AX2500S

Troubleshooting Guide

AX25S-T001X-70

Relevant products

This manual applies to the models in the AX2500S series of switches.

Export restrictions

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

Trademarks

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.
Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
RSA and RSA SecurID are trademarks or registered trademarks of RSA Security Inc. in the United States and other countries.
sFlow is a registered trademark of InMon Corporation in the United States and other countries.
Wake-on-LAN is a registered trademark of IBM Corporation.
MagicPacket is a registered trademark of Advanced Micro Devices, Inc.
Other company and product names in this document are trademarks or registered trademarks of their respective owners.

Reading and storing this manual

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

Notes

Information in this document is subject to change without notice.

Editions history

January 2013 (Edition 8) AX25S-T001X-70

Copyright

History of Amendments

(Edition 8)

Summary of amendments

Location and title	Changes
2. Troubleshooting Switch Failures	● A description of DC models and external redundant power units (EPU-D) was added.
Appendix A. Detailed Display Contents of the show tech-support Command	● Commands were added to the Displayed information.

In addition to the above changes, minor editorial corrections were made.

(Edition 7)

Summary of amendments

Location and title	Changes
Troubleshooting the sFlow statistics (flow statistics) functionality	● This subsection was added.
Appendix A. Detailed Display Contents of the show tech-support Command	● Commands were added to the Displayed information.

In addition to the above changes, minor editorial corrections were made.

(Edition 6)

Summary of amendments

Location and title	Changes
Failures occurring when the Spanning Tree functionality is used	● Actions to be taken when the Spanning Tree functionality is used with the Ring Protocol were added.
Failures occurring when the Ring Protocol functionality is used	● Actions to be taken when the master node is supported were added. ● Actions to be taken when the Spanning Tree functionality is used with the Ring Protocol were added. ● Descriptions of the multi-fault monitoring functionality were added.
IPv6 network communication failures	● This subsection was added.
Appendix A. Detailed Display Contents of the show tech-support Command	● Commands were added to the Displayed information.

In addition to the above changes, minor editorial corrections were made.

(Edition 5)

Summary of amendments

Location and title	Changes
Appendix A. Detailed Display Contents of the show tech-support Command	● The layer-2 specified column was added to indicate whether each command is displayed when the `layer-2` parameter is specified.

In addition to the above changes, minor editorial corrections were made.

(Edition 4)

Summary of amendments

Location and title	Changes
--	● A description of AX2530S-24T4X/AX2530S-48T2X switches was added.

In addition to the above changes, minor editorial corrections were made.

(Edition 3)

Summary of amendments

Location and title	Changes
SNMP communication failures	● A description of SNMPv3 was added.
NTP communication failures	● A description related to checking of the time zone was changed.
Loop connector loopback test	● A description of a loop connector when SFP for 10BASE-T/100BASE-TX/1000BASE-T is used was added.
Creating loop connectors	● This subsection was added.
Detailed display contents of the `show tech-support` command	● Commands were added to the Displayed information.

In addition to the above changes, minor editorial corrections were made.

(Edition 2)

Summary of amendments

Location and title	Changes
--	● A description of AX2530S-24S4X switches was added.
Procedure for handling Switch faults	● A description of the 10GBASE-R interface was added to Table 2-1.
Information cannot be entered from the console or does not display correctly	● Items to check when login fails were changed.

Location and title	Changes
Login from a remote operation terminal is not possible	● Items to check when login fails were changed.
Updates by using the `ppupdate` operation command are not possible	● A description related to notes on update files was added.
Restoring data by using the `restore` operation command is not possible	● A description related to notes on backup files was added.
Actions to be taken for 100BASE-FX [24S4X]/1000BASE-X problems	● A description of 100BASE-FX was added.
Actions to be taken for 10GBASE-R problems [24S4X]	● This subsection was added.
Actions to be taken for direct attach cable problems [24S4X]	● This subsection was added.
Problems related to the support regarding long life solutions	● This subsection was added.
Detailed display contents of the `show tech-support` command	● Commands were added to the Displayed information.

In addition to the above changes, minor editorial corrections were made.

Preface

Applicable products and software versions

This manual applies to the models in the AX2500S series of switches. It also describes the functionality of version 3.4 of the software for the AX2500S series of switches. The described functionality is that supported by the OS-L2B-A/OS-L2B and the advanced software upgrade license (the "License").

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.

Unless otherwise noted, this manual describes the functionality applicable commonly to AX2500S series switches. The functionalities specific to each model are indicated as follows:

[24T]:

This description applies to AX2530S-24T switches.

[24T4X]:

This description applies to AX2530S-24T4X switches.

[48T]:

This description applies to AX2530S-48T switches.

[48T2X]:

This description applies to AX2530S-48T2X switches.

[24S4X]:

This description applies to AX2530S-24S4X switches.

[10G models]:

The description applies to AX2530S-24T4X, AX2530S-48T2X, and AX2530S-24S4X switches.

Unless otherwise noted, this manual describes the functionality for OS-L2B-A/OS-L2B. Functionality related to the Software License Agreement and License Sheet is indicated as follows:

[OS-L2A]:

The description indicates functionality supported by the Software License Agreement and License Sheet.

Corrections to the manual

Corrections to this manual might be contained in the *Release Notes* and *Manual Corrections* that come with the software.

Intended readers

This manual is intended for system administrators who wish to configure and operate a network system that uses the Switch.

Readers must have an understanding of the following:

- The basics of network system management

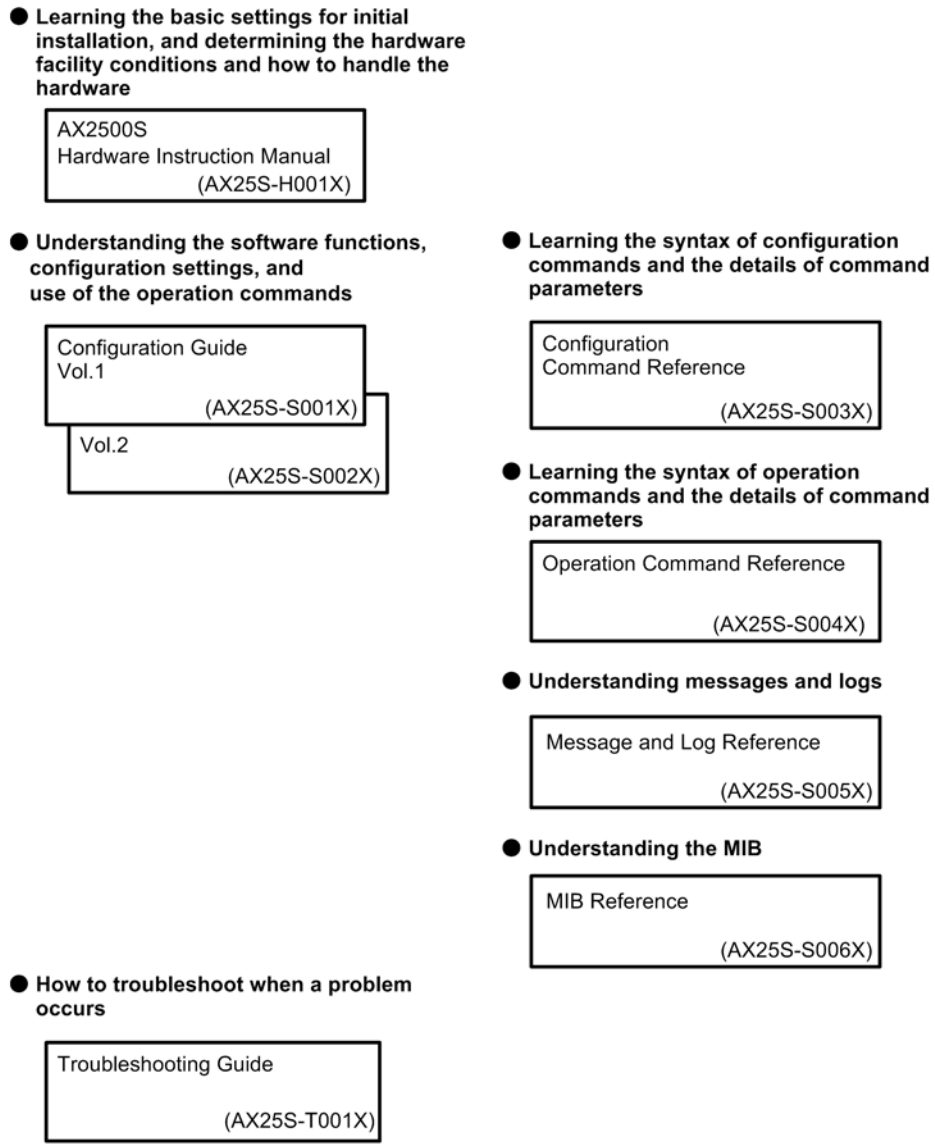
Manual URL

You can view this manual on our website at:

http://www.alaxala.com/en/

Reading sequence of the manuals

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



Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bits/s	Bits per second (can also appear as bps)

BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol

IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding

PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Enhanced Small Form factor Pluggable
SML	Split Multi Link
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
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
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

Conventions: The terms "Switch" and "switch"

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

- AX2500S series switch

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

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

1 KB (kilobyte) is 1024 bytes.

1 MB (megabyte) is 1024^2 bytes.

1 GB (gigabyte) is 1024^3 bytes.

1 TB (terabyte) is 1024^4 bytes.

Safety Information

Using AX2500S series switches correctly and safely

- This guide provides important information for ensuring safe use of AX2500S series switches. Please read this manual completely before using the Switch.
- Keep this manual handy after reading it, so that it is available for later reference.
- Operate the Switch according to the instructions and procedures provided in this manual.
- Heed all warnings and cautions for the Switch in this guide. Failure to do so could result in injury or damage to the Switch.

Before using the Switch

- Caution indications

  These indications are intended to ensure safe and correct use of the Switch and to prevent serious injury, and equipment and property damage. Caution information in this manual and on the Switch is preceded by the indications shown below. Make sure you fully understand the meaning of the indications before continuing with the main body of this manual.

⚠WARNING	Ignoring instructions preceded by this indication and using the Switch incorrectly could result in death or serious injury to yourself and others.
⚠CAUTION	Ignoring instructions preceded by this indication and using the Switch incorrectly could result in injury to yourself and others.
CAUTION	Ignoring instructions preceded by this indication and using the Switch incorrectly could result in serious damage to the Switch or nearby property.
NOTE	Information preceded by this indication is supplementary information that, if ignored, will not result in physical injury or serious damage to the Switch.

Unauthorized operations

- Do not attempt to perform any operations that are not described in this guide.

  In the event of a Switch problem, turn off the power, unplug the power cable, and contact maintenance personnel.

Using common sense

The warnings and cautions provided on the Switch and in this guide have been selected after careful consideration.

Nevertheless, there is always the possibility of the unexpected occurring. Therefore, while using a Switch, stay alert and use common sense in addition to all following instructions.

⚠WARNING

If anything seems wrong, immediately turn off the power.

- If smoke or an unusual smell is emanating from the Switch, or if liquid is spilled into the Switch or a foreign object falls into the Switch, immediately turn off Switch power as described below. Continuing operation could result in fire or electric shock.

Actions to take for abnormal conditions

Device in which an error occurred		Action to take
AC model	When an external redundant power unit (EPU-A) is not used	Turn off the Switch and unplug the power cable.
	When an external redundant power unit (EPU-A) is used	Turn off the Switch and the power supply module supplying power to the Switch, and then unplug the power cable.
DC model		Turn off the Switch, and then set the power supply circuit breaker to OFF.
External redundant power unit (EPU-D)		
External redundant power unit (EPU-A)		Turn off the external redundant power unit (EPU-A), and then unplug the power cable.

Do not allow any foreign objects to get into the Switch.

- Do not insert or drop any foreign objects, such as anything metallic or flammable, through the Switch's ventilation slots. Doing so could result in fire or electric shock.

When pressing the RESET button, do not use anything with a fragile tip, or anything that might become caught in the Switch, such as a pin or paper clip.

- When pressing the RESET button, do not use anything with a fragile tip, or anything that might become caught in the Switch, such as a pin or paper clip. Doing so could result in fire or electric shock.

Do not modify the Switch.

- Do not alter the physical makeup of the Switch. Doing so could result in a fire or electric shock.

Do not subject the Switch to shocks.

- In the event that the Switch is dropped or any of its components damaged, turn off the power, unplug the power cable, and contact maintenance personnel. Discontinue using the cable to avoid the risk of fire or electric shock.

Do not place any objects on the Switch.

- Do not place any metallic object such as a small pin or a paper clip or any container with a liquid, such as a vase or a flowerpot, on the Switch. Liquid or metallic objects falling into the Switch could result in fire or electric shock.

Use the Switch only with the indicated power supply.

- Do not use the Switch at any voltage other than the indicated voltage. Doing so could result in fire or electric shock.

⚠WARNING

Ensure that the capacity for incoming current to the distribution board is greater than the operating current of the circuit breaker.

- Ensure that the capacity for incoming current to the distribution board is greater than the operating current of the circuit breaker. If it is not, the circuit breaker might not operate properly in the event of a failure, which could result in a fire.

Ground the Switch.

- When using an AC model and external redundant power unit (EPU-A), always use a grounded power outlet. Using the Switch and an EPU without grounding could result in electric shock or failures due to electrical noise.
- When using a DC model and an external redundant power unit (EPU-D), make sure to connect a ground cable to ground the switch. Using the switch without grounding could result in electric shock or failures.

Use a DC power supply for which the primary side and the secondary side are insulated.

- When using DC power, use a power supply for which the primary side and the secondary side are insulated. Using a power supply that is not insulated could result in electric shock.

Connecting and disconnecting a DC power cable must be performed by a trained technician or maintenance personnel.

- Connecting or disconnecting the DC power cable to the power supply unit must be performed by a trained technician or maintenance personnel. Terminal connections are required for connection of the DC power cable to the power facility. For this reason, incorrect handling of the DC power cable could result in fire or electric shock.

Before connecting or disconnecting a DC power cable, set the power supply circuit breaker to OFF.

- Before connecting or disconnecting a DC power cable, set the power supply circuit breaker to OFF. Connecting or disconnecting the cable with the circuit breaker set to ON could result in a fire or electric shock.

Place an insulation cover over the G and -48 V terminals of DC power cables.

- Place an insulation cover on the G and -48 V terminals of a DC power cable (on the side grounded to the power supply). Using the terminals without an insulation cover could result in electric shock.

When using a DC power supply unit of an external redundant power unit (EPU-D), do not use the terminal block with its cover removed.

- When using a DC power supply unit of an external redundant power unit (EPU-D), after connecting the DC power cable, make sure to attach the terminal block cover. Using the terminal block without a cover could result in electric shock.

⚠WARNING

Do not use the Switch with the protection cap removed.

- Do not remove the protection cap except when attaching a cable. Using an AX2500S series switch without a protection cap could result in a fire or electric shock.

Handle power cables carefully.

- Do not place anything heavy on a power cable. Do not pull, bend, or process a cable. Doing so could damage the cable, resulting in fire or electric shock. If the power cable is covered with a carpet or the like, it is easy to forget that the cable is there and to place something heavy on it.
- Use the supplied or a designated power cable. Using another cable could result in fire or electric shock. In addition, do not use the supplied cable with other devices. Doing so could result in a fire or electric shock.
- If the power cable is damaged so that the wires underneath the covering are visible or cut, stop using it, and ask maintenance personnel to replace it. Discontinue using the cable to avoid the risk of fire or electric shock.
- Make sure the power plug is free of dust, and insert the plug completely up to the base of the prongs to prevent any looseness. Using a power plug with dust on it or one that is imperfectly connected could result in fire or electric shock.
- Do not touch the power plug with a wet hand. Doing so could result in electric shock.

Do not overload the power outlet.

- Do not overload the power outlet by connecting multiple power plugs to the same outlet. Overloading the outlet could result in fire or the circuit breaker tripping due to excessive power used. This might affect other equipment.

Adding or replacing a module must be performed by a trained technician or maintenance personnel.

- Adding or replacing a power supply module must be performed by a trained technician or maintenance personnel. If anyone other than those mentioned above performs these tasks incorrectly, a fire, electric shock, or failure could result.

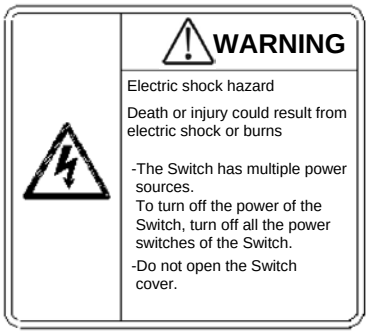
Do not use an air duster near a flame.

- When cleaning the optical connectors, do not use an air duster that contains flammable gas near a flame. Doing so could result in a fire.

⚠WARNING

Do not open the Switch cover.

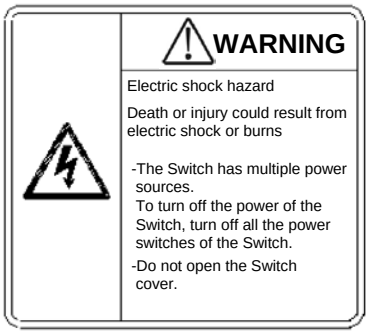
- Do not open the Switch cover. Doing so could result in electric shock. The label below is attached to a Switch.



When turning off the power, stop the supply of all power to the Switch.

- If power is supplied from an external redundant power unit, the Switch cannot be turned off by just setting the power switch of the Switch to OFF. To turn off the power, turn off the power switches of both the Switch and power supply modules. The label below is attached to the Switch.

For the Switch



For an external redundant power unit (EPU-D)

⚠CAUTION

Do not place the Switch in an unstable location.

- When installing the Switch on a table, position the Switch horizontally on a worktable strong enough to bear the weight of the Switch. Placing the Switch in an unstable location, such as on an unsteady or tilting surface, might cause the Switch to fall, resulting in injury.
- When mounting the Switch in a rack, make sure that the Switch is stable. If the Switch is unstable, it might fall, resulting in injury.

Do not position the Switch and external redundant power unit (EPU-D) vertically or lean them against a wall.

- When installing the Switch and external redundant power unit (EPU-D) on a table, position the devices horizontally. If they are positioned vertically or leaned against a wall, they might fall, which could result in injury or damage.

Do not allow hair or objects near the ventilation slots.

- Cooling fan units are mounted in AX2530S-24T4X, AX2530S-48T, AX2530S-48T2X, AX2530S-24S4X, AX2530S-48TD, AX2530S-24S4XD switches and external redundant power units. Do not allow hair or other objects near the ventilation slots. They might be sucked into the Switch, resulting in injury.

Do not hold the handle of the power supply module when moving an EPU.

- Do not hold the handle of the power supply module when moving an external redundant power unit. The handle might come off, resulting in the device falling and possibly causing injury. Also, the EPU or the power supply module might become damaged, resulting in a fire or electric shock.

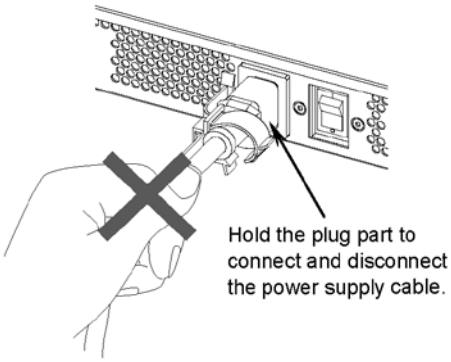
When moving a Switch

- Before moving a Switch, you must turn it off and unplug all cables. Failure to do so might cause the Switch or cable to become deformed, or might damage the Switch, resulting in fire or electric shock.
- If you must stack multiple Switches during transport, use appropriate packaging. Failure to do so might cause the Switch to become deformed or might damage the Switch, resulting in fire or electric shock.

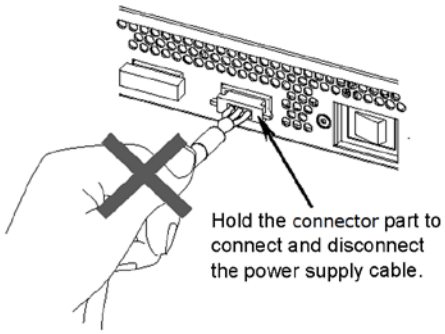
⚠CAUTION

Handle the power cable carefully.

- Do not place the power cable near a heat-generating apparatus. The heat could melt the cable coating, resulting in fire or electric shock.
- When connecting or disconnecting the AC power cable from the outlet, always hold the plug, not the cable itself. Pulling the cable itself might cause the wires to break.



- When connecting or disconnecting a DC power cable, always hold the connector of the cable. Pulling the cable itself might cause the wires to break.



Do not touch the Switch directly if you have a metal allergy.

- The Switch is coated with zinc, nickel, gold, and other elements. Do not touch the Switch directly if you have an allergic reaction to these metallic elements. Doing so might cause eczema or skin irritation.

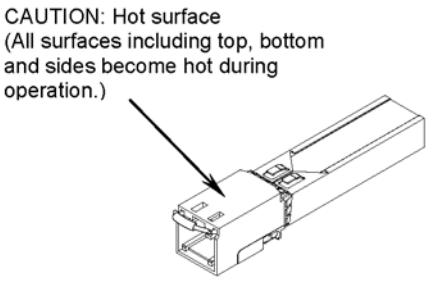
Avoid looking directly at laser beams.

- The Switch uses laser beams that are colorless and transparent, and invisible to the eye. Never look directly into the optical transceiver.

⚠CAUTION

Do not touch the SFP-T during operation and just after operation stops.

- During operation (when a link is established), the temperature of the SFP-T can rise to 65ºC. Do not touch the device while it is operating or just after it stops. Doing so could result in burns.



To remove the SFP-T, use the procedure below. Failure to do so could result in burns.

- To remove the device when the Switch is turned on, block the SFP slot or the SFP+ slot, and then wait five minutes before removing the SFP-T.

- To remove the device after turning off the Switch, turn off the Switch, wait five minutes, and then remove the device.

The following label is attached to the SFP-T.

Do not install the Switch in a dusty or humid location.

- Do not install the Switch in a dusty or humid location. Doing so could result in fire or electric shock.
- Condensation might form on the surfaces and the inside of the Switch if it is moved from a cold location to a warm location. Using the Switch in this condition could result in fire or electric shock. After moving the Switch between two locations with a large temperature variation, let the Switch stand a few hours before using it.

Do not step on the Switch, lean against it, or place anything on it.

- Do not step on the Switch or lean against it. Doing so might damage the Switch. Furthermore, the Switch might fall, or become unbalanced, resulting in injury.
- Do not place any objects on the Switch. Doing so might damage the Switch. Furthermore, the Switch might fall, or become unbalanced, resulting in injury.

Do not touch the inside of the Switch with your hands.

- Do not carelessly put your hands inside the Switch. The frame and components might cause injury.

⚠CAUTION

Attach a blank panel to a slot in which a power supply module for an EPU is not installed.

- Be sure to attach a blank panel to any slots for which a power supply module for an external redundant power unit is not installed. If you use the Switch without attaching the blank panel, you might be injured by a moving part. In addition, if foreign objects fall into the Switch, the Switch might no longer work properly.

