AX2630S/AX2340S

Troubleshooting Guide

AX23S-T001X-40

AlaxalA

■ Relevant products

This manual applies to the models in the AX2630S and AX2340S series.

■ 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

Cisco is a registered trademark of Cisco Systems, Inc. in the United States and other countries.
Ethernet is a registered trademark of Xerox Corporation.
Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and other countries.
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.
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

June 2024 (Edition 1) AX23S-T001X-40

■ Copyright

Preface

■ Relevant products

This manual applies to the models in the AX2630S and AX2340S series.

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

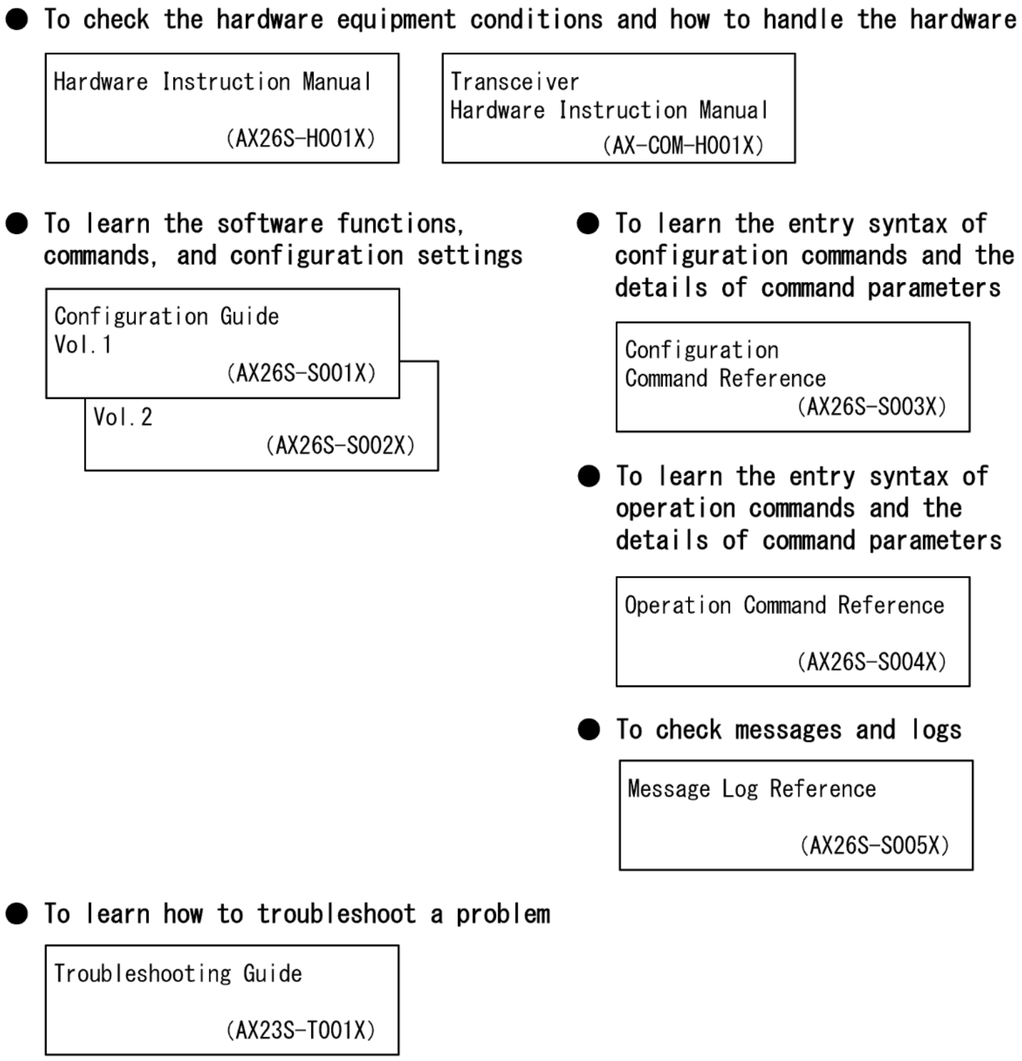
You can view this manual on our website at:

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.

For AX2630S series switches:



- To check the hardware equipment conditions and how to handle the hardware
  - Hardware Instruction Manual (AX26S-H001X)
  - Transceiver Hardware Instruction Manual (AX-COM-H001X)
- To learn the software functions, commands, and configuration settings
  - Configuration Guide Vol.1 (AX26S-S001X)
  - Vol.2 (AX26S-S002X)
- To learn the entry syntax of configuration commands and the details of command parameters
  - Configuration Command Reference (AX26S-S003X)
- To learn the entry syntax of operation commands and the details of command parameters
  - Operation Command Reference (AX26S-S004X)
- To check messages and logs
  - Message Log Reference (AX26S-S005X)
- To learn how to troubleshoot a problem
  - Troubleshooting Guide (AX23S-T001X)

For AX2340S series switches:

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

Hardware Instruction Manual (AX23S-H001X)

Transceiver Hardware Instruction Manual (AX-COM-H001X)

- ● To learn the software functions, commands, and configuration settings

Configuration Guide Vol.1 (AX23S-S001X)

Vol.2 (AX23S-S002X)

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

Configuration Command Reference (AX23S-S003X)

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

Operation Command Reference (AX23S-S004X)

- ● To check messages and logs

Message Log Reference (AX23S-S005X)

- ● To learn how to troubleshoot a problem

Troubleshooting Guide (AX23S-T001X)

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

The term Switch (upper-case "S") is an abbreviation for any or all of the following models:
- AX2630S series switch
- AX2340S 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
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CFM	Connectivity Fault Management
CIST	Common and Internal Spanning Tree
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRR	Deficit Round Robin
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
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
EEE	Energy Efficient Ethernet
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
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
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
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
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PoE	Power over Ethernet
PQ	Priority Queueing
PS	Power Supply
QoS	Quality of Service
RA	Router Advertisement

RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RMON	Remote Network Monitoring MIB
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
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
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
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
USB	Universal Serial Bus
VLAN	Virtual LAN
WAN	Wide Area Network
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.

Table of 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. - For AC power supply Unplug all power cables connected to the Switch from the outlets. - For DC power supply Turn off the breakers on all distribution boards that supply power to the Switch. After completing the above procedure, replace the device.
2	The login prompt does not appear.	1. If a memory card is inserted, remove it. 2. Unplug the device's power cable from the outlet, and then plug it back in. 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. If 1 above does not apply, check to see if there is a power failure. For AX2630S series switches: - When using a power supply unit Replace the failed power supply unit. When a failure occurs on a power supply unit, either of the following applies: (a) The AC OK LED is lit in red. (b) The AC OK LED is off. (c) The DC OK LED is lit in red. (d) The DC OK LED is off. Also, if you are also using a fixed power source, restart the device. Unplug the power supply unit and then perform step 3 below. - When using only fixed power supply Restart the device. Please execute step 3 below. For AX2340S series switches: - If you are using a power supply with an LED display Replace the device whose power supply has failed. When a failure occurs on a power supply unit, either of the following applies: (a) The AC OK LED is lit in red. (b) The AC OK LED is off. (c) The DC OK LED is lit in red. (d) The DC OK LED is off.

