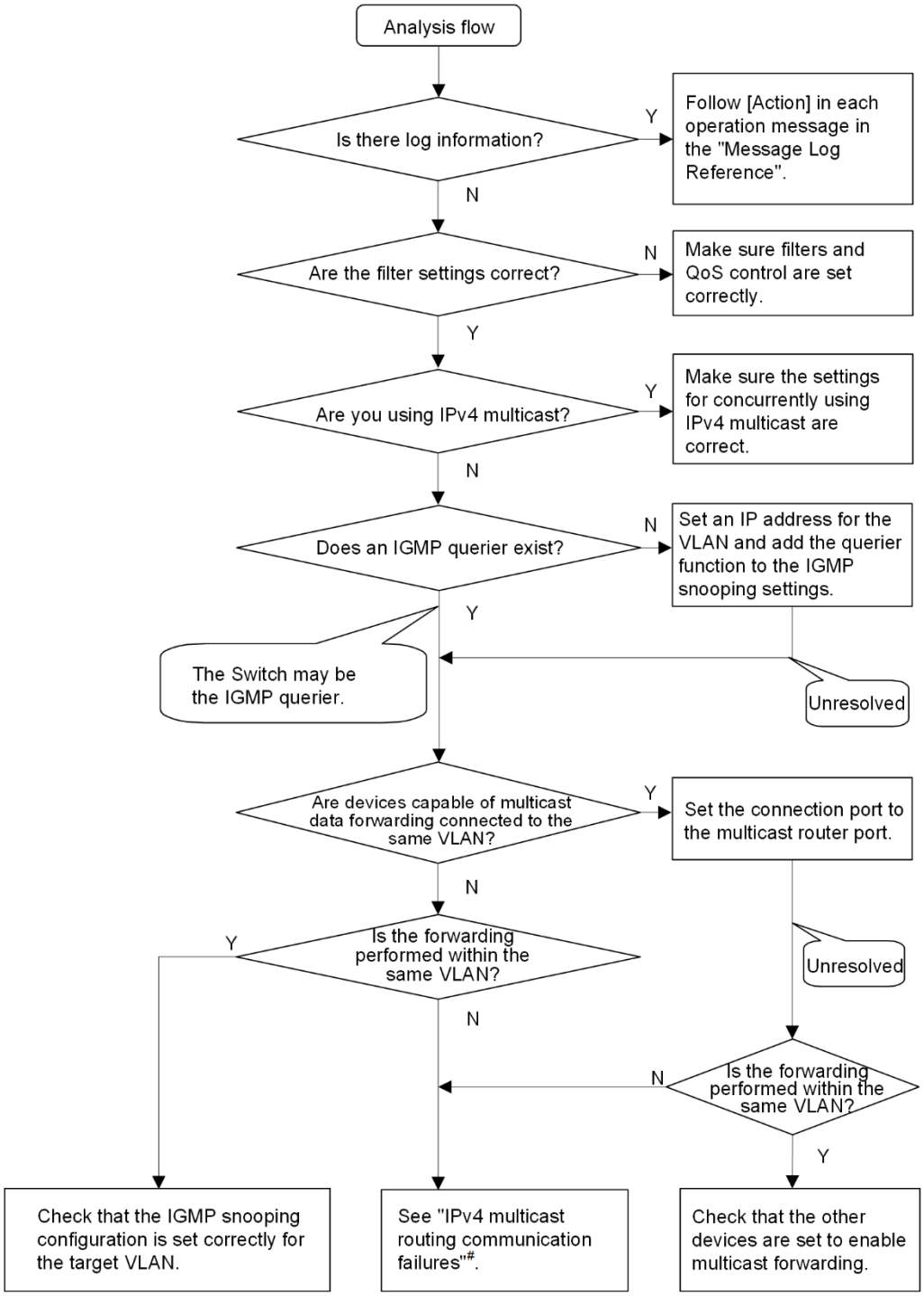
No.	Items to check and commands	Action
4	Use the "show axrp detail" command and check the control VLAN ID.	If the VLAN ID defined in the network configuration is displayed for "Control VLAN ID", go to No. 5.
		If any other information is displayed, check the configuration. For example, the Control VLAN IDs might be different for each device in a ring topology.
5	Use the "show axrp detail" command and check the VLAN IDs that belong to the VLAN group.	If the VLAN IDs defined in the network configuration are displayed for "VLAN ID", go to No. 6.
		If any other information is displayed, check the configuration. For example, the VLAN IDs that belong to the VLAN group might be different for each device in a ring topology.
6	Use the "show axrp detail" command and check the timer value of the health-check frame sending interval and the timer value of the health-check frame hold time.	If the "Health Check Hold Time" timer value of the health-check frame hold time is larger than the "Health Check Interval" timer value of the health-check frame sending interval (i.e., transmission delay is taken into account), go to No. 7.
		If the timer value of the health-check frame hold time is equal to or smaller than that of the health-check frame sending interval (i.e., transmission delay is not taken into account), check and review the settings in the configuration.
7	Use the "show vlan detail" command and check the state of the VLAN used for the Ring Protocol and the VLAN port states.	If there is no anomaly in the states of the VLAN and its ports, go to No. 8. Also, go to No. 9 for the configuration in which a Spanning Tree Protocol or GSRP is used together with the Ring Protocol, go to No. 10 for the configuration in which the multi-fault monitoring function is applied, and go to No. 13 for the stack configuration.
		If there is any anomaly, check the configuration and restore the states of the VLAN and its ports.
8	Check whether the control frames used for Ring Protocol have been discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
9	If a Spanning Tree Protocol or GSRP is set to be used together with the Ring Protocol, check the virtual link settings.	Check whether the virtual link settings in the configuration are the same as those defined in the network configuration. - Check whether the virtual link is set for devices that use a Spanning Tree Protocol or GSRP together with the Ring Protocol. - For devices in the entire ring network, check whether the VLANs used in the virtual link are included in the VLAN group for the Ring Protocol.
10	If the multi-fault monitoring function is applied, use the "show axrp detail" command to check the monitoring mode of the multi-fault monitoring.	If the "monitor-enable" parameter has been specified for shared nodes and the transport-only parameter has been specified for other devices, go to No. 11.
		If any other information is displayed, check the configuration.
11	Use the "show axrp detail" command and check the backup ring IDs and VLAN IDs for the multi-fault monitoring.	If the backup ring ID and the VLAN ID for the multi-fault monitoring defined in the network configuration are displayed for "Backup Ring ID" and "Control VLAN ID", go to No. 12.
		If any other information is displayed, check the configuration.
12	Use the "show axrp detail" command and check the timer value of the multi-fault monitoring frame sending interval and the timer value of the hold time to determine that multiple faults have occurred when multi-fault monitoring frames are not received.	Make sure that the "Multi Fault Detection Hold Time" timer value is larger than the "Multi Fault Detection Interval" timer value (i.e., transmission delay is taken into account).
		If any other information is displayed, check the configuration.

No.	Items to check and commands	Action
13	If a stack is configured, execute the "show qos queueing" command and check whether packets are discarded at the stack port.	When packets are discarded, check whether the stack link has a sufficient bandwidth for the bandwidth used by the ring network. If the stack link bandwidth is insufficient, expand the bandwidth by changing the line type used for stack link or adding more stack links.

4.5 IGMP snooping communication failures

If multicast forwarding is not possible when IGMP snooping is used, use the analysis flowchart shown below and determine the problem and isolate the cause by actions in the following table.

Figure 4-2 Analysis flowchart



#: See "7.4 Communication failures in the IPv4 multicast routing function".

Table 4-4 Failure analysis method for multicast forwarding

No.	Items to check and commands	Action
1	Use the "show logging" command and check whether a failure has occurred.	Check the following: - Check whether log information about a physical failure has been recorded.
2	Check whether the control frames used for IGMP snooping have been discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".

3	Make sure that the settings for simultaneously using IPv4 multicast are correct.	Check the following:
		- Check whether the setting of the "swrt_multicast_table" configuration command is applied.
		If the "swrt_multicast_table" configuration command is correctly set, On is displayed for "Current selected swrt_multicast_table:" when the "show system" command is executed.
		`Current selected swrt_multicast_table: On`
		If Off is displayed when the "swrt_multicast_table" configuration command has been set, the device must be restarted.
		- When using IPv4 multicast and IGMP snooping at the same time, make sure that you use IPv4 multicast on the target VLAN.
		If the IPv4 multicast is used for the target VLAN, On is displayed for "IPv4 Multicast routing:" when the "show igmp-snooping" command is executed.
		`IPv4 Multicast routing: On`
		- If the join static group function of IPv4 multicast is used for the target VLAN, set the multicast router port for ports that require the multicast communication.
		- If the number of entries registered for IGMP snooping exceeds the capacity limit, multicast forwarding entries of IPv4 multicast generated subsequently are for communications only for multicast router ports. Set up the network so that the number of entries registered for IGMP snooping does not exceed the capacity limit.
		If the number of entries registered for IGMP snooping exceeds the capacity limit, the following log information is displayed:
		`IGMP snooping: The number of the IGMP snooping entry exceeded the capacity of this system.`

4	Use the "show igmp-snooping" command and check the IGMP snooping configuration.	Check the following:
		- To check whether the IGMP querier that monitors the group members exists, make sure that one of the following messages is displayed.
		(1) If the IGMP querier exists, the IP address of the IGMP querier is displayed.
		`IGMP querying system: 192.168.11.20#`
		(2) If the IGMP querier does not exist, nothing is displayed for "IGMP querying system:".
		`IGMP querying system:`
		- If the Switch is the IGMP querier, make sure that the IP address has been set for the VLAN.
		(1) If the IP address has been set for the VLAN, the following message is displayed.
		`IP Address: 192.168.11.20#`
		(2) If the IP address has not been set for the VLAN, nothing is displayed for "IP Address:".

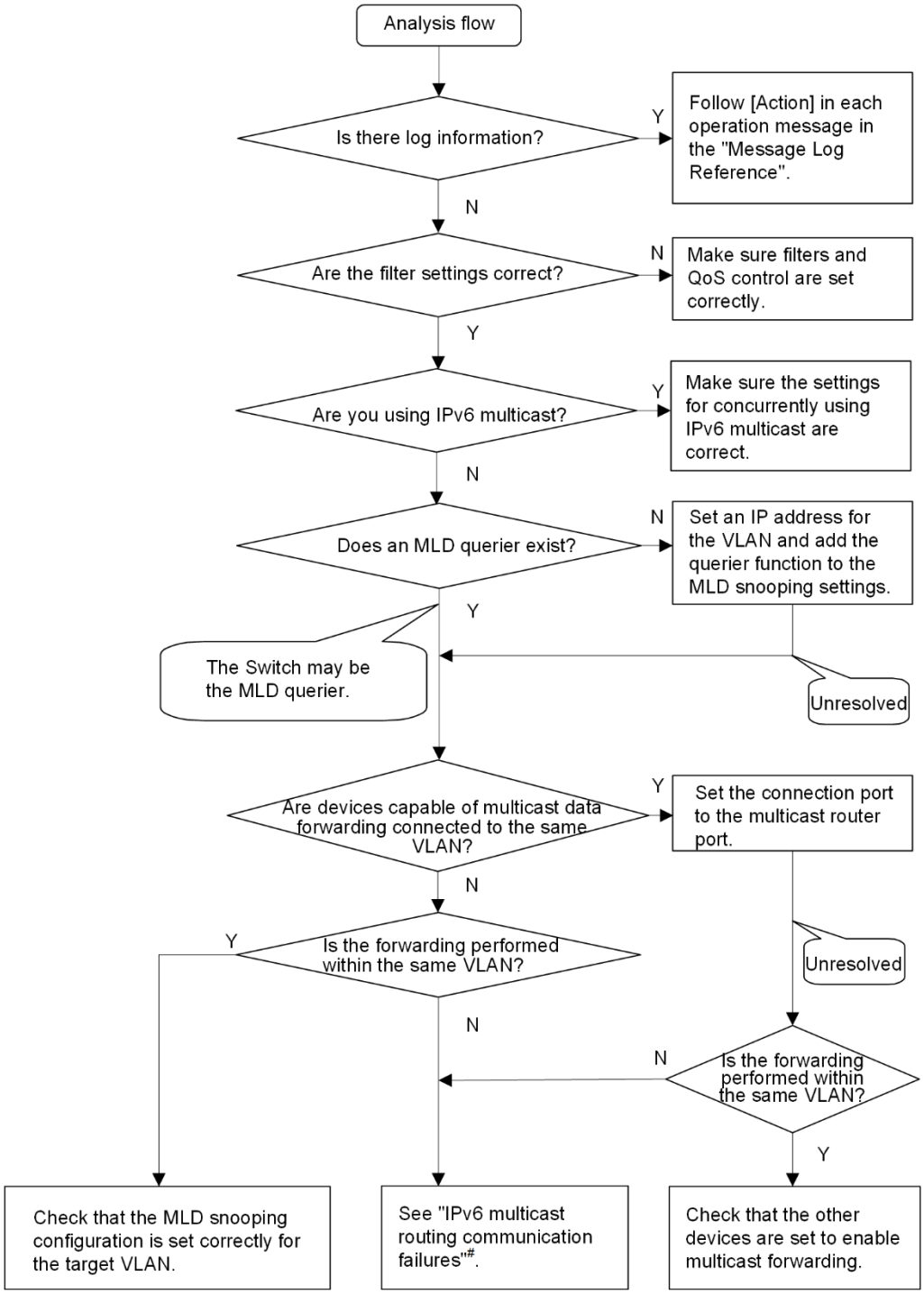
No.	Items to check and commands	Action
		IP Address: - If a multicast router is connected, check the setting of the "mrouter-port" subcommand. > show igmp-snooping 100 Date 20XX/05/15 15:20:00 VLAN 100: IP Address:192.168.11.20 Querier : enable IGMP querying system : 192.168.11.20 Port (2): 0/1,0/3 Mrouter-port:0/1 Group Counts: 3
5	Use the "show igmp-snooping" command with the group parameter specified and check the IPv4 multicast group address.	Check the following: - Make sure that the joined IPv4 multicast group address is displayed by the "show igmp-snooping group" command. > show igmp-snooping group 100 Date 20XX/05/15 15:20:00 VLAN 100 Group counts:3 Group Address MAC Address 224.10.10.10 0100.5e0a.0a0a Port-list 0/1-3 225.10.10.10 0100.5e0a.0a0a Port-list 0/1-2 239.192.1.1 0100.5e40.1606 Port-list 0/1

#: If the Switch is the IGMP querier, the same address is displayed for IGMP querying system and IP Address. If any other device is the IGMP querier, the address displayed for IGMP querying system is not the same as the address displayed for IP Address.

4.6 MLD snooping communication failures

If multicast forwarding is impossible when MLD snooping is used, use the analysis flowchart shown below and determine the problem and isolate the cause by actions in the following table.

Figure 4-3 Analysis flowchart



#: See "7.7 Communication failures in the IPv6 multicast routing function".

Table 4-5 Failure analysis method for multicast forwarding

No.	Items to check and commands	Action
1	Use the "show logging" command and check whether a failure has occurred.	Check the following: - Check whether log information about a physical failure has been recorded.
2	Check whether the control frames used for MLD snooping have been discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".

3	Make sure that the settings for simultaneously using IPv6 multicast are correct.	Check the following:
		- Check whether the setting of the "swrt_multicast_table" configuration command is applied.
		If the "swrt_multicast_table" configuration command is correctly set, On is displayed for "Current selected swrt_multicast_table:" when the "show system" command is executed.
		`Current selected swrt_multicast_table: On`
		If Off is displayed when the "swrt_multicast_table" configuration command has been set, the device must be restarted.
		- When using IPv6 multicast and MLD snooping at the same time, make sure that you use IPv6 multicast on the target VLAN.
		If the IPv6 multicast is used for the target VLAN, On is displayed for "IPv6 Multicast routing:" when the "show mld-snooping" command is executed.
		`IPv6 Multicast routing: On`
		- If the join static group function of IPv6 multicast is used for the target VLAN, set the multicast router port for ports that require the multicast communication.
		- If the number of entries registered for MLD snooping exceeds the capacity limit, multicast forwarding entries of IPv6 multicast generated subsequently are for communications only for multicast router ports. Set up the network so that the number of entries registered for MLD snooping does not exceed the capacity limit.
		If the number of entries registered for MLD snooping exceeds the capacity limit, the following log information is displayed.
		`MLD snooping: The number of the MLD snooping entry exceeded the capacity of this system.`

4	Use the "show mld-snooping" command and check the "MLD snooping" configuration.	Check the following:
		- To check whether the MLD querier that monitors the group members exists, make sure that one of the following messages is displayed.
		(1) If the MLD querier exists, the IP address of the MLD querier is displayed.
		`MLD querying system: fe80::200:87ff:fe10:1959#`
		(2) If the MLD querier does not exist, nothing is displayed for "MLD querying system:".
		`MLD querying system:`
		- If the Switch is the MLD querier, make sure that the IP address has been set for the VLAN.
		(1) If the IP address has been set for the VLAN, the following message is displayed.
		`IP Address: fe80::200:87ff:fe10:1959#`
		(2) If the IP address has not been set for the VLAN, nothing is displayed for "IP Address:".

No.	Items to check and commands	Action
		IP Address: - If a multicast router is connected, check the setting of the "mrouter-port" subcommand. >show mld-snooping 100 Date 20XX/05/15 15:20:00 VLAN 100: IP Address:fe80::200:87ff:fe10:1959 Querier : enable MLD querying system: fe80::200:87ff:fe10:1959 Port(2): 0/1,0/3 Mrouter-port: 0/1 Group Count :3
5	Use the "show mld-snooping" command with the group parameter specified and check the IPv6 multicast group address.	Check the following: - Make sure that the joined IPv6 multicast group address is displayed by the "show mld-snooping group" command. > show mld-snooping group 100 Date 20XX/05/15 15:20:00 VLAN 100 Group count:2 Group Address MAC Address ff0e::0e0a:0a01 3333.0e0a.0a01 Port-list 0/1-3 ff0e::0102:0c11 3333.0102.0c11 Port-list 0/1-2

#: If the Switch is the MLD querier, the same address is displayed for MLD querying system and IP Address. If any other device is the MLD querier, the address displayed for MLD querying system is not the same as the address displayed for IP Address.

5 Troubleshooting of Layer 2 Authentication

This chapter describes what to do when a failure occurs in layer 2 authentication.

5.1 Communication failures occurring when IEEE 802.1X is used

5.1.1 Authentication is not possible when IEEE 802.1X is used

If authentication is not possible when IEEE 802.1X is used, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 5-1 Authentication failure analysis method for IEEE 802.1X

No.	Items to check and commands	Action
1	Use the "show dot1x" command and check the running status of IEEE 802.1X.	If "Dot1x doesn't seem to be running" is displayed, IEEE 802.1X is not running. Check whether the "dot1x system-auth-control" command is set in the configuration. If "System 802.1X : Enable" is displayed, go to No. 2.
2	Execute the "show dot1x statistics" command and check that an EAPOL handshake has been performed.	If the value displayed for RxTotal under [EAPOL frames] is 0, EAPOL frames have not been sent from the terminal. If a value other than 0 is displayed for RxInvalid or RxLenErr, an invalid EAPOL frame has been received from the terminal. If an invalid EAPOL is received, a log will be collected. Use the "show dot1x logging" command to view the log. The "Invalid EAPOL frame received "message is also logged to describe the invalid EAPOL frame. If any of the above conditions exists, check the Supplicant setting on the terminal. For other cases, go to No. 3.
3	Execute the "show dot1x statistics" command and check that data has been sent to the RADIUS server.	If the value displayed for TxNoNakRsp under [EAPoverRADIUS frames] is 0, no data has been sent to the RADIUS server. Check the following: - Check whether aaa authentication dot1x default group radius has been specified in a configuration command. - Check whether the "radius-server host" configuration command is set correctly. - If the authentication mode is port-based authentication or VLAN-based authentication (static), make sure that the authentication terminal has not been registered with the "mac-address-table static" configuration command. For VLAN-based authentication (dynamic), make sure that the authentication terminal has not been registered with the "mac-address" configuration command. - If the authentication mode is VLAN-based authentication (dynamic), check whether aaa authorization network default group radius has been set in a configuration command. For other cases, go to No. 4.
4	Execute the "show dot1x statistics" command and check that packets have been received from the RADIUS server.	If the value displayed for RxTotal under [EAP overRADIUS frames] is 0, packets have not been received from the RADIUS server. Check the following: - If the RADIUS server is associated with the remote network, make sure that a route to the remote network exists. - Make sure that the ports on the RADIUS server are not subject to authentication. For other cases, go to No. 5.
5	Execute the "show dot1x logging" command and check data exchange with the RADIUS server.	- If "Invalid EAP over RADIUS frames received" is displayed, invalid packets are received from the RADIUS server. Check whether the RADIUS server is running normally.

No.	Items to check and commands	Action
		- If "Failed to connect to RADIUS server" is displayed, an attempt to establish a connection with the RADIUS server has failed. Check whether the RADIUS server is running normally. For other cases, go to No. 6.
6	Execute the "show dot1x logging" command and check whether authentication failed.	- If "New Supplicant Auth Fail." is displayed, authentication failed for either of the following reasons. Check for problems. (1) The user ID or password has not been registered on the authentication server. (2) The user ID or password is entered incorrectly. - If "The number of supplicants on the switch is full" is displayed, authentication failed because the maximum number of supplicants for the device was exceeded. - If "The number of supplicants on the interface is full" is displayed, authentication failed because the maximum number of supplicants for the interface was exceeded. - If "Failed to authenticate the supplicant because it could not be registered to mac-address-table." is displayed, authentication was successful, but an attempt to set the MAC address table for the hardware failed. See the appropriate part in the "Message Log Reference", and take the action described in Action. - If "Failed to authenticate the supplicant because it could not be registered to MAC VLAN." is displayed, authentication was successful, but an attempt to set the MAC VLAN table for the hardware failed. See the appropriate part in the "Message Log Reference", and take the action described in Action. If the above does not apply and the port to be authenticated is VLAN-based authentication (dynamic), go to No. 7. For other authentication units, see the RADIUS server log to check whether authentication has failed.
7	Execute the "show dot1x logging" command and check whether dynamic allocation in VLAN-based authentication (dynamic) failed.	- If "Failed to assign VLAN.(Reason: No Tunnel-Type Attribute)" is displayed, dynamic allocation has failed because the Tunnel-Type attribute is not set for the RADIUS attribute of the RADIUS frame. Add the Tunnel-Type attribute in the RADIUS attribute setting of the RADIUS server. - If "Failed to assign VLAN.(Reason:Tunnel-Type Attribute is not VLAN(13))" is displayed, dynamic allocation has failed because the value of the Tunnel-Type attribute for the RADIUS attribute is not VLAN(13). Set VLAN(13) for the Tunnel-Type attribute of the RADIUS server. - If "Failed to assign VLAN.(Reason: No Tunnel-Medium-Type Attribute)" is displayed, dynamic allocation has failed because the Tunnel-Medium-Type attribute is not set for the RADIUS attribute. Set the Tunnel-Medium-Type attribute for the RADIUS attribute of the RADIUS server. - If "Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE 802(6))" is displayed, dynamic allocation has failed. This is because the value of the Tunnel-Medium-Type attribute is not IEEE 802(6) or because the value of the Tunnel-Medium-Type attribute is correct but the tag value does not match the tag of the Tunnel-Type attribute. Set the correct value or tag for the Tunnel-Medium-Type attribute for the RADIUS attribute of the RADIUS server.

No.	Items to check and commands	Action
		- If "Failed to assign VLAN. (Reason: No Tunnel-Private-Group-ID Attribute)" is displayed, dynamic allocation has failed because the Tunnel-Private-Group-ID attribute is not set for the RADIUS attribute of the RADIUS server. Set the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server. - If "Failed to assign VLAN. (Reason: Invalid Tunnel-Private-Group-ID Attribute)" is displayed, dynamic allocation has failed because an invalid value is set for the Tunnel-Private-Group-ID attribute for the RADIUS attribute. Set the correct VLAN ID for the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server. - If "Failed to assign VLAN. (Reason: The VLAN ID is out of range.)" is displayed, dynamic allocation has failed. This is because a VLAN ID that is out of range is set for the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server. Set the correct VLAN ID for the Tunnel-Private-Group-ID attribute. - If "Failed to assign VLAN. (Reason: The port doesn't belong to VLAN.)" is displayed, dynamic allocation has failed. This is because the authentication port does not belong to the VLAN ID specified for the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server. Correct the configuration so that the VLAN ID specified for the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server matches the VLAN ID of the MAC VLAN specified for the authentication port. - If "Failed to assign VLAN. (Reason: The VLAN ID is not set to radius-vlan.)" is displayed, the VLAN ID specified for the Tunnel-Private-Group-ID attribute of the RADIUS attribute of the RADIUS server is not enabled for VLAN-based authentication (dynamic). Correct the configuration so that the VLAN ID specified for the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server matches the VLAN ID of the MAC VLAN specified for the authentication port. If none of the above apply, see the RADIUS server log to check whether authentication has failed.

5.1.2 Communication failures occurring when IEEE 802.1X is used

If communication is not possible on a port or VLAN that uses IEEE 802.1X, isolate the cause of the problem according to the failure analysis method described in the table below. For other cases, see "4 Troubleshooting of Layer 2 Switching".

Table 5-2 Communication failure analysis method for IEEE 802.1X

No.	Items to check and commands	Action
1	Make sure that VLANs with a VLAN-based authentication (static) setting and VLANs with another setting are not set simultaneously for the trunk port.	Communication is possible only for VLANs with a VLAN-based authentication (static) setting. Set all those VLANs for a port excluded from authentication, or set the VLANs with a VLAN-based authentication (static) setting for one port and the VLANs with another setting for another port.
2	Check whether the authenticated terminal has moved to an unauthenticated port in the same VLAN.	If the terminal authenticated on the Switch has moved to an unauthenticated port, communication is disabled until the authentication information is cleared. Use the "clear dot1x auth-state" command to clear the authentication status of the terminal.

5.2 Communication failures occurring when Web authentication is used

5.2.1 Problems occurring when Web authentication is used

If a failure occurs when Web authentication is used, isolate the cause of the problem according to the following table.

Table 5-3 Failure analysis method for Web authentication

No.	Items to check and commands	Action
1	Check whether the login page appears on the terminal.	- If the login page and logout page do not appear, go to No. 2. - If the login page appears in local authentication method, go to No. 5. - If the login page appears in RADIUS authentication method, go to No. 7. - If the operation message is displayed, go to No. 14.
2	Check whether the URLs specified for login and logout are correct.	- If incorrect URLs are specified for login or logout, use the correct URLs. - If the login page or logout page is not displayed in fixed or dynamic VLAN mode, check and modify the following settings: - Check whether the Web authentication IP address has been set in the "web-authentication ip address" configuration command or URL redirection has been enabled by the "web-authentication redirect enable" configuration command. - For other cases, go to No. 3.
3	Make sure that the Web server is running.	- Execute the following command and check whether the Web server is running. If the Web server is running, go to No. 4. [Command] `# ps -auwx | grep httpd` [Check procedure] If /usr/local/sbin/httpd is displayed in the result of the "ps" command, the Web server is running. - If the Web server is not running, check the "web-authentication web-port" configuration command. - If the Web authentication configuration command has been set correctly, use the "restart web-authentication web-server" command to restart the Web server. - If the Web server does not start with the above steps, stop Web authentication by using the "no web-authentication system-auth-control" command, and wait about 10 seconds. After that, use the "web-authentication system-auth-control" configuration command to restart Web authentication.
4	Check the setting of the authentication IPv4 access list.	- If an unauthenticated terminal sends certain types of packets to destinations outside the device, make sure that an authentication IPv4 access list is set. When both a standard access list and an authentication IPv4 access list are set, make sure that the filter conditions in the authentication IPv4 access list are also set in the standard access list. - Make sure that a filter condition for discarding IP packets (such as deny ip) is not set in the standard access list or authentication IPv4 access list. - Make sure that addresses including the Web authentication IP address are not set in the filter conditions in the authentication IPv4 access list. - Make sure that any is not set for the destination IP address in the filter conditions in the authentication IPv4 access list. - For other cases, go to No. 9.
5	Use the "show web-authentication user" command	- If the user ID is not registered, use the "set web-authentication user" command to register the user ID, password, and VLAN ID.

No.	Items to check and commands	Action
	and check whether the user ID is registered.	- For other cases, go to No. 6.
6	Check whether the entered password is correct.	- If the password does not match, use the "set web-authentication passwd" command to change the password. Alternatively, you can use the "remove web-authentication user" command to delete the user ID, and then use the "set web-authentication user" command to register the user ID, password, and VLAN ID again. - For other cases, go to No. 9.
7	Use the "show web-authentication statistics" command and check the communication status with the RADIUS server.	- If the value displayed for "TxTotal" under "[RADIUS frames]" is 0, check whether the "aaa authentication web-authentication default group radius" and "radius-server host" configuration commands have been set correctly. - Even if communication is restored from the no-response state of the RADIUS server caused by the dead interval function, an authentication error occurs. This is because no authentication check is performed on the RADIUS server during the time interval specified by the "authentication radius-server dead-interval" configuration command. In this case, if the authentication failure due to no response from the RADIUS server continues too long, change the setting value of the "authentication radius-server dead-interval" configuration command or execute the "clear web-authentication dead-interval-timer" command. The authentication by the first RADIUS server resumes. - For other cases, go to No. 8.
8	Check whether the password and user ID are registered on the RADIUS server.	- If the user ID is not registered, register it on the RADIUS server. - For other cases, go to No. 9.
9	Use the "show web-authentication statistics" command and check whether Web authentication statistics are displayed.	- If Web authentication statistics are not displayed, go to No. 10. - For other cases, go to No. 11.
10	Check whether the "web-authentication system-auth-control" configuration command has been set.	- If the "web-authentication system-auth-control" configuration command has not been set, set the command. - For other cases, go to No. 11.
11	Execute the "show web-authentication logging" command and check for problems in the authentication.	- If authentication information for the port to which the authentication terminal is connected is not displayed in fixed VLAN mode, use the "web-authentication port" configuration command and check whether the authentication target port has been set correctly. Also, make sure that the authentication target port to which the terminal is connected is neither in the link-down status nor is shut down. - For other cases, go to No. 13.
12	If no account is recorded on the accounting server, use the "show web-authentication statistics" command and check the communication status with the accounting server.	- If the value displayed for "TxTotal" under "[Account frames]" is 0, check whether the "aaa accounting web-authentication default start-stop group radius" and "radius-server host" configuration commands have been set correctly. - For other cases, check the Web authentication configuration.
13	Check whether authentication fails on the connected terminal.	- If a terminal subject to authentication cannot be authenticated at all, use the "restart web-authentication web-server" command to restart the Web server. - If authentication still fails after the Web server restarts, execute the "restart vlan mac-manager" command.

No.	Items to check and commands	Action
		- For other cases, check the Web authentication configuration and correct the configuration.
14	Use the "show logging" command and check the operation log.	- If the following steps are taken, a Web server (httpd) stop message and Web server (httpd) restart message might be displayed in the operation log. (1) Web authentication is stopped (by executing the "no web-authentication system-auth-control" command) and then restarted (by executing the "web-authentication system-auth-control" command). (2) The "restart web-authentication web-server" command is used to restart the Web server. [Web server (httpd) stop message] Level: E7 Message ID: 2a001000 Message: httpd aborted. [Web server (httpd) restart message] Level: R7 Message ID: 2a001000 Message: httpd restarted. These messages indicate that the Web server (httpd) stopped and is automatically restarted. After the Web server (httpd) restarts, the authentication resumes. - For other cases, see "Message Log Reference".

5.2.2 Checking the Web authentication configuration

Check the following for the configuration related to Web authentication.