Cleaning

- Remove dust on and around the Switch regularly. In addition to causing the Switch to stop, accumulated dust could result in a fire or electric shock.

CAUTION

Ensure adequate heat dissipation from the Switch by not stacking devices.

- Heat dissipates from the top panels of the AX2530S-24T (fanless), AX2530S-24TD (fanless), AX2530S-48T (semi-fanless), and AX2530S-48TD (semi-fanless) models. To ensure adequate heat dissipation, do not stack another device on top of or below the Switch. Doing so could result in Switch malfunction.

  When the Switch is installed in a rack, ensure 1U or more of space between the switch and other devices.

Do not place a Switch in a high-temperature location.

- Do not place a Switch in direct sunlight or near a heater or other heat-generating apparatus. Doing so could adversely affect parts of the Switch.

Do not use a TV or a radio near a Switch.

- Placing a Switch near a TV or a radio could affect both devices. If you hear noise on the TV or radio, do the following:

  - Place the Switch as far away as possible from the TV or radio.

  - Adjust the orientation of the TV or radio antenna.

  - Use separate outlets.

Do not place the Switch in an undesirable environment.

- Using the switch in the following locations might shorten the life of the switch or result in a switch malfunction.

  - An area with salty air, such as the coast

  - An area where corrosive gases are present, such as a hot-springs area

  - An area where oily smoke is present

  - An area where continuous vibrations are present

Do not obstruct the ventilation slots.

- Do not obstruct the ventilation slots of the Switch. Doing so causes heat to accumulate inside the switch, and could result in a switch malfunction. Maintain a space of at least 50 mm around the ventilation slots.

Ensure that voltage drop does not occur in the power facility due to inrush current.

- Turning on the Switch causes inrush current. Ensure that voltage drop does not occur in the power facility due to the inrush current. Voltage drops affect not only the Switch, but also the devices connected to the same power facility.

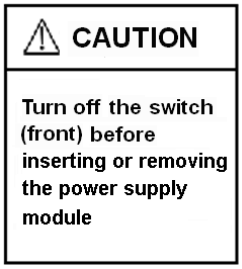
Turn off the power before connecting or disconnecting the power cable.

- Turn off the power of the Switch before connecting or disconnecting the power cable of an AC model and an external redundant power unit (EPU-A).
- For a standby power cable, turn off the power of the power supply module first.

CAUTION

Turn off the power before installing or removing a power supply module.

- Before installing or removing a power supply module, turn off its power. Installing or removing the module with the power supply module turned on causes a (Switch) failure. The following label is attached to the external redundant power unit.



Turn off the power of the power supply modules before turning on the main power switch of an EPU.

- Before setting the main power switch of the external redundant power unit to ON, you must set the power switches of the installed power supply modules to OFF.

Do not turn off the main power switch of an EPU if the standby power supply unit is used for the Switch.

- Turning off the main power switch of an external redundant power unit stops the supply of all standby power to the Switch. Do not turn off the main power switch if a standby power supply unit is being used for the Switch.

Handle memory cards and dummy memory cards carefully.

- When installing a memory card and a dummy memory card, do not force the card. When removing a memory card, do not forcibly pull out the card if it is locked. Doing so might damage the connector of the memory card slot.
- When moving the Switch, remove memory cards and dummy memory cards. If a card is subjected to excessive force when the switch is moved, the connector of the memory card slot might be damaged.

When the ACC LED is lit, do not remove the memory card or turn off the power.

- When the ACC LED on the front panel of the Switch is lit, the memory card is being accessed. When a memory card is being accessed, do not remove the memory card or turn off the power. Doing so might damage the memory card.

  In addition, some commands require a certain amount of time after being entered to finish accessing the card. Make sure that the memory card is no longer being accessed before removing the card or turning off the power.

CAUTION

Do not attach any labels to a transceiver or a direct attach cable connector.

- A label attached to the transceiver or direct attach cable connector indicates that the transceiver or direct attach cable connector is a standard product from ALAXALA or another manufacturer. However, such labels are attached where they do not interfere with heat dissipation from the transceiver or from the direct attach cable connector or interfere with the mechanism that prevents the transceiver or the direct attach cable connector from coming loose from the cage.

  Attaching a label to a location that interferes with these functions could cause a malfunction in the transceiver or a direct attach cable connector, or cause damage to the Switch.

Make sure that you use a valid combination for the direct attach cable and the Switch.

- The switches below support SFPP-CU30C/CU1M/CU3M/CU5M. Use direct attach cables only for connections between the indicated Switches. Not doing so could result in a Switch malfunction.

  - AX2530S-24T4X (Supported ports: 25 to 28)

  - AX2530S-24S4X (Supported ports: 25 to 28)

  - AX2530S-48T2X (Supported ports: 51 to 52)

  - AX2530S-24S4XD (Supported ports: 25 to 28)

Make sure that you use a valid combination for the transceiver and the Switch.

- The switches below support SFP-FX. Use the transceivers only with the indicated Switches. Not doing so could result in a Switch malfunction.

  - AX2530S-24S4X (Supported ports: 1 to 24)

  - AX2530S-24S4XD (Supported ports: 1 to 24)

- The switches below support SFP-SX2. Use the transceivers only with the indicated Switches. Not doing so could result in a Switch malfunction.

  - AX2530S-24T (Supported ports: 25 to 28)

  - AX2530S-48T (Supported ports: 49 to 52)

  - AX2530S-48T2X (Supported ports: 49 to 50)

  - AX2530S-24S4X (Supported ports: 1 to 24)

  - AX2530S-24TD (Supported ports: 25 to 28)

  - AX2530S-48TD (Supported ports: 49 to 52)

  - AX2530S-24S4XD (Supported ports: 1 to 24)

When carrying or packing a Switch and its optional modules, wear a wrist strap to protect against static electricity.

- Be sure to wear an antistatic wrist strap. If you handle the Switch without wearing an antistatic wrist strap, the Switch might be damaged by static electricity.

When carrying and packing optional modules, handle them carefully.

- Do not touch a connector when carrying or packaging a transceiver, direct attach cable, memory card, or power supply module. Also, when storing an optional module, use an antistatic bag.

CAUTION

Use care when handling an air duster.

- Use an air duster specially designed for cleaning optical connectors. Using another type of air duster could cause the ferrule tip to become dirty.
- Keep the nozzle or container of the air duster from coming into contact with the ferrule tip. Contact could result in a malfunction.

Use care when handling an optical connector cleaner.

- Always use a dedicated optical connector cleaner. If you use another type of cleaner, the ferrule tip might become dirty.
- Before cleaning, make sure that the tip of the optical connector cleaner is clean and free of defects, such as lint, dirt, or other foreign substances. Using a cleaner with a defective tip might damage the ferrule tip.
- Do not apply excessive pressure when cleaning. Doing so might damage the ferrule tip.
- Rotate the optical connector cleaner (stick) clockwise only. Rotating the cleaner alternately clockwise and counterclockwise might damage the ferrule tip.

Maintenance

- Clean any dirty areas on the exterior of the switch with a clean, dry cloth, or a cloth damp with (but not soaked with) water or a neutral detergent. Do not use volatile organic solutions (such as benzene or paint thinner), chemicals, chemically treated cloths, or pesticides because these substances might deform, discolor, or damage the switch.

If the Switch will not be used for a long time

- For safety reasons, unplug the power cable from the outlet if the Switch will not be used for a long time. If you are using a DC power supply unit, turn off the circuit breaker at the supply of power.

Disposing of a Switch

- When disposing of a switch, you should either follow local ordinances or regulations or contact your local waste disposal and treatment facility.

Contents

1. Overview

This chapter provides an overview of failure analysis.

1.1 Overview of analyzing failures

Use this manual when there is a problem in an AX2500S series switch.

When failure analysis requires looking at the actual Switch, do the analysis according to *1.2 Overview of analyzing failures of all or part of the Switch*.

When failure analysis requires logging in to the Switch, do the analysis according to *1.3 Overview of analyzing failures of functionality*.

1.2 Overview of analyzing failures of all or part of the Switch

If a failure occurs during operation and the actual Switch can be looked at, take appropriate action as described in *2.1 Procedure for handling Switch failures* to troubleshoot the failure.

For a description of the LEDs on the Switch, see the example of the AX2530S-24T switch shown in the following figure and *Table 1-1 LED indications, buttons, and connectors*.

Figure 1-1 Front panel layout

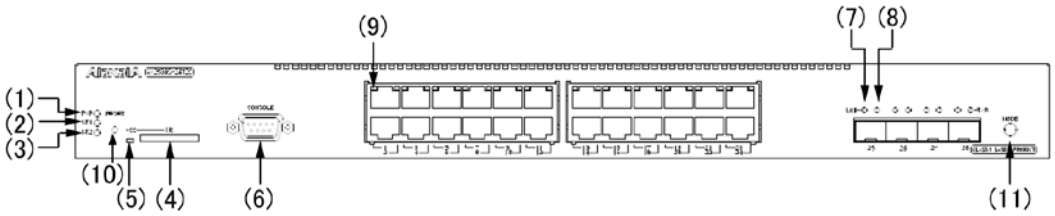


Table 1-1 LED indications, buttons, and connectors

No.	Name	Type	Description	Details
(1)	PWR	LED: Green	Indicates power supply status.	Lit in green: Power is on. Green, slowly blinking: The Switch is in the sleep state. Off: Power off or failure in the power supply unit
(2)	ST1	LED: Green, orange, or red	Indicates the Switch status.	Lit in green: Operation is possible. Blinking green: Getting ready (startup) Blinking green at long intervals: LED operation OFF setting Lit in orange: Initial state at power-up Blinking red: Partial failure in the device Lit in red: Fatal failure in the device (operation cannot continue) Off: Power off or failure in the power supply unit
(3)	ST2	LED: Green or orange	Indicates the SML operation status.	Lit in green: SML full Blinking green: SML conflict or SML standalone Lit in orange: Initial state at power-up Off: Normal operation (SML disabled)
(4)	MC	Connector	Memory card slot	Memory card slot
(5)	ACC	LED: Green	Indicates the memory card status.	Lit in green: The memory card is being accessed. Do not remove the memory card. Off: The memory card is idle. The memory card can be inserted or removed.
(6)	CONSOLE	Connector	CONSOLE port	RS232C port to connect a console terminal
(7)	LINK	LED: Green or orange	Indicates the operating status of an SFP (1000BASE-X)	Lit in green: Initial state at power-up, or a link has been established. Lit in orange: Detecting line disturbances Off: Link failure or block when the green ST1 LED is lit

No.	Name	Type	Description	Details
(8)	T/R	LED: Green	Ethernet port.	Blinking green: A frame is being transmitted.
(9)	1-24	LED: Green or orange	Indicates the operating status of the 10/100/1000BASE-T Ethernet port.	Lit in green: A link is established. Blinking green: A link is established and frames are being sent or received Lit in orange: Initial state at power-up Off: Link failure or block when the green ST1 LED is lit
(10)	RESET	Button (non-locking)	Manual reset button of the Switch[#1]	Restarts the device. When pressed continuously until all LEDs on the front panel are lit (3 seconds or more), the Switch is released from sleep mode.
(11)	MODE	Button (non-locking)	Not supported	––

#1

The button is behind the front panel. Use a screwdriver with a small head to press the button.

Figure 1-1 and Table 1-1 describe a typical switch. For details about a specific switch, see the *Hardware Instruction Manual* for the switch.

1.3 Overview of analyzing failures of functionality

The following table provides an overview of analyzing functional failures on a Switch.

Table 1-2 Status of functional failures and where to find information

Category	Sub-category	Reference
Forgotten login password	Forgotten login user password	*3.1.1 Forgotten login user password*
		3.1.2 Forgotten device administrator password
Operation terminal problems	Data cannot be input from or displayed in the console.	*3.2.1 Information cannot be entered from the console or does not display correctly*
	Remote login to the switch not possible	*3.2.2 Login from a remote operation terminal is not possible*
	Login authentication not possible	*3.2.3 Login authentication using RADIUS is not possible*
	Commands cannot be entered	*3.2.4 Commands cannot be entered*
Problems occurring while saving files	Copying data to the startup configuration file not possible	*3.3.1 Information cannot be saved in the startup configuration file*
	Copying data to a memory card not possible	*3.3.2 Copying or writing information to a memory card is not possible*
	Copying data to the RAMDISK not possible	*3.3.3 Copying or writing information to the RAMDISK is not possible*
	Updates by using the `ppupdate` operation command are not possible	*3.3.4 Update by using the "ppupdate" operation command is not possible*
	Restoring data by using the `restore` operation command is not possible	*3.3.5 Restoring data by using the "restore" operation command is not possible*
	Saving or restoring the binding database is not possible	*3.3.6 Saving or restoring the binding database is not possible*
Network interface communication failures	Ethernet port communication failure	*3.4.1 Ethernet port cannot be connected*
	10BASE-T/100BASE-TX/1000BASE-T communication failure	*3.4.2 Actions to be taken for 10BASE-T/100BASE-TX/1000BASE-T problems*
	100BASE-FX/1000BASE-X communication failure	*3.4.3 Actions to be taken for 100BASE-FX [24S4X]/1000BASE-X problems*
	10GBASE-R communication failure	*3.4.4 Actions to be taken for 10GBASE-R problems [10G models]*

Category	Sub-category	Reference
	Directly attached cable communication failure	*3.4.5 Actions to be taken for direct attach cable problems [10G models]*
	Link aggregation failure	*3.4.6 Communication failures when link aggregation is used*
Layer 2 network communication failures	VLAN failure	*3.5.1 Layer 2 communication by VLANs is not possible*
	Spanning Tree failure	*3.5.2 Failures occurring when the Spanning Tree functionality is used*
	Ring Protocol failure	*3.5.3 Failures occurring when the Ring Protocol functionality is used*
	DHCP snooping failure	*3.5.4 Failures when the DHCP snooping functionality is used*
	IGMP snooping failure	*3.5.5 Multicast forwarding by IGMP snooping is not possible*
	MLD snooping failure	*3.5.6 Multicast forwarding by MLD snooping is not possible*
IPv4 network communication failures	Communication not possible	*3.6.1 Communication is not possible or is disconnected*
	IP addresses cannot be assigned by the DHCP server	*3.6.2 Communication failures occurring when the DHCP server is used*
IPv6 network communication failures	Communication not possible	*3.7.1 Communication is not possible or is disconnected*
Layer 2 authentication communication failures	--	*3.8.1 Communication failures occurring when IEEE 802.1X is used*
	--	*3.8.2 Communication failures occurring when Web authentication is used*
	--	*3.8.3 Communication failures occurring when MAC-based authentication is used*
	--	*3.8.4 Communication failures occurring when secure Wake-on-LAN is used [OS-L2A]*
Communication failures in the high-reliability functionality based on a redundant configuration	Uplink redundancy failure	*3.9.1 Communication failures occurring when uplink redundancy is used*
	SML failure	*3.9.2 Communication failures occurring when SML is used* [OS-L2A]
SNMP communication failures	The MIB cannot be obtained.	*3.10.1 MIBs cannot be obtained from the SNMP manager*

Category	Sub-category	Reference
	Traps cannot be received.	*3.10.2 Traps cannot be received by the SNMP manager*
	SNMPv3 cannot be used.	*3.10.3 When SNMPv3 cannot be used*
sFlow statistics failures	sFlow packets cannot be sent.	*3.11.1 sFlow packets cannot be sent to the collector*
	Flow samples cannot be sent.	*3.11.2 Flow samples cannot be sent to the collector*
	Counter samples cannot be sent.	*3.11.3 Counter samples cannot be sent to the collector*
Neighboring device information cannot be obtained by the LLDP functionality	--	*3.12.1 Neighboring device information cannot be obtained by the LLDP functionality*
NTP communication failures	--	*3.13 NTP communication failures*
Communication failures when the IEEE 802.3ah/UDLD functionality is used	Port in inactivate status	*3.14.1 Port is in inactivate status by the IEEE 802.3ah/UDLD functionality*
Communication failures caused by discarded packets	--	*3.15.1 Checking the filters and QoS control configuration information*
Port mirroring failures	--	*3.16 Port mirroring failures*
Power saving functionality failures	--	*3.17.1 LED brightness control is disabled*
	--	*3.17.2 Power saving scheduling is disabled*
Problems related to the support regarding long life solutions	--	*3.18.1 Dates are not displayed correctly in temperature history information*
Other cases	--	Check the settings again by referring to the configuration guides.

2. Troubleshooting Switch Failures

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

2.1 Procedure for handling Switch faults

2.1.1 Procedure for handling Switch faults

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

Table 2-1 Troubleshooting Switch failures

No.	Problem	Action
1	● Smoke emanates from the Switch. ● An abnormal odor emanates from the Switch. ● An abnormal sound emanates from the Switch.	Immediately take the following actions: 1. Turn off the Switch. 2. Remove the power cable from the Switch. After completing the above procedure, replace the Switch.
2	The login prompt does not appear.	1. If a memory card has been inserted, remove the card, and turn the Switch off and then on again to restart the Switch. 2. If a memory card has not been inserted, turn the Switch off and then on again to restart the Switch. 3. If restarting the Switch does not solve the problem, replace the Switch.
3	The PWR LED of the Switch is off.	Follow the procedure shown below: 1. Perform the steps shown in *Table 2-2 Isolating the cause of power failures*. 2. If the above step fails to isolate the problem, restart the Switch, and then check whether there are any problems in the environment. (1) Turn the Switch off and then on again to restart the Switch. (2) If you can restart the Switch, execute the `show logging` operation command to check the failure information, and then take an appropriate action. `>show logging` (3) If step (1) above fails to restart the Switch, a Switch failure has occurred. In this case, replace the Switch.
4	The red ST1 LED of the Switch is on.	A Switch failure might have occurred. Collect Switch information using the show `tech-support` operation command as described in *4. Obtaining Failure Information*. After collecting the information, restart the Switch to check whether there are any problems with the Switch. 1. Turn the Switch off and then on again to restart the Switch. 2. If you can restart the Switch, execute the `show logging` operation command to check the failure information. `>show logging` 3. If the failure information contains a high-temperature warning message, the operating environment might be the cause of the problem. Ask the system administrator to improve the environment. 4. If you cannot restart the Switch in step 1, or if failure information cannot be obtained in step 3 or does not contain a high-temperature warning message, a

No.	Problem	Action
		failure has occurred on the Switch. In this case, replace the Switch.
5	The red ST1 LED of the Switch blinks. The LINK LED (10GBASE-R port [10G models] and 1000BASE-X port) and the 1-48 LED (10/100/1000BASE-T port) of ports on the Switch are lit in orange or off.	A problem has occurred on the Switch or line. 1. Check the error message and take appropriate action. Use the `show logging` command to check the failure information and take action. `>show logging` If a failure has occurred on an external power unit (EPU), identify the problem by referring to *2.1.2 Isolating the cause of external power unit failures*.
6	The ST2 LED of the Switch is blinking green.	See *3.9.2 Communication failures occurring when SML is used* [OS-L2A].
7	LED indications of the Switch and EPU show no abnormality, but the device administrator command displays `EPU:notconnect`.	Make sure that the cable is properly connected between the Switch and EPU. If the cable is disconnected, follow the procedure below to restart the Switch: 1. Turn off the Switch. 2. Properly connect the disconnected cable. 3. Turn on the Switch.

Table 2-2 Isolating the cause of power failures

No.	Problem	Action
1	The power switch of the Switch is off.	Turn the power switch on.
2	The power cable is disconnected or loose.	Perform the following procedure: 1. Turn the power switch off. 2. Connect the power cable correctly. 3. Turn the power switch on.
3	The measured input power supply is outside the following range: For 100 V AC: 90 to 127 V AC For 200 V AC: 180 to 254 V AC For -48 V DC: -40.5 to -57 V DC Note: Take this action only if the input power supply can be measured.	Ask the person responsible for the facility where the switch is housed to take action regarding the input power supply.

2.1.2 Isolating the cause of external power unit failures

Use the procedure described below to isolate the cause of the failure if a failure occurs on an EPU.

Table 2-3 Isolating the cause of external power unit failures

No.	Problem	Action
1	The POWER LED of the EPU is lit in green.	Identify the power supply module that is not operating properly by checking the LEDs of the power supply modules mounted on the EPU. When power supply modules are operating properly, the following conditions apply: ● For EPU-A and EPU-D DC-OK: Lit in green, DC-ALM: Off Perform the steps shown in *Table 2-6 Isolating the cause of power supply module failures* on the power supply module that is not operating properly.
2	The POWER LED of the EPU is off.	Perform the steps shown in the tables below to isolate the cause of the failure. ● For EPU-A *Table 2-4 Isolating the cause of external redundant power unit (EPU-A) hardware failures* ● For EPU-D *Table 2-5 Isolating the cause of external redundant power unit (EPU-D) hardware failures*

Table 2-4 Isolating the cause of external redundant power unit (EPU-A) hardware failures

No.	Problem	Action
1	The power switch of the external redundant power unit (EPU-A) is off.	Turn the main power switch on.
2	The power cable of the external redundant power unit (EPU-A) is not correctly connected to the switch.	1. Turn the main power switch off. 2. Connect the power cable correctly. 3. Turn the main power switch on.
3	The input power supply to the external redundant power unit (EPU-A) is outside the following range: (AC power supply: 90 to 132 V)	This is a power facility failure (not a Switch failure). Ask the system administrator to take action.
4	Failure other than the above	Replace the external redundant power unit (EPU-A).

Table 2-5 Isolating the cause of external redundant power unit (EPU-D) hardware failures

No.	Problem	Action
1	The main power switch of the external redundant power unit (EPU-D) is off.	Turn the main power switch on.

No.	Problem	Action
2	The power cable of the external redundant power unit (EPU-D) is not correctly connected to the switch.	1. Turn off the circuit breaker at the supply of power. 2. Turn the main power switch off. 3. Connect the power cable correctly. 4. Turn on the circuit breaker at the supply of power. 5. Turn the main power switch on.
3	The input power supply to the external redundant power unit (EPU-D) is outside the following range: (-48 V DC: -40.5 to -57 V DC)	This is a power facility failure (not a Switch failure). Ask the system administrator to take action.
4	Failure other than the above	Replace the external redundant power unit (EPU-D).

Table 2-6 Isolating the cause of power supply module failures

No.	Problem	Action
1	The power switch of the power supply module is off.	Set the power switch of the power supply module to ON.
2	The power cable of the power supply module is not correctly connected to the switch.	1. Set the power switch of the power supply module to OFF. 2. Connect the power cable correctly. 3. Set the power switch of the power supply module to ON.
3	The power supply module is not properly installed on the EPU.	1. Turn the power switch off. 2. Install the power supply module correctly. 3. Turn the power switch on.
4	Failure other than the above	Replace the power supply module.

2.1.3 Replacing the switch and optional modules

The procedure to replace the switch and optional modules[#] is described in the *Hardware Instruction Manual*. Follow the instructions in the manual.

#: Optional modules include the following:

Transceiver (SFP, SFP+), direct attach cable, EPU, power supply module, and memory card

3. Troubleshooting Functional Failures During Operation

This chapter describes what actions to take when a problem occurs, such as when a Switch does not operate correctly or cannot communicate.