No.	Failure details	Action
		- If you are using a power supply that does not have an LED display Restart the device. Please execute step 3 below. 3. If a failed power supply does not apply to step 2 above, 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. (2) If the device does not restart, a failure has occurred in the device. Replace the device. 4. If you are able to restart in step 3 above, check whether there is an error in the environment. (1) Execute the "show logging" command to check the failure information. `>show logging | grep ERR` (2) If the failure information obtained contains a "high-temperature warning" message, the running environment might be the cause of the problem. Ask the system administrator to improve the environment. 5. If failure information does not exist in 4 above 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 orange.	A fatal failure has occurred in the device. Replace the device.
5	- The ST1 LED of the device blinks in orange. - The LINK LED of each port on the device blinks in orange.	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 cable is disconnected or loose.	Connect the power cable correctly.
2	The measured input power supply is outside the following range: For 100 V AC: 90 to 132 V AC For 200 V AC: 180 to 264 V AC For -48 V DC: -40 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.

1.1.2 How to replace the device

The procedures to replace the device 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:
  You can initialize user accounts/passwords, license information, startup configuration, log information, etc.
  Turn on the power to the device, and when the BootROM message is output to the console window, hold down the [Ctrl] + [N] keys at the same time. When the message "Do you erase system setting ? (Y/N):" is output, press the [Y] key (the [Y] key is an uppercase letter). When initialization is complete, the device is automatically restarted, and after the restart, you can log in to the device as the user used during initial installation. Set the console communication speed to 115200 bit/s.

Figure 2-2 Example of device information initialization

```
BootROM: Image checksum verification PASSED
BootROM: Boot image signature verification PASSED
1
Do you erase system setting ? (Y/N): Y

Boot device 0
Starting kernel ...
```

2.1.2 Forgotten administrator mode password

You can initialize the administrator mode password in the same way as when there are no users able to log in, as specified in "2.1.1 Forgotten login user password".

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 the table below.

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: 115200 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 115200 bit/s. 2. If the communication speed of CONSOLE (RS232C) has been set to 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+ authentication is not set. (For details, see "2.2.3 Login authentication using RADIUS/TACACS+ is not possible".)

No.	Failure details	Items to check
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.

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 2-2 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. 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 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 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".)

No.	Symptom	Action or location to check
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.

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.

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 2-3 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 2-4 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 2-5 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.

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 2-6 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 2-7 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 2-8 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 2-9 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 2-10 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 2-2 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 the stack correctly, sequentially check the optional license information, the status of the member switches, and the status of the stack ports.

1. Checking the log

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

2. Isolation of the cause based on optional license information, member switch status, and stack port status

   Isolate the cause according to the following table.

Table 2-3 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 information about the optional licenses of the member switch. show license	Switches without the optional license OP-STK cannot form a stack. Use the "set license" command to set the optional license OP-STK on the member switch. To enable license keys applied by using these commands, 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 status 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. 3.
3	Execute the following commands on each member switch to check the status 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-L2N)
- 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 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 NTP communication failures

2.6.1 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 2-4 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 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. If communication is possible, go to No. 3.
		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.
3	Check the time difference between the Switch and the NTP server.	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.

2.7 Memory card problems

2.7.1 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 2-5 Action to take when "MC : --------" is displayed

No.	Items to check and commands	Action
1	Check the memory card LED.	If the memory card LED is flashing in green, another process might be accessing the memory card. After the memory card LED turns off, execute the command again. If the memory card LED is not flashing 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 the USB port 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 USB port might have failed. Replace the device.

2.7.2 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 2-6 Action to take when "MC not found." is displayed

No.	Items to check and commands	Action
1	Check the memory card LED.	If the memory card LED is flashing in green, another process might be accessing the memory card. After the memory card LED turns off, execute the command again. If the memory card LED is not flashing 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 the USB port 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 USB port might have failed. Replace the device.

2.7.3 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 2-7 Action to take when execution of a command to access the memory card fails

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 USB port might have failed. Replace the device.

2.8 SNMP communication failures

2.8.1 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)#
```

2.8.2 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.

2.8.3 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.

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.	Not provided
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 - 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 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 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.

No.	Port status	Cause	Action
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	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/2.5GBASE-T

If a problem occurs in 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T, 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/2.5GBASE-T problems

No.	Items to check	Cause	Action
1	Use the "show interfaces" command to display the failure	Line quality is degraded.	Check whether the cable types are correct. For the types, see "Hardware Instruction Manual".

No.	Items to check	Cause	Action
	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		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	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 cable is not compatible.	Check whether the cable types are correct. For the types, see "Hardware Instruction Manual".
		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".
4	Use the "show interfaces" command to display the failure statistics, and check whether any of the	Packets exceeding the maximum allowed frame	Adjust the jumbo frame settings to those on the remote device.

No.	Items to check	Cause	Action
	following statistics items is counted for the target port. If any item is counted, see the Cause and Action columns. - Long frames	length are received.	
5	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. - HOL1 - Tail_drop	Packets are discarded.	Check whether drop control and the shaper are being used appropriately in the system configuration.

3.1.3 Problems in 1000BASE-X

If a problem occurs in 1000BASE-X, 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 3-3 Failure analysis method for 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.
			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	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

No.	Items to check	Cause	Action
	item is counted, see the Cause and Action columns. - CRC errors - Symbol errors		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	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. - HOL1 - Tail_drop	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

If a problem occurs in 10GBASE-R, 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 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. - CRC errors - Symbol 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".
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.

No.	Items to check	Cause	Action
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. - HOL1 - Tail_drop	Packets are discarded.	Check whether drop control and the shaper are being used appropriately in the system configuration.

3.1.5 Troubleshooting when using PoE

If no power supply or other problem occurs when using PoE, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-5 Communication failure analysis method when using PoE

No.	Items to check and commands	Action
1	Use the "show power inline" command to check the Status display of the target port.	- If the Status display is off No power is being supplied. Go to No. 2. - If the Status display is denied There is a power shortage for the entire device. Go to No. 4. - If the Status display is faulty Power cannot be supplied to the connected device. Go to No. 5. - If the Status display is inact Power supply is being stopped by an operation command. Go to No. 5. - If the Status display is wait Waiting for the power supply to start using the PoE power supply distribution function. Wait until the waiting time is over.
2	Use the "show power inline" command to check the Priority display of the target port.	- If the Priority display is never Use the "power inline" configuration command to set a priority other than never. - If the Priority display is other than never Go to No. 3.
3	Check whether the "shutdown" configuration command is set for the target port.	- If already set Use the configuration command to set no shutdown. - If not set Check whether the powered device is connected.
4	Use the "show power inline" command to check Threshold(W) and Total Allocate(W).	Power cannot be supplied because the Total Allocate(W) value is greater than Threshold(W). Before adjusting the allocation amount using the configuration, check the power supply for the entire device, the power allocation amount for the ports, and the power consumption for the ports.
5	Execute the "activate power inline" command, and then use the "show power inline" command to check the Status display of the target port.	- If the Status display is off Check whether the powered device is connected. - If the Status display is on Continue with use. - If the Status display is faulty There may be a problem with the powered device or the connecting cable. Go to No. 6.

No.	Items to check and commands	Action
6	Use the "show logging" command and check the presence of a log.	There may be a problem with the powered device or the connecting cable. - If "Supplying power was stopped by the overload detection" is displayed Power cannot be supplied because an overload has been detected. Check the powered device or connection cable. If the problem is not resolved, check the cable length and cable type in the "Hardware Instruction Manual" and replace it. Also, if devices that can supply PoE power are connected to each other, use the "power inline" configuration command to disable the PoE function of the target port. - If "Supplying power was stopped by the thermal shutdown" is displayed A temperature abnormality was detected in the PoE controller and the power supply was stopped. Please review the installation environment of the device and reconnect. If the problem is not resolved, check the powered device or connection cable. - If "Supplying power was stopped by the PD disorder" is displayed The power supply has been stopped because a failure was detected in the powered device. Check the powered device or connection cable.

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 3-6 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.

No.	Items to check and commands	Action
		- Partner Key Unmatch 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 status

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 a VLAN in which Web authentication (fixed VLAN mode) or MAC-based authentication (fixed VLAN mode) is set and a VLAN which does not have these set are both set 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            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.
  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 (macauth)
```

- 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 (macauth)
VLAN ID:600     MAC Counts:1
  * 0012.e200.aa01 (macauth)
```

(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.

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

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

```
> 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 "4.4 IGMP snooping communication failures" and "4.5 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 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 4-1 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.
		For AX2630S series switches: 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.
		For AX2630S series switches: 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.