Table 5-4 Checking the Web authentication configuration

No.	Check point	Items to check
1	Web authentication configuration settings	Make sure that the following configuration commands have been set correctly. <Common configuration> - aaa accounting web-authentication default start-stop group radius - aaa authentication web-authentication default group radius - web-authentication system-auth-control <Settings for dynamic VLAN mode> - web-authentication auto-logout - web-authentication max-timer - web-authentication max-user - web-authentication vlan <Settings for fixed VLAN mode> - web-authentication ip address - web-authentication port - web-authentication static-vlan max-user - web-authentication web-port Additionally, check the settings of the following commands. - authentication arp-relay - authentication ip access-group - web-authentication redirect enable - web-authentication redirect-mode
2	IP address settings for VLAN interfaces	For dynamic VLAN mode, make sure that the IP addresses for the following VLAN interfaces are set correctly:

No.	Check point	Items to check
		- Pre-authentication VLAN - Post-authentication VLAN
3	DHCP relay agent setting	For dynamic VLAN mode, if an external DHCP server is used on an L3 switch, make sure that DHCP relay agents are correctly set between the following VLANs: - Between the pre-authentication VLAN and the VLAN for the server - Between the post-authentication VLAN and the VLAN for the server
4	Filter setting	For dynamic VLAN mode, when the filtering is used for an L3 switch, make sure that the filters are correctly set between the following VLANs: - From the VLAN used for authentication to the post-authentication VLAN: A filter is set to disable all IP communication. - From the post-authentication VLAN to the VLAN used for authentication: A filter is set to forward only communication by Web browsers. Also, check whether specific packets are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets".
5	Check the settings of the access filter for authentication.	For fixed or dynamic VLAN mode, make sure that the filter conditions required for communication from unauthenticated terminals to destinations outside the device have been set correctly by using the "authentication ip access-group" and "ip access-list extended" configuration commands.
6	Check the ARP relay settings.	For fixed or dynamic VLAN mode, make sure that the "authentication arp-relay" configuration command has been set correctly so that unauthenticated terminals can send ARP packets to devices outside the Switch.

5.2.3 Checking the accounting of Web authentication

Check the following for the accounting of Web authentication.

Table 5-5 Checking the accounting for Web authentication

No.	Check point	Items to check
1	Check whether authentication result account logs have been correctly recorded.	- If no authentication state is displayed in the execution result of the "show web-authentication login" command, follow "Table 5-3 Failure analysis method for Web authentication". - If the logs are not recorded on the accounting server, go to No. 2. - If the logs are not recorded on the syslog server, go to No. 3.
2	Use the "show web-authentication statistics" command and check the communication status with the accounting server.	- If the value displayed for "TxTotal" under "[Account frames]" is 0, check whether the "aaa accounting web-authentication default start-stop group radius" or "radius-server host" configuration commands have been set correctly. - For other cases, check the Web authentication configuration.
3	Check the syslog server settings.	Make sure that the following configuration commands have been set correctly. - Make sure that the syslog server has been set by the "logging host" command. - Make sure that aut has been set for the event type in the "logging event-kind" command. - Make sure that the "web-authentication logging enable" command has been set.

5.2.4 Problems occurring when the SSL server certificate and private key are used

For problems related to the operation of SSL server certificates and private keys, isolate the cause of the problem according to the following table.

Table 5-6 Failure analysis method when SSL server certificates and private keys are used

No.	Failure details	Items to check and commands	Action to take
1	The server certificate and private key registered on the authentication terminal cannot be confirmed.	Execute the "ps -axuw | grep httpd" command and check the startup time of the Web server (httpd).	If the startup time of the Web server (httpd) is older than the time when the server certificate and private key were registered, execute the "restart web-authentication web-server" command to restart the Web server.
2	Unable to authenticate after registering a server certificate and private key	Execute the "ps -axuw | grep httpd" command and check whether the Web server (httpd) is running.	If the Web server (httpd) is not running, the combination of the server certificate and private key is incorrect. Follow the steps below to register the correct combination of the server certificate and private key. 1. Execute the "clear web-authentication ssl-crt" command to delete the registered certificate and private key. 2. Execute the "restart web-authentication web-server" command to restart the Web server. 3. Execute the "set web-authentication ssl-crt" command to specify and register the correct server certificate and private key. 4. Execute the "restart web-authentication web-server" again to restart the Web server.
3	The Web server repeats restarting when it is restarted after registration of the server certificate and private key.	Check if a restart message is displayed.	If the Web server (httpd) repeats restarting, take the same action as No. 2.
4	Authentication fails when the server certificate and private key created by the "openssl" command are used.	Check that there are no errors in the settings information or omissions in the creation procedure using the "openssl" command.	- Confirm that the procedure you followed is the same as the procedure described in the "Configuration Guide". - If you have followed the procedure, carry out the items to check and action in No. 1.
5	Parameters cannot be specified with "openssl" command.	Execute the "openssl version" command to check the openssl version.	Use openssl 1.0.2 or newer version.

5.3 Communication failures occurring when MAC-based authentication is used

5.3.1 Problems occurring when MAC-based authentication is used

If a failure occurs when MAC-based authentication is used, isolate the cause of the problem according to the following table.

Table 5-7 Failure analysis method for MAC-based authentication

No.	Items to check and commands	Action
1	Check whether communication with the terminal is possible.	- If authentication in local authentication method is not possible, go to No. 2. - If authentication in RADIUS authentication method is not possible, go to No. 3. - For other cases, go to No. 5.
2	Use the "show mac-authentication mac-address" command and make sure that the MAC address and VLAN ID are registered.	- If the MAC address is not registered, use the "set mac-authentication mac-address" command to register the MAC address and VLAN ID. - For other cases, go to No. 5.
3	Use the "show mac-authentication statistics" command and check the communication status with the RADIUS server.	- If the value displayed for "TxTotal" under "[RADIUS frames]" is 0, check whether the "aaa authentication mac-authentication default group radius", "radius-server host", and "mac-authentication radius-server host" configuration commands have been set correctly. - Even if communication is restored from the no-response state of the RADIUS server caused by the dead interval function, an authentication error occurs. This is because no authentication check is performed on the RADIUS server during the time interval specified by the "authentication radius-server dead-interval" configuration command. In this case, if the authentication failure due to no response from the RADIUS server continues on for too long, change the setting value of the "authentication radius-server dead-interval" configuration command or execute the "clear mac-authentication dead-interval-timer" command. The authentication by the first RADIUS server resumes. - For other cases, go to No. 4.
4	Check whether the MAC address and password are registered on the RADIUS server.	- If the MAC address is not registered as the user ID of the RADIUS server, register the MAC address on the RADIUS server. - If a MAC address is used as the password, set the MAC address that has been set for the user ID. - If a value common to the RADIUS server is set as the password, make sure that the value matches the password set with the "mac-authentication password" configuration command. - For other cases, go to No. 5.
5	Check the setting of the authentication IPv4 access list.	- If an unauthenticated terminal sends certain types of packets to destinations outside the device, make sure that an authentication IPv4 access list is set. When both a standard access list and an authentication IPv4 access list are set, make sure that the filter conditions in the authentication IPv4 access list are also set in the standard access list. - If communication is possible without authentication, make sure that a filter condition for permitting IP packet communication (such as permit ip any) is not set in the access list. - Even if the deny ip any any filter condition is set in the authentication IPv4 access list specified for the authentication target port, MAC-based authentication is

No.	Items to check and commands	Action
		performed depending on the received ARP packets. To remove the target port from the ports subject to MAC-based authentication, use the "no mac-authentication port" configuration command. - For other cases, go to No. 6.
6	Use the "show mac-authentication statistics" command to check whether the MAC-based authentication statistics are displayed.	- If the MAC-based authentication statistics are not displayed, go to No. 7. - For other cases, go to No. 8.
7	Check whether the "mac-authentication system-auth-control" configuration command has been set.	- If the "mac-authentication system-auth-control" configuration command has not been set, set the command. - Check whether the authentication target port is correctly set by the "mac-authentication port" configuration command. - Also, make sure that the authentication target port to which the terminal is connected is neither in the link-down status nor is shut down. - For other cases, go to No. 8.
8	Execute the "show mac-authentication logging" command and check for problems in the authentication.	- If the number of authenticated devices has reached the maximum capacity limit, wait a while until the authentication of another terminal is cancelled. - For other cases, check the MAC-based authentication configuration.

5.3.2 Checking the MAC-based authentication configuration

Check the following for the configuration related to MAC-based authentication.

Table 5-8 Checking the MAC-based authentication configuration

No.	Check point	Items to check
1	MAC-based authentication configuration settings	Make sure that the following configuration commands have been set correctly. - aaa accounting mac-authentication default start-stop group radius - aaa authentication mac-authentication default group radius - mac-authentication password - mac-authentication port - mac-authentication radius-server host - mac-authentication static-vlan max-user - mac-authentication system-auth-control
2	Check the settings of the access filter for authentication.	Make sure that the filter conditions required for communication from unauthenticated terminals to destinations outside the device have been set correctly by using the "authentication ip access-group" and "ip access-list extended" configuration commands.

5.3.3 Checking the accounting of MAC-based authentication

Check the following for the accounting of MAC-based authentication.

Table 5-9 Checking the accounting for MAC-based authentication

No.	Check point	Items to check
1	Check whether authentication result account logs have been	- If no authentication state is displayed in the execution result of the "show mac-authentication login" command, follow "Table 5-7 Failure analysis method for

No.	Check point	Items to check
	correctly recorded.	MAC-based authentication". - If the logs are not recorded on the accounting server, go to No. 2. - If the logs are not recorded on the syslog server, go to No. 3.
2	Use the "show mac-authentication statistics" command and check the communication status with the accounting server.	- If the value displayed for "TxTotal" under "[Account frames]" is 0, check whether the "aaa accounting mac-authentication default start-stop group radius", "radius-server host", or "mac-authentication radius-server host" configuration command has been set correctly. - For other cases, check the MAC-based authentication configuration.
3	Check the syslog server settings.	Make sure that the following configuration commands have been set correctly. - Make sure that the syslog server has been set by the "logging host" command. - Make sure that aut has been set for the event type in the "logging event-kind" command. - Make sure that the "mac-authentication logging enable" command has been set.

5.4 Communication failures occurring when the authentication VLAN is used

5.4.1 Problems occurring when the authentication VLAN is used

If a failure occurs when an authentication VLAN is used, isolate the cause of the problem according to the following table.

Table 5-10 Failure analysis method for the authentication VLAN

No.	Items to check and commands	Action
1	Execute the "show logging" command, and check whether any hardware failure is recorded in the operation log.	- If any hardware failure is recorded in the operation log, replace the device. - For other cases, go to No. 2.
2	Execute the "show fense server" command to make sure that the VLAN is running normally.	- If the error message "Connection failed to VAA program." is displayed, take action described in No. 8. - For other cases, go to No. 3.
3	Execute the "show fense server" command and check the running status of the authentication VLAN.	- If VAA NAME is not set (i.e., "-" is displayed), the "fense vaa-name" command is not set in the configuration. Set the "fense vaa-name" command in the configuration. - If disable is displayed for Status of <vaa_id>, the authentication VLAN is not running. Check the configuration. - For other cases, go to No. 4.
4	Execute the "show fense server" command and check the connection status to the authentication server.	- If the IP address of the authentication server is not displayed for Server Address of <vaa_id>, communication with the authentication server is not possible. That is also the case if the TCP port number of the authentication server is not displayed for Port of VAA IDs. Check the configuration. - If a value other than CONNECTED is displayed for Agent Status of <vaa_id>, the VLAN is not connected to the authentication server. Check the status and settings of the authentication server. - For other cases, go to No. 5.
5	Execute the "show fense server" command with the detail parameter specified and check the setting of the "fense vlan" configuration.	- If no VLAN ID is displayed for <vaa_id> or incorrect information is displayed, there is no VLAN to be switched after authentication of terminals. Check the configuration. - For other cases, go to No. 6.
6	Execute the "show fense statistics" command multiple times and check the connection status to the authentication server.	- If the values of Connect Failure Count and Timeout Disconnect Count increase for <vaa_id>, the connection to the authentication server is unstable. Check the status of the network between the authentication server and authentication VLAN. - If the network status is normal, make sure that the alive-time value set by the "fense alive-timer" configuration command and the setting parameters (HCinterval and RecvMsgTimeout) for the authentication server meet the following conditions. alive-time >= HCinterval + 5 RecvMsgTimeout >= HCinterval + 5 - If the authentication VLAN repeats connecting and disconnecting to the authentication server, use the "restart vaa" command to restart the authentication VLAN. Furthermore, restart VLANaccessController on the authentication server as well as the respective functions of the authentication VLAN. - For other cases, go to No. 7.

No.	Items to check and commands	Action
7	Execute the "show fense statistics" command, and make sure that communication with the MAC VLAN function is running normally.	- If the Request count of VLANaccessAgent Recv Message of <vaa_id> does not match the Request count of Terget-VLAN Registration, an internal inconsistency has occurred. Use the "restart vaa" command to restart the authentication VLAN. - For other cases, go to No. 8.
8	Execute the "show vlan mac-vlan" command, and make sure that authenticated MAC addresses have been registered for the MAC VLAN function.	- If the "show vlan mac-vlan" command shows that authenticated MAC addresses have been registered, authentication of those MAC addresses cannot be enabled. Delete the registered MAC addresses. - If MAC addresses authenticated for each VLAN are not displayed, an internal inconsistency has occurred. Use the "restart vaa" command to restart the authentication VLAN. - If the authentication VLAN restarts but authenticated MAC addresses are not displayed, execute the "restart vlan" command with the mac-manager parameter specified to restart the L2MAC manager program. - For other cases, go to No. 9.
9	Execute the "show fense logging" command and check that communication with the authentication server is running normally.	Check the configuration of the authentication VLAN.

5.4.2 Checking the configuration of the authentication VLAN

Check the following for the configuration related to the authentication VLAN.

Table 5-11 Checking the configuration of the authentication VLAN

No.	Check point	Items to check
1	Authentication VLAN configuration settings	Make sure that the following configuration commands have been set correctly. - fense vaa-name - fense vlan - fense server - fense retry-count - fense retry-timer - fense alive-timer
2	IP address settings for VLAN interfaces	Make sure that the IP addresses for the following VLAN interfaces are set correctly: - VLAN used for authentication - Authenticated VLAN - VLAN for the authentication server - VLAN for the network to be accessed
3	DHCP relay agent settings	Make sure that the DHCP relay agents are correctly set between the following VLANs: - Between the VLAN used for authentication and the VLAN for the authentication server - Between the authenticated VLAN and the VLAN for the authentication server
4	Filter setting	Make sure that the filters are correctly set between the following VLANs: - Between the VLAN used for authentication and the authenticated VLAN: A filter is set to disable all IP communication. - Between the VLAN used for authentication and the VLAN for the authentication server: A filter is set to forward only HTTP, DHCP, and ICMP communication.

No.	Check point	Items to check
		- Between the VLAN used for authentication and the VLAN for the network to be accessed: A filter is set to disable all IP communication. - Between the authenticated VLAN and the VLAN for the authentication server: A filter is set to forward only HTTP, DHCP, and ICMP communication. - Between the VLAN for the authentication server and the VLAN for the network to be accessed: A filter is set to disable all IP communication. Also, check whether specific packets are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets".

6 Troubleshooting of High-reliability Functions

This chapter describes what to do when a failure occurs in high-reliability functions.

6.1 GSRP communication failures

If communication is not possible in a GSRP configuration, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 6-1 How to analyze communication failure in GSRP configuration

No.	Items to check and commands	Action
1	On the Switch and remote device that make up a GSRP group, execute the "show gsrp" command and check the status of the VLAN group containing the target VLAN that causes the communication failure.	If the status of one of them is Master and the status of the other is other than Master, go to No. 2.
		If the status of one of them is Backup(No Neighbor), resolve the communication problem in the direct link. Also, check whether GSRP Advertise frames are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets". If necessary, on the one whose status is Backup(No Neighbor), use the "set gsrp master" command to change the status to Master.
		If the status of both of them is either Backup or Backup(Waiting), make sure that the method for selecting the master or backup status (Selection-Pattern) is the same between the devices.
		If the status of both of them is Backup(Lock), cancel the lock status of one or both of them.
		If the status of both of them is Master, use the "restart gsrp" command to restart the GSRP program on one of them.
		For other cases, the devices are temporarily undergoing a status transition. Wait a while until communication is restored.
2	Check the status of the target VLAN port on the Switch and the devices on the communication path.	If the target VLAN port on the Switch or a device on the communication path has a failure, restore the port or device.
		If all of the following conditions are met, use the "activate" command to activate the target VLAN port. - The method for flushing the MAC address table of the target VLAN port is Reset. (To check this, use the "show gsrp" command with the port parameter specified.)
		If the target VLAN port on the Switch and the devices on the communication path have no problem, go to No. 3.
3	Use the "show gsrp" command with the port parameter specified and check the method (GSRP, Reset, or No) for flushing the MAC address table of the target VLAN port on the Switch.	If the method for flushing the MAC address table is GSRP or Reset and is not suitable for the current GSRP configuration, modify the "gsrp reset-flush-port" or "gsrp no-flush-port" configuration command.
		If the method for flushing the MAC address table is GSRP or Reset and is suitable for the current GSRP configuration, use the "restart gsrp" command to restart the GSRP program on the Switch.
		If the method for flushing the MAC address table is No, wait a while until aging occurs on the MAC address table for the neighboring device on the communication path.

If intended switching between master and backup statuses does not occur in a GSRP configuration, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 6-2 Failure analysis method for state abnormalities in a GSRP configuration

No.	Items to check and commands	Action
1	Use the "show gsrp" command and check the status of the VLAN group in which intended switching between master and backup states does not occur.	If the status of one of them is Master and the status of the other is other than Master, go to No. 2.
		If the status of one of them is Backup(No Neighbor), resolve the communication problem in the direct link. If necessary, also use the "set gsrp master" command for the one whose status is Backup(No Neighbor) to change the status to Master.
		If the status of both of them is either Backup or Backup(Waiting), make sure that the method for selecting the master or backup status (Selection-Pattern) is the same between the devices.
		If the status of both of them is Backup(Lock), cancel the lock status of one or both of them.
		If the status of both of them is Master, use the "restart gsrp" command to restart the GSRP program on one of them.
		For other cases, the devices are temporarily undergoing a status transition. Wait a while.
2	Execute the "show gsrp" and "show gsrp <GSRP-ID> vlan-group <VLAN group ID list>" commands. Based on the information displayed by the commands, make sure that the master and backup states are correctly selected. The information includes the method for selecting the master or backup state (Selection-Pattern), the number of active ports on the Switch and on the remote device (Active-Ports), the priority information (Priority), and the MAC addresses.	If the selected statuses are correct but the number of active ports (Active Ports) does not match the number of up ports (Up Ports), go to No. 3.
		If the selected statuses are not correct, use the "restart gsrp" command to restart the GSRP program on the Switch.
3	Use the "show gsrp detail" and "show gsrp <GSRP-ID> port <Port list>" commands to check the delay time before up ports are counted for the number of active ports (port-up-delay) and also the remaining delay time (delay).	If the delay time (port-up-delay) is infinity and you want to include the number of up ports (UP Ports) in the number of active ports (Active Ports), execute the "clear gsrp port-up-delay" command.
		If the delay time (port-up-delay) is not infinity and the remaining delay time (delay) is not zero, wait a while. The up ports are counted as active ports after the remaining delay time passes. If you want to count the up ports as active ports immediately, execute the "clear gsrp port-up-delay" command.

In a GSRP configuration, if a reception timeout for GSRP Advertise frames is detected and a neighbor unknown state occurs, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 6-3 Failure analysis method when a neighbor unknown state occurs in a GSRP configuration

No.	Items to check and commands	Action
1	Use the "show gsrp detail" command and check the sending interval (Advertise Interval) and retention time (Advertise Hold Time) of GSRP Advertise frames.	If the retention time of GSRP Advertise frames is smaller than or equal to the sending interval of GSRP Advertise frames, set the retention time to a value larger than the sending interval.
		If the retention time of GSRP Advertise frames is larger than the sending interval of GSRP Advertise frames, set the retention time to a value larger than the current value depending on the network environment.
		Check whether GSRP Advertise frames are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking

No.	Items to check and commands	Action
		discarded packets".

6.2 VRRP communication failures

6.2.1 Communication is not possible with the VRRP configuration of IPv4 networks

If communication is not possible in a VRRP configuration, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 6-4 Failure analysis method for VRRP

No.	Items to check and commands	Action
1	On the Switch and remote devices that make up a virtual router, check the status of the virtual router, and check whether only one device is the master router and the others are backup routers.	For devices that make up a virtual router, if only one device is the master router and the others are the backup routers, check the following: - 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 Switch. If there is no problem with the terminal settings and with the routing information of the devices on the communication path, go to No. 2.
		If the status of the virtual router is not correct, go to No. 3.
2	Execute the "show vlan" command with the detail parameter specified, and check that the status of the physical port is Forwarding in the VLAN to which the virtual router is connected.	- If the status of the physical port is Blocking, communication might have been temporarily blocked due to, for example, the topology change for STP. Wait a while, and then make sure that the status of the physical port is Forwarding. If you wait a while but the status of the physical port is not Forwarding, check the configuration and physical network configuration. - If the status of the physical port is down, the port is not physically connected. Check whether connectors and cables are connected correctly.
		If the status of the physical port is Forwarding, check whether the load of the routing destination network is high.
3	For the virtual routers of the Switch and remote devices that make up a virtual router, check whether only one virtual router is the master router.	If multiple virtual routers are master routers, go to No. 4.
		If only one virtual router is the master router, go to No. 8.
4	Check communication between routers that make up the virtual router by using the "ping" command with actual IPv4 addresses.	If communication with actual IPv4 addresses is not possible between routers that make up the virtual router, check the physical network configuration.
		If the result of the "ping" command indicates that communication with actual IPv4 addresses is possible between routers that make up the virtual router, go to No. 5.
5	Use the "show logging" command and the "show vrrpstatus" command with the statistics parameter specified and check the reception status of ADVERTISEMENT packets.	- You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router. In this case, if the value of "<Number of packets> with bad advertisement interval" increases in the statistics, check whether the setting value of the ADVERTISEMENT packet-sending interval matches between the Switch and remote devices. - You might find that the following is registered in the reference log:

No.	Items to check and commands	Action
		Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check. In this case, if the value of "<Number of packets> with authentication failed" increases in the statistics, check whether the authentication password setting matches between the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet with IP TTL not equal to 255. In this case, if the value of "<Number of packets> with bad ip ttl" increases in the statistics, check that there is no other router between the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router. In this case, if the value of "<Number of packets> with bad ip address list" increases in the statistics, make sure that the virtual IP address setting is the same between the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check. In this case, if the value of "<Number of packets> with bad authentication type" increases in the statistics, check whether the authentication password setting exists in the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet that length less than the length of the VRRP header. In this case, if the value of "<Number of packets> with packet length error" increases in the statistics, make sure that the VRRP running mode setting is the same between the Switch and remote devices. - You might find that the following is registered in the reference log: VRRP packet received with unsupported version number. In this case, if the value of "<Number of packets> with invalid type" increases in the statistics, make sure that the VRRP running mode setting is the same between the Switch and remote devices.
		If ADVERTISEMENT packets are received correctly, check the remote device. If ADVERTISEMENT packets are not received, go to No. 6.
6	Execute the "show interfaces" command and check the statistics for the physical port to which a remote device that makes up the same virtual router is connected. Also, execute the "show cpu" command and check the CPU usage.	For the physical port to which a remote device that makes up the same virtual router is connected, you might find that the Input rate and Output rate values are large and the line load is high. In addition, the CPU usage displayed by using the "show cpu" command might be high. If these are the cases, take the following actions: - If a loop occurs in the line, check the use of STP and the physical network configuration, and resolve the loop. - Use the "vrrp timers advertise" configuration command and 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 at the physical port is not high, go to No. 7.
7	Check whether ADVERTISEMENT packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets". If such a filter or QoS is not set, check the running status of the remote device that makes up the same virtual router.

No.	Items to check and commands	Action
		If ADVERTISEMENT packets are not discarded, go to No. 8.
8	If the fault monitoring interface is set, check the status of the fault monitoring interface.	Make sure that another virtual router is set on the interface for which the fault monitoring interface is set and the fault monitoring interface of the virtual router is not the interface of the target virtual router. If the fault monitoring interface of the virtual router is the interface of the target virtual router, delete the setting of either of the fault monitoring interfaces.
		If there is no setting of the fault monitoring interface described above, go to No. 9.
9	Execute the "show vrrpstatus" command with detail parameter specified and check that the status of the virtual router is not Initial.	If the status of the virtual router is Initial, check the following: - If the current priority is not zero, resolve the cause of disabling the virtual router that is displayed for Admin State. (For details about the cause of disabling the virtual router, see "Operation Command Reference".) - Execute the "show logging" command and check the log. If the log contains the message "The VRRP virtual MAC address entry can't be registered at hardware tables.", the setting of the MAC address table has failed on the hardware. The virtual router might be enabled if you do the following. Delete the configuration of the target virtual router, and then set the configuration again with a different virtual router number or change the VLAN ID of the VLAN for which the virtual router is set.
		If the status of the virtual router is not Initial, check the running status of the remote device that makes up the same virtual router.

6.2.2 Communication is not possible with the VRRP configuration of IPv6 networks

If communication is not possible in a VRRP configuration, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 6-5 Failure analysis method for VRRP

No.	Items to check and commands	Action
1	On the Switch and remote devices that make up a virtual router, check the status of the virtual router, and check whether only one device is the master router and the others are backup routers.	For devices that make up a virtual router, if only one device is the master router and the others are the backup routers, check the following: - 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 Switch. If there is no problem with the terminal settings and with the routing information of the devices on the communication path, go to No. 2.
		If the status of the virtual router is not correct, go to No. 3.
2	Execute the "show vlan" command with the detail parameter specified, and check that the status of the physical port is Forwarding in the VLAN to which the virtual router is connected.	- If the status of the physical port is Blocking, communication might have been temporarily blocked due to, for example, the topology change for STP. Wait a while, and then make sure that the status of the physical port is Forwarding. If you wait a while but the status of the physical port is not Forwarding, check the configuration and physical network configuration. - If the status of the physical port is down, the port is not physically

No.	Items to check and commands	Action
		connected. Check whether connectors and cables are connected correctly.
		If the status of the physical port is Forwarding, check whether the load of the routing destination network is high.
3	For the virtual routers of the Switch and remote devices that make up a virtual router, check whether only one virtual router is the master router.	If multiple virtual routers are master routers, go to No. 4.
		If only one virtual router is the master router, go to No. 8.
4	Check communication between routers that make up the virtual router by using the "ping ipv6" command with actual IPv6 addresses.	If communication with actual IPv6 addresses is not possible between routers that make up the virtual router, check the physical network configuration.
		If the result of the "ping ipv6" command indicates that communication with actual IPv6 addresses is possible between routers that make up the virtual router, go to No. 5.
5	Execute the "show vrrpstatus" command with the statistics parameter specified and check the reception status of ADVERTISEMENT packets.	- You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router. In this case, if the value of "<Number of packets> with bad advertisement interval" increases in the statistics, make sure that the setting value of the ADVERTISEMENT packet-sending interval matches between the Switch and remote devices. Also make sure that the VRRP running mode setting matches between them. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check. In this case, if the value of "<Number of packets> with authentication failed" increases in the statistics, make sure that the authentication password setting matches between the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet with IP HopLimit not equal to 255. In this case, if the value of "<Number of packets> with bad ipv6 hoplimit" increases in the statistics, make sure that there is no other router between the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router. In this case, if the value of "<Number of packets> with bad ipv6 address" increases in the statistics, make sure that the virtual IP address setting and VRRP running mode setting are the same between the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check. In this case, if the value of "<Number of packets> with bad authentication type" increases in the statistics, check whether the authentication password setting exists in the Switch and remote devices. - You might find that the following is registered in the reference log: Virtual router <VRID> of <Interface Name> received VRRP packet that length less than the length of the VRRP header. In this case, if the value of "<Number of packets> with packet length error" increases in the statistics, make sure that the VRRP running mode setting is the

No.	Items to check and commands	Action
		same between the Switch and remote devices. - You might find that the following is registered in the reference log: VRRP packet received with unsupported version number. In this case, if the value of "<Number of packets> with invalid type" increases in the statistics, make sure that the VRRP running mode setting is the same between the Switch and remote devices.
		If ADVERTISEMENT packets are received correctly, check the remote device. If ADVERTISEMENT packets are not received, go to No. 6.
6	Execute the "show interfaces" command and check the statistics for the physical port to which a remote device that makes up the same virtual router is connected. Also, execute the "show cpu" command and check the CPU usage.	For the physical port to which a remote device that makes up the same virtual router is connected, you might find that the Input rate and Output rate values are large and the line load is high. In addition, the CPU usage displayed by using the "show cpu" command might be high. If these are the cases, take the following actions: - If a loop occurs in the line, check the use of STP and the physical network configuration, and resolve the loop. - Use the "vrrp timers advertise" configuration command and 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 at the physical port is not high, go to No. 7.
7	Check whether ADVERTISEMENT packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets". If such a filter or QoS is not set, check the running status of the remote device that makes up the same virtual router.
		If ADVERTISEMENT packets are not discarded, go to No. 8.
8	If the fault monitoring interface is set, check the status of the fault monitoring interface.	Make sure that another virtual router is set on the interface for which the fault monitoring interface is set and the fault monitoring interface of the virtual router is not the interface of the target virtual router. If the fault monitoring interface of the virtual router is the interface of the target virtual router, delete the setting of either of the fault monitoring interfaces.
		If there is no setting of the fault monitoring interface described above, go to No. 9.
9	Execute the "show vrrpstatus" command with the detail parameter specified and check the status of the virtual router.	If the status of the virtual router is Initial, check the following: - If the current priority is not zero, resolve the cause of disabling the virtual router that is displayed for Admin State. (For details about the cause of disabling the virtual router, see "Operation Command Reference".) - Execute the "show logging" command and check the log. If the log contains the message "The VRRP virtual MAC address entry can't be registered at hardware tables.", the setting of the MAC address table has failed on the hardware. The virtual router might be enabled if you do the following. Delete the configuration of the target virtual router, and then set the configuration again with a different virtual router number or change the VLAN ID of the VLAN for which the virtual router is set.
		If the status of the virtual router is not Initial, check the running status of the remote device that makes up the same virtual router.

6.3 Uplink redundancy communication failures

6.3.1 Communication is not possible with uplink redundancy

If communication is not possible in an uplink redundancy configuration, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 6-6 Failure analysis method for uplink redundancy

No.	Items to check and commands	Action
1	Execute the "show switchport-backup" command, and make sure that the statuses of the primary and secondary ports are Forwarding or Blocking correctly.	If neither the primary port nor the secondary port is Forwarding, check the following: - If both of them are Blocking, the active port locking function might be enabled. Execute the "show switchport-backup" command and check whether the active port locking function is enabled. If the active port locking function is enabled, wait a while until the primary port is linked up. Alternatively, use the "set switchport-backup active" command to activate the secondary port. - If Down is displayed, check the line status. For the checking method, see "3.1 Ethernet communication failures".
		If there is no problem with the Forwarding or Blocking status of the devices, go to No. 2.
2	Check the upstream devices for the uplink redundancy.	If the upstream devices do not support the flush control frame reception function, check whether the MAC address update function is enabled on the device that uses the uplink redundancy. The MAC address update function might be disabled or the network configuration might not allow MAC address update frames to be received. In such a case, if switchover or switchback occurs due to uplink redundancy, communication of the upstream devices is not restored until the MAC address table is aged out. If this is the case, wait a while and check the communication status again. Alternatively, clear the MAC address table on the upstream devices.
		If the upstream devices support the flush control frame reception function, go to No. 3.
3	Check whether the settings are correct for the VLAN to which flush control frames are sent.	Execute the "show switchport-backup" command, and make sure that the VLAN to which flush control frames are sent is displayed as specified in the configuration. If expected information is not displayed, the settings in the configuration are not correct. Check the settings of the VLAN to which flush control frames are sent and the VLAN settings for the primary and secondary ports in the configuration.
		If the settings are correct for the VLAN to which flush control frames are sent, go to No. 4.
4	Make sure that the upstream devices can receive flush control frames.	Execute the "show logging" command, and check that the upstream devices can receive flush control frames. If the upstream devices cannot receive flush control frames, check whether a VLAN that can receive flush control frames has been set.