3.1 Login-related problems

3.1.1 Forgotten login user password

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

(1) If another user can log in:

Ask the user who can log in to execute the `password` operation command in administrator mode to reset the forgotten login user password. Alternatively, ask the user to use the `clear password` operation command to delete the password.

Execute these commands in administrator mode. Therefore, the user who logs in must know the password for the `enable` operation command for changing the input mode to administrator mode.

The following figure shows an example of resetting the forgotten password for user1 in administrator mode.

Figure 3-1 Example of resetting the password for user1

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

(2) If no users can log in:

If no user can log in or if a user can log in but does not know the password for the `enable` operation command, take the following steps:

1. Restart the Switch, and then press and hold down **Ctrl**+**N** until `login` is displayed on the console.

   By doing so, the startup configuration file and the login user information are not loaded.

2. When the Switch has restarted, the user can use the login user ID `operator` to log in to the Switch.

3. After logging in to the Switch, use the `adduser` operation command to set the login user ID and password.

4. Restart the Switch.

   The startup configuration file and the set password information are loaded.

3.1.2 Forgotten device administrator password

During operation, if the user forgets the device administrator password and is unable to enter administrator mode, perform the following procedure:

1. Restart the Switch, and then press and hold down **Ctrl**+**N** until `login` is displayed on the console.

   By doing so, the startup configuration file and the password information are not loaded.

2. When the Switch has restarted, use the `password` operation command to set the device administrator password.

3. Restart the Switch.

   The startup configuration file and the set password information are loaded.

3.2 Operation terminal problems

3.2.1 Information cannot be entered from the console or does not display correctly

If a problem occurs during connection to the console, check the problem and take action according to the following table.

Table 3-1 Problems occurring during connection to the console and action to take

No.	Problem	Items to check
1	Nothing is displayed on the screen.	Perform the following procedure: 1. Make sure the ST1 LED on the front panel of the Switch is green. If it is not, see *1.2 Overview of analyzing failures of all or part of the Switch*. 2. Check whether the cables are connected correctly. 3. Make sure an RS232C cross cable is being used. 4. Make sure the communication software settings, including port number, communication speed, data length, parity bit, stop bit, and flow control, are specified as follows: Communication speed: 9600 bits/s (or the set value if you have changed this value) Data length: 8 bits Parity bit: None Stop bit: 1 bit Flow control: None
2	Key entry is not accepted.	Perform the following procedure: 1. Data transmission might have been interrupted by XON/XOFF flow control. End the interruption by pressing **Ctrl+Q**. If the Switch still does not accept entry from the keys after this operation, perform steps 2 and 3. 2. Make sure that the communication software settings are correct. 3. The screen might not be responding because **Ctrl+S** was pressed. Press any key.
3	Unexpected characters are displayed at login	Negotiation with the communication software might not have been performed correctly. Check the communication speed of the communication software by doing the following: 1. If the communication speed of CONSOLE (RS232C) was not specified by using the `config-line` mode of the `line console 0` configuration command, make sure that the communication speed of the communication software is set to 9600 bits/s. 2. If the communication speed of CONSOLE (RS232C) has been set to 1200, 2400, 4800, 9600, or 19200 bits/s by using the `config-line` mode of the `line console 0` configuration command, make sure that the communication speed of the communication software is set correctly.
4	Unexpected characters are displayed when a user ID is being entered.	The communication speed of CONSOLE (RS232C) might have been changed. See No. 3.

No.	Problem	Items to check
5	Login is not possible.	Perform the following procedure: 1. Make sure that the login prompt is displayed on the screen. If it is not, the Switch is starting up. Wait a while. 2. Take the actions specified in *3.1 Login-related problems*. 3. If you still cannot log in after taking the actions described above, the internal flash memory might be corrupted. Try to execute the `format flash` operation command. After you execute the `format flash` operation command, all the previously saved information will be lost. For what information will be lost, see the description of the `format flash` operation command in the manual *Operation Command Reference*.
6	When the communication speed of the communication software is changed after login, unexpected characters are displayed and no commands can be entered.	Despite changing the communication speed of the communication software after login, correct display is not possible. Restore the original communication speed of the communication software.
7	A user wants to use Tera Term Pro to log in, but unexpected characters are displayed during login.	Negotiation with the communication software might not have been performed correctly. See No. 3. Issue a break signal by pressing the **Alt**+**B** keys simultaneously. 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 80 digits by 24 lines to increase the number of characters that can be displayed on one line.
9	Information is not displayed even when you execute an operation command.	Check the message for the command execution result. 1. `Can't execute.`: The execution of the command might have been temporarily disabled. Re-execute the command. 2. `There is no memory.`: Enough temporary memory space might not have been reserved for storing display data. Re-execute the command. If one of the above messages still appears even after you re-execute the command, restart the Switch by executing the `reload` command or by turning the Switch off and then on again.

3.2.2 Login from a remote operation terminal is not possible

If a problem occurs during connection to a remote operation terminal (telnet, FTP, etc.), check the status according to the following table.

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

No.	Problem	Action
1	Remote connection is not possible.	Perform the following procedure: 1. Use the `ping` operation command from a PC or workstation to make sure that a route for remote connection has been established.
2	Login is not possible.	Perform the following procedure: 1. Make sure that the `line vty` configuration command or `ftp-server` has been set. (For details, see the *Configuration Guides*.) 2. Make sure that the terminal you are using has an IP address that is permitted in the access list for the configuration command `line vty` mode. Also, make sure that `deny` is not specified for the IP address set in the configuration command access list. (For details, see the *Configuration Guides.*) 3. Make sure that the maximum number of users who can log in has not been exceeded. (For details, see the *Configuration Guides*.) 4. Check if there are any terminals for which login operation has not been completed. (Login is incomplete if the terminal is waiting for user ID and password entry or if a login attempt has failed.) If such terminals are present, finish the communication software of those terminals. 5. Check if there was any event that might have caused connection from a remote operation terminal to the Switch to be temporarily lost during a login attempt. If a user is logged in and connection from a remote operation terminal to the Switch is lost and then restored, the Switch retains the session information. Due to this, no more users will be able to log in from a remote operation terminal until the TCP protocol of the session times out and the session is disconnected. Although the timeout period of the TCP protocol varies depending on the status of a remote operation terminal or the network, the protocol usually times out after 10 minutes.
3	Key entry is not accepted.	Perform the following procedure: 1. Data transmission might have been interrupted by XON/XOFF flow control. End the interruption by pressing **Ctrl+Q**. If the Switch still does not accept entry from the keys after this operation, perform steps 2 and 3. 2. Make sure that the communication software settings are correct. 3. The screen might not be responding because **Ctrl+S** was pressed. Press any key.
4	A user remains logged in.	Wait until the user is automatically logged out (a maximum of 60 minutes). If you were editing the configuration, log in to the Switch again and enter configuration mode to save the configuration, and then finish editing.

3.2.3 Login authentication using RADIUS is not possible

If a login cannot be authenticated by using RADIUS, check the following.

(1) Communication with the RADIUS server

Use the `ping` operation command to check if a connection from the Switch to the RADIUS server has been established. If a connection has not been established, see *3.6.1 Communication is not possible or is disconnected*. If an IP address is specified for the VLAN interface in the configuration, use the `ping` operation command from the IP address to make sure that a connection from the Switch to the RADIUS server has been established.

(2) Settings for the response timeout value and the number of resending attempts

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 it is unable to connect to the RADIUS server is calculated as follows: *<set-response-timeout-value-(in-seconds)>* x (*<set-number-of-resend-attempts>* + 1) x *<set-number-of-RADIUS-servers>*.

If the time increases significantly, an application on a remote operation terminal, such as Telnet, might have terminated due to a timeout. If this occurs, change the RADIUS configuration settings or the timeout setting of an application running on a remote operation terminal. In addition, Telnet or FTP might have failed even when a message indicating successful RADIUS authentication is output to the operation log. In this case, an application running on a remote operation terminal might time out before it can connect to a running RADIUS server of those you specified in the configuration. Change the settings so that a running RADIUS server takes precedence, or decrease the value of *<response-timeout-value-(in-seconds)>* x *<number-of-resend-attempts>*.

3.2.4 Commands cannot be entered

Due to a failure or another reason, if the Switch is restarted, failure information about the Switch is automatically collected (auto-log) two minutes after the restart. During this period, it is not possible to enter a command. Wait a while and try again.

Note, however, that this problem does not occur when the `reload` operation command is executed or the Switch is turned on or off.

3.3 Problems occurring while saving files

3.3.1 Information cannot be saved in the startup configuration file

If a problem such as inability to copy information to the startup configuration file by using an operation command occurs, check the status according to the following table.

Table 3-3 Problems occurring while copying information to the startup configuration file and action to take

No.	Items to check and commands	Items to check
1	Check the response message to the command.	If `Can't execute.` is displayed, do the following: 1. Make sure the specified file exists. 2. Make sure the name of the specified file is correct. 3. For all other cases, see No. 2.
2	Try to execute the `format flash` operation command.	Perform the following procedure: 1. Use the `format flash` operation command to format the file system. When `Flash format complete.` indicating successful formatting is displayed, specify the configuration again, and then save it to the startup configuration file. After you execute the `format flash` operation command, all the previously saved information will be lost. For what information will be lost, see the description of the `format flash` operation command in the manual *Operation Command Reference*. 2. If a message other than `Flash format complete.` is displayed, the file system might be corrupted.

3.3.2 Copying or writing information to a memory card is not possible

If an operation command-related problem such as inability to copy information to a memory card occurs, take action according to the following table.

Table 3-4 Problems occurring while copying information to a memory card and action to take

No.	Items to check and commands	Items to check
1	Check the response message to the command.	Perform the following procedure: 1. If `MC is not inserted.` is displayed, no memory card is inserted. Insert a memory card. 2. If `Can't access to MC by write protection.` is displayed, the memory card is write-protected. Remove the memory card, and slide the write-protect switch (▼Lock) in the opposite direction to enable writing to the memory card. 3. If `No enough space on device.` is displayed, capacity on the memory card is insufficient. Use the `del` operation command to delete unnecessary files, and then re-execute the operation. 4. If `Can't execute.` is displayed, see No. 2.
2	Use the `show ramdisk-file` operation command to check the file on the RAMDISK.	Perform the following procedure: 1. Make sure the specified file exists. 2. Make sure the name of the specified file is correct. 3. If the problem is not resolved by the above two actions, see No. 3.

No.	Items to check and commands	Items to check
3	Try to execute the `format mc` operation command.	Perform the following procedure: 1. When only the prompt without any message is displayed, memory card formatting has terminated normally. Try to write the specified file to the memory card again. 2. If `Can't gain access to MC.` is displayed, remove the memory card, and then make sure that no dust is on the memory card or in the slot. If there is dust, wipe it off with a dry cloth, and then insert the memory card into the slot again. After inserting the memory card, execute the `format mc` operation command again. 3. If `Can't execute.` is displayed, remove the memory card, and then make sure no dust is on the memory card or in the slot. If there is dust, wipe it off with a dry cloth, and then insert the memory card into the slot again. After inserting the memory card, execute the `format mc` operation command again. If the same message appears again, the memory card might have been corrupted. Replace it with another memory card.

3.3.3 Copying or writing information to the RAMDISK is not possible

If an operation command-related problem such as inability to copy information to the RAMDISK occurs, check the status according to the following table.

Table 3-5 Problems occurring while copying information to the RAMDISK and action to take

No.	Items to check and commands	Items to check
1	Check the response message to the command.	Perform the following procedure: 1. Make sure the specified file exists. 2. Make sure the name of the specified file is correct. 3. If `Not enough space on device.` is displayed, see No. 2.
2	Execute the `show ramdisk` operation command to check the RAMDISK status.	Perform the following procedure: 1. Make sure the amount of space in the `free` section displayed by executing the `show ramdisk` operation command is sufficient. If the available space is insufficient, execute the `del` operation command to delete unnecessary files. 2. To copy the configuration file, make sure there is at least 1 MB of free space. 3. To execute the `show tech-support ramdisk` command to save Switch information to the RAMDISK, execute the `del` command to delete unnecessary files. 4. For all other cases, see No. 3.
3	Try to execute the `format flash` operation command.	Perform the following procedure: 1. Use the `format flash` operation command to format the file system. When `Flash format complete.` indicating successful formatting is displayed, specify the configuration again, and then save it to the startup configuration file. After you execute the `format flash` operation command, all the previously saved information will be lost. For what information will be lost, see the description of the `format flash` operation command in the manual *Operation Command Reference*. 2. If the formatting has not been successful, the file system might be corrupted.

3.3.4 Update by using the "ppupdate" operation command is not possible

Check the following:

1. Check whether the update file specified by using the `ppupdate` operation command is applicable for the Switch.
   - Make sure that the update file is appropriate for AX2500S series switches.
   - Make sure that the version of the update file is appropriate to the Switch model to be updated.
   - Check the update file, and then execute the `ppupdate` operation command again.
2. When `FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]` is obtained by the `show logging` operation command:
   - Execute the `ppupdate` operation command again. If an error still occurs, the internal flash memory might be corrupted. Replace the Switch.

3.3.5 Restoring data by using the "restore" operation command is not possible

Check the following:

1. Check if the backup file has been created on the same Switch model as the one for which data is to be restored.
   - To check the model name of the Switch, refer to the `Model` value displayed by using the `show version` operation command.
   - If `no-software` is specified for the `backup` operation command, `no-software` must be specified for the `restore` operation command as well.
   - Make sure that the version of the software at the time when the backup file was created is appropriate for the Switch for which data is to be restored. If the backup file contains a software version not supported by the target Switch model, data cannot be restored. If `no-software` is specified, all non-software backup data is restored.
   - After checking the backup file, execute the `restore` operation command again.
   - If the error still occurs, the backup file might be corrupted.
2. When `FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]` is obtained by the `show logging` operation command:
   - Execute the `restore` operation command again. If an error still occurs, the internal flash memory might be corrupted. Replace the Switch.

3.3.6 Saving or restoring the binding database is not possible

For the actions to be taken when the binding database used for DHCP snooping cannot be saved or restored, see *3.5.4 Failures when the DHCP snooping functionality is used*.

3.4 Network interface communication failures

3.4.1 Ethernet port cannot be connected

If it is possible that the Ethernet port caused the communication failure, check the port status as described below.

(1) Checking the port status

Use the `show port` operation command to check the port status. The following table describes the actions to be taken for the port status.

Table 3-6 Checking the port status and action to take

No.	Port state	Cause	Action
1	`up`	The target port is operating normally.	None
2	`down`	A line failure has occurred on the target port.	Based on the log entry for the target port displayed by the `show logging` operation command, see *Message and Log Reference* and take the action described in *Action*.
3	`inact`	The port is in inactive status due to one of the following reasons: ● `inactivate` operation command ● The standby link functionality of link aggregation ● The BPDU guard functionality of a Spanning Tree Protocol ● Failure detection in the IEEE 802.3ah/UDLD functionality ● The port is deactivated by the L2 loop detection functionality. ● The port is deactivated by the storm control functionality. ● SML (Split Multi Link) functionality	● If the port is deactivated by the standby link functionality of the link aggregation, this is a normal operating status. Do not activate the port by using the `activate` operation command. Use the `show channel-group` operation command with the `detail` parameter to check the standby link functionality. ● If the port is deactivated by the BPDU guard functionality of a Spanning Tree Protocol, check the settings of the partner switch, modify the configuration so that the Switch does not receive BPDUs, and use the `activate` operation command to activate the target port. Use the `show spanning-tree` operation command with the `detail` parameter to check the BPDU guard functionality. ● If the port is deactivated due to the unidirectional link failure detection or L2 loop detection in the IEEE 802.3ah/UDLD functionality, see *3.14 Communication failures in the IEEE 802.3ah/UDLD functionality*. After restoration from the failure, use the `activate` operation command to activate the target port. ● If the port is deactivated by the L2 loop detection functionality, modify the configuration in which the loop occurs, and then use the `activate` operation command to activate the target port. Also, if `loop-detection auto-restore-time` is specified by a configuration command, the port will automatically return to the active status. ● If the port is deactivated by the storm control functionality, after the LAN is restored from the storm, use the `activate` operation command to activate the target port. ● If the port is deactivated by the SML functionality,

No.	Port state	Cause	Action
			see *3.9.2 Communication failures occurring when SML is used* [OS-L2A]. ● If any of the reasons described above do not apply and you want to activate the port, make sure the cable is connected to the target port, and then use the `activate` operation command to activate the target port.
4	`test`	A line test is being performed at the port by the `test interfaces` operation command.	To resume the communication, use the `no test interfaces` operation command to stop the line test, and then use the `activate` operation command to activate the target port.
5	`fault`	The port hardware at the target port causes the failure.	Based on the log entry for the target port displayed by the `show logging` operation command, see *Message and Log Reference* and take the action described in *Action*.
6	`init`	The target port is being initialized.	Wait until the initialization is complete.
7	`dis`	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.

3.4.2 Actions to be taken for 10BASE-T/100BASE-TX/1000BASE-T problems

If a 10BASE-T/100BASE-TX/1000BASE-T problem occurs, use the procedure below to isolate the failure.

1. Viewing logged data

   For details about the information in the operation 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.

Table 3-7 Failure analysis method for 10BASE-T/100BASE-TX/1000BASE-T problems

No.	Items to check	Cause	Action
1	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below for the target line. If there is a count, see the *Cause* and *Action* columns. ● Link down	Line quality is degraded.	Check the cable type. For the cable types, see the *Hardware Instruction Manual*.
			If the Switch is set as follows, make sure that the pin mapping is for MDI-X: ● A fixed connection is set for the target port. ● Auto-negotiation is enabled and the automatic MDIX functionality is disabled for the target port.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.

No.	Items to check	Cause	Action
			Check whether the cables are connected correctly. For cable connections, see the *Hardware Instruction Manual*.
			Replace with the connection interface supported by the Switch. For the connection interfaces supported by the Switch, see the *Hardware Instruction Manual* and the *Configuration Guides*.
			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` operation command, and take the action described in *Action*. For the test types to be specified, see *5.1 Testing a line*.
2	Use the `show interfaces` operation command to display the receive-error statistics, and check whether there is a count for the item shown below for the target line. If there is a count, see the *Cause* and *Action* columns. ● CRC errors ● Symbol errors	Line quality is degraded.	Check the cable type. For the cable types, see the *Hardware Instruction Manual*.
			If the Switch is set as follows, make sure that the pin mapping is for MDI-X: ● A fixed connection is set for the target port. ● Auto-negotiation is enabled and the automatic MDIX functionality is disabled for the target port.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly. For cable connections, see the *Hardware Instruction Manual*.
			Replace with the connection interface supported by the Switch. For the connection interfaces supported by the Switch, see the *Hardware Instruction Manual* and the *Configuration Guides*.
			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` operation command, and take the action described in *Action*. For the test types to be specified, see *5.1 Testing a line*.
3	Use the `show interfaces` operation command to check the line type and line speed on the target line. If the line type or speed is invalid, see the *Cause* and *Action* columns.	The cable is not compatible.	Check the cable type. For the cable types, see the *Hardware Instruction Manual*.
		The values specified for the `speed` and `duplex` configuration commands are different from those on the remote device.	For the `speed` and `duplex` configuration commands, specify the same values that are on the remote device.
		Other than the above	To use a specific speed in auto-negotiation, set the line speed for auto-negotiation. For details, see the *Configuration Guides*.

No.	Items to check	Cause	Action
4	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below 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.

3.4.3 Actions to be taken for 100BASE-FX [24S4X]/1000BASE-X problems

If a 100BASE-FX [24S4X]/1000BASE-X problem occurs, use the procedure below to isolate the failure.

1. Viewing logged data

   For details about the information in the operation 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.

Table 3-8 Failure analysis method for 100BASE-FX [24S4X]/1000BASE-X problems

No.	Items to check	Cause	Action
1	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below for the target line. If there is a count, see the *Cause* and *Action* columns. ● Link down	Line quality on the receiving side is degraded.	Check the type of the optical fiber.
			If an optical attenuator is used, check the attenuation value.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cable is connected correctly (for example, check for incomplete insertion). For cable connections, see the *Hardware Instruction Manual*. Make sure that the end sections of the cables are clean. If they are dirty, clean them.
			Check whether the transceiver (SFP) is connected correctly (for example, check for incomplete insertion).
			Comply with the segment standard of the remote device.
			Check whether the optical level is correct.
			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` operation command, and take the action described in *Action*. For the test types to be specified, see *5.1 Testing a line*.

No.	Items to check	Cause	Action
2	Use the `show interfaces` operation command to display the receive-error statistics, and check whether there is a count for the item shown below for the target line. 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.
			If an optical attenuator is used, check the attenuation value.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly. For cable connections, see the *Hardware Instruction Manual*. Make sure that the end sections of the cables are clean. If they are dirty, clean them.
			Check that the transceiver (SFP) is connected correctly.
			Comply with the segment standard of the remote device.
			Check whether the optical level is correct.
			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` operation command, and take the action described in *Action*. For the test types to be specified, see *5.1 Testing a line*.
3	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below 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.
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	[24S4X] When 100BASE-FX is used, execute the `show interfaces` operation 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 settings specified for the `speed` and `duplex` configuration commands are invalid.	Use configuration commands to specify the following settings: speed: 100 duplex: full

No.	Items to check	Cause	Action
6	If the LINK LED of the port is blinking green, check the status of the cable and transceiver.	The link-up and link-down of a port are detected frequently.	Check the type of the optical fiber.
			Check whether the cables are connected correctly. For cable connections, see the *Hardware Instruction Manual*. Make sure that the end sections of the cables are clean. If they are dirty, clean them.
			Check that the transceiver (SFP) is connected correctly.

3.4.4 Actions to be taken for 10GBASE-R problems [10G models]

If a 10GBASE-R problem occurs, use the procedure below to isolate the failure.

1. Viewing logged data

   For details about the information in the operation 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.

Table 3-9 Failure analysis method for 10GBASE-R problems [10G models]

No.	Items to check	Cause	Action
1	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below for the target line. If there is a count, see the *Cause* and *Action* columns. ● Link down	Line quality on the receiving side is degraded.	Check the type of the optical fiber.
			If an optical attenuator is used, check the attenuation value.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cable is connected correctly (for example, check for incomplete insertion). For cable connections, see the *Hardware Instruction Manual*. 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 example, check for incomplete insertion).
			Adjust the transceiver to comply with the segment standard of the remote device.
			Check whether the optical level is correct.
			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` operation command, and take the action described in *Action*. For the test types to be specified, see *5.1 Testing a line*.

No.	Items to check	Cause	Action
2	Use the `show interfaces` operation command to display the receive-error statistics, and check whether there is a count for the item shown below for the target line. If there is a count, see the *Cause* and *Action* columns. ● CRC errors	Line quality on the receiving side is degraded.	Check the type of the optical fiber.
			If an optical attenuator is used, check the attenuation value.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly. For cable connections, see the *Hardware Instruction Manual*. 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.
			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` operation command, and take the action described in *Action*. For the test types to be specified, see *5.1 Testing a line*.
3	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below 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.

3.4.5 Actions to be taken for direct attach cable problems [10G models]

If a direct attach cable problem occurs, use the procedure below to isolate the failure.

1. Viewing logged data

   For details about the information in the operation 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.

