AX2630S・AX2340S

Troubleshooting Guide

AX23S-T001-30

■Applicable products

This documentation is intended for AX2630S and AX2340S.

■Precautions for export

If you plan to export any of the models, complete the necessary procedures after checking the Foreign Exchange and Foreign Trade Act and U.S. laws and regulations concerning such exports. If you require more information, please contact an Alaxala sales representative.

■Trademark List

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 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.

■Read and store the manual carefully.

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

■Notes

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

■Issue

November 2022 (4th edition) AX23S-T001-30

■Copyright

Preface

■Applicable products

This documentation is intended for AX2630S and AX2340S.
Before you operate the equipment, carefully read the manual and make sure that you understand all instructions and cautionary notes. After reading the manual, keep it in a convenient place for easy reference.

■Corrections to this manual

Corrections to this manual are contained in the Manual Corrections.

■Intended readers

This manual is intended for system administrators who wish to configure and operate a network system that uses the Switch.
Readers must have an understanding of the following:
・Basic knowledge of network system management

■URL of this documentation

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

■Manual reading procedure

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

For AX2630S

● Determining the hardware installation conditions and how to handle the hardware

Hardware Instruction Manual (AX26S-H001X)

Transceiver Hardware Instruction Manual (AX-COM-H001X)

● Understanding the software functions and the configuration settings

Configuration Guide Vol.1 (AX26S-S001X)

Vol.2 (AX26S-S002X)

● Understanding the syntax of configuration commands and the details of command parameters

Configuration Command Reference (AX26S-S003X)

● Understanding the syntax of operation commands and the details of command parameters

Operation Command Reference (AX26S-S004X)

● Understanding messages and logs

Message and Log Reference (AX26S-S005X)

● How to troubleshoot when a problem occurs

Troubleshooting Guide (AX23S-T001X)

For AX2340S

● Determining the hardware installation conditions and how to handle the hardware

Hardware Instruction Manual (AX23S-H001X)

Transceiver Hardware Instruction Manual (AX-COM-H001X)

● Understanding the software functions and the configuration settings

Configuration Guide Vol.1 (AX23S-S001X)

Vol.2 (AX23S-S002X)

● Understanding the syntax of configuration commands and the details of command parameters

Configuration Command Reference (AX23S-S003X)

● Understanding the syntax of operation commands and the details of command parameters

Operation Command Reference (AX23S-S004X)

● Understanding messages and logs

Message and Log Reference (AX23S-S005X)

● How to troubleshoot when a problem occurs

Troubleshooting Guide (AX23S-T001X)

■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　＊Sometimes written "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 ＊ Sometimes written "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: 1KB (kilobytes), 1MB (megabytes), 1GB (gigabytes), and 1TB (terabytes) are 1024 bytes, 1024^2 bytes, 1024^3 bytes, and 1024^4 bytes respectively.

Contents

1 Troubleshooting Equipment Faults

This chapter describes the actions to be taken in the event of a device failure.

1.1 Device failure analysis

1.1.1 Procedures for responding to device failures

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

For the status of each LED on the device, refer to the "Hardware Instruction Manual" for each model. Even when the device cannot be visually monitored, LED status can be checked by operation commands from a remote operation terminal to perform troubleshooting as if the device can be visually monitored.

Table1-1 Troubleshooting Device Faults

No.	Problem	Action
1	・Smoking from the equipment ・There is an abnormal smell from the device. ・An abnormal sound is generated from the device.	Follow the steps below to stop the power supply to the equipment. ・For AC power supply Disconnect all the power cables connected to this equipment from the power outlets. ・For DC power supply Turn OFF the breakers of all power distribution boards supplying power to this equipment. After completing the above procedure, replace the switch.
2	The login prompt does not appear.	1. If a MC is inserted, disconnect it. 2. Unplug the power cable from the unit and then reinsert it. 3. If restarting the device does not solve the problem, replace the device.
3	The PWR LED of the switch is off.	Follow the procedure shown below: 1. Execute "Table1-2 Power Failure Isolation". 2. If this does not apply to step 1 above, check if the power supply has failed. For AX2630S ・When using a power supply Replace the failed power supply. When a malfunction occurs on a power supply unit, either of the following applies: (a)AC OK LED is red. (b)AC OK LED is off (c)DC OK LED is red. (d)DC OK LED is off In addition, if you are using a fixed power source, restart the equipment. Disconnect the power supply unit, and then execute the following 3. ・When only a fixed power supply is used Restarts the switch. Execute the following 3. For AX2340S ・When using a power supply with a LED indicator Replace the unit with a failed power source. When a malfunction occurs on a power supply unit, either of the following applies: (a)AC OK LED is red. (b)AC OK LED is off (c)DC OK LED is red. (d)DC OK LED is off ・When using a power supply without a LED indicator

No.	Problem	Action
		Restarts the switch. Execute the following 3. 3. If the above step 2 does not correspond to a power failure, restart the Equipment and check for any environmental problems. (1)Turn OFF the power and turn it ON again to restart the unit. (2)If the equipment does not restart, the equipment has failed. Replace the Switch. 4. If you were able to restart with step 3 above, check if there was an error in the environment. (1)Execute show logging command. Check the fault data. `>show logging | grep ERR` (2)If the error message "Hot Caution" exists in the collected error information, ask the person in charge of the facility to improve the environment because the error is probably caused by the operating environment. 5. If there is no error information or there is no message "Hot Caution" in step 4 above, the equipment has failed. Replace the equipment.
4	ST1 LED on the device is lit orange.	A fatal failure has occurred in the system. Replace the Switch.
5	・ST1 LED on the device is blinking orange ・LINK LED on the device is lit in orange.	A partial failure has occurred in the device or line. Refer to the error message and take appropriate action for the error. Use the show logging command to check the failure information and take action. `>show logging | grep ERR`

Table1-2 Power Failure Isolation

No.	Problem	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 AC100V: AC90～132V For AC200V: AC180～264V For DC-48V: DC-40～-57V Note: Take this action only if the input power supply can be measured.	Ask the person responsible for the facility where the switch is housed to take action regarding the input power supply.

1.1.2 How to replace the equipment

For information on how to replace the equipment, refer to the Hardware Instruction Manual. Follow the instructions in the manual.

2 Troubleshooting operations management

This chapter describes the actions to be taken in the event of a problem in operation and administration.

2.1 Login problems

2.1.1 Forgot the password of the logged-in user

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.
  Execute these commands 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.

Figure2-1 user1 passwords are reset

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

- If no users can log in:
  User account/password, license information, startup configuration, log information, etc. can be initialized.
  Turn ON the power to the device. When BootROM message is displayed on the console screen, press [Ctrl] + [N] simultaneously to continue. When the message "Do you erase system setting ? (Y/N)" is displayed, press the [Y] key (the [Y] key is uppercase). After the initialization is completed, the Switch is automatically restarted, and after the restart, you can log in to the Switch with the user at the initial installation. The baud rate of the console should be 115200bit/s.

Figure2-2Example of Initializing Device Information

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

Boot device 0
Starting kernel ...
```

2.1.2 Forgot password for administrator mode

You can initialize the password in administrator mode in the same way as when there is no user who can log in with "2.1.1 Forgot the password of the logged-in user".

2.2 Operation terminal problems

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

If you encounter problems connecting to the console, check the following table.

Table2-1 Console Connection Problems and Responses

No.	Problem	Items to check
1	Nothing is displayed on the screen.	Perform the following procedure: 1. Make sure that the green ST1 LED on the front of the machine is lit. If it is not illuminated in green, refer to the Hardware Instruction Manual. 2. Check if the cable connection is correct. 3. Check that a RS232C cross cable is used. 4. Check whether the communication software settings such as port number, communication speed, data length, parity bit, stop bit, and flow control are as follows. Baud rate: 115200bit/s (if changed, set) 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/reception may be interrupted by XON/XOFF flow-control. Cancel interruption of data transmission/reception (press [Ctrl] + [Q]). If you are still unable to enter a key, check 2. and later. 2. Check that the communication software settings are correct. 3. The window may be stopped due to [Ctrl] + [S]. 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) is not set in the configuration command line console 0, check that the communication speed of the communication software is set to 115200bit/s. 2. If the communication speed of CONSOLE(RS232C) is set to 2400, 4800, 9600 or 19200bit/s by the configuration command line console 0, check 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. Check that the login prompt is displayed on the screen. If it is not, the Switch is starting up. Wait a while. 2. When logging in with local authentication, make sure that you do not attempt to log in with an account that does not exist on the appliance. 3. Make sure that RADIUS/TACACS + Authentication is not set in aaa authentication login console and aaa authentication login configuration commands (see " 2.2.3Unable to authenticate login using RADIUS/TACACS + “for more information).
6	When the communication speed of the communication software is changed after login,	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.

No.	Problem	Items to check
	unexpected characters are displayed and no commands can be entered.	
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. Press [Alt] + [B] to issue the break signal. 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 content are displayed out of alignment.	The displayed information might be greater than the maximum number of characters that can be displayed on one line. Change the screen size setting of the communication software to increase the number of characters that can be displayed on one line.

2.2.2 Login from a remote operation terminal

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

Table2-2 Connection problems with remote operation terminals and their corresponding actions

No.	Problem	Action
1	Remote connection is not possible.	Perform the following procedure: 1. Use ping commandfrom PC or WS to check whether a route for remote connectivity has been established. 2. If it takes a while for the prompt to appear after the connection establishment message is displayed, communication with DNS server may not be possible. (If communication with DNS server is not possible, it takes about 5 minutes for the prompt to appear. This time is a general estimate and varies depending on the network status.)
2	Login is not possible.	Perform the following procedure: 1. Verify that you are using a terminal that has IP allowed in the access list in line vty mode of the configuration command. Also, make sure that no deny is specified for IP addressset in the configuration command access list (see the "Configuration Guide" for more information). 2. When logging in with local authentication, make sure that you do not attempt to log in with an account that does not exist on the appliance. 3. Ensure that you do not exceed the maximum number of users that can log in (see the Configuration Guide for more information). If the number of login users has reached the maximum and if connection from a remote terminal to the Switch is lost and then restored, no more users will be able to log in from a remote 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 terminal or the network, the protocol usually times out after 10 minutes. 4. In transport input of line vty configuration command mode, check whether the protocol that prohibits accessing the Switch is used (for more information, see "Configuration Command Reference"). 5. In the configuration command aaa authentication login, make sure that RADIUS/TACACS + Authentication is not set (see "2.2.3Unable to authenticate login using RADIUS/TACACS +” for more information).
3	Key entry is not accepted.	Perform the following procedure: 1. Data transmission/reception may be interrupted by XON/XOFF flow-control. Cancel interruption of data transmission/reception (press [Ctrl] + [Q]). If you are still unable to enter a key, check 2. and later. 2. Check that the communication software settings are correct.

No.	Problem	Action
		3. The window may be stopped due to [Ctrl] + [S]. 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 Switch again and enter configuration mode to save the configuration, and then finish editing.

2.2.3 Unable to authenticate login using RADIUS/TACACS +

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

1. Communication with the RADIUS or TACACS+ server
   Use the ping command to check if a connection from the Switch to the RADIUS or TACACS+ server has been established. If communication is not possible, refer to "7.1.1Cannot communicate 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 or 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: <set-response-timeout-value-(in-seconds)> x <set-number-of-retries> x <set-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: <set-response-timeout-value-(in-seconds)> x <set-number-of-TACACS+-servers>. If the time increases significantly, an application on a remote terminal, such as Telnet, might have terminated due to a timeout. If this happens, change the RADIUS or TACACS+ configuration settings or the timeout setting of an application running on a remote terminal. In addition, Telnet or FTP might have failed even when a message indicating successful RADIUS or TACACS+ authentication is output to the operation log. In this case, an application running on a remote terminal might time out before the application can connect to a running RADIUS or TACACS+ server of those servers you specified in the configuration. Change the settings so that a running RADIUS or TACACS+ server takes priority, or decrease the value of <response-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 Command authorization using RADIUS/TACACS+ /local is not possible

After RADIUS, TACACS+, or local authentication is successful and you log in to the Switch, if command authorization fails or if a command cannot be executed due to an authorization error, 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 or 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 or 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 local command authorization is used, make sure that the settings in the configuration are correct. For details on 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 permission command list, the show ip interface is permitted, but the show ipv6 interface command is not permitted.

3. Action to take when all commands are restricted
If all commands are restricted due to, for example, incorrect settings, log in from the console and modify the settings.

2.3 SSH problems

2.3.1 Unable to connect to the Switch by SSH

If a SSH client on another device cannot connect to the Switch using SSH(ssh,scp, and sftp) check the following:

(1) Checking the establishment of a remote connection route

The communication path between the Switch and the operation terminal may not be established. Use ping commandto check the communication path.

(2) Checking the configuration of SSH servers

If SSH server-related configuration has not been set, the Switch cannot be connected by SSH. Also, if the settings of SSH servers of the Switch and the settings of SSH clients of other switches do not coincide with the authentication methods, you cannot connect.

Make sure that SSH servers are configured correctly in the configuration. If an access list is specified in remote access control, check whether the connection is made from a terminal with the permitted address.

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

To log in to the Switch using public key authentication, check again to make sure that the user public key registered in the Switch configuration is the correct key.

Figure2-3 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. Verify that the correct public key is registered with the correct user name.

(4) Confirm whether the password for the login account is set

By SSH, if you omit the password when authenticating, you cannot log in. Set a password for the account.

(5) Check the number of logged-in users

Use show logging command to check whether the operation log shown in the following figure has been output when attempting to log in beyond the maximum number of users that can log in to the Switch.

Figure2-4 Example of exceeding the maximum number of logins on the Switch

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

(6) Checking the Switch for Unauthorized Access

To prevent unauthorized access, SSH servers feature of the Switch limits the number of login users, the number of accesses during the authentication process, and the time (two minutes) until login completion, in addition to the limit on the number of login users. Therefore, if SSH cannot connect to the Switch even though the number of logged-in users on the Switch displayed by show sessions command is small, there may be sessions that are not logged in even if they are connected. Check the following points

1. Execute show ssh logging command on the Switch to check the trace log of SSH server.
   The following illustration shows an example in which a connection is rejected due to a large number of sessions connecting to SSH server. This example is displayed if there are sessions that are connected but not logged in.

   Figure2-5 Connection rejected because there are many sessions connecting to 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. Check the connection source of the illegal session even if you are connected but not logged in, and take measures such as restricting remote access.
   If you are still connected but are not logged in, the incorrect session will be released after two minutes, and you will be able to log in with SSH again.

2.3.2 The Switch cannot execute commands remotely.

(1) Check SSH client-specified options

If you execute an operation command (execute the command remotely) from a SSH client on another device to the Switch without logging in as a SSH, the command execution result may not be displayed and an error may be displayed. The following figure shows an example of a failure in executing a command remotely to the Switch.

Figure2-6 Example of Remote Command Execution Failure for the Switch

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

To execute commands remotely to the Switch without logging in as a SSH, you must assign a virtual terminal with-t parameter. The following figure shows an example of successful execution of a command remotely to the Switch.

Figure2-7 Example of Successful Command Execution for the Switch from a Remote

```
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.

