ALAXALA AX2200S/AX1250S/AX1240S

Troubleshooting Guide

AX1240S-T001X-70

AlaxalA

■ Relevant products

This manual applies to models of the AX2200S series switch, the AX1250S series switch, and the AX1240S series switch.

■ 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.
- Wake on LAN is a registered trademark of IBM Corp.
- 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 using the product, 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

July 2012 (Edition 8) AX1240S-T001X-70

■ Copyright

■ History of Amendments

(Edition 8)

Summary of amendments

Location and title	**Changes**
Addition of series	● A description of AX2200S series switches was added.
3.3.4 Update by using the ppupdate operation command is not possible	● The description related to action against failure to update prior to Ver. 2.4 software was changed. [AX1240S]
3.3.5 Restoring data by using the restore operation command is not possible	● The description related to action against failure to restore backup files including those prior to Ver. 2.4 software was changed. [AX1240S]
3.4.5 Actions to be taken for PoE problems [AX2200S] [AX1240S]	● A description of AX2200S series switches was added.

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

(Edition 7)

Summary of amendments

Location and title	Changes
Failures occurring when the Ring Protocol functionality is used	● A description of the multi-fault monitoring functionality was added.

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

(Edition 6)

Summary of amendments

Location and title	Changes
Update by using the ppupdate operation command is not possible	● A description related to action against failure to update prior to Ver. 2.3.A software was added. [AX1240S]
Restoring data by using the restore operation command is not possible	● A description related to action against failure to restore backup files including those prior to Ver. 2.3.A software was added. [AX1240S]

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

(Edition 5)

Summary of amendments

Location and title	Changes
NTP communication failures	● The description related to checking the time zone was changed.
Failures in long-life solution support	● This subsection was added.
Appendix A Detailed Description of the "show tech-support" Command	● This chapter was added.

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

(Edition 4)

Summary of amendments

Location and title	Changes
Addition of series	● A description of AX1250S was added.
Actions to be taken for 100BASE-FX [AX1250S]/1000BASE-X problems	● A description of 100BASE-FX was added.

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

(Edition 3)

Summary of amendments

Location and title	**Changes**
Login-related problems : troubleshooting : login-related problem : login	● The actions to be taken were changed.
Failures occurring when the Ring Protocol functionality is used	● This subsection was added.

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

(Edition 2)

Summary of amendments

Location and title	**Changes**
Overview of failure analysis of the Switch or a part of the Switch	● Some of the description of LEDs were changed.
Restoring information by using the restore operation command not possible	● The actions to be taken were changed.
Communication failures when using IEEE 802.1X	● The actions to be taken were changed.
Communication failures occurring when Web authentication is used	● The actions to be taken were changed.
Communication failures occurring when MAC-based authentication is used	● The actions to be taken were changed.
Communication failures when using secure Wake-on-LAN [OP-WOL]	● The actions to be taken were changed.
Communication failures occurring when uplink redundancy is used : when uplink redundancy used : troubleshooting communication failures	● Items for analyzing failures were added. ● The actions to be taken were changed.
Power saving functionality failures	● This subsection was added.

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

Preface

Relevant products

This manual applies to the models of AX2200S, AX1250S, and AX1240S series switches. The manual describes the functionality of software supported by OS-LT4, OS-LT3, and OS-LT2 software and the optional licenses.

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 to both AX2200S, AX1250S, and AX1240S series switches. Functionality specific to either AX2200S, AX1250S, or AX1240S series switches are indicated as follows:

[AX2200S]:

The description applies to the AX2200S switch.

[AX1250S]:

The description applies to the AX1250S switch.

[AX1240S]:

The description applies to the AX1240S switch.

Unless otherwise noted, this manual describes the functionality applicable to the OS-LT4, OS-LT3, and OS-LT2 functionalities. Functionality specific to an optional license is indicated as follows:

[OP-WOL]:

The description applies to the OP-WOL optional license.

[OP-OTP]:

The description applies to the OP-OTP optional license.

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

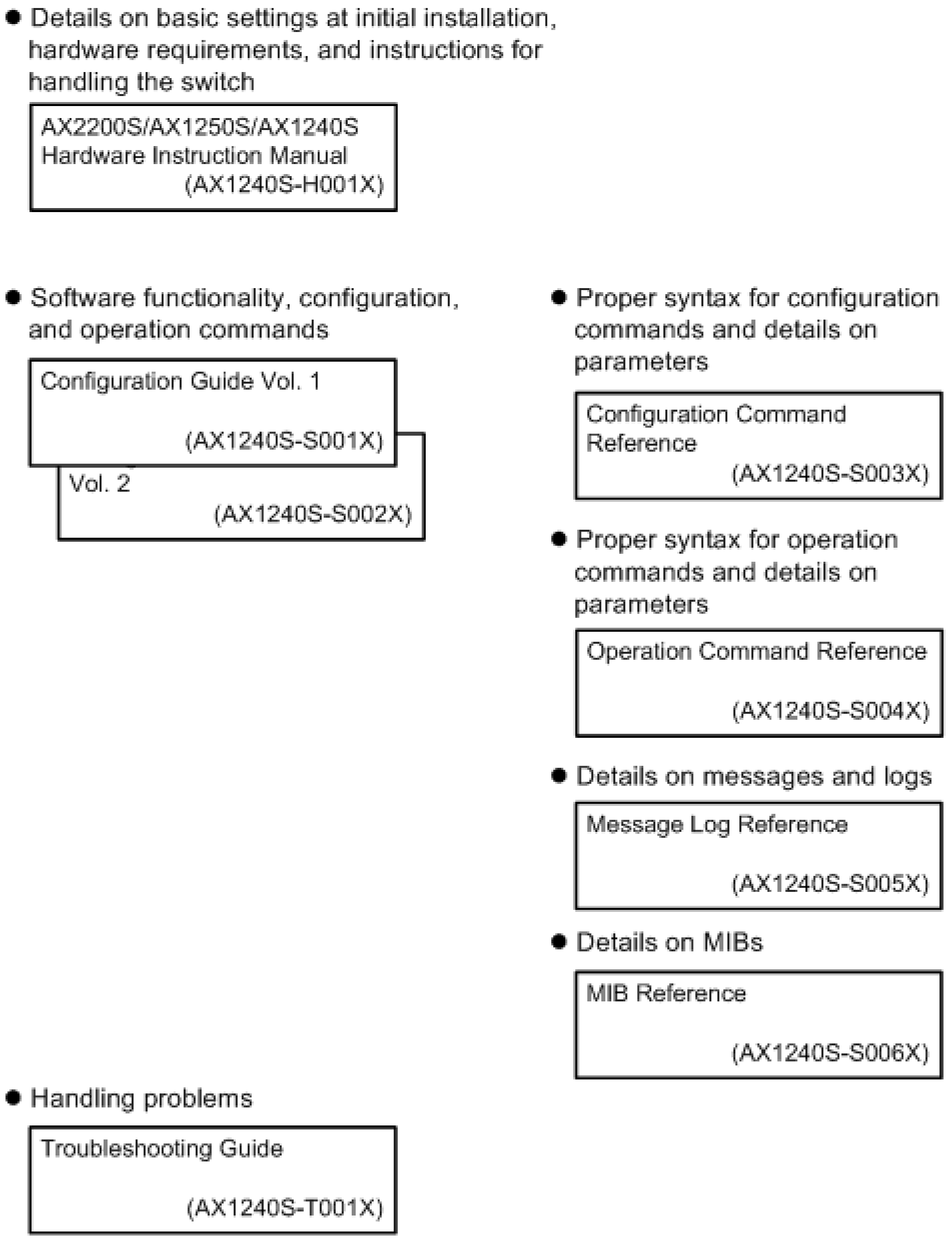
Manual URL

You can view this manual at the following Web site:

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.



- Details on basic settings at initial installation, hardware requirements, and instructions for handling the switch

AX2200S/AX1250S/AX1240S Hardware Instruction Manual (AX1240S-H001X)

- Software functionality, configuration, and operation commands

Configuration Guide Vol. 1 (AX1240S-S001X)

Vol. 2 (AX1240S-S002X)

- Proper syntax for configuration commands and details on parameters

Configuration Command Reference (AX1240S-S003X)

- Proper syntax for operation commands and details on parameters

Operation Command Reference (AX1240S-S004X)

- Details on messages and logs

Message Log Reference (AX1240S-S005X)

- Details on MIBs

MIB Reference (AX1240S-S006X)

- Handling problems

Troubleshooting Guide (AX1240S-T001X)

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

bit/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
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: KB, MB, GB, and TB

This manual uses the following conventions: 1 KB (kilobyte) is 1,024 bytes.1 MB (megabyte) is 1,024^2 bytes.1 GB (gigabyte) is 1,024^3 bytes.1 TB (terabyte) is 1,024^4 bytes.

Conventions: The terms "Switch" and "switch"

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

- AX2200S series switches
- AX1250S series switches
- AX1240S series switches

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.

⚠ Safety Information

Using AX2200S, AX1250S, and AX1240S series switches correctly and safely

- This manual provides important information intended to ensure safe use of AX2200S, AX1250S, and AX1240S series switches. Please read this manual completely before using the Switches.
- 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 regarding 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 serious 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 coming from the Switch, or if liquid is spilled into the Switch or a foreign object falls into the Switch, immediately turn off power to the Switch as described below. Continuing operation could result in a fire or electric shock.

Actions to take for abnormal conditions

Action to take
Turn off the Switch and 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 a fire or electric shock.

Do not alter the physical makeup of 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 a fire or electric shock.

Do not place anything 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 flower pot, on the Switch. Liquid or metallic objects falling into the Switch could result in a fire or electric shock.

Use the Switch only with the indicated power supply setting.

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

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.

⚠WARNING

Ground the Switch.

- Always use a grounded outlet. Failure to do so might not only result in electric shock, but it might also introduce unwanted electrical noise that could cause a Switch failure.

Handle power cables carefully.

- Do not place anything heavy on a power cable. Do not pull, bend, or modify a cable. Doing so could damage the cable, resulting in a fire or electric shock. If the power cable is covered by a carpet, it is easy to forget that the cable is there and to place something heavy on it.
- Do not use any power cables other than those included with or specified for the AX2200S or AX1250S series switch. Using another power cable could result in a fire or electric shock. Do not use the supplied power cable for any device. Doing so could result in a fire or electric shock.
- The AC power supply cable included with the AX1240S series is for use only with the Switch. It cannot be used with any other device. Using the power cable with another device is very dangerous and could result in fire or electric shock.
- When using the switch at 200 V AC, use a power cable that satisfies the specified specifications. Using another power cable 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 a 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, so that it is not loose. Using a power plug with dust on it or one that is imperfectly connected could result in a 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, which can then affect other equipment.

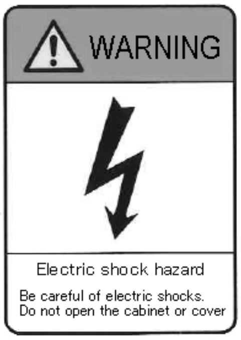
Do not use an air duster near a flame.

- 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 remove the Switch cover.

- Do not remove the Switch cover. Doing so could result in electric shock. The following label is affixed to a Switch.



⚠ WARNING

Electric shock hazard

Be careful of electric shocks.
Do not open the cabinet or cover

⚠CAUTION

Do not place the Switch in a place where it is unstable.

- If placing the Switch on a desk, lay it on its side on a workbench capable of withstanding the weight of the Switch. If, for example, you place the Switch on a shaky table or a tilted surface, the Switch might fall and possibly injure someone.
- When installing the Switch in a rack, make sure the Switch in the rack is stably positioned. If the Switch is not positioned correctly, injury could result from falling equipment or stumbling over the equipment.

Do not position the Switch vertically or lean it against a wall

- When installing the Switch on a table, position the Switch horizontally. If the switch is positioned vertically or leaned against a wall, the switch might fall, which could result in injury or damage.

Do not allow hair or objects near the ventilation slots

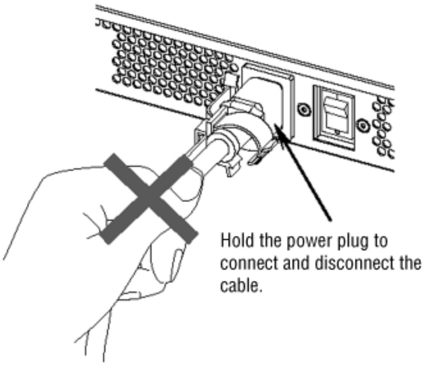
- The AX2230S-24P, AX1240S-24P2C, and AX1240S-48T2C is equipped with internal cooling fan units. Do not allow hair or other objects near the ventilation slots, because they might be sucked into the Switch, resulting in injury.

When moving the Switch

- Before moving the Switch, you must turn it off and unplug all cables. Failure to do so might cause the Switch or cable to become damaged, resulting in a 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.

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.



Hold the power plug to connect and disconnect the cable.

⚠CAUTION

Use the Switch's power button to turn off the Switch power.

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 metals. 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.

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.

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

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

Cleaning

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

CAUTION

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

- As the AX2230S-24T, AX1250S-24T2C, and AX1240S-24T2C are fanless models, heat also dissipates from the top panels of these switches. To ensure adequate heat dissipation, do not stack another device on top of or below the Switch. Contact could result in a malfunction.
  When mounting these switches in a rack, keep a space of 1U or more between them.