Table 3-10 Failure analysis method for direct attach cable problems [10G models]

No.	Items to check	Cause	Action
1	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below for the target line. If there is a count, see the *Cause* and *Action* columns. ● Link down	Line quality on the receiving side is degraded.	Check the direct attach cable type. Check whether the cable is connected correctly (for example, check for incomplete insertion). For cable connections, see the *Hardware Instruction Manual*.
2	Use the `show interfaces` operation command to display the receive-error statistics, and check whether there is a count for the item shown below for the target line. If there is a count, see the *Cause* and *Action* columns. ● CRC errors	Line quality on the receiving side is degraded.	Check whether the cable is connected correctly (for example, check for incomplete insertion). For cable connections, see the *Hardware Instruction Manual*.
3	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the item shown below 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.

3.4.6 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.

Table 3-11 Communication failure analysis method when link aggregation is used

No.	Items to check and commands	Action
1	Use the `show channel-group detail` operation command 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, set the same link aggregation mode that is set 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`.

No.	Items to check and commands	Action
2	Use the `show channel-group detail` operation command 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 link aggregation group have gone down, the link aggregation group also goes down.
		● Detached The port went down or is reserved, a port speed mismatch occurred, or half-duplex mode is set.
		● Attached The port is in a transition state or is negotiating.
		● Collecting The port is in a transition state or is negotiating (data can be received).
		● Distributing Data can be sent and received.

3.5 Layer 2 network communication failures

3.5.1 Layer 2 communication by VLANs is not possible

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

(1) Checking the VLAN status

Execute the `show vlan` or `show vlan detail` operation command 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.

(b) For protocol VLANs

- When you are using a protocol VLAN, execute the `show vlan` operation 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   Uplink-VLAN:       Uplink-Block:    Tag-Translation:
       ...
```

(c) For MAC VLANs

- When you are using a MAC VLAN, execute the `show vlan mac-vlan` operation 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.

  `web-auth`: The MAC address is set by the Web authentication functionality.

  `mac-auth`: The MAC address is set by the MAC-based authentication functionality.

```
# show vlan mac-vlan
       ...
VLAN ID:100     MAC Counts:4
    0012.e200.0001 (static)        0012.e200.00:02 (static)
    0012.e200.0003 (static)        0012.e200.00:04 (dot1x)
```

- Execute the `show vlan mac-vlan` operation 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. A MAC address with an asterisk (*) shown next to it represents an entry that has not been registered in the hardware due to capacity limit.

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

(2) Checking the port status

- Execute the `show vlan detail` operation command and make sure the port status is `Up`. If the status is `Down`, see *3.4 Network interface communication failures*.
- 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 stopped by link aggregation functionality.

`STP`: Transfer has been stopped by the Spanning Tree functionality.

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

`ULR`: Transfer has been suspended by uplink redundancy functionality.

`AXRP`: Transfer has been suspended by the Ring Protocol.

```
> show vlan 2048 detail

Date 2010/08/09 03:21:25 UTC
VLAN counts: 1
VLAN ID: 2048  Type: Port based  Status: Up
       ...
       ...
  Port Information
   0/3          Up   Forwarding      Untagged
   0/4          Up   Forwarding      Untagged
   0/5          Down -               Untagged
   0/6          Down -               Untagged
```

(3) Checking the MAC address table

(a) Checking the status of MAC address learning

- Execute the `show mac-address-table` operation command and check the

information about the destination MAC address that caused the communication failure.

```
> show mac-address-table
Date 2010/08/09 21:30:08 UTC
Aging time : 300
MAC address        VLAN    Type     Port-list
0012.e2cf.fd5d        1    Dot1x    0/6
0012.e203.0110        1    Dynamic  0/15
0012.e203.0132        1    Dynamic  0/49
0012.e27f.fffa        1    Snoop    0/6
0012.e2a5.429c        2    Dynamic  0/24,0/48
0012.e2a5.e756        2    MacAuth  0/50
0012.e2a5.e895     4094    Static   0/24,0/48
0012.e2a5.ee4e     4094    WebAuth  0/5