Only commands in user mode can be executed remotely to the Switch without logging in as a SSH. If you execute a command in administrator mode, an error occurs.

Log in to the Switch using SSH to enter the administrator mode, and then execute the command in administrator mode.

(3) Checking for Commands That Require y/n Entry

Commands that prompt you to enter (y/n) in response to a confirmation message such as a reload command cannot be executed remotely on the Switch. Execute such a command by specifying any parameters that are forcibly executed

without displaying a confirmation message, or after logging in to the Switch using SSH.

2.3.3 A secure copy cannot be made to the Switch.

Some SSH clients log in to an interactive session (CLI) without assigning a virtual terminal and forward the files after logging in. The Switch does not support logging in to CLI. Check the trace log on the client side and check that the message shown in the following figure has not been received from the Switch. Secure copying cannot be performed from such SSH clients for the Switch.

Figure2-8 Client-Side Trace Logs That Fail to Make a Secure Copy to the Switch

```
Not tty allocation error.
```

Even with such a SSH client, if secure FTP is supported, it can be used to transfer the files.

2.3.4 Forgot the passphrase for public key authentication

If you forget the passphrase you enter when logging in to the Switch with SSH public key authentication, you cannot use that user key pair (user public key and user private key). Take action according to the following procedure:

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

Use the configuration command ip ssh authkey on the Switch to remove the user public key of the user who forgot the passphrase. The following figure shows an example of deleting a user public key from SSH configuration of the Switch.

Figure2-9 Deleting the user public key from 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) Deleting a SSH Client-Side Terminal User Key Pair

On SSH client-side terminal, remove the user key pair (user public key and user private key) of the user who forgot the passphrase and unregister. To use public key authentication again, re-create the user key pair on SSH client to be used, and then register the user public key again in SSH configuration of the Switch.

2.3.5 Host Public Key Change Warning Appears When Connecting

If the message "@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @" is displayed when a SSH is connected to the Switch from another device, this indicates that the host public key on the Switch has been changed since the previous connection.

If this message is displayed, a malicious third party may impersonate the server. Follow the steps below to check the message carefully before connecting to the server using SSH.

(1) Contact the administrator of the Switch

Contact your appliance administrator for the following information:

- Have you intentionally changed the host key pair using set ssh hostkey command.?
- Is the device configuration changed?

If the administrator has not changed the host key pair on the Switch, there is a risk of spoofing or connecting to other hosts. Interrupt SSH connection and contact the network administrator. The following figure shows an example of interrupting the connection with SSH.

Figure2-10 Example of Interrupting Connectivity in SSH

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

1. Enter "no" here and do not connect.

If there is no risk of spoofing and the host public key of the Switch has been changed, follow the procedure below to reconnect the Switch.

(2) Reconnect if the host public key is changed

From SSH client, connect to SSH servers of the Switch whose host key pairs have been changed using SSHv2 protocol. To make the connection more secure, check Fingerprint to make sure that SSH servers of the Switch you are trying to connect to are the hosts with the correct connection.

1. Pre-confirmation of Fingerprint
   Log in to the Switch in advance and use show ssh hostkey commandto check Fingerprint. It is safer to check it in a secure way other than via the network, such as a console connection.
2. Notify client users of Fingerprint
   Notifies SSH client user of the confirmed Fingerprint. It is safer to notify them in a secure manner other than via the network, such as by mail or by telephone.
3. Check Fingerprint and connect to SSH.
   On the client, confirm that Fingerprint displayed when connecting SSH to SSH servers of the Switch is the same as that notified in step 2, and then connect.
   Some clients show Fingerprint in HEX format and some in bubblebabble format. In addition, some SSHv1 do not support Fingerprint. Check in a format suitable for the client.

(3) Register or delete a user's host public key database

Depending on SSH client to be used, the host public key registered in the user's host public key database and the host public key of the Switch's SSH server may not be automatically deleted, and a warning may be displayed or connection may not be established each time a connection is made. In this case, edit or delete the file manually and reconnect.

2.4 Configuration problems

2.4.1 Unable to return to administrator mode from configuration mode

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

(1) When connected to a console

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

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 is the login number of the corresponding 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 terminal

Temporarily shut down the remote terminal, and then re-connect it.

If any user remains logged in, take action according to “Table2-2 Connection problems with remote operation terminals and their corresponding actions” item 4 in the section.

2.5 Stack configuration problems

2.5.1 Stack configuration is not possible

If you are unable to configure the stack successfully, check the option license information, the member switch state, and then the stack port state.

1. Checking the Log
   For log information, see "Message and Log Reference".
2. Isolating causes by option license information, member switch state, and stack port state
   Isolate the cause according to the following table.

Table2-3 What to do if a stack cannot be configured

No.	Items to check and commands	Action
1	Execute the following command on each member switch to check the optional license information of the switch: show license	Switches that do not have an optional licensing OP-STK cannot be stacked. Use set license command to set the optional licensing OP-STK on the member switches. 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 state of the switch: show switch detail	If the stack status is Disable, standalone operation is in progress. After setting the configuration command to stack enable and saving it to the startup configuration, restart the device and execute the stack functionality.
		If Switch No is the same for multiple member switches, 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.
		If not applicable, go to Item 3.
3	Execute the following commands on each member switch to check the state of the stack ports: show port show switch detail	If Status is not up when show port command is executed, check the status of the Ethernet port by referring to "3.1.1The Ethernet port cannot be connected. ".
		In the results of executing the show port command, if Status is up, yet in the results of executing the show switch command with the detail parameter specified, Status is Down, there might be a mistake in the configuration of the member switches connected via stack port. Check the configuration as follows: ・Setting the Switch Number and Device Model Make sure the switch numbers and device models set by using the configuration command switch provision are consistent with the switch numbers and device models of the member switches that are actually connected. ・Configuring Stack Ports Make sure the stack ports set by using the stack parameter of the configuration command switchport mode are consistent with the ports that are actually connected.

2.5.2 Stack configuration cannot be edited

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

On the master switch, run show version command. Check the software for all member switches that make up the stack. Even if you already have a stack configuration, the following software information must be consistent before you can edit the configuration:

- SoftwareType (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 Configuring 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
- Updating the Software Before Startup

If you want to the member switch that becomes the master switch to be fixed, 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 The Switch cannot be synchronized by 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.

Table2-4 Fault Analysis Methods for NTP

No.	Items to check and commands	Action
1	Use the show clock command to make sure 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 Item 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 MC problems

2.7.1 MC status is not displayed

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

Table2-5 "MC :--------" is displayed. Correspondence method

No.	Items to check and commands	Action
1	Check LED of MC.	Other processes might be accessing MC if LED on MC is blinking blue. After LED of MC turns off, re-execute the command. If LED on MC is not blinking blue, go to item 2.
2	Remove the memory card and insert it again.	After removing and inserting the memory card, execute the command again. When inserting MC, make sure that there is no dust adhering to USB ports on MC and the equipment. 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 the problem persists after replacing MC, USB may be faulty. Replace the Switch.

2.7.2 Errors occur when accessing MC

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.

Table2-6 Correspondence when "MC not found." is displayed

No.	Items to check and commands	Action
1	Check LED of MC.	Other processes might be accessing MC if LED on MC is blinking blue. After LED of MC turns off, re-execute the command. If LED on MC is not blinking blue, go to item 2.
2	Remove the memory card and insert it again.	After removing and inserting the memory card, execute the command again. When inserting MC, make sure that there is no dust adhering to USB ports on MC and the equipment. 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 the problem persists after replacing MC, USB may be faulty. Replace the Switch.

2.7.3 MC cannot be accessed

If the command accessing MC fails, check the following:

Table2-7What to do if the command for accessing the MC fails

No.	Items to check and commands	Action
1	Please check if the target MC is our recommendation.	If MC is not the one recommended by us, it may not be accessed correctly. If this is MC of our recommendation, go to Item 2.
2	Check that MC has been formatted on the Switch.	If our recommended MC is formatted on another device (such as a PC), it may not be accessible correctly. Insert MC into the Switch and execute format mc command. Then, format MC. If formatting MC does not improve the problem, go to Item 3.
3	Replace the memory card.	After replacing the memory card, execute the command again. If the problem persists after replacing MC, USB may be faulty. Replace the Switch.

2.8 SNMP communication failures

2.8.1 MIBs cannot be obtained from the SNMP manager

Make sure 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 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 this happens, review the trap reception settings in SNMP Manager according to the object ID of the traps described in MIB Reference.

2.8.3 Unable to receive informs in SNMP Manager

Execute the configuration command show snmp-server to check whether SNMP manager and the inform are set in the Switch configuration. If it is not set, execute the configuration command snmp-server host to set SNMP manager and inform.

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

Some SNMP Manager systems may not be able to receive informs of ospf,bgp issued by SNMPv2C,SNMPv3. If this happens, review the settings for receiving SNMP Manager informs according to ID of the informs listed in MIB Reference.

3 Troubleshooting a Network Interface

This chapter describes the actions to be taken in the event of a network interface failure.

3.1 Ethernet communication failure

3.1.1 The Ethernet port cannot be connected.

If the Ethernet port is considered to be the cause of the communication failure, check the port status and port statistics in this order.

(1) Checking the port status

1. Checking the log
   For log information, see "Message and Log Reference".
2. Isolating the cause of the problem by checking the port status
   Use the show interfaces command to check the port status, and isolate the cause of the problem according to the following table.

Table3-1 Checking and responding to port status

No.	Port status	Cause	Action
1	active up	The target port is operating normally.	No
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 “Message and 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 functionality of link aggregation ・Inactive due to the BPDU guard functionality of the Spanning Tree Protocol ・Fault detected by IEEE802.3ah/UDLD function ・L2 loop-detection function is used to turn inactive the port. ・The port was placed in inactive status by the storm control function.	・If the standby link function of link aggregation is in inactive status, do not use activate command to place the link in active status because the operation is normal. Use the show channel-group command with the detail parameter to check the standby link functionality. ・If BPDU guard function of Spanning Tree Protocols is used to inactive the Switch, review the settings on the partner switch, configure the Switch not to receive BPDU, and use activate command to active the corresponding switch. Use the show spanning-tree command with the detail parameter to check the BPDU guard functionality. ・If IEEE802.3ah/UDLD function is inactive because a one-way link failure or L2 looping has been detected, see ” 8.4IEEE802.3ah/UDLD function problems”. After restoration from the failure, use the activate command to activate the target port. ・If L2 loop detection function is used for inactive, change the configuration in which the loop occurs, and then use activate command to place the corresponding port in active status. Also, if loop-detection auto-restore-time is specified by a configuration command, the port will automatically return to the active status. ・If the storm control function is used to place inactive port, use activate command to place the port in active status after LAN recovers from the storm. ・If none of the above conditions exist, and you want to turn active the port, make sure that the cable is connected to the port to be used, and then turn active the port by using activate command.
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

No.	Port status	Cause	Action
			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 “Message and 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 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.