Do not place the 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 the Switch.

- Placing the 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 near an ocean

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

  - An area where oily smoke is present

  - An area where continuous vibrations are present

Do not obstruct the ventilation slots.

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

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

- Turn off the power of the Switch before connecting or disconnecting the power supply cable.

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

- Turning on the Switch causes an 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 electrical power equipment.

CAUTION

Handle memory cards carefully.

- When inserting a memory card, do not push the card too strongly or flick it with your finger. 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. 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.

Do not attach any labels to a transceiver.

- A label attached to the transceiver indicates that the transceiver 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 the mechanism that prevents the transceiver from coming loose from the cage.

  Attaching a label on an interfering part with heat radiation or the mechanism to avoid dropping from the cage might cause a failure in the transceiver or damage to the device.

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

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

  - AX1250S-24T2C (ports 25 to 26)

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

  - AX2230S-24T (ports 25 to 28)

  - AX2230S-24P (ports 25 to 28)

  - AX1250S-24T2C (ports 25 to 26)

  - AX1240S-24T2C (ports 25 to 26)

  - AX1240S-24P2C (ports 25 to 26)

  - AX1240S-48T2C (ports 49 to 50)

CAUTION

Wear an antistatic wrist strap when carrying or packing a switch.

- 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 packing a transceiver or a memory card. Also, when storing a module, use an antistatic bag.

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.

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 on an AX2200S, AX1250S, or AX1240S series switch.

When failure analysis requires looking at the actual Switch, do the analysis according to *1.2 Overview of failure analysis for the entire Switch or a part of the Switch*.

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

1.2 Overview of failure analysis for the entire Switch or a 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 AX1240S-24T2C switch shown in the following figure and Table *1-1 LED indications, buttons, and connectors*.
Front panel layout

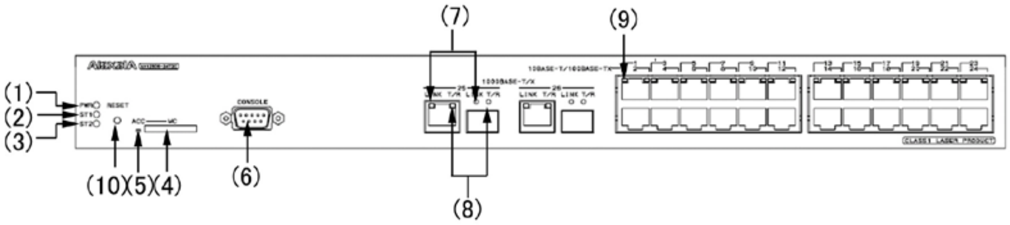


Table 1-1 LED indications, buttons, and connectors

No.	Model name	Type	Functionality	Description
1	PWR	LED: Green	Indicates whether the Switch is on.	Green: Power is on. Green, slowly blinking: The Switch is in the sleep state. Off: Power is off or the power supply failed.
2	ST1	LED: Green, orange, or red	Indicates the Switch status.	Green: Available for operation Blinking green: Preparatory state (switch starting up) Green, slowly blinking: The LED is set to be turned off. Orange: Initial state after the Switch is turned on. Red, blinking: A failure has occurred in a part of the Switch. Red: A fatal error has occurred on the Switch (the Switch is no longer usable). Off: The Switch is off or a power failure has occurred.
3	ST2	LED:Orange	(Not used)	Orange: Initial state after the Switch is turned on. Off: Turned off because it is no longer used after Switch startup has been completed.
4	MC	Connector	Memory card slot	Memory card slot
5	ACC	LED: Green	Indicates the memory card status.	On: 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	RS-232C port to connect a console terminal

No.	Model name	Type	Functionality	Description
7	LINK	LED: Green	Indicates the operating status of a 1000BASE-T/1000BASE-X Ethernet port.	Green: Initial state after the Switch is turned on or a link is established. Off: If the ST1 LED is green, a link failure has occurred or the port is blocked.
8	T/R	LED: Green		Blinking green: Frames are being sent or received.
9	1-24	LED: Green or orange	Indicates the operating status of a 10BASE-T/100BASE-TX Ethernet port.	Green: A link has been established. Green, blinking: A link has been established and a frame is being transmitted. Orange: Initial state after the Switch is turned on. Off: If the ST1 LED is green, a link failure has occurred or the port is blocked.
10	RESET	Button (Non-locking)	Manual reset button for the device	Restarts the Switch. The Switch is in the sleep state: Pressing and holding this button until all front LEDs turn on (three seconds or more) wakes the Switch up.

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 functional failure analysis

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

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

Category	**Sub-category**	**See**
Forgotten login password	Forgotten login user password	*3.1.1 Forgotten login password*
	Forgotten login user ID	*3.1.2 Forgotten login user ID*
	Forgotten device administrator password	*3.1.3 Forgotten administrator mode 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 appear correctly*
	Remote login to the switch not possible	*3.2.2 Login from a remote terminal is not possible*
	Login authentication not possible	*3.2.3 Login authentication using RADIUS is not possible*
	Commands cannot be entered : cannot be entered	*3.2.4 Commands cannot be entered*
Problems occurring while saving files : troubleshooting : saving	Copying data to the startup configuration file	*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*
	Update by using the ppupdate operation command is 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 : troubleshooting	*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 communication failure	*3.4.2 Actions to be taken for 10BASE-T/100BASE-TX problems [AX1250S] [AX1240S]*
	10BASE-T/100BASE-TX/1000BASE-T communication failure	*3.4.3 Actions to be taken for 10BASE-T/100BASE-TX/1000BASE-T problems*

Category	Sub-category	See
	100BASE-FX [AX1250S] /1000BASE-X communication failure	*3.4.4 Actions to be taken for 100BASE-FX [AX1250S]/1000BASE-X problems*
	PoE problems [AX2200S] [AX1240S]	*3.4.5 Actions to be taken for PoE problems [AX2200S] [AX1240S]*
	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*
Layer 2 authentication communication failures	––	*3.7.1 Communication failures occurring when IEEE 802.1X is used*
	––	*3.7.2 Communication failures occurring when Web authentication is used*
	––	*3.7.3 Communication failures occurring when MAC-based authentication is used*
	––	*3.7.4 Communication failures occurring when secure Wake-on-LAN is used [OP-WOL]*
Communication failures in the high-reliability functionality based on a redundant configuration : in high-reliability functionality based on redundant configuration : communication failures in high-reliability functionality based on redundant configuration : troubleshooting	Uplink redundancy failure	*3.8.1 Communication failures occurring when uplink redundancy is used*
SNMP communication failures	The MIB cannot be obtained.	*3.9.1 MIBs cannot be obtained from the SNMP manager*