>
```

- 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` operation 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 *3.5.5 Multicast forwarding by IGMP snooping is not possible* and *3.5.6* Multicast forwarding by MLD snooping is not possible.

  When `Dot1x` is displayed for `Type`:

  See *3.8.1 Communication failures occurring when IEEE 802.1X is used*.

  When `WebAuth` is displayed for `Type`:

  See *3.8.2 Communication failures occurring when Web authentication is used*.

  When `MacAuth` is displayed for `Type`:

  See *3.8.3 Communication failures occurring when MAC-based authentication is used*.

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

(4) Checking filters and QoS control

Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper. Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.

3.5.2 Failures occurring when the Spanning Tree functionality is used

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*.

Table 3-12 Failure analysis method for Spanning Tree Protocols

No.	Items to check and commands	Action
1	Execute the `show spanning-tree` operation command for the Spanning Tree Protocol that caused the failure, and then check the status of the Spanning Tree Protocol.	If the displayed status is `Enable`, go to No. 2.
		If Ring Protocol and PVST+ are used together, but the tree information of the target VLAN is not displayed, go to No. 7.
		If the displayed status is `Disable`, the Spanning Tree Protocol has stopped. Check the following configurations: ● spanning-tree disable ● switchport backup ● system sml peer-link ● system sml domain ● system sml id
		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 limits.
2	Execute the `show spanning-tree` operation 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` operation 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 status of a port for which the loop guard functionality is enabled is `Blocking` or `Discarding`, check whether the port is a designated port. If it is a designated port, delete the setting of the loop guard functionality.
		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.

No.	Items to check and commands	Action
4	Execute the `show spanning-tree statistics` operation command for the Spanning Tree Protocol that caused the failure, and then check whether BPDUs were sent and received on the failed port.	Check the BPDU sending or receiving counter. For a root port: If the BPDU receiving counter has been incremented, go to No. 5. If the counter has not been incremented, BPDUs might have been discarded by either filters or the QoS control shaper. See *3.15.1 Checking the filters and QoS control configuration information* and check for a problem. If you do not find any problems, check the neighboring devices. For a designated port: If the BPDU sending counter has been incremented, go to No. 5. If the counter has not been incremented, see *3.4 Network interface communication failures*.
5	Execute the `show spanning-tree detail` operation command 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 the maximum number of Spanning Tree Protocol, one of which caused the failure, is within the capacity limits.	Set a value within the capacity limits. For details about capacity limits, see the *Configuration Guides*.
7	Make sure that only one VLAN intended to be used in PVST+ mode is set in `vlan-mapping` for Ring Protocol.	Set the target VLAN in `vlan-mapping` for Ring Protocol if not set. If multiple VLANs are set in `vlan-mapping`, specify only one VLAN in the `vlan-mapping` setting.
8	Make sure that VLANs intended to be used in an MST instance are 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.

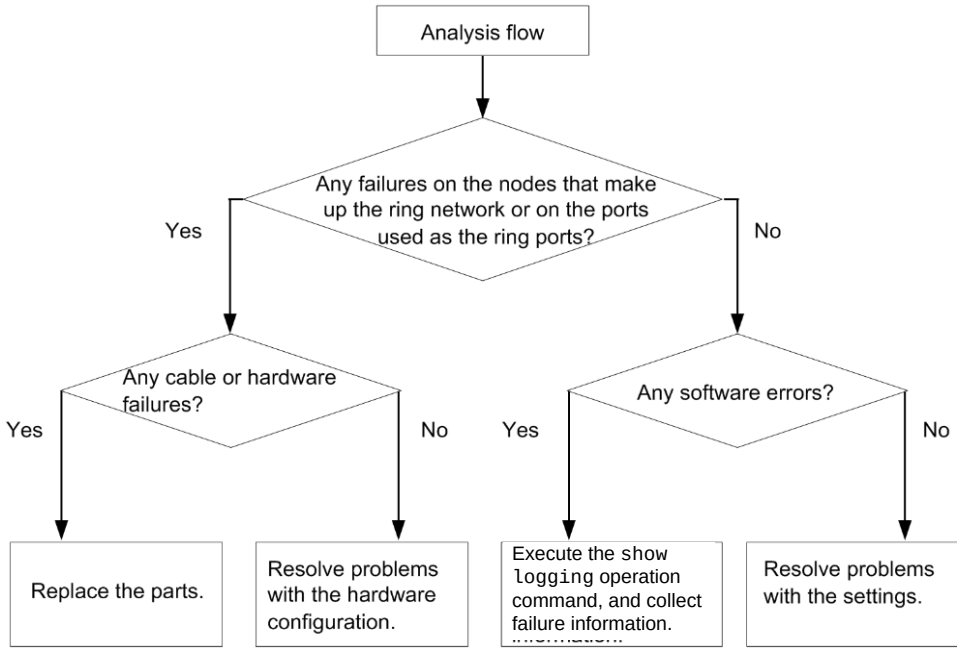
3.5.3 Failures occurring when the Ring Protocol functionality is used

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

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

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

Figure 3-2 Analysis flowchart



If operation cannot be performed correctly or a ring network failure is detected when the Ring Protocol is used, use the failure analysis method described in the table below to isolate the cause of the problem for the relevant node in the target ring network.

The analysis method described in the table below applies to AX2500S series switches. For other AX switch series, see the manuals for the appropriate models.

Table 3-13 Failure analysis method for the Ring Protocol

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

No.	Items to check and commands	Action
4	Use the `show axrp detail` operation command to check the control VLAN ID.	If the VLAN ID defined in the network configuration is displayed for `Control VLAN ID`, go to No. 5.
		If any other information is displayed, check the configuration. For example, the Control VLAN IDs might be different for each device in a ring topology.
5	Use the `show axrp detail` operation command to check the VLAN IDs that belong to the VLAN group.	If the VLAN IDs defined in the network configuration are displayed for `VLAN ID`, go to No. 6.
		If any other information is displayed, check the configuration. For example, the VLAN IDs that belong to the VLAN group might be different for each device in a ring topology.
6	Use the `show axrp detail` operation command to check the timer value of the health-check frame sending interval and that of the health-check frame hold time.	If the Health Check Hold Time timer value of the health-check frame hold time is larger than the Health Check Interval timer value of the health-check frame sending interval (i.e., transmission delay is taken into account), go to No. 7.
		If the timer value of the health-check frame hold time is equal to or smaller than that of the health-check frame sending interval (i.e., transmission delay is not taken into account), check the settings in the configuration.
7	Use the `show vlan detail` operation command to check the state of the VLAN used for the Ring Protocol and the VLAN port states.	If there is no anomaly in the states of the VLAN and its ports, go to No. 8. In addition to the above, go to No. 9 for configurations in which a Spanning Tree Protocol is also used, and go to No. 10 for configurations in which the multi-fault monitoring functionality is applied.
		If there is any anomaly, check the configuration and restore the states of the VLAN and its ports.
8	Check the filters and QoS control configurations.	The control frames used for the Ring Protocol might have been discarded by filters or QoS control. See *3.15.1 Checking the filters and QoS control configuration information* and check for a problem. Also, see the *Configuration Guide*.
9	If Spanning Tree Protocols are set to be used together with the Ring Protocol, check the virtual link settings.	Check whether the virtual link settings in the configuration are the same as those defined in the network configuration. ● Check whether virtual links are set for devices that use Spanning Tree Protocols together with the Ring Protocol. ● For devices in the entire ring network, check whether the VLANs used in the virtual link are included in the VLAN group for the Ring Protocol.
10	If the multi-fault monitoring functionality is applied, use the `show axrp detail` operation command to check the operating mode for the multi-fault monitoring functionality.	If shared nodes have `monitor-enable` configured and other devices have `transport-only` configured, go to No. 11.
		If any other information is displayed, check the configuration.

No.	Items to check and commands	Action
11	Use the `show axrp detail` operation command to check the backup ring IDs and VLAN IDs for the multi-fault monitoring functionality.	If the backup ring ID and the VLAN ID for the multi-fault monitoring functionality defined in the network configuration are displayed for Backup Ring ID and Control VLAN ID, go to No. 12.
		If any other information is displayed, check the configuration.
12	Use the `show axrp detail` operation 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.

3.5.4 Failures when the DHCP snooping functionality is used

(1) When a DHCP client terminal cannot establish communication

If a DHCP client terminal cannot establish communication when the DHCP snooping functionality is used, take action as described in the following table.

Table 3-14 Action to take when a DHCP client terminal cannot establish communication

No.	Items to check and commands	Action
1	Use the `show ip dhcp snooping binding` operation command to check whether the IP address and MAC address for the target terminal are registered in the binding database.	If the addresses are registered, go to No. 4.
		If the addresses are not registered, go to No. 2.
2	Check the connection between the DHCP server and the DHCP client terminal.	Make sure the DHCP server is connected to a trusted port. If the DHCP server is connected to an untrusted port, connect the server to a trusted port.
		Make sure the DHCP client terminal is connected to an untrusted port. If the DHCP client terminal is connected to a trusted port, connect the client to an untrusted port.
		If the connection is correct, go to No. 3.
3	Try to clear the IP address on the DHCP client terminal.	The Switch might have been restarted by, for example, turning the power off and on. Clear the IP address. Example: In Windows, in the Command Prompt window, execute `ipconfig /release` and then `ipconfig /renew`.
4	Make sure the filters and the Layer 2 authentication functionality are configured correctly.	Authentication might have failed because certain packets have been discarded by filters or Layer 2 authentication functionality is used for the port or VLAN to which the terminal is connected. Make sure the setting conditions for filters and the Layer 2 authentication functionality in the configuration are correct.

(2) When the binding database cannot be saved

If the binding database cannot be saved when the DHCP snooping functionality is used, take action according to the tables below.

(a) The database cannot be saved to internal flash memory

Table 3-15 When the save location for the binding database is internal flash memory

No.	Items to check and commands	Action
1	Use the `show ip dhcp snooping binding` operation command to check the time that the database was saved.	If a hyphen (`-`) is displayed for `Agent URL`, go to No. 2.
		Saving data might not have started yet because the wait-to-write time# defined in the configuration has not elapsed since the save event#. Wait a while.
		If the wait-to-write time# has elapsed since the save event#, and if the time displayed for `Last Succeeded time` is one of the following, go to No. 3: - Hyphen (-) - Time before the save event#
2	Use the `show running-config` operation command to check the configuration.	If `ip dhcp snooping database url flash` is set, go to No. 3.
		If `ip dhcp snooping database url flash` is not set, set the `ip dhcp snooping database url flash` configuration command.
3	Use the `show logging` operation command to check the operation log for saving the binding database.	If `It was not able to store binding database in flash.` has been recorded, use the following procedure to change the save location to a memory card (MC). 1. Use the `ip dhcp snooping database url` configuration command to change the save location to the memory card. 2. Use the `save` command to save the configuration. 3. Insert the memory card into the Switch. 4. Restart the Switch. 5. Set internal flash memory as the save location again. 6. Use the `save` command to save the configuration. 7. Restart the Switch. Go to No. 4.
4	After restarting the Switch, use the `show logging` operation command to check the operation log for saving the binding database.	If the status is the same as in No. 3, internal flash memory might be corrupted. Use the following procedure to replace the Switch. 1. Execute the `backup` operation command. (At this time, the file specified for the `backup` operation command and the file specified for the `ip dhcp snooping database url mc` configuration command used in No. 3 will have been saved to the memory card.) 2. Replace the Switch. 3. Insert the memory card into the new Switch. 4. Execute the `restore` operation command. (The data is restored to the switch from the backup created by the backup operation command.) 5. Use the `ip dhcp snooping database url` configuration command to change the save location to the memory card. 6. Use the `save` command to save the configuration. 7. Restart the Switch. The binding database on the memory card is restored.

#

For details about save events and the wait-to-write time, see the *Configuration Guide Vol. 2*.

(b) The database cannot be saved to a memory card

Table 3-16 When the save location for the binding database is a memory card

No.	Items to check and commands	Action
1	Use the `show ip dhcp snooping binding` operation command to check the time that the database was saved.	If a hyphen (`-`) is displayed for `Agent URL`, go to No. 2.
		Saving data might not have started yet because the wait-to-write time# defined in the configuration has not elapsed since the save event#. Wait a while.
		If the wait-to-write time# has elapsed since the save event#, and if the time displayed for `Last Succeeded time` is one of the following, go to No. 3: - Hyphen (-) - Time before the save event#
2	Use the `show running-config` operation command to check the configuration.	If `ip dhcp snooping database url mc` is set, go to No. 3.
		If `ip dhcp snooping database url mc` is not set, set the `ip dhcp snooping database url mc` *<saved file name>* configuration command.
3	Use the `show logging` operation command to check the operation log for saving the binding database.	If `It was not able to store binding database in mc.`*<retry>* *<reason>* has been recorded, the database could not be saved to the memory card.
		If `MC is not inserted.` is displayed for *<reason>*, the memory card might not be inserted or might not be fully inserted. If the memory card is not inserted, insert it. If the memory card is inserted, remove the memory card, and then insert it again until you hear it click. (When inserting the memory card, do not push it with force or flick it.) Go to No. 5.
		If `Can't access to MC by write protection.` is displayed for *<reason>*, the memory card is write-protected. Remove the memory card, slide the write-protect switch (▼Lock) in the opposite direction to enable writing to the memory card, and then insert the memory card into the Switch again. (When inserting the memory card, do not push it with force or flick it.) Go to No. 5.
		If `MC file is not writing.` is displayed for *<reason>*, free space might be insufficient. Go to No. 4.
4	Use the `show mc` operation command to check the amount of free space on the memory card.	If the amount of free space is not more than 1 MB, use the `del` operation command to delete unnecessary files, and then retry the operation. Go to No. 5.

No.	Items to check and commands	Action
5	Execute the `backup` operation command. After the backup process is complete, execute the `show mc-file` operation command.	If the file specified for the `ip dhcp snooping database url mc` configuration command exists in addition to the file specified for the `backup` operation command, the binding database has been saved. If the database has not been saved, the memory card might be corrupted. Go to No. 6.
6	Try to execute the `format mc` operation command.	When only the prompt without any message is displayed, memory card formatting has terminated normally. Take action as described in No. 5.
		If `Can't gain access to MC.` is displayed, remove the memory card and check the memory card and memory card slot for dust. If there is dust, wipe it off with a dry cloth, and then insert the memory card into the slot again. After inserting the memory card, execute the `format mc` operation command again.
		If `Can't execute.` is displayed, remove the memory card and check the memory card and memory card slot for dust. If there is dust, wipe it off with a dry cloth, and then insert the memory card into the slot again. After inserting the memory card, execute the `format mc` operation command again. If the same message appears again, the memory card might have been corrupted. Replace it with another memory card.

#

For details about save events and the wait-to-write time, see the *Configuration Guide Vol. 2*.

(3) When the binding database cannot be restored

If the binding database cannot be restored when the DHCP snooping functionality is used, take action according to the tables below.

(a) Database cannot be restored from internal flash memory

Table 3-17 When the save location for the binding database is internal flash memory

No.	Items to check and commands	Action
1	Use the `show ip dhcp snooping binding` operation command to check the time that the database was saved.	If a hyphen (`-`) is displayed for `Agent URL`, go to No. 2.
		If the time displayed for `Last succeeded time` is too old, go to No. 3.
2	Use the `show running-config` operation command to check the configuration.	If `ip dhcp snooping database url flash` is set, go to No. 3.
		If `ip dhcp snooping database url flash` is not set, set the `ip dhcp snooping database url flash` configuration command.

No.	Items to check and commands	Action
3	Use the `show logging` operation command to check the operation log for restoration of the binding database.	If `It was not able to restore binding database from flash.` has been recorded, restoration has failed. The binding database saved in internal flash memory might be corrupted. Clear the IP addresses on the DHCP client terminal. (In Windows, in the Command Prompt window, execute `ipconfig /release`, and then `ipconfig /renew`.)

(b) The database cannot be restored from a memory card

Table 3-18 When the save location for the binding database is a memory card

No.	Items to check and commands	Action
1	Use the `show ip dhcp snooping binding` operation command to check the time that the database was saved.	If a hyphen (`-`) is displayed for `Agent URL`, go to No. 2.
		If the time displayed for `Last succeeded time` is too old, go to No. 3.
2	Use the `show running-config` operation command to check the configuration.	If `ip dhcp snooping database url mc` is set, go to No. 3.
		If `ip dhcp snooping database url mc` is not set, set the `ip dhcp snooping database url mc` *<saved file name>* configuration command.
3	Use the `show logging` operation command to check the operation log for restoration of the binding database.	If `It was not able to restore binding database from mc.` *<retry>* *<reason>* has been recorded, restoration from the memory card has failed.
		If `MC is not inserted.` is displayed for *<reason>*, the memory card might not be inserted or might not be fully inserted. If the memory card is not inserted, insert it. If the memory card is inserted, remove the memory card, and then insert it again until you hear it click. (When inserting the memory card, do not push it with force or flick it.) Go to No. 4.
		If `MC file is not found.` is displayed for *<reason>*, the inserted memory card does not contain the file, or the memory card contains a file whose name has not been specified by the `ip dhcp snooping database url mc` configuration command. Replace the memory card with the one on which the binding database was saved. Go to No. 4.
		If information other than the above is displayed for *<reason>*, restoration from the memory card has failed. Go to No. 4.

No.	Items to check and commands	Action
4	Restart the Switch.	If `MC file is not reading.` is displayed for *<reason>*, the file saved on the memory card or the memory card itself might be corrupted. Clear the IP addresses on the DHCP client terminal. (In Windows, in the Command Prompt window, execute `ipconfig /release`, and then `ipconfig /renew`.)

3.5.5 Multicast forwarding by IGMP snooping is not possible

If multicast forwarding is not possible when IGMP snooping is used, use the following analysis flowchart to determine the problem and isolate the cause.

Figure 3-3 Analysis flowchart

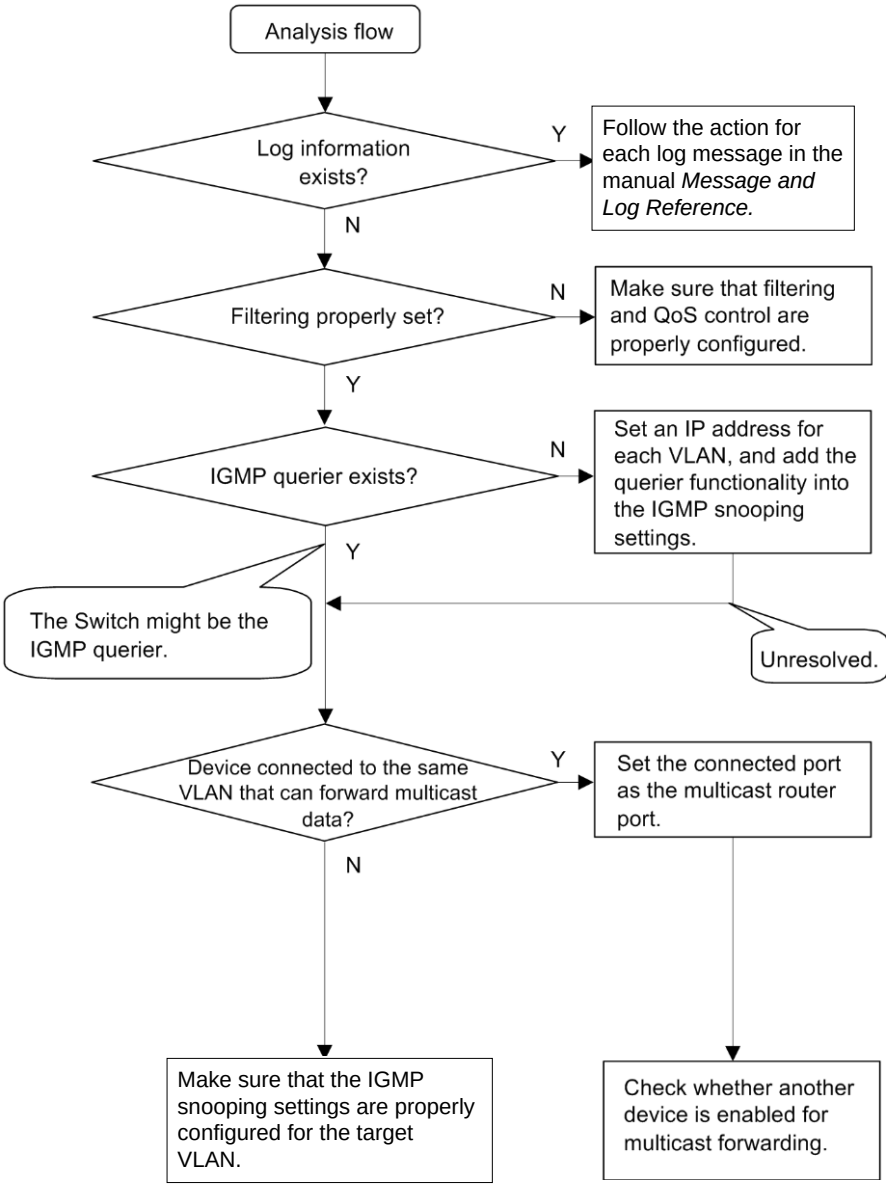


Table 3-19 Failure analysis method for multicast forwarding

No.	Items to check and commands	Action
1	If multicast forwarding is not performed, use the `show logging` operation command to check whether a failure has occurred.	Check the following: - Check whether log information about a physical fault has been recorded.
2	Make sure filters and QoS control are configured correctly.	Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper. Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.

3	If multicast forwarding is not performed, use the `show igmp-snooping` operation command to check the IGMP snooping configuration.	Check the following:
		- To check whether the IGMP querier that monitors the group members exists, make sure one of the following messages is displayed:
		(1) If the IGMP querier exists, the IP address of the IGMP querier is displayed.
		`IGMP querying system: 192.168.11.20#`
		(2) If the IGMP querier does not exist, nothing is displayed for `IGMP querying system:`.
		`IGMP querying system:`
		- If the Switch is the IGMP querier, make sure the IP address has been set for the VLAN.
		(1) If the IP address has been set for the VLAN, the following message is displayed:
		`IP Address: 192.168.11.20#`
		(2) If the IP address has not been set for the VLAN, nothing is displayed for `IP Address:`.
		`IP Address:`
		- If a multicast router is connected, check the `mrouter-port` setting.
		`> show igmp-snooping 3253`
		
		`Date 2010/08/14 15:59:14 UTC`
		`VLAN counts: 3`
		`VLAN 3253:`
		`  IP Address: 192.168.53.100/24   Querier: enable`
		`  IGMP querying system: 192.168.53.100`
		`  Port (4): 0/13-16`
		`  Mrouter-port: 0/13-16`
		`  Group counts: 5`

4	If multicast forwarding is not performed, use the `show igmp-snooping group` operation command to check the IPv4 multicast group address.	Check the following:
		- Make sure the joined IPv4 multicast group address is displayed by the `show igmp-snooping group` command.
		`> show igmp-snooping group 3253`
		
		`Date 2010/08/14 16:02:03 UTC`
		`Total Groups: 15`
		`VLAN counts: 3`
		`VLAN 3253 Group counts: 5`
		`  Group Address     MAC Address`
		`   230.0.0.11        0100.5e00.000b`
		`     Port-list: 0/13`
		`   230.0.0.10        0100.5e00.000a`
		`     Port-list: 0/13`

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

3.5.6 Multicast forwarding by MLD snooping is not possible

If multicast forwarding is impossible when MLD snooping is used, use the following analysis flowchart to determine the problem and isolate the cause.

Figure 3-4 Analysis flowchart

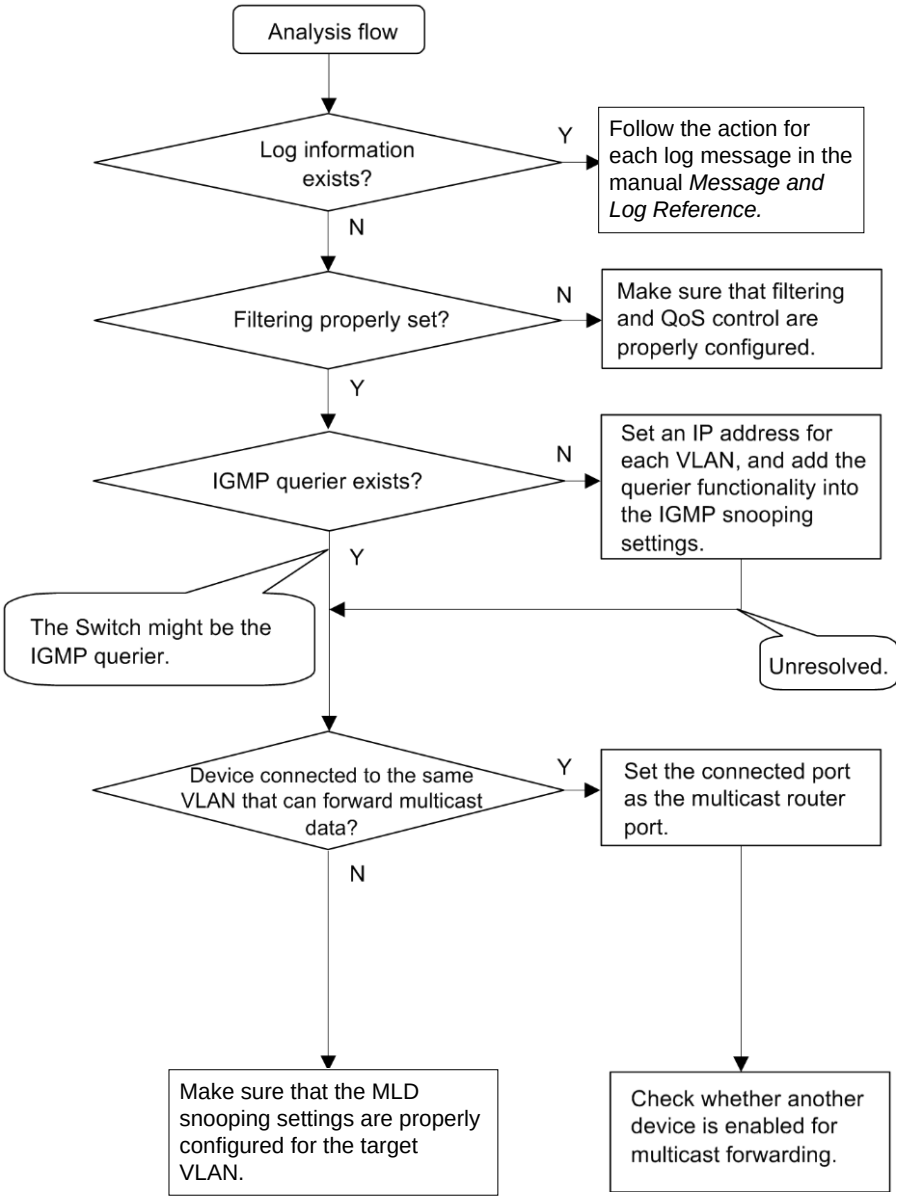


Table 3-20 Failure analysis method for multicast forwarding

No.	Items to check and commands	Action
1	If multicast forwarding is not performed, use the `show logging` operation command to check whether a failure has occurred.	Check the following: - Check whether log information about a physical fault has been recorded.

No.	Items to check and commands	Action
2	Make sure filters and QoS control are configured correctly.	Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper. Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.

3	If multicast forwarding is not performed, use the `show mld-snooping` operation command to check the MLD snooping configuration.	Check the following:
		- To check whether the MLD querier that monitors the group members exists, make sure one of the following messages is displayed:
		(1) If the MLD querier exists, the IP address of the MLD querier is displayed.
		`MLD querying system: ff03::3`
		(2) If the MLD querier does not exist, nothing is displayed for `MLD querying system:`.
		- If the Switch is the MLD querier, make sure the sender IP address has been set by using the `ipv6 mld snooping source` configuration command.
		`MLD querying system:`
		(3) If the sender IP address has not been set by the `ipv6 mld snooping source` configuration command, nothing is displayed for `IP Address`:.
		`IP Address:`
		- If a multicast router is connected, check the `mrouter-port` setting.
		`> show mld-snooping 300`
		
		`Date 2011/06/28 05:40:20 UTC`
		`VLAN counts: 3`
		`VLAN 300:`
		`  IP Address: ff03::3  Querier: enable`
		`  MLD querying system: ff03::3`
		`  Querier version: v1`
		`  Port (2): 0/1,0/7`
		`  Mrouter-port: 0/1`
		`  Group counts: 2`

4	If multicast forwarding is not performed, use the `show mld-snooping group` operation command to check the IPv6 multicast group address.	Check the following:
		- Make sure the joined IPv6 multicast group address is displayed by the `show mld-snooping group` command.
		`> show mld-snooping group 300`
		
		`Date 2011/06/28 05:39:57 UTC`
		`Total Groups: 8`
		`VLAN counts: 3`
		`VLAN 300  Group counts: 2`
		`  Group Address  MAC Address  Version  Mode`
		`  ff03::11  3333.0000.0011  v1  -`
		`  Port-list: 0/7`
		`  ff03::10  3333.0000.0010  v1  -`
		`  Port-list: 0/7`

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

3.6 IPv4 network communication failures

3.6.1 Communication is not possible or is disconnected

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

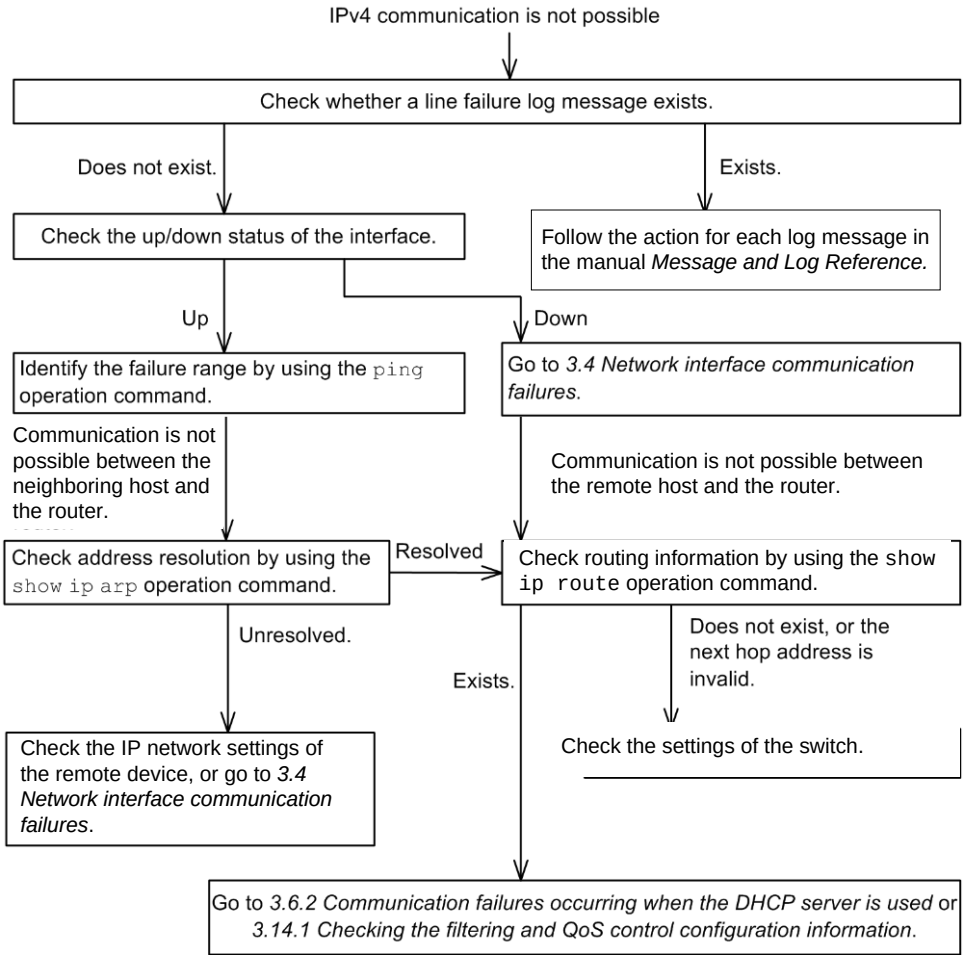
1. A configuration related to IP communication is changed.
2. The network configuration is changed.
3. A network device fails.

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

This subsection describes the procedure for isolating the fault location to 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.

Figure 3-5 Failure analysis procedure when IPv4 communication is not possible



(1) Checking the log

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

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

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

(2) Checking the interface status

Even 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` operation command to check whether the status of the interface with the target neighboring device is `Up` or `Down`.
3. If the status of the target interface is `Down`, see *3.4 Network interface communication failures*.
4. If the status of the target interface is `Up`, see *(3)Identifying the range for a failure (from the Switch)*.

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

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

1. Log in to the Switch.
2. Use the `ping` operation command to check the communication with the two remote devices that are unable to communicate. For details about examples of using the `ping` operation command and how to interpret the execution result, see the *Configuration Guides*.
3. If communication with the remote devices cannot be verified by the `ping` operation 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. If the execution result of the ping operation command indicates that the failure occurred on a neighboring device, see *(5) Checking the ARP resolution information with a neighboring device*. If the execution result indicates a failure on the remote device, see *(6) Checking the unicast routing information*.

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

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

1. Make sure 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` operation 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 the ARP resolution information with a neighboring device

If the execution result of the `ping` operation 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` operation 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 has been resolved (ARP entry information exists), see *(6) Checking the unicast routing information*.
4. If the address has not been resolved (no ARP entry information exists), check whether the IP network settings between the neighboring device and the Switch are identical. Alternatively, see *3.4 Network interface communication failures*.

(6) Checking the unicast routing information

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

1. Log in to the Switch.
2. Execute the `show ip route` operation command to check the routing information obtained by the Switch.
3. If the displayed information contains routing information, check the settings of the IPv4 network interface functionality.
4. If the displayed information does not contain the routing information or contains an incorrect address for the interface's next hop, check the Switch settings.
5. If the routing information obtained by the Switch contains routing information about the interface that caused the communication failure, the interface might have a problem with the functionality shown below. That functionality must be checked.
   - DHCP server functionality

     See *(7) Checking the DHCP server configuration information.*
   - Filter functionality

- *See (8) Checking the filters and QoS configuration information*.

(7) Checking the DHCP server configuration information

If IP addresses for clients are assigned by the DHCP server functionality on the Switch, the IP addresses might have not been properly assigned. Check whether the setting conditions for the DHCP server functionality in the configuration are correct. For details about the procedure, see *3.6.2 Communication failures occurring when the DHCP server is used*.

(8) Checking the filters and QoS configuration information

Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper.

Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.

3.6.2 Communication failures occurring when the DHCP server is used

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

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

First, check for cause 1. Described below are likely examples of incorrect configuration. For cause 2, check the differences in the network configuration before and after the change to uncover any cause that could disable communication. If you have checked the client and server settings (such as network card settings and cable connections) and concluded that cause 3 applies (for example, the configuration and network configuration are correct, but IP communication is not possible due to disabled allocation of IP addresses to clients), see *(b) Checking the operation log and interface* through *(d) Checking the filters and QoS control configuration information*.

(a) Checking the configuration

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

- In the configuration, make sure there is an `ip dhcp pool` setting that contains the network setting for the IP addresses to be assigned to the DHCP clients.
- 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.
- When an external DHCP server is used, check the setting on the device to be used as a DHCP relay agent.

(b) Checking the operation log and interface

One probable cause of disabled assignment of IP addresses to clients is that communication between the client and the server has been disabled. Check the operation log displayed by the Switch or use the `show ip interface` operation command to check whether the interface status is `Up` or `Down`. For details about the procedure, see *3.4 Network interface communication failures*.

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

If a failure has not occurred on the Switch, a failure might have occurred somewhere on the route between the Switch and the remote device. To identify the range for a failure in order

to determine the fault location on the route, do the following:

- Log in to the Switch.
- If there are devices such as an L3 switch between the client and the server, use the `ping` operation command to check the communication between the L3 switch and the remote device (DHCP client). If the communication with the remote device cannot be verified by using the `ping` operation command, execute the `ping` operation command again to check communication with each of the devices up to the client, beginning with the device closest to the Switch. For details about examples of using the `ping` operation command and how to interpret the execution result, see the *Configuration Guides*.
- If the server and the client are directly connected, check the hub and cable connections.

(d) Checking the filters and QoS control configuration information

If communication is not possible even when there is no physical failure on the Switch, certain packets might have been discarded by the filter functionality or packets might have been discarded by the QoS functionality shaper. Therefore, on the Switch and the relay device between the client and server, check in the system configuration whether the setting conditions for the filter functionality and QoS control in the configuration are correct and whether the shaper is used appropriately. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.

(e) Checking the Layer 2 network

If you do not find any incorrect settings or a failure in the steps (a) to (e), there might be a problem with the Layer 2 network. Check the Layer 2 network according to *3.5 Layer 2 network communication failures*.

3.7 IPv6 network communication failures

3.7.1 Communication is not possible or is disconnected

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

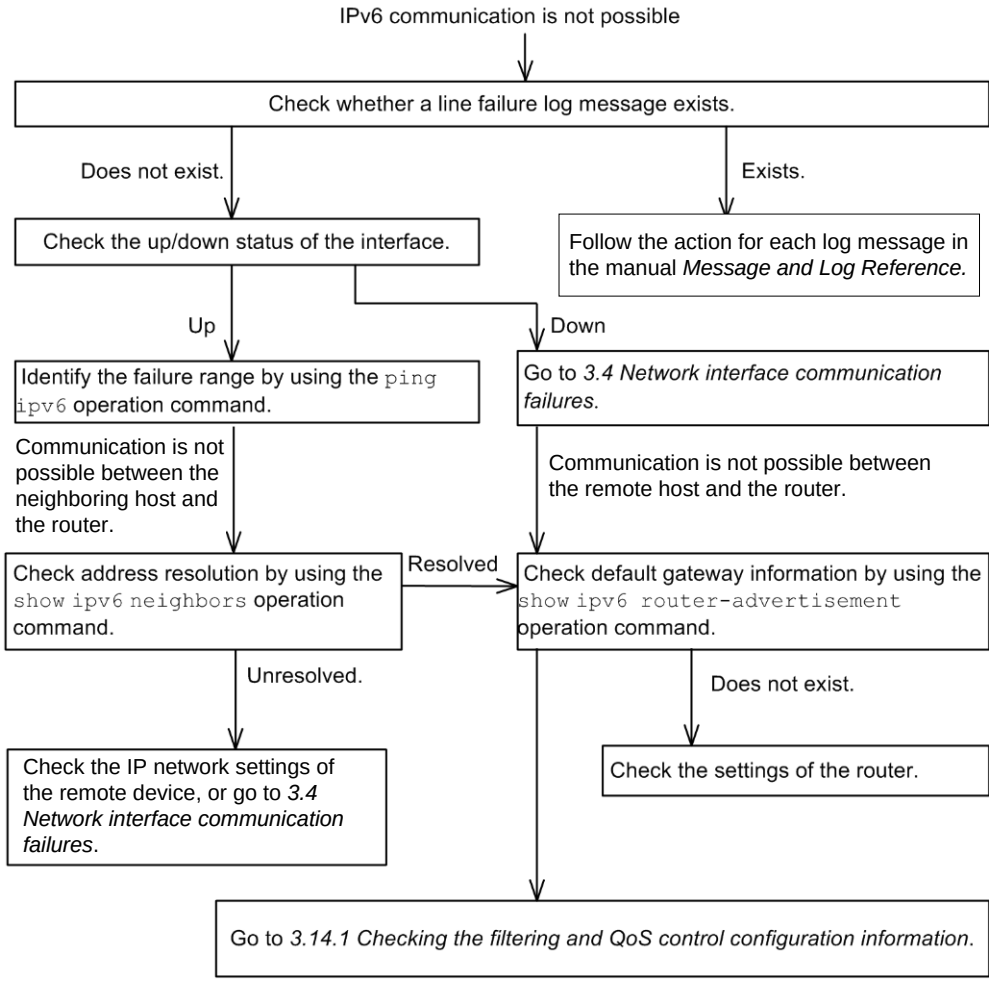
1. A configuration related to IPv6 communication is changed.
2. The network configuration is changed.
3. A network device fails.

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

This subsection describes the procedure for isolating the fault location to determine the cause of a problem, and applies mainly to cause 3 failures. For example, IPv6 communication might not be possible even when the configuration and the network configuration are correct, or 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.

Figure 3-6 Failure analysis procedure when IPv6 communication is not possible



(1) Checking the log

One probable cause of disabled communication is a line failure (or damage). To display the

messages that indicate a hardware failure, carry out the procedure below. You can find these messages in the log displayed by the Switch.

For details about the contents of the log, see the manual *Message and Log Reference*.

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

(2) Checking the interface status

Even 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` operation command to check whether the status of the interface with the target neighboring device is `Up` or `Down`.
3. If the status of the target interface is `Down`, see *3.4 Network interface communication failures*.
4. If the status of the target interface is `Up`, see *(3) Identifying the range for a failure (from the Switch).*

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

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

1. Log in to the Switch.
2. Use the `ping ipv6` operation command to check the communication with the two remote devices that are unable to communicate. For details about examples of using the `ping ipv6` operation command and how to interpret the execution result, see the *Configuration Guides*.
3. If communication with the remote devices cannot be verified by the `ping ipv6` operation 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. If the execution result of the ping operation command indicates that the failure occurred on a neighboring device, see *(5) Checking the NDP resolution information with a neighboring device*. If the execution result indicates a failure on the remote device, see *(6) Checking the default gateway information*.

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

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

1. Make sure 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` operation 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 the NDP resolution information with a neighboring device

If the execution result of the `ping ipv6` operation 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` operation 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 has been resolved (NDP entry information exists), see *(6) Checking the default gateway 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. Alternatively, see *3.4 Network interface communication failures*.

(6) Checking the default gateway information

You need to check the default gateway 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 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 router-advertisement` operation command to check the default gateway information obtained by the Switch.
3. If the displayed information contains the default gateway information, check the settings of the IPv6 network interface functionality.
4. If the displayed information does not contain the default gateway information, check the router settings.
5. If the default gateway information obtained by the Switch contains the default gateway information about the interface that caused the communication failure, the interface might have a problem with the functionality shown below. The following functionality must be checked:
   - Filters and QoS functionality

     (7) Checking the filters and QoS configuration information

(7) Checking the filters and QoS configuration information

Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper.

Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration*

information

3.8 Layer 2 authentication communication failures

3.8.1 Communication failures occurring when IEEE 802.1X is used

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

Table 3-21 Failure analysis method for IEEE 802.1X

No.	Items to check and commands	Action
1	Use the `show dot1x` operation command to check the operating status of IEEE 802.1X.	● If `System 802.1X : Disable` or `Dot1x doesn't seem to be running` is displayed: The IEEE 802.1X program has stopped. Check whether the `dot1x system-auth-control` configuration command is set in the configuration. ● If `System 802.1X : Enable` is displayed, go to No. 2.