Figure3-1 Example of "Checking the operating status of the port"

```
> 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 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T problems

If a problem occurs in 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T, separate the failure according to the following order.

1. Checking the log
   For log information, see "Message and 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.

Table3-2How to analyze faults in the event of 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T troubles

No.	Items to check	Cause	Action
1	Use the show interfaces command to display the failure statistics, and check whether there is a count for the following item for the target port. If there is a count, see the Cause and Action columns. ・Link down	Line quality is degraded.	Check whether the cable types are correct. For the types, see “Hardware Instruction Manual”.
			If the Switch is set as follows, make sure that the pin mapping is for MDIX. ・When the setting of the corresponding port is fixed ・When the setting of the applicable port is auto-negotiated and the auto MDI/MDIX function is disabled
			Check the cable length. For the cable length, see

No.	Items to check	Cause	Action
			“Hardware Instruction Manual”.
			Check whether the cables are connected correctly (for example, check for incomplete insertion).
			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 functionality of the receiving side has no problem. Check the results of the no test interfaces (Ethernet) command, and take the action described in Action. See “10.1Testing the Line” for the type of test you want to specify.
2	Use the show interfaces command to display the failure statistics for the receiving side, and check whether there are counts for the following items for the target port. If there is a count, 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 MDIX. ・When the setting of the corresponding port is fixed ・When the setting of the applicable port is auto-negotiated and the auto MDI/MDIX function is disabled
			Check the cable length. For the cable length, see “Hardware Instruction Manual”.
			Check whether the cables are connected correctly (for example, check for incomplete insertion).
			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 functionality of the receiving side has no problem. Check the results of the no test interfaces command, and take the action described in Action. See “10.1Testing the Line” for the type of test you want to specify.
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. See “Configuration Guide” for more information.
4	Use the show interfaces command to display the failure statistics, and check whether there is a count for the following item for the target port. If	Packets exceeding the maximum	Adjust the jumbo frame settings to those on the remote device.

No.	Items to check	Cause	Action
	there is a count, see the Cause and Action columns. ・Long frames	allowed frame length are received.	
5	Use the show qos queueing command to check whether there is a count for the following item. If there is a count, 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 1000BASE-X problems

If a problem occurs in 1000BASE-X, separate the failure according to the following order.

1. Checking the log
   For information about the log, see "Message and 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.

Table3-3How to analyze faults in the event of 1000BASE-X troubles

No.	Items to check	Cause	Action
1	Use the show interfaces command to display the failure statistics, and check whether there is a count for the following item for the target port. If there is a count, 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 (for example, check for incomplete insertion). 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 functionality of the receiving side has no problem. Check the results of the no test interfaces command, and take the action described in Action. See “10.1Testing the Line” for the type of test you want to specify.
2	Use the show interfaces command to display the failure statistics for the receiving side, and check whether there are counts for the following items for the target port. If there is a count, see the Cause and Action columns. ・CRC errors ・Symbol errors	Line quality on the receiving side is degraded.	Check the type of the optical fiber. For the mode, see “Hardware Instruction Manual”.
			If an optical attenuator is used, check the attenuation value. For the optical level, see "Hardware Instruction Manual".
			Check the cable length. For the cable length, see “Hardware Instruction Manual”.
			Check whether the cables are connected correctly (for example, check for incomplete insertion). Make sure that

No.	Items to check	Cause	Action
			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 functionality of the receiving side has no problem. Check the results of the no test interfaces command, and take the action described in Action. See “10.1Testing the Line” for the type of test you want to specify.
3	Check whether the following statistical information is counted for the applicable port according to the failure statistical information of show interfaces command. If there is a count, 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 there is a count for the following item for the target port. If there is a count, 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 there is a count for the following item. If there is a count, 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 10GBASE-R problems

If a problem occurs in 10GBASE-R, separate the failure according to the following order.

1. Checking the log
   For information about the log, see "Message and 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.

Table3-4How to analyze faults in the event of 10GBASE-R troubles

No.	Items to check	Cause	Action
1	Use the show interfaces command to display the failure statistics, and check whether there is a count for the following item for the target port. If there is a count, 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 (for example, check for incomplete insertion). 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 functionality of the receiving side has no problem. Check the results of the no test interfaces command, and take the action described in Action. See “10.1Testing the Line” for the type of test you want to specify.
2	Use the show interfaces command to display the failure statistics for the receiving side, and check whether there are counts for the following items for the target port. If there is a count, 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 (for example, check for incomplete insertion). 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 functionality of the receiving side has no problem. Check the results of the no test interfaces command, and take the action described in Action. See “10.1Testing the Line” for the type of test you want to specify.
3	Use the show interfaces command to display the failure statistics, and check whether there is a count for the following item for the target port. If there is a count, 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 there is a count for the following item. If there is a count, 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 Actions to be taken for PoE problems

If a problem such as a disabled power supply unit occurs when PoE is used, isolate the cause of the problem according to the failure analysis method described in the following table.

Table3-5Communication failure analysis when using PoE

No.	Items to check and commands	Action
1	Use show power inline command. Check Status of the corresponding port.	・When Status is set to off Power is not being supplied. Go to Item 2. ・When Status is set to denied The supplied power is insufficient for the entire switch. Go to Item 4. ・When Status is set to faulty The power supply unit to the connected device is disabled. Go to Item 5. ・When Status is set to inact Power supply has been stopped by an operation command. Go to Item 5. ・When Status is set to wait The distributed PoE power supply function waits for power to be supplied. Wait until the waiting time is over.
2	Use show power inline command. Check Priority of the corresponding port.	・When Priority is set to never Use the configuration command power inline to set priorities other than never. ・When Priority is not never Go to Item 3.
3	Check that the configuration command shutdown is set for the corresponding port.	・If it has already been set Use the configuration command to set no shutdown. ・If not set Make sure a power-receiving device is connected.
4	Use show power inline command. Check Threshold (W) and Total Allocate (W).	Total Allocate (W) value is larger than Threshold (W) and cannot be supplied. Check the amount of power being supplied to the entire switch, the amount of power allocation to the ports, and the power consumption by the ports, and then adjust the allocation amount in the configuration.
5	Execute activate power inline command. Use show power inline to check Status of the corresponding port.	・When Status is set to off Make sure a power-receiving device is connected. ・When Status is set to on Continue to use. ・Status indication is faulty indication There might be a problem with the power-receiving device or a connection cable. Go to Item 6.
6	Execute show logging command. Check for	There might be a problem with the power-receiving device or a

No.	Items to check and commands	Action
	logging.	connection cable. ・When "Supplying power was stopped by the overload detection." is displayed Power cannot be supplied because an overload was detected. Check the power-receiving device or connection cables. If the problem cannot be corrected, check the cable length and cable type in the Hardware Instruction Manual, and replace the cables. If devices to which PoE power can be supplied are connected, use the power inline configuration command to disable PoE on the target port. ・When "Supplying power was stopped by the thermal shutdown." is displayed A thermal error was detected in PoE controller. Supplying power was stopped. Review the installation environment of the equipment and reconnect. If not, check the powered device or connection cable. ・When "Supplying power was stopped by the PD disorder" is displayed Power supply was stopped because a failure of the power receiving device was detected. Check the power-receiving device or connection cables.

3.2 Communication failures when 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.

Table3-6Communication 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 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 to check the operating 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 "3.1Ethernet communication failure”. ・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 operating 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 operating 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 operating 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 to check the statistics for the LACPDU. Also, check the operating 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 operating 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 operating 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 functionality is activated, and the channel group is down.

4 Troubleshooting layer 2 switching

This chapter describes the actions to be taken in the event of a Layer 2 switching failure.

4.1 VLAN communication failure

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 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 configured 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 is set in allowed vlan for trunk ports.
  - The port is specified as a mirror port.
- Is Web Authentication (Fixed VLAN Mode) or MAC Authentication (Fixed VLAN Mode) configured for a trunk port mixed with a VLAN that is not configured?

(b) For protocol VLANs

When you are using a protocol VLAN, execute the show vlan command and make sure the protocol has been configured 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) For MAC VLANs

- When you are using a MAC VLAN, execute the show vlan mac-vlan command and make sure 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 functionality used to register the MAC address.

  [Functionality]

  static: The MAC address is set in the configuration.
  dot1x: The MAC address is set by the IEEE 802.1X functionality.
  wa: MAC addresss by Web authorization.
  macauth: MAC addresss by MAC 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 the MAC address set for a VLAN by using the Layer 2 authentication functionality 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 and make sure the port status is Up. For Down status, refer to "3.1Ethernet communication failure".
- Make sure the port status is Forwarding. If it is Blocking, the cause is indicated in parentheses. Check the status of the functionality that caused the problem.

[Cause]

VLAN: Suspend is specified for the VLAN.

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

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

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

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 "4.4IGMP snooping communication failure" and "4.5MLD snooping communication failure".

When Dot1x is displayed for Type:

See "5.1Communication failure when using IEEE802.1X”.

When Wa is displayed for Type:

See "5.2Communication failure when using Web authorization”.

When Macauth is displayed for Type:

See "5.3Communication failure when using MAC authorization”.

- 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 functionality.

(4) Checking frame discard

The frames may have been discarded by filters or QoS. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

4.2 Spanning tree communication failure

If Layer 2 communication fails or the operating status of the Spanning Tree Protocol does not conform to the network configuration when the Spanning Tree functionality is used, use the analysis method described below to 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.

Table4-1 Spanning Tree Fault Analysis Methods

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 status of the protocol of the Spanning Tree Protocol.	If the displayed status is Enable, go to No. 2.
		For AX2630S 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 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 identifier of the root bridge for the Spanning Tree Protocol.	If the bridge identifier of the root bridge indicates the root bridge defined in the network configuration, go to No. 3.
		If the bridge identifier 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 applicable port is the root port and BPDU reception counters are counting up, go to Item 5.
		If the applicable port is the root port and BPDU reception counters have not counted up, check that BPDU has not been discarded by filtering or QoS. For details on how to confirm and how to respond, see "10.2Checking packet discard”. If you do not find any problems, check the neighboring devices.
		If the corresponding port is the specified port and BPDU transmit counters are counting up, go to Item 5.
		If the applicable port is the specified port and BPDU transmit counters have not counted up, see "3Troubleshooting a Network Interface".
5	Execute the show spanning-tree command with the detail parameter for the Spanning Tree Protocol that caused the failure, and then check the bridge identifier for the received BPDUs.	Make sure the root bridge identifier and sending bridge identifier for the received BPDUs are the same as those defined in the network configuration. If they are different from the network configuration, check the status of the neighboring devices.
6	Check whether the value for maximum number of Spanning Tree Protocols, one of	Set a value within the capacity limit. For details about capacity limits, see “Configuration Guide”.

No.	Items to check and commands	Action
	which caused the failure, is within the capacity limit.	
7	For AX2630S 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 Make sure that VLANs intended to be used in an MST instance are correctly 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.

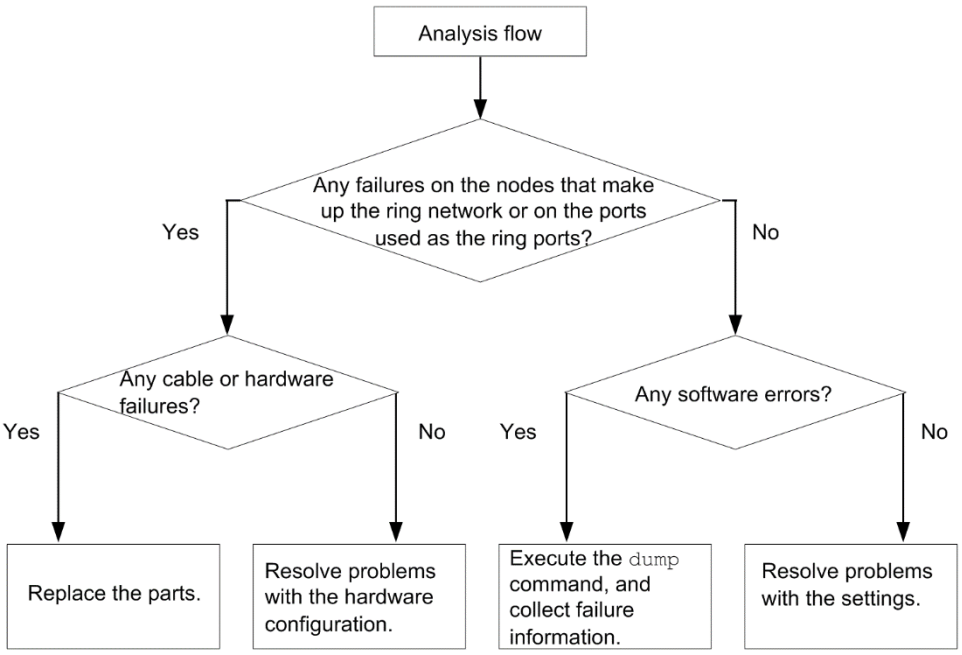
4.3 Ring Protocol communication failure

This section describes Autonomous Extensible Ring Protocol failures.

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.

Figure4-1 analysis flow



If the system does not operate normally during Ring Protocol operation, or if a ring network failure is detected, isolate the cause of the failure for all the nodes that comprise the ring network.

Table4-2How to analyze Ring Protocol for failures (for AX2630S)

No.	Items to check and commands	Action
1	Use the show axrp command to check the operating status of the Ring Protocol.	If "enable" is displayed in "Oper State", go to Item 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 functionality is not running. Check the configuration for any conflict (for example, an incorrect combination of the attribute and ring port for the operating mode of the Switch).
2	Use the show axrp command to check the operating mode and attribute.	If the "Mode" and "Attribute" are in the same operating mode and attributes as the network configuration, go to Item 3.
		If any other information is displayed, check the configuration.
3	Use the show axrp command to check the ring port and its status for each VLAN group.	If the contents of "Ring Port" and "Role/State" are set to the ports according to the network configuration, go to Item 4.
		If any other information is displayed, check the configuration.

No.	Items to check and commands	Action
4	Use the show axrp detail command to check the control VLAN ID.	If the content of "Control VLAN ID" is a VLAN ID according to the networking configuration, go to Item 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 to check the VLAN IDs that belong to the VLAN group.	If the content of "VLAN ID" is VLAN ID according to the networking configuration, go to Item 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 to check the timer value of the health-check frame sending interval and that of the health-check frame hold time.	If the timer value "Health Check Hold Time" of the protection time of the health check frame is greater than the timer value "Health Check Interval" of the transmission interval of the health check frame (the transmission delay is also considered), go to Item 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 the settings in the configuration.