No.	Items to check and commands	Action
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".
7	For AX2630S series switches: 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	For AX2630S series switches: 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.

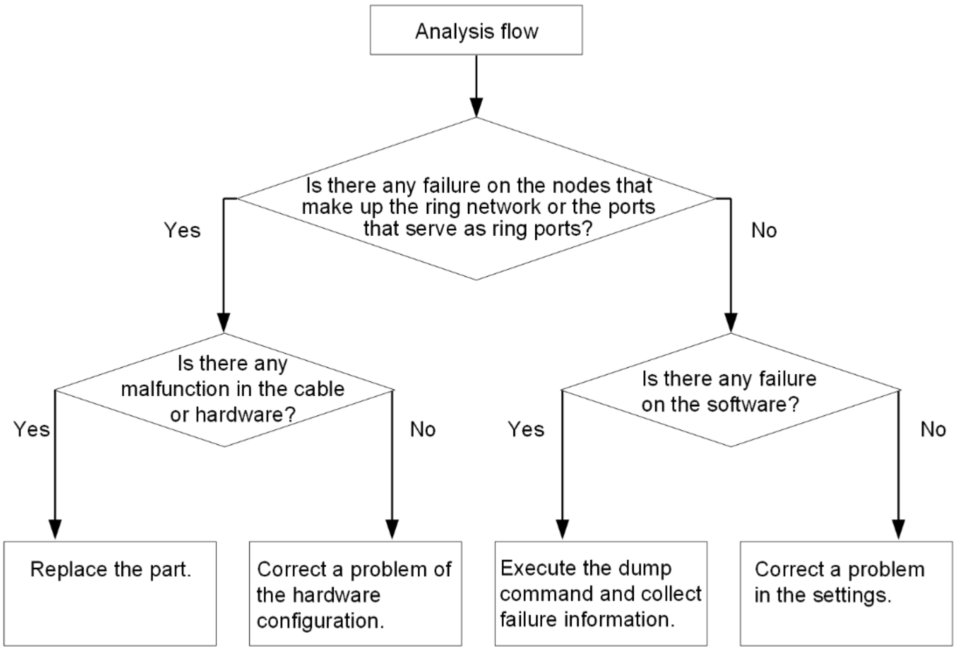
4.3 Ring Protocol communication failures

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


Analysis flow
Is there any failure on the nodes that make up the ring network or the ports that serve as ring ports?
Yes
No
Is there any malfunction in the cable or hardware?
Yes
No
Is there any failure on the software?
Yes
No
Replace the part.
Correct a problem of the hardware configuration.
Execute the dump command and collect failure information.
Correct a problem in the settings.

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

Table 4-2 Failure analysis method for the Ring Protocol (for AX2630S)

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. 2.
		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).
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 status of the VLAN used for the Ring Protocol and the VLAN port statuses.	If there is no anomaly in the statuses of the VLAN and its ports, go to No. 8. Also, go to No. 9 for the configuration in which a Spanning Tree Protocol 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 statuses of the VLAN and its ports.
8	Revise the filter and QoS settings.	There is a possibility that 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 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 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	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
	multi-fault monitoring frames are not received.	
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.

Table 4-3 Failure analysis method for the Ring Protocol (for AX2340S)

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. 2.
		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 inconsistencies.
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", 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.
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 vlan detail" command and check the status of the VLAN used for the Ring Protocol and the VLAN port statuses.	If there is no anomaly in the statuses of the VLAN and its ports, go to No. 7. Also, if there is a configuration that applies the multi-fault monitoring function, go to No. 8 as well.
		If there is any anomaly, check the configuration and restore the statuses of the VLAN and its ports.
7	Revise the filter and QoS settings.	There is a possibility that 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".
8	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 "transport-only" is set, go to No. 9.
		If any other information is displayed, check the configuration.

No.	Items to check and commands	Action
9	Execute the "show axrp detail" command and check the control VLAN ID for the multi-fault monitoring.	If the "Control VLAN ID" is the VLAN ID for the multi-fault monitoring according to the network configuration, the multi-fault monitoring device on the shared node will not receive the multi-fault monitoring, send frame interval timer values, and multi-fault monitoring frame. Check the timer value for the protection time until it is determined that multiple failures have occurred.
		If any other information is displayed, check the configuration.

4.4 IGMP snooping communication failures

If multicast forwarding is impossible when IGMP snooping is used, determine the problem and isolate the cause using the actions specified below.

(1) Checking the log

Use the "show logging" command to check if there is a log indicating a physical failure. For details about the contents of the log, see "Message Log Reference".

(2) Checking frame discarding

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) Checking the IGMP querier

Execute the "show igmp-snooping" command to check whether an IGMP querier exists. If an IGMP querier exists, the IP address of the IGMP querier is displayed in the "IGMP querying system:". If an IGMP querier does not exist (IP address is not displayed), take the following actions.

- If you want to use the Switch as an IGMP querier, set an IP address for the VLAN, and set the "ip igmp snooping querier" configuration command for the target VLAN.
- If the other device is an IGMP querier, connect the target device to the same VLAN.

(4) Checking the connection of devices that can relay multicast data

If a device that can relay multicast data is connected to the same VLAN, execute the "show igmp-snooping" command and check whether the connected port is displayed in the "Mrouter-port:". If the connection port is not displayed, use the "ip igmp snooping mrouter" configuration command to set the connection port to a multicast router port for the target VLAN, or set up multicast router port automatic learning. If multicast router port automatic learning has already been configured, check the multicast router connection.

(5) Checking the subscribed multicast group address

Execute the "igmp-snooping group" command and confirm the subscribed multicast group address. If the subscribed multicast group address is not displayed, check whether the recipient is correctly connected to the same VLAN. If the subscribed multicast group address is displayed, check whether the sender is correctly connected to the same VLAN.

4.5 MLD snooping communication failures

If multicast forwarding is impossible when MLD snooping is used, determine the problem and isolate the cause using the actions specified below.

(1) Checking the log

Use the "show logging" command to check if there is a log indicating a physical failure. For details about the contents of the log, see "Message Log Reference".

(2) Checking frame discarding

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) Checking the MLD querier

Execute the "show mld-snooping" command to check whether an MLD querier exists. If an MLD querier exists, the IP address of the MLD querier is displayed in the "MLD querying system:". If an MLD querier does not exist (IP address is not displayed), take the following actions.

- If you want to use the Switch as an MLD querier, set an IP address for the VLAN, and set the "ipv6 mld snooping querier" configuration command for the target VLAN.
- If the other device is an MLD querier, connect the device to the same VLAN.

(4) Checking the connection of devices that can relay multicast data

If a device that can relay multicast data is connected to the same VLAN, execute the "show mld-snooping" command and check whether the connected port is displayed in the "Mrouter-port:". If the connection port is not displayed, use the "ipv6 mld snooping mrouter" configuration command to set the connection port to a multicast router port for the target VLAN.

(5) Checking the subscribed multicast group address

Execute the "show mld-snooping group" command and confirm the subscribed multicast group address. If the subscribed multicast group address is not displayed, check whether the recipient is correctly connected to the same VLAN. If the subscribed multicast group address is displayed, check whether the sender is correctly connected to the same VLAN.