2	Execute the `show dot1x statistics` operation 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 a value other than `0` is displayed for `RxInvalid` or `RxLenErr`, an invalid EAPOL frame has been received from the terminal, in which case the event is logged. Use the `show dot1x logging` operation 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 exist, check the `Supplicant` setting on the terminal. ● For other cases, go to No. 3.
3	Execute the `show dot1x statistics` operation command, and make sure data has been sent to the RADIUS server.	If the value displayed for `TxTotal` under `[EAPoverRADIUS frames]` is `0`, no data has been sent to the RADIUS server. Check the following: ● Check whether `aaa authentication dot1x default group radius` has been specified in a configuration command. ● Check whether the `dot1x radius-server host` or `radius-server host` configuration command is set correctly.
		For port-based authentication (static): ● Make sure the MAC address on the authentication terminal has not been registered with the `mac-address-table static` configuration command.
		For port-based authentication (dynamic): ● Make sure the MAC address on the authentication terminal has not been registered with the `mac-address-table static` and `mac-address` configuration commands.
		● For other cases, go to No. 4.

No.	Items to check and commands	Action
4	Execute the `show dot1x statistics` operation command, and make sure packets have been received from the RADIUS server.	If the value displayed for `RxTotal` under `[EAPoverRADIUS frames]` is `0`, packets have not been received from the RADIUS server. Check the following: ● If the RADIUS server is associated with the remote network, make sure a route to the remote network exists. ● Make sure the ports on the RADIUS server are not subject to authentication. ● For other cases, go to No. 5.
5	Execute the `show dot1x logging` operation command, and check data exchange with the RADIUS server.	● If `Invalid EAP over RADIUS frames received` is displayed, invalid packets were received from the RADIUS server. Check whether the RADIUS server is running normally. ● If `Failed to connect to RADIUS server` is displayed, an attempt to establish a connection with the RADIUS server has failed. Check whether the RADIUS server is running normally. ● For other cases, go to No. 6.
6	Execute the `show dot1x logging` operation command, and check whether authentication failed.	● If `RADIUS authentication failed` is displayed: Authentication failed for either of the reasons shown below. Check for problems. (1) The user ID or password has not been registered on the authentication server. (2) The user ID or password is entered incorrectly.
		● If `The number of supplicants on the switch is full` is displayed: Authentication failed because the maximum number of supplicants for the device was exceeded.
		● If `Failed to authenticate the supplicant because it could not be registered to mac-address-table.` is displayed: Authentication was successful, but an attempt to set the MAC address table for the hardware failed. See the appropriate location in the manual *Message and Log Reference*, and take the action described in *Action*.
		● If none of the above apply and the authentication mode is set to port-based authentication (dynamic), go to No. 7. For all other cases, see the RADIUS server log to check whether authentication failed.
7	Execute the `show dot1x logging` operation command, and check whether dynamic allocation in port-based authentication (dynamic) failed.	If `Failed to assign VLAN (Reason:`*xxxxx*`)` is displayed, check the information displayed for `(Reason:`*xxxxx*`)` and take action as described below.
		● `(Reason: No Tunnel-Type Attribute)` Dynamic allocation has failed because the `Tunnel-Type` attribute is not set for the `RADIUS` attribute. Set the `Tunnel-Type` attribute for the `RADIUS` attribute of the RADIUS server.

No.	Items to check and commands	Action
		● (Reason: Tunnel-Type Attribute is not VLAN(13)) Dynamic allocation has failed because the value of the Tunnel-Type attribute for the RADIUS attribute is not (13). Set VLAN(13) for the Tunnel-Type attribute for the RADIUS attribute of the RADIUS server.
		● (Reason: No Tunnel-Medium-Type Attribute) Dynamic allocation has failed because the Tunnel-Medium-Type attribute is not set for the RADIUS attribute. Set the Tunnel-Medium-Type attribute for the RADIUS attribute of the RADIUS server.
		● (Reason: Tunnel-Medium-Type Attribute is not IEEE802(6)) Dynamic allocation has failed because the value of the Tunnel-Medium-Type attribute is not IEEE802(6), or because the value of the Tunnel-Medium-Type attribute is correct but the tag value does not match the tag of the Tunnel-Type attribute. Set the correct value or tag for the Tunnel-Medium-Type attribute for the RADIUS attribute of the RADIUS server.
		● (Reason: Invalid Tunnel-Private-Group-ID Attribute) Dynamic allocation has failed because an invalid value is set for the Tunnel-Private-Group-ID attribute for the RADIUS attribute. Set the correct VLAN ID for the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server. If a VLAN name has been registered on the RADIUS server, make sure the target VLAN name matches the VLAN name specified in the name[#2] configuration command.
		● (Reason: The port doesn't belong to VLAN) Dynamic allocation has failed because the authentication port does not belong to the VLAN ID specified for the Tunnel-Private-Group-ID attribute for the RADIUS attribute. Correct the configuration so that the VLAN ID specified for the Tunnel-Private-Group-ID attribute of the RADIUS attributes for the RADIUS server matches the VLAN ID of the authenticating port[#1]. If a VLAN name has been registered on the RADIUS server, make sure the target VLAN name matches the VLAN name specified in the name[#2] configuration command.
		● If none of the above applies, see the RADIUS server log to check whether authentication has failed.

No.	Items to check and commands	Action
8	If authentication linked with the NAP quarantine system cannot be performed in port-based authentication (static) mode, check the setting of the authentication IPv4 access list.	● Make sure access permission for the quarantine server is set in the authentication IPv4 access list. ● Correct the configuration so that the `Filter-ID` value specified for the `RADIUS` attribute of the RADIUS server matches the authentication IPv4 access list name for the Switch.

#1

Check the following configuration command settings:

1. When both the `switchport mac vlan` and `no switchport mac auto-vlan` are not set

   - The VLAN ID for the RADIUS server has been set by `vlan mac-based`.

   - The VLAN ID of the authenticating port does not match `switchport mac dot1q vlan`.

2. When both the `switchport mac vlan` and `no switchport mac auto-vlan` are set

   - The VLAN ID of the authenticating port matches `switchport mac vlan`.

#2

Be careful of the following when using a VLAN name configured using the `name` configuration command as a VLAN after RADIUS authentication.

- Specify a unique VLAN name. If the same VLAN name is used for two or more VLANs, the smallest VLAN ID is allocated as the post-authentication VLAN in RADIUS authentication mode.
- Do not specify a number at the beginning of the VLAN name. A number at the beginning will be recognized as the VLAN ID, which might result in an authentication failure.

If communication is not possible on a port or VLAN that uses IEEE 802.1X, isolate the cause of the problem according to the failure analysis method described in the table below. If neither is the case, see *3.5 Layer 2 network communication failures*.

Table 3-22 Communication failure analysis method for IEEE 802.1X

No.	Items to check and commands	Action
1	Check whether the authenticated terminal has moved to an unauthenticated port in the same VLAN.	If the terminal authenticated on the Switch has moved to an unauthenticated port, communication is disabled until the authentication information is cleared. Use the `clear dot1x auth-state` operation command to clear the authentication status of the terminal.

3.8.2 Communication failures occurring when Web authentication is used

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

Table 3-23 Failure analysis method for Web authentication

No.	Items to check and commands	Action
1	Check whether the login page appears on the terminal.	● If the login page and logout page do not appear, go to No. 2. ● If the login page appears in local authentication method, go to No. 5. ● If the login page appears in RADIUS authentication method, go to No. 7.
2	Check whether the URLs specified for login and logout are correct.	● If incorrect URLs are specified for login or logout, use the correct URLs. ● If the Web authentication IP address has been set, make sure the IP address for the VLAN (dynamic or fixed VLAN) for which Web authentication is to be performed has been set by the `ip address` configuration command. ● If fixed VLAN mode or dynamic VLAN mode is set, go to No. 3. ● For other cases, go to No. 9.
3	Check the setting of the Web authentication IP address or URL redirection in fixed VLAN mode and dynamic VLAN mode.	● Check whether the Web authentication IP address has been set in the `web-authentication ip address` configuration command or URL redirection has been enabled by the `web-authentication redirect enable` configuration command. ● If URL redirection is enabled, make sure the IP address is set for a VLAN that is authenticated in fixed VLAN mode or dynamic VLAN mode by using the `ip address` configuration command. ● For other cases, go to No. 4.
4	Check the setting of the authentication IPv4 access list.	● If an unauthenticated terminal sends certain types of packets to destinations outside the Switch, make sure an authentication IPv4 access list is set. When both a standard access list and an authentication IPv4 access list are set for an authenticating port, make sure the filter conditions in the authentication IPv4 access list are also set in the standard access list. ● Make sure a filter condition for discarding IP packets (such as `deny ip`) is not set in the standard access list or authentication IPv4 access list for the authenticating port. ● Make sure `any` is not set for the destination IP address in the filter condition in the authentication IPv4 access list. ● For other cases, go to No. 10.
5	Use the `show web-authentication user` operation command to check whether the user ID is registered.	● If the user ID is not registered, use the `set web-authentication user` operation command to register the user ID, password, and VLAN ID. After the registration, use the `commit web-authentication` operation command to apply the information to the operation. ● For other cases, go to No. 6.

No.	Items to check and commands	Action
6	Check whether the entered password is correct.	● If the password does not match, use the `set web-authentication passwd` operation command to change the password, or use the `remove web-authentication user` operation command to delete the user ID, and then use the `set web-authentication user` operation command to register the user ID, password, and VLAN ID again. After the change, use the `commit web-authentication` operation command to apply the information to the operation. ● For other cases, go to No. 10.
7	Use the `show web-authentication statistics` operation command to check the communication status with the RADIUS server.	● If the value displayed for `TxTotal` under `[RADIUS frames]` is `0`, check whether the following configurations are specified correctly: `aaa authentication web-authentication default web-authentication radius-server host` or `radius-server host` ● For other cases, go to No. 8.
8	Check whether the password and user ID are registered on the RADIUS server.	● If the user ID is not registered, register it on the RADIUS server. [Fixed VLAN mode] ● Check whether the RADIUS server's VLAN ID indicated by `NAS-Identifier` matches the VLAN ID to which the terminal to be authenticated belongs. [Dynamic VLAN mode] ● Correct the configuration so that the VLAN ID specified for the `Tunnel-Private-Group-ID` attribute of the `RADIUS` attributes for the RADIUS server matches the VLAN ID of the authenticating port[#1]. ● If a VLAN name has been registered on the RADIUS server, make sure the target VLAN name matches the VLAN name specified in the `name`[#2] configuration command. ● For other cases, go to No. 10.
9	Use the `show logging` operation command to check whether `HTTP server initialization failed.` is recorded in the log.	● If the log data is recorded, the SSL certificate and private key are not correct. Obtain the correct certificate and private key, and then re-install them on the switch. ● For other cases, go to No. 10.
10	Use the `show web-authentication statistics` operation command to check whether Web authentication statistics are displayed.	● If Web authentication statistics are not displayed, go to No. 11. ● For other cases, go to No. 12.
11	Check whether the `web-authentication system-auth-control` configuration command has been set.	● If the `web-authentication system-auth-control` configuration command has not been set, set the command. ● For other cases, go to No. 12.

No.	Items to check and commands	Action
12	Execute the `show web-authentication logging` command and check for operation problems.	If the following operation log data is not displayed with operation log type `LOGIN`, authentication has failed: ● Login succeeded ● Login update succeeded Check the operation log, and review the settings of the RADIUS server, internal Web authentication DB, and configuration. (For details about the operation log, see the manual *Operation Command Reference*)
		● If authentication information for the port to which the authentication terminal is connected is not displayed, check whether the authenticating port has been configured correctly by using the `web-authentication port` configuration command.
		● Make sure the authenticating port to which the terminal is connected is neither in the link-down status nor shut down.
		● For other cases, check the Web authentication configuration.

#1

Check the following configuration command settings:

1. When both the `switchport mac vlan` and `no switchport mac auto-vlan` are not set

   - The VLAN ID for the RADIUS server has been set by `vlan mac-based`.

   - The VLAN ID of the authenticating port does not match `switchport mac dot1q vlan`.

2. When both the `switchport mac vlan` and `no switchport mac auto-vlan` are set:

   - The VLAN ID of the authenticating port matches `switchport mac vlan`.

#2

Be careful of the following when using a VLAN name configured using the `name` configuration command as a VLAN after RADIUS authentication.

- Specify a unique VLAN name. If the same VLAN name is used for two or more VLANs, the smallest VLAN ID is allocated as the post-authentication VLAN in RADIUS authentication mode.
- Do not specify a number at the beginning of the VLAN name. A number at the beginning will be recognized as the VLAN ID, which might result in an authentication failure.

Check the following for the configuration related to Web authentication.

Table 3-24 Checking the configuration of Web authentication

No.	Items to check and commands	Action
1	Web authentication configuration	Make sure the following configuration commands have been set correctly. [Common to Web authentication] ● `aaa authentication web-authentication default group radius` ● `web-authentication auto-logout` ● `web-authentication max-timer` ● `web-authentication system-auth-control` [Fixed VLAN mode] ● `web-authentication port` ● `authentication arp-relay` ● `authentication ip access-group` ● `web-authentication redirect enable` ● `web-authentication redirect-mode` [Dynamic VLAN mode] ● `web-authentication port` ● `authentication arp-relay` ● `authentication ip access-group` ● `web-authentication redirect enable` ● `web-authentication redirect-mode`
2	IP addresses set for the VLAN interfaces	[Fixed VLAN mode] Make sure the IP address for the VLAN interface is set correctly. [Dynamic VLAN mode] Make sure the IP addresses for the following VLAN interfaces are set correctly: ● Pre-authentication VLAN ● Post-authentication VLAN
3	DHCP server setting	When the DHCP server is used, see *3.6.2 Communication failures occurring when the DHCP server is used*.
4	Filter setting	Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper. Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.
5	Setting of the authentication IPv4 access list	Make sure the filter conditions required for communication from unauthenticated terminals to destinations outside the Switch have been set correctly by using the `authentication ip access-group` and `ip access-list extended` configuration commands.
6	Setting of ARP packet forwarding	Make sure the `authentication arp-relay` configuration command has been set correctly so that unauthenticated terminals can send ARP packets to devices outside the Switch.

3.8.3 Communication failures occurring when MAC-based authentication is used

If communication is not possible when MAC-based authentication is used, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-25 Failure analysis method when MAC-based authentication is used

No.	Items to check and commands	Action
1	Check whether communication with the terminal is possible.	● If authentication in local authentication method is not possible, go to No. 2. ● If authentication in RADIUS authentication method is not possible, go to No. 3. ● For other cases, go to No. 6.
2	Use the `show mac-authentication mac-address` operation command to make sure the MAC address and VLAN ID are registered.	● If the MAC address is not registered, use the `set mac-authentication mac-address` operation command to register the MAC address and VLAN ID. After registration, use the `commit mac-authentication` operation command to apply the information to the operation.
		[Fixed VLAN mode] ● If the `mac-authentication vlan-check` configuration command is set, make sure the MAC address and the VLAN ID to which the terminal to be authenticated belongs are registered.
		[Dynamic VLAN mode] ● Make sure the MAC address and the post-authentication VLAN ID are registered.
		● For cases other than above, if fixed VLAN mode or dynamic VLAN mode is used, go to No. 5. ● For other cases, go to No. 6.
3	Check whether the MAC address is registered on the RADIUS server.	● If the MAC address is not registered as the user ID of the RADIUS server, register the MAC address on the RADIUS server. ● If the MAC address is registered for the user ID and password, check the value of the MAC address. Also check whether the MAC address format matches the format set in the `mac-authentication id-format` configuration command. ● If a character string is specified for the password, check whether it matches the character string set in the `mac-authentication password` configuration command.
		[Fixed VLAN mode] ● Check whether the RADIUS server's VLAN ID indicated by `NAS-Identifier` matches the VLAN ID to which the terminal to be authenticated belongs. ● If the `mac-authentication vlan-check` configuration command is set, check whether the character string registered as the user ID matches the combination of VLAN ID and separator characters specified in that command.

No.	Items to check and commands	Action
		[Dynamic VLAN mode] Correct the configuration so that the VLAN ID specified for the `Tunnel-Private-Group-ID` attribute of the `RADIUS` attributes for the RADIUS server matches the VLAN ID of the authenticating port[#1]. ● If a VLAN name has been registered on the RADIUS server, make sure the target VLAN name matches the VLAN name specified in the `name`[#2] configuration command.
		● For other cases, go to No. 4.
4	Use the `show mac-authentication statistics` operation command to check the communication status with the RADIUS server.	● If the value displayed for `TxTotal` under `[RADIUS frames]` is `0`, check whether the following configurations are specified correctly: `aaa authentication mac-authentication default mac-authentication radius-server host` or `radius-server host`
		● If fixed VLAN mode or dynamic VLAN mode is set, go to No. 5. ● For other cases, go to No. 6.
5	Check the setting of the authentication IPv4 access list.	● If an unauthenticated terminal sends certain types of packets to destinations outside the Switch, make sure an authentication IPv4 access list is set. When both a standard access list and an authentication IPv4 access list are set for an authenticating port, make sure the filter conditions in the authentication IPv4 access list are also set in the standard access list. ● Make sure `any` is not set for the destination IP address in the filter condition in the authentication IPv4 access list. ● For other cases, go to No. 6.
6	Use the `show mac-authentication statistics` operation command to check whether the MAC-based authentication statistics are displayed.	● If the MAC-based authentication statistics are not displayed, go to No. 7. ● For other cases, go to No. 8.
7	Check whether the `mac-authentication system-auth-control` configuration command has been set.	● If the `mac-authentication system-auth-control` configuration command has not been set, set the command. ● For other cases, go to No. 8.
8	Execute the `show mac-authentication logging` operation command and check for operation problems.	If the following operation log data is displayed with operation log type `LOGIN`, authentication has failed: ● `Login failed :` xxxxxxxxxxx Check the operation log, and review the settings of the RADIUS server, internal MAC authentication DB, and configuration. For details about the operation log, see the manual *Operation Command Reference*.

No.	Items to check and commands	Action
		● If authentication information for the port to which the authentication terminal is connected is not displayed, check whether the authenticating port has been configured correctly by using the `mac-authentication port` configuration command.
		● Make sure the authenticating port to which the terminal is connected is neither in the link-down status nor shut down.
		● For other cases, check the MAC-based authentication configuration.

#1

Check the following configuration command settings:

1. When both the `switchport mac vlan` and `no switchport mac auto-vlan` are not set

   - The VLAN ID for the RADIUS server has been set by `vlan mac-based`.

   - The VLAN ID of the authenticating port does not match `switchport mac dot1q vlan`.

2. When both the `switchport mac vlan` and `no switchport mac auto-vlan` are set

   - The VLAN ID of the authenticating port matches `switchport mac vlan`.

#2

Be careful of the following when using a VLAN name configured using the `name` configuration command as a VLAN after RADIUS authentication.

- Specify a unique VLAN name. If the same VLAN name is used for two or more VLANs, the smallest VLAN ID is allocated as the post-authentication VLAN in RADIUS authentication mode.
- Do not specify a number at the beginning of the VLAN name. A number at the beginning will be recognized as the VLAN ID, which might result in an authentication failure.

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

Table 3-26 Checking the configuration of MAC-based authentication

No.	Items to check and commands	Action
1	MAC-based authentication configuration	Make sure the following configuration commands have been set correctly. [Common to MAC-based authentication] ● `aaa authentication mac-authentication default group radius` ● `mac-authentication access-group` ● `mac-authentication auto-logout` ● `mac-authentication id-format` ● `mac-authentication interface` ● `mac-authentication max-timer` ● `mac-authentication password` ● `mac-authentication system-auth-control` [Fixed VLAN mode] ● `mac-authentication port` ● `mac-authentication vlan-check` ● `authentication arp-relay` ● `authentication ip access-group` [Dynamic VLAN mode] ● `mac-authentication port` ● `authentication arp-relay` ● `authentication ip access-group`
2	VLAN interface setting	[Fixed VLAN mode] Make sure the IP address for the VLAN interface is set correctly. [Dynamic VLAN mode] Make sure the IP addresses for the following VLAN interfaces are set correctly: ● Pre-authentication VLAN ● Post-authentication VLAN
3	Filter setting	Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper. Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.
4	Setting of the authentication IPv4 access list	Make sure the filter conditions required for communication from unauthenticated terminals to destinations outside the Switch have been set correctly by using the `authentication ip access-group` and `ip access-list extended` configuration commands.
5	Setting of ARP packet forwarding	Make sure the `authentication arp-relay` configuration command has been set correctly so that unauthenticated terminals can send ARP packets to devices outside the Switch.

3.8.4 Communication failures occurring when secure Wake-on-LAN is used [OS-L2A]

If a failure occurs when secure Wake-on-LAN is used, isolate the cause of the problem according to the failure analysis method described in the table below.

- Internal DB for registering the terminal that sends the startup command: WOL terminal DB
- Internal DB for user authentication: WOL user DB

Table 3-27 Failure analysis method for secure Wake-on-LAN

No.	Items to check and commands	Action
1	Check whether the user authentication page for secure Wake-on-LAN appears on the terminal.	If the user authentication page does not appear, go to No. 2.
		If the user authentication page appears: ● If user authentication is not possible, go to No. 3. ● If user authentication is possible: If `Not available.` appears on the page used for selecting the terminal and sending the startup command, go to No. 5. If startup of the terminal cannot be confirmed after the startup command is sent, go to No. 6.
2	Make sure the URL of the user authentication page is correct.	If the URL of the user authentication page is not correct, use the correct URL. For the IP address of the URL, use the IP address of the VLAN used for secure Wake-on-LAN.
3	Use the `show wol-authentication user` operation command to check whether user information is registered.	If the user is not registered, use the `set wol-authentication user` operation command to register the user. If the user ID is not correct, delete it with the `remove wol-authentication user` operation command, and then use the `set wol-authentication user` operation command to register the correct user ID. After the change, use the `commit wol-authentication` operation command to apply the information to the operation. For other cases, go to No. 4.
4	Use the `show wol` operation command to check the number of users who are using the secure Wake-on-LAN functionality.	A maximum of 32 users can use the secure Wake-on-LAN functionality concurrently. If the maximum number of users is exceeded, this functionality cannot be used. Wait a while until the processing of other users terminates.
5	Use the `show wol-authentication user` operation command with the target user ID and `detail` option specified to check the terminal access permissions and the terminal name.	If an asterisk (`*`) appears for the target user's entry: The terminal name is not registered in the WOL terminal DB. Use the `show wol-device name` operation command to check the terminal name, and then use the `set wol-authentication permit` operation command to change the terminal name. After the change, use the `commit wol-authentication` operation command to apply the information to the operation.

No.	Items to check and commands	Action
6	Use the `show wol-device name` operation command to check the information registered in the WOL terminal DB.	Check whether the terminal name, the terminal MAC address, and information for the VLAN to which the terminal belongs are correct. If these items are not correct, the startup command cannot be sent. ● If the items are not correct: Use the set `wol-device mac` and `set wol-device vlan` operation commands to change the information. After the changes, use the `commit wol-device` operation command to apply the information to the operation. ● If all items are correct, go to No. 7.
7	Use the `show wol-device name` operation command to check the information displayed for `Alive` for the terminal.	● If `no-check` is displayed: The terminal has been registered with the startup check disabled. Use the `set wol-device alive` operation command to change the setting so that the startup check will be performed, and then use the `set wol-device ip` operation command to add the IP address information#. After the changes, use the `commit wol-device` operation command to apply the information to the operation. # IP address information For a DHCP client: Specify `dhcp` and configure DHCP snooping for the Switch. For a fixed-IP address terminal: Set the IP address of the terminal. ● For other cases, go to No. 8.
8	If the startup check is enabled, check the IP address information.	● For a DHCP client: Make sure that `dhcp` is registered. Also make sure that DHCP snooping is configured for the Switch. ● For a fixed-IP address terminal: Make sure the IP address of the terminal is registered. If the settings are not correct, use the `set wol-device ip` operation command to change them. After the changes, use the `commit wol-device` operation command to apply the information to the operation. ● When the IP address information is correct, go to No. 9.
9	Use the `show running-config` operation command to check the VLAN interface configuration.	Check whether the IP address is set for the VLAN to which the terminal belongs. If the IP address is not set, set it.

3.9 Communication failures in the high-reliability functionality based on a redundant configuration

3.9.1 Communication failures occurring when uplink redundancy is used

If switching cannot be performed as expected when uplink redundancy is used, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-28 Failure analysis method for uplink redundancy

No.	Items to check and commands	Action
1	Use the `show switchport-backup` operation command to check the primary and secondary pair information.	● Pair information is not displayed: Go to No. 2. ● Pair information is displayed: - If the `Status` information for the port displayed by the `show switchport-backup` operation command does not change immediately after the physical port enters the link-down status, go to No. 3. - If automatic preemption or timer preemption is not possible after the primary port enters the link-up status, go to No. 4.
2	Use the `show running-config` operation command to check the uplink redundancy configuration.	The port channel interface is specified for the secondary port: The configuration for the target port channel interface might have not been set. Check the configuration of the target port channel interface. If the configuration has not been set, set it.
3	Check the link debounce setting for the target port.	If the `link debounce` configuration command has not been set (that is, the default of 2000 milliseconds is used for operation) or if a value greater than `2000` (milliseconds) is set, reduce the set value.
4	If automatic preemption or timer preemption to the primary port is not possible, use the `show switchport-backup` operation command to check the information displayed for `Status` for the primary port.	● `Blocking` displayed: - If a hyphen (`-`) is displayed for `Delay` under `Preemption`, neither automatic preemption nor timer preemption has been set. Use the `switchport backup interface` configuration command to set preemption. - If a value other than `0` is displayed for `Limit` (time) under `Preemption`, the preemption time has not been reached. Wait a while. Alternatively, execute the `set switchport-backup active` operation command. ● `Down` displayed: The status of the port is link down. Check the status of the upstream switch and the cable connection. ● For other cases, go to No. 5.
5	Check whether a Spanning Tree Protocol is running on the upstream switch of the primary port.	When a Spanning Tree Protocol is running, the port enters the `Listening` or `Learning` status after recovery from a link-down condition, and therefore communication is disabled for a while. If a Spanning Tree Protocol is running on the upstream switch, set the timer preemption to 30 seconds or longer. For other cases, go to No. 6.
6	Check whether the upstream switch can receive flush control frames.	Reception is possible: Go to No. 7. Reception is not possible: Go to No. 8.

No.	Items to check and commands	Action
7	Check whether the sending of flush control frames is set on the Switch.	● When not set: Wait until aging of the MAC address table on the upstream switch has finished. ● When set: Check the configuration of the port and the sending VLAN for which sending of flush control frames has been set. If the configuration is not correct, set the configuration again.
8	Check whether the sending of MAC address update frames is set on the Switch.	● When not set: Wait until aging of the MAC address table on the upstream switch has finished. ● When set: - Check whether the VLAN that has learned the MAC addresses on the port connected to the terminal is included in the uplink port pair. If the VLAN is not included, specify the setting again. - Check whether the same VLAN is set for both ports of the uplink port pair (primary and secondary). If different VLANs are set, set the same VLAN. For other cases, go to No. 9.
9	Use the operation command `show switchport-backup mac-address-table update statistics` to make sure the value displayed for `Transmission over flows` has been incremented.	If the value has been incremented, the number of applicable MAC addresses for MAC address update frames exceeds 1024. ● If the MAC addresses not applicable for MAC address update frames can be deleted at the VLAN level: Set the VLAN to be processed. ● If the VLAN cannot be processed: Wait until aging of the MAC address table on the upstream switch has finished.

3.9.2 Communication failures occurring when SML is used [OS-L2A]

If a failure occurs when SML is used, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-29 Failure analysis method for SML

No.	Items to check and commands	Action
1	Use the `show sml` operation command to check the SML status.	If `Conflict` is displayed for `SML Status`, go to No. 2.
		If `Standalone` is displayed for `SML Status`, go to No. 3.
		If `Full` is displayed for `SML Status`, go to No. 4.
		If the SML domain is different from that set on the peer: For `sml domain`, set the same domain ID as that set on the peer.

No.	Items to check and commands	Action
2	Check if more than two devices configuring the SML are connected, and if the same SML ID is set for the devices configuring the SML.	If more than two devices configuring the SML are connected: Perform the following procedure for recovery: 1. Connect no more than two devices configuring the SML. 2. Remove from the peer link port the cable connecting the excess SML devices to the devices configuring the SML. 3. Use the `activate` operation command to activate all ports specified for a peer link on the devices configuring the SML. 4. Wait until `Full` is indicated for `SML Status`.
		If the same SML ID is set for the devices configuring the SML: The same SML ID is set for both SML devices. Perform the following procedure for recovery: 1. Set a new SML ID for either of the SML devices and then restart the Switch. 2. For the other SML device, use the `activate` operation command to activate all ports specified for a peer link. 3. Wait until `Full` is indicated for `SML Status`.
3	Check the cables connecting the peer link ports of the SML devices.	If a line failure has occurred on the peer link ports: Perform the following procedure for recovery: 1. See *3.4.3 Actions to be taken for 100BASE-FX [24S4X]/1000BASE-X problems*, *3.4.4 Actions to be taken for 10GBASE-R problems [10G models]*, and *3.4.5 Actions to be taken for direct attach cable problems [10G models]*. 2. Put the peer link into the link-down status by, for example, removing and then reconnecting the cables connected to all peer link ports or by executing the `inactivate/activate` operation command. 3. After the peer link ports enter the link-up status, wait until `Full` is indicated for `SML Status`. If the peer link ports are deactivated: See *3.4.1 Ethernet port cannot be connected*. When `Full` is not indicated for `SML Status`: ● Make sure that the cables are connected from the peer link ports to the partner SML device. ● Make sure that the SML functionality is enabled on the partner SML device.
4	Use the `ping` operation command to check the connectivity of the Switch.	If the connectivity is lost, go to No. 5.
5	Use the `show sml channel-group` operation command to check the `SML ChGr` status.	● When the `channel-group status` of the Switch is `Down` and the `channel-group status` of the neighboring device is `Up`: When the channel group of the Switch is down, the VLAN for IP communication might also be down Check the status of the Ethernet port belonging to the channel group, and bring the channel group up.

3.10 SNMP communication failures

3.10.1 MIBs cannot be obtained from the SNMP manager

Make sure the configuration has been registered correctly.

When using SNMPv1 or SNMPv2C

Execute the `show running-config` operation command, and check whether the community name and access list have been registered correctly. If IP addresses for the SNMP manager to which access is permitted are not restricted, an access list need not be set.

If the community name and access list have not been registered, execute the `snmp-server community` configuration command to set information about the SNMP manager.