7	Use the show vlan detail command to check the state of the VLAN used for the Ring Protocol and the VLAN port states.	If the status of VLAN and its ports is normal, go to Item 8. Also check Item 9 for configurations that use Spanning Tree Protocols, Item 10 for configurations that use the Multiple Failure Monitoring feature, and Item 13 for stacked configurations.
		If there is any anomaly, check the configuration and restore the states of the VLAN and its ports.
8	Check the setting of filters and QoS.	Filtering, or QoS, may discard the control frames used by Ring Protocol. For details on how to confirm and how to respond, see "10.2Checking packet discard”.
9	For a configuration that uses Spanning Tree Protocols together, 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 virtual linking is set on the switch that uses both Ring Protocol and Spanning Tree Protocols. ・On the entire ring network, check that VLAN used for the virtual link is set for Ring Protocol unit.
10	If the multi-fault monitoring functionality is applied, use the show axrp detail command to check the operating mode for the multi-fault monitoring functionality.	If "monitor-enable" is set for a shared node and "transport-only" is set for another device, go to Item 11.
		If any other information is displayed, check the configuration.
11	Use the show axrp detail command to check the backup ring IDs and VLAN IDs for the multi-fault monitoring functionality.	If "Backup Ring ID" and "Control VLAN ID" are set to the backup ring ID and multiple failure monitoring VLAN ID according to the network configuration, go to Item 12.
		If any other information is displayed, check the configuration.
12	Use the show axrp detail command to check the timer value of the multi-fault monitoring functionality frame sending interval and that of the hold time to determine that multiple faults have occurred when multi-fault monitoring frames are not received.	Make sure that the Multi Fault Detection Hold Time timer value is larger than the Multi Fault Detection Interval timer value (i.e., transmission delay is taken into account).
		If any other information is displayed, check the configuration.
13	For a stacked configuration, execute show	If packets are discarded, check whether the stack link bandwidth is

No.	Items to check and commands	Action
	qos queueing command. Check whether packets are discarded on the stack port.	sufficient 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 the stack link and adding the number of stack links.

Table4-3How to analyze Ring Protocol for failures (for AX2340S)

No.	Items to check and commands	Action
1	Use the show axrp command to check the operating status of the Ring Protocol.	If "enable" is displayed in "Oper State", go to Item 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 functionality is not running. Check the configuration for any inconsistencies.
2	Use the show axrp command to check the operating mode and attribute.	If the content of "Mode" is an attribute of the operation mode according to the network configuration, go to Item 3.
		If any other information is displayed, check the configuration.
3	Use the show axrp command to check the ring port and its status for each VLAN group.	If the contents of "Ring Port" and "Role/State" are set to the ports according to the network configuration, go to Item 4.
		If any other information is displayed, check the configuration.
4	Use the show axrp detail command to check the control VLAN ID.	If the content of "Control VLAN ID" is a VLAN ID according to the networking configuration, go to Item 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 to check the VLAN IDs that belong to the VLAN group.	If the content of "VLAN ID" is VLAN ID according to the networking configuration, go to Item 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 to check the state of the VLAN used for the Ring Protocol and the VLAN port states.	If the status of VLAN and its ports is normal, go to Item 7. Also check Item 8 for the configuration to which the multiple failure monitoring feature is applied.
		If there is any anomaly, check the configuration and restore the states of the VLAN and its ports.
7	Check the setting of filters and QoS.	Filtering, or QoS, may discard the control frames used by Ring Protocol. For details on how to confirm and how to respond, see "10.2Checking packet discard”.
8	If the multi-fault monitoring functionality is applied, use the show axrp detail command to check the operating mode for the multi-fault monitoring functionality.	If "transport-only" is set, go to Item 9.
		If any other information is displayed, check the configuration.
9	Execute show axrp detail command. Check VLAN ID for monitoring multiple failures.	If "Control VLAN ID" is VLAN ID for monitoring multiple failures in the network configuration, check the multiple failures monitoring unit of the shared node for the timer value of the frame transmission interval

No.	Items to check and commands	Action
		and the timer value of the protection time until multiple failures are determined without receiving the multiple failures monitoring frame.
		If any other information is displayed, check the configuration.

4.4 IGMP snooping communication failure

If multicast forwarding cannot be performed when IGMP snooping is used, use the following actions to identify the cause and isolate the cause.

(1) Checking the log

Use show logging command. Check for any physical faults. For information about the log contents, see Message Log Reference.

(2) Checking frame discard

Check that the control frames used by IGMP snooping have not been discarded by filters or QoS. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

(3) Checking IGMP Querier

Execute show igmp-snooping command. Check whether IGMP querier exists. If a IGMP querier exists, IGMP querying system: displays IP of the querier. If IGMP querier does not exist (IP is not displayed), take the following action.

- To set the Switch as IGMP querier, set VLAN to IP address. Then, set the configuration command ip igmp snooping querier in VLAN.
- If the other device is a IGMP querier, connect the device to the same VLAN.

(4) Checking the connections of devices that can forward multicast data

If a device capable of multicast data forwarding is connected to the same VLAN, execute show igmp-snooping command. Check that the connected port is displayed in "Mrouter-port:". If the connection port is not displayed, either set the connection port as a multicast router port or configure multicast router port auto-learning using the configuration command ip igmp snooping mrouter in the relevant VLAN. If you have already configured multicast router port auto-learning, check the multicast router connection.

(5) Checking the Subscribed Multicast Group Address

Execute show igmp-snooping group command. Check the subscription multicast group address. If the subscribing multicast group address is not displayed, check that the recipients are correctly connected to the same VLAN. If the subscribed multicast group address is displayed, check that the sender is correctly connected to the same VLAN.

4.5 MLD snooping communication failure

If multicast forwarding cannot be performed when MLD snooping is used, use the following actions to identify the cause and isolate the cause.

(1) Checking the log

Use show logging command. Check for any physical faults. For information about the log contents, see Message Log Reference.

(2) Checking frame discard

Check that the control frames used by MLD snooping have not been discarded by filters or QoS. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

(3) Checking MLD Querier

Execute show mld-snooping command. Check whether MLD querier exists. If a MLD querier exists, MLD querying system: displays IP of the querier. If MLD querier does not exist (IP is not displayed), take the following action.

- To set the Switch as MLD querier, set VLAN to IP address. Then, set the configuration command ipv6 mld snooping querier in VLAN.
- If the other device is a MLD querier, connect the device to the same VLAN.

(4) Checking the connections of devices that can forward multicast data

If a device capable of multicast data forwarding is connected to the same VLAN, execute show mld-snooping command. Check that the connected port is displayed in "Mrouter-port:". If the connection port is not displayed, use the configuration command ipv6 mld snooping mrouter to set the connection port as a multicast router port in the relevant VLAN.

(5) Checking the Subscribed Multicast Group Address

Execute show mld-snooping group command. Check the subscription multicast group address. If the subscribing multicast group address is not displayed, check that the recipients are correctly connected to the same VLAN. If the subscribed multicast group address is displayed, check that the sender is correctly connected to the same VLAN.

5 Troubleshooting Layer 2 authentication

This chapter describes the actions to be taken in the event of a Layer 2 authentication failure.

5.1 Communication failure when using IEEE802.1X

5.1.1 Problems When Using IEEE802.1X

If you cannot authenticate while using IEEE802.1X, use the failure analysis methods listed in the following tables to isolate the cause.

Table5-1 Authentication Fault Analysis Methods for IEEE802.1X

No.	Items to check and commands	Action
1	Use the show dot1x command to check the operating 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 make sure 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 RxInvalid or RxLenErr is not 0, an invalid EAPOL was received from the terminal. If an invalid EAPOL is received, it is logged. Use the show dot1x logging command to view the log. The Invalid EAPOL frame received message is also logged to describe the invalid EAPOL frame. If any of the above conditions exists, check the Supplicant setting on the terminal. If not applicable, go to Item 3.
3	Execute the show dot1x statistics command, and make sure data has been sent to the RADIUS server.	If the value displayed for TxNoNakRsp under [EAPoverRADIUS frames] is 0, no data has been sent to the RADIUS server. Check the following: ・Check that aaa authentication dot1x default group radius is set by using the configuration command. ・Check that the configuration command dot1x radius-server host or radius-server host is set correctly. If not applicable, go to Item 4.
4	Execute the show dot1x statistics command, and make sure 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 RADIUS server is contained in a remote network, check that a route to the remote network exists. ・Make sure that RADIUS servers are not authenticated. If not applicable, go to Item 5.
5	Execute the show dot1x logging command, and check data exchange with the RADIUS server.	・"Invalid EAP over RADIUS frames received" indicates that an illegal packet was received from RADIUS servers. Check whether the RADIUS server is running normally. ・If there is a Failed to connect to RADIUS server, connecting to RADIUS servers has failed. Check whether the RADIUS server is running normally. If not applicable, go to Item 6.
6	Check the authentication-only access list setting.	・When performing a specific packet communication from a terminal in the pre-authentication state outside the Switch, make sure that an authentication-only access list is set. ・If not applicable, go to Item 7.
7	Execute the show dot1x logging command, and check whether authentication failed.	・If there is “New Supplicant Auth Fail.”, authentication has failed due to the following factors: Check for problems. (1)The user ID or password has not been registered on the authentication server.

No.	Items to check and commands	Action
		(2)The user ID or password is entered incorrectly. ・If there is a The number of supplicants on the switch is full, the device has exceeded its max supplicant count, and authorization has failed. ・If there is a The number of supplicants on the interface is full, the authorization has failed because the max supplicant count on the interfaces has been exceeded. ・If there is a Failed to authenticate the supplicant because it could not be registered to mac-address-table., the authorization was successful, but H/W failed to set MAC address table. Refer to the relevant section in "Message and Log Reference" and follow the instructions in [Action]. If none of the above apply, see the RADIUS server log to check whether authentication has failed.

5.1.2 Checking IEEE802.1X configuration

Check the following for the configuration related to IEEE802.1X.

Table5-2Checking the configuration of I EEE802.1X

No.	Items to check	Items to check
1	IEEE802.1X configuration settings.	Make sure 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	Verify Authentication Only Access List Settings	Make sure that the filtering criteria required for communication from a terminal in the pre-authentication status to an external device are set correctly in the configuration command authentication ip access-group and ip access-list extended, or authentication mac access-group and mac access-list extended.

5.2 Communication failure when using Web authorization

5.2.1 Problems When Using Web authentication

Use the following tables to isolate problems when using Web authentication.

Table5-3 Fault Analysis Methods for Web authentication

No.	Items to check and commands	Action
1	Check whether the login page appears on the terminal.	・If the login screen and logout screen are not displayed, go to Item 2. ・If the login screen is displayed using the local authentication method, go to Item 5. ・If the login page is displayed using RADIUS authentication method, go to Item 7. ・If an operation message is displayed, go to Item 14.
2	Check whether the URLs specified for login and logout are correct.	・If URL for logging in and logging out is incorrect, use the correct URL. ・If the login screen and logout screen are not displayed in fixed VLAN mode or dynamic VLAN mode, check the following settings and set them correctly. ・Check whether Web authentication-only IP is set in the configuration command web-authentication ip address or whether URL redirection is enabled in the configuration command web-authentication redirect enable. ・If not applicable, go to Item 3.
3	Make sure that the Web server is running.	・Verify that Web servers are running by running the following command: 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 Web servers are not running, check the configuration command web-authentication web-port. ・If Web authentication configuration command is set correctly, restart Web servers using restart web-authentication web-server command. ・If Web server does not start even after the above operation, stop Web authentication using the configuration command no web-authentication system-auth-control, and after about 10 seconds, start Web authentication using the configuration command web-authentication system-auth-control.
4	Check the authentication-only access list setting.	・When performing a specific packet communication from a terminal in the pre-authentication state outside the Switch, make sure that an authentication-only access list is set. ・Make sure that the filtering criteria for the authentication-only IPv4 access list does not have an address that includes Web authentication-only IP address. ・If not applicable, go to Item 9.
5	Use the show web-authentication user command to check whether the user ID is registered.	・If the user ID is not registered, use set web-authentication user command. Register the user ID, password and VLAN ID. ・If not applicable, go to Item 6.
6	Check whether the entered password is correct.	・If the passwords do not match, use set web-authentication passwd command to change the passwords, or use remove web-authentication user command to delete the user ID, and then use set web-authentication user command to register the user ID, password and VLAN ID again. ・If not applicable, go to Item 9.

No.	Items to check and commands	Action
7	Use the show web-authentication statistics command to check the communication status with the RADIUS server.	・When the value of "TxTotal" of the displayed item "[RADIUS frames]" is "0", check that aaa authentication web-authentication default group radius and web-authentication radius-server host (or radius-server host) of the configuration command are set correctly. ・Even if dead interval function is used to restore RADIUS server from a non-responsive status to a communicating status, authentication radius-server dead-interval of the configuration command is not verified with RADIUS server, resulting in an authentication error. 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 operation by the first RADIUS server resumes. ・If not applicable, go to Item 8.
8	Check whether the password and user ID are registered on the RADIUS server.	・If the user ID is not registered, register it in RADIUS servers. ・If not applicable, go to Item 9.
9	Use the show web-authentication statistics command to check whether Web authentication statistics are displayed.	・If statistics of Web authentication are not displayed, go to Item 10. ・If not applicable, go to Item 11.
10	Check whether the web-authentication system-auth-control configuration command has been set.	・If the configuration command web-authentication system-auth-control is not set, set it. ・If not applicable, go to Item 11.
11	Execute the show web-authentication logging command and check for operation problems.	・If the authentication information for the port to which the authentication terminal is connected is not displayed in the fixed VLAN mode, check if the authentication target port is set correctly in the configuration command web-authentication port. Also, make sure that the authenticating port to which the terminal is connected is neither in the link-down status nor is shut down. ・If not applicable, go to Item 13.