7 Troubleshooting of IP and Routing

This chapter describes what to do when a failure occurs in communication and routing on an IP network.

7.1 IPv4 network communication failures

7.1.1 Communication is not possible or is disconnected

There are three probable causes of problems that occur during communication on an IPv4 network employing a Switch:

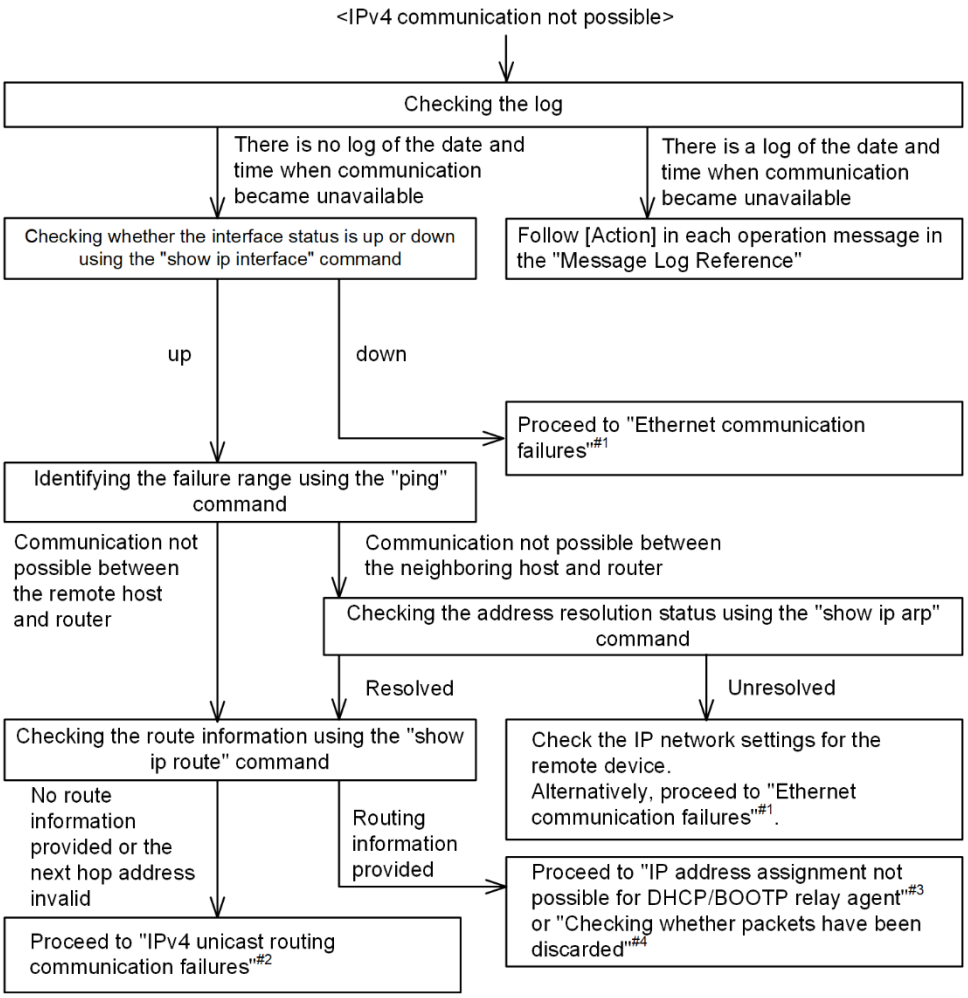
1. A configuration related to IP communication is changed.
2. The network configuration is changed.
3. A network device fails.

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

This subsection describes the procedure for isolating the fault location to identify the cause of a problem, and applies mainly to cause 3 failures. For example, IP communication might not be possible even when the configuration and the network configuration are correct, or when IP communication is disabled even though it was normally performed so far.

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

Figure 7-1 Failure analysis procedure for when IPv4 communication is not possible



#1: See "3.1 Ethernet communication failures".

#2: See "7.3 IPv4 unicast routing communication failures".

#3: See "7.1.2 IP address is not assigned for the DHCP/BOOTP relay agent".

#4: See "10.2 Checking discarded packets".

(1) Checking the log

One probable cause of disabled communication is a line failure (or damage). To display the messages that indicate a hardware failure, carry out the procedure below. You can find these messages in the log displayed by the Switch.

For details about the contents of the log, see "Message Log Reference".

1. Log in to the Switch.
2. Use 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, see "Message Log Reference", and then follow the instructions given in the manual.
5. If a log entry was not displayed for the date and time when communication was disabled, go to "(2) Checking the interface status".

(2) Checking the interface status

Even when the Switch hardware is running normally, a failure could have occurred on the hardware of a neighboring device connected to the Switch.

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

1. Log in to the Switch.
2. Use the "show ip interface" command and check whether the status of the interface between the Switch and the target device is Up or Down.
3. If the status of the target interface is "Down", see "3.1 Ethernet communication failures".
4. If the status of the target interface is "Up", go to "(3) Identifying the range for a failure (from the Switch)".

(3) Identifying the range for a failure (from the Switch)

If a failure has not occurred on the Switch, a failure might have occurred somewhere on the route between the Switch and the remote devices. To identify the range for a failure in order to determine the fault location on the route, do the following:

1. Log in to the Switch.
2. Use the "ping" command and check the communication with the two remote devices that are unable to communicate. For details about examples of using the "ping" command and how to interpret the execution result, see "Configuration Guide".
3. If communication with the remote devices cannot be verified by the "ping" command, execute the command again and check communication with each of the devices up to the remote device, beginning with the device closest to the Switch.
4. If the range for a failure is determined to be a neighboring device as a result of executing the "ping" command, go to "(5) Checking the ARP resolution information with a neighboring device". If the range is determined to be a remote device, go to "(6) Checking the unicast routing information".

(4) Identifying the range for a failure (from a customer's terminal)

To use the customer's terminal to identify the range for a failure so that you can determine the fault location on the route with a remote device in an environment in which login to the Switch is not possible, do the following:

1. Make sure that the customer's terminal has the ping function.

2. Use the ping function and 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 function, use the "ping" command and 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 determine the range for the failure by using the ping function and pinpoint the Switch that is likely to have the failure, log in to the Switch and investigate the cause of the failure based on the failure analysis flowchart.

(5) Checking the ARP resolution information with a neighboring device

If the execution result of the "ping" command indicates that communication with a neighboring device is impossible, the address might not have been resolved by ARP. To check the status of address resolution between the Switch and the neighboring device, do the following:

1. Log in to the Switch.
2. Use the "show ip arp" command and check the status of address resolution (whether ARP entry information exists) between the Switch and the neighboring device.
3. If address resolution with the neighboring device is completed (ARP entry information exists), go to "(6) Checking the unicast routing information".
4. If address resolution with the neighboring device is not completed (no ARP entry information exists), check whether the IP network settings between the neighboring device and the Switch are identical.
5. If DHCP snooping is used, packets might have been discarded by dynamic ARP inspection. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

(6) Checking the unicast routing information

You need to check the routing information obtained by the Switch if (a) communication is still disabled after address resolution with the neighboring device is completed, (b) communication is disabled on the route to the remote device during IPv4 unicast communication, or (c) the route to the remote device has a problem. To carry out the check, do the following:

1. Log in to the Switch.
2. Execute the "show ip route" command and check the routing information obtained by the Switch.
3. If the routing information obtained by the Switch 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, go to "7.3 IPv4 unicast routing communication failures".
4. If the routing information obtained by the Switch contains routing information about the interface that caused the communication failure, the interface might have a problem with any of the functions shown below. Inspect the function associated with the problem.
   - DHCP/BOOTP function
     Go to "(7) Checking the DHCP/BOOTP setting information".
   - Filters, QoS, or DHCP snooping
     Go to "(8) Checking discarded packets".

(7) Checking the DHCP/BOOTP setting information

If IP addresses are assigned to neighboring devices by the relay or server function of DHCP or BOOTP on the Switch, the IP addresses might have not been properly assigned.

Make sure that the setting conditions for the relay or server function of DHCP and BOOTP are correct in the configuration. For the procedure, see "7.1.2 IP address is not assigned for the DHCP/BOOTP relay agent".

(8) Checking discarded packets

Packets might have been discarded by a filter or QoS control. For the checking method and action to take, see "10.2 Checking discarded packets".

In addition, if DHCP snooping is used, packets might have been discarded by a terminal filter. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

7.1.2 IP address is not assigned for the DHCP/BOOTP relay agent

(1) DHCP/BOOTP relay communication problems

There are three probable causes for communication problems on DHCP and BOOTP relays:

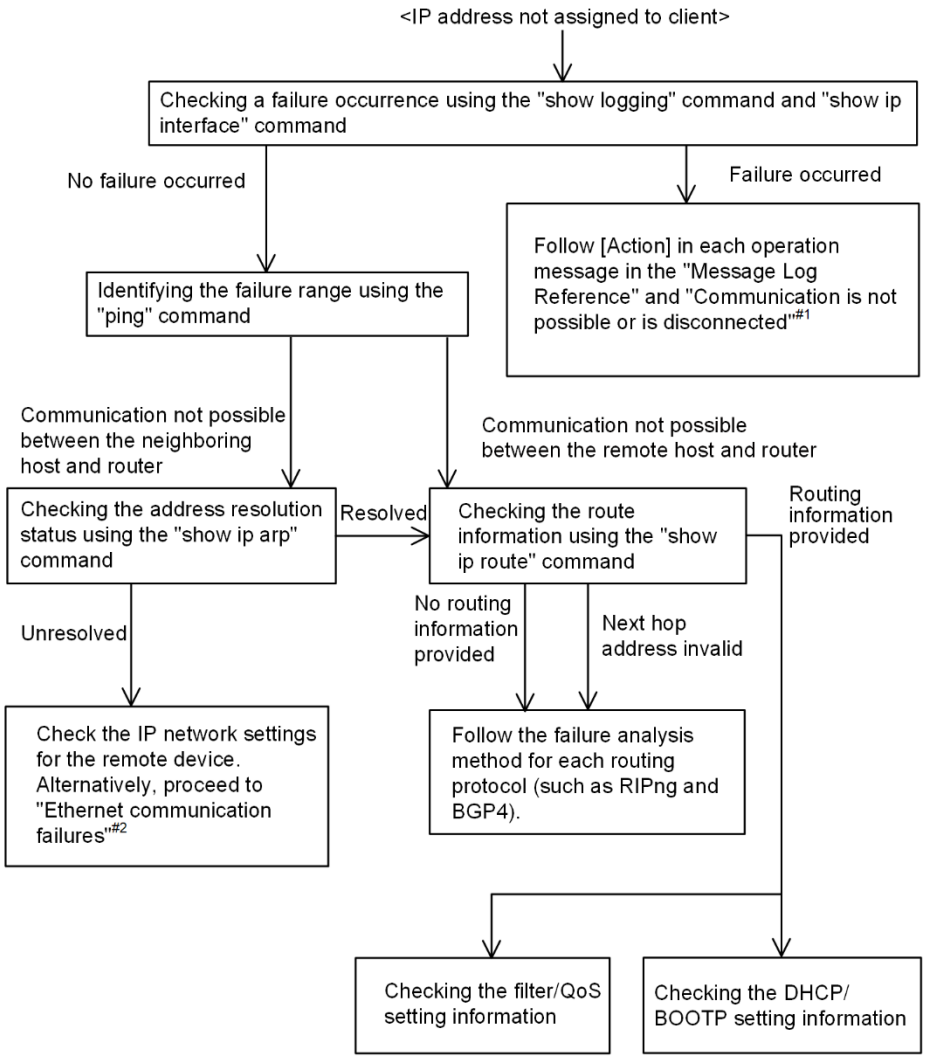
1. A configuration related to the DHCP or BOOTP relay communication is changed.
2. The network configuration is changed.
3. The DHCP or BOOTP server fails.

For cause 2, check the differences in the network configuration before and after the change to uncover any cause that could disable communication.

In this section, ALAXALA Networks Corporation considers a case to which the cause 1 or 3 applies, assuming that you have checked the client settings (such as network card settings and cable connections). This is a case when, for example, after the configuration is changed, the DHCP or BOOTP server cannot assign IP addresses, or when the configuration and network configuration are correct, but IP addresses cannot be assigned to clients and IP communication fails. The following describes the procedure for isolating the fault location to identify the cause of the problem.

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

Figure 7-2 Failure analysis procedure for DHCP/BOOTP relays



#1: See "7.1.1 Communication is not possible or is disconnected".

#2: See "3.1 Ethernet communication failures".

(a) Checking the log and interface

One probable cause of disabled assignment of IP addresses to clients is that communication between the client and the server has been disabled. Check the log displayed by the Switch or use the "show ip interface" command and check whether the interface status is Up or Down. For the procedure, see "7.1.1 Communication is not possible or is disconnected".

(b) Identifying the range for a failure (from the Switch)

If a failure has not occurred on the Switch, a failure might have occurred somewhere on the route between the Switch and the remote device. To identify the range for a failure in order to determine the fault location on the route, do the following:

1. Log in to the Switch.
2. Use the "ping" command and check the communication with the two remote devices that are unable to communicate. For details about examples of using the "ping" command and how to interpret the execution result, see "Configuration Guide".

3. If communication with the remote devices cannot be verified by the "ping" command, execute the command again and check communication with each of the devices up to the remote device, beginning with the device closest to the Switch.
4. If the range for a failure is determined to be a neighboring device as a result of executing the "ping" command, go to "(d) Checking the ARP resolution information with a neighboring device". If the range is determined to be a remote device, go to "(e) Checking the routing information".

(c) Identifying the range for a failure (from a customer's terminal)

To use the customer's terminal to identify the range for a failure so that you can determine the fault location on the route with a remote device in an environment in which login to the Switch is not possible, do the following:

1. Make sure that the customer's terminal has the ping function.
2. Use the ping function and 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 function, use the "ping" command and 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 determine the range for the failure by using the ping function and pinpoint the Switch that is likely to have the failure, log in to the Switch and investigate the cause of the failure based on the failure analysis flowchart.

(d) Checking the ARP resolution information with a neighboring device

If the execution result of the "ping" command indicates that communication with a neighboring device is impossible, the address might not have been resolved by ARP. To check the status of address resolution between the Switch and the neighboring device, do the following:

1. Log in to the Switch.
2. Use the "show ip arp" command and check the status of address resolution (whether ARP entry information exists) between the Switch and the neighboring device.
3. If address resolution with the neighboring device is completed (ARP entry information exists), go to "(e) Checking the routing information".
4. If address resolution with the neighboring device is not completed (no ARP entry information exists), check whether the IP network settings between the neighboring device and the Switch are identical.
5. If DHCP snooping is used, packets might have been discarded by dynamic ARP inspection. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

(e) Checking the routing information

You need to check the routing information obtained by the Switch if (a) communication is still disabled after address resolution with the neighboring device is completed, (b) communication is disabled on the route to the remote device, or (c) the route to the remote device has a problem. To carry out the check, do the following:

1. Log in to the Switch.
2. Use the "show ip route" command and check the routing information obtained by the Switch.
3. If the routing information obtained by the Switch 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, go to "7.3 IPv4 unicast routing communication failures".
4. If the routing information obtained by the Switch contains routing information about the interface that caused the communication failure, the interface might have a problem with any of the functions shown below. Inspect the

function associated with the problem.

- Filters, QoS, or DHCP snooping
  Go to "(f) Checking discarded packets".
- DHCP/BOOTP function
  Go to "(g) Checking the DHCP/BOOTP setting information".

(f) Checking discarded packets

Packets might have been discarded by a filter or QoS control. For the checking method and action to take, see "10.2 Checking discarded packets".

In addition, if DHCP snooping is used, packets might have been discarded by a terminal filter. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

(g) Checking the DHCP/BOOTP setting information

If many of the IP addresses to be leased are left on the DHCP or BOOTP server, it can be assumed that IP addresses cannot be assigned to clients due to incorrect configuration settings for the DHCP or BOOTP relay. The following describes the procedure for checking the configuration.

1. Check whether the IP address of the DHCP or BOOTP server or the IP address of the next router with the DHCP or BOOTP relay agent function is set for ip helper-address.
2. Check whether ip helper-address is set for the client interface.
3. Check whether the value of ip bootp-hops is set to a bootp hops value that is correct from the viewpoint of the client.
4. For a multihomed configuration, check whether the value of ip relay-agent-address is the same as the subnet of the IP address distributed by the DHCP or BOOTP server.
5. If DHCP snooping is used, packets might have been discarded by DHCP snooping. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

(h) Checking when the DHCP relay and VRRP are operated on the same interface

If the DHCP or BOOTP relay and VRRP are operated on the same interface, the DHCP or BOOTP client gateway address (router option) on the DHCP or BOOTP server must be set to the virtual router address that is set in the VRRP configuration. If the gateway address is not set as above, after switching between the master and standby routers is performed by VRRP, the communication of the DHCP or BOOTP clients might be disabled. To check the settings, follow the procedure for checking the settings for each DHCP or BOOTP server.

(2) Communication problems on the DHCP server

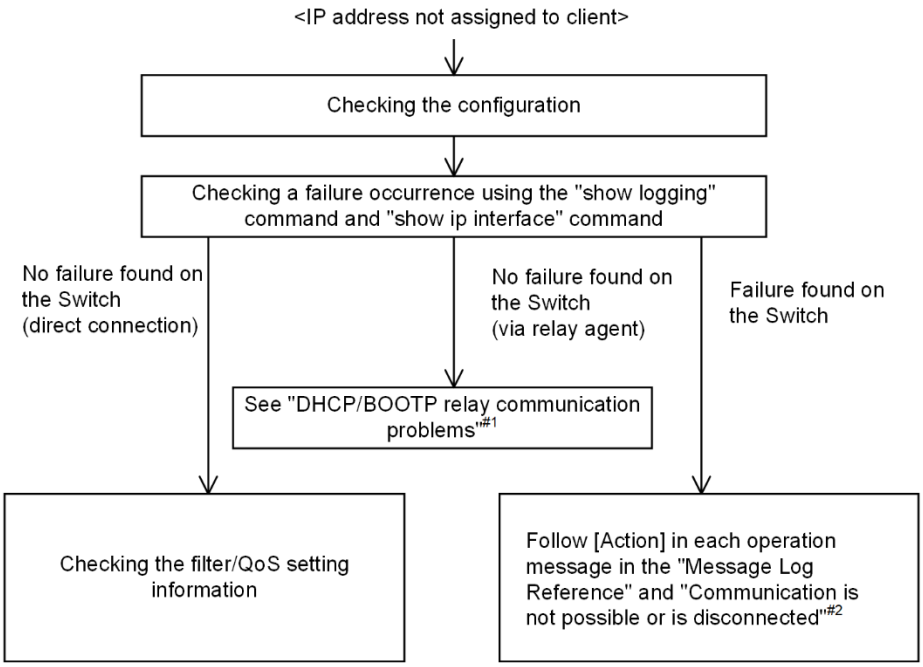
There are three probable causes for problems (such as disabled address distribution to clients) that might occur during communication with the DHCP server:

1. A configuration is set incorrectly.
2. The network configuration is changed.
3. The DHCP server fails.

First, check for cause 1. Described below are likely examples of incorrect configuration. For cause 2, check the differences in the network configuration before and after the change to uncover any cause that could disable communication. You might have checked the client and server settings (such as network card settings and cable connections) and concluded that cause 3 applies. For example, the configuration and network configuration are correct, but IP communication is not possible due to disabled allocation of IP addresses to clients. In such a case, see "(b) Checking the operation messages and interface" through "(e) Checking discarded packets" for details.

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

Figure 7-3 Failure analysis procedure for DHCP servers



#1: See "(1) DHCP/BOOTP relay communication problems".

#2: See "7.1.1 Communication is not possible or is disconnected".

(a) Checking the configuration

It can be assumed that IP addresses cannot be assigned to clients because the resources on the DHCP server are configured incorrectly. To check the configuration, do the following:

1. In the configuration, make sure that there is an ip dhcp pool setting that contains the network setting for the IP addresses to be assigned to the DHCP clients.
2. In the configuration, make sure that the number of DHCP address pools to be assigned to a DHCP client is larger than the number of concurrently used clients set in the "ip dhcp excluded-address" configuration command.
3. If the Switch has assigned addresses to the clients but the clients cannot communicate with other devices, the default router might have not been set. Make sure that the router address (default router) of the network to which the clients are connected has been set by the "default-router" configuration command (see "Configuration Command Reference").
4. Check the settings of the device used as the DHCP relay agent. If the Switch is used also as the relay agent, see "(1) DHCP/BOOTP relay communication problems".
5. If DHCP snooping is used, packets might have been discarded by DHCP snooping. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

(b) Checking the operation messages and interface

One probable cause of disabled assignment of IP addresses to clients is that communication between the client and the server has been disabled. Check the operation messages displayed by the Switch or use the "show ip interface" command and check whether the interface status is Up or Down. For the procedure, see "7.1.1 Communication is not possible or is disconnected".

(c) Identifying the range for a failure (from the Switch)

If a failure has not occurred on the Switch, a failure might have occurred somewhere on the route between the Switch and the remote device. To identify the range for a failure in order to determine the fault location on the route, do the following:

1. Log in to the Switch.
2. If there are devices such as a router between the client and the server, use the "ping" command and check the communication between the router and the remote device (DHCP client). If the communication with the remote device cannot be verified by using the "ping" command, execute the "ping" command again and check communication with each of the devices up to the client, beginning with the device closest to the Switch. For details about examples of using the "ping" command and how to interpret the execution result, see "Configuration Guide".
3. If the server and the client are directly connected, check the hub and cable connections.
4. Select a suitable next step in the failure analysis flowchart depending on whether the range for the failure determined by the "ping" command is in the neighboring device or remote device.

(d) Checking the routing information

You need to check the routing information obtained by the Switch if (a) communication is still disabled after address resolution with the neighboring device is completed, (b) communication is disabled on the route to the remote device, or (c) the route to the remote device has a problem. To carry out the check, do the following:

1. Log in to the Switch.
2. Use the "show ip route" command and check the routing information obtained by the Switch.

(e) Checking discarded packets

Packets might have been discarded by a filter or QoS control. For the checking method and action to take, see "10.2 Checking discarded packets".

In addition, if DHCP snooping is used, packets might have been discarded by a terminal filter. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

(f) Checking the Layer 2 network

If you do not find any incorrect settings or a failure in the steps (a) to (e), there might be a problem with the Layer 2 network. See "4 Troubleshooting of Layer 2 Switching" and check the Layer 2 network.

7.1.3 Dynamic DNS link of the DHCP server function does not work

(1) Communication problems on the DHCP server

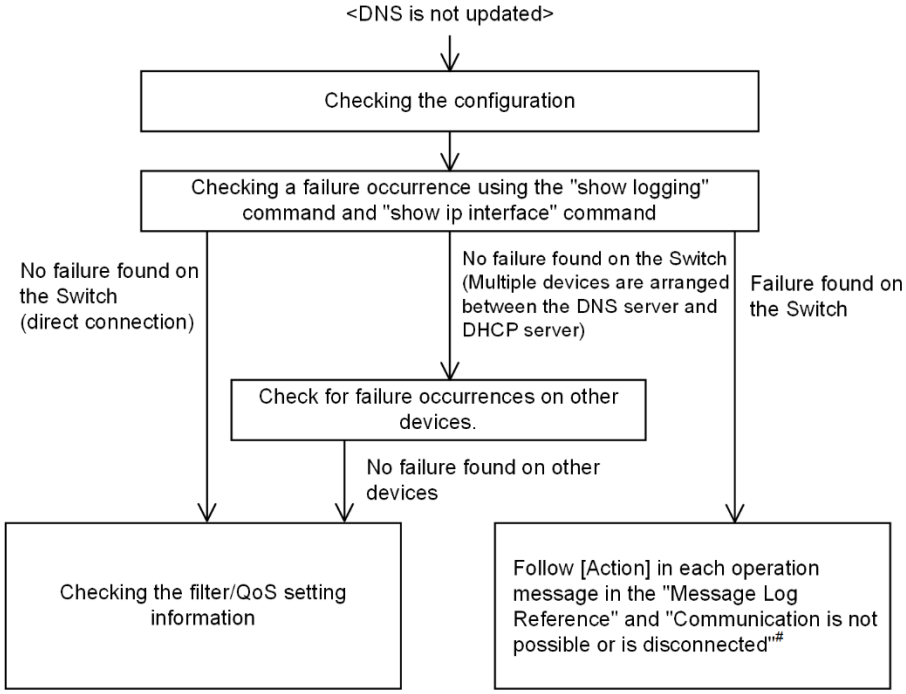
There are three probable causes for communication problems on a DHCP server:

1. A configuration is set incorrectly.
2. The network configuration is changed.
3. The DHCP server fails.

First, check for cause 1. Described below are likely examples of incorrect configuration. For cause 2, check the differences in the network configuration before and after the change to uncover any cause that could disable communication. You might have checked the settings of the DNS server and DHCP server (such as network card settings and cable connections) and concluded that cause 3 applies. For example, the configuration and network configuration are correct, but the Dynamic DNS link does not work. In such a case, see "(b) Checking the time information" through "(f) Checking discarded packets" for details.

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

Figure 7-4 Failure analysis procedure for DHCP servers with DNS link established



#: See "7.1.1 Communication is not possible or is disconnected".

(a) Checking the configuration

The probable cause is that DNS updating is not working properly for Dynamic DNS because some settings on the DHCP server are incorrect or not consistent with the settings on the DNS server. To check the configuration, do the following:

1. First, check the method for permitting DNS updating on the DNS server. For access permission based on IP addresses and networks, see the items 3 onwards. For permission based on authentication keys, see the items 2 onwards.
2. Make sure that the key information and the authentication key specified on the DNS server are consistent with the key information included in the DHCP server configuration (see "Configuration Command Reference").
3. Make sure that the zone information specified on the DNS server is consistent with the zone information included in the DHCP server configuration (see "Configuration Command Reference"). Also, make sure that both the normal and reverse lookups are set.
4. Make sure that DNS updating is set (see "Configuration Command Reference"). This setting is required to enable DNS updating because DNS updating is disabled by default.
5. Make sure that the domain name used by the client is consistent with the domain name registered in the DNS server. If the DHCP is used to distribute domain names, make sure that the setting is correct in the configuration (see "Configuration Command Reference" and "Operation Command Reference").

(b) Checking the time information

If an authentication key is used in DNS updating, in most cases, the difference between the UTC time on the Switch and that on the DNS server must be five minutes or less. Use the "show clock" command and check the time information on the Switch. If necessary, see "Configuration Command Reference" and synchronize the time information.

(c) Checking the operation messages and interface

One of the causes of the failure in communication with the DNS server might be the communication failure between the DNS server and the DHCP server. Check the operation messages displayed by the Switch or use the "show ip interface" command and check whether the interface status is Up or Down. For the procedure, see "7.1.1 Communication is not possible or is disconnected".

(d) Identifying the range for a failure (from the Switch)

If a failure has not occurred on the Switch, a failure might have occurred somewhere on the route between the Switch and the remote device. To identify the range for a failure in order to determine the fault location on the route, do the following:

1. Log in to the Switch.
2. If there are devices such as a router between the DNS server and the DHCP server, use the "ping" command and check the communication between the router and the remote device (DNS server). If the communication with the remote device cannot be verified by using the "ping" command, execute the "ping" command again and check communication with each of the devices up to the client, beginning with the device closest to the Switch. For details about examples of using the "ping" command and how to interpret the execution result, see "Configuration Guide".
3. If the DNS server and the DHCP server are directly connected, check the hub and cable connections.
4. Select a suitable next step in the failure analysis flowchart depending on whether the range for the failure determined by the "ping" command is in the neighboring device or remote device.

(e) Checking the routing information

You need to check the routing information obtained by the Switch if (a) communication is still disabled after address resolution with the neighboring device is completed, (b) communication is disabled on the route to the remote device, or (c) the route to the remote device has a problem. To carry out the check, do the following:

1. Log in to the Switch.
2. Use the "show ip route" command and check the routing information obtained by the Switch.

(f) Checking discarded packets

Packets might have been discarded by a filter or QoS control. For the checking method and action to take, see "10.2 Checking discarded packets".

In addition, if DHCP snooping is used, packets might have been discarded by a terminal filter. Check whether the setting conditions for DHCP snooping in the configuration are correct. For the procedure, see "8.1 DHCP snooping problems".

(g) Checking the Layer 2 network

If you do not find any incorrect settings or a failure in the steps (a) to (f), there might be a problem with the Layer 2 network. See "4 Troubleshooting of Layer 2 Switching" and check the Layer 2 network.

7.2 Policy-based routing communication failures

7.2.1 Packets are not forwarded in policy-based routing

If packets are not forwarded to the specified route when a policy-based routing group is used, resolve the problem by actions shown in the following table.

Table 7-1 Action to take when packets are not forwarded in policy-based routing

No.	Items to check and commands	Action
1	Check the running status of the filter for which the policy-based routing list information is set - Execute the "show access-filter" command, and in the "matched packets :" part, check whether the number of packets matches the filter conditions.	If the number of packets that could not be transmitted differs from the "matched packets" value, it is possible that the filter detection conditions are incorrect, causing implicit discards. Revise the filter settings.
		If the number of packets that could not be transmitted is the same as the "matched packets" value, go to No. 2.
2	Check the running status of the policy-based routing group - Execute the "show ip cache policy" command, and check the display status of "*>".	If the status is not displayed, the group might be in the process of starting, or in the default process, causing default forwarding or discards to be performed. To check if the group is in the process of starting, go to No. 3.
		If the status is displayed, go to No. 4.
3	Check the running status of path switching in policy-based routing - Check the "Start Time" and "End Time" values of the "Policy Base Routing Default Init Interval" of the "show ip cache policy" command.	If "-" is displayed only for "End Time", the packets might have been discarded because the group is in the process of starting. Wait until startup finishes.
		If "Start Time" and "End Time" are both "-", or the date is displayed, go to No. 5.
4	Check the running status of path switching in policy-based routing - Check the "Start Time" and "End Time" values of the "Policy Base Routing Default Aging Interval" of the "show ip cache policy" command.	If "-" is displayed only for "End Time", the packets might have been discarded because the group is in the process of path switching. Wait until path switching finishes.
		If "Start Time" and "End Time" are both "-", or the date is displayed, go to No. 5.
5	Check the status of the VLAN interface and tracking function of the policy-based routing forwarding destination - Execute the "show vlan" command, and check the "Status:" item. - Execute the "show track-object" command, and check the track status of the "State" item.	If the status of either the VLAN interface or the tracking function of the policy-based routing forwarding destination is not "Up", packets are being forwarded normally or discarded due to the default process. Make sure that the VLAN interface and tracking function of the forwarding destination are both in the "Up" status.
		If both are in the "Up" status, go to No. 6.
6	Check the path switchback process setting of policy-based routing - Execute the "show ip cache policy" command, and check the "Recover" item.	If the setting is "Off", path switchback processes are not performed, and thus the path is not being re-selected. Execute the "reset policy-list" command to re-select the path.
		If the setting is "On", go to No. 7.
7	Check the ARP information of the policy-based routing forwarding destination - Execute the "show ip arp" command, and check if the next hop of the forwarding destination is registered. - Execute the "show mac-address-table"	If ARP is not registered, specify static ARP. If the MAC address is not registered, specify a MAC address static entry. Also, use the tracking function of policy-based routing.
		If the ARP and MAC address are registered, go to No. 8.

No.	Items to check and commands	Action
	command, and check if the MAC address of the forwarding destination is registered.	
8	Check if a network communication failure has occurred in the destination interface - See "7.1 IPv4 network communication failures".	If a communication failure has occurred, follow the instructions in the referenced section.
		If a communication failure has not occurred, go to No. 9.
9	Collect analysis information - Execute the "show tech-support" command and the "dump policy" command, twice in that order.#	Send the information you collected to the support center.

#

The second time you execute the "dump policy" command, the memory dump file you collected the first time is deleted. Therefore, be sure to save the first memory dump file you collected before executing the command for the second time.