Category	Sub-category	See
	Traps cannot be received.	*3.9.2 Traps cannot be received by the SNMP manager*
Information about neighboring devices by the LLDP functionality cannot be obtained.	––	*3.10.1 Neighboring device information cannot be obtained by the LLDP functionality*
NTP communication failures	––	*3.11 NTP communication failures*
Communication failures when the IEEE 802.3ah/UDLD functionality is used	Port in inactivate status	*3.12.1 Port is in inactivate status by the IEEE 802.3ah/UDLD functionality*
Communication failures caused by discarded packets	––	*3.13.1 Checking the filtering and QoS control configuration information*
Port mirroring failures : failures : port mirroring failures : port mirroring failures	––	*3.14 Port mirroring failures*
Power saving functionality failures	––	*3.15.1 LED brightness control is disabled*
	––	*3.15.2 Power saving functionality scheduling is disabled*
Failures in long-life solution support	––	*3.16.1 Failures occurring when long-life solution is supported*
Additional Information	––	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

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

Table 2-1 Troubleshooting switch failures

No.	Failure description	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. 3. 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.	See *2.1(1) Action to take when the Switch stops and the PWR LED turns off* to isolate the problem.
4	The red ST1 LED of the switch is on.	The Switch may be experiencing a failure. See*4 Obtaining Failure Information* in this manual to use the `show tech-support` operation command to collect switch information. 1. Turn the Switch off and then on again to restart the Switch. 2. If you can restart the Switch, execute the `show critical-logging` operation command to check the failure information. `>show critical-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 (see the *Message Log Reference*).
5	The red ST1 LED of the switch blinks.	See*(2) Action to take when the red ST1 LED blinks and the LINK LED turns off* to isolate the problem.
6	The orange ST1 LED of the Switch is on.	This indicates the initial state when the power is turned on. Wait a while.
7	The LINK LED (1000BASE-T or 1000BASE-X port) and the 1-48 LED (10BASE-T or 100BASE-TX port) of each port on the Switch are off.	See *(2) Action to take when the red ST1 LED blinks and the LINK LED turns off* to isolate the problem.

(1) Action to take when the Switch stops and the PWR LED turns off

Take action according to the following table.

Table 2-2 Action to take when the Switch stops and the PWR LED turns off

No.	Failure description	Action
1	The power button of the Switch is off.	Turn on the Switch.
2	The power cable is disconnected or loose.	Perform the following procedure: 1. Turn off the Switch. 2. Connect the power cable correctly. 3. Turn on the Switch.
3	The measured input voltage is outside the following range: For 100 V AC: 90 to 127 V AC For 200 V AC: 180 to 254 V AC Note: Take this action only if the input voltage can be measured.	This is a power facility failure (not a Switch failure). Ask the person responsible for the facility to take action.

(2) Action to take when the red ST1 LED blinks and the LINK LED turns off

Take action according to the following table.

Table 2-3 Action to take when the red ST1 LED blinks and the LINK LED is off

No.	Failure description	Action
1	When failure information can be checked by executing the `show logging` operation command as follows: `>show logging`	Take action according to the failure information (see the manual *Message Log Reference*). More specifically, take the following actions: 1. Replace the Switch. 2. Replace the transceiver (SFP). 3. Modify the configuration. 4. Replace the software. 5. Check the cable connection. 6. Check the status of the installed transceiver (SFP). 7. Additional Information
2	When failure information cannot be checked	Replace the Switch.

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 password

During operation, if a user forgets his or her password and is unable to log in to the Switch, perform the following procedure:

- Restart the Switch, and then press CTRL+N three or more times.

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

- When the Switch has restarted, use the `password` operation command to set a password.
- Restart the Switch.

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

3.1.2 Forgotten login user ID

During operation, if the user forgets the login user ID and is unable to log in to the Switch, perform the following procedure:

- Restart the Switch, and then press **CTRL**+**N** three or more times.

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

- When the Switch has restarted, the user can use the login user ID `operator` to log in to the Switch.
- After logging in to the Switch, use the `rename user` operation command to change the login user ID.
- Restart the Switch.

  The startup configuration file and the changed login user ID information are loaded.

3.1.3 Forgotten administrator mode password

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

- Restart the Switch, and then press **CTRL**+**N** three or more times.

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

- When the Switch has restarted, use the `password` operation command to set the device administrator password.
- 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 appear 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.	Failure description	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 failure analysis for the entire Switch or a part of the Switch*. 2. Check whether the cables are connected correctly (for example, check for incomplete insertion). 3. Make sure an RS-232C 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: 9,600 bps (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 software communication speed by doing the following: 1. If the communication speed of CONSOLE (RS-232C) was not specified by using the `line console speed` operation command, make sure that the communication speed of the communication software is set to 9,600 bps. 2. If the communication speed of CONSOLE (RS-232C) has been set to 1,200, 2,400, 4,800, 9,600, or 19,200 bps by using the `line console speed` operation command, make sure that the communication speed of the communication software is set correctly.
4	Unexpected characters are displayed when entering a user ID.	The communication speed of CONSOLE (RS-232C) might have been changed. See No. *3*.

No.	Failure description	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. Execute the procedure described in *3.1 Login-related problems*. If you are unable to log in, the internal flash memory might be corrupted. Try to execute the `format flash` operation command.
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 window 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 window size setting of the communication software to 80 characters by 24 lines to increase the number of characters that can be displayed on one line.

3.2.2 Login from a remote terminal is not possible

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

Table 3-2 Problems occurring during connection to a remote 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.

No.	Problem	Action
2	Login is not possible.	Perform the following procedure: 1. Make sure that the `line vty` or `ftp-server` configuration command 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 whether there is no terminal left and waiting for a login operation to be completed (that is, a terminal waiting for a user ID or password to be entered or which has failed to log in). If there is such a terminal, terminate the communication software at the terminal. 5. Check whether a connection from a remote terminal to the Switch was temporarily lost and then restored during a login operation. If a connection from a remote operation terminal to the Switch has been lost and then restored when the terminal is being logged in, the session information will remain in the Switch, which will prevent the remote operation terminal from newly logging in to the Switch until the TCP protocol of the session times out and the session is disconnected. Although the timeout period of the TCP protocol varies depending on the status of a remote terminal or the network, the protocol usually times out after 10 minutes.
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 logged out automatically (a maximum of 30 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 to the RADIUS server

Use the `ping` operation command if 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) × (*set-number-of-retry-attempts* + 1) ×

set-number-of-RADIUS-servers

If the time increases significantly, an application on a remote terminal, such as Telnet, might have terminated due to a timeout. If this happens, change the RADIUS configuration settings or the timeout setting of an application running on a remote terminal. In addition, Telnet or FTP might have failed even when a message indicating successful RADIUS authentication is output to the operation log. In this case, an application running on a remote 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) × *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` 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 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. If the "`Flash format complete.`" message indicating successful formatting is displayed, set the configuration again, and then save it in the startup configuration file. 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 not connected.` 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` 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 a 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` 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 too small, 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 critical-logging ramdisk` operation command to save a log file to the RAMDISK, make sure there is at least 300 KB of free space. 4. To execute the `show tech-support ramdisk` command to save Switch information to the RAMDISK, execute the del command to delete unnecessary files. 5. 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. If the "`Flash format complete.`" message indicating successful formatting is displayed, set the configuration again, and then save it in the startup configuration file. 2. If a message other than "`Flash format complete.`" is displayed, the file system might be corrupted.