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 Problems occurring 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. Execute 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 [EAP overRADIUS 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 "dot1x radius-server host" or "radius-server host" configuration command is set correctly. 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. - 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	Check the setting of the authentication access list.	- If an unauthenticated terminal sends certain packets to destinations outside the device, make sure that an authentication access list is set. - For other cases, go to No. 7.

No.	Items to check and commands	Action
7	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 none of the above apply, see the RADIUS server log to check whether authentication has failed.

5.1.2 Checking the configuration of IEEE 802.1X

Check the following for the configuration related to IEEE 802.1X.

Table 5-2 Checking the configuration of IEEE 802.1X.

No.	Check point	Items to check
1	IEEE 802.1X configuration settings	Make sure that the following configuration commands have been set correctly. - aaa accounting dot1x default start-stop group radius - aaa authentication dot1x default group radius - dot1x multiple-authentication - dot1x port-control - dot1x radius-server host - dot1x system-auth-control
2	Check the setting of the authentication access list.	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, or by using the "authentication mac access-group" and "mac access-list extended" configuration commands.

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 access list.	- If an unauthenticated terminal sends certain packets to destinations outside the device, make sure that an authentication access list is set. - Make sure that addresses including the Web authentication IP address are not set 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 and check whether the user ID is registered.	- If the user ID is not registered, use the "set web-authentication user" command to register the user ID, password, and VLAN ID. - 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.

No.	Items to check and commands	Action
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 "web-authentication radius-server host" (or "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 "web-authentication radius-server host" (or "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. - 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.

No.	Items to check and commands	Action
		[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 <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. - 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: - Pre-authentication VLAN - Post-authentication VLAN
3	Check the setting of the authentication access list.	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, or by using the "authentication mac access-group" and "mac access-list extended" configuration commands.
4	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. Note that if you configure the authentication MAC access list to allow ARP packets to pass from unauthenticated terminals, ARP relay settings are not required.

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" and "web-authentication radius-server host" (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.

No.	Failure details	Items to check and commands	Action to take
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" and "mac-authentication radius-server host" (or "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 access list.	- If an unauthenticated terminal sends certain packets to destinations outside the device, make sure that an authentication access list is set. - 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.

No.	Items to check and commands	Action
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 setting of the authentication access list.	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, or by using the "authentication mac access-group" and "mac 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 correctly recorded.	- 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 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" and "mac-authentication radius-server host" (or "radius-server host") configuration commands have been set correctly. - For other cases, check the MAC-based authentication configuration.

No.	Check point	Items to check
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.

6 Troubleshooting of High-reliability Functions

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

6.1 Uplink redundancy communication failures

6.1.1 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 6-1 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 Communication

This chapter describes what to do when a failure occurs in communication 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:

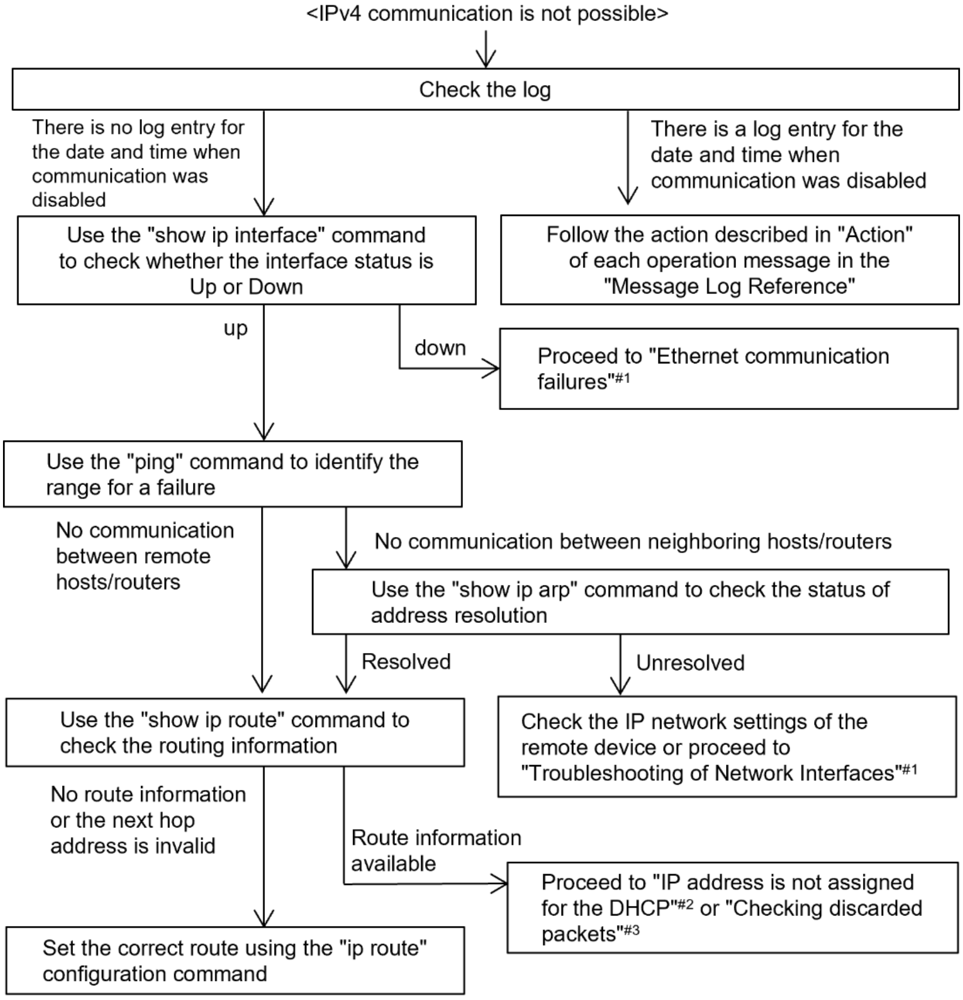
1. A configuration related to IP communication is changed.
2. The network configuration is changed.
3. A network device fails.

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



<IPv4 communication is not possible>
Check the log
There is no log entry for the date and time when communication was disabled
There is a log entry for the date and time when communication was disabled
Use the "show ip interface" command to check whether the interface status is Up or Down
Follow the action described in "Action" of each operation message in the "Message Log Reference"
up
down
Proceed to "Ethernet communication failures"#1
Use the "ping" command to identify the range for a failure
No communication between remote hosts/routers
No communication between neighboring hosts/routers
Use the "show ip arp" command to check the status of address resolution
Resolved
Unresolved
Use the "show ip route" command to check the routing information
Check the IP network settings of the remote device or proceed to "Troubleshooting of Network Interfaces"#1
No route information or the next hop address is invalid
Route information available
Proceed to "IP address is not assigned for the DHCP"#2 or "Checking discarded packets"#3
Set the correct route using the "ip route" configuration command

#1: See "3.1 Ethernet communication failures".

#2: See "7.1.2 IP address is not assigned for DHCP".

#3: 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 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 the address with the neighboring device has been resolved (ARP entry information exists), go to "(6) Checking the routing information".
4. If the address has not been resolved (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 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 to the destination that caused the communication failure or contains an incorrect address of the next hop, use the "ip route" configuration command to set the correct route.
4. If the routing information obtained by the Switch does not contain the routing information to the destination that caused the communication failure, the send/receive interface for the destination that cannot be communicated with might have a problem with any of the functions shown below. Inspect the function associated with the problem.
   - DHCP server function
     Go to "(7) Checking the DHCP server setting information".
   - Filters, QoS, or DHCP snooping
     Go to "(8) Checking discarded packets".