```
# show running-config
 ...
 ...
ip access-list standard SNMPMNG
  permit host 128.1.1.2

snmp-server community "NETWORK" ro SNMPMNG

#
```

When using SNMPv3

Execute the `show running-config` 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

```
# show running-config
    ...
    ...
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
!
    ...
    ...
#
```

3.10.2 Traps cannot be received by the SNMP manager

Make sure the configuration has been registered correctly.

When using SNMPv1 or SNMPv2C

Execute the `show running-config` operation command, and check whether the information about the SNMP manager and traps has been registered in the configuration for the Switch.

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

```
# show running-config
 ...
 ...
snmp-server host 20.1.1.1 traps "event-monitor" snmp

#
```

When using SNMPv3

Execute the `show running-config` 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

```
# show running-config
    ...
    ...
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
!
    ...
    ...
#
```

3.10.3 When SNMPv3 cannot be used

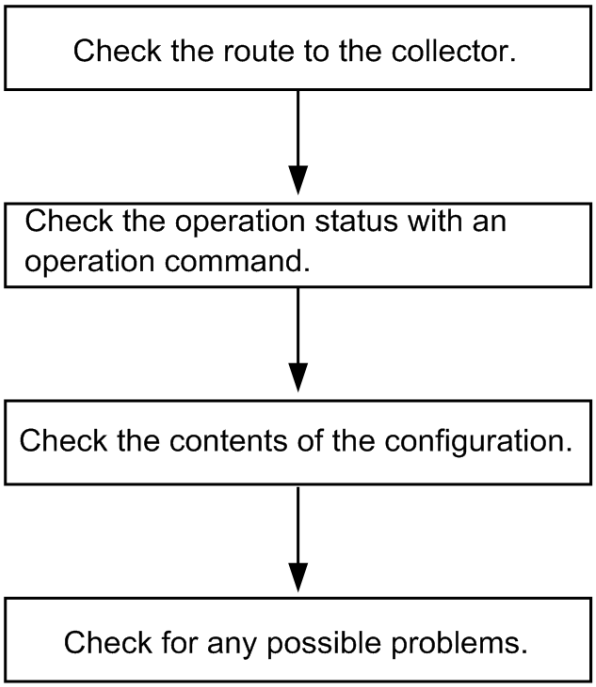
When an unexpected reboot (due to power outage, etc.) occurs when the Switch starts or immediately after the input of the `snmp-server engineID local` configuration command, the Engine ID and the restart count after changing the Engine ID that are recorded in the internal flash memory might become corrupted.

When SNMPv3 cannot be used, see *Procedure for recovering the SNMP engine ID* under *Using SNMP to Manage Networks* in the *Configuration Guide Vol. 2* to recover the engine ID.

3.11 Troubleshooting the sFlow statistics (flow statistics) functionality

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

Figure 3-7 Workflow for troubleshooting the sFlow statistics functionality



3.11.1 sFlow packets cannot be sent to the collector

(1) Checking the route to the collector

See *3.6.1 Communication is not possible or is disconnected* and *3.7.1 Communication is not possible or is disconnected*, and make sure that the network is correctly connected to the collector. If the maximum size of an sFlow packet (`sflow-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` operation command a few times to display the sFlow statistics, and check whether the sFlow statistics functionality is running. If the underlined values do not increase, see *(3) Checking the configuration*. If the values increase, see *3.6.1 Communication is not possible or is disconnected* and *3.7.1 Communication is not possible or is disconnected*, and *(5) Checking the settings on the collector*, and make sure the network is correctly connected to the collector.

Figure 3-8 Example of the "show sflow" command

```
> show sflow

Date 2012/07/20 02:46:42 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 0:03:42
sFlow agent data :
 sFlow service version: 4
```

```
 CounterSample interval rate: 20 seconds
 Default configured rate: 1 per 2097152 packets
 Default actual rate    : 1 per 2097152 packets
 Configured sFlow ingress ports: 0/1,0/5,0/23
 Configured sFlow egress ports : ----
 Received sFlow samples:          3  Dropped sFlow samples        :          0
 Exported sFlow samples:          3  Couldn't export sFlow samples:          0
 Overflow time of sFlow queue: 0 seconds
sFlow collector data :
 Collector IP address: 192.168.1.1  UDP: 6343  Source IP address: 192.168.1.100
  Send FlowSample UDP packets   :          3  Send failed packets:          0
  Send CounterSample UDP packets:         23  Send failed packets:          0
 Collector IP address: 192.168.1.1  UDP: 6343  Source IP address: 192.168.1.100
  Send FlowSample UDP packets   :          3  Send failed packets:          0
  Send CounterSample UDP packets:         23  Send failed packets:          0

>
```

Note: Make sure that the underlined values increase.

(3) Checking the configuration

Check the following in the active configuration:

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

Figure 3-9 Example of displaying a configuration 1

```
(config)# show

sflow destination 192.1.1.1 6455    ← Collector information must be set correctly.
sflow sample 2048
!
          ...

(config)#
```

- Make sure that the sampling interval has been set.

If the sampling interval is not set, a large default value is used. This value is too large, and almost no flow samples are sent to the collector. Therefore, set an appropriate value for the sampling interval. Note that if a value that is much smaller than the recommended value is set, the CPU usage might increase.

Figure 3-10 Example of displaying a configuration 2

```
(config)# show

sflow destination 192.1.1.1 6455
sflow sample 2048      ← An appropriate value for the sampling interval must be set.
!
          ...

(config)#
```

Figure 3-11 Example of the operation command

```
> show sflow

Date 2012/07/20 02:47:51 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 0:04:51
```

```
sFlow agent data :
 sFlow service version: 4
 CounterSample interval rate: 20 seconds
 Default configured rate: 1 per 2048 packets
 Default actual rate    : 1 per 2048 packets
 Configured sFlow ingress ports: 0/1,0/5,0/23
 Configured sFlow egress ports : ----
 Received sFlow samples:          3  Dropped sFlow samples        :          0
 Exported sFlow samples:          3  Couldn't export sFlow samples:          0
                          ...

>
```

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

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

Figure 3-12 Example of displaying a configuration 3

```
(config)# show interface gigabitethernet 0/2
interface gigabitethernet 0/2
  switchport mode access
  sflow forward ingress      ←sflow forward must be set.
!
(config)#
```

- Make sure that `filter` has not been set for the physical port at which the flow statistics are recorded. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.
- If the sender (agent) IP address of an sFlow packet has been set by using the `sflow source` command, make sure that the IP address has been assigned to the port of the Switch.

Figure 3-13 Example of displaying a configuration 4

```
(config)#  show
         ...
sflow  destination  192.1.1.1  6455
sflow  sample  2048
sflow  source  192.1.1.100         ←This IP address must be the one assigned to the
                                     port of the Switch.
!
         ...
(config)#
```

(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).

Figure 3-14 Example of displaying the port status

```
> show interfaces gigabitethernet 0/5

Date 2010/08/04 15:02:35 UTC
Port 0/5 : active up  1000BASE-T full(auto)  00eb.f103.0102
    Time-since-last-status-change:1:47:47
    Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
    Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
    Output rate:    4893.5kbps       16.8kpps
    Input  rate:    4893.5kbps       16.8kpps
```

```
    Flow control send   :off
    Flow control receive:off
    TPID:8100
                            ...

>
```

Note: Make sure that the underlined parts are `active` or `active up`.

If the port status is `Down`, see *3.6.1 Communication is not possible or is disconnected* and *3.7.1 Communication is not possible or is disconnected*.

(5) Checking the settings on the collector

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

3.11.2 Flow samples cannot be sent to the collector

If you have taken actions according to 3.11.1 sFlow packets cannot be sent to the collector but your problem is not resolved, check the following.

(1) Checking whether packets are forwarded

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

Figure 3-15 Example of displaying the port status

```
> show interfaces gigabitethernet 0/5

Date 2010/08/04 15:02:35 UTC
Port 0/5 : active up  1000BASE-T full(auto)  00eb.f103.0102
  Time-since-last-status-change:1:47:47
    Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
    Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
    Output rate:    4893.5kbps       16.8kpps
    Input  rate:    4893.5kbps       16.8kpps
    Flow control send   :off
    Flow control receive:off
    TPID:8100
                               :

>
```

Note: Check the underlined parts to confirm that packets are being forwarded.

(2) Checking the settings on the collector

Make sure that the collector currently used is configured correctly.

3.11.3 Counter samples cannot be sent to the collector

(1) Checking the sending interval of counter samples

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

Figure 3-16 Example of displaying a configuration

```
(config)# show
         :
sflow  destination  192.1.1.1  6455
sflow  sample  2048
sflow  polling-interval  60            ←This value must not be set to zero.
!
         :
(config)#
```

3.12 Communication failures in the neighboring device management functionality

3.12.1 Neighboring device information cannot be obtained by the LLDP functionality

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.

Table 3-30 Failure analysis method when the LLDP functionality is used

No.	Items to check and commands	Action
1	Execute the `show lldp` operation command and check the operating status of the LLDP functionality.	If `Enabled` is displayed for `Status`, go to No. 2.
		If the response message `LLDP is not configured` is displayed, the LLDP functionality has stopped. Enable the LLDP functionality.
2	Execute the `show lldp` operation 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` operation 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` operation command and check the port status in the information for the port to which the neighboring device is connected.	If `Up` is displayed for `Link`, go to No. 5.
		If `Down` is displayed for `Link`, check the line status. For details about the check procedure, see *3.4 Network interface communication failures*.
5	Execute the `show lldp` operation command, and check the number of neighboring devices 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 devices is also `0` on the neighboring device, the connection between the devices might be incorrect. Check the connection. • Certain packets might have been discarded by filters or packets might have been discarded by the QoS control shaper. Make sure that the setting conditions for filters and QoS control in the configuration are correct, and that the shaper is used appropriately in the system configuration. For details about the procedure, see *3.15.1 Checking the filters and QoS control configuration information*.

3.13 NTP communication failures

3.13.1 Time information cannot be obtained from the NTP server

If time information cannot be obtained from the NTP server, isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-31 Failure analysis method for NTP

No.	Items to check and commands	Action
1	Use the `show clock` operation 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	Use the `show ntp-client` operation command to check the information obtained from the NTP server.	If `Timeout` or `Error` is displayed in the `Status` field for the latest information in `NTP Execute History`, go to No. 3.
3	Check communication with the NTP server via IPv4.	Use the `ping` operation command to check whether communication is possible via IPv4 between the NTP server and the Switch.

3.14 Communication failures in the IEEE 802.3ah/UDLD functionality

3.14.1 Port is in inactivate status by the IEEE 802.3ah/UDLD functionality

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.

Table 3-32 Failure analysis method when the IEEE 802.3ah/UDLD functionality is used

No.	Items to check and commands	Action
1	Execute the `show efmoam` operation command and check the failure type for the port that was deactivated by the IEEE 802.3ah/UDLD functionality.	If `Down` 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` operation command and check the information displayed for `Thrashings`.	● If the value of `Thrashings` has been incremented, a prohibited configuration (multiple connection destinations) is being used. Make sure only one device is specified as the destination for the target physical port. ● If the `Thrashings` value 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 (this action is not recommended, however). ● If the switches are directly connected, go to No. 5.
5	Execute the `show efmoam` operation 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 the filters and QoS control configurations.	● The control frames (`slow-protocol`) used for the IEEE 802.3ah/UDLD functionality might have been discarded by filters or QoS control. See *3.15.1 Checking the filters and QoS control configuration information*. ● If there is no problem, go to No. 7.
7	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 that uses IEEE 802.3ah/OAM

3.15 Communication failures in filters and QoS configurations

3.15.1 Checking the filters and QoS control configuration information

If a communication problem occurs on a network employing the Switch, it is possible that certain packets have been discarded either by filters or by the QoS control shaper.

To determine which functionality discarded which packets when packets have been discarded in the Switch by filters and QoS control, do the following.

(1) Checking whether packets have been discarded by filters

1. Log in to the Switch.
2. Execute the `show access-filter` operation command, and check the filter conditions in the access list applied to the interface, the number of packets that match the filter conditions, and the number of packets discarded by a filter entry for implicit discard.
3. Compare the filter conditions you checked in step 2 and the contents of the packets that cannot be forwarded to determine whether the target packets were discarded. If the contents of the packets that cannot be forwarded do not match any of the applied filter conditions, the packets might have been discarded implicitly.
4. Check whether the setting conditions in the filter configuration are correct.

(2) Checking whether packets have been discarded by the QoS control shaper

1. Log in to the Switch.
2. Use the `show qos queueing` operation command to check the information displayed for `discard packets` in the output interface statistics.
3. Check whether the shaper is being used appropriately in the system configuration.

3.16 Port mirroring failures

3.16.1 BPDUs are sent from a mirror port

To stop sending BPDUs from a mirror port when the port mirroring functionality is enabled, use the `spanning-tree bpdufilter` configuration command to configure the BPDU filter functionality for the mirror port.

3.17 Power saving functionality failures

3.17.1 LED brightness control is disabled

If a problem occurs in LED brightness control during a power saving operation, perform the check procedure described in the following table.

Table 3-33 Problems in power saving operation and action to take

No.	Items to check and commands	Action
1	The LEDs do not light when the status of the ports changes to link up.	Perform the following procedure: 1. Use the `show system` operation command to check the information displayed for `Brightness mode`. ● `off` displayed: LED operation is disabled. ● `economy` displayed: LED operation is set to power saving brightness. 2. Use the `show power-control schedule` operation command to check whether the problem occurred within the scheduled time range. ● Scheduled time range: Execute the `schedule-power-control port-led` configuration command with `enable` specified. ● Normal time range: Execute the `system port-led` configuration command with `enable` specified.
2	When the status of the ports changes to link up, the LEDs do not light at normal brightness (automatic operation is disabled).	Use the `show system` operation command to check the information displayed for `Brightness mode`. ● `normal` displayed: LED operation is set to normal brightness. Check the setting of the `system port-led trigger` configuration command. If `interface` is not set in the `system port-led trigger` command, no physical port is specified as the trigger for automatic operation. Specify a physical port as the trigger for automatic operation. ● Other than above: Check the configuration.
3	When a memory card is inserted or removed, the LEDs do not light at normal brightness (automatic operation is disabled).	Use the `show system` operation command to check the information displayed for `Brightness mode`. ● `normal` displayed: LED operation is set to normal brightness. Check the setting of the `system port-led trigger` configuration command. If `mc` is not set in the `system port-led trigger` command, insertion or removal of a memory card is not specified as the trigger for automatic operation. Specify the insertion or removal of a memory card as the trigger for automatic operation. ● Other than above: Check the configuration.

No.	Items to check and commands	Action
4	When the user logs in to the console (RS232C), the LEDs do not light at normal brightness (automatic operation is disabled).	Use the `show system` operation command to check the information displayed for `Brightness mode`. ● `normal` displayed: LED operation is set to normal brightness. Check the setting of the `system port-led trigger` configuration command. If `console` is not set in the `system port-led trigger` command, the console is not specified as the trigger for automatic operation. Specify the console as the trigger for automatic operation. ● Other than above: Check the configuration.

3.17.2 Power saving scheduling is disabled

If a problem occurs in scheduling power saving, perform the check procedure described in the following table.

Table 3-34 Problems in power saving scheduling, and action to take

No.	Items to check and commands	Action
1	The Switch does not enter sleep mode at the scheduled time.	Check whether a user who has logged in (via serial cable or Telnet) to the Switch used configuration command mode. If there was such a user, save the settings and exit configuration command mode.
		Check whether `action disable` is set for the scheduled time range (`schedule-power-control time-range`). If it is set, change the setting to `action enable` and save the setting.
2	After the sleep period ends, the Switch does not run with the specified configuration.	When the Switch enters sleep mode on a schedule, any configuration that has not been saved to that point is discarded. Set the configuration again and save it by using the `save` command.
3	Sleep mode needs to be temporarily canceled.	Hold down the **RESET** button on the Switch for at least three seconds until all LEDs on the front of the Switch turn on. Note that the schedule-disabled mode is set after the sleep mode is canceled. The Switch will automatically enter schedule-enabled mode when the scheduled time range expires and a normal time range begins.
4	After the forced cancellation of sleep mode, the Switch enters sleep mode again after startup.	When the wake-up option (`schedule-power-control wakeup-option`) is set, briefly pressing the **RESET** button for less than three seconds does not trigger the forced cancellation of sleep mode. To forcibly cancel sleep mode, hold down the **RESET** button until all LEDs on the front panel of the Switch turn on.
5	When the wake-up option is set, sending WOL packets to the port configured to detect the reception of WOL packets fails to cancel sleep mode.	1. Make sure that the wake-up option is configured. 2. Specify the MAC address of the Switch as the MAC address of WOL packets. If you specify the MAC address of the port, the WOL packets will not be recognized as the packets for which the wake-up option is configured.

No.	Items to check and commands	Action
6	When the wake-up option is set, linking up the port configured to detect link-up fails to cancel sleep mode.	1. Make sure that the wake-up option is configured. 2. Make sure that the Switch is connected correctly with the port configured to detect link-up.

3.18 Problems related to the support of a long life solution

3.18.1 Dates are not displayed correctly in temperature history information

If some of the date and time information is missing from the output of the `show environment temperature-logging` operation command, the following problems might have occurred:

1. The Switch was restarted, for example, by turning the power off and on, while temperature history information was being saved to the internal flash memory, which resulted in a failure to save the temperature data.
2. Due to the change made to the time setting on the Switch, the information collection time became older than the previous log information.

Even when these problems occur, the collection of temperature history information continues. You can continue using the temperature logging functionality.

4. Obtaining Failure Information

This chapter describes how to obtain failure information.

4.1 Obtaining failure information

You can use the `show tech-support` operation command to collect information in a batch operation when a failure has occurred.

It might take tens of minutes for the `show tech-support` operation command to display information on the screen. As described below, we recommend that you save the information onto the RAMDISK, and then write the information to a memory card or transfer the information via FTP.

This command allows you to save the collected information on the RAMDISK in text format and then write the information to a memory card or transfer the information via FTP.

Figure 4-1 Saving information to the RAMDISK by using the show tech-support command