3.3.4 Update by using the ppupdate operation command is not possible

If update by using the `ppupdate` operation command is not possible or if another similar problem occurs, check the status according to the following table.

Table 3-6 Problems occurring while using the `ppupdate` configuration command and action to take

No.	Items to check and commands	Items to check
1	Check the response message to the command.	1. When `Can't update software [ Hardware rev.x ]` is displayed, [AX1240S] Check the hardware revision number by using the `show version` operation command. If the hardware revision is shown as `1` or `9`, the normal procedure cannot be used to update with the update file for prior to Ver. 2.4 software. In this case, see the *Software Update Guide*. 2. When a response message other than the above is displayed, Check whether the update file specified by using the `ppupdate` operation command is applicable for the Switch. ● Check that the update file is applicable to the target Switch model. ● Check the update file, and then execute the `ppupdate` command again. 3. For all other cases, see No. *2*.
2	Try to execute the `show critical-logging` command.	● When `FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]` is obtained, 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

If restoring data by using the `restore` command is not possible or if another similar problem occurs, check the status according to the following table.

(1) When the restore command is executed on a restore from a AX2200S series Switch:

Table 3-7 Problems occurring while using the `restore` command and action to take [AX2200S]

No.	Items to check and commands	Items to check
1	Check the response message to the command.	When `Restore operation failed.` is displayed, ● If `no-software` is specified for the `backup` operation command, no-software must be specified for the `restore` operation command as well. ● Check that the backup file was created on the Switch that has the same model name as the Switch you are restoring the information to. ● Check the backup file, and then execute the `restore` operation command again. ● If an error still occurs, the backup file might be corrupted. For all other cases, see No. *2*.

No.	Items to check and commands	Items to check
2	Try to execute the `show critical-logging` command.	● When `FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]` is obtained, execute the `restore` operation command again. If an error still occurs, the internal flash memory might be corrupted. Replace the Switch.

(2) When the restore command is executed on a restore from a AX1250S series Switch:

Table 3-8 Problems occurring while using the `restore` command and action to take [AX1250S]

No.	Items to check and commands	Items to check
1	Check the response message to the command.	When `Restore operation failed.` is displayed, ● If `no-software` is specified for the backup operation command, `no-software` must be specified for the `restore` operation command as well. ● If software for an AX1240S or AX1230S switch is contained in the backup file, Switch information other than the software is restored. ● A backup file created by using the `backup` operation command with the AX1230 option specified is created as the Switch information, but without the software. To include software for AX1250S switches, create a backup file without specifying any options. ● Check the backup file, and then execute the `restore` operation command again. ● If an error still occurs, the backup file might be corrupted. For all other cases, see No. *2*.
2	Try to execute the `show critical-logging` command.	● When `FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]` is obtained, execute the `restore` operation command again. If an error still occurs, the internal flash memory might be corrupted. Replace the Switch.

(3) When the restore operation command is executed on a restore from a AX1240S series switch:

Table 3-9 Problems occurring while using the `restore` operation command and action to take [AX1240S]

No.	Items to check and commands	Items to check
1	Check the response message to the command.	When `Restore operation failed.` is displayed, Check the hardware revision number by using the `show version` command. ● If the hardware revision is shown as `1` or `9`, proceed to No. *2*. ● For other cases, go to No. *3*.
2	If the hardware revision is shown as `1` or `9`	The normal procedure cannot be used to restore a backup file containing software prior to Ver. 2.4. See the *Software Update Guide* to update the Switch to Ver. 2.4 or later. Then, execute the `restore` operation command again with the backup file for that prior to the Ver. 2.4 software.

No.	Items to check and commands	Items to check
3	If the hardware revision is shown as a number other than 1 and 9	● If no-software is specified for the backup operation command, no-software must be specified for the restore operation command as well. ● If software for an AX1250S or AX1230S switch is contained in the backup file, Switch information other than the software is restored. ● A backup file created by using the backup operation command with the AX1230 option specified is created as the Switch information, but without the software. To include software for AX1240S switches, create a backup file without specifying any options. ● Check the backup file, and then execute the restore operation command again. ● If an error still occurs, the backup file might be corrupted. For all other cases, see No. *4*.
4	Try to execute the show critical-logging command.	● When FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx] is obtained, 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 3.3.4*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 3-10 Checking the port status and action to take

No.	Items to check and commands	Action
1	Use the `show port` operation command to check the status of the target port.	For `dis`, continue with No. *2*. For `inact`, continue with No. *3* through *6*. For `down`, continue with No. *9*.
2	Use the `show running-config` operation command to check the configuration of the target port.	Check whether `no shutdown` is set for the target port. If `shutdown` is set, make sure the cable is connected to the target port, and then set `no shutdown` in the configuration.
3	Use the `show spanning-tree` operation command with the `detail` parameter specified to check the BPDU guard status of the target port.	If `Down` and `PortFast:BPDUguard(BPDU received)` are displayed for the target port, the BPDU guard functionality of Spanning Tree is being used, and the port has been blocked because the target port was receiving BPDs. Review the settings on the partner switch, and correct the configuration so that the Switch will not receive BPDUs. Go to No. *7*.
4	Use the `show logging` operation command to check the operation log for storm control.	If `STORM:Port<IF#> inactivated because of xxxx storm detection.` is recorded, the port has been blocked because a storm was detected on the target port. Use the `show logging` operation command to make sure the target port has recovered from the storm. Continue with No. *7*.
5	Use the `show efmoam` operation command to check the status of the target port.	If `Forced Down` is displayed, the port has been blocked because the IEEE 802.3ah/UDLD functionality detected a unidirectional link failure. After correcting the unidirectional link failure according to *3.12 Communication failures in the IEEE 802.3ah/UDLD functionality*, continue with No. *7*.
6	Use the `show loop-detection` operation command to check the status of the target port.	If `Down(loop)` is displayed, the port has been blocked due to reception of an L2 loop detection frame. Go to No. *7*.
7	Execute the `activate` operation command.	Use the `show spanning-tree` operation command to make sure that the target port is in the Up status and that `PortFast:BPDUguard(BPDU not received)` is displayed.
		Use the `show logging` operation command to make sure the target port's recovery from the storm has been completed.