(7) Checking the DHCP server setting information

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

Check whether the setting conditions for DHCP server functions in the configuration are correct. For the procedure, see "7.1.2 IP address is not assigned for DHCP".

(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 DHCP

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. If the client and server settings (such as network card settings and cable connections) have been checked and it has been concluded that "the configuration and network configuration are correct, but IP communication is not possible due to disabled allocation of IP addresses to clients", such as the case in 3 above, see "(2) Checking the operation messages and interface". If no failure has occurred on the Switch, see "(3) Identifying the range for a failure (from the Switch)".

(1) 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.
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".

(2) 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".

(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 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. Execute the "show ip route" command and check the routing information. If you are using a DHCP relay, make sure that the route for the client is registered correctly. Also, use the "ping" command to check communication with a router that is working as a DHCP relay.
3. If the server and the client are directly connected, check the hub and cable connections.

(4) 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".

(5) Checking the Layer 2 network

If you do not find any incorrect settings or a failure in the steps (1) to (4), 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

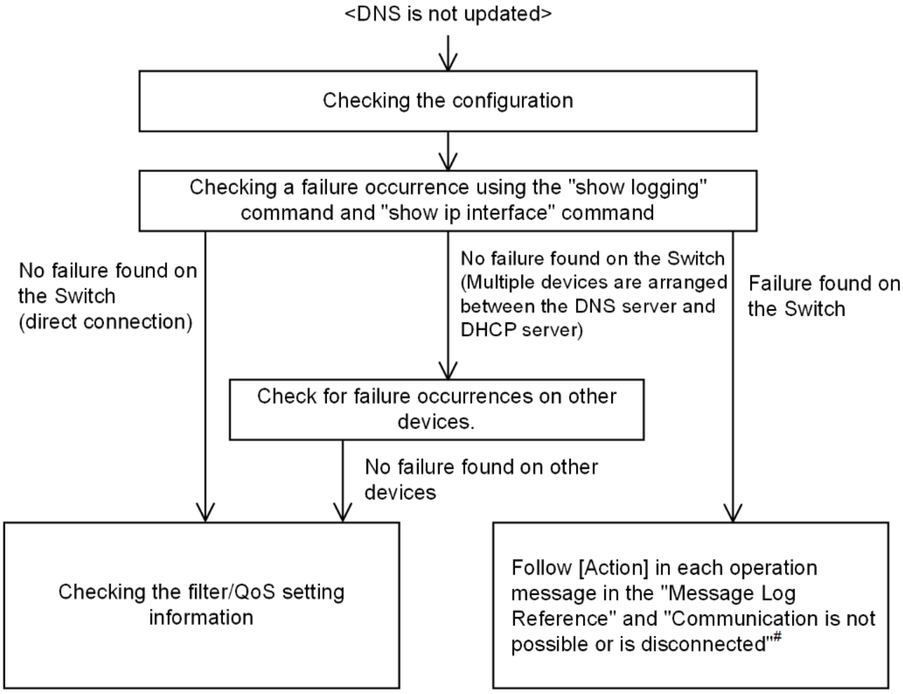
There are three probable causes for communication problems on a DHCP server:

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 "(2) Checking the time information" through "(5) Checking discarded packets" for details.

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

Figure 7-2 Failure analysis procedure for DHCP servers with DNS link established


<DNS is not updated>
Checking the configuration
Checking a failure occurrence using the "show logging" command and "show ip interface" command
No failure found on the Switch (direct connection)
No failure found on the Switch (Multiple devices are arranged between the DNS server and DHCP server)
Failure found on the Switch
Check for failure occurrences on other devices.
No failure found on other devices
Checking the filter/QoS setting information
Follow [Action] in each operation message in the "Message Log Reference" and "Communication is not possible or is disconnected"#

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

(1) 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").

(2) 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.

(3) 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".

(4) 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. Execute the "show ip route" command and check the routing information. If the DNS server is connected to a remote network, make sure that the route for the DNS server is registered correctly.
3. 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 device (router) and the other device in which communication is disabled (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".
4. If the DNS server and the DHCP server are directly connected, check the hub and cable connections.

(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".

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".

(6) Checking the Layer 2 network

If you do not find any incorrect settings or a failure in the steps (1) to (5), 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 IPv6 network communication failures

7.2.1 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:

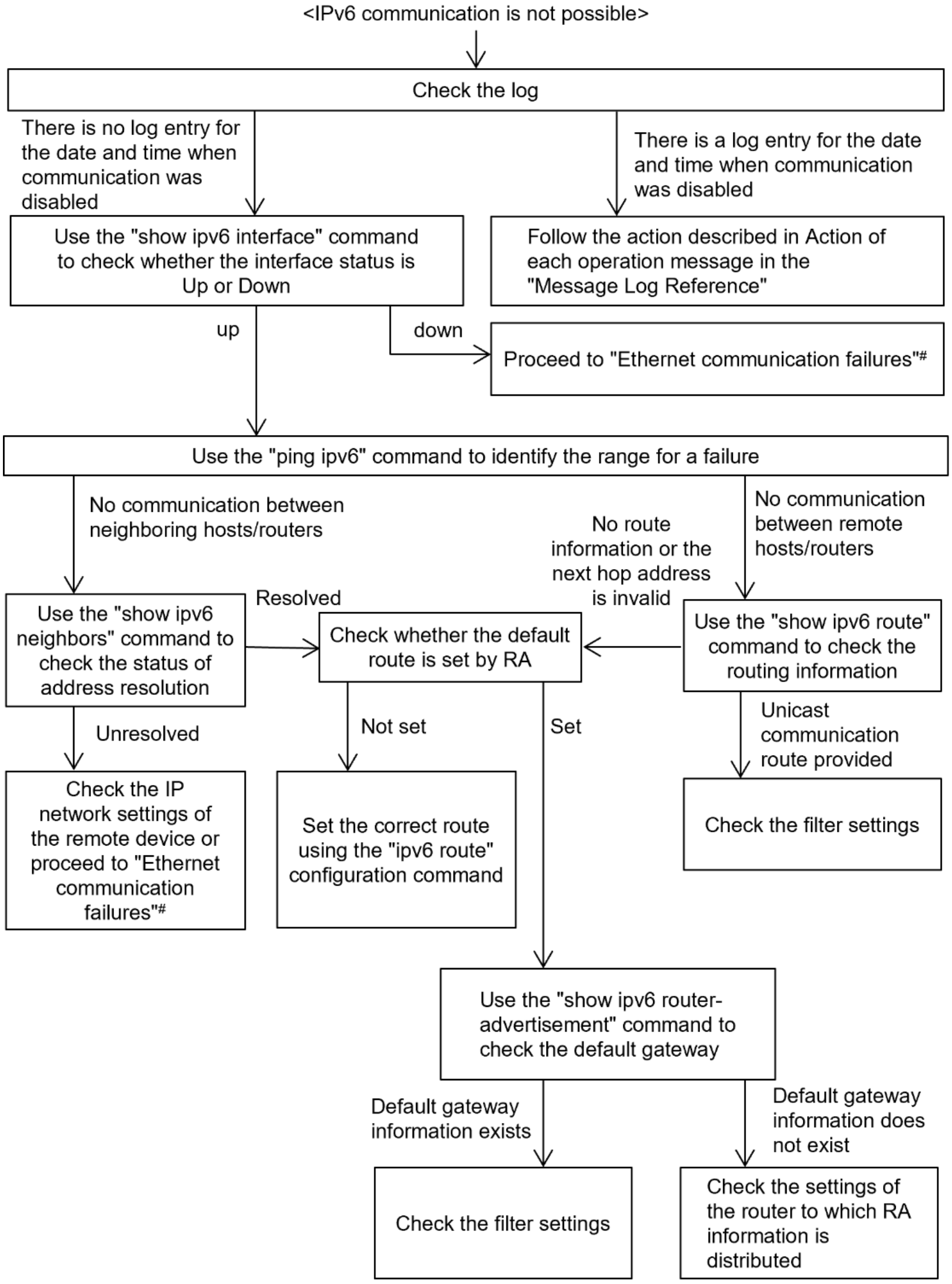
1. A configuration related to IPv6 communication is changed.
2. The network configuration is changed.
3. A network device fails.