7.2.2 Tracking function problems

The Switch might have an unexpected track status for one of the following three reasons:

1. The track configuration was changed.
2. Due to a network failure, communication cannot be made with the polling monitoring track target.
3. Due to network congestion, communication with the polling monitoring track target is unstable.

To investigate the cause of the current unexpected track status, you must follow the methods of analysis shown in the following table to determine the cause.

Table 7-2 Action to take when the track status is unexpected

No.	Items to check and commands	Action
1	Check the track information - Specify the <track-object id> parameter for the "show track-object" command, and display the track information.	If the information is not displayed, or the track type is UNSPECIFIED, the track is not set. If the track running status is Disable, the track is stopped in the configuration. Check the configuration.
		If the track running status is Init, the track is stopped because it is immediately after startup. Wait until the startup waiting time elapses.
		If the track is running, yet the track type is ICMP, go to No. 2.
2	Check whether IPv4 communication can be made with the track target For the destination address, source address, and next hop, use the same values as for the track settings. - Execute the "ping" command.	If the ping destination address and responding address are different, the address that responded is the subnet broadcast address of the destination address. IPv4 ICMP polling monitoring will not be enabled when the destination is a broadcast address. Check the configuration.
		If the track has no next hop specified, and there is no response or the response is unstable, check the IPv4 network communication between the Switch and the track target device.
		If the track has a next hop specified, and there is no response or the response is unstable, go to No. 3.

No.	Items to check and commands	Action
3	Check whether IPv4 communication can be made with the router specified as the next hop - Execute the "ping" command.	If communication with the device specified as the next hop is unstable, check the IPv4 network communication between the Switch and the next hop device.
		If communication with the device specified as the next hop is stable, check the IPv4 network communication between the next hop device and the track target device.

7.3 IPv4 unicast routing communication failures

7.3.1 No RIP routing information exists

If RIP routing information cannot be found in the routing information obtained by the Switch, isolate the cause of the problem according to the failure analysis method described in the following table.

Also, if network partitioning is used and the maximum number of routes is set by the "maximum routes" configuration command, first, follow the failure analysis method described in "7.3.4 No IPv4 routing information exists in the VRF".

Table 7-3 Failure analysis method for RIP

No.	Items to check and commands	Action
1	Display the RIP neighboring information. show ip rip neighbor	If the interface of the neighboring router is not displayed, go to No. 2.
		If the interface of the neighboring router is displayed, go to No. 3.
2	Check whether the RIP setting in the configuration is correct.	If the configuration is correct, go to No. 3.
		If the configuration is not correct, modify the configuration.
3	Check whether RIP packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
		If the packets are not discarded, check whether the neighboring router is advertising the RIP route.

7.3.2 No OSPF routing information exists

If OSPF routing information cannot be found in the routing information obtained by the Switch, isolate the cause of the problem according to the failure analysis method described in the following table.

Also, if network partitioning is used and the maximum number of routes is set by the "maximum routes" configuration command, first, follow the failure analysis method described in "7.3.4 No IPv4 routing information exists in the VRF".

Table 7-4 Failure analysis method for OSPF

No.	Items to check and commands	Action
1	Display the OSPF interface status. show ip ospf interface <IP Address>	If the interface status is DR or P to P, go to No. 3.
		If the interface status is BackupDR or DR Other, go to No. 2.
		If the interface status is Waiting, wait for a while and execute the command again. Go to No. 1.
2	Check the neighboring router status with DR in Neighbor List.	If the neighboring router status with DR is other than Full, go to No. 4.
		If the neighboring router status with DR is Full, go to No. 5.
3	Check the status of every neighboring router in Neighbor List.	If the status of any neighboring router is other than Full, go to No. 4.
		If the status of every neighboring router is Full, go to No. 5.
4	Check whether the OSPF setting in the configuration is correct.	If the configuration is correct, go to No. 5.
		If the configuration is not correct, modify the configuration.
5	Check the route that has learned the OSPF route. show ip route all-routes	If the route is InActive, go to No. 6.
		If the route does not exist, check whether the neighboring router is advertising the OSPF route.
6	Check whether OSPF packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
		If the packets are not discarded, check whether the neighboring router is advertising the OSPF route.

7.3.3 No BGP4 routing information exists

If BGP4 routing information cannot be found in the routing information obtained by the Switch, isolate the cause of the problem according to the failure analysis method described in the following table.

Also, if network partitioning is used and the maximum number of routes is set by the "maximum routes" configuration command, first, follow the failure analysis method described in "7.3.4 No IPv4 routing information exists in the VRF".

Table 7-5 Failure analysis method for BGP4

No.	Items to check and commands	Action
1	Check the BGP4 peer status. show ip bgp neighbors	If the peer status is other than Established, go to No. 2.
		If the peer status is Established, go to No. 3.
2	Check whether the BGP4 setting in the configuration is correct.	If the configuration is correct, go to No. 3.
		If the configuration is not correct, modify the configuration.
3	Check whether the BGP4 route has been learned. show ip bgp received-routes	If the route exists but its status is not active, go to No. 4.
		If the route does not exist, go to No. 5.
4	Check whether the routing information that resolves the next hop address of the BGP4 route exists. show ip route	If the routing information that resolves the next hop address exists, go to No. 5.
		If the routing information that resolves the next hop address does not exist, perform the failure analysis for the protocol for learning the routing information.
5	Check whether BGP4 packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
		If the packets are not discarded, check whether the neighboring router is advertising the BGP4 route.

7.3.4 No IPv4 routing information exists in the VRF

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

Table 7-6 Failure analysis method for VRF

No.	Items to check 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	If the number of routes is equal to or larger than the maximum value, go to No. 2.
		If the number of routes is less than the maximum value, perform the failure analysis for the protocol for the route that does not exist. RIP: "7.3.1 No RIP routing information exists" OSPF: "7.3.2 No OSPF routing information exists" BGP4: "7.3.3 No BGP4 routing information exists"
2	Check the maximum number of routes in VRF specified in the configuration.	Increase the maximum number, or reduce the number of routes by, for example, aggregating the routes.

7.4 Communication failures in the IPv4 multicast routing function

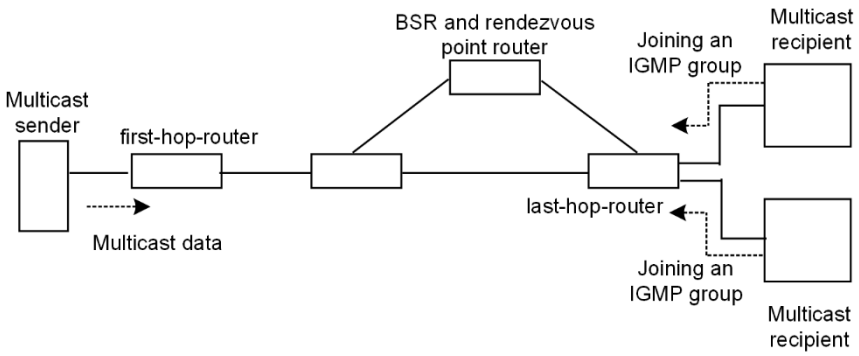
This section describes actions to be taken when an IPv4 multicast communication failure occurs on the Switch.

7.4.1 Communication is not possible on the IPv4 PIM-SM networks

If multicast forwarding is not possible in an IPv4 PIM-SM network configuration, isolate the cause of the problem according to the failure analysis method described below.

The following figure shows an example of an IPv4 PIM-SM network.

Figure 7-5 Example of IPv4 PIM-SM network



Notes

- BSR: The router that distributes rendezvous point information (For details, see "Configuration Guide".)
- Rendezvous point router: The router that forwards packets to the multicast receivers if the destination of the packets has not been determined (For details, see "Configuration Guide".)
- first-hop-router: The router that is connected directly to the multicast sender
- last-hop-router: The router that is connected directly to the multicast receivers

(1) Items checked in common

The following table shows the items checked in common for all the Switches in an IPv4 PIM-SM network configuration.

Table 7-7 Items checked in common

No.	Items to check and commands	Action
1	Make sure that the setting for using the multicast function (ip multicast routing) exists in the configuration. show running-config	If the setting for using the multicast function does not exist, modify the configuration.
2	Make sure that PIM-SM is running on one or more interfaces. show ip pim interface	If PIM-SM is not running, check and modify the configuration so that PIM-SM runs on at least one of the interfaces. For AX3800S and AX3650S, if the configuration contains the setting for running PIM on an interface but the interface is not displayed by the "show ip pim interface" command, make sure that multihoming is not set for the target interface.

No.	Items to check and commands	Action
3	Check whether IGMP snooping is set for the interface on which PIM runs. show igmp-snooping	If IGMP snooping is set, check the following: - Check whether the multicast router port for IGMP snooping is set for the port connected to the neighboring router. - See "4.5 IGMP snooping communication failures".
4	Check whether protocol packets or multicast packets are discarded by a filter or QoS on the interfaces on which PIM and IGMP run.	For the checking method and action to take, see "10.2 Checking discarded packets".
5	Check the PIM neighboring information. show ip pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ip pim interface" command and check that PIM-SM is running on the interface connected with the neighboring routers. - Check the settings of the neighboring routers.
6	Check whether the unicast route to the multicast data sender exists. show ip route	If the unicast route does not exist, see "7.3 IPv4 unicast routing communication failures".
7	Make sure that PIM is running on the interface connected to the next hop address to the multicast data sender. show ip pim interface	If PIM is not running, check and modify the configuration so that PIM runs on the interface connected to the next hop address to the multicast data sender.
8	Check the configuration to make sure that the PIM-SSM group addresses do not contain the forwarding target group address. show running-config	If the PIM-SSM group addresses contain the forwarding target group address, modify the configuration.
9	Make sure that BSR has been determined. This checking is not required if the rendezvous point for the forwarding target group address is a static rendezvous point. show ip pim bsr	If BSR has not been determined, check whether the unicast route to BSR exists. If the unicast route does not exist, see "7.3 IPv4 unicast routing communication failures". If the unicast route exists, check whether PIM-SM is set up on the interface directed toward BSRs. If PIM-SM is set, check the BSR settings. If the Switch is used as the BSR, see "(2) Items to check for BSR".
10	Make sure that the rendezvous point has been determined. show ip pim rp-mapping	If the rendezvous point has not been determined, check whether the unicast route to the rendezvous point exists. If the unicast route does not exist, see "7.3 IPv4 unicast routing communication failures". If the unicast route exists, check whether PIM-SM is set up on the interface directed toward rendezvous points. If the PIM-SM is set, check the rendezvous point settings. If the Switch is used as the rendezvous point, see "(3) Items to check for the rendezvous point router".
11	Make sure that the rendezvous point group addresses contain the forwarding target group address. show ip pim rp-mapping	If the forwarding target group address is not contained, check the rendezvous point router settings. If the Switch is used as the rendezvous point, see "(3) Items to check for the rendezvous point router".
12	Make sure that multicast forwarding entries exist. show ip mcache	If multicast forwarding entries do not exist, make sure that multicast data has reached the upstream port. If multicast data has not reached the upstream port, check the settings of the multicast sender or upstream router.
13	Make sure that multicast routing information exists. show ip mroute	If multicast routing information does not exist, check the downstream router settings.

No.	Items to check and commands	Action
14	Check whether the number of the multicast routing information entries or multicast forwarding entries exceeds its upper limit. For the multicast routing information entries: show ip mroute For the multicast forwarding entries: show ip mcache netstat multicast	If a warning is displayed, check whether an unexpected multicast routing information entry or unexpected multicast forwarding entry has been created. If many negative caches are found among the multicast forwarding entries, check whether there is a terminal that is sending unnecessary packets.

(2) Items to check for BSR

The following table shows the items to check when the Switch is used as BSR in an IPv4 PIM-SM network configuration.

Table 7-8 Items to check for BSR

No.	Items to check and commands	Action
1	Make sure that the Switch is a BSR candidate. show ip pim bsr	If the Switch is not a BSR candidate, check and modify the configuration so that the Switch can work as a BSR candidate. If a loopback interface is set as a BSR candidate but an address is not set to the loopback interface, the interface will not work as the BSR candidate. Therefore, check that the address is set to the loopback interface. If a VLAN interface is set as a BSR candidate but the VLAN interface status is not Up, the interface will not work as the BSR candidate. Therefore, check that the VLAN interface status is Up.
2	Make sure that the Switch is used as BSR. show ip pim bsr	If the Switch is not used as BSR, check the priorities of other BSR candidates. A larger value represents a higher priority. If the priority is the same among BSR candidates, the BSR candidate that has the highest BSR address becomes BSR.

(3) Items to check for the rendezvous point router

The following table shows the items to check when the Switch is used as a rendezvous point router in an IPv4 PIM-SM network configuration.

Table 7-9 Items to check for the rendezvous point router

No.	Items to check and commands	Action
1	Make sure that the Switch is a rendezvous point candidate for the forwarding target group address. show ip pim rp-mapping	If the Switch is not a rendezvous point candidate for the forwarding target group address, check and modify the configuration so that the Switch can work as a rendezvous point candidate for the forwarding target group address. If a loopback interface is set as a rendezvous point candidate but an address is not set to the loopback interface, the interface will not work as the rendezvous point candidate. Therefore, check that the address is set to the loopback interface. If a VLAN interface is set as a rendezvous point candidate but the VLAN interface is not in the Up status, the interface will not work as the rendezvous point candidate. Therefore, check that the VLAN interface is in the Up status.
2	Make sure that the Switch is the rendezvous point for the forwarding target group address. show ip pim rp-hash <Group Address>	If the Switch is not the rendezvous point, check the priorities of other rendezvous point candidates. A smaller value represents a higher priority. If the priority of another rendezvous point candidate is higher than that of the Switch, the Switch does not work as the rendezvous point. If the priority is the same between another candidate and the Switch, they are assigned to a different group address due to the

No.	Items to check and commands	Action
		protocol specification, and the Switch might not work as the rendezvous point for the target group. If you want to use the Switch as the rendezvous point, set a higher priority for the Switch than other rendezvous point candidates.

(4) Items to check for last-hop-router

The following table shows the items to check when the Switch is used as last-hop-router in an IPv4 PIM-SM network configuration.

Table 7-10 Items to check for last-hop-router

No.	Items to check and commands	Action
1	Make sure that IGMP is running on the interface connected to the multicast receivers. show ip igmp interface	If IGMP is not running, check and modify the configuration so that IGMP runs on the interface.
2	Make sure that the multicast receivers participate in the forwarding target group through IGMP. show ip igmp group	If a multicast receiver does not participate in the forwarding target group, check the multicast receiver settings.
3	If the interface in which the forwarding target group participates exists, make sure that the Switch is DR. show ip pim interface	If the Switch is not DR, check the DR of the forwarding target interface.
4	Check whether IGMP snooping is set for the interface on which the join static group function is used. show igmp-snooping	If IGMP snooping is set, check the following: - Check whether the multicast router port for IGMP snooping is set for the destination port. - See "4.5 IGMP snooping communication failures".
5	Check whether any anomaly has been detected on any interface. show ip igmp interface	Make sure that no warning information is displayed for Notice. If warning information is displayed, check the following: - L: More participation requests than the expected maximum number have occurred. Check the number of connected users. - Q: The IGMP version is different from that on the neighboring router. Use the same IGMP version. - R: A user is sending a report that cannot be received with the current settings. Change the IGMP version on the Switch, or check the settings of the participation user.

(5) Items to check for first-hop-router

The following table shows the items to check when the Switch is used as first-hop-router in an IPv4 PIM-SM network configuration.

Table 7-11 Items to check for first-hop-router

No.	Items to check and commands	Action
1	Make sure that the Switch is directly connected to the multicast sender.	If the Switch is not connected directly, check the network configuration.
2	Make sure that PIM-SM or IGMP is running on the interface connected to the multicast sender. show ip pim interface show ip igmp interface	If PIM-SM or IGMP is not running, check and modify the configuration so that PIM-SM or IGMP runs on the interface.

No.	Items to check and commands	Action
3	Check whether multicast routing information exists. show ip mroute	If multicast routing information does not exist, make sure that the multicast data source address is the network address of the interface directly connected to the multicast sender.

7.4.2 Multicast data is forwarded twice in an IPv4 PIM-SM network

If multicast data is forwarded twice in an IPv4 PIM-SM network configuration, check the settings of each router and if multiple routers exist in one network, modify the settings so that PIM-SM runs on the interface in the network.

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

Table 7-12 Items to check when data continues to be forwarded twice

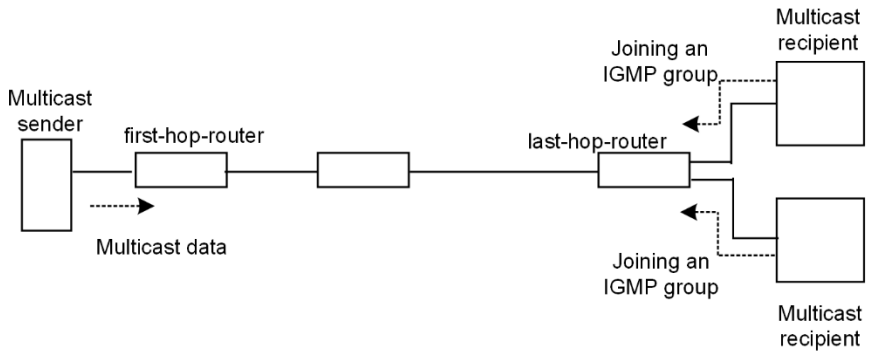
No.	Items to check and commands	Action
1	Check the PIM neighboring information of the interface belonging to the network with multiple routers. show ip pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ip pim interface" command and check that PIM-SM is running on the interface connected with the neighboring routers. - Check whether protocol packets are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets". - Check the settings of the neighboring routers.

7.4.3 Communication is not possible on the IPv4 PIM-SSM networks

If multicast forwarding is not possible in an IPv4 PIM-SSM network configuration, isolate the cause of the problem according to the failure analysis method described below.

The following figure shows an example of an IPv4 PIM-SSM network.

Figure 7-6 Example of IPv4 PIM-SSM network



Notes

- first-hop-router: The router that is connected directly to the multicast sender
- last-hop-router: The router that is connected directly to the multicast receivers

(1) Items checked in common

The following table shows the items checked in common for all the Switches in an IPv4 PIM-SSM network configuration.

Table 7-13 Items checked in common

No.	Items to check and commands	Action
1	Make sure that the setting for using the multicast function (ip multicast routing) exists in the configuration. show running-config	If the setting for using the multicast function does not exist, modify the configuration.
2	Make sure that PIM-SM is running on one or more interfaces. show ip pim interface	If PIM-SM is not running, check and modify the configuration so that PIM-SM runs on at least one of the interfaces. For AX3800S and AX3650S, if the configuration contains the setting for running PIM on an interface but the interface is not displayed by the "show ip pim interface" command, make sure that multihoming is not set for the target interface.
3	Check whether IGMP snooping is set for the interface on which PIM runs. show igmp-snooping	If IGMP snooping is set, check the following: - Check whether the multicast router port for IGMP snooping is set for the port connected to the neighboring router. - See "4.5 IGMP snooping communication failures".
4	Check whether protocol packets or multicast packets are discarded by a filter or QoS on the interfaces on which PIM and IGMP run.	For the checking method and action to take, see "10.2 Checking discarded packets".
5	Check the PIM neighboring information. show ip pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ip pim interface" command and check that PIM is running on the interface connected with the neighboring routers. - Check the settings of the neighboring routers.
6	Check whether the unicast route to the multicast data sender exists. show ip route	If the unicast route does not exist, see "7.3 IPv4 unicast routing communication failures".
7	Make sure that PIM is running on the unicast route send interface to the multicast data sender. show ip pim interface	If PIM is not running, check and modify the configuration so that PIM runs on the unicast route send interface.
8	Check the configuration to make sure that the PIM-SSM group addresses contain the forwarding target group address. show running-config	If the PIM-SSM group addresses do not contain the forwarding target group address, modify the configuration.
9	Check whether multicast routing information exists. show ip mroute	If multicast routing information does not exist, check the downstream router settings.
10	Check whether the number of the multicast routing information entries or multicast forwarding entries exceeds its upper limit. For the multicast routing information entries: show ip mroute For the multicast forwarding entries: show ip mcache netstat multicast	If a warning is displayed, check whether an unexpected multicast routing information entry or unexpected multicast forwarding entry has been created. If many negative caches are found among the multicast forwarding entries, check whether there is a terminal that is sending unnecessary packets.

(2) Items to check for last-hop-router

The following table shows the items to check when the Switch is used as last-hop-router in an IPv4 PIM-SSM network configuration.

Table 7-14 Items to check for last-hop-router

No.	Items to check and commands	Action
1	Make sure that the configuration contains the setting (ip igmp ssm-map enable) to enable the PIM-SSM linkage behavior in IGMPv1 and IGMPv2. show running-config	If the configuration does not contain the setting to enable the PIM-SSM linkage behavior in IGMPv1 and IGMPv2, modify the configuration.
2	Make sure that the configuration contains the setting (ip igmp ssm-map static) to enable the group address and source address forwarded via PIM-SSM to work with PIM-SSM in IGMPv1 and IGMPv2. show running-config	If the configuration does not contain the setting to enable the linkage behavior with PIM-SSM in IGMPv1 and IGMPv2, modify the configuration.
3	Make sure that IGMP is running on the interface connected to the multicast receivers. show ip igmp interface	If IGMP is not running, check and modify the configuration so that IGMP runs on the interface.
4	Make sure that the multicast receivers participate in the forwarding target group through IGMP. show ip igmp group	If a multicast receiver does not participate in the forwarding target group, check the multicast receiver settings.
5	If the interface in which the forwarding target group participates exists, make sure that the Switch is DR. show ip pim interface	If the Switch is not DR, check the DR of the forwarding target interface.
6	Check whether IGMP snooping is set for the interface on which the join static group function is used. show igmp-snooping	If IGMP snooping is set, check the following: - Check whether the multicast router port for IGMP snooping is set for the destination port. - See "4.5 IGMP snooping communication failures".
7	Check whether any anomaly has been detected on any interface. show ip igmp interface	Make sure that no warning information is displayed for Notice. If warning information is displayed, check the following: - L: More participation requests than the expected maximum number have occurred. Check the number of connected users. - Q: The IGMP version is different from that on the neighboring router. Use the same IGMP version. - R: A user is sending a report that cannot be received with the current settings. Change the IGMP version on the Switch, or check the settings of the participation user. - S: Parts of the participation information have been discarded because the number of sources stored in a message exceeds the maximum number for IGMPv3. Check the settings of the participation user.

(3) Items to check for first-hop-router

The following table shows the items to check when the Switch is used as first-hop-router in an IPv4 PIM-SSM network configuration.

Table 7-15 Items to check for first-hop-router

No.	Items to check and commands	Action
1	Make sure that the Switch is directly connected to the multicast sender.	If the Switch is not connected directly, check the network configuration.
2	Make sure that PIM-SM or IGMP is running on the interface connected to the multicast sender. show ip pim interface show ip igmp interface	If PIM-SM or IGMP is not running, check and modify the configuration so that PIM-SM or IGMP runs on the interface.
3	Check whether multicast data has reached the Switch.	If the multicast data has not reached the Switch, check the settings of the multicast sender.
4	Check whether the group address and source address are the same between multicast data and multicast routing information. show ip mroute show netstat multicast	If the different group address and source address are used, check the settings of the multicast sender and last-hop-router.

7.4.4 Multicast data is forwarded twice in an IPv4 PIM-SSM network

If multicast data is forwarded twice in an IPv4 PIM-SSM network configuration, check the settings of each router and if multiple routers exist in one network, modify the settings so that PIM-SM runs on the interface in the network.

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

Table 7-16 Items to check when data continues to be forwarded twice

No.	Items to check and commands	Action
1	Check the PIM neighboring information of the interface belonging to the network with multiple routers. show ip pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ip pim interface" command and check that PIM-SM is running on the interface connected with the neighboring routers. - Check whether protocol packets are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets". - Check the settings of the neighboring routers.

7.4.5 IPv4 multicast communication problems in VRF

If a problem on IPv4 multicast communication occurs in VRF, check the following.

Table 7-17 Items to check for VRF

No.	Items to check and commands	Action
1	Check the port number and VLAN ID to make sure that the interface for VRF is correct. show ip vrf show vlan show ip pim interface	If the settings are not correct, modify the configuration or connection.

No.	Items to check and commands	Action
2	If the Switch is used as the rendezvous point or BSR, check the configuration to make sure that the loopback interface is set for the target VRF. show ip vrf show running-config	If a loopback interface is set as a rendezvous point candidate or BSR candidate, set the same loopback interface ID as that of the target VRF. Also, set the IPv4 address for the loopback interface if no address has been set. If a VLAN interface is set as a rendezvous point candidate or BSR candidate, set the VLAN interface that belongs to the target VRF. Since a VLAN interface will not work as a rendezvous point candidate or BSR candidate if the interface is not in the Up status, check that the VLAN interface is in the Up status.
3	If multiple VRFs are used, check whether a global network or specific VRF occupies an unexpectedly large number of multicast forwarding entries. show ip mcache vrf all	If a global network or specific VRF occupies more multicast forwarding entries than expected in the network design, check whether any unexpected multicast forwarding entries are created. If many negative caches are found, check whether there is a terminal that is sending unnecessary packets. Also, set the maximum number of forwarded entries for each VRF to prevent a global network or specific VRF from occupying forwarded entries. Target configuration: ip pim vrf <vrf id> mcache-limit <number>
4	For each VRF, check the items described in "7.4.1 Communication is not possible on the IPv4 PIM-SM networks" through "7.4.4 Multicast data is forwarded twice in an IPv4 PIM-SSM network".	Specify the target VRF for each command to check the information of the VRF. For details about specifying VRF, see "Operation Command Reference".

7.4.6 IPv4 multicast communication problems in an extranet

For IPv4 multicast communication problems in an extranet, firstly check the items described in "7.4.5 IPv4 multicast communication problems in VRF" to confirm that multicast communication can be performed in each VRF. After that, check the following.

Table 7-18 Items to check for an extranet

No.	Items to check and commands	Action
1	Make sure that the unicast route from the destination VRF to the source address is the expected VRF or global network. show ip rpf	If it is not the case, check the settings of the unicast extranet.
2	Make sure that the protocol (PIM-SM or PIM-SSM) for the IPv4 multicast address used in the extranet is the same between the destination VRF and the upstream VRF. show running-config	If the protocol is different between the destination VRF and the upstream VRF, select a suitable IPv4 multicast address so that the protocol can be the same between them.
3	For the upstream VRF, check whether the unicast route to the source address is not another VRF. show ip rpf	Set the upstream VRF so that the unicast route to the source address is a VRF with an actual interface in the VRF.
4	If the PIM-SM VRF gateway is used, make sure that (*,G) entries have been generated in the upstream VRF. Also, make sure that V is displayed for Flags for the target (*,G) entry. show ip mroute	If (*,G) entries are not generated correctly, make sure that the IPv4 multicast address used in extranet communication has been specified as the host address and permitted for the IPv4 multicast route filtering for the upstream VRF.

No.	Items to check and commands	Action
5	If the PIM-SM VRF gateway is used, make sure that the destination VRF is displayed for the downstream interface for the (*,G) entry generated in the upstream VRF. show ip mroute	If the destination VRF does not exist in the downstream interface for the (*,G) entry of the upstream VRF, make sure that the destination VRF has been permitted for route-map that specifies the host address for IPv4 multicast route filtering in the upstream VRF. If no specific VRF is specified for route-map by the "match vrf" command, every VRF is permitted to be a destination.
6	If "(denied)" is displayed for the VRF of the upstream interface by the "show ip mroute" command, IPv4 multicast route filtering for the upstream VRF has not been set correctly. If the route does not exist, check the IPv4 multicast route filtering of the upstream VRF in the configuration. show ip mroute show running-config	Make sure that the IPv4 multicast address and destination VRF that are used in extranet communication have been permitted for the IPv4 multicast route filtering for the upstream VRF. If neither specific IPv4 multicast address nor specific VRF is specified for the IPv4 multicast route filtering, all IPv4 multicast addresses and VRFs are permitted.

7.5 IPv6 network communication failures

7.5.1 Communication is not possible or is disconnected

There are three probable causes of problems that occur during communication on an IPv6 network employing a Switch:

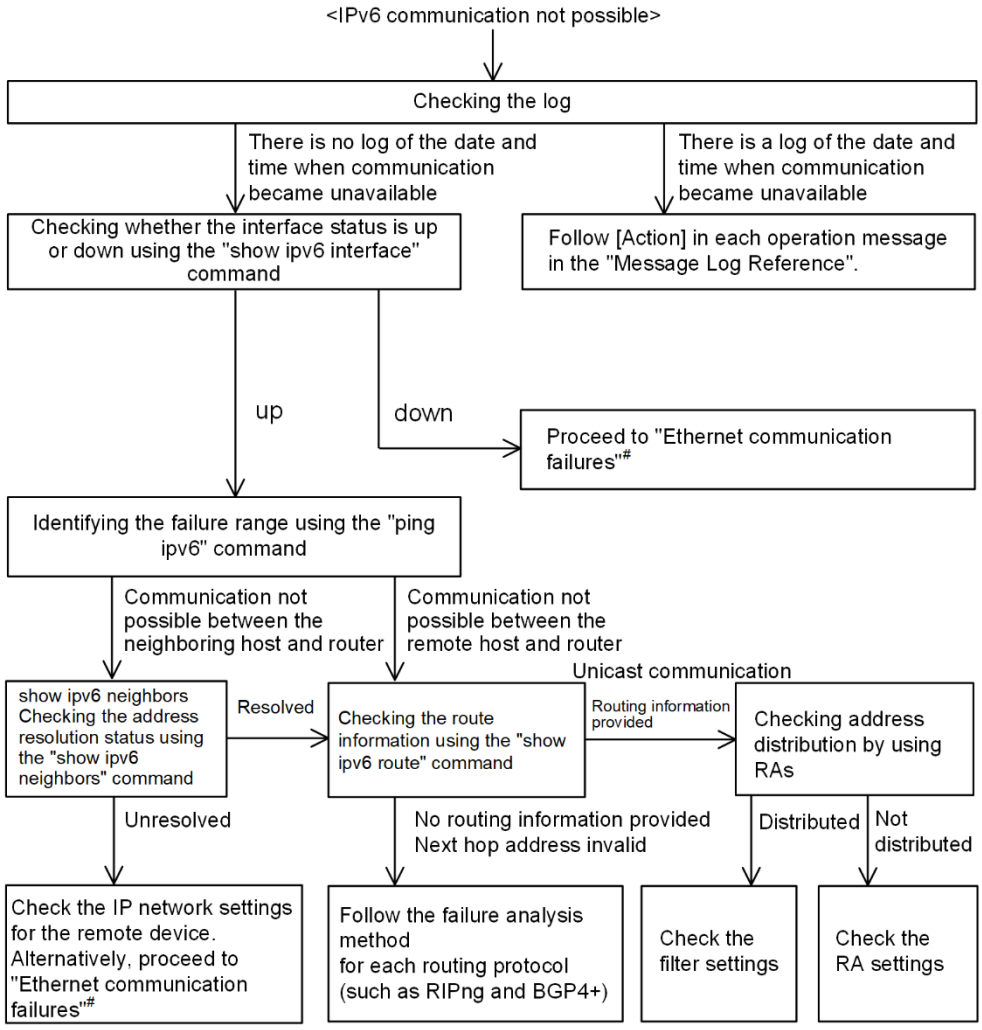
1. A configuration related to IPv6 communication is changed.
2. The network configuration is changed.
3. A network device fails.

For causes 1 and 2, check the differences in the configuration and network configuration before and after the change to uncover any cause 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 cause 3 failures. For example, IPv6 communication might not be possible even when the configuration and the network configuration are correct, or when IPv6 communication is disabled even though it was normally performed so far.

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

Figure 7-7 Failure analysis procedure for when IPv6 communication is not possible



#: See "3.1 Ethernet communication failures".

(1) Checking the log

One probable cause of disabled communication is a line failure (or damage). To display the messages that indicate a hardware failure, carry out the procedure below. You can find these messages in the log displayed by the Switch.