No.	Items to check and commands	Action
		Use the `show efmoam` operation command to make sure information other than `Forced Down` or `Down` is displayed for the target port.
		Use the `show loop-detection` operation command to make sure that the port has been released from the blocked state set by the L2 loop detection frame and that `Up` is displayed.
		After checking the port as described above, if you are using the link aggregation standby link functionality, continue with No. *8*.
		If you are not using that functionality, continue with No. *9*.
8	Use the `show channel-group` operation command to check the link aggregation standby link status.	If `Mode:Static` and `Max Active Port:number-of-ports(link-down mode)` are displayed and `State:Detached` is displayed for the target port, the standby status is set. (The link-down port used as the operating port has been switched to the standby port by the standby link functionality). Wait until the display changes to `State:Distributing`.
9	Use the `show logging` operation command to check the operation log for the port.	Based on the log entry for the line displayed by the `show logging` operation command, see the *Message Log Reference* and take the action described for *Action*.

3.4.2 Actions to be taken for 10BASE-T/100BASE-TX problems [AX1250S] [AX1240S]

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

1. Viewing logged data

   For details about the information in the operation log, see the *Message Log Reference*.

2. Isolating the cause of the problem according to the failure analysis method

   Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-11 Failure analysis method for 10BASE-T/100BASE-TX problems [AX1250S] [AX1240S]

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 following item for the target line: If there is a count, see	Line quality is degraded.	Check the cable type. For the cable types, see the *Hardware Instruction Manual*.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly (for example, check for incomplete insertion). For cable connections, see the *Hardware Instruction Manual*.

No.	Items to check	Cause	Action
	the *Cause* and *Action* columns. ● `Link down`		Replace with the connection interface supported by the Switch. For the connection interfaces supported by the Switch, see the *Hardware Instruction Manual* and *Configuration Guides*.
2	Use the `show interfaces` operation command to display the receive-error statistics, and check whether there is a count for the following items for the target line: If there is a count, see the *Cause* and *Action* columns. ● `CRC errors` ● `Symbol errors`		Check the cable type. For the cable types, see the *Hardware Instruction Manual*.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly (for example, check for incomplete insertion). 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 *Configuration Guides*.
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.

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

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

1. Viewing logged data

   For details about the information in the operation log, see the *Message Log Reference*.

2. Isolating the cause of the problem according to the failure analysis method

   Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-12 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	Line quality is degraded.	Check the cable type. For the cable types, see the *Hardware Instruction Manual*.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.

No.	Items to check	Cause	Action
	whether there is a count for the following item for the target line: If there is a count, see the *Cause* and *Action* columns. ● `Link down`		Check whether the cables are connected correctly (for example, check for incomplete insertion). 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 *Configuration Guides*.
2	Use the `show interfaces` operation command to display the receive-error statistics, and check whether there is a count for the following items for the target line: If there is a count, see the *Cause* and *Action* columns. ● `CRC errors` ● `Symbol errors`		Check the cable type. For the cable types, see the *Hardware Instruction Manual*.
			Check the cable length. For the cable length, see the *Hardware Instruction Manual*.
			Check whether the cables are connected correctly (for example, check for incomplete insertion). 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 *Configuration Guides*.
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.
4	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the following item for the target port: If there is a count, see the *Cause* and *Action* columns. ● `Long frames`	Packets exceeding the maximum allowed frame length are received.	Adjust the jumbo frame settings to those on the remote device.

3.4.4 Actions to be taken for 100BASE-FX [AX1250S]/1000BASE-X problems

If a 100BASE-FX [AX1250S] /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 the *Message Log Reference*.

2. Isolating the cause of the problem according to the failure analysis method

Isolate the cause of the problem according to the failure analysis method described in the following table.

Table 3-13 Failure analysis method for 100BASE-FX [AX1250S] /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 following item 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. and remove any dirt.
			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.
2	Use the `show interfaces` operation command to display the receive-error statistics, and check whether there is a count for the following items for the target line: If there is a count, see the *Cause* and *Action* columns. ● `CRC errors` ● `Symbol errors`		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 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 that the transceiver (SFP) is connected correctly.
			Comply with the segment standard of the remote device.
			Check whether the optical level is correct.
3	Use the `show interfaces` operation command to display the failure statistics, and check whether there is a count for the following item for the target port: If there is a count, see the *Cause* and *Action* columns. ● `Long frames`	Packets exceeding the maximum allowed frame length are received.	Adjust the jumbo frame settings to those on the remote device.

No.	Items to check	Cause	Action
4	If automatic switching to the SFP transceiver does not occur when 1000BASE-SX2 is used, check the usage of the RJ45 port and the `media-type` setting.	Both an SFP transceiver and RJ45 cable are inserted when automatic media detection has been set.	When 1000BASE-SX2 and RJ45 are used, automatic switching to the SFP transceiver does not occur even if automatic media detection has been set because the 1000BASE-X (SFP) link is never enabled. To use 1000BASE-SX2, use either of the following methods: ● Use the `media-type` configuration command to set a fixed media (specify `sfp` or `rj45`). ● Make sure an optical fiber cable and a UTP (RJ45) cable are not inserted at the same time.
5	[AX1250S] 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 setting of the `speed`, `duplex`, or `media-type` configuration command is invalid.	Use configuration commands to specify the following settings: ● `speed:100` ● `duplex:full` ● `media-type:sfp`

3.4.5 Actions to be taken for PoE problems [AX2200S] [AX1240S]

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

Table 3-14 Communication failure analysis method when PoE is used

No.	Items to check and commands	Action
1	Use the `show power inline` operation command to check the information displayed for `Status` for the target port.	● `off` displayed: Power is not being supplied. Go to No. *2*. ● `denied` displayed: The supplied power is insufficient for the entire switch. Go to No. *3*. ● `faulty` displayed: The power supply unit to the connected device is disabled. Go to No. *4*. ● `inact` displayed: The supply of power has been stopped by an operation command. Go to No. *5*.
2	Check whether `shutdown` is set for the target port.	● When set: Set `no shutdown`. ● When not set: Make sure a power-receiving device is connected.
3	Use the `show power inline` operation command to check the values of `Threshold(W)` and `Total Allocate(W)`.	Power cannot be supplied because the value of `Total Allocate(W)` is larger than the value of `Threshold(W)`. Check the amount of power being supplied to the entire switch, the amount of power allocation to the ports, and the power consumption by the ports, and then adjust the allocation amount in the configuration.