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 7-3 Failure analysis procedure for when IPv6 communication is not possible


<IPv6 communication is not possible>
Check the log
There is no log entry for the date and time when communication was disabled
There is a log entry for the date and time when communication was disabled
Use the "show ipv6 interface" command to check whether the interface status is Up or Down
Follow the action described in Action of each operation message in the "Message Log Reference"
up
down
Proceed to "Ethernet communication failures"#
Use the "ping ipv6" command to identify the range for a failure
No communication between neighboring hosts/routers
No route information or the next hop address is invalid
No communication between remote hosts/routers
Use the "show ipv6 neighbors" command to check the status of address resolution
Resolved
Check whether the default route is set by RA
Use the "show ipv6 route" command to check the routing information
Unresolved
Not set
Set
Unicast communication route provided
Check the IP network settings of the remote device or proceed to "Ethernet communication failures"#
Set the correct route using the "ipv6 route" configuration command
Check the filter settings
Use the "show ipv6 router-advertisement" command to check the default gateway
Default gateway information exists
Default gateway information does not exist
Check the filter settings
Check the settings of the router to which RA information is distributed

#: 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 "(7) Checking the RA 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) Checking the RA information".
4. If the routing information obtained by the Switch does not contain the routing information to the destination that caused the communication failure, the send/receive interface for the destination that cannot be communicated with might have a problem with any of the functions shown below. Inspect the function associated with the problem.
   - Filters or QoS function
     Go to "(8) Checking discarded packets".

(7) Checking the RA information

1. Log in to the Switch.
2. Check whether the "ipv6 nd accept-ra default-gateway" configuration command is set for the interface you are trying to communicate with.
3. If the "ipv6 nd accept-ra default-gateway" configuration command is not set, use the "ipv6 route" configuration command to set the correct route.
4. If the "ipv6 nd accept-ra default-gateway" configuration command is set, execute the "show ipv6 router-advertisement" command to check the default gateway information acquired by the Switch.
5. If there is no default gateway information, check the settings of the router that distributes RA information.
6. If the routing information obtained by the Switch does not contain the routing information to the destination that caused the communication failure, the send/receive interface for the destination that cannot be communicated with might have a problem with any of the functions shown below. Inspect the function associated with the problem.
   - Filters or QoS function
     Go to "(8) Checking discarded packets".

(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".

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 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.	Make sure that the DHCP server 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.

No.	Items to check	Action
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. 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.

No.	Items to check	Action
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. 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.

No.	Items to check	Action
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.

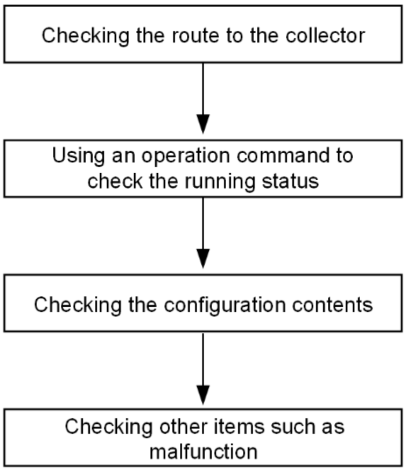
Table 8-5 Failure analysis method for when the target flow is not mirrored

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 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 - show channel-group	If the mirror port is an Ethernet interface and the port status is other than active up, set the port status to active up.
		If the mirror port is a port channel interface and the channel group status is other than Up, set the channel group status to 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


Checking the route to the collector
Using an operation command to check the running status
Checking the configuration contents
Checking other items such as malfunction

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 "7.2.1 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", "7.2.1 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 "7.2.1 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".

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	/dump/rmdump /dump/osdump /usr/var/hardware/ni00.000	- 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	You can check the log information using the "show logging" operation command.	- You can output to a file using the CLI redirection function. - 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.

In a stack configuration, only files on the master switch can be transferred using the "ftp" command. 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 /dump                                            <-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.

9.3 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, the collected information can be transferred by specifying the ftp parameter of the "show tech-support" command only when executed on the master switch. If you execute the "show tech-support" command on a member switch other than the master switch, you cannot specify the ftp parameters.

If you execute the "show tech-support" command on a member switch other than the master switch and transfer the collected information to a file, collect the output of the "show tech-support" command executed on the member switch as a file on the master switch, and transfer the file from the master switch. For the procedure for collecting the output of the "show tech-support" command executed on a member switch as a file on the master switch, see "(2) Collecting information using the show tech-support command (with a stack configuration)". For the procedures to transfer the file on the master switch, see "9.2 Transferring maintenance information files".

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

Figure 9-4 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 9-5 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, if you connect to the stack using the "ftp" command from a remote operation terminal or remote server, you will be connected to the master switch. You cannot connect to member switches other than the master switch by using the "ftp" command.

To obtain failure information and maintenance information from a remote operation terminal or remote server on a member switch 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.
3. Connect to the stack using the "ftp" command from a remote operation terminal or remote server, and transfer the collected information from each member switch on the master switch to a file.

(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

Figure 9-6 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 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.)

(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 /dump and /usr/var/hardware (compressed)
.dump0	Files in /dump (compressed)
.hardware	Files in /usr/var/hardware (compressed)

Figure 9-7 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 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
 Volume in drive C has no label
 Volume Serial Number is C2E0-C0F0
Directory for C:/