For details about the contents of the log, see "Message Log Reference".

1. Log in to the Switch.
2. Use 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, see "Message Log Reference", and then follow the instructions given in the manual.
5. If a log entry was not displayed for the date and time when communication was disabled, go to "(2) Checking the interface status".

(2) Checking the interface status

Even when the Switch hardware is running normally, a failure could have occurred on the hardware of a neighboring device connected to the Switch.

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

1. Log in to the Switch.
2. Use the "show ipv6 interface" command and check whether the status of the interface between the Switch and the target neighboring device is Up or Down.
3. If the status of the target interface is "Down", see "3.1 Ethernet communication failures".
4. If the status of the target interface is "Up", go to "(3) Identifying the range for a failure (from the Switch)".

(3) Identifying the range for a failure (from the Switch)

If a failure has not occurred on the Switch, a failure might have occurred somewhere on the route between the Switch and the remote devices. To identify the range for a failure in order to determine the fault location on the route, do the following:

1. Log in to the Switch.
2. Use the "ping ipv6" command and check the communication with the two remote devices that are unable to communicate. For details about examples of using the "ping ipv6" command and how to interpret the execution result, see "Configuration Guide".
3. If communication with the remote devices cannot be verified by the "ping ipv6" command, execute the command again and check communication with each of the devices up to the remote device, beginning with the device closest to the Switch.
4. If the range for a failure is determined to be a neighboring device as a result of executing the "ping ipv6" command, go to "(5) Checking the NDP resolution information with a neighboring device". If the range is determined to be a remote device, go to "(6) Checking the unicast interface information".

(4) Identifying the range for a failure (from a customer's terminal)

To use the customer's terminal to identify the range for a failure so that you can determine the fault location on the route with a remote device in an environment in which login to the Switch is not possible, do the following:

1. Make sure that the customer's terminal has the ping ipv6 function.
2. Use the ping ipv6 function and 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 function, use the "ping ipv6" command and 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 determine the range for the failure by using the ping ipv6 function and pinpoint the Switch that is likely to have the failure, log in to the Switch and investigate the cause of the failure based on the failure analysis flowchart.

(5) Checking the NDP resolution information with a neighboring device

If the execution result of the "ping ipv6" command indicates that communication with a neighboring device is impossible, the address might not have been resolved by NDP. To check the status of address resolution between the Switch and the neighboring device, do the following:

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

(6) Checking the unicast interface information

You need to check the routing information obtained by the Switch if (a) communication is still disabled after address resolution with the neighboring device is completed, (b) communication is disabled on the route to the remote device during IPv6 unicast communication, or (c) the route to the remote device has a problem. To carry out the check, do the following:

1. Log in to the Switch.
2. Execute the "show ipv6 route" command and check the routing information obtained by the Switch.
3. If the routing information obtained by the Switch 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, go to "7.6 IPv6 unicast routing communication failures".
4. If the routing information obtained by the Switch contains routing information about the interface that caused the communication failure, the interface might have a problem with any of the functions shown below. Inspect the function associated with the problem.
   - RA function
     Go to "(8) Checking the RA setting information".

(7) Checking discarded packets

Packets might have been discarded by a filter or QoS control. For the checking method and action to take, see "10.2 Checking discarded packets".

(8) Checking the RA setting information

If communication between the Switch and a terminal directly connected to the Switch is not possible, address information might not be correctly distributed by RA. Therefore, check whether the RA function is correctly set in the configuration. To carry out the check, do the following:

1. Log in to the Switch.
2. Execute the "show ipv6 routers" command and check the RA information for the Switch.

3. If the IPv6 address information has been correctly distributed, the interface might have a problem with any of the functions shown below. Inspect the function associated with the problem.
   - Filter/QoS function
     See "(7) Checking discarded packets".

7.5.2 IPv6 address is not assigned for the DHCPv6 relay agent

There are three probable causes for communication problems on an IPv6 DHCP relay.

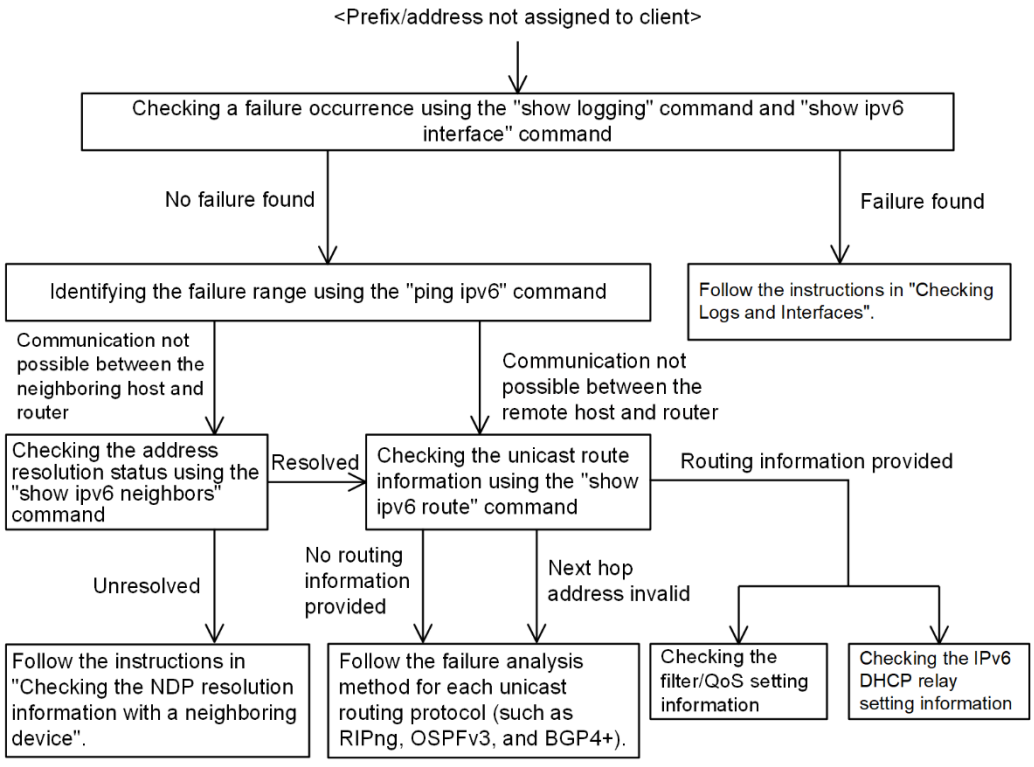
1. A configuration related to the IPv6 DHCP relay is changed.
2. The network configuration is changed.
3. The IPv6 DHCP server fails.

For cause 2, check the differences in the network configuration before and after the change to uncover any cause that could disable communication.

In this subsection, ALAXALA Networks Corporation considers a case to which the cause 1 or 3 applies, assuming that you have checked the client settings. This is a case when, for example, after the configuration is changed, the IPv6 DHCP server cannot distribute information, or when the configuration and network configuration are correct, but prefixes (addresses) cannot be assigned to clients and IP communication fails. The following describes the procedure for isolating the fault location to identify the cause of the problem.

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

Figure 7-8 Failure analysis procedure for IPv6 DHCP relays



(1) Checking the log and interface

One probable cause of disabled assignment of prefixes or addresses to clients is that communication between the client and the server has been disabled. Check the log displayed by the Switch or use the "show ipv6 interface" command to check whether the interface status is Up or Down. For the procedure, see "7.5.1 Communication is not possible or is disconnected".

(2) Identifying the range for a failure

If a failure has not occurred on the Switch, a failure might have occurred somewhere on the route between the Switch and the remote devices. To identify the range for a failure in order to determine the fault location on the route, do the following:

1. Log in to the Switch.
2. Use the "ping ipv6" command and check the communication with the two remote devices that are unable to communicate. For details about examples of using the "ping ipv6" command and how to interpret the execution result, see "Configuration Guide".
3. If communication with the remote devices cannot be verified by the "ping ipv6" command, execute the command again and check communication with each of the devices up to the remote device, beginning with the device closest to the Switch.
4. If the range for a failure is determined to be a neighboring device as a result of executing the "ping ipv6" command, go to "(3) Checking the NDP resolution information with a neighboring device". If the range is determined to be a remote device, go to "(4) Checking the unicast route information".

(3) Checking the NDP resolution information with a neighboring device

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

1. Log in to the Switch.
2. Use the "show ipv6 neighbors" command and check the status of address resolution (whether NDP entry information exists) between the Switch and the neighboring device.
3. If the address with the neighboring device has been resolved (NDP entry information exists), go to "(4) Checking the unicast route information".
4. If the address has not been resolved (no NDP entry information exists), check whether the IP network settings between the neighboring device and the Switch are correctly set to allow communication between them.

(4) Checking the unicast route information

You need to check the routing information obtained by the Switch if (a) communication is still disabled after address resolution with the neighboring device is completed, (b) communication is disabled on the route to the remote device, or (c) the route to the remote device has a problem. To carry out the check, do the following:

1. Log in to the Switch.
2. Use the "show ipv6 route" command and check the routing information obtained by the Switch.
3. If the routing information obtained by the Switch 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, go to "7.6 IPv6 unicast routing communication failures".
4. If the routing information obtained by the Switch contains routing information about the interface that caused the communication failure, the interface might have a problem with any of the functions shown below. Inspect the function associated with the problem.
   - Filters or QoS
     Go to "(5) Checking discarded packets".
   - IPv6 DHCP relays
     Go to "(6) Checking the IPv6 DHCP relay setting information".

(5) Checking discarded packets

Packets might have been discarded by a filter or QoS control. For the checking method and action to take, see "10.2 Checking discarded packets".

(6) Checking the IPv6 DHCP relay setting information

If many of the prefixes or addresses to be leased are left on the IPv6 DHCP server, it can be assumed that the prefixes or addresses cannot be assigned to clients due to incorrect configuration settings for the IPv6 DHCP relay.

The following describes the procedure for checking the configuration.

1. Check whether the IPv6 address of the IPv6 DHCP server or IPv6 DHCP relay, or the interface to the network in which the IPv6 DHCP server exists, is specified by the "ipv6 dhcp relay destination" configuration command.
2. Check whether the "ipv6 dhcp relay destination" configuration command is set for the client interface.
3. Check whether the IPv6 address (or interface) of the IPv6 DHCP server that must lease a prefix or address to the target client is set by the "ipv6 dhcp relay destination" configuration command.
4. Check whether the hop-limit value specified for the "ipv6 dhcp relay hop-limit" configuration command is equal to or larger than an appropriate hop value for the client.

7.5.3 IPv6 DHCP server function problems

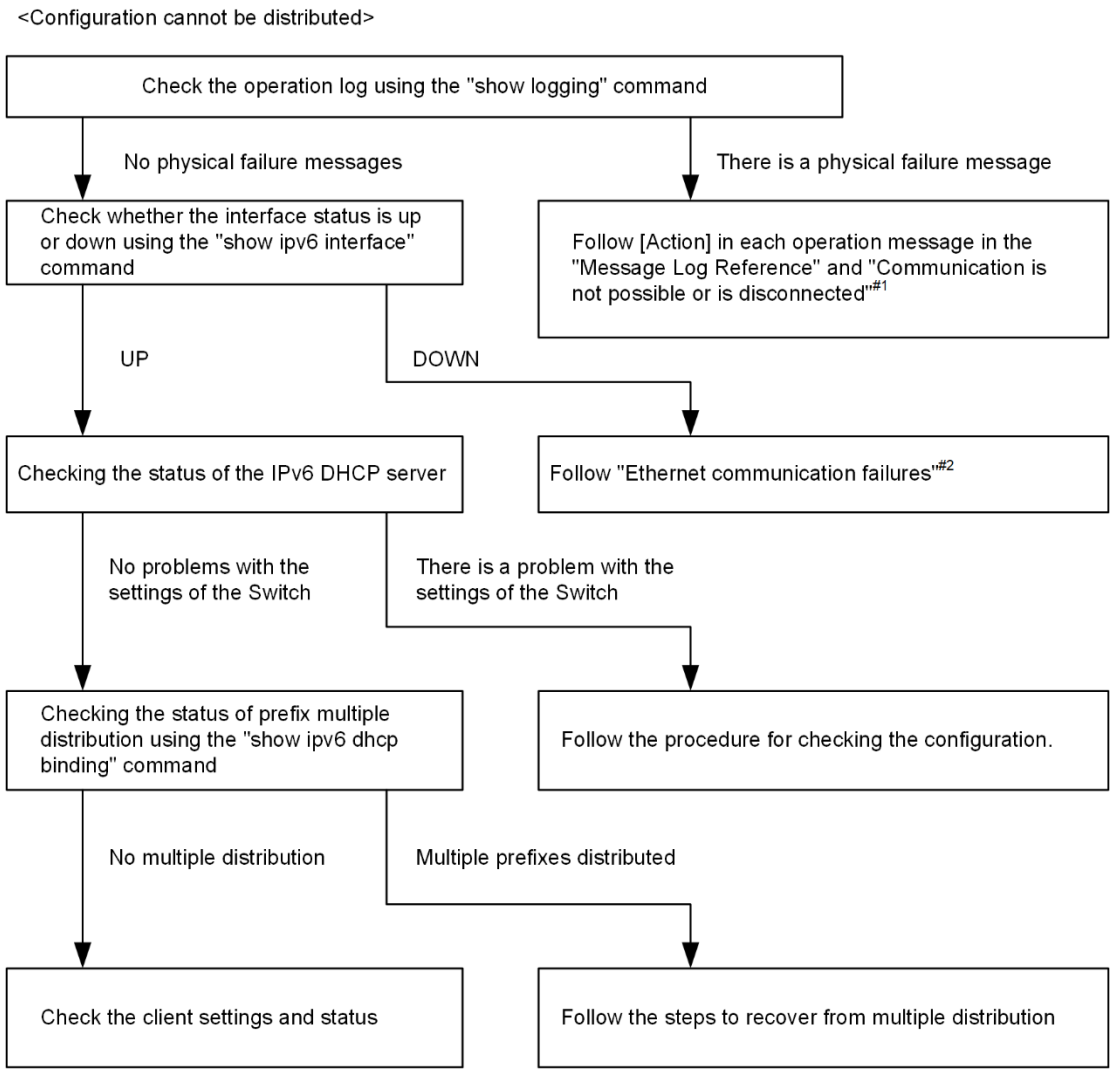
(1) The configuration distribution fails

There are five probable causes of a service-running failure that occurs when you use the prefix distribution function of the IPv6 DHCP server on the Switch.

1. The number of actual clients is larger than the specified number of prefixes available for distribution.
2. An incorrect client DUID (DHCP Unique Identifier) is specified.
3. The ipv6 dhcp server setting is not correct.
4. A failure occurs during IPv6 DHCP server operation.
5. Other failures

Use the following procedure to isolate the failures listed above.

Figure 7-9 Failure analysis procedure for IPv6 DHCP servers



#1: See "7.5.1 Communication is not possible or is disconnected".

#2: See "3.1 Ethernet communication failures".

(a) Checking the log and interface

Probable causes of disabled communication are a failure (or damage) of the NIM or interface and a failure of a neighboring device. Check the log displayed by the Switch or use the "show ipv6 interface" command and check whether the interface status is Up or Down. For the procedure, see "7.5.1 Communication is not possible or is disconnected".

(b) Checking the status of the IPv6 DHCP server on the Switch

1. Checking whether the IPv6 DHCP server service is running
   Use the "show ipv6 dhcp server statistics" command and check whether information can be obtained from the IPv6 DHCP server daemon. If the following result is displayed by executing the "show ipv6 dhcp server statistics" command, use the "service ipv6 dhcp" configuration command to set the IPv6 DHCP server function again.

   [Execution result]

   ```
   > show ipv6 dhcp server statistics
   > < show statistics >: dhcp6_server doesn't seem to be running.
   ```

2. Checking the remainder of the prefixes available for distribution
   Use the "show ipv6 dhcp server statistics" command and check the remainder of the prefixes available for distribution by the IPv6 DHCP server. For details about the checking procedure, see "Configuration Guide". If it is found that the remainder of the prefixes is zero, increase the total number of prefixes available for distribution. Note that the upper limit of the number of prefixes available for distribution is 1024.

(c) Procedure for checking the configuration

1. Checking whether the IPv6 DHCP server function is set to be enabled
   Use the "show service" configuration command and check whether the IPv6 DHCP server is enabled. In the following execution result, the underlined line indicates that the IPv6 DHCP server function is disabled. If this underlined part is not displayed, the IPv6 DHCP server function is enabled.

   [Execution result]

```
(config)# show service
no service ipv6 dhcp
!
(config)#
```

2. Checking the ipv6 dhcp server setting
   Use the "show" configuration command and check whether the ipv6 dhcp server setting exists. If the setting does not exist, add the setting. If the setting exists, make sure that the specified interface is set up for a network for client connections.

   [Execution result]

```
(config)# show
interface vlan 10
  ipv6 address 3ffe:1:2:: linklocal
  ipv6 enable
  ipv6 dhcp server Tokyo preference 100
!
(config)#
```

3. Checking the settings of ipv6 dhcp pool, ipv6 local pool, prefix-delegation, and prefix-delegation pool
   Use the "show ipv6 dhcp" configuration command and check whether the setting for prefix distribution by the IPv6 DHCP server exists. If the setting does not exist, add the setting. If the setting exists, check the setting values for prefix-delegation and ipv6 local pool that specify prefixes to be distributed. Also, check whether the duid is set to specify the clients to which the prefixes are distributed. Furthermore, check whether the client DUID values specified for duid are correct.

   [Execution result]

```
(config)# show ipv6 dhcp
ipv6 dhcp pool Tokyo
  prefix-delegation 3ffe:1:2::/48 00:03:00:01:11:22:33:44:55
!
(config)#
```

(d) Duplicate assignment to a client

1. Checking the binding information
   Use the "show ipv6 dhcp binding" command with the detail parameter specified and check whether multiple prefixes have been distributed to a single DUID. The following shows an example.

   [Execution result]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
```

```
<Prefix>           <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48     XX/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48     XX/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

If the same DUIDs are displayed multiple times as shown in the underlined parts, the relevant client might have incorrectly received prefix information. Check the prefix value distributed to each client.

2. Establishing correspondences between the distributed prefixes and clients
   If you cannot find a client with duplicate prefixes in the result of the "show ipv6 dhcp binding detail" command, establish correspondences between the displayed DUIDs and client devices. To establish correspondences between them, check the binding information to compare the distributed prefix values and the information of the prefixes distributed to the client devices.

(e) Checking the client setting status

To check the setting status of the clients, follow the documentation provided with each client.

(f) Procedure for recovering from duplicate distribution

If you have confirmed that the IPv6 DHCP server on the Switch distributed multiple prefixes to a client, find currently unused prefixes, based on correspondences between the displayed DUIDs and clients. Use the "clear ipv6 dhcp binding <unused prefix>" command to delete the binding information of each currently unused prefix.

[Execution result]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>           <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48     XX/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48     XX/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
> clear ipv6 dhcp binding 3ffe:1234:5678::/48
> show ipv6 dhcp binding detail
<Prefix>           <Lease expiration>  <Type>
  <DUID>
3ffe:aaaa:1234::/48     XX/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

(2) Communication to a prefix distribution target is not possible

The automatic routing information setting function can be used for distributing prefixes from the DHCP server for the Switch to prefix assignment targets. If the routing information cannot be set with the function, there are two probable causes.

1. The configuration has been set but not distributed.
2. An operation or event has occurred that affects functions related to the automatic routing information setting.

To isolate the cause of the problem, first, execute the "show ipv6 route -s" command to display the routing information. Next, execute the "show ipv6 dhcp server binding" command to display the information of the distributed prefixes. Then, compare the information obtained from the results of the both commands.

Table 7-19 Isolating the cause of a failure related to the routing information setting for prefix distribution targets

Condition		Cause
binding information	Routing information	
Provided	Route provided	Not applicable. The status is active.
Provided	Not provided	Cause 2
Not provided	Route provided	Cause 2
Not provided	Not provided	Causes 1 and 2

The routing information for prefix distribution targets is not always retained, as shown in the following table.

Table 7-20 Conditions that affect whether the routing information for prefix distribution targets is retained

Prefix-related information to be retained	Events that affect whether the information is retained			
	Server function is restarted		Routing manager is restarted	Switch is restarted
	Command execution	Server failure		
Routing information to clients	Y	Y/N	Y	N

Legend:

Y: Retained

Y/N: Not retained (The information of each state might be retained.)

N: Not retained (The information is initialized and needs to be set again.)

Notes

The route management function needed to set the routing information for prefix distribution targets

For other failures, see "7.5.1 Communication is not possible or is disconnected".

(a) Checking the routing information

Consider the case where the automatic route setting function is used for distributing prefixes from the IPv6 DHCP server on the Switch to distribution targets. In this case, use the "show ipv6 route" command with the -s parameter specified and check the routing information after prefix distribution.

Figure 7-10 Checking the routing information with an operation command

```
> show ipv6 route -s
Total: 10routes
Destination           Next Hop     Interface       Metric  Protocol  Age
3ffe:1234:5678::/48    ::1          tokyo           0/0     Static    45m
       <Active Gateway Dhcp>
3ffe:aaaa:1234::/48    ::1          osaka           0/0     Static    23m
       <Active Gateway Dhcp>
    :
>
```

(b) Setting the routing information again

Consider the case where the automatic route setting function is used for distributing prefixes from the IPv6 DHCP server on the Switch to distribution targets. In this case, if an event has cleared the routing information due to a failure, the prefixes must be distributed again. Perform necessary operations to obtain the prefix information again on the clients.

(3) The DUID is duplicated between the Switch and another device

In a network where multiple IPv6 DHCP servers including the Switch are operated, if the DUID is duplicated between the Switch and another server, use the following procedure to set the DUID of the Switch again.

(a) Deleting the file that contains the DUID information

The DUID of the Switch is saved in /usr/var/dhcp6/dhcp6s_duid. Use the "rm" command on the operation command line to explicitly delete the file.

(b) Regenerating the DUID

After the DUID file is deleted, use the "restart ipv6-dhcp server" command to restart the server or add the IPv6 DHCP server setting in the configuration. At startup, the IPv6 DHCP server on the Switch obtains the MAC address of the IPv6 interface that is used as the IPv6 DHCP server interface. Then, the IPv6 DHCP server regenerates the DUID based on the obtained MAC address and time information.

(c) Checking the DUID

To check the DUID, execute the "show ipv6 dhcp server statistics" command. The DUID is displayed for < Server DUID >. For details, see "Configuration Guide".

7.6 IPv6 unicast routing communication failures

7.6.1 No RIPng routing information exists

If RIPng routing information cannot be found in the routing information obtained by the Switch, isolate the cause of the problem according to the failure analysis method described in the following table.

Also, if network partitioning is used and the maximum number of routes is set by the "maximum routes" configuration command, first, follow the failure analysis method described in "7.6.4 No IPv6 routing information exists in the VRF".

Table 7-21 Failure analysis method for RIPng

No.	Items to check and commands	Action
1	Display the RIPng neighboring information. show ipv6 rip neighbor	If the interface of the neighboring router is not displayed, go to No. 2.
		If the interface of the neighboring router is displayed, go to No. 3.
2	Check whether the RIPng setting in the configuration is correct.	If the configuration is correct, go to No. 3.
		If the configuration is not correct, modify the configuration.
3	Check whether RIPng packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
		If the packets are not discarded, check whether the neighboring router is advertising the RIPng route.

7.6.2 No OSPFv3 routing information exists

If OSPFv3 routing information cannot be found in the routing information obtained by the Switch, isolate the cause of the problem according to the failure analysis method described in the following table.

Also, if network partitioning is used and the maximum number of routes is set by the "maximum routes" configuration command, first, follow the failure analysis method described in "7.6.4 No IPv6 routing information exists in the VRF".

Table 7-22 Failure analysis method for OSPFv3

No.	Items to check and commands	Action
1	Displays the OSPFv3 interface status. show ipv6 ospf interface <Interface Name>	If the interface status is DR or P to P, go to No. 3.
		If the interface status is BackupDR or DR Other, go to No. 2.
		If the interface status is Waiting, wait for a while and execute the command again. Go to No. 1.
2	Check the neighboring router status with DR from the information in Neighbor List.	If the neighboring router status with DR is other than Full, go to No. 4.
		If the neighboring router status with DR is Full, go to No. 5.
3	Check the status of every neighboring router from the information in Neighbor List.	If the status of any neighboring router is other than Full, go to No. 4.
		If the status of every neighboring router is Full, go to No. 5.
4	Check whether the OSPFv3 setting in the configuration is correct.	If the configuration is correct, go to No. 5.
		If the configuration is not correct, modify the configuration.
5	Check the route that has learned the OSPFv3 route. show ipv6 route all-routes	If the route is InActive, go to No. 6.
		If the route does not exist, check whether the neighboring router is advertising the OSPFv3 route.
6	Check whether OSPFv3 packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
		If the packets are not discarded, check whether the neighboring router is advertising the OSPFv3 route.

7.6.3 No BGP4+ routing information exists

If BGP4+ routing information cannot be found in the routing information obtained by the Switch, isolate the cause of the problem according to the failure analysis method described in the following table.

Also, if network partitioning is used and the maximum number of routes is set by the "maximum routes" configuration command, first, follow the failure analysis method described in "7.6.4 No IPv6 routing information exists in the VRF".

Table 7-23 Failure analysis method for BGP4+

No.	Items to check and commands	Action
1	Check the BGP4+ peer status. show ipv6 bgp neighbors	If the peer status is other than Established, go to No. 2.
		If the peer status is Established, go to No. 3.
2	Check whether the BGP4+ setting in the configuration is correct.	If the configuration is correct, go to No. 3.
		If the configuration is not correct, modify the configuration.
3	Check whether the BGP4+ route has been learned. show ipv6 bgp received-routes	If the route exists but its status is not active, go to No. 4.
		If the route does not exist, go to No. 5.
4	Check whether the routing information that resolves the next hop address of the BGP4+ route exists. show ipv6 route	If the routing information that resolves the next hop address exists, go to No. 5.
		If the routing information that resolves the next hop address does not exist, perform the failure analysis for the protocol for learning the routing information.
5	Check whether BGP4+ packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
		If the packets are not discarded, check whether the neighboring router is advertising the BGP4+ route.

7.6.4 No IPv6 routing information exists in the VRF

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

Table 7-24 Failure analysis method for VRF

No.	Items to check 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 ipv6 vrf	If the number of routes is equal to or larger than the maximum value, go to No. 2.
		If the number of routes is less than the maximum value, perform the failure analysis for the protocol for the route that does not exist. RIPng: "7.6.1 No RIPng routing information exists" OSPFv3: "7.6.2 No OSPFv3 routing information exists" BGP4+: "7.6.3 No BGP4+ routing information exists"
2	Check the maximum number of routes in VRF specified in the configuration.	Increase the maximum number, or reduce the number of routes by, for example, aggregating the routes.

7.7 Communication failures in the IPv6 multicast routing function

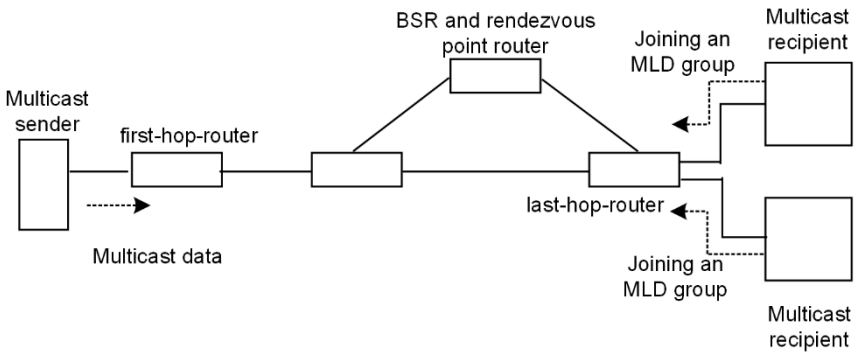
This section describes actions to be taken when an IPv6 multicast communication failure occurs on the Switch.

7.7.1 Communication is not possible on the IPv6 PIM-SM networks

If multicast forwarding is not possible in an IPv6 PIM-SM network configuration, isolate the cause of the problem according to the failure analysis method described below.

The following figure shows an example of an IPv6 PIM-SM network.

Table 7-11 Example of IPv6 PIM-SM network



Notes

- BSR: The router that distributes rendezvous point information (For details, see "Configuration Guide".)
- Rendezvous point router: The router that forwards packets to the multicast receivers if the destination of the packets has not been determined (For details, see "Configuration Guide".)
- first-hop-router: The router that is connected directly to the multicast sender
- last-hop-router: The router that is connected directly to the multicast receivers

(1) Items checked in common

The following table shows the items checked in common for all the Switches in an IPv6 PIM-SM network configuration.

Table 7-25 Items checked in common

No.	Items to check and commands	Action
1	Make sure that the setting for using the multicast function (ipv6 multicast routing) exists in the configuration. show running-config	If the setting for using the multicast function does not exist, modify the configuration.
2	Make sure that the address setting for the loopback interface exists in the configuration. show running-config	If the address setting for the loopback interface does not exist in the configuration, modify the configuration.
3	Make sure that PIM is running on one or more interfaces. show ipv6 pim interface	If PIM is not running, check and modify the configuration so that PIM runs on at least one of the interfaces.

No.	Items to check and commands	Action
4	Check whether MLD snooping is set for the interface on which PIM runs. show mld-snooping	If MLD snooping is set, check the following: - Check whether the multicast router port for MLD snooping is set for the port connected to the neighboring router. - See "4.6 MLD snooping communication failures".
5	Check whether protocol packets or multicast packets are discarded by a filter or QoS on the interfaces on which PIM and MLD run.	For the checking method and action to take, see "10.2 Checking discarded packets".
6	Check the PIM neighboring information. show ipv6 pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ipv6 pim interface" command and check that PIM is running on the interface connected with the neighboring routers. - Check the settings of the neighboring routers.
7	Check whether the unicast route to the multicast data sender exists. show ipv6 route	If the unicast route does not exist, see "7.6 IPv6 unicast routing communication failures".
8	Make sure that PIM is running on the interface connected to the next hop address to the multicast data sender. show ipv6 pim interface	If PIM is not running, check and modify the configuration so that PIM runs on the interface connected to the next hop address to the multicast data sender.
9	Check the configuration to make sure that the PIM-SSM group addresses do not contain the forwarding target group address. show running-config	If the PIM-SSM group addresses contain the forwarding target group address, modify the configuration.
10	Make sure that BSR has been determined. This checking is not required if the rendezvous point for the forwarding target group address is a static rendezvous point. show ipv6 pim bsr	If BSR has not been determined, check whether the unicast route to BSR exists. If the unicast route does not exist, see "7.6 IPv6 unicast routing communication failures". If the unicast route exists, check whether PIM-SM is set up on the interface directed toward BSRs. If PIM-SM is set, check the BSR settings. If the Switch is used as the BSR, see "(2) Items to check for BSR".
11	Make sure that the rendezvous point has been determined. show ipv6 pim rp-mapping	If the rendezvous point has not been determined, check whether the unicast route to the rendezvous point exists. If the unicast route does not exist, see "7.6 IPv6 unicast routing communication failures". If the unicast route exists, check whether PIM-SM is set up on the interface directed toward rendezvous points. If the PIM-SM is set, check the rendezvous point settings. If the Switch is used as the rendezvous point, see "(3) Items to check for the rendezvous point router".
12	Make sure that the rendezvous point group addresses contain the forwarding target group address. show ipv6 pim rp-mapping	If the forwarding target group address is not contained, check the rendezvous point router settings.
13	Make sure that multicast forwarding entries exist. show ipv6 mcache	If multicast forwarding entries do not exist, make sure that multicast data has reached the upstream port. If multicast data has not reached the upstream port, check the settings of the multicast sender or upstream router.
14	Make sure that multicast routing information exists. show ipv6 mroute	If multicast routing information does not exist, check the downstream router settings.

No.	Items to check and commands	Action
15	Check whether the number of the multicast routing information entries or multicast forwarding entries exceeds its upper limit. For the multicast routing information entries: show ipv6 mroute For the multicast forwarding entries: show ipv6 mcache netstat multicast	If a warning is displayed, check whether an unexpected multicast routing information entry or unexpected multicast forwarding entry has been created. If many negative caches are found among the multicast forwarding entries, check whether there is a terminal that is sending unnecessary packets.