12	If no account is recorded on the accounting server, use the show web-authentication statistics command to check the communication status with the accounting server.	・When the value of "TxTotal" of the displayed item "[Account frames]" is "0", check that aaa accounting web-authentication default start-stop group radius and web-authentication radius-server host (or radius-server host) of the configuration command are set correctly. ・If the above does not apply, check Web authentication configuration.
13	Check whether authentication fails on the connected terminal.	・If the authenticated terminal cannot be authenticated at all, use restart web-authentication web-server command to restart Web servers. ・If you cannot authenticate even after restarting Web servers, execute restart vlan mac-manager command. ・If the above does not apply, check Web authentication configuration and set the correct configuration.
14	Use the show logging command to check the operation log.	・If the following actions are taken, Web server (httpd) shutdown message and Web server (httpd) restart message may 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) When Web servers are restarted using restart web-authentication web-server command.・

No.	Items to check and commands	Action
		Web server (httpd) stop message: Level: E7 Message identifier: 2a001000 Message: httpd aborted. Web server (httpd) restart message: Level: R7 Message identifier: 2a001000 Message: httpd restarted. These messages indicate that the Web server (httpd) stopped and then automatically restarted. After the Web server (httpd) restarts, the authentication operation resumes. ・If not, see "Message and Log Reference" section.

5.2.2 Confirm Web Authentication Configuration

Check the following for the configuration related to Web authentication.

Table5-4 Checking the Configuration of Web authentication

No.	Items to check	Items to check
1	Check the Web authentication configuration settings.	Make sure 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 Configuration for dynamic VLAN mode: ・web-authentication auto-logout ・web-authentication max-timer ・web-authentication max-user Configuration for fixed VLAN mode: ・web-authentication ip address ・web-authentication port ・web-authentication static-vlan max-user ・web-authentication web-port In addition, check the settings of the following commands. ・web-authentication redirect enable ・web-authentication redirect-mode
2	Check the IP address settings for the VLAN interfaces.	For dynamic VLAN mode, make sure the IP addresses for the following VLAN interfaces are set correctly: ・Pre-certification VLAN ・Post-authentication VLAN
3	Verify Authentication Only Access List Settings	Make sure that the filtering criteria required for communication from a terminal in the pre-authentication status to an external device are set correctly in the configuration command authentication ip access-group and ip access-list extended, or authentication mac access-group and mac access-list extended.
4	Check the ARP relay configuration.	In fixed VLAN mode or dynamic VLAN mode, check whether the configuration command authentication arp-relay for communicating ARP packets from a terminal in the pre-authentication status to a device outside the Switch is set correctly. Note that ARP relay setting is not required if the authentication-only MAC access list is set to allow ARP packets from the pre-authentication terminal to pass.

5.2.3 Checking accounting for Web authentication

Check the following for the accounting of Web authentication.

Table5-5Checking Accounting for Web Authentication

No.	Items to check	Items to check
1	Check whether authentication result account logs have been correctly recorded.	・If the authentication status is not displayed when show web-authentication login command is executed, execute "Table5-3 Fault Analysis Methods for Web authentication". ・If it is not recorded on the accounting server, go to item 2. ・If it is not recorded on syslog server, go to Item 3.
2	Use the show web-authentication statistics command to check the communication status with the accounting server.	・If the value of "TxTotal" of the displayed items "[Account frames]" is "0", check that the configuration command aaa accounting web-authentication default start-stop group radius,web-authentication radius-server host (or radius-server host) is set correctly. ・If the above does not apply, check Web authentication configuration.
3	Check the syslog server configuration.	Make sure the following configuration commands have been set correctly. ・Make sure that syslog servers are configured in logging host. ・Make sure that aut is set for the event type in logging event-kind. ・Make sure that web-authentication logging enable is set.

5.2.4 Problems with SSL Servers Certificates and Private Key Operation

Use the following tables to isolate failures related to the operation of SSL server certificates and private keys.

Table5-6Fault analysis methods for SSL server certificate and private key operation

No.	Problem	Items to check and commands	Response method
1	The server certificate and private key registered in the authentication terminal cannot be checked.	Run ps-axuw | grep httpd command. Check the startup time of Web servers (httpd).	If the startup time of Web server (httpd) is older than the time when the server certificate and private key are registered, restart Web server with restart web-authentication web-server command.
2	Unable to authenticate after registering the server certificate and private key.	Execute ps-axuw | grep httpd command. Check whether Web servers (httpd) are running.	If Web server (httpd) is not running, the pairing of the server certificate and private key is incorrect. Use the following procedure to register the correct combination of the server certificate and private key. 1. Deletes the certificate and private key registered by clear web-authentication ssl-crt command will. 2. Restart Web servers with restart web-authentication web-server command will. 3. Specify the correct server certificate and private key with set web-authentication ssl-crt command register. 4. Restart Web servers again with restart web-authentication web-server command.
3	After registering the server certificate and private key, restart Web server repeatedly.	Check that the restart message is displayed.	If Web server (httpd) restarts repeatedly, take the same action as in item 2.
4	I registered using the server certificate and private key created by	In openssl creation process, confirm that there are no	・Confirm whether the operation is as described in "Configuration Guide". ・If the procedure is followed, perform the check contents and

No.	Problem	Items to check and commands	Response method
	openssl command. However, I cannot authenticate.	disconnections or incorrect settings.	corrective actions in item 1.
5	Parameter cannot be specified by openssl command will.	Use openssl version command. Check the version of openssl.	Use a version of openssl 1.0.2 or later.

5.3 Communication failure when using MAC authorization

5.3.1 Problems When Using MAC Authorization

Use the following tables to isolate problems when using MAC authorization.

Table5-7 Fault Analysis Methods for MAC-based authentication

No.	Items to check and commands	Action
1	Check whether communication with the terminal is possible.	・If the local authentication method cannot be used, go to item 2. ・If authentication is not possible with RADIUS authentication method, go to Item 3. ・If not applicable, go to Item 5.
2	Use the show mac-authentication mac-address command to make sure the MAC address and VLAN ID are registered.	・If MAC address is not registered, use set mac-authentication mac-address command to register MAC address and VLAN ID. ・If not applicable, go to Item 5.
3	Use the show mac-authentication statistics command to check the communication status with the RADIUS server.	・If the value of "TxTotal" of the displayed items "[RADIUS frames]" is "0", check that the configuration command aaa authentication mac-authentication default group radius,mac-authentication radius-server host (or radius-server host) is set correctly. ・Even if dead interval function is used to restore RADIUS server from a non-responsive status to a communicating status, authentication radius-server dead-interval of the configuration command is not verified with RADIUS server, resulting in an authentication error. 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 operation by the first RADIUS server resumes. ・If not applicable, go to Item 4.
4	Check whether the MAC address and password are registered on the RADIUS server.	・Register in RADIUS server if the user ID of MAC server is not registered. ・If MAC address is used as the password, set the same address as MAC address set in the user ID. ・If the same password is set for RADIUS servers, check that the password matches the password set in the configuration command mac-authentication password. ・If not applicable, go to Item 5.
5	Check the authentication-only access list setting.	・When performing a specific packet communication from a terminal in the pre-authentication state outside the Switch, make sure that an authentication-only access list is set. ・If not applicable, go to Item 6.
6	Use the show mac-authentication statistics command to check whether the MAC-based authentication statistics are displayed.	・If statistics of MAC-based authentication are not displayed, go to Item 7. ・If not applicable, go to Item 8.
7	Check whether the mac-authentication system-auth-control configuration command has been set.	・If the configuration command mac-authentication system-auth-control is not set, set it. ・Check that the port to be authenticated is set correctly in the configuration command mac-authentication port.

No.	Items to check and commands	Action
		・Make sure that the authenticated port to which the terminal is connected is not linked down or shut down. ・If not applicable, go to Item 8.
8	Execute the show mac-authentication logging command and check for operation problems.	・If the maximum capacity limit has been reached, wait until another terminal is deactivated. ・If the above does not apply, check MAC certification configuration.

5.3.2 Confirm MAC-based Authentication Configuration

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

Table5-8 Checking the Configuration of MAC-based authentication

No.	Items to check	Items to check
1	Check the MAC-based authentication configuration settings.	Make sure 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	Verify Authentication Only Access List Settings	Make sure that the filtering criteria required for communication from a terminal in the pre-authentication status to an external device are set correctly in the configuration command authentication ip access-group and ip access-list extended, or authentication mac access-group and mac access-list extended.

5.3.3 Checking accounting for MAC-based authentication

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

Table5-9 Checking Accounting for MAC-based authentication

No.	Items to check	Items to check
1	Check whether authentication result account logs have been correctly recorded.	・If the authentication status is not displayed on show mac-authentication login, execute "Table5-7 Fault Analysis Methods for MAC-based authentication". ・If it is not recorded on the accounting server, go to item 2. ・If it is not recorded on syslog server, go to Item 3.
2	Use the show mac-authentication statistics command to check the communication status with the accounting server.	・If the value of "TxTotal" of the displayed items "[Account frames]" is "0", check that the configuration command aaa accounting mac-authentication default start-stop group radius,mac-authentication radius-server host (or radius-server host) is set correctly. ・If the above does not apply, check MAC-based authentication configuration.
3	Check the syslog server configuration.	Make sure the following configuration commands have been set correctly. ・Make sure that syslog servers are configured in logging host. ・Make sure that aut is set for the event type in logging event-kind. ・Make sure that mac-authentication logging enable is set.

6 Troubleshooting High Reliability Functions

This chapter describes the actions to be taken in the event of a failure in the High Reliability feature.

6.1 Uplink redundant communication failure

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.

Table6-1 Uplink Redundant Fault Analysis Methods

No.	Items to check and commands	Action
1	Execute the show switchport-backup command, and make sure that the states 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 it is a Blocking, the Active Port Locking feature may be running. Execute the show switchport-backup command, and check whether active port locking is operating. If active port locking is operating, wait a while until the primary port is linked up. Alternatively, use the set switchport-backup active command to activate the secondary port. ・For Down, check the line status. Refer to "3.1Ethernet communication failure " for the check method.
		If there is no problem with the Forwarding or Blocking state 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 functionality, check whether the MAC address update functionality is enabled on the device that uses the uplink redundancy. The MAC address update functionality 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 functionality, 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 make sure 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 IP Communication

This section describes the actions to be taken in the event of a communication failure on IP network.

7.1 IPv4 networking communication failure

7.1.1 Cannot communicate or is disconnected

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

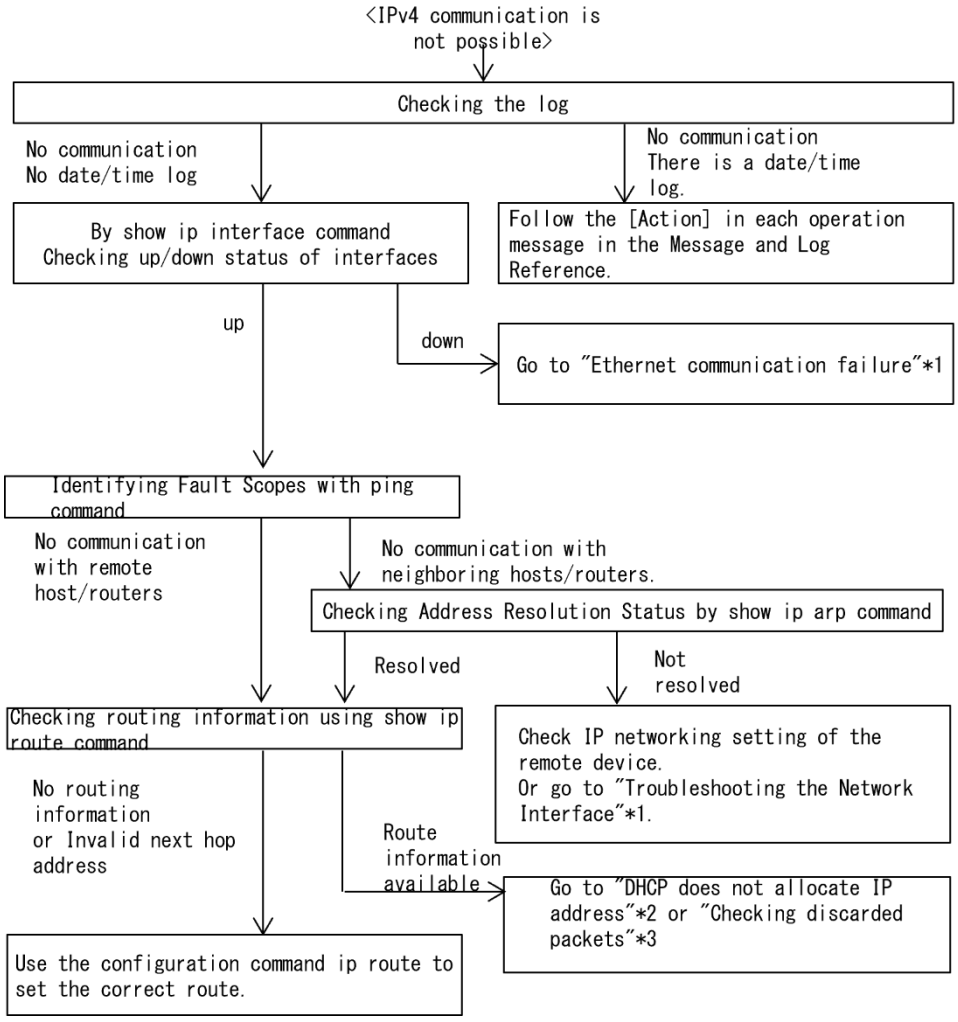
1. A configuration related to IP communication is changed.
2. The network configuration is changed.
3. A network device fails.

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 determine 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 for operation that hitherto has been normal, IP communication is no longer possible.

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

Figure7-1 Fault analysis when IPv4 communication is not possible



*1 For details, see "3.1Ethernet communication failure ".

*2 For details, see "7.1.2DHCP Does Not Assign IP Addresses”.

*3 For details, see "10.2Checking packet discard”.

(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 log contents, see the Message and 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. Details of the log failures that are displayed at the time of communication failure and responses to the failures are described in the Message Log Reference. and then follow the instructions given in the manual.
5. If the log is not displayed when communication is no longer possible, go to "(2)Checking the interface status”.

(2) Checking the interface status

Even when the Switch hardware is operating normally, a fault 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 to check whether the status of the interface with the target neighboring device is Up or Down.
3. If the applicable interface is in the "Down" status, see "3.1Ethernet communication failure".
4. Proceed to "(3)Specifying the range of failures (when implemented from the Switch)" when the interface with the corresponding interface is in "Up" status.

(3) Specifying the range of failures (when implemented 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 to check the communication with the two remote devices that are unable to communicate. For examples of ping commands and how to read the results, see the Configuration Guide.
3. If communication with the remote devices cannot be verified by the ping command, execute the command again to check communication with each of the devices up to the remote device, beginning with the device closest to the Switch.
4. After executing ping command, proceed to "(5)Checking ARP resolution with neighboring devices" if the failure range is a neighboring device, and to "(6)Checking route information" if the failure range is a remote destination device.

(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 the customer's terminal has the ping functionality.
2. Use the ping functionality to check whether communication between the customer's terminal and the remote device is possible.
3. If communication with the remote device cannot be verified by using the ping functionality, use the ping command to check communication with each of the devices up to the remote device, beginning with the device closest to the customer's terminal.
4. If you are able to determine the range for the failure by using the ping functionality 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 ARP resolution with neighboring devices

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 to 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 is resolved (ARP entry data is available), proceed to "(6)Checking route 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 instructions, see”8.1DHCP snooping problems”.

(6) Checking route information

If communication is not possible even though the address with the neighboring device has been resolved, or if communication with the other party becomes impossible due to a route in the middle of communication with IPv4 unicast communication, or if the route to the other party of communication is incorrect, you need to check the routing information held by the Switch. To carry out the check, do the following:

1. Log in to the Switch.
2. Execute show ip route command. Check the routing information that is retained by the Switch.
3. If the routing information held by the Switch does not include routing information for the destination that is causing a communication error, or if the next hop address is invalid, use the configuration command ip route to set the correct routing information.