No.	Items to check and commands	Action
4	Execute the `activate power inline` operation command, and then use the `show power inline` operation command to check the information displayed for `Status` for the target port.	● `off` displayed: Make sure a power-receiving device is connected. ● `on` displayed: Continue using the switch. ● `faulty` displayed: There might be a problem with the power-receiving device or a connection cable. Go to No. *6*.
5	Execute the `activate power inline` operation command, and then use the `show power inline` operation command to check the information displayed for `Status` for the target port.	● `off` displayed: Make sure a power-receiving device is connected. ● `on` displayed: Continue using the switch.
6	Use the `show logging` operation command to check whether a `POE` log is being recorded.	● When `0/x Supplying power was stopped by the overload detection.` is displayed: Power cannot be supplied because an overload was detected. Check the power-receiving device or connection cables. If the problem cannot be corrected, check the cable length and cable type in the *Hardware Instruction Manual*, and replace the cables. If devices to which PoE power can be supplied are connected, use the `power inline` configuration command to disable PoE on the port.
		● When `0/x Supplying power was stopped by the thermal shutdown.` is displayed: The supply of power was stopped because a thermal anomaly was detected in the PoE controller. Check the power-receiving device or connection cables. ● When `0/x Supplying power was stopped by the PD disorder (`*xxxx*`) is displayed:` Check the information displayed for *xxxx*. ● `MPS Absent`: An error might have occurred on the power-receiving device or a connection cable. ● `Startup Failure`: An error might have occurred on the power-receiving device. ● `Short:` The current flowing between the Switch and the power-receiving device might have exceeded the defined value. ● Classification Failure: [AX2200S] The class identification between the Switch and the power-receiving device has failed. Check the power-receiving device or connection cables.

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 3-15 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 mode matches: ● 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`. ● Make sure the key is correctly set on the Actor device.
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 in the table 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 shown with an * (asterisk) indicates that the entry has not been registered in the hardware due to device capacity.

```
# 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 Ring Protocol.

```
> show vlan 2048 detail Date 2008/10/29 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 16.03.09 11:24:47 PM UTC
Aging time : 300
MAC address        VLAN    Type     Port-list
0000.0088.7701        2    Dynamic  0/49-50
000b.972f.e22b        2    Dot1x    0/35
0000.ef01.34f4     1000    Static   0/30
0000.ef01.3d17     1000    Static   0/30
000b.9727.ee41     1024    WebAuth  0/28
```

```
0010.c6ce.e1c6     1024    MacAuth  0/29
0012.e284.c703     1024    Dynamic  0/49-50
001b.7887.a492     1024    Dynamic  0/49-50
0100.5e00.00fc     1024    Snoop    0/49-50