(2) Items to check for BSR

The following table shows the items to check when the Switch is used as BSR in an IPv6 PIM-SM network configuration.

Table 7-26 Items to check for BSR

No.	Items to check and commands	Action
1	Make sure that the Switch is a BSR candidate. show ipv6 pim bsr	If the Switch is not a BSR candidate, check and modify the configuration so that the Switch can work as a BSR candidate. If an address is not set for the loopback interface, the Switch does not work as a BSR candidate. Also make sure that a loopback interface address is set.
2	Make sure that the Switch is used as BSR. show ipv6 pim bsr	If the Switch is not used as BSR, check the priorities of other BSR candidates. A larger value represents a higher priority. If the priority is the same among BSR candidates, the BSR candidate that has the highest BSR address becomes BSR.

(3) Items to check for the rendezvous point router

The following table shows the items to check when the Switch is used as a rendezvous point router in an IPv6 PIM-SM network configuration.

Table 7-27 Items to check for the rendezvous point router

No.	Items to check and commands	Action
1	Make sure that the Switch is a rendezvous point candidate for the forwarding target group address. show ipv6 pim rp-mapping	If the Switch is not a rendezvous point candidate for the forwarding target group address, check and modify the configuration so that the Switch can work as a rendezvous point candidate for the forwarding target group address. If an address is not set for the loopback interface, the Switch does not work as a rendezvous point candidate. Also make sure that a loopback interface address is set.
2	Make sure that the Switch is the rendezvous point for the forwarding target group address. show ipv6 pim rp-hash <Group Address>	If the Switch is not the rendezvous point, check the priorities of other rendezvous point candidates. A smaller value represents a higher priority. If the priority of another rendezvous point candidate is higher than that of the Switch, the Switch does not work as the rendezvous point. If the priority is the same between another candidate and the Switch, they are assigned to a different group address due to the protocol specification, and the Switch might not work as the rendezvous point for the target group. If you want to use the Switch as the rendezvous point, set a higher priority for the Switch than other rendezvous point candidates.

(4) Items to check for last-hop-router

The following table shows the items to check when the Switch is used as last-hop-router in an IPv6 PIM-SM network configuration.

Table 7-28 Items to check for last-hop-router

No.	Items to check and commands	Action
1	Make sure that MLD is running on the interface connected to the multicast receivers. show ipv6 mld interface	If MLD is not running, check and modify the configuration so that MLD runs on the interface.
2	Make sure that the multicast receivers participate in the forwarding target group through MLD. show ipv6 mld group	If a multicast receiver does not participate in the forwarding target group, check the multicast receiver settings.
3	If the interface in which the forwarding target group participates exists and PIM runs, make sure that the Switch is DR. show ipv6 pim interface	If the Switch is not DR, check the DR of the forwarding target interface.
4	Check whether MLD snooping is set for the interface on which the join static group function is used. show mld-snooping	If MLD snooping is set, check the following: - Check whether the multicast router port for MLD snooping is set for the destination port. - See "4.6 MLD snooping communication failures".
5	Check whether any anomaly has been detected on any interface. show ipv6 mld interface	Make sure that no warning information is displayed for Notice. If warning information is displayed, check the following: - L: More participation requests than the expected maximum number have occurred. Check the number of connected users. - Q: The MLD version is different from that on the neighboring router. Use the same MLD version. - R: A user is sending a report that cannot be received with the current settings. Change the MLD version on the Switch, or check the settings of the participation user. - S: Parts of the participation information have been discarded because the number of sources stored in a message exceeds the maximum number for MLDv2. Check the settings of the participation user.

(5) Items to check for first-hop-router

The following table shows the items to check when the Switch is used as first-hop-router in an IPv6 PIM-SM network configuration.

Table 7-29 Items to check for first-hop-router

No.	Items to check and commands	Action
1	Make sure that the Switch is directly connected to the multicast sender.	If the Switch is not connected directly, check the network configuration.
2	Make sure that PIM or MLD is running on the interface connected to the multicast sender. show ipv6 pim interface show ipv6 mld interface	If PIM or MLD is not running, check and modify the configuration so that PIM or MLD runs on the interface.

No.	Items to check and commands	Action
3	Check whether multicast routing information exists. show ipv6 mroute	If multicast routing information does not exist, make sure that the multicast data source address is the network address of the interface directly connected to the multicast sender.

7.7.2 Multicast data is forwarded twice in an IPv6 PIM-SM network

If multicast data is forwarded twice in an IPv6 PIM-SM network configuration, check the settings of each router and if multiple routers exist in one network, modify the settings so that PIM runs on the interface in the network.

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

Table 7-30 Items to check when data continues to be forwarded twice

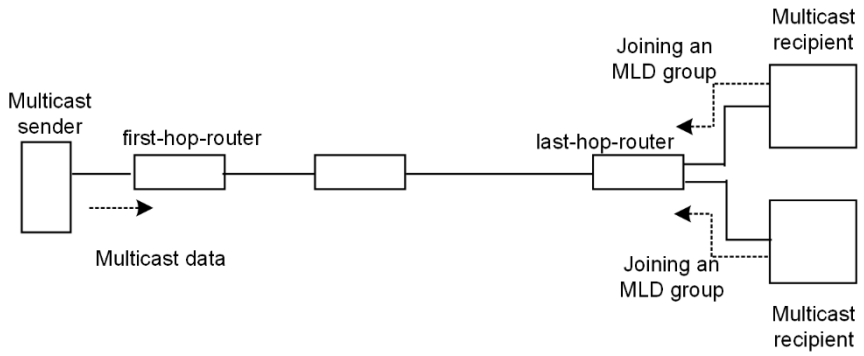
No.	Items to check and commands	Action
1	Check the PIM neighboring information of the interface belonging to the network with multiple routers. show ipv6 pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ipv6 pim interface" command and check that PIM is running on the interface connected with the neighboring routers. - Check whether protocol packets are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets". - Check the settings of the neighboring routers.

7.7.3 Communication is not possible on the IPv6 PIM-SSM networks

If multicast forwarding is not possible in an IPv6 PIM-SSM network configuration, isolate the cause of the problem according to the failure analysis method described below.

The following figure shows an example of an IPv6 PIM-SSM network.

Table 7-12 Example of IPv6 PIM-SSM network



Notes

- first-hop-router: The router that is connected directly to the multicast sender
- last-hop-router: The router that is connected directly to the multicast receivers

(1) Items checked in common

The following table shows the items checked in common for all the Switches in an IPv6 PIM-SSM network configuration.

Table 7-31 Items checked in common

No.	Items to check and commands	Action
1	Make sure that the setting for using the multicast function (ipv6 multicast routing) exists in the configuration. show running-config	If the setting for using the multicast function does not exist, modify the configuration.
2	Make sure that the address setting for the loopback interface exists in the configuration. show running-config	If the address setting for the loopback interface does not exist in the configuration, modify the configuration.
3	Make sure that PIM is running on one or more interfaces. show ipv6 pim interface	If PIM is not running, check and modify the configuration so that PIM runs on at least one of the interfaces.
4	Check whether MLD snooping is set for the interface on which PIM runs. show mld-snooping	If MLD snooping is set, check the following: - Check whether the multicast router port for MLD snooping is set for the port connected to the neighboring router. - See "4.6 MLD snooping communication failures".
5	Check whether protocol packets or multicast packets are discarded by a filter or QoS on the interfaces on which PIM and MLD run.	For the checking method and action to take, see "10.2 Checking discarded packets".
6	Check the PIM neighboring information. show ipv6 pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ipv6 pim interface" command and check that PIM is running on the interface connected with the neighboring routers. - Check the settings of the neighboring routers.
7	Check whether the unicast route to the multicast data sender exists. show ipv6 route	If the unicast route does not exist, see "7.6 IPv6 unicast routing communication failures".
8	Make sure that PIM is running on the unicast route send interface to the multicast data sender. show ipv6 pim interface	If PIM is not running, check and modify the configuration so that PIM runs on the unicast route send interface.
9	Check the configuration to make sure that the PIM-SSM group addresses contain the forwarding target group address. show running-config	If the PIM-SSM group addresses do not contain the forwarding target group address, modify the configuration.
10	Check whether multicast routing information exists. show ipv6 mroute	If multicast routing information does not exist, check the downstream router settings.
11	Check whether the number of the multicast routing information entries or multicast forwarding entries exceeds its upper limit. For the multicast routing information entries: show ipv6 mroute For the multicast forwarding entries: show ipv6 mcache netstat multicast	If a warning is displayed, check whether an unexpected multicast routing information entry or unexpected multicast forwarding entry has been created. If many negative caches are found among the multicast forwarding entries, check whether there is a terminal that is sending unnecessary packets.

(2) Items to check for last-hop-router

The following table shows the items to check when the Switch is used as last-hop-router in an IPv6 PIM-SSM network configuration.

Table 7-32 Items to check for last-hop-router

No.	Items to check and commands	Action
1	If the mode of the multicast receivers is MLDv1 or MLDv2 (EXCLUDE mode), make sure that ipv6 mld ssm-map enable is set in the configuration. This setting enables the use of PIM-SSM in MLDv1 or MLDv2 (EXCLUDE mode). show running-config	If the configuration does not contain the setting to enable the use of PIM-SSM in MLDv1 or MLDv2 (EXCLUDE mode), modify the configuration.
2	If the mode of the multicast receivers is MLDv1 or MLDv2 (EXCLUDE mode), make sure that ipv6 mld ssm-map static is set in the configuration. This setting enables the linkage behavior with PIM-SSM in MLDv1 or MLDv2 (EXCLUDE mode) for the group address and source address that are forwarded via PIM-SSM. show running-config	If the configuration does not contain the setting to enable the linkage behavior with PIM-SSM in MLDv1 or MLDv2 (EXCLUDE mode), modify the configuration.
3	Make sure that MLD is running on the interface connected to the multicast receivers. show ipv6 mld interface	If MLD is not running, check and modify the configuration so that MLD runs on the interface.
4	Make sure that no MLD warning information is displayed on the interface connected to the multicast receivers. show ipv6 mld interface	If any warning information is displayed, take action according to the information. For details about the contents of each warning, see "Operation Command Reference".
5	Make sure that the multicast receivers participate in the forwarding target group through MLD. show ipv6 mld group	If a multicast receiver does not participate in the forwarding target group, check the multicast receiver settings.
6	Check whether the source address is registered in the MLD group information. show ipv6 mld group	If the mode of the multicast receivers is MLDv2 (INCLUDE mode) and the source address is not registered, check the multicast receivers. If the mode of the multicast receivers is MLDv1 or MLDv2 (EXCLUDE mode), make sure that the configuration contains the setting to enable the linkage behavior with PIM-SSM.
7	If the interface in which the forwarding target group participates exists and PIM runs, make sure that the Switch is DR. show ipv6 pim interface	If the Switch is not DR, check the DR of the forwarding target interface.
8	Check whether MLD snooping is set for the interface on which the join static group function is used. show mld-snooping	If MLD snooping is set, check the following: - Check whether the multicast router port for MLD snooping is set for the destination port. - See "4.6 MLD snooping communication failures".
9	Check whether any anomaly has been detected on any interface. show ipv6 mld interface	Make sure that no warning information is displayed for Notice. If warning information is displayed, check the following: - L: More participation requests than the expected maximum number have occurred. Check the number of connected users.

No.	Items to check and commands	Action
		- Q: The MLD version is different from that on the neighboring router. Use the same MLD version. - R: A user is sending a report that cannot be received with the current settings. Change the MLD version on the Switch, or check the settings of the participation user. - S: Parts of the participation information have been discarded because the number of sources stored in a message exceeds the maximum number for MLDv2. Check the settings of the participation user.

(3) Items to check for first-hop-router

The following table shows the items to check when the Switch is used as first-hop-router in an IPv6 PIM-SSM network configuration.

Table 7-33 Items to check for first-hop-router

No.	Items to check and commands	Action
1	Make sure that the Switch is directly connected to the multicast sender.	If the Switch is not connected directly, check the network configuration.
2	Make sure that PIM or MLD is running on the interface connected to the multicast sender. show ipv6 pim interface show ipv6 mld interface	If PIM or MLD is not running, check and modify the configuration so that PIM or MLD runs on the interface.
3	Check whether multicast data has reached the Switch.	If the multicast data has not reached the Switch, check the settings of the multicast sender.
4	Check whether the group address and source address are the same between multicast data and multicast routing information. show ipv6 mroute show netstat multicast	If the different group address and source address are used, check the settings of the multicast sender and last-hop-router.

7.7.4 Multicast data is forwarded twice in an IPv6 PIM-SSM network

If multicast data is forwarded twice in an IPv6 PIM-SSM network configuration, check the settings of each router and if multiple routers exist in one network, modify the settings so that PIM runs on the interface in the network.

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

Table 7-34 Items to check when data continues to be forwarded twice

No.	Items to check and commands	Action
1	Check the PIM neighboring information of the interface belonging to the network with multiple routers. show ipv6 pim neighbor	If neighboring routers are not displayed, check the following: - Use the "show ipv6 pim interface" command and check that PIM is running on the interface connected with the neighboring routers. - Check whether protocol packets are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets". - Check the settings of the neighboring routers.

7.7.5 IPv6 multicast communication problems in VRF

If a problem on IPv6 multicast communication occurs in VRF, check the following.

Table 7-35 Items to check for VRF

No.	Items to check and commands	Action
1	Check the port number and VLAN ID to make sure that the interface for VRF is correct. show ipv6 vrf show vlan show ipv6 pim interface	If the settings are not correct, modify the configuration or connection.
2	If the Switch is used as the rendezvous point, make sure that the Switch is working as a rendezvous point candidate on the target VRF. show ipv6 pim vrf all rp-mapping	If the Switch is not working as a rendezvous point candidate, check whether the address of the loopback interface for the target VRF is specified in the rendezvous point candidate setting in the configuration. show running-config
3	If the Switch is used as BSR, make sure that the Switch is working as a BSR candidate on the target VRF. show ipv6 pim vrf all bsr	If the Switch is not working as a BSR candidate, check whether the address of the loopback interface for the target VRF is specified in the BSR candidate setting in the configuration. show running-config
4	If multiple VRFs are used, check whether a global network or specific VRF occupies an unexpectedly large number of multicast forwarding entries. show ipv6 mcache vrf all	If a global network or specific VRF occupies more multicast forwarding entries than expected in the network design, check whether any unexpected multicast forwarding entries are created. If many negative caches are found, check whether there is a terminal that is sending unnecessary packets. Also, set the maximum number of forwarded entries for each VRF to prevent a global network or specific VRF from occupying forwarded entries. Target configuration: ipv6 pim vrf <vrf id> mcache-limit <number>
5	For each VRF, check the items described in "7.7.1 Communication is not possible on the IPv6 PIM-SM networks" through "7.7.4 Multicast data is forwarded twice in an IPv6 PIM-SSM network".	Specify the target VRF for each command to check the information of the VRF. For details about specifying VRF, see "Operation Command Reference".

7.7.6 IPv6 multicast communication problems in an extranet

To resolve problems on IPv6 multicast communication in an extranet, first, try to use the check items described in "7.7.5 IPv6 multicast communication problems in VRF" and make sure that multicast communication is possible in each VRF. After that, check the following.

Table 7-36 Items to check for an extranet

No.	Items to check and commands	Action
1	Make sure that the unicast route from the destination VRF to the source address is the expected VRF or global network. show ipv6 rpf	If it is not the case, check the settings of the unicast extranet.
2	Make sure that the protocol (PIM-SM or PIM-SSM) for the IPv6 multicast address used in the extranet is the same between the	If the protocol is different between the destination VRF and the upstream VRF, select a suitable IPv6 multicast address so that the protocol can be the same between them.

No.	Items to check and commands	Action
	destination VRF and the upstream VRF. show running-config	
3	For the upstream VRF, check whether the unicast route to the source address is not another VRF. show ipv6 rpf	Set the upstream VRF so that the unicast route to the source address is a VRF with an actual interface in the VRF.
4	If the PIM-SM VRF gateway is used, make sure that (*,G) entries have been generated in the upstream VRF. Also, make sure that V is displayed for Flags for the target (*,G) entry. show ipv6 mroute	If (*,G) entries are not generated correctly, make sure that the IPv6 multicast address used in extranet communication has been specified as the host address and permitted for the IPv6 multicast route filtering for the upstream VRF.
5	If the PIM-SM VRF gateway is used, make sure that the destination VRF is displayed for the downstream interface for the (*,G) entry generated in the upstream VRF. show ipv6 mroute	If the destination VRF does not exist in the downstream interface for the (*,G) entry of the upstream VRF, make sure that the destination VRF has been permitted for route-map that specifies the host address for IPv6 multicast route filtering in the upstream VRF. If no specific VRF is specified for route-map by the "match vrf" command, every VRF is permitted to be a destination.
6	If (denied) is displayed for the VRF of the upstream interface by the "show ipv6 mroute" command, IPv6 multicast route filtering for the upstream VRF has not been set correctly. Check the IPv6 multicast route filtering of the upstream VRF in the configuration. show ipv6 mroute show running-config	Make sure that the IPv6 multicast address and destination VRF that are used in extranet communication have been permitted for the IPv6 multicast route filtering for the upstream VRF. If neither specific IPv6 multicast address nor specific VRF is specified for the IPv6 multicast route filtering, all IPv6 multicast addresses and VRFs are permitted.

8 Troubleshooting by Function

This chapter describes how to take actions when a failure occurs on each function.

8.1 DHCP snooping problems

8.1.1 Problems related to DHCP

If DHCP cannot distribute IP addresses in a DHCP snooping configuration, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 8-1 Failure analysis method for when DHCP cannot distribute IP addresses in a DHCP snooping configuration

No.	Items to check	Action
1	Execute the "show logging" command, and check whether any hardware failure is recorded in the operation log.	If any hardware failure is recorded in the operation log, replace the device.
		For other cases, go to No. 2.
2	Check whether IP addresses cannot be newly distributed or only IP addresses already assigned cannot be updated.	If IP addresses cannot be newly distributed, go to No. 3.
		If assigned IP addresses cannot be updated, go to No. 9.
3	Execute the "show ip dhcp snooping statistics" command and check the running status of DHCP snooping.	If a port is displayed as an untrusted port at which DHCP snooping is enabled and the port is the one connected to the target device (to which an IP address cannot be distributed), go to No. 4.
		If the target device is connected to another port, DHCP snooping is not enabled for the device. Check the network configuration and the settings of the DHCP server, and if there is no problem, go to No. 10.
4	Check the connection method between the clients and server.	If the Switch is connected as a Layer 2 switch between the clients and server, go to No. 8.
		If the DHCP server on the Switch is used, go to No. 5.
		If the DHCP relay on the Switch is used, go to No. 5.
		If there is a DHCP relay between the Switch and clients, go to No. 6.
		If a device that adds Option 82 data is located between the Switch and clients, go to No. 7.
		If multiple conditions described above are met, see each item in the order above.
5	Make sure that there is no problem with the behavior of the DHCP server and DHCP relay.	See "7.1.2 IP address is not assigned for the DHCP/BOOTP relay agent" and make sure that the DHCP server and DHCP relay can distribute IP addresses. If there is no problem, go to No. 8.
6	If packets via DHCP relay are forwarded, make sure that the "no ip dhcp snooping verify mac-address" configuration command is set.	DHCP packets forwarded via DHCP relay are discarded because the client hardware address and the source MAC address in the packets are different. To forward those packets, set the "no ip dhcp snooping verify mac-address" configuration command.
7	If packets that contain the relay agent information option are forwarded, make sure that the "ip dhcp snooping information option allow-untrusted" configuration command is set.	By default, packets that contain the relay agent information option (Option 82) are discarded. To forward those packets, set the "ip dhcp snooping information option allow-untrusted" configuration command.
8	Make sure that the DHCP server is connected to a trusted port.	DHCP server response packets from an untrusted port are discarded. If the target DHCP server is an authorized one, set the "ip dhcp snooping trust" configuration command for the port to which the DHCP server is connected.

No.	Items to check	Action
		Note that if the DHCP server on the Switch is used, the port can be an untrusted port. If the DHCP relay on the Switch is used, the DHCP server must be connected to a VLAN exempt from DHCP snooping or to a trusted port.
9	Use the "show ip dhcp snooping binding" command and check the binding information.	If the IP address cannot be updated after the device restarts, check the save status of the binding database. See "8.1.2 Problems related to saving the binding database".
		You might find that a different port or VLAN ID is displayed in the binding information for a target entry (that has the target MAC address and target IP address). In this case, the connection port or the VLAN capacity limit might have been changed after assignment of an IP address. To continue using the current port or VLAN, obtain an IP address again.
10	Others	If any of the above actions do not resolve your problem, check other functions used in the device according to this manual.

8.1.2 Problems related to saving the binding database

If binding information cannot be inherited at a device restart, probable causes are problems related to saving the binding database. Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 8-2 Failure analysis method for problems related to saving the binding database

No.	Items to check	Action
1	Use the "show mc" or "show flash" command and check whether there is a sufficient amount of unused space in the flash memory or memory card.	If there is not a sufficient amount of unused space, delete unnecessary files to have an enough space.
		If there is no problem, go to No. 2.
2	Check the storage destination of the binding database.	If the binding database is saved in the flash memory, go to No. 4.
		If the binding database is saved in a memory card, go to No. 3.
3	Execute the "ls mc-dir" command to check whether the directory for saving the database exists in the memory card.	If the directory does not exist, use the "mkdir" command to create the directory.
		If there is no problem, go to No. 4.
4	Check the setting of the "ip dhcp snooping database write-delay" configuration command. Also, execute the "show ip dhcp snooping binding" command and check the last time when the binding database was saved.	Even if the binding information is updated, the binding database is not saved until the specified time passes. After an IP address is distributed, wait a while until the specified time passes, and then make sure that the last time when the binding database was saved is updated.
		If there is no problem, go to No. 5.
5	Make sure that the lease time of the IP addresses distributed to the DHCP clients is longer than the wait time for saving the database.	If the lease time is shorter, the lease of the IP addresses might expire before the binding database is completely read in. Use the "ip dhcp snooping database write-delay" configuration command to shorten the wait time for saving the database on the Switch. Alternatively, on the DHCP server, extend the lease time of the IP addresses.
		If there is no problem, go to No. 6.
6	Others	If there is no problem when the binding database is saved in the flash memory, but the binding information cannot be inherited when the database is saved in a memory card, replace the memory card.

No.	Items to check	Action
		Note that if you are planning long-term operation, save the binding database in a memory card.

8.1.3 Problems related to ARP

If ARP packets are discarded, IPv4 communication is not possible. A probable cause of ARP packets being discarded is dynamic ARP inspection. Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 8-3 Failure analysis method for problems caused by dynamic ARP inspection

No.	Items to check	Action
1	Check the DHCP snooping setting information.	See "8.1.1 Problems related to DHCP", and make sure that DHCP snooping is working normally.
		If there is no problem, go to No. 2.
2	Execute the "show ip arp inspection statistics" command and check the running status of dynamic ARP inspection.	If a port is displayed as an untrusted port at which dynamic ARP inspection is enabled and the port is the one at which IPv4 communication is not possible, go to No. 3.
		If the target device is connected to another port, dynamic ARP inspection is not enabled for the device. Check the network configuration and the settings of the device on which IPv4 communication is not possible, and if there is no problem, go to No. 4.
3	Execute the "show ip dhcp snooping binding" command, and make sure that the binding information is present for the device on which communication is not possible.	If the binding information is not present and the target device has a fixed IP address, set the "ip source binding" configuration command. If the binding information is not present and the target device obtains an IP address by DHCP, obtain an IP address again.
4	Others	If any of the above actions do not resolve your problem, check other functions used in the device according to this manual.

8.1.4 Communication problems due to causes other than DHCP and ARP

If terminal filters are enabled, all packets are discarded, except DHCP and ARP packets from devices not in the binding information. Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 8-4 Failure analysis method for problems caused by terminal filters

No.	Items to check	Action
1	Check the DHCP snooping setting information.	See "8.1.1 Problems related to DHCP", and make sure that DHCP snooping is working normally.
		If there is no problem, go to No. 2.
2	Check whether the "ip verify source" configuration command is set for the target port.	If the "ip verify source" configuration command is set, packets from devices not in the binding information are discarded. If there is no problem, go to No. 3.
		If the "ip verify source" configuration command is not set, go to No. 4.
3	Execute the "show ip dhcp snooping binding" command, and make sure that the binding information is present for the device on which communication is not possible.	If the binding information is not present and the target device has a fixed IP address, set the "ip source binding" configuration command. If the binding information is not present and the target device obtains an IP address by DHCP, obtain an IP address again.
4	Others	If any of the above actions do not resolve your problem, check other functions used in the device according to this manual.

8.2 Policy-based mirroring problems

8.2.1 Mirroring fails

If the target flow is not mirrored while the policy-based mirroring is enabled, isolate the cause of the problem according to the failure analysis method described in the following table.

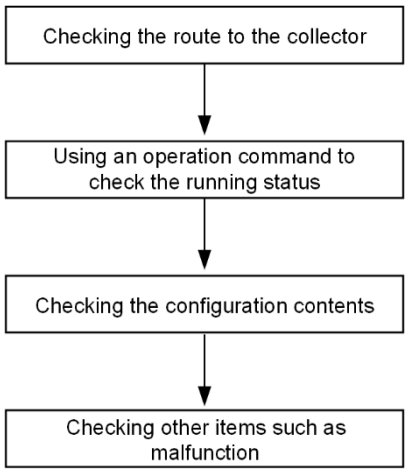
Table 8-5 Failure analysis method for when the target flow is not mirrored

No.	Items to check and commands	Action
1	In the configuration, check that there is the setting of an access list in which the destination interface list for policy-based mirroring is specified as the behavior target. - show running-config	If there is no setting of an access list in which the destination interface list for policy-based mirroring is specified as the behavior target, modify the configuration.
		If there is the setting of an access list in which the destination interface list for policy-based mirroring is specified as the behavior target, go to No. 2.
2	Make sure that the flow detection mode on the receiving side is set to a mode that supports policy-based mirroring. - show system	If Flow detection mode is not set to the mode that supports policy-based mirroring, modify the configuration.
		If the number of entries for the target access list type of Used resources for Mirror inbound(Used/Max) is outside the scope of flow detection mode, modify the configuration.
		If the appropriate flow detection mode is set, go to No. 3.
3	On Matched packets, check the number of frames that matched the access list in which the destination interface list for policy-based mirroring is specified as the behavior target. - show access-filter	If the number of policy-based mirroring target frames and the value of Matched packets are different, the access list settings may be incorrect. Review the configuration.
		If the number of policy-based mirroring target frames matches the value of Matched packets, or if the configuration was reviewed and the access list settings were correct, go to No. 4.
4	Check the configuration for the mirror port set in the destination interface list. - show running-config	If the mirror port is not the expected interface, review the configuration.
		If the mirror port is the expected interface, go to No. 5.
5	Check the mirror port status. - show interfaces	If the mirror port is an Ethernet interface and the port status is other than active up, set the port status to active up.
		For other cases, go to No. 6.
6	Check the monitor port status. - show interfaces - show vlan detail	If the monitor port is an Ethernet interface and the port status is other than active up, set the port status to active up.
		Execute the "show vlan detail" command and check that the target VLAN status is Up and the data transfer status of the monitor port is Forwarding.
		If there is no abnormality in the status of the monitor port, go to No. 7.
7	Check whether the target frames are discarded by the sending-side filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".

8.3 sFlow statistics problems

The following figure shows the workflow for troubleshooting the sFlow statistics function on the Switch.

Figure 8-1 Workflow for troubleshooting the sFlow statistics function



8.3.1 sFlow packets cannot be sent to the collector

(1) Checking the route to the collector

See "7.1.1 Communication is not possible or is disconnected" and "7.5.1 Communication is not possible or is disconnected" and make sure that the network is appropriately connected to the collector. If the maximum size of an sFlow packet (max-packet-size) has been modified in the configuration, check whether it is possible to connect to the collector with the specified packet size.

(2) Using an operation command to check the behavior

Execute the "show sflow" command a few times to display the sFlow statistics, and check whether the sFlow statistics function is running. If the underlined values do not increase, see "(3) Checking the configuration". If the values increase, see "7.1.1 Communication is not possible or is disconnected", "7.5.1 Communication is not possible or is disconnected", and "(5) Checking the settings on the collector", and check whether the network is appropriately connected to the collector.

Figure 8-2 Example of the "show sflow" command output

```
> show sflow
Date 20XX/12/09 11:03:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  1:17:49
sFlow agent data :
 sFlow service version  : 4
 CounterSample interval rate: 2 seconds
 Default configured rate: 1 per 10430000 packets
 Default actual rate    : 1 per 2097152 packets
 Configured sFlow ingress ports : 1/0/3
 Configured sFlow egress  ports : ----
 Received sFlow samples :     2023   Dropped sFlow samples         :         0
 Exported sFlow samples :     2023   Couldn't export sFlow samples :         0
```

```
 Overflow time of sFlow queue: 0 seconds
sFlow collector data :
 Collector IP address: 192.168.0.251  UDP: 6343  Source IP address: 192.168.0.9
  Send FlowSample UDP packets   :     1667  Send failed packets:        0
  Send CounterSample UDP packets:     1759  Send failed packets:        0
```

Note: Make sure that the underlined values increase.

(3) Checking the configuration

Check the following in the active configuration:

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

Figure 8-3 Display example of configuration 1

```
(config)# show sflow
sflow destination 192.168.0.251  <-1
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2
sflow sample 10430000
sflow source 192.168.0.9
!
```

1. Collector information must be set correctly

- 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. Note that if a value that is much smaller than the recommended value is set, the CPU usage might increase.

Figure 8-4 Display example of configuration 2

```
(config)# show sflow
sflow destination 192.168.0.251
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2
sflow sample 10430000     <-1
sflow source 192.168.0.9
!
```

1. An appropriate value for the sampling interval must be set

Figure 8-5 Display example of operation command

```
> show sflow
Date 20XX/12/09 11:03:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  1:17:49
sFlow agent data :
 sFlow service version  : 4
 CounterSample interval rate: 2 seconds
 Default configured rate: 1 per 10430000 packets
 Default actual rate    : 1 per 2097152 packets
 Configured sFlow ingress ports : 1/0/3
```

```
 Configured sFlow egress  ports : ----
 Received sFlow samples :     2023   Dropped sFlow samples         :         0
 Exported sFlow samples :     2023   Couldn't export sFlow samples :         0
 Overflow time of sFlow queue: 0 seconds
sFlow collector data :
 Collector IP address: 192.168.0.251  UDP: 6343  Source IP address: 192.168.0.9
  Send FlowSample UDP packets   :     1667  Send failed packets:       0
  Send CounterSample UDP packets:     1759  Send failed packets:       0
                       :
```

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

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

Figure 8-6 Display example of configuration 3

```
(config)# show interface gigabitethernet 1/0/3
 interface gigabitethernet 1/0/3
 switchport mode trunk
 switchport trunk allowed vlan 20,2001,2251,2501,2751,3001-3004
                       :
 sflow forward ingress     <-1
!
```

1. sflow forward must be set here.

- Check whether sFlow packets are discarded by a filter or QoS for the physical port where flow statistics are implemented. For the checking method and action to take, see "10.2 Checking discarded packets".
- If the sender (agent) IP address of an sFlow packet has been set by using the "sflow source" command, make sure that the IP address has been assigned to the port of the Switch.

Figure 8-7 Display example of configuration 4

```
(config)# show sflow
sflow destination 192.168.0.251
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2
sflow sample 10430000
sflow source 192.168.0.9     <-1
!
```

1. The IP address assigned to a Switch port

(4) Checking the port status

Execute the "show interfaces" command, and make sure that the up/down status of the physical port on the Switch monitored by the sFlow statistics and the physical port connected to the collector is "active" (running normally).