tech-1   log    648467 2021-05-26  12:11
        1 file              648 467 bytes
                        837 599 232 bytes free
>
```

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

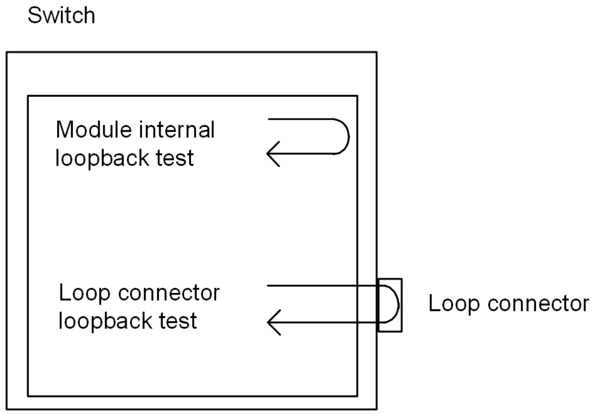


Table 10-1 Test types and fault locations to be identified

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.

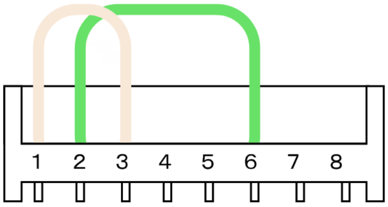
Note that you can check the test results in the same way as described in "10.1.1 Module internal loopback test".

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.

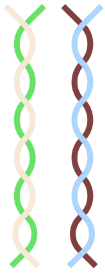
Figure 10-3 10BASE-T/100BASE-TX loop connector wiring specification



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

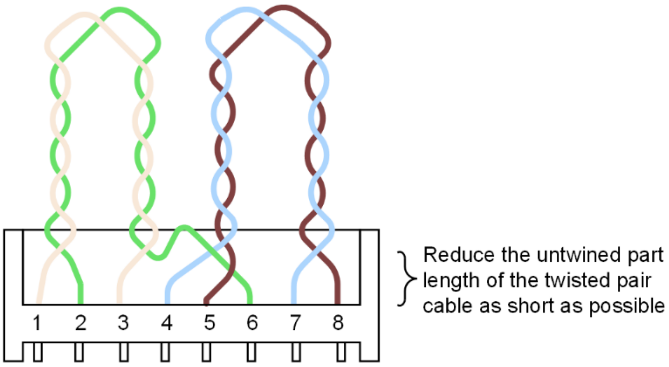
1. Create two 6-to-7-cm long twisted pair cables before you start the procedure.

   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

   Reduce the untwined part length of the twisted pair cable as short as possible

Note that loop behavior using the 1000BASE-T connector is a unique behavior that is not specified in the standard. Therefore, it can only be used for line tests.

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.

(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 due to changes in network topology, etc. 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 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 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 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.

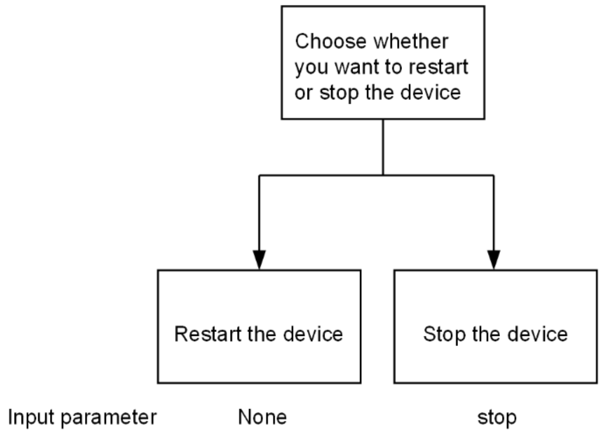
For details on the syntax and parameters of the command, see "Operation Command Reference".

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

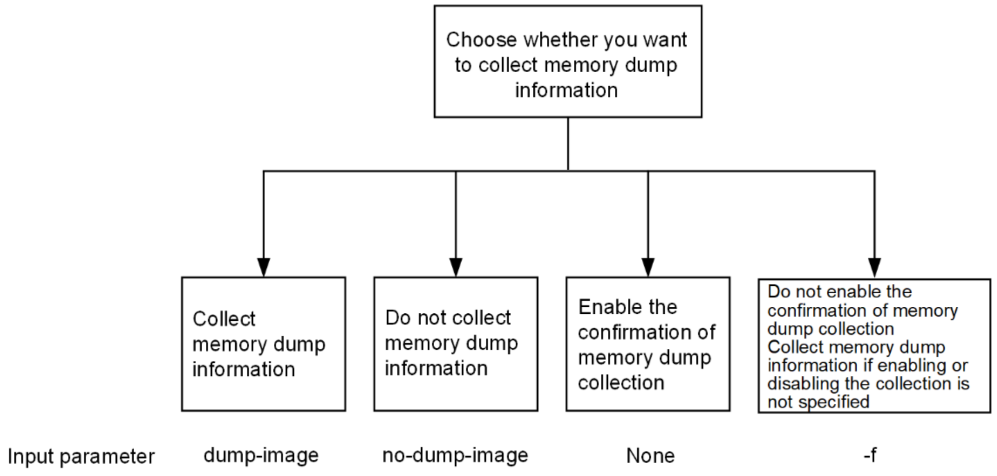


In step 1, you restart the device. So according to the figure above, you do not use any parameters.

Step2

In this step, choose whether you capture the dump.

Figure 11-2 Selection of the CPU memory dump collection type


Choose whether you want to collect memory dump information
Collect memory dump information
Do not collect memory dump information
Enable the confirmation of memory dump collection
Do not enable the confirmation of memory dump collection Collect memory dump information if enabling or disabling the collection is not specified
Input parameter
dump-image
no-dump-image
None
-f

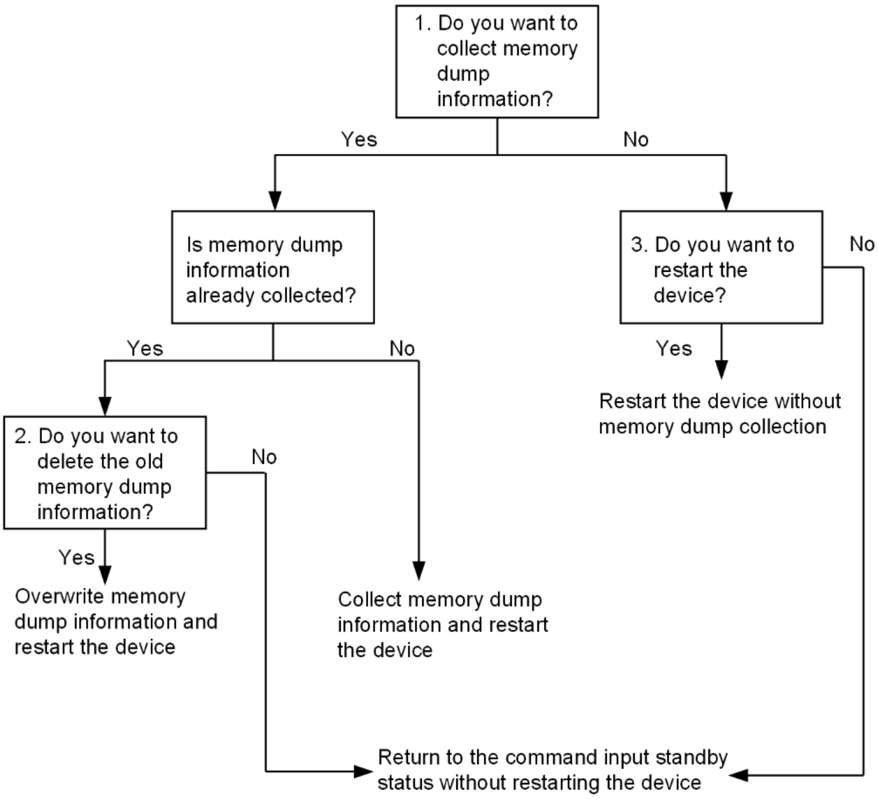
In step 2, you will be asked whether you want to collect the CPU memory dump. According to the figure above, you do not use any parameters.

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 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


1. Do you want to collect memory dump information?
Yes
No
Is memory dump information already collected?
3. Do you want to restart the device?
No
Yes
No
Yes
Restart the device without memory dump collection
2. Do you want to delete the old memory dump information?
No
Yes
Overwrite memory dump information and restart the device
Collect memory dump information and restart the device
Return to the command input standby status without restarting the device

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
1	show version	Software version and hardware information of the Switch
2	show license	Optional license information
3	show system	Operating status of the device
4	show environment	FAN/power supply unit/uptime information
5	show switch detail	Stack details
6	show process cpu	CPU usage of processes
7	show process memory	Memory usage of processes
8	show cpu days hours minutes seconds	CPU utilization
9	show memory	Memory usage of the device
10	show dumpfile	Information on collected dump files
11	ls -leiR /dump	Dump file information
12	ls -leiR /usr/var/hardware	Hardware dump file information
13	ls -leiR /usr/var/core	core file information
14	show running-config	Configuration information for operation
15	show logging	Chronological log information for the active system
16	show logging reference	Log information for each active system
17	/usr/local/diag/statShow	Kernel internal statistics
18	lsof	File descriptor information
19	df	Disk usage
20	df -i	Disk usage
21	du -k /	File capacity in directory
22	show mc	Memory card format and usage status
23	/usr/local/diag/procShow	Process file system information
24	/bin/dmesg	Kernel event information
25	zcat /var/run/dmesg.boot.gz	Kernel event information
26	/usr/local/diag/nodeShow	Device management internal information
27	ls -leiR /config	config file information
28	ls -leiR /var	Memory file system information

No.	Command (displayed)	Description
29	/usr/bin/w	Login-related information
30	show session	Login session information
31	stty -a -F /dev/ttyS0	Console terminal information
32	cat /var/log/clitrace1	CLI trace information 1
33	cat /var/log/clitrace2	CLI trace information 2
34	cat /var/log/mmitrace	Operation command trace information
35	show ip-dual interface	IP interface information
36	show netstat numeric	Layer 4-related statistics
37	show netstat statistics	Layer 3-related statistics
38	show netstat statistics addressfamily inet6	Layer 3-related statistics (IPv6)
39	show netstat interface	Kernel interface information
40	show netstat routing-table numeric	Route-related information in the kernel (unicast)
41	show netstat routing-table numeric addressfamily inet6	Route-related information in the kernel (IPv6 unicast)
42	show ip arp	ARP information
43	show ipv6 neighbors	NDP information
44	show ipv6 router-advertisement	RA advertising information
45	show ntp associations	Information of NTP server behaviors
46	/usr/local/diag/ntpdebug	NTP server debug information
47	show vlan list	VLAN information list
48	show port	Port information
49	show port vlan	Port VLAN information
50	show port statistics	Port statistics
51	show port protocol	Protocol information for ports
52	/usr/local/bin/port show transceiver debug	Transceiver details for ports
53	show port eee	Port EEE information
54	show interfaces nif <nif no.> line <port no.> debug	Detailed statistics for ports
55	/usr/local/bin/information -internal	Detailed statistics for internal ports
56	show power inline	PoE information
57	show vlan detail	VLAN details
58	show vlan mac-vlan	MAC VLAN information