>
```

- 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 *3.7.1* Communication failures occurring when IEEE 802.1X is used.

  When `WebAuth` is displayed for `Type`:

  See *3.7.2* Communication failures occurring when Web authentication is used.

  When `MacAuth` is displayed for `Type`:

  See *3.7.3* 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 filtering and QoS control

Certain packets might have been discarded by filtering or packets might have been discarded by the shaper of QoS control. Make sure that the setting conditions for filtering 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 *3.13.1 Checking the filtering 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 Spanning Tree 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 route bridge, for example, replace the word *route bridge* with *CIST route bridge* or *route bridge for each MST instance*.

Table 3-16 Failure analysis method for Spanning Tree

No.	Items to check and commands	Action
1	Execute the `show spanning-tree` operation command for Spanning Tree that caused the failure, and then check the status of the protocol for Spanning Tree.	If the displayed status is `Enable`, go to No. *2*.
		If the displayed status is `Disable`, Spanning Tree has stopped. Check the following configurations: ● `spanning-tree disable` ● `switchport backup`
2	Execute the `show spanning-tree` operation command for Spanning Tree that caused the failure, and then check the bridge identifier of the route bridge for Spanning Tree.	If the bridge identifier of the route bridge indicates the route bridge defined in the network configuration, go to No. *3*.
		If the bridge identifier of the route bridge does not indicate the route bridge defined in the network configuration, check the network configuration and other configurations.
3	Execute the `show spanning-tree` operation command for Spanning Tree that caused the failure, and then check the port status and port role for Spanning Tree.	If the port status and port role for Spanning Tree 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 Spanning Tree are different from the network configuration, check the status of neighboring devices and their configurations.
4	Execute the `show spanning-tree statistics` operation command for Spanning Tree 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 filtering or the shaper of QoS control. See *3.13.1 Checking the filtering 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 Spanning Tree that caused the failure, and then check the bridge identifier for the received BPDUs.	Make sure the route bridge identifier and sending bridge identifier for the received BPDUs are the same as those defined in the network configuration. If they are different from the network configuration, check the status of the neighboring devices.
6	Check whether the value for maximum number of the Spanning Tree protocols, one of which caused the failure, is within the device capacities.	Set a value within the device capacities. For details about device capacities, see the *Configuration Guides*.

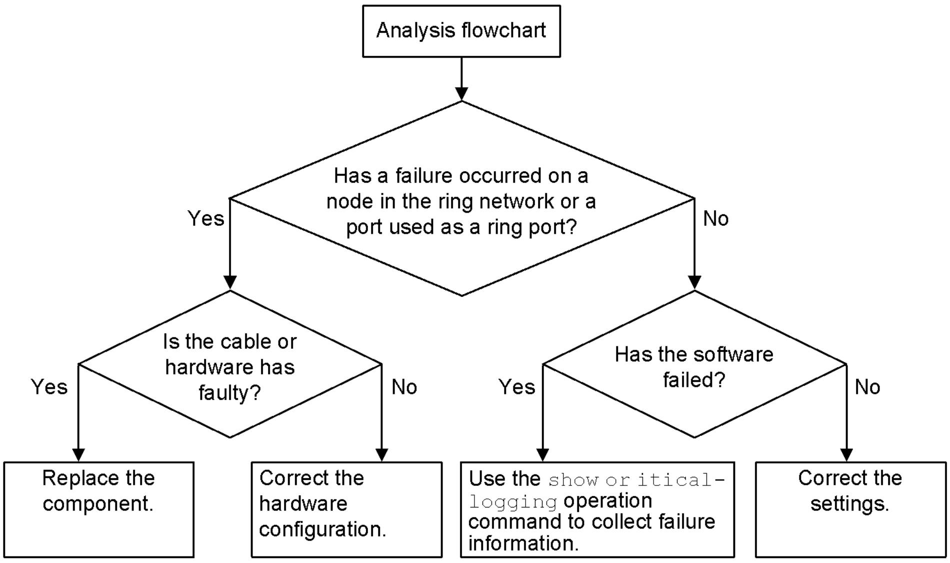
3.5.3 Failures occurring when the Ring Protocol functionality is used

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 3-1 Analysis flowchart


Analysis flowchart
Has a failure occurred on a node in the ring network or a port used as a ring port?
Yes
No
Is the cable or hardware has faulty?
Yes
No
Has the software failed?
Yes
No
Replace the component.
Correct the hardware configuration.
Use the show or itical-logging operation command to collect failure information.
Correct the settings.

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 the AX1250S and AX1240S series of switches. For other AX switch series, see the manuals for the appropriate models.

Table 3-17 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`, go to No. *3*.
		If any other information is displayed, check the configuration.

No.	Items to check and commands	Action
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.
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.
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*.
6	Use the `show vlan detail` operation command to check the VLAN used for the Ring Protocol and its port status.	Make sure there are no errors on the VLAN and its ports. If the multi-fault monitoring functionality is to be applied for the configuration, also check No. 7. If there is any anomaly, check the configuration and restore the states of the VLAN and its ports.
7	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 `transport-only` is set, go to No. *8*. If any other information is displayed, check the configuration.
8	Use the `show axrp detail` operation command to check the multi-fault monitoring VLAN ID.	If the Control VLAN ID is set as a multi-fault monitoring VLAN ID according to the network configuration, check the multi-fault-monitoring device on the shared node to confirm 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. 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 3-18 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*.

No.	Items to check and commands	Action
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 it 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 it 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 filtering and Layer 2 authentication functionality are configured correctly.	Authentication might have failed because certain packets have been discarded by filtering or Layer 2 authentication functionality is used for the port or VLAN to which the terminal is connected. Make sure the setting conditions for filtering 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 3-19 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# since the save event# has elapsed and the value displayed for `Last succeeded time` is either a hyphen (`-`) or a time earlier than the time that the save event occurred, 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	Check the status of the ST1 LED on the front of the switch, and then use the show logging operation command to check the operation log for saving of the binding database.	If the ST1 LED is blinking red and 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 the restart, check the status of the ST1 LED on the front of the switch, and then 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. Restarts 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. 1*.

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

Table 3-20 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# since the save event# has elapsed, and the value displayed for Last succeeded time is either a hyphen (-) or a time earlier than the time that the save event occurred, go to No. *3*.
2	Use the show running-config	If ip dhcp snooping database url mc is set, go to No. *3*.

No.	Items to check and commands	Action
	operation command to check the configuration.	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 file 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 clicks. (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*.
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.

No.	Items to check and commands	Action
		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. 1*.

(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 3-21 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, continue with No. *2*.
		If the time displayed for Last succeeded time is too old, continue with No. *3*.
2	Use the `show running-config` operation command to check the configuration.	If `ip dhcp snooping database url flash` is set, continue with 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 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 3-22 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`	If a hyphen (-) is displayed for Agent URL, continue with No. *2*.

No.	Items to check and commands	Action
	binding operation command to check the time that the database was saved.	If the time displayed for Last succeeded time is too old, continue with No. *3*.
2	Use the show running-config operation command to check the configuration.	If ip dhcp snooping database url mc is set, continue with 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 clicks. (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 the displayed <reason> is not any of the above, the restoration from the memory card has failed. Go to No. *4*.
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 might itself 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 3-2 Analysis flowchart

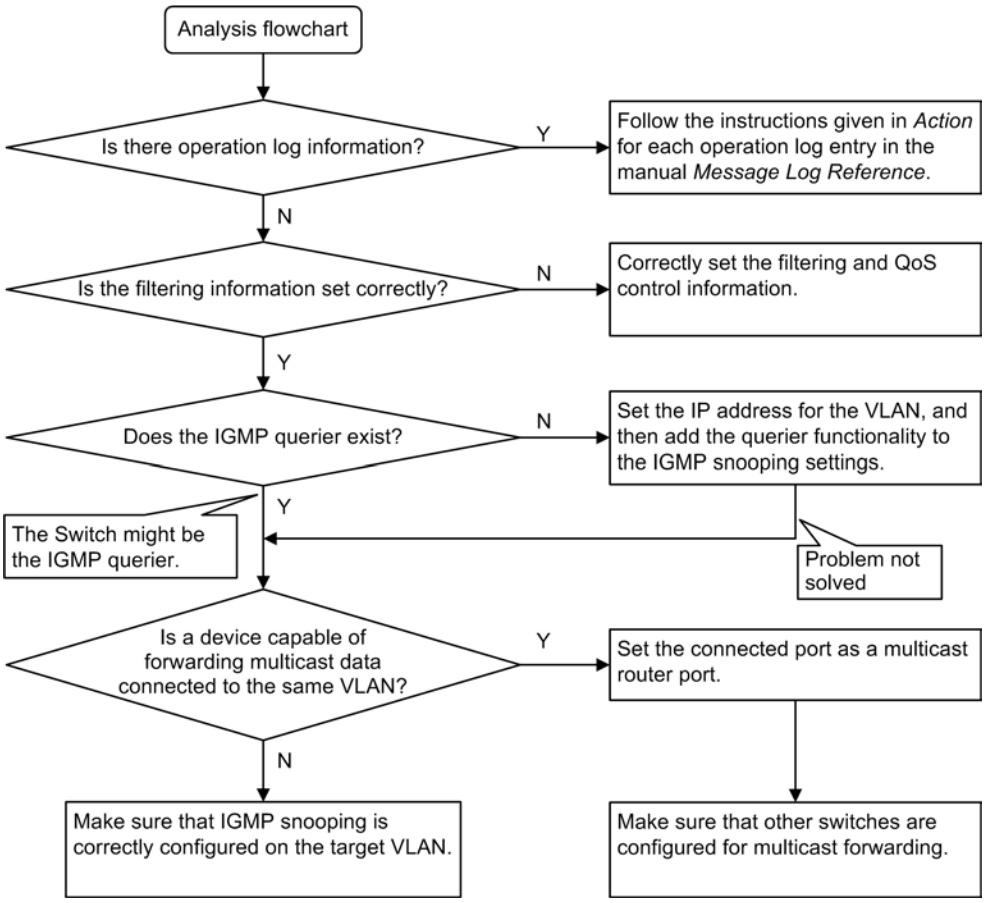

Analysis flowchart
Is there operation log information?
Y
Follow the instructions given in *Action* for each operation log entry in the manual *Message Log Reference*.
N
Is the filtering information set correctly?
N
Correctly set the filtering and QoS control information.
Y
Does the IGMP querier exist?
N
Set the IP address for the VLAN, and then add the querier functionality to the IGMP snooping settings.
Y
The Switch might be the IGMP querier.
Problem not solved
Is a device capable of forwarding multicast data connected to the same VLAN?
Y
Set the connected port as a multicast router port.
N
Make sure that IGMP snooping is correctly configured on the target VLAN.
Make sure that other switches are configured for multicast forwarding.

Table 3-23 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 filtering and QoS control are configured correctly.	Certain packets might have been discarded by filtering, or packets might have been discarded by the shaper of QoS control. Make sure that the setting conditions for filtering 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 *3.13.1 Checking the filtering and QoS control configuration information*.

No.	Items to check and commands	Action

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 14.11.08 03:59:14 PM 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 14.11.08 04:02:03 PM 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 3-3 Analysis flowchart