Figure 8-8 Display example of port status

```
> show interfaces gigabitethernet 1/0/3
Date 20XX/12/09 11:03:36 UTP
NIF0: -
Port3: active up  1000BASE-T full(auto)    0012.e23e.f43f
       Time-since-last-status-change:1:17:21
       Bandwidth:1000000kbps  Average out:1Mbps  Average in:861Mbps
       Peak out:4Mbps at 10:57:49  Peak in:1000Mbps at 09:47:16
```

```
       Output rate:     9600bps         15pps
       Input  rate:    865.8Mbps     850.0kpps
       Flow control send   :off
       Flow control receive:off
       TPID:8100
                           :
>
```

Note: Make sure that the underlined part is "active up".

If the port status is DOWN, see "7.1.1 Communication is not possible or is disconnected" and "7.5.1 Communication is not possible or is disconnected".

(5) Checking the settings on the collector

- Make sure that the UDP port number (6343 by default) of the collector has been set so that data can be received. If data cannot be received, ICMP ([Type]Destination Unreachable [Code]Port Unreachable) is sent to the Switch.
- In addition, make sure that the collector currently used is correctly set.

8.3.2 Flow samples cannot be sent to the collector

If the problem cannot be resolved by checking the items in "8.3.1 sFlow packets cannot be sent to the collector", check the following.

(1) Checking whether packets are forwarded

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

Figure 8-9 Display example of port status

```
> show interfaces gigabitethernet 1/0/3
Date 20XX/12/09 11:03:36 UTP
NIF0: -
Port3: active up  1000BASE-T full(auto)   0012.e23e.f43f
       Time-since-last-status-change:1:17:21
       Bandwidth:1000000kbps  Average out:1Mbps  Average in:861Mbps
       Peak out:4Mbps at 10:57:49  Peak in:1000Mbps at 09:47:16
       Output rate:     9600bps         15pps
       Input  rate:    865.8Mbps     850.0kpps
       Flow control send   :off
       Flow control receive:off
       TPID:8100
                           :
>
```

Note: Check the underlined parts whether packets are forwarded.

(2) Checking the settings on the collector

Make sure that the collector currently used is correctly set.

8.3.3 Counter samples cannot be sent to the collector

If the problem cannot be resolved by checking the items in "8.3.1 sFlow packets cannot be sent to the collector", check the following.

(1) Checking the sending interval of counter samples

Make sure that the sending interval of counter samples related to the flow statistics is not zero in the configuration of the Switch. If the value is zero, counter sample data cannot be sent to the collector.

Figure 8-10 Display example of configuration

```
(config)# show sflow
sflow destination 192.168.0.251
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2     <-1
sflow sample 10430000
sflow source 192.168.0.9
!
```

1. 0 must not be set here

8.4 IEEE 802.3ah/UDLD function problems

8.4.1 Port enters inactive status

If the IEEE 802.3ah/UDLD function has deactivated a port, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 8-6 Failure analysis method for when the IEEE 802.3ah/UDLD function is used

No.	Items to check and commands	Action
1	Execute the "show efmoam" command and check the failure type for the port that was deactivated by the IEEE 802.3ah/UDLD function.	If Down(loop) is displayed for Link status, an L2 loop might have occurred in this network configuration. Revise the network configuration.
		If Down(uni-link) is displayed for Link status, go to No. 2.
2	Make sure that the IEEE 802.3ah/OAM function is enabled on the partner switch.	If the IEEE 802.3ah/OAM function is not enabled on the partner switch, enable the function.
		If the IEEE 802.3ah/OAM function is enabled on the partner switch, go to No. 3.
3	Execute the "show efmoam statistics" command and make sure that a prohibited configuration is not used.	If the count of Unstable displayed for Info TLV has been incremented, a configuration prohibited for the IEEE 802.3ah/UDLD function might be used. Make sure that only one device is specified as the destination for the target physical port.
		If the count of Unstable for Info TLV has not been incremented, go to No. 4.
4	Make sure that the Switch is directly connected to the partner switch.	If a media converter or hub is connected between switches, review and correct the network configuration so that the Switch is directly connected to the partner switch. If a relay device is absolutely necessary, use a media converter that allows the link status on both sides to be identical (however, using a relay device is not recommended).
		If the switches are directly connected, go to No. 5.
5	Execute the "show efmoam" command and check the number of times a response timeout occurred during failure detection.	If the value displayed for udld-detection-count is less than the initial value, a unidirectional link failure is more likely to be detected even if a failure has not actually occurred. Change this value.
		If the value displayed for udld-detection-count is equal to or more than the initial value, go to No. 6.
6	Check whether the control frames used for the IEEE 802.3ah/UDLD function have been discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
		If the control frames are not discarded, go to No. 7.
7	Test the line.	See "10.1 Line test" and test the line. If there is no problem, go to No. 8.
8	Check the cable connection.	The cable might be defective. Replace the cable used for the target port.

Note: IEEE 802.3ah/OAM: An OAM protocol defined in IEEE 802.3ah

IEEE 802.3ah/UDLD: Unidirectional link failure detection function specific for a Switch that uses IEEE 802.3ah/OAM

8.5 Neighboring device management function problems

8.5.1 Neighboring device information cannot be obtained by the LLDP function

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

Table 8-7 Failure analysis method for when the LLDP function is used

No.	Items to check and commands	Action
1	Execute the "show lldp" command and check the running status of the LLDP function.	If Enabled is displayed for Status, go to No. 2.
		If the displayed status is Disabled, the LLDP function has been disabled. Enable the LLDP function.
2	Execute the "show lldp" command and check the port information.	If information for the port to which the neighboring device is connected is displayed, go to No. 3.
		If information for the port to which the neighboring device is connected is not displayed, the LLDP function is disabled for the target port. Enable the LLDP function for the target port.
3	Execute the "show lldp statistics" command and check the statistics for the port to which the neighboring device is connected.	If the Tx count has been incremented but the Rx count has not, check No. 1 through No. 3 on the neighboring device. If the Tx count has also been incremented on the neighboring device, the connection between the devices might be incorrect. Check the connection.
		If the Discard count has been incremented, check the connection between the devices.
		For other cases, go to No. 4.
4	Execute the "show lldp" command and check the port status in the information for the port to which the neighboring device is connected.	If Up is displayed for Link, go to No. 5.
		If Down is displayed for Link, check the line status. For the checking method, see "3.1 Ethernet communication failures".
5	Execute the "show lldp" command, and check the number of neighboring device information items on the port to which the neighboring device is connected.	If 0 is displayed for Neighbor Counts, check No. 1 through No. 5 on the neighboring device. If the number of neighboring device information items is also 0 on the neighboring device, the connection between the devices might be incorrect. Check the connection. Also, check whether LLDP control frames are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets".

8.5.2 Neighboring device information cannot be obtained by the OADP function

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

Table 8-8 Failure analysis method for when the OADP function is used

No.	Items to check and commands	Action
1	Execute the "show oadp" command and check the running status of the OADP function.	If Enabled is displayed for Status, go to No. 2.
		If the displayed status is Disabled, the OADP function has been disabled. Enable the OADP function.
2	Execute the "show oadp" command and check the port information.	If information for the port to which the neighboring device is connected is displayed for Enabled Port, go to No. 3.
		If the port to which the neighboring device is connected is not displayed for Enabled Port, the OADP function is disabled for the port.

No.	Items to check and commands	Action
		Enable the OADP function for the port. Note that the OADP function is not enabled for a port that belongs to a channel group. Enable the OADP function for the channel group.
3	Execute the "show oadp statistics" command and check the statistics for the port to which the neighboring device is connected.	If the Tx count has been incremented but the Rx count has not, check No. 1 through No. 3 on the neighboring device. If the Tx count has also been incremented on the neighboring device, the connection between the devices might be incorrect. Check the connection.
		If the Discard/ERR count has been incremented, check the connection between the devices.
		For other cases, go to No. 4.
4	Execute the "show interfaces" command, and check the status of the port to which the neighboring device is connected.	If the status of the target port is active up, go to No. 5.
		For other cases, see "3.1 Ethernet communication failures".
5	Execute the "show vlan" command, and check the status of the VLAN that contains the port to which the neighboring device is connected.	If Up is displayed for Status, go to No. 6.
		If the displayed status is Disable, the OADP function is disabled. Enable the VLAN.
		For other cases, see "4 Troubleshooting of Layer 2 Switching".
6	Execute the "show oadp" command, and check the neighboring device information for the port to which the neighboring device is connected.	If the information is not displayed, check No. 1 through No. 6 on the neighboring device. If the neighboring device also does not display the neighboring device information for the target port, the connection between the devices might be incorrect. Check the connection. Also, check whether OADP control frames are discarded by a filter or QoS. For the checking method and action to take, see "10.2 Checking discarded packets".

8.6 BFD problems

8.6.1 Unable to generate a BFD session

If the "show bfd session" command does not display a BFD session that corresponds to the BFD monitoring target, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 8-9 Failure analysis method for when a BFD session cannot be generated

No.	Items to check and commands	Action
1	Make sure that the configuration for BFD monitoring has correctly been set on the Switch. - show running-config	If the configuration for BFD monitoring (bfd name and BFD linkage specification using BGP4) is not correctly set, modify the configuration.
2	Make sure that the number of BFD session does not exceed the capacity limit. - show logging	If the operation message "The number of BFD sessions exceeded the limit." is output, delete unnecessary BFD monitoring from the configuration, and then execute the "clear bfd session all" command. After command execution, make sure that similar operation messages are not output.
3	Check if setting the BFD session has failed. - show logging	If the operation message "BFD sessions could not be set because an error occurred." is output, the BFD program is not working correctly. Execute the "restart bfd" command. Make sure that similar operation messages are not output after restarting the BFD program.
4	Check that communication with the BFD monitoring target address is possible. - ping For multi-hop monitoring, use the source parameter to specify the loopback address as the source address.	If communication is not possible, see "7.1 IPv4 network communication failures".
5	Check whether packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
6	Check the settings of the partner switch.	BGP4 may not be able to recognize the partner switch or may not be able to select it as a monitoring target. Set BGP4 correctly on the partner switch as well.

8.6.2 Unable to establish a BFD session

If a BFD session cannot be established, or if the session status is unstable even after it is established, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 8-10 Failure analysis method for when a BFD session cannot be established

No.	Items to check and commands	Action
1	Check if setting the BFD session has failed. - show logging	If the operation message "BFD sessions could not be set because an error occurred." is output, the BFD program is not working correctly. Execute the "restart bfd" command. Make sure that similar operation messages are not output after restarting the BFD program.
2	For multi-hop monitoring, check the IPv4 address of the loopback interface. - show logging - show running-config	If the operation message "BFD packets cannot be sent because no valid loopback interface address has been set." is output, BFD packets will not be sent because an IPv4 address has not been set for the loopback interface. To send the packets, set an IPv4 address for the loopback

No.	Items to check and commands	Action
		interface. If VRF is used for the route to the partner switch, VRF must also be set to the loopback interface.
3	Check that communication with the BFD monitoring target address is possible. - ping For multi-hop monitoring, use the source parameter to specify the loopback address as the source address.	If communication is not possible, see "7.1 IPv4 network communication failures".
4	Make sure that BFD packets have not been discarded. - show bfd discard-packets	A BFD session cannot be established until a valid BFD packet is received. Check the number of discarded packets. - The Unknown Session count has increased The corresponding BFD session is not set on the Switch. Review the settings for the Switch. - The Invalid TTL/HopLimit count has increased Make sure that unintended packets are not forwarded. To establish a BFD session for multi-hop monitoring, set the "multihop" configuration command. - The Authentication Failure count has increased The partner switch has requested the use of an unsupported authentication method. Review the settings for the partner switch. - The Other Errors count has increased The partner switch may have requested a setting that causes the failure detection time to exceed 300 seconds. Review the settings for the partner switch. - Other cases BFD packet values are invalid. Review the settings and network status.
5	Check whether packets are discarded by a filter or QoS.	For the checking method and action to take, see "10.2 Checking discarded packets".
6	If the session status is unstable, check the cause of the BFD session down. - show bfd session	If Control Detection Time Expired is displayed for Diagnostic, BFD packets from the partner switch have not been received for a certain period of time. - A communication failure may have occurred. Check the route and partner switch. - If the detection multiplier (Multiplier) is less than 3, the packet delays will more easily be detected as a failure. If you want to stabilize the BFD session, set the detection multiplier to 3 or higher.
		If Neighbor Signaled Session Down is displayed for Diagnostic, the partner switch has brought down the BFD session. - Make sure that the BFD monitoring settings have not been changed or deleted on the partner switch. - Make sure that the BFD session is not disconnected on the partner switch. - The partner switch may not be able to receive BFD packets from the Switch. Check the route and BFD settings.
		If Path Down is displayed for Diagnostic, a valid route does not exist or is down. - Make sure that the source interface is not a management port. - Check the status of the source interface. For the checking method, see "3 Troubleshooting of Network Interfaces".

No.	Items to check and commands	Action
		If Administratively Down is displayed for Diagnostic, a BFD session is intentionally suppressed due to the operational status of the Switch. - Make sure that the BFD monitoring settings have not been changed or deleted on the Switch or the partner switch. - Check the configuration according to Nos. 1 and 2 in this table. - If neither of the above applies, specify the target BFD session number and execute the "clear bfd session" command. If the problem cannot be resolved or recurs frequently, execute the "clear bfd session all" command.
7	Check the configuration of the Switch to make sure that BFD monitoring is set correctly for the partner switch. - show running-config	If the BFD monitoring is not correctly set, modify the configuration.
8	Check the settings of the partner switch.	BFD must be set bidirectionally. Set BFD correctly on the partner switch as well.

9 How to Obtain Failure Information

This chapter mainly describes how to obtain failure information.

9.1 Collecting maintenance information

When a failure occurs with the device during operation, log information and dump information are automatically collected. You can also use operation commands to collect dump information.

9.1.1 Maintenance information

The maintenance information is shown in the table below. Note that when you are configuring a stack, maintenance information is stored in each member switch. For this reason, collect information from each member switch at the time of stack configuration.

Table 9-1 Maintenance information

Item	Path and file name	Remarks
Dump information file created when the device restarts	/dump0/rmdump	- Use binary mode to transfer these files with the "ftp" command. - Delete these files after the transfer is completed.
Dump information file created when the network interface fails	/usr/var/hardware/ni00.000	
Log information	Depending on the source directory, the files are stored with the following names: Operation log: log.txt Reference log: log_ref.txt	- Use ASCII mode to transfer these files with the "ftp" command.
Information when a failure arises in the configuration file	In administrator mode, execute the following commands to copy two files to the home directory. Then transfer these files. cp /config/system.cnf system.cnf cp /config/system.txt system.txt When configuring a stack, copy the files of each member switch to the master switch. cp switch <switch no.> /config/system.cnf system_<switch no.>.cnf cp switch <switch no.> /config/system.txt system_<switch no.>.txt	- Use binary mode to transfer these files with the "ftp" command. - Delete the source files after the transfer is completed.
Failure save information	/usr/var/core/*.core	- Use binary mode to transfer these files with the "ftp" command. - Delete these files after the transfer is completed.

9.2 Transferring maintenance information files

This section describes how to transfer files that contain log information or dump information.

The "ftp" command available for the Switch allows you to transfer files containing maintenance information to a remote operation terminal or remote host. Also, you can use "zmodem" command to transfer files to a console.

In a stack configuration, files containing maintenance information can be transferred from only the master switch. To transfer maintenance information files of member switches other than the master switch, use the "cp" command to copy the files from each member switch to the master switch, and then transfer the files from the master switch.

9.2.1 Transferring files using the ftp command

Use the "ftp" command to transfer files between the Switch and a remote operation terminal.

(1) Transferring a dump file to a remote operation terminal

Figure 9-1 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 FTP server (Version 6.00LS) 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> bin                                      <-4
200 Type set to I.
ftp>cd /usr/home/operator                     <-5
250 CMD command successful.
ftp> put rmdump                               <-6
local: rmdump remote: rmdump
200 EPRT command successful.
150 Opening BINARY mode data connection for 'rmdump'.
100% |************************************|  3897      2.13 MB/s    00:00 ETA
226 Transfer complete.
3897 bytes sent in 00:00 (82.95 KB/s)
ftp> bye
221 Goodbye.
>
```

1. Specify the source directory.
2. Specify the destination terminal address.
3. Change the interactive mode.
4. Set the mode to binary mode.#
5. Specify the destination directory.

6. Transfer the dump file.

#

Make sure that you use binary mode to transfer dump files. If dump files are transferred in ASCII mode, correct dump information cannot be obtained.

(2) Transferring log information to a remote operation terminal

Figure 9-2 Transferring log information 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 FTP server (Version 6.00LS) 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/operator                   <-3
250 CMD 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% |************************************| 89019    807.09 KB/s    --:-- ETA
226 Transfer complete.
89019 bytes sent in 00:00 (315.22 KB/s)
ftp> put log_ref.txt
local: log_ref.txt remote: log_ref.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log_ref.txt'.
100% |************************************|  4628      1.04 MB/s    --:-- ETA
226 Transfer complete.
4628 bytes sent in 00:00 (102.86 KB/s)
ftp> bye
221 Goodbye.
>
```

1. Specify the destination terminal address.
2. Set the mode to ASCII mode.
3. Specify the destination directory.
4. Transfer the log information.

(3) Transferring a core file to a remote operation terminal

Figure 9-3 Transferring a core file to a remote operation terminal

```
> cd /usr/var/core/
```

```
> ls                                    <-1
nimd.core      nodeInit.core
> ftp 192.168.0.1                       <-2
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) 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> bin                                <-4
200 Type set to I.
ftp>cd /usr/home/operator               <-5
250 CMD command successful.
ftp> mput *.core                        <-6
local: nimd.core remote: nimd.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nimd.core'.
100% |***********************************************************************|
272 KB    1.12 MB/s    00:00 ETA
226 Transfer complete.
278528 bytes sent in 00:00 (884.85 KB/s)
local: nodeInit.core remote: nodeInit.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nodeInit.core'.
100% |***********************************************************************|
1476 KB    1.40 MB/s    00:00 ETA
226 Transfer complete.
1511424 bytes sent in 00:01 (1.33 MB/s)
ftp> bye
221 Goodbye.
>
```

1. Make sure that the core file exists.
   If the file does not exist, exit the procedure without doing anything.
2. Specify the destination terminal address.
3. Change the interactive mode.
4. Set the mode to binary mode.#
5. Specify the destination directory.
6. Transfer the core file.

#

Make sure that you use binary mode to transfer core files. If core files are transferred in ASCII mode, the correct core file cannot be obtained.

9.2.2 Transferring files using the zmodem command

You can use the "zmodem" command to transfer files between the Switch and a console connected via an RS232C cable. To do this, before starting communication, you must run the communication program on the console to start receiving files.

(1) Transferring a dump file to a console

Figure 9-4 Transferring a dump file to a console

```
> cd /dump0                                  <-1
> zmodem put rmdump                          <-2
>
```

1. Specify the source directory.
2. Transfer the dump file.

(2) Transferring log information to a console

Figure 9-5 Transferring a log file to a console

```
> show logging > log.txt
> show logging reference > log_ref.txt
> zmodem put log.txt                         <-1
> zmodem put log_ref.txt
>
```

1. Transfer the log file.

(3) Transferring a core file to a console

Figure 9-6 Transferring a core file to a console

```
> cd /usr/var/core/
> ls                                         <-1
interfaceControl.core   nodeInit.core
> zmodem put interfaceControl.core           <-2
> zmodem put nodeInit.core
>
```

1. Make sure that the core file exists.
   If the file does not exist, exit the procedure without doing anything.
2. Transfer the log file.

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

You can use the "show tech-support" command to collect failure occurrence information in a batch. You can also specify the ftp parameter for this command to transfer the collected information to a remote operation terminal or remote host.

In a stack configuration, you can transfer files with the ftp parameter specified, only by executing the "show tech-support" command on the master switch. For member switches other than the master switch, you cannot use the "show tech-support" command with the ftp parameter specified.

To collect information and transfer files by using the "show tech-support" command on member switches other than the master switch, perform the following procedure:

1. Execute the following command on the master switch to collect the failure occurrence information:
   ```
   show tech-support switch <switch no.>
   ```
2. Use the "cp" command to copy the information collected from each member switch from the member switches to the master switch, and then transfer the files from the master switch.
   For the file transfer procedure, see "9.2 Transferring maintenance information files".

(1) Collecting information and transferring files by using the show tech-support command

Figure 9-7 Transferring maintenance information files to a remote operation terminal

```
> show tech-support ftp                                    <-1
Specify Host Name of FTP Server.      : 192.168.0.1         <-2
Specify User ID for FTP connections.   : staff1             <-3
Specify Password for FTP connections.  :                    <-4
Specify Path Name on FTP Server.      : /usr/home/staff1    <-5
Specify File Name of log and Dump files: support            <-6
Mon Dec 18 20:42:58 UTC 20XX
Transferred support.txt .
Executing.
...
Operation normal end.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 2344
-rwxrwxrwx  1 root  wheel  2400114 Dec  8 16:46 rmdump
***** ls -l /usr/var/hardware *****
-rwxrwxrwx  1 root  wheel  264198 Dec  8 16:43 ni00.000
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /usr/var/core *****
No Core files
########## End of Core files' Information ##########
Transferred support.tgz .
Executing.
...
```

```
Operation normal end.
>
```

1. Execute the command.
2. Specify the remote host name.
3. Specify a user name.
4. Enter the password.
5. Specify the destination directory.
6. Specify a file name.

(2) Collecting information using the show tech-support command (with a stack configuration)

Figure 9-8 Collecting member switch maintenance information (switch number 2) to the master switch (with a stack configuration)

```
> show tech-support switch 2 > support.txt                  <-1
Executing.
...
Operation normal end.
>
```

1. Execute the command.

9.4 Collecting information and transferring files by using the ftp command on a remote operation terminal

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

In a stack configuration, you can connect to the master switch by using the "ftp" command. You cannot connect to member switches other than the master switch by using the "ftp" command.

To collect failure information or maintenance information or to transfer files by using member switches other than the master switch, perform the following procedure:

1. Use each member switch to collect the failure information or maintenance information.
2. Use the "cp" command to copy the information collected from each member switch from the member switches to the master switch, and then transfer the files from the master switch.
   For the file transfer procedure, see "9.2 Transferring maintenance information files".

(1) Collecting "show tech-support" information

The procedures below describe how to connect a remote operation terminal, as a client, to the Switch 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.

Table 9-2 Information that can be obtained with the "ftp" command

File name to specify in the "get" subcommand	Information to be obtained
.show-tech	Results displayed by the "show tech-support" command
.show-tech-unicast	Results displayed by the "show tech-support unicast" command
.show-tech-multicast	Results displayed by the "show tech-support multicast" command
.show-tech-layer-2	Results displayed by the "show tech-support layer-2" command

Figure 9-9 Obtaining the basic "show tech-support" information

```
client-host> ftp 192.168.0.60                  <-1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) 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> get .show-tech show-tech.txt               <-2
local: show-tech.txt remote: .show-tech
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
270513 bytes received in 8.22 seconds (32.12 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. Use FTP on a client to connect to the Switch.
2. Transfer the .show-tech file to the client. (The file name show-tech.txt is specified.)

Figure 9-10 Obtaining the "show tech-support" unicast information

```
client-host> ftp 192.168.0.60                  <-1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) 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> get .show-tech-unicast show-tech-uni.txt  <-2
local: show-tech-uni.txt remote: .show-tech-uni.txt
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
343044 bytes received in 30.43 seconds (11.01 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. Use FTP on a client to connect to the Switch.
2. Transfer the .show-tech-unicast file to the client. (The file name show-tech-uni.txt is specified.)

Notes

- "ftp" subcommands such as "ls" cannot view a file specified for the "get" subcommand. Therefore, you cannot check the file size before transferring the file.
- When you obtain the information, execute the commands on the device. In this case, the file transfer might take a long time. However, you must not interrupt the transfer before it ends.
- 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.
- When you use FTP to obtain failure information, you cannot collect results of executing any command that can only be executed in administrator mode, such as the "show running-config" command.
- When you obtain show tech-support information, the system writes the user name ftpuser to the log information.

(2) Obtaining a dump information file

The procedures below describe how to connect a remote operation terminal, as a client, to the Switch by using the "ftp" command, and how to obtain information by specifying the name of a file that contains the required dump information.

Table 9-3 Files that can be obtained with the "ftp" command

File name to specify in the "get" subcommand	Files to be obtained
.dump	Files in /dump0 and files in /usr/var/hardware (compressed)
.dump0	Files in /dump0 (compressed)
.hardware	Files in /usr/var/hardware (compressed)

Figure 9-11 Obtaining a dump file 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 (NetBSD-ftpd) 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
150 Opening BINARY mode data connection for '/etc/ftpdump'.
226 Transfer complete.
2411332 bytes received in 5.78 seconds (407.13 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. Use FTP on a client to connect to the device.
2. Make sure that you use binary mode to transfer dump information files.
   You cannot transfer files in ASCII mode.
3. Transfer the .dump files to the client. (The file name dump.tgz is specified.)

Notes

- "ftp" subcommands such as "ls" cannot view a file specified for the "get" subcommand. Therefore, you cannot check the file size before transferring the file.
- 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.

9.5 Writing to a memory card

Failure information and maintenance information can be written to a memory card. Note, however, that memory cards have a capacity limit.

9.5.1 Writing data to a memory card by using an operation terminal

This section describes how to write the device information to a memory card by using an operation terminal.

1. Insert a memory card to which information is to be written into the device.
2. Use the "ls -l" 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 available space.

```
>show mc
Date 20XX/11/15 15:50:40 UTC
MC  : Enabled
   Manufacture ID : 00000003
   16,735kB used
   106,224kB free
   122,959kB total
```

The underlined part is the available space.

4. Use the "cp" command to copy the source file to the memory card with the file name "tech-1.log".

```
> cp tech.log mc-file tech-1.log
```

5. Make sure that the file has been written to the memory card.

```
> ls mc-dir
Name           Size
tech-1.log            234803
>
```

10 Communication Failure Analysis

This chapter describes how to take actions when a communication failure occurs.

10.1 Line test

In line tests, what loops back test frames varies depending on the test type. The following figure shows what loops back the test frames for various line test types.

Note that line testing for stack configuration is not supported.

Figure 10-1 What loops back the test frames for various line test types

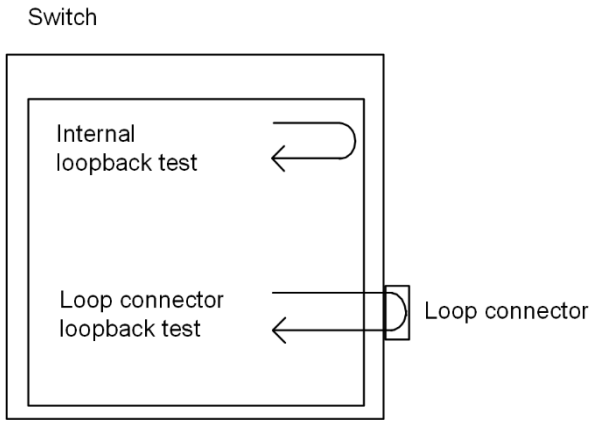


Table 10-1 Test types and fault locations to be identified

Test type	What loops back frames	Fault location to be identified
Module internal loopback test	Device	Device (except for the RJ45 connector and transceiver)
Loop connector loopback test	Loop connector	Device (including the RJ45 connector and transceiver)

10.1.1 Module internal loopback test

The module internal loopback test, which loops back frames on the device, is executed to check for any failures. You can execute this test for all line types.

The test procedure is described below.

1. Use the "inactivate" command to put the port to be tested into an inactive status.
2. Execute the "test interfaces" command with the internal parameter specified. Wait about one minute after the execution of the command.
3. Execute the "no test interfaces" command, and then check the displayed results.
4. Use the "activate" command to place the port back into an active status.

The following figure shows an example of a test in which the sending interval of test frames is set to two seconds on port number 1.

Figure 10-2 Example of a module internal loopback test

```
> inactivate gigabitethernet 1/0/1
> test interfaces gigabitethernet 0/1 internal interval 2 pattern 4

> no test interfaces gigabitethernet 0/1
Date 20XX/03/10 00:20:21 UTC
Interface type           :100BASE-TX
```

```
Test count              :30
Send-OK                 :30          Send-NG              :0
Receive-OK              :30          Receive-NG           :0
Data compare error      :0           Out underrun         :0
Out buffer hunt error   :0           Out line error       :0
In CRC error            :0           In frame alignment   :0
In monitor time out     :0           In line error        :0
H/W error               :none
> activate gigabitethernet 1/0/1
```

After the test is completed, check the following:

If both "Send-NG" and "Receive-NG" are 0, the line test has successfully completed.

If either "Send-NG" or "Receive-NG" is not 0, there might be some sort of problem. See the description of the "no test interfaces" command in the "Operation Command Reference".

10.1.2 Loop connector loopback test

The loop connector loopback test, which loops back frames on the loop connector, is executed to check for any failures. You can execute this test for all line types.

The test procedure is described below.

1. Use the "inactivate" command to put the port to be tested into an inactive status.
2. Remove the cable from the target port, and then connect the loop connector to that port.#
3. Execute the "test interfaces" command with the connector parameter specified. Wait about one minute after the execution of the command.
4. Execute the "no test interfaces" command, and then check the displayed results.
5. Remove the loop connector, and then reconnect the cable to the port.
6. Use the "activate" command to place the port back into an active status.

#

Note that if the loop connecter is not connected, or if the connected loop connector is inappropriate for the port, the test might provide invalid results.

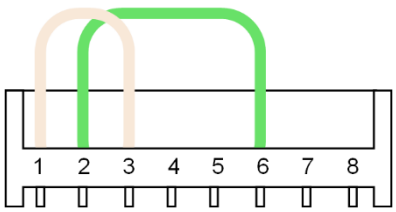
Note that you can check the test results in the same way as described in "10.1.1 Module internal loopback test".

10.1.3 Loop connector wiring specifications

(1) 10BASE-T/100BASE-TX loop connector

As shown in the following figure, insert the cables into the connector and crimp them by using a crimping tool.

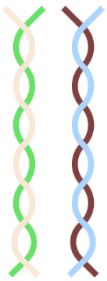
Figure 10-3 10BASE-T/100BASE-TX loop connector wiring specification



(2) 10BASE-T/100BASE-TX/1000BASE-T loop connector

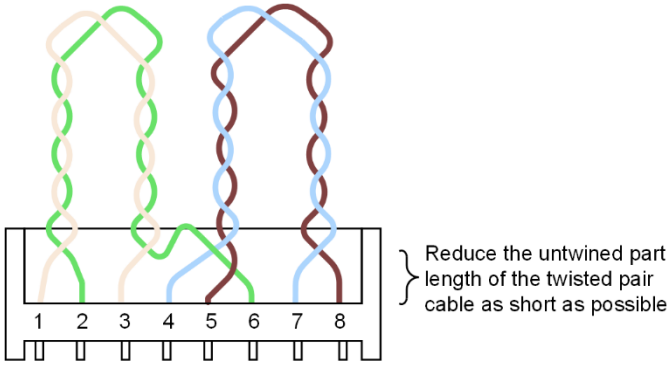
1. Create two 6-to-7-cm long twisted pair cables before you start the procedure.

   Figure 10-4 Twisted pair cable



2. As shown in the following figure, insert the cables into the connector and crimp them by using a crimping tool.

   Figure 10-5 10BASE-T/100BASE-TX/1000BASE-T loop connector wiring specification

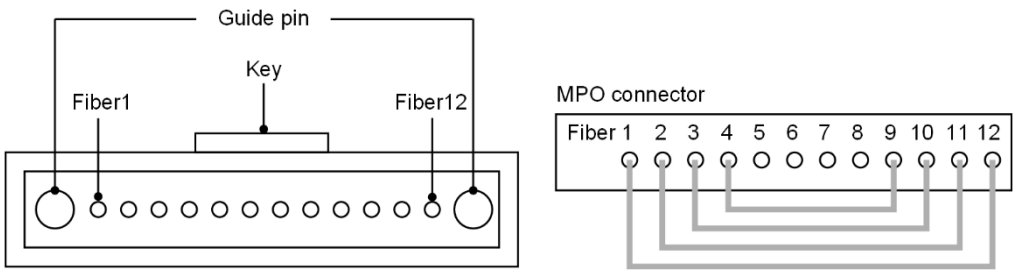


Note that the 1000BASE-T loop connector above is only supported for the loop behavior for the Switch. (Loop behavior by the 1000BASE-T connector is a non-standard, proprietary action.)