4. If the routing information held by the Switch includes routing information to a destination that is causing a communication failure, the following functions that are set for the sending/receiving interface to the destination that cannot be used for communication may be defective: That functionality must be checked.
   - DHCP Server Functionality
     Proceed to "(7)Checking DHCP Servers Configuration".
   - Filters, QoS,, or DHCP snooping
     Proceed to "(8)Checking packet discard".

(7) Checking DHCP Servers Configuration

If IP addresses are allocated to neighboring devices by DHCP server function of the Switch, IP addresses may not be

allocated appropriately.

Review whether the settings for DHCP servers in the configuration are correct. For instructions, see”7.1.2DHCP Does Not Assign IP Addresses”.

(8) Checking packet discard

Filters or QoS may be dropping packets. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

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 instructions, see”8.1DHCP snooping problems”.

7.1.2 DHCP Does Not Assign IP Addresses

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 the above item 1. The following describes an example of an easy-to-mistake configuration setting. 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/server settings (network card settings, cable connections, etc.) have been verified, and the case is as shown in 3. above: "The configuration and network configuration are correct, but the IP address is not assigned to the client and the IP communication is not successful", refer to " (2) Confirming operation messages and interfaces" to see if a failure has occurred on the Switch. If there is no error in the Switch, see "(3)Specifying the range of failures (when implemented 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 there is an ip dhcp pool setting that contains the network setting for the DHCP addresses to be assigned to the DHCP clients.
2. In the configuration, make sure the number of IP 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. Check that the router address (default router) of the network to which the client is connected is set in the configuration command default-router (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 instructions, see”8.1DHCP snooping problems”.

(2) Confirming operation messages and interfaces

One probable cause of disabled assignment of IP addresses to clients is that communication between the client and the server has been disabled. Check up/down status of the interfaces using the operation messages or show ip interface commands displayed by the Switch. See “7.1.1Cannot communicate or is disconnected” for instructions.

(3) Specifying the range of failures (when implemented from the Switch)

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

1. Log in to the Switch.
2. Use show ip route commandto check the routing information. If you are going through DHCP relays, make sure that the client-facing route is correctly registered. In addition, use ping commands to check communication with routers that are operating as DHCP relays.
3. If the server and the client are directly connected, check the hub and cable connections.

(4) Checking packet discard

Filters or QoS may be dropping packets. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

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 instructions, see”8.1DHCP snooping problems”.

(5) Checking the Layer 2 network

If the steps (1) through (4) do not identify any misconfigurations or faults, there may be a Layer 2 network problem. Check the Layer 2 network referring to "4Troubleshooting layer 2 switching".

7.1.3 DynamicDNS linkage of DHCP servers does not work

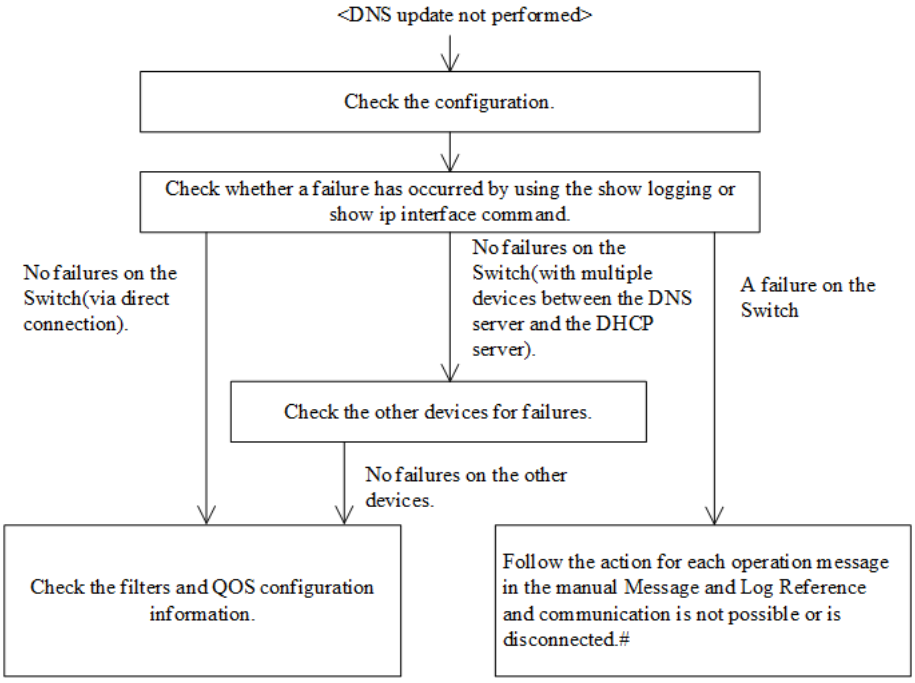
There are three probable causes for communication problems on a DHCP server:

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

First, check the above item 1. The following describes an example of an easy-to-mistake configuration setting. 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 settings of DNS server /DHCP server (network card settings, cable connections, etc.) have been verified, for the case that "DynamicDNS linkage does not work even though the configuration and network configuration is correct" shown in 3. above, refer to "(2)Checking the time information”~"(5)Checking packet discard” for details.

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

Figure7-2 DNS linkage DHCP servers failure analysis



Note * Refer to "7.1.1Cannot communicate 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 authentication key specified on DNS server and the key information set in DHCP server configuration are the same (see "Configuration Command Reference").
3. Make sure that the zone information specified on DNS server side matches the zone information in 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 configured (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. When distributing the domain name by DHCP, confirm that it is correctly set 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 show clock command to check the time information of the Switch, and if required, synchronize the time information by referring to the Configuration Command Reference.

(3) Confirming operation messages and interfaces

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 up/down status of the interfaces using the operation messages or show ip interface commands displayed by the Switch. See “7.1.1Cannot communicate or is disconnected” for instructions.

(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. Use show ip route commandto check the routing information. If DNS server is connected to a remote network, make sure that the route to DNS server is correctly registered.
3. If there are devices such as a router between the DNS server and the DHCP server, use the ping command to check the communication between the router and the remote device (DNS server). If the communication with the remote device cannot be verified by using the ping command, execute the ping command again to check communication with each of the devices up to the client, beginning with the device closest to the Switch. For examples of ping commands and how to read the results, see the Configuration Guide.
3. If the DNS server and the DHCP server are directly connected, check the hub and cable connections.

(5) Checking packet discard

Filters or QoS may be dropping packets. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

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 instructions, see” 8.1DHCP snooping problems”.

(6) Checking the Layer 2 network

If the steps (1) through (5) do not identify any misconfigurations or faults, there may be a Layer 2 network problem. Check the Layer 2 network referring to "4Troubleshooting layer 2 switching".

7.2 IPv6 networking communication failure

7.2.1 Cannot communicate or is disconnected

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

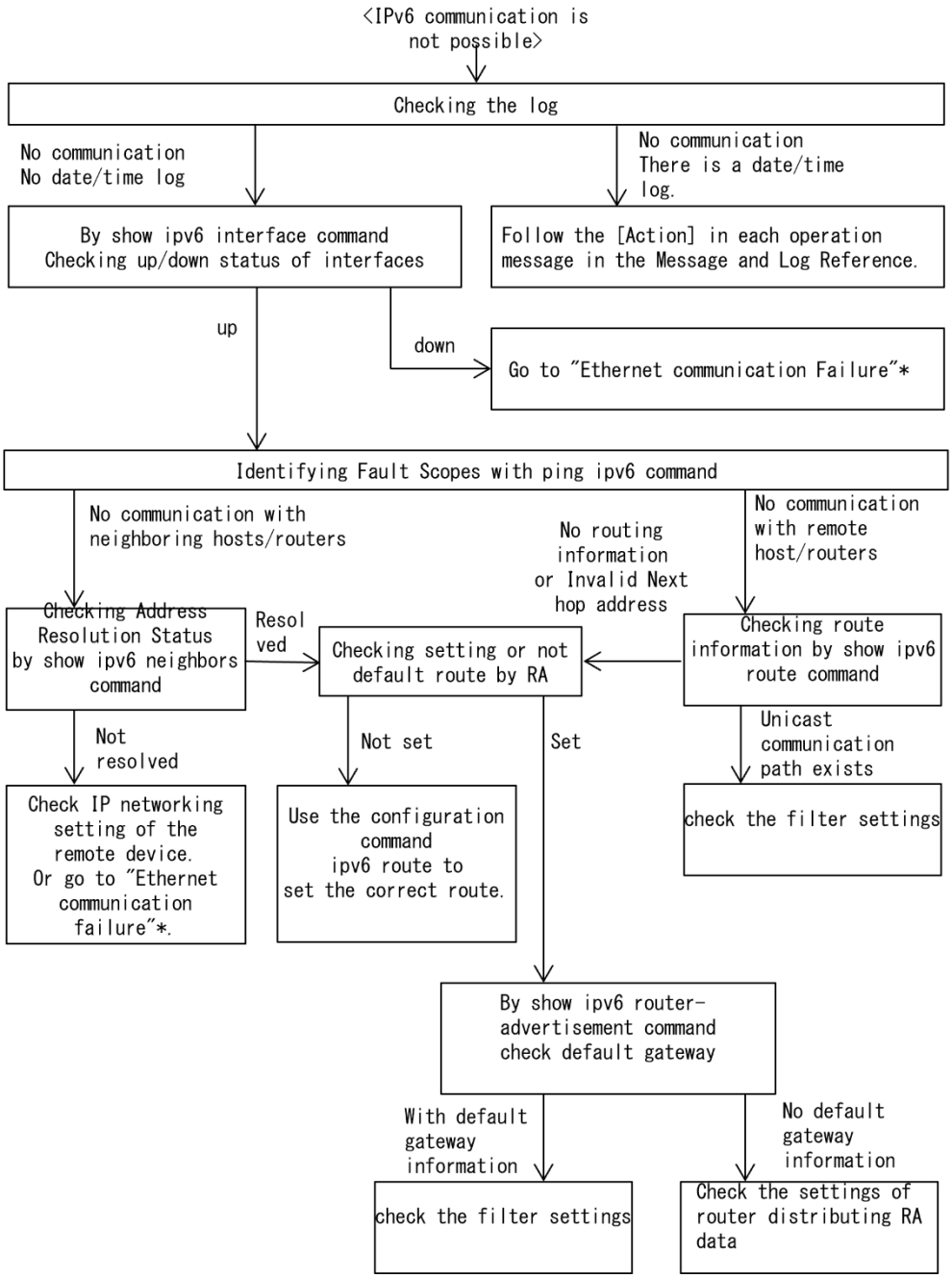
1. A configuration related to IPv6 communication is changed.
2. The network configuration is changed.
3. A network device fails.

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 for operation that hitherto has been normal, IPv6 communication is no longer possible.

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

Figure7-3 Fault analysis when IPv6 communication is not possible



Note * Refer to "3.1Ethernet communication failure ".

(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 log contents, see the Message and 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. Details of the log failures that are displayed at the time of communication failure and responses to the failures are described in the Message Log Reference. and then follow the instructions given in the manual.
5. If the log is not displayed when communication is no longer possible, go to "(2)Checking the interface status”.

(2) Checking the interface status

Even when the Switch hardware is operating normally, a fault 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 to check whether the status of the interface with the target neighboring device is Up or Down.
3. If the applicable interface is in the "Down" status, see "3.1Ethernet communication failure".
4. Proceed to "(3)Specifying the range of failures (when implemented from the Switch)" when the interface with the corresponding interface is in "Up" status.

(3) Specifying the range of failures (when implemented 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 to check the communication with the two remote devices that are unable to communicate. For examples of ping ipv6 commands and how to read the results, see the Configuration Guide.
3. If communication with the remote devices cannot be verified by the ping ipv6 command, execute the command again to check communication with each of the devices up to the remote device, beginning with the device closest to the Switch.
4. After executing ping ipv6 command, proceed to "(5)Checking NDP resolution with neighboring devices" if the failure range is a neighboring device, and to "(6)Checking unicast interface information" if the failure range is a remote destination device.

(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 the customer's terminal has the ping ipv6 functionality.
2. Use the ping ipv6 functionality to check whether communication between the customer's terminal and the remote device is possible.
3. If communication with the remote device cannot be verified by using the ping ipv6 functionality, use the ping ipv6 command to check communication with each of the devices up to the remote device, beginning with the device closest to the customer's terminal.
4. If you are able to determine the range for the failure by using the ping ipv6 functionality 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 NDP resolution with neighboring devices

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 to 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 is resolved (NDP entry data is available), proceed to "(7)RA confirmation of 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 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 to check the routing information obtained by the Switch.
3. If the routing information acquired by the Switch does not include routing information for the interface resulting in a communication failure, or if the next hop address is invalid, proceed to "(7)RA confirmation of information".
4. If the routing information held by the Switch includes routing information to a destination that is causing a communication failure, the following functions that are set for the sending/receiving interface to the destination that cannot be used for communication may be defective: That functionality must be checked.
   - Filtering or QoS functions
     Proceed to "(8)Checking packet discard".

(7) RA confirmation of information

1. Log in to the Switch.
2. Check that the configuration command ipv6 nd accept-ra default-gateway is set for the interface to be communicated.
3. If the configuration command ipv6 nd accept-ra default-gateway is not set, use the configuration command ipv6 route to set the correct route.
4. If the configuration command ipv6 nd accept-ra default-gateway is set, execute 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 held by the Switch includes routing information to a destination that is causing a communication failure, the following functions that are set for the sending/receiving interface to the destination that cannot be used for communication may be defective: That functionality must be checked.
   - Filtering or QoS functions
     Proceed to "(8)Checking packet discard".

(8) Checking packet discard

Filters or QoS may be dropping packets. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

8 Troubleshooting by Function

This chapter explains how to remedy problems that occur with each function.

8.1 DHCP snooping problems

8.1.1 DHCP Problems

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.

Table8-1 Fault analysis when IP addressing of DHCP cannot be distributed in 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 to check the operation 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 DHCP servers are operating properly.	Make sure that DHCP servers are ready to 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.	Packets forwarded via DHCP relay are discarded because the client hardware address and the source MAC address in the packets are different. To forward those packets, set the no ip dhcp snooping verify mac-address configuration command.
7	If packets that contain the relay agent information option are forwarded, make sure that the ip dhcp snooping information option allow-untrusted configuration command is set.	By default, packets that contain the relay agent information option (Option 82) are discarded. To forward those packets, set the ip dhcp snooping information option allow-untrusted configuration command.
8	Make sure 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.

No.	Items to check	Action
9	Use the show ip dhcp snooping binding command to check the binding information.	If the IP address cannot be updated after the device restarts, check the save status of the binding database. See "8.1.2Binding Database Storage Problems”.
		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	Other cases	If any of the above actions do not resolve your problem, check other functionality used in the device according to this manual.

8.1.2 Binding Database Storage Problems

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.

Table8-2 Fault analysis methods for binding database storage problems

No.	Items to check	Action
1	Use the show mc or show flash command to 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 no problem is found, go to Item 4.
4	Check the setting of the ip dhcp snooping database write-delay configuration command. Also, execute the show ip dhcp snooping binding command to 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 no problem is found, go to Item 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 no problem is found, go to Item 6.
6	Other cases	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.

Table8-3How to Analyze Problems Caused by Dynamic ARP Checks

No.	Items to check	Action
1	Check the DHCP snooping configuration.	See “8.1.1DHCP Problems” to verify that DHCP snooping is working properly.
		If there is no problem, go to No. 2.
2	Execute the show ip arp inspection statistics command to check the operation 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	Other cases	If any of the above actions do not resolve your problem, check other functionality 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.

Table8-4Fault analysis method of trouble caused by terminal filter

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

8.2 Policy-Based Mirroring Problems

8.2.1 Not Mirrored

If the target flow is not mirrored while using policy-based mirroring, use the failure analysis methods listed in the following table to isolate the cause.

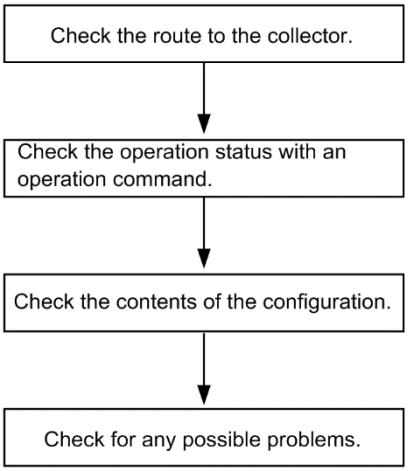
Table8-5 Fault analysis method when the target flow is not mirrored

No.	Items to check and commands	Action
1	Confirm in the configuration that the access list for which the destination interface list for policy-based mirroring is specified for operation is set. ・show running-config	If an access list for which the destination interface list for policy-based mirroring is specified for operation is not set, modify the configuration.
		If an access list for which the destination interface list for policy-based mirroring is specified for operation is set, go to step 2.
2	Make sure that the flow detection mode is set to a policy-based mirroring-enabled mode. ・show system	If Flow detection mode is not in policy-based mirroring-enabled mode, modify the configuration.
		If the number of entries for the target access list type in Used resources for Mirror inbound(Used/Max) is not subject to flow detection mode, correct the configuration.
		If an appropriate flow detection mode has been set, go to Item 3.
3	Use Matched packets to check the frame count that matches the access list for which the destination interface list for policy-based mirroring is specified for operation. ・show access-filter	If the target frame count for policy-based mirroring differs from Matched packets, the access list might be incorrectly configured. Please review the configuration.
		If the target frame count for policy-based mirroring matches Matched packets value. Or, if the access list settings are correct as a result of reviewing the configuration, go to Item 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 Item 5.
5	Check the status of the mirror port. ・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 not Up, set the channel group status to Up.
		If not applicable, go to Item 6.
6	Check the status of the monitor port. ・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 show vlan detail command. Check that the status of the target VLAN is Up and that the data transfer status of the monitor port is Forwarding.
		If the status of the monitor port is normal, go to Item 7.
7	Check whether the target frame has been discarded by the sending-side filters or QoS.	For details on how to confirm and how to respond, see "10.2Checking packet discard”.

8.3 sFlow statistical problems

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

Figure8-1 sFlow Statistical Function Troubleshooting Flow



8.3.1 sFlow Packets Not Reaching Collectors

(1) Checking the route to the collector

See "7.1.1Cannot communicate or is disconnected " and "7.2.1Cannot communicate or is disconnected " to make sure that the network is properly 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 operation

Execute the show sflow command a few times to display the sFlow statistics, and check whether the sFlow statistics functionality is running. If the underlined values are not increasing, see ”(3)Verifying the configuration”. If it is increasing, see "7.1.1Cannot communicate or is disconnected”,”7.2.1Cannot communicate or is disconnected " and "(5)Checking the settings on the collector side " to make sure that the network is properly connected to the collector.

Figure8-2 Sample show sflow Command-View

```
> 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) Verifying 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.

Figure8-3 Configuration Display Example 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. The 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.

Figure8-4 Configuration Display Example 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. The appropriate sampling interval is set.

Figure8-5 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.

Figure8-6 Configuration Display Example 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" is set here.

- Make sure that the filters or QoS do not discard sFlow for the physical ports on which the flow statistics are performed. For details on how to confirm and how to respond, see "10.2Checking packet discard".
- 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.

Figure8-7 Configuration Display Example 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. This is IP address assigned to the port of the Switch.

(4) Checking the port status

Execute the show interfaces command, and make sure 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 (normal operation).

Figure8-8 Example of Port Status Display

```
> 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 that the underlined part is "active up".

If the port is DOWN, see “7.1.1Cannot communicate or is disconnected” and “7.2.1Cannot communicate or is disconnected”.

(5) Checking the settings on the collector side

- 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 configured correctly.

8.3.2 Flow samples cannot be sent to the collector

If “8.3.1 sFlow Packets Not Reaching Collectors” does not solve the problem, check the following.

(1) Checking whether packets are forwarded

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

Figure8-9 Example of Port Status Display

```
> 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 parts to make sure packets are forwarded.

(2) Checking the settings on the collector

Make sure that the collector currently used is configured correctly.

8.3.3 Counter samples cannot be sent to the collector

If “8.3.1 sFlow Packets Not Reaching Collectors” does not solve the problem, 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.

Figure8-10 Configuration Display Example

```
(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 is not set here.

8.4 IEEE802.3ah/UDLD function problems

8.4.1 Turn inactive the ports

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

Table8-6 Fault analysis when using IEEE802.3ah/UDLD facility

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 functionality.	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 the IEEE 802.3ah/OAM functionality is enabled on the partner switch.	If the IEEE 802.3ah/OAM functionality is not enabled on the partner switch, enable the functionality.
		If the IEEE 802.3ah/OAM functionality 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 functionality might be used. Make sure 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 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, an 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 frame used by IEEE802.3ah/UDLD function is discarded by filters or QoS.	For details on how to confirm and how to respond, see "10.2Checking packet discard”.
		If the control frame has not been discarded, go to Item 7.
7	Test the line.	Refer to "10.1Testing the Line" to 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 functionality specific for a Switch that uses IEEE 802.3ah/OAM

8.5 Problems with the neighbor management function

8.5.1 Neighbor device data cannot be acquired by LLDP facility

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

Table8-7Fault analysis when using LLDP

No.	Items to check and commands	Action
1	Execute the show lldp command and check the operating status of the LLDP functionality.	If Enabled is displayed for Status, go to No. 2.
		If the displayed status is Disabled, the LLDP functionality has been disabled. Enable the LLDP functionality.
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 functionality is disabled for the target port. Enable the LLDP functionality 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. Refer to "3.1Ethernet communication failure " for the check method.
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, make sure that the filters or QoS do not discard LLDP control frames. For details on how to confirm and how to respond, see "10.2Checking packet discard”.

9 How to acquire error information

This chapter mainly describes the procedure for acquiring fault information.

9.1 Collecting maintenance information

When a fault occurs with the switch during operation, log and dump information is automatically collected. You can also use operation commands to capture dump information.

9.1.1 Maintenance information

The following table describes the maintenance information.

During stack configuration, maintenance information is available on each member switch. For this reason, collect information from each member switch at the time of stack configuration.

Table9-1 maintenance information

Item	Path and file name	Remarks
Dump information file created when the switch restarts	/dump/rmdump /dump/osdump /usr/var/hardware/ni00.000	・Use the binary mode when transferring files with ftp command. ・Delete after file transfer.
Dump information file created when the network interface fails	/usr/var/hardware/ni00.000	
Log information	You can use the operation-command show logging to check the log-information.	・CLI redirection function can be used for outputting to a file. ・Use ASCII mode when transferring files using ftp command.
Information when the configuration file encounters an error	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 the binary mode when transferring files with ftp command. ・Delete the copied file after file transfer.
Error save information	/usr/var/core/*.core	・Use the binary mode when transferring files with ftp command. ・Delete after file transfer.

9.2 File transfer of maintenance information

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

The ftp command available for the Switch allows you to transfer files containing maintenance information to a remote terminal or remote host.

In a stacked configuration, ftp commands can only transfer files on the master switch. To transfer maintenance information files of member switches other than the master switch, use the cp command to copy the files from each member switch to the master switch, and then transfer the files from the master switch.

9.2.1 Transferring files using the "ftp" command

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

(1) Transferring a dump file to a remote terminal

Figure9-1 Transferring dump files 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 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 terminal

Figure9-2 File transfer of 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. Specify ASCII mode.
3. Specify the destination directory.
4. Transfer the log information.

(3) Transferring an error save information file to a remote terminal

Figure9-3 Transferring an error-saving information 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 error save information 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 to binary mode*
5. Specify the destination directory.
6. Transfer the error save information file.

#

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

9.3 show tech-support Command-Based Data Collection and File-Transfer

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

In a stacked configuration, ftp parameter specification of show tech-support commandallows the collection data to be transferred only when the command is executed on the master switch. If show tech-support command is executed for a member switch other than the master switch, ftp parameter cannot be specified.

When executing show tech-support command for a member switch other than the master switch and transferring the collected information to a file, collect the output of show tech-support executed for the member switch as a file of the master switch and transfer the file from the master switch. See for instructions on collecting show tech-support output from a member switch as a file on the master switch. See “9.2File transfer of maintenance information” for instructions on transferring files on the master switch.

(1) Use show tech-support command to collect data and transfer files.

Figure9-4File transfer of maintenance information to 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 Data with show tech-support Commands (Stacking)

Figure9-5 Collecting maintenance information of the member switch (switch number 2) to the master switch (in 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 terminal

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

In a stack configuration, when a remote operation terminal or remote server connects to the stack by ftp commandI will connect to the master switch. A member switch other than the master switch cannot be connected by FTP.

To acquire failure information and maintenance information from a remote operation terminal or remote server using a member switch other than the master switch, follow the procedure below.

1. Use each member switch to collect the failure or maintenance information.
2. Use cp command to copy the data collected by each member switch from each member switch to the master switch.
2. A remote operation terminal or remote server connects to the stack by ftp commandand transfers the collection data of the member switches 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.

Table9-2 Data that can be acquired by using ftp command.

File name to specify in the "get" subcommand	Information to be obtained
.show-tech	Results obtained from the show tech-support command

Figure9-6Obtaining Basic data of show tech-support

```
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 dump information files

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 dump information.

Table9-3Files that can be acquired with ftp command.

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

Figure9-7 Acquisition of dump files from remote operation terminals

```
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 switch.
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 switch 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 data to a memory card

Failure 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 Switch information to a memory card by using an operation terminal.

1. Insert a memory card into the Switch to which information is to be written.
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 area indicates free space.

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

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

5. Make sure 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 Analysis of communication failures

This chapter describes the actions to be taken in the event of a communication failure.

10.1 Testing the Line

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.

Figure10-1Reflow position of the frame for each line test type

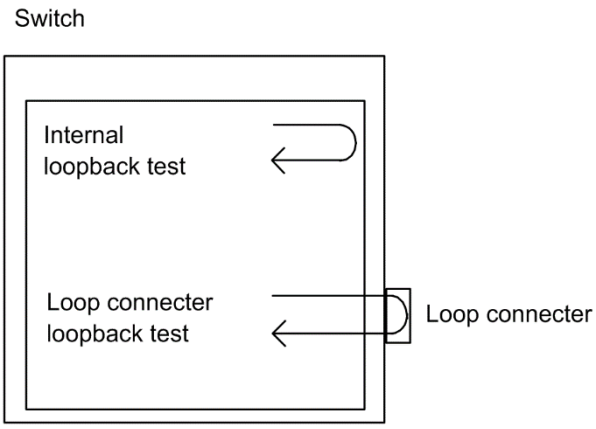


Table10-1 Test Types and Identifiable Fault Locations

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

10.1.1 Module internal loopback test

The internal loopback test, which loops back frames on the Switch, is executed to check for any faults. 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 state.
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 state.

The following figure shows an example of a test performed by setting the transmission interval of the test frame to 2 seconds for port number 1.

Figure10-2 Module Internal Loopback Test Example

```
> 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 information displayed by no test interfaces command in “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 faults. 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 state.
2. Disconnect the cable of the target port and connect the loop connector.*
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 state.

#

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.

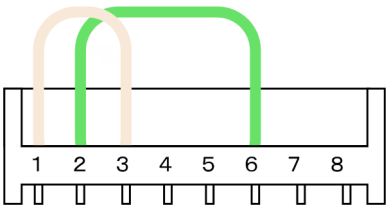
Check the test execution result in the same way as "10.1.1Module internal loopback test".

10.1.3 Loop connectors specification

(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.

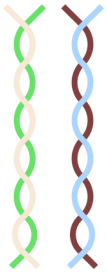
Figure10-3 Wiring of loop connector for 10BASE-T/100BASE-TX



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

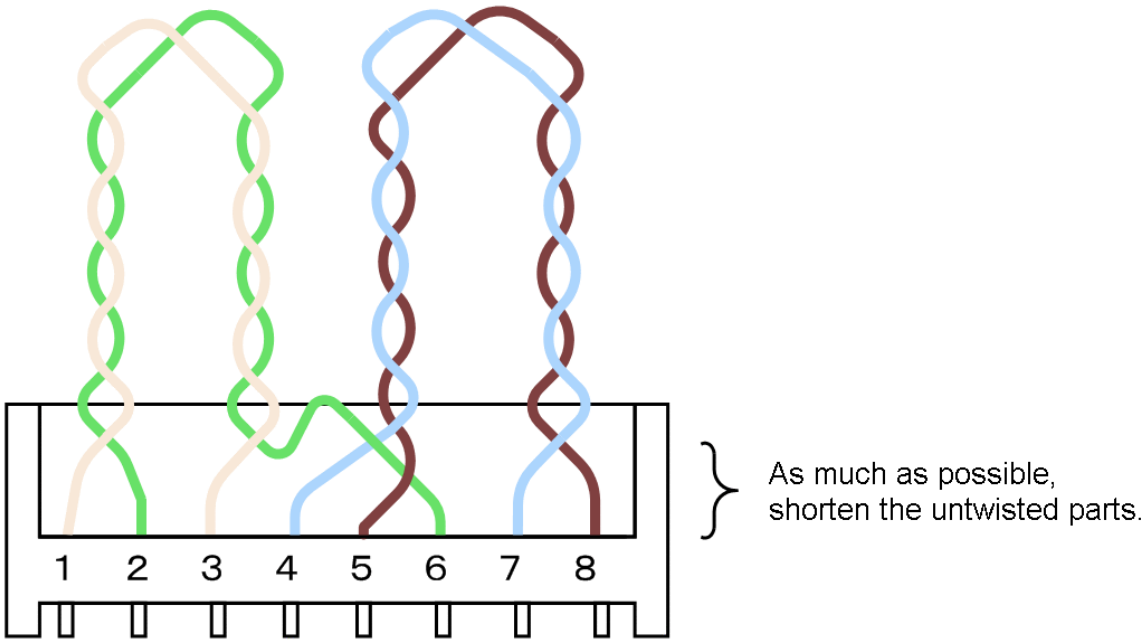
1. Create two 6-to-7-cm long twisted pair cables before you start the procedure.

Figure10-4 Twisted-pair



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

Figure10-5 Wiring of loop connector for 10BASE-T/100BASE-TX/1000BASE-T



Note that looping operation using 1000BASE-T connector is available only for line testing because it is independent operation that is not specified in the standard.

10.2 Checking packet discard

10.2.1 Confirm discard by filter

A possible cause of communication problems on the network where the Switch is used is that certain frames may be discarded by the filter. The following shows how to check frame discard by filtering.

(1) How to check frame discard by filtering

1. Execute show access-filter command to check the number of packets matching the filter conditions of the access list applied to the interface and the number of packets discarded by the filter entries of implicit discard.
2. 1. Compare the filter condition checked with the contents of the frame that cannot be communicated to check whether the frame has been discarded. If the contents of a frame that cannot be communicated do not match all the applicable filter conditions, the frame may have been discarded by an implicit discard filter entry.
3. If the filter discards frames, review whether the filter configuration settings are appropriate.

10.2.2 Confirm whether QoS is used for disposal.

One possible cause of communication problems on the network that uses the Switch is that frames have been discarded by QoS control bandwidth monitoring, discard control, or the shaper. The following shows how to check frame discard by using QoS.

(1) How to check frame discard by bandwidth monitoring

1. Execute show qos-flow command to check the flow detection condition, operation specification, and the number of packets matching the flow detection condition of bandwidth monitoring applied to the interface.
2. 1. Compare the flow detection condition checked with the contents of the frame that cannot be communicated to check whether the frame has been discarded. Frames that violate the maximum bandwidth control are discarded and counted in "matched packets(max-rate over" of the statistical data. If this value is counted, frames may have been discarded due to bandwidth monitoring applied to the interface.
3. Review whether QoS control configuration settings are appropriate and whether bandwidth monitoring settings for system configuration are appropriate.

(2) How to check frame discard by discard control and legacy shaper

1. Execute show qos queueing command. Check discard packets of the statistical information for the output interfaces.
2. 1. If the statistical data checked is counting up, the frame was discarded by QoS control discard control and legacy shaper.
3. Check whether drop control and the 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 handled by CPU may occur even if the packet is operating normally, for example, when a large number of packets are temporarily received due to a change in the network topology. 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.

Table10-2 What to do if congestion on packets handled by CPU does not recover

No.	Items to check and commands	Action
1	Identify packet types. ・Execute show netstat statistics command continuously every 20 seconds to compare the results.	If, as a result of the comparison, total packets received whose packet type is in Ip statistical items significantly increases in counting, go to Item 2.
		If, as a result of the comparison, packets received whose packet type is in Arp statistical items significantly increases in counting, go to Item 2.
		For other cases, go to No. 4.
2	Identify the VLAN interface that is receiving the packets. ・Execute show netstat interface command continuously every 20 seconds to 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. ・ Execute show tcpdump interface command for VLAN interface specified in No. 2 to check the source address and destination address of the packet type specified in No. 1.	If the packet type is Ip and the destination address of the corresponding packet is the Switch, the packet may have been 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 show tech-support command twice.	Send the information you collected to the support center.

11 Device restart

This chapter mainly describes how to restart the device.

11.1 Restarting the device

11.1.1 Device restart

You can use the reload command to restart the device. Log data is stored when the device restarts.

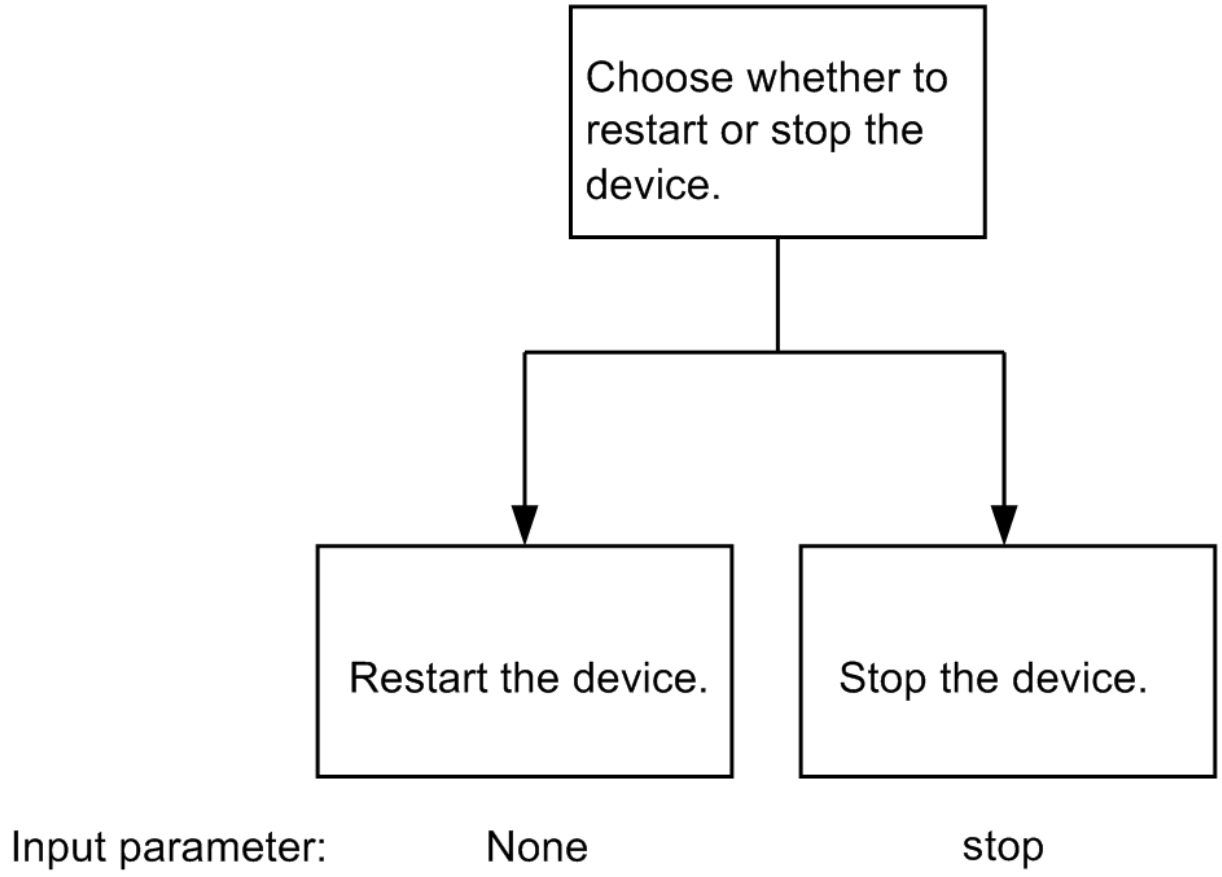
For details about command informats and parameters, see Operation Command Reference.

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 capture the CPU memory dump by interacting with the confirmation messages.

Step1

Choose whether you want to restart or stop the device.

Figure11-1 Device restart/stop selection

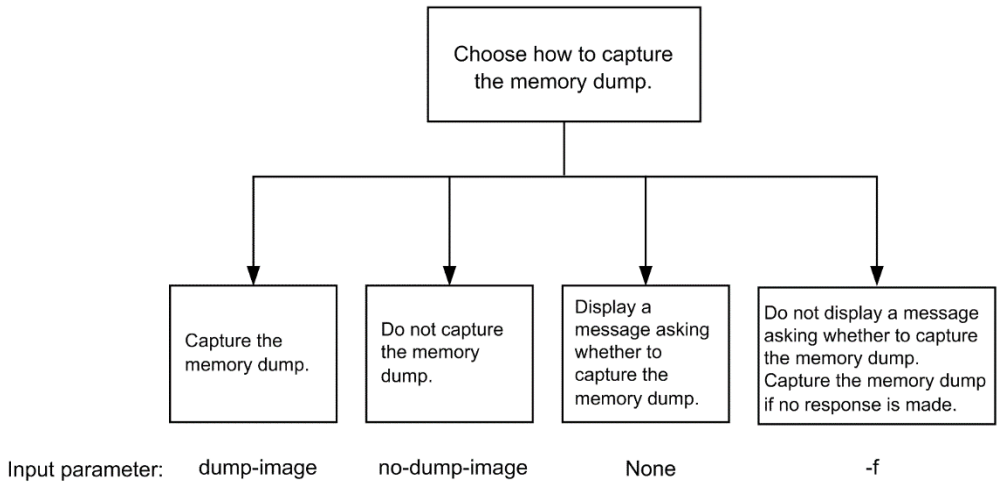


In step 1, you restart the device. So according to the figure above, you do not use any parameters.

Step2

In this step, choose whether you capture the dump.

Figure11-2 CPU memory dump collection selection



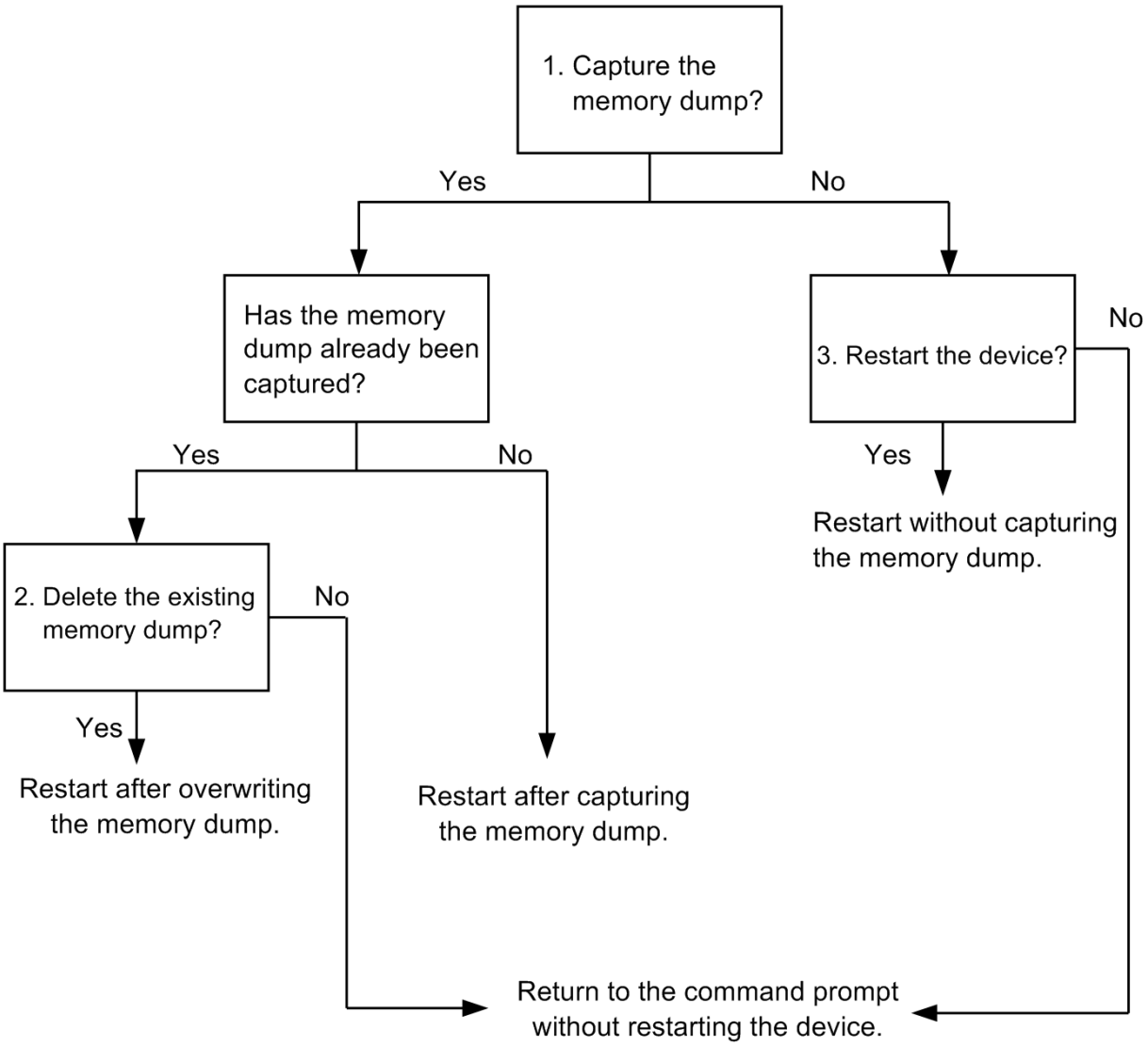
In step 2, you will be asked whether you want to capture the CPU memory dump. According to the figure above, you do not use any parameters.

Combining the parameters selected in steps 1 and 2 results in the command reload. When you enter this command, the dump capture 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.

Figure11-3 CPU Memory Dump Collection Confirmation Message



Appendix

AppendixA Detailed description of displayed show tech-support command

The following table shows the commands that are displayed for each parameter specification in show tech-support command.

For details about the displayed contents, see the operation command reference.

Note

Some of the information displayed by show tech-support command is not described in the "Operation Command Reference". The details of these information are not disclosed because they contain internal information of the device.

Some software versions may or may not be displayed. Please understand in advance.

TableA-1Details of displayed command

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/uptime data
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 captured 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	Operational configuration information
15	show logging	Chronological log information for the active system
16	show logging reference	Log information for each active system type
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 size in the directory
22	show mc	MC format and usage
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

No.	Command (displayed)	Description
28	ls -leiR /var	Memory file system information
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 tracing info 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 statistical data (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	Intranet route-related data (IPv6 unicast)
42	show ip arp	ARP data
43	show ipv6 neighbors	NDP data
44	show ipv6 router-advertisement	RA advertising information
45	show ntp associations	Operation of NTP servers
46	/usr/local/diag/ntpdebug	Debugging info on NTP servers
47	show vlan list	VLAN information list
48	show port	Port information
49	show port vlan	Port-specific VLAN data
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-specific EEE data
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 info
57	show vlan detail	VLAN description
58	show vlan mac-vlan	MAC VLAN info
59	nimdump stack aging info	Stack switching aging time
60	show channel-group detail	Link aggregation details
61	show spanning-tree detail	Spanning tree details
62	show gsrp aware	GSRP aware info
63	show axrp detail	Detailed Autonomous Extensible Ring Protocol info
64	show switchport-backup	Uplink redundant information
65	show switchport-backup detail	Uplink redundant details
66	show switchport-backup statistics	Uplink redundant statistics
67	show efmoam detail	IEEE 802.3ah/OAM functionality configuration information and port status
68	show efmoam statistics	IEEE 802.3ah/OAM functionality statistics

No.	Command (displayed)	Description
69	show lldp detail	Neighboring device information for the LLDP functionality
70	show lldp statistics	LLDP functionality statistics
71	show loop-detection	L2 Loop-Detect Info
72	show loop-detection statistics	L2 Loop-Detect Statistics
73	show loop-detection logging	Logging 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's mrouter data
85	show igmp-snooping mrouter statistics	Mrouter statistic for IGMP snooping
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 statistic
90	show ip arp inspection statistics	Dynamic ARP study statistic
91	show ip dhcp snooping logging info	DHCP snooping logging info
92	/usr/local/bin/dhsn debug	DHCP snooping event-information
93	show dot1x logging	Operation log messages collected by IEEE802.1X certification
94	show dot1x statistics	IEEE802.1X authentication-related stats
95	show dot1x detail	Authentication-status information related to IEEE802.1X authentication
96	show web-authentication user edit	Displaying registered/changed contents of the internal Web authentication DB
97	show web-authentication user commit	Displaying registered data of the internal Web authentication DB
98	show web-authentication statistics	Viewing Web authentication Statistics
99	show web-authentication login	Viewing Authenticated User Information (Account Information)
100	show web-authentication logging	Viewing Web authentication Activation Logging
101	/usr/local/diag/wainfo	Displaying Session Information for Web Servers
102	show mac-authentication	Viewing MAC-based authentication Settings
103	show mac-authentication statistics	Viewing MAC-based authentication Statistics
104	show mac-authentication mac-address edit	Displaying registered/changed contents of internal MAC-based authentication DB

No.	Command (displayed)	Description
105	show mac-authentication mac-address commit	Displaying registered data of internal MAC-based authentication DB
106	show mac-authentication login	Viewing Authenticated User Information (Account Information)
107	show mac-authentication logging	Viewing MAC Activation Logging
108	show authentication multi-step	Multi-Step Credentials
109	show sflow detail	Displaying sFlow stats (detailed)
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	Event information registered from scripts during monitoring
113	/usr/local/bin/scriptshow 1 applet detail	Event information being monitored by the applet function
114	show event manager history script	History of events registered for monitoring from scripts
115	show event manager history applet	History of events that are being monitored by the applet function
116	show script installed-file	List of installed script files
117	show script running-state	Operating status of the advanced scripts
118	show logging script-only	Operation log data with a message type of SKY,SRS
119	show environment temperature-logging	Historical temperature 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 logging info
129	cat /usr/var/pplog/ppupdate.log	Log information when software update is executed
130	cat /usr/var/pplog/ppupdate2.log	Log information when software update is executed
131	tail -n 30 /var/log/authlog	Authentication trace information
132	tail -n 30 /var/log/xferlog	FTP tracing info
133	cat /var/log/ssh.log	SSH logging info
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 switch debug	Stack debug information
141	cat /var/tmp/stack/stacklog	Stack log information