```
# show tech-support ramdisk
```

The file containing the information is saved as `showtech.txt`. See *4.2 Writing data to a memory card* for the procedure for writing the information to a memory card. For details about transferring the information via FTP, see *4.3 Transferring files via FTP*. We recommend that you delete files and directories on the RAMDISK by using the `del` operation command before executing the `show tech-support ramdisk` operation command.

4.2 Writing data to a memory card

Failure information copied to the RAMDISK can be written to a memory card. Note, however, that memory cards have a capacity limit. This section describes how to write the Switch information to a memory card via an operation terminal.

Figure 4-2 Writing information to a memory card

Insert a memory card into the Switch to which information is to be written.

Use the `show ramdisk-file` operation command to check the capacity of the source file (`showtech.txt`).`> show ramdisk-file`

```
Date 2010/08/06 17:38:20 UTC
    File Date               Size Name
    2010/08/06 17:37       1,265 showtech.txt

>
```

Use the `show mc` operation command to check available space.
`>show mc`

```
Date 2010/08/06 17:38:24 JST
    MC : enable
    Manufacture ID : 00000003
       used     5,750,272 byte
       free   120,160,256 byte    ← Available space
       total  125,910,528 byte

>
```

Use the `copy` operation command to copy the source file named `showtech.txt` to the memory card.

```
> copy ramdisk showtech.txt mc showtech.txt
```

Make sure the file has been written to the memory card by executing the following command:

```
> show mc-file

Date 2010/08/06 17:38:28 UTC
    File Date               Size Name
    2010/08/06 17:35       1,265 showtech.txt


>
```

4.3 Transferring files via FTP

Failure information copied to the RAMDISK can be transferred to a remote terminal via FTP by logging in to the Switch via FTP.

Make sure a VLAN and an IP address are set for the port used for the FTP connection.

On your PC, open the command prompt window. (For a standard Windows XP PC, select **Start**, **All Programs**, **Accessories**, and then **Command Prompt**.)

The following figure shows an example of transferring a file to the `C:\TEMP` directory on a PC with a Switch IP address of 192.168.0.1.

Figure 4-3 Transferring files via FTP

Log in to the Switch via FTP from an FTP client PC.

```
C:\TEMP>ftp 192.168.0.1            . . . . . Log in to the Switch from an FTP client PC.
Connected to 192.168.0.1
220 AX2530S-24T FTP server ready
User (192.168.0.1:(none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp> get showteck.txt              . . . . . Transfer the failure information file.
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp:xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye...see you later
C:\TEMP>
```

The failure information file is successfully transferred to the FTP client PC.

5. Line Testing

5.1 Testing a 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.

Figure 5-1 What loops back the test frames for various line test types

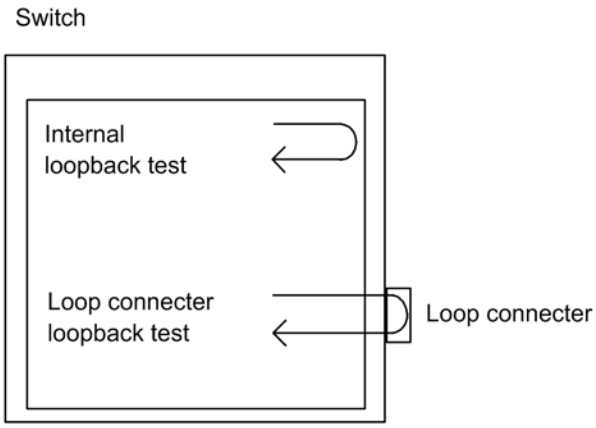


Table 5-1 Test types and fault locations to be identified

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)

The following table shows the fault locations suspected from the results of a line test.

Table 5-2 Fault locations suspected from the results of a line test

Internal loopback test results	Loop connector loopback test results	Suspected fault locations
Normal	Normal	● Cables in use ● Remote device
Normal	Error	● Cables in use ● Transceivers (SFP, SFP+) ● Loop connector
Error	Normal	Switch
Error	Error	Switch

For details about the conditions used to determine the normal and error statuses, see *5.1.1 Internal loopback test*.

5.1.1 Internal loopback test

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

The test procedure is described below.

1. Use the `inactivate` operation command to change the port to be tested into an inactive state.
2. Execute the `test interfaces` operation command with the `internal` parameter specified. Wait about one minute after the command is executed.
3. Execute the `no test interfaces` operation command, and then check the displayed results.
4. Use the `activate` operation command to change the port back into an active state.

The following figure shows an example of a test in which the sending interval of test frames is set to five seconds on port number 0/2.

Figure 5-2 Example of an internal loopback test

```
> inactivate gigabitethernet 0/2
> test interfaces gigabitethernet 0/2 internal interval 5 pattern 1 length 100
> no test interfaces gigabitethernet 0/2

Date 2010/08/06 04:07:39 UTC
Interface type             :100BASE-TX
Test count                 :13
Send-OK                    :13             Send-NG                :0
Receive-OK                 :13             Receive-NG             :0
Data compare error         :0
Out buffer hunt error      :0              Out line error         :0
In CRC error               :0              In alignment           :0
In monitor time out        :0              In line error          :0
H/W error                  :none

> activate gigabitethernet 0/2
```

After the test completes, check the following:

1. If the line test yields all of the following results, it has successfully completed:
   - `0` is indicated for `Send-NG`.
   - `0` is indicated for `Receive-NG`.
   - `0` is indicated for other error items (displayed items starting from `Data compare error`).
2. If the line test yields any of the following results, there might be some sort of problem:
   - A value other than `0` is indicated for `Send-NG`.
   - A value other than `0` is indicated for `Receive-NG`.
   - A value other than `0` is indicated for any other error items (displayed items starting from `Data compare error`).

   See the description of the `no test interfaces` operation command in the manual *Operation Command Reference*.

5.1.2 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` operation command to change the port to be tested into an inactive state.
2. Remove the cable from the target port, and then connect the loop connector to that port.#
3. Execute the `test interfaces` operation command with the `connector` parameter specified. Wait about one minute after the command is executed.
4. Execute the `no test interfaces` operation command, and then check the displayed results.
5. Remove the loop connector, and then reconnect the cable to the port.
6. Use the `activate` operation command to change 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.

For 10BASE-T, 100BASE-TX, and 1000BASE-T SFP ports, use the following loop connectors:

Table 5-3 Loop connectors for 10BASE-T, 100BASE-TX, and 1000BASE-T SFP ports

Model	Port number	
AX2530S-24T AX2530S-24T4X	0/25 to 0/28	10BASE-T/100BASE-TX/1000BASE-T loop connector
AX2530S-48T AX2530S-48T2X	0/49 to 0/52	10BASE-T/100BASE-TX/1000BASE-T loop connector
AX2530S-24S4X	0/1 to 0/24	10BASE-T/100BASE-TX loop connector or 10BASE-T/100BASE-TX/1000BASE-T loop connector
	0/25 to 0/28	10BASE-T/100BASE-TX/1000BASE-T loop connector

You can check the test results in the same way as described in *5.1.1 Internal loopback test*.

5.1.3 Creating loop connectors

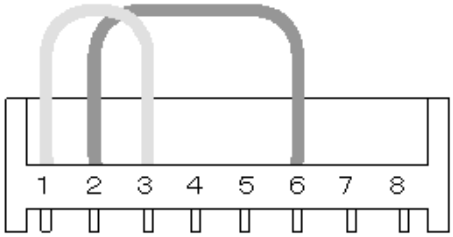
(1) Required tools and materials

- Cable
- Modular plug
- Crimping tool
- Nipper
- Cutter

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

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

Figure 5-3 Overview of a 10BASE-T/100BASE-TX loop connector



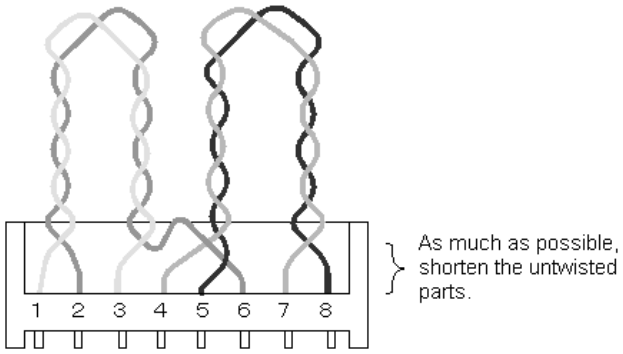
(3) 10BASE-T/100BASE-TX/1000BASE-T loop connector

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

Figure 5-4 Twisted pair cable

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

Figure 5-5 Overview of a 10BASE-T/100BASE-TX/1000BASE-T loop connector



Note that the 1000BASE-T loop connector above is only supported for loop operation for the Switch. (Loop operation by the 1000BASE-T connector is a non-standard, proprietary action.)

Appendix

A Detailed Display Contents of the show tech-support Command

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

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

The following table lists descriptions of the content that is displayed when protocol parameters are used with the `show tech-support` operation command.

For details on the displayed information, see the manual *Operation Command Reference*. For details about the commands for which the Description field indicates "OAN", see the OAN manuals.

[Note]

The manual *Operation Command Reference* does not cover part of the information displayed by the `show tech-support` operation command. Such information is not disclosed to the public because it contains internal information related to the Switch (the commands for which the Description field indicates "Switch internal information").

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

Table A-1 Displayed information

No.	Command (displayed)	Description	No parameter specified	layer-2 specified
1	`show clock`	Time set on the Switch	Y	Y
2	`show version`	Software version and hardware information of the Switch	Y	Y
3	`show system`	Operating status of the device	Y	Y
4	`show environment`	FAN/power supply/operating time information	Y	Y
5	`show environment temperature-logging`	Temperature history information	Y	Y
6	`show running-config`	Running configuration	Y	Y
7	`show startup-config`	Startup configuration file	Y	Y
8	`show sessions`	Login session information	Y	Y
9	`show users`	User information	Y	Y
10	`show radius-server`	RADIUS server information	Y	Y
11	`show radius-server statistics`	RADIUS server statistics	Y	Y
12	`show radius-server statistics summary`	RADIUS server statistics summary	Y	Y
13	`show ntp-client`	NTP client information	Y	Y
14	`show power`	Power consumption information	Y	Y
15	`show power-control port`	Port power saving status information	Y	Y

No.	Command (displayed)	Description	No parameter specified	layer-2 specified
16	show power-control schedule	Power saving schedule information	Y	Y
17	show mc-file	Information on files stored on the memory card	Y	Y
18	show ramdisk-file	Information on files stored on the RAMDISK	Y	Y
19	show mc	Memory card usage	Y	Y
20	show ramdisk	RAMDISK usage	Y	Y
21	show critical-logging summary	Switch failure log information	Y	Y
22	show critical-logging	Detailed switch failure log information	Y	Y
23	show logging	Operation log information	Y	Y
24	show logging reference	Reference log information	Y	Y
25	show logging	Log information at the specified event level	Y	Y
26	show cpu (days/hours)	CPU usage (in days or hours)	Y	Y
27	show cpu (minutes/seconds)	CPU usage (in minutes or seconds)	Y	Y
28	show memory summary	Memory usage of the device	Y	Y
29	show interfaces detail	Detailed statistics for ports	Y	Y
30	show port	Port information	Y	Y
31	show port statistics	Port statistics	Y	Y
32	show port protocol	Protocol information for ports	Y	Y
33	show port transceiver	Transceiver details for ports	Y	Y
34	show port vlan	VLAN information for ports	Y	Y
35	show channel-group summary	Link aggregation information	Y	Y
36	show channel-group detail	Link aggregation details	Y	Y
37	show channel-group statistics	Link aggregation statistics	Y	Y
38	show channel-group statistics lacp	LACP statistics for link aggregation	Y	Y
39	show mac-address-table	MAC address table information	Y	Y
40	show mac-address-table learning-counter	Number of learned addresses in the MAC address table	Y	Y

No.	Command (displayed)	Description	No parameter specified	layer-2 specified
41	`show vlan summary`	VLAN information	Y	Y
42	`show vlan detail`	VLAN details	Y	Y
43	`show vlan mac-vlan`	MAC VLAN information	Y	Y
44	`show spanning-tree detail`	Spanning Tree details	Y	Y
45	`show spanning-tree port-count`	Numbers handled by Spanning Tree Protocols	Y	Y
46	`show spanning-tree statistics`	Spanning Tree statistics	Y	Y
47	`show axrp detail`	Ring Protocol details	Y	Y
48	`show ip dhcp snooping`	DHCP snooping information	Y	Y
49	`show ip dhcp snooping binding`	DHCP snooping binding database information	Y	Y
50	`show ip dhcp snooping statistics`	DHCP snooping statistics	Y	Y
51	`show ip arp inspection statistics`	Dynamic ARP inspection statistics	Y	Y
52	`show igmp-snooping`	IGMP snooping information	Y	Y
53	`show igmp-snooping group`	IGMP snooping group information	Y	Y
54	`show igmp-snooping statistics`	IGMP snooping statistics	Y	Y
55	`show mld-snooping`	MLD snooping information	Y	Y
56	`show mld-snooping group`	MLD snooping group information	Y	Y
57	`show mld-snooping statistics`	MLD snooping statistics	Y	Y
58	`show ip-dual interface`	Information for IPv4 and IPv6 interfaces	Y	Y
59	`show ip arp`	ARP information	Y	Y
60	`show ip route`	Static route information	Y	Y
61	`show ipv6 neighbors detail`	NDP information	Y	Y
62	`show ipv6 router-advertisement`	RA information	Y	Y
63	`show access-filter`	Statistics on filters	Y	Y
64	`show qos-flow`	QoS control function statistics	Y	Y
65	`show qos queueing`	Statistics on the send queues of all ports	Y	Y

No.	Command (displayed)	Description	No parameter specified	layer-2 specified
66	`show authentication fail-list`	Information on terminals that failed to pass Layer 2 authentication	Y	Y
67	`show authentication logging`	Operation log information for all Layer 2 authentication events	Y	Y
68	`show dot1x detail`	IEEE 802.1X authentication status information	Y	Y
69	`show dot1x statistics`	IEEE 802.1X statistics	Y	Y
70	`show dot1x logging`	IEEE 802.1X operation log information	Y	Y
71	`show web-authentication`	Web authentication settings	Y	Y
72	`show web-authentication html-files detail`	Information on the registered Web authentication page files	Y	Y
73	`show web-authentication user edit`	Entries registered or changed in the internal Web authentication DB	Y	Y
74	`show web-authentication user commit`	Entries registered in the internal Web authentication DB	Y	Y
75	`show web-authentication login select-option detail`	Detailed information on users authenticated by Web authentication	Y	Y
76	`show web-authentication login summary port`	Information on users authenticated by Web authentication (by port)	Y	Y
77	`show web-authentication login summary vlan`	Information on users authenticated by Web authentication (by VLAN)	Y	Y
78	`show web-authentication logging`	Operation log information for Web authentication.	Y	Y
79	`show web-authentication redirect target`	External Web server redirection information used for Web authentication	Y	Y
80	`show web-authentication statistics`	Web authentication statistics	Y	Y
81	`show ip dhcp binding`	Binding information on the DHCP server	Y	Y
82	`show ip dhcp conflict`	Information on IP address conflicts detected on the DHCP server	Y	Y
83	`show ip dhcp server statistics`	Statistics about the DHCP server	Y	Y
84	`show mac-authentication`	MAC-based authentication settings	Y	Y
85	`show mac-authentication login select-option detail`	Detailed information on terminals authenticated by MAC-based authentication	Y	Y
86	`show mac-authentication login summary port`	Information on terminals authenticated by MAC-based authentication (by port)	Y	Y

No.	Command (displayed)	Description	No parameter specified	layer-2 specified
87	`show mac-authentication login summary vlan`	Information on terminals authenticated by MAC-based authentication (by VLAN)	Y	Y
88	`show mac-authentication logging`	Operation log information for MAC-based authentication	Y	Y
89	`show mac-authentication statistics`	MAC-based authentication statistics	Y	Y
90	`show mac-authentication mac-address edit`	Entries registered or changed in the internal MAC-based authentication DB	Y	Y
91	`show mac-authentication mac-address commit`	Entries registered in the internal MAC-based authentication DB	Y	Y
92	`show authentication multi-step`	Information on terminals authenticated by multistep authentication	Y	Y
93	`show wol`	Information on users using Secure Wake-on-LAN	Y	Y
94	`show wol-authentication user edit`	Entries registered or changed in the internal DB for Secure Wake-on-LAN user authentication	Y	Y
95	`show wol-authentication user commit`	Entries registered in the internal DB for Secure Wake-on-LAN user authentication	Y	Y
96	`show wol-device name edit`	Entries registered or changed in the internal DB for registering terminals that send the Secure Wake-on-LAN startup command	Y	Y
97	`show wol-device name commit`	Entries registered in the internal DB for registering terminals that send the Secure Wake-on-LAN startup command	Y	Y
98	`show license`	License information	Y	Y
99	`show gsrp aware`	GSRP aware information	Y	Y
100	`show switchport-backup`	Uplink redundancy information	Y	Y
101	`show switchport-backup statistics`	Statistics on the flush control frame transmission functionality of uplink redundancy	Y	Y
102	`show switchport-backup mac-address-table update`	MAC address update functionality settings for uplink redundancy	Y	Y
103	`show switchport-backup mac-address-table update statistics`	Statistics on the MAC address update functionality for uplink redundancy	Y	Y
104	`show sml`	SML status information	Y	Y
105	`show sml channel-group`	SML channel group information	Y	Y

No.	Command (displayed)	Description	No parameter specified	layer-2 specified
106	show sml channel-group summary	SML channel group summary information	Y	Y
107	show efmoam	IEEE 802.3ah/OAM functionality information	Y	Y
108	show efmoam statistics	Statistics on the IEEE 802.3ah/OAM functionality	Y	Y
109	show storm-control detail	Storm control information	Y	Y
110	show loop-detection	Information on the L2 loop detection functionality	Y	Y
111	show loop-detection logging	Log information for the L2 loop detection functionality	Y	Y
112	show loop-detection statistics	Statistics on the L2 loop detection functionality	Y	Y
113	show cfm	CFM information	Y	Y
114	show cfm summary	CFM details (the number of MPs and CFM ports that can be accommodated)	Y	Y
115	show cfm remote-mep	CFM remote MEP information	Y	Y
116	show cfm remote-mep detail	CFM remote MEP details	Y	Y
117	show cfm fault	Information on faults detected by CFM continuity checks	Y	Y
118	show cfm fault detail	Details on faults detected by CFM continuity checks	Y	Y
119	show cfm l2traceroute-db	CFM linktrace database information	Y	Y
120	show cfm l2traceroute-db detail	CFM linktrace database details	Y	Y
121	show cfm statistics	CFM statistics	Y	Y
122	show snmp engineID local	Engine ID of the SNMP agent	Y	Y
123	show sflow detail	Display of sFlow statistics (details)	Y	Y
124	show lldp neighbors	Summary of neighboring device information for the LLDP functionality	Y	Y
125	show lldp detail	Neighboring device information for the LLDP functionality	Y	Y
126	show lldp statistics	LLDP functionality statistics	Y	Y
127	show auto-config	OAN: AUTOCONF functionality status information	Y	Y

No.	Command (displayed)	Description	No parameter specified	layer-2 specified
128	`show auto-config neighbor`	OAN: AUTOCONF functionality neighboring information	Y	Y
129	`show config-lock-status`	OAN: Locking status	Y	Y
130	`show netconf`	OAN: NETCONF functionality status information	Y	Y
131	`show netconf denied-host`	OAN: Access rejected status information	Y	Y
132	`show software-update user`	OAN: User list information for software updates	Y	Y
133	`show on-api webauth-html-file user`	OAN: User list information related to replacement HTML files for the Web authentication login page	Y	Y
134	`show on-api energy-saving user`	OAN: User list information for the power saving setting functionality	Y	Y
135	`Detail Information`	Switch internal information	Y	Y
136	`Detail Layer-2 Information`	Switch internal information: L2 protocol detailed information	N	Y

Legend: Y: Displayed, N: Not displayed

Index