59	nimdump stack aging info	Stack switchover aging time
60	show channel-group detail	Link aggregation details
61	show spanning-tree detail	Spanning Tree details
62	show gsrp aware	GSRP aware information
63	show axrp detail	Detailed information about Autonomous Extensible Ring Protocol
64	show switchport-backup	Uplink redundancy information
65	show switchport-backup detail	Uplink redundancy detailed information
66	show switchport-backup statistics	Uplink redundancy statistics
67	show efmoam detail	IEEE 802.3ah/OAM function setting information and port status
68	show efmoam statistics	IEEE 802.3ah/OAM function statistics

No.	Command (displayed)	Description
69	show lldp detail	Neighboring device information for the LLDP function
70	show lldp statistics	LLDP function statistics
71	show loop-detection	L2 loop detection function information
72	show loop-detection statistics	L2 loop detection function statistics
73	show loop-detection logging	Log information of L2 loop detection function
74	show channel-group statistics	Link aggregation statistics
75	show channel-group statistics lacp	LACP statistics for link aggregation
76	show spanning-tree statistics	Spanning Tree statistics
77	show qos queueing	Statistics on all queues
78	show access-filter	Statistics on filtering
79	show qos-flow	QoS control function statistics
80	show mac-address-table	MAC address table information
81	show igmp-snooping	IGMP snooping information
82	show igmp-snooping group	IGMP snooping group information
83	show igmp-snooping statistics	IGMP snooping statistics
84	show igmp-snooping mrouter	IGMP snooping mrouter information
85	show igmp-snooping mrouter statistics	IGMP snooping mrouter statistics
86	show mld-snooping	MLD snooping information
87	show mld-snooping group	MLD snooping group information
88	show mld-snooping statistics	MLD snooping statistics
89	show ip dhcp snooping statistics	DHCP snooping statistics
90	show ip arp inspection statistics	Dynamic ARP inspection statistics
91	show ip dhcp snooping logging info	DHCP snooping log information
92	/usr/local/bin/dhsn debug	DHCP snooping event information
93	show dot1x logging	Action log messages collected for IEEE 802.1X authentication
94	show dot1x statistics	Statistics on IEEE 802.1X authentication
95	show dot1x detail	Authentication status information on IEEE 802.1X authentication
96	show web-authentication user edit	Display of registrations and changes in the internal Web authentication DB
97	show web-authentication user commit	Display of entries registered in the internal Web authentication DB
98	show web-authentication statistics	Items displayed for statistics related to Web authentication
99	show web-authentication login	Display of authenticated-user information (account information)
100	show web-authentication logging	Display of the action logs for Web authentication.
101	/usr/local/diag/wainfo	Display of Web server session information
102	show mac-authentication	Display of the MAC-based authentication setting information
103	show mac-authentication statistics	Display of MAC-based authentication statistics
104	show mac-authentication mac-address edit	Display of registrations and changes in the internal MAC-based authentication DB

No.	Command (displayed)	Description
105	show mac-authentication mac-address commit	Display of registrations in the internal MAC-based authentication DB
106	show mac-authentication login	Display of authenticated-user information (account information)
107	show mac-authentication logging	Display of action logs for MAC-based authentication
108	show authentication multi-step	Multistep authentication information
109	show sflow detail	Display of sFlow statistics (details)
110	show ip dhcp server statistics	DHCP server statistics
111	show ip dhcp conflict	Information on conflicted IP addresses detected by a DHCP server
112	/usr/local/bin/scriptshow 1 script detail	Monitoring event information registered from the script
113	/usr/local/bin/scriptshow 1 applet detail	Information of event monitored using the applet functions
114	show event manager history script	Event occurrence history monitored and registered from a script
115	show event manager history applet	Event occurrence history being monitored by the applet functions
116	show script installed-file	List of installed script files
117	show script running-state	Running status of advanced script
118	show logging script-only	Operation log information for message type SKY and SRS
119	show environment temperature-logging	Temperature history information
120	cat /var/log/messages.old	Internal information of the kernel and daemons
121	cat /var/log/messages	Internal information of the kernel and daemons
122	cat /var/log/kern.log.old	Internal trace information of the kernel
123	cat /var/log/kern.log	Internal trace information of the kernel
124	cat /var/log/daemon.log.old	Daemon-related internal trace information
125	cat /var/log/daemon.log	Daemon-related internal trace information
126	cat /var/log/diskmount	Disk mount information
127	cat /var/log/kmod.log	Kernel module information
128	cat /var/log/bootcheck.log	u-boot log information
129	cat /usr/var/pplog/ppupdate.log	Log information created when software is updated
130	cat /usr/var/pplog/ppupdate2.log	Log information created when software is updated
131	tail -n 30 /var/log/authlog	Authentication trace information
132	tail -n 30 /var/log/xferlog	FTP trace information
133	cat /var/log/ssh.log	SSH log information
134	show accounting	Accounting information
135	cat /var/tmp/gen/trace/mng.trc	Configuration command trace information
136	cat /var/tmp/gen/trace/mng_sub.trc	Configuration command trace information
137	cat /var/tmp/gen/trace/api.trc	Configuration command trace information
138	cat /var/tmp/gen/trace/ctl.trc	Configuration command trace information
139	/usr/local/diag/drvShow	Driver internal information
140	show snmp	SNMP information

No.	Command (displayed)	Description
141	/usr/local/diag/snmp-dp -mem	SNMP function memory counter
142	cat /var/log/snmp_debug.log	SNMP function debug information
143	show switch debug	Stack debug information
144	cat /var/tmp/stack/stacklog	Stack log information
145	show storm-control detail	Storm control information