(3) 40GBASE-SR4 loop connector

Use a loop connector in the wiring specification as shown in the figure below.

Figure 10-6 40GBASE-SR4 loop connector wiring specification



10.2 Checking discarded packets

10.2.1 Checking discarding by a filter

A possible cause of communication problems on the network using the Switch is that certain frames are discarded by filtering. The following shows how to check whether frames are discarded by filtering.

Note that, even if the policy-based routing specified for filtering follows default behaviors and their default behavior is to discard frames, the same behavior as the discarding of packets by filtering applies. In addition to the following steps, see "7.2.1 Packets are not forwarded in policy-based routing".

(1) How to check whether frames have been discarded by filtering

1. Execute the "show access-filter" command, and check the filter conditions in the access list applied to the interface, the number of packets that match the filter conditions, and the number of packets discarded by a filter entry for implicit discard.
2. Compare the filter conditions you checked in step 1 and the contents of the frame that cannot be communicated to determine whether the target frames were discarded. If the contents of the frame that cannot be communicated do not match any of the applied filter conditions, the frames might have been discarded by an implicit discard filter entry.
3. If frames are discarded by a filter, check whether the filter configuration settings are appropriate.

10.2.2 Checking discarding by QoS

If a communication problem occurs on a network employing the Switch, it is possible that certain frames might have been discarded by bandwidth monitoring, drop control, or shaper of the QoS control. The following shows how to check frame discard by QoS.

(1) How to check frame discard using bandwidth monitoring

1. Execute the "show qos-flow" command, and check the flow detection conditions and behavior settings of the bandwidth monitoring applied to the interface and also the number of packets that match the flow detection conditions.
2. Compare the flow detection conditions you checked in step 1 and the contents of the packets that cannot be communicated to determine whether the target frames were discarded. If a frame violates the maximum bandwidth control conditions, the frame is discarded and the count of the "matched packets(max-rate over)" statistics item is incremented. If the count of this statistics item has been incremented, frames might have been discarded by bandwidth monitoring applied to the interface.
3. Make sure that the setting conditions for QoS control in the configuration are correct, and that the bandwidth monitoring has been set appropriately in the system configuration.

(2) How to check whether frames have been discarded by drop control and legacy shaper

1. Use the "show qos queueing" command and check the information displayed for "discard packets" in the output interface statistics.
2. If the count of the statistics item checked in step 1 is incremented, frames are discarded by drop control and legacy shaper of the QoS control.
3. Check whether drop control and legacy shaper are being used appropriately in the system configuration.

10.3 Packet congestion in CPU processing does not recover

This section describes how to take actions if packet congestion in CPU processing is not cleared up.

Packet congestion in CPU processing occurs due to the overflow of the input queue when the CPU receives a large number of packets to be processed in software.

When packet congestion in CPU processing is detected, the following message is output:

"E3 SOFTWARE 00003303 1000:XXXXXXXXXXXX Received many packets and loaded into the queue to CPU."

When packet congestion is cleared, the following message is output:

"E3 SOFTWARE 00003304 1000:XXXXXXXXXXXX Processed the packets in the queue to CPU."

Packet congestion in CPU processing might occur even if the system is working normally such as when the CPU receives a large number of packets with unknown destinations due to the aging of routing information. If packet congestion is not cleared up or packet congestion occurs repeatedly, the setting of the Switch or the network configuration might have a problem. When such an event occurs, take action according to the following table.

Table 10-2 Action to take when packet congestion in CPU processing is not cleared

No.	Items to check and commands	Action
1	Identify packet types. - Execute the "show netstat statistics" command at 20-second intervals, and compare the results.	If the comparison shows that the count of the "total packets received" statistics item increases drastically for the ip or ip6 packet type, go to No. 2.
		If the comparison shows that the count of the "packets received" statistics item increases drastically for the arp packet type, go to No. 2.
		For other cases, go to No. 4.
2	Identify the VLAN interface that is receiving the packets. - Execute the "show netstat interface" command at 20-second intervals, and compare the results.	If the comparison shows that the count of the "Ipkts" statistics item increases drastically for a specific VLAN interface, go to No. 3.
		For other cases, go to No. 4.
3	Identify the source and destination addresses of the packets. - For the VLAN interface identified in No. 2, execute the "show tcpdump interface" command. Check the source and destination addresses for the packet type identified in No. 1.	If the packet type is ip or ip6 and the destination address of the target packets is the address of the Switch, the packets might be sent incorrectly. Check the settings of the terminal that has the source address or check the network configuration. Modify them so that the target packets are not sent to the Switch.
		If the packet type is ip or ip6 and the destination address of the target packets is the address of another device, the address of ARP information might not be resolved or a large number of packets with unknown destination might be sent. - When the packet type is ip, see "7.1.1 Communication is not possible or is disconnected, (5) Checking the ARP resolution information with a neighboring device". - When the packet type is ip6, see "7.5.1 Communication is not possible or is disconnected, (5) Checking the NDP resolution information with a neighboring device".
		If the packet type is arp, a large number of ARP packets have been received. In this case, an L2 loop configuration might be used. Revise the network configuration. If there is no problem in the network configuration, check the settings of the terminal that has the source address.
4	Collect analysis information - Execute the "show tech-support" command twice.	Send the information you collected to the support center.

11 Restart of the Device

This chapter mainly describes how to restart the device.

11.1 Restarting the device

11.1.1 Restart of the device

You can use the "reload" command to restart the device. Log data is stored when the device restarts.

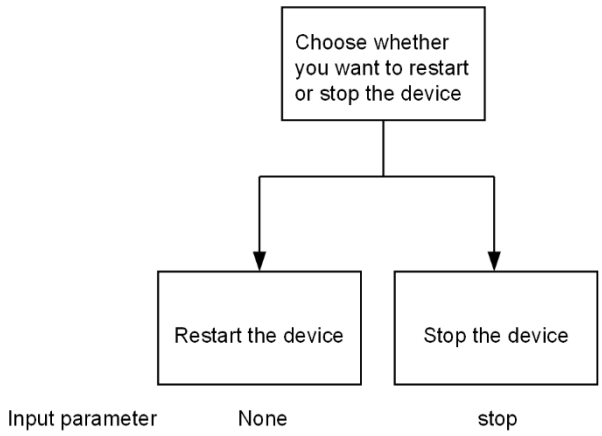
For details on the syntax and parameters of the command, see "Operation Command Reference".

As an example, the following steps describe how to select parameters for the "reload" command. In this example, you choose to restart the device and collect the CPU memory dump by interacting with the confirmation messages.

Step1

Choose whether you want to restart or stop the device.

Figure 11-1 Selecting to restart or stop the device

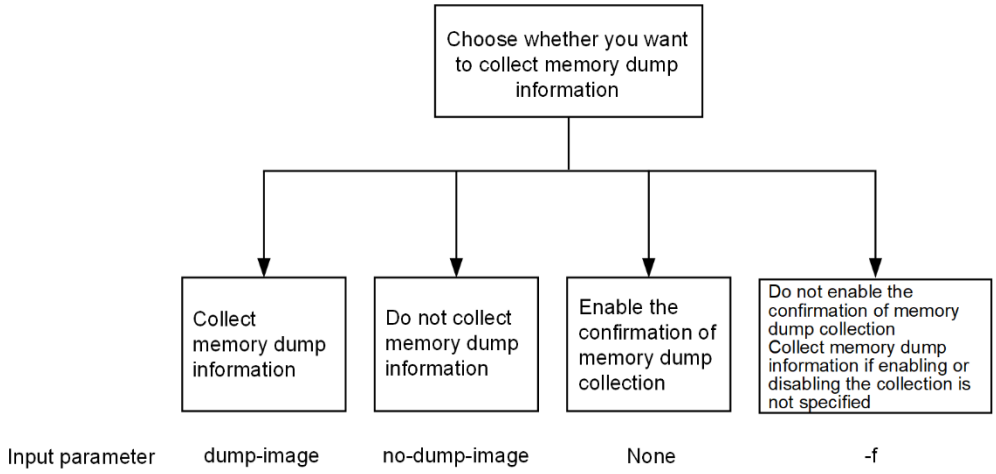


In step 1, you restart the device. So according to the figure above, you do not use any parameters.

Step2

In this step, choose whether you capture the dump.

Figure 11-2 Selection of the CPU memory dump collection type



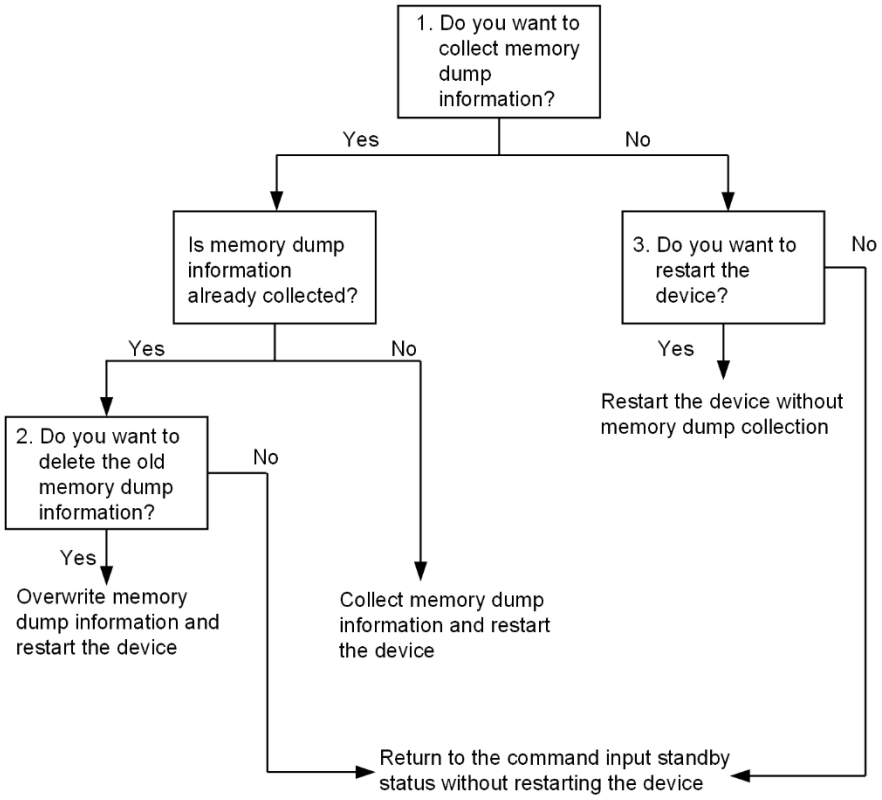
In step 2, you will be asked whether you want to collect the CPU memory dump. According to the figure above, you do not use any parameters.

Combining the parameters selected in steps 1 and 2 results in the "reload" command. When you enter this command, the dump collection confirmation messages are displayed as follows:

1. Dump information extracted?(y/n):_
2. old dump file(rmdump 01/01 00:00) delete OK? (y/n):_
3. Restart OK? (y/n):_

The numbers in the flow chart below correspond to each numbered message above, indicating when each message is displayed.

Figure 11-3 Confirmation messages for CPU memory dump collection



Appendix

Appendix A 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 details on the displayed information, see "Operation Command Reference".

Note

"Operation Command Reference" does not cover part of the information displayed by the "show tech-support" command. Such information is not disclosed to the public because it contains internal information of the device.

Note that some information might not appear depending on the software version. Please be aware of that fact beforehand.

Table A-1 Detailed display contents of commands

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
1	show version	Software version and hardware information of the Switch	Y	Y	Y	Y
2	show license	Optional license information	Y	Y	Y	Y
3	show system	Operating status of the device	Y	Y	Y	Y
4	show environment	Fan/power supply unit/uptime information	Y	Y	Y	Y
5	show process cpu	CPU usage of processes	Y	Y	Y	Y
6	show process memory	Memory usage of processes	Y	Y	Y	Y
7	show cpu days hours minutes seconds	CPU utilization	Y	Y	Y	Y
8	show memory summary	Memory usage of the device	Y	Y	Y	Y
9	/sbin/dmesg	Kernel event information	Y	Y	Y	Y
10	cat /var/run/dmesg.boot	Kernel event information	Y	Y	Y	Y
11	cat /var/log/messages	Internal information of the kernel and daemons	Y	Y	Y	Y
12	/usr/local/diag/statShow	Kernel internal statistics	Y	Y	Y	Y
13	/usr/local/diag/pk_tmrd	Uptime information	Y	Y	Y	Y
14	fstat	File descriptor information	Y	Y	Y	Y
15	/usr/local/diag/rtsystat	Internal device-related information	Y	Y	Y	Y
16	/usr/local/diag/rtastat	Path distribution-related information	Y	Y	Y	Y
17	show netstat all-protocol-address numeric	Layer 4-related statistics	Y	Y	Y	Y
18	show netstat statistics	Layer 3-related statistics	Y	Y	Y	Y
19	show dumpfile	Information on collected dump files	Y	Y	Y	Y
20	ls -lTiR /dump0	Dump file information	Y	Y	Y	Y
21	ls -lTiR /usr/var/hardware	Hardware dump file information	Y	Y	Y	Y

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
22	ls -lTiR /usr/var/core	core file information	Y	Y	Y	Y
23	ls -lTiR /config	config file information	Y	Y	Y	Y
24	ls -lTiR /var	Memory file system information	Y	Y	Y	Y
25	df -ik	Partition information	Y	Y	Y	Y
26	du -Pk /	File system usage	Y	Y	Y	Y
27	show logging	Chronological log information for the active system	Y	Y	Y	Y
28	show logging reference	Reference log information for the active system	Y	Y	Y	Y
29	show ntp associations	Information of NTP server behaviors	Y	Y	Y	Y
30	/usr/bin/w -n	Login-related information	Y	Y	Y	Y
31	show session	Login session information	Y	Y	Y	Y
32	/usr/sbin/pstat -t	Terminal information	Y	Y	Y	Y
33	stty -a -f /dev/tty00	Console terminal information	Y	Y	Y	Y
34	cat /var/log/clitrace1	CLI trace information 1	Y	Y	Y	Y
35	cat /var/log/clitrace2	CLI trace information 2	Y	Y	Y	Y
36	cat /var/log/mmitrace	Operation command trace information	Y	Y	Y	Y
37	cat /var/log/kern.log	Internal trace information of the kernel	Y	Y	Y	Y
38	cat /var/log/daemon.log	Daemon-related internal trace information	Y	Y	Y	Y
39	cat /var/log/fixsb.log	Internal trace information of the kernel	Y	Y	Y	Y
40	cat /usr/var/pplog/ppupdate.log	Log information created when software is updated	Y	Y	Y	Y
41	cat /usr/var/pplog/ppupdate2.log	Log information created when software is updated	Y	Y	Y	Y
42	tail -n 30 /var/log/authlog	Authentication trace information	Y	Y	Y	Y
43	tail -n 30 /var/log/xferlog	FTP trace information	Y	Y	Y	Y
44	cat /var/log/ssh.log	SSH log information	Y	Y	Y	Y
45	show accounting	Accounting information	Y	Y	Y	Y
46	cat /var/tmp/gen/trace/mng.trc	Configuration command trace information 1	Y	Y	Y	Y
47	cat /var/tmp/gen/trace/mng_sub.trc	Configuration command trace information 3	Y	Y	Y	Y
48	tail -n 400 /var/tmp/gen/trace/api.trc	Configuration command trace information 4	Y	Y	Y	Y
49	tail -n 400 /var/tmp/gen/trace/ctl.trc	Configuration command trace information 5	Y	Y	Y	Y
50	show netstat interface	Kernel interface information	Y	Y	Y	Y
51	show vlan list	VLAN information list	Y	Y	Y	Y

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
52	show port	Port information	Y	Y	Y	Y
53	show port statistics	Port statistics	Y	Y	Y	Y
54	show port protocol	Protocol information for ports	Y	Y	Y	Y
55	show port transceiver debug	Transceiver details for ports	Y	Y	Y	Y
56	show interfaces nif XXX_NIF line XXX_LINE debug	Detailed statistics for ports	Y	Y	Y	Y
57	show network-clock	Sync-E running status (for AX3660S Ver.12.1.E and later)	Y	Y	Y	Y
58	nimdump stack aging info	Stack switchover aging time (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y
59	show switch detail	Stack detailed information (for AX3800S Ver.11.10 and later, AX3660S, and AX3650S Ver.11.8 and later)	Y	Y	Y	Y
60	show switch debug	Stack debug information (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y
61	show running-config	Configuration for operation	Y	Y	Y	Y
62	show channel-group detail	Link aggregation details	Y	Y	Y	Y
63	show spanning-tree detail	Spanning Tree details	Y	Y	Y	Y
64	show gsrp all	Details for all GSRPs	Y	Y	Y	Y
65	show axrp detail	Ring Protocol details	Y	Y	Y	Y
66	show switchport-backup detail	Uplink redundancy information	N	N	N	Y
67	show switchport-backup statistics	Uplink redundancy statistics	N	N	N	Y
68	show efmoam detail	IEEE 802.3ah/OAM function setting information and port status	Y	Y	Y	Y
69	show efmoam statistics	IEEE 802.3ah/OAM function statistics	Y	Y	Y	Y
70	show lldp detail	Neighboring device information for the LLDP function	Y	Y	Y	Y
71	show oadp detail	Neighboring device information for the OADP function	Y	Y	Y	Y
72	show loop-detection	L2 loop detection function information	N	N	N	Y
73	show loop-detection statistics	L2 loop detection function statistics	N	N	N	Y
74	show loop-detection logging	Log information of L2 loop detection function	N	N	N	Y
75	show channel-group statistics	Link aggregation statistics	N	N	N	Y
76	show channel-group statistics lacp	LACP statistics for link aggregation	N	N	N	Y
77	show spanning-tree statistics	Spanning Tree statistics	N	N	N	Y
78	show vlan detail	VLAN details	N	Y	Y	Y
79	show vlan mac-vlan	MAC VLAN information	N	N	N	Y
80	show qos queueing	Statistics on all queues	Y	Y	Y	Y

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
81	show ip cache policy	Status display of policy-based routing (for AX3800S Ver.11.9 and later, AX3660S, and AX3650S Ver.11.7 and later)	Y	Y	Y	Y
82	policy tool tech	Internal trace of policy-based program (for AX3800S Ver.11.9 and later, AX3660S, and AX3650S Ver.11.7 and later)	Y	Y	Y	Y
83	show access-filter	Statistics on filtering	N	Y	Y	Y
84	show qos-flow	QoS control function statistics	N	Y	Y	Y
85	show lldp statistics	LLDP function statistics	N	N	N	Y
86	show oadp statistics	OADP function statistics	N	N	N	Y
87	show mac-address-table	mac-address-table information	N	Y	Y	Y
88	show fense server detail	FENSE server information for VAA function (for AX3800S and AX3650S)	N	N	N	Y
89	show fense statistics	VAA function statistics (for AX3800S and AX3650S)	N	N	N	Y
90	show fense logging	Action log information of VAA function (for AX3800S and AX3650S)	N	N	N	Y
91	show dot1x logging	Action log messages collected for IEEE 802.1X authentication	N	N	N	Y
92	show dot1x statistics	Statistics on IEEE 802.1X authentication	N	N	N	Y
93	show dot1x detail	Authentication status information on IEEE 802.X authentication	N	N	N	Y
94	show igmp-snooping	IGMP snooping information	N	N	N	Y
95	show igmp-snooping group	IGMP snooping group information	N	N	N	Y
96	show igmp-snooping statistics	IGMP snooping statistics	N	N	N	Y
97	show mld-snooping	MLD snooping information	N	N	N	Y
98	show mld-snooping group	MLD snooping group information	N	N	N	Y
99	show mld-snooping statistics	MLD snooping statistics	N	N	N	Y
100	show netstat routing-table numeric	Route-related information in the kernel (unicast)	N	Y	Y	N
101	show netstat multicast numeric	Route-related information in the kernel (multicast)	N	N	Y	N
102	show ip multicast statistics	IPv4 multicast statistics	N	N	Y	N
103	show ipv6 multicast statistics	IPv6 multicast statistics	N	N	Y	N
104	show ip multicast resources	Number of entries used in IPv4 multicast routing	N	N	Y	N
105	show ip igmp interface	Information on interfaces with IGMP enabled	N	N	Y	N
106	show ip igmp group	Information on groups managed	N	N	Y	N

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
		by IGMP				
107	show ip pim interface detail	Information on interfaces with IPv4 PIM enabled	N	N	Y	N
108	show ip pim neighbor detail	IPv4 PIM neighbor information	N	N	Y	N
109	show ip pim bsr	IPv4 PIM BSR information	N	N	Y	N
110	show ip pim rp-mapping	IPv4 PIM rendezvous point information	N	N	Y	N
111	show ip mroute	IPv4 multicast routing information	N	N	Y	N
112	show ip mcache	IPv4 multicast forwarding entry	N	N	Y	N
113	show ipv6 multicast resources	Number of entries used in IPv6 multicast routing	N	N	Y	N
114	show ipv6 mld interface	Information on interfaces with MLD enabled	N	N	Y	N
115	show ipv6 mld group	Information on groups managed by MLD	N	N	Y	N
116	show ipv6 pim interface detail	Information on interfaces with IPv6 PIM enabled	N	N	Y	N
117	show ipv6 pim neighbor detail	IPv6 PIM neighbor information	N	N	Y	N
118	show ipv6 pim bsr	IPv6 PIM BSR information	N	N	Y	N
119	show ipv6 pim rp-mapping	IPv6 PIM rendezvous point information	N	N	Y	N
120	show ipv6 mroute	IPv6 multicast routing information	N	N	Y	N
121	show ipv6 mcache	IPv6 multicast forwarding entry	N	N	Y	N
122	show vrrpstatus detail statistics	VRRP virtual router status and statistics	N	Y	N	N
123	show track detail	VRRP fault monitoring interface information	N	Y	N	N
124	show ip interface ipv4-unicast	Interface information on the Switch recognized by the unicast routing program	N	Y	N	N
125	show processes memory unicast	Available memory amount and memory usage for the unicast routing program	N	Y	N	N
126	show processes cpu minutes unicast	CPU usage for the unicast routing program	N	Y	N	N
127	show ip udp forward	UDP broadcast relay statistics (for AX3660S Ver.12.1.G and later)	N	Y	N	N
128	show dhcp giaddr all	Destination IP address information for DHCP packets sent from a DHCP relay agent	N	Y	N	N
129	show dhcp traffic	DHCP relay agent statistics	N	Y	N	N
130	show ip dhcp server statistics	DHCP server statistics	N	Y	N	N
131	show ip dhcp conflict	Information on conflicted IP	N	Y	N	N

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
		addresses detected by a DHCP server				
132	show ipv6 dhcp server statistics	IPv6 DHCP server statistics	N	Y	N	N
133	show ipv6 dhcp traffic	IPv6 DHCP relay statistics	N	Y	N	N
134	show ip dhcp snooping statistics	DHCP snooping statistics	Y	Y	Y	Y
135	show ip arp inspection statistics	Dynamic ARP inspection statistics	Y	Y	Y	Y
136	show ip dhcp snooping logging info	DHCP snooping log information	N	N	N	Y
137	dhsn debug	DHCP snooping event information	N	N	N	Y
138	show ip route summary	Number of active and inactive routes maintained by routing protocols	Y	Y	Y	Y
139	show ip rip statistics	RIP statistics	N	Y	N	N
140	show ip rip advertised-routes summary	Number of routes advertised by RIP	N	Y	N	N
141	show ip rip received-routes summary	Number of routes learned by RIP	N	Y	N	N
142	show ip ospf	OSPF global information	N	Y	N	N
143	show ip ospf discard-packets	Information on packets discarded by OSPF	N	Y	N	N
144	show ip ospf statistics	Statistics on sent/received packets collected by OSPF	N	Y	N	N
145	show ip ospf neighbor detail	OSPF neighboring router details	N	Y	N	N
146	show ip ospf virtual-links detail	OSPF virtual link details	N	Y	N	N
147	show ip ospf database database-summary	Number of LSAs for each OSPF LS type	N	Y	N	N
148	show ip bgp neighbor detail	BGP4 peering information	N	Y	N	N
149	show ip bgp notification-factor	Messages that caused the disconnection of BGP4 connections	N	Y	N	N
150	show ip bgp received-routes summary	Number of routes received from BGP4 peers	N	Y	N	N
151	show ip bgp advertised-routes summary	Number of routes advertised to BGP4 peers	N	Y	N	N
152	show ip vrf all	Number of routes learned for each VRF	Y	Y	Y	Y
153	show graceful-restart unicast	Running status of restart routers that perform graceful restarts in the unicast routing protocol (for AX3660S)	N	Y	N	N
154	show ipv6 interface ipv6-unicast	Interface information on the Switch recognized by the unicast routing program	N	Y	N	N

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
155	show ipv6 route summary	Number of active and inactive routes maintained by the unicast routing program	Y	Y	Y	Y
156	show ipv6 rip advertised-routes summary	Number of routes advertised by RIPng	N	Y	N	N
157	show ipv6 rip received-routes summary	Number of routes learned by RIPng	N	Y	N	N
158	show ipv6 rip statistics	RIPng statistics	N	Y	N	N
159	show ipv6 ospf	OSPFv3 global information	N	Y	N	N
160	show ipv6 ospf discard-packets	Information on packets discarded by OSPFv3	N	Y	N	N
161	show ipv6 ospf statistics	Statistics on packets collected by OSPFv3	N	Y	N	N
162	show ipv6 ospf neighbor detail	OSPFv3 neighboring router status	N	Y	N	N
163	show ipv6 ospf virtual-links detail	OSPFv3 virtual link information	N	Y	N	N
164	show ipv6 ospf database database-summary	Number of LS-Databases for OSPFv3	N	Y	N	N
165	show ipv6 bgp neighbor detail	BGP4+ peering information	N	Y	N	N
166	show ipv6 bgp notification-factor	Packets that caused the disconnection of BGP4+ connections	N	Y	N	N
167	show ipv6 bgp received-routes summary	Number of routes received from BGP4+ peers	N	Y	N	N
168	show ipv6 bgp advertised-routes summary	Number of routes advertised to BGP4+ peers	N	Y	N	N
169	show ipv6 vrf all	Number of routes learned for each VRF	Y	Y	Y	Y
170	show web-authentication user edit	Display of registrations and changes in the internal Web authentication DB	N	N	N	Y
171	show web-authentication user commit	Display of entries registered in the internal Web authentication DB	N	N	N	Y
172	show web-authentication statistics	Items displayed for statistics related to Web authentication	N	N	N	Y
173	show web-authentication login	Display of authenticated-user information (account information)	N	N	N	Y
174	show web-authentication logging	Display of the action logs for Web authentication.	N	N	N	Y
175	show web-authentication http information	Display of Web server session information	N	N	N	Y
176	show sflow detail	Display of sFlow statistics (details)	Y	Y	Y	Y
177	port snd/rcv statistics	Statistics on sent/received data on ports	Y	Y	Y	Y
178	internal SW HW event statistics0	Internal software event statistics 0	Y	Y	Y	Y
179	internal SW HW event statistics1	Internal software event statistics 1	Y	Y	Y	Y

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
180	show mac-authentication	Display of the MAC-based authentication setting information	N	N	N	Y
181	show mac-authentication statistics	Display of MAC-based authentication statistics	N	N	N	Y
182	show mac-authentication mac-address edit	Display of registrations and changes in the internal MAC-based authentication DB	N	N	N	Y
183	show mac-authentication mac-address commit	Display of registrations in the internal MAC-based authentication DB	N	N	N	Y
184	show mac-authentication login	Display of authenticated-user information (account information)	N	N	N	Y
185	show mac-authentication logging	Display of action logs for MAC-based authentication	N	N	N	Y
186	show power-control schedule	Display of power saving function schedule	Y	Y	Y	Y
187	swdev logging	Display of SW subunit logs	Y	Y	Y	Y
188	SW MMU statistics0	SW subunit MMU statistics 0	Y	Y	Y	Y
189	DRV internal event log	Event information in the driver (for AX3660S Ver.12.0.A and later)	Y	Y	Y	Y
190	DRV packet classification statistics	Statistics for each driver packet type (for AX3660S Ver.12.0.A and later)	Y	Y	Y	Y
191	DRV packet reason code statistics	Driver packet factor statistics (for AX3660S Ver.12.0.A and later)	Y	Y	Y	Y
192	DRV authentication statistics	Driver packet authentication statistics (for AX3660S Ver.12.0.A and later)	Y	Y	Y	Y
193	DRV internal discard statistics	Discard statistics in the driver (for AX3660S Ver.12.0.A and later)	Y	Y	Y	Y
194	show environment temperature-logging	Temperature history information	Y	Y	Y	Y
195	show track-object detail	Detailed information of tracking function for policy-based routing (for AX3800S Ver.11.9 and later, AX3660S, and AX3650S Ver.11.7 and later)	Y	Y	Y	Y
196	/usr/local/bin/trackobj -t | tail -n 1024	Trace information of tracking function for policy-based routing (for AX3800S Ver.11.9 and later, AX3660S, and AX3650S Ver.11.7 and later)	Y	Y	Y	Y
197	/usr/local/bin/fdbmerge_show -s	Information of MAC address table synchronization function (for AX3800S Ver.11.10 and later, AX3660S, and AX3650S Ver.11.8 and later)	Y	Y	Y	Y

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
198	/usr/local/bin/fdbmerge_show	Information of MAC address table synchronization function (for AX3800S Ver.11.10 and later, AX3660S, and AX3650S Ver.11.8 and later)	N	N	N	Y
199	show bfd session detail	Display of BFD session information (for AX3800S Ver.11.14 and later, AX3660S, and AX3650S Ver.11.14 and later)	N	Y	N	N
200	show bfd discard-packets	Display of information about discarding of BFD packets (for AX3800S Ver.11.14 and later, for AX3660S, for AX3650S Ver.11.14 and later)	N	Y	N	N
201	show vxlan	VXLAN setting information (for AX3660S)	N	N	N	Y
202	show vxlan vni	VXLAN VNI information (for AX3660S)	N	N	N	Y
203	show vxlan peers	VXLAN tunnel peer information (for AX3660S)	N	N	N	Y
204	show vxlan mac-address-table	VXLAN MAC address table information (for AX3660S)	N	N	N	Y
205	show vxlan statistice vni	VXLAN statistics (per VNI) (for AX3660S)	N	N	N	Y
206	show ptp	PTP settings and operating status (for AX3660S Ver.12.1.G and later)	N	N	N	Y
207	show event manager monitor script detail	Monitoring event information registered from the script (for AX3660S Ver.12.1.B and later)	Y	N	N	N
208	show event manager monitor applet detail	Information of event monitored using the applet functions (for AX3660S Ver.12.1.B and later)	Y	N	N	N
209	show event manager history script	Event occurrence history monitored and registered from a script (for AX3660S Ver.12.1.B and later)	Y	N	N	N
210	show event manager history applet	Event occurrence history being monitored by the applet functions (for AX3660S Ver.12.1.B and later)	Y	N	N	N
211	show script installed-file	List of installed script files (for AX3660S Ver.12.1.B and later)	Y	N	N	N
212	show script running-state	Running status of advanced scripts (for AX3660S Ver.12.1.B and later)	Y	N	N	N
213	DRV l2 aging info	L2 aging information in the driver (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y

No.	Command (displayed)	Description	No parameter specified	unicast	multicast	layer-2
214	DRV ctl packet aging info	Driver internal control packet filter aging information (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y
215	stack aging info	Stack aging information (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y
216	DRV stack master change info	Driver internal stack master switching information (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y
217	DRV l3 aging info	Driver internal L3 aging information (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y
218	stack sw add info	Complete stack distribution information (for AX3660S Ver.12.1.N and later)	Y	Y	Y	Y

Legend: Y: Displayed, N: Not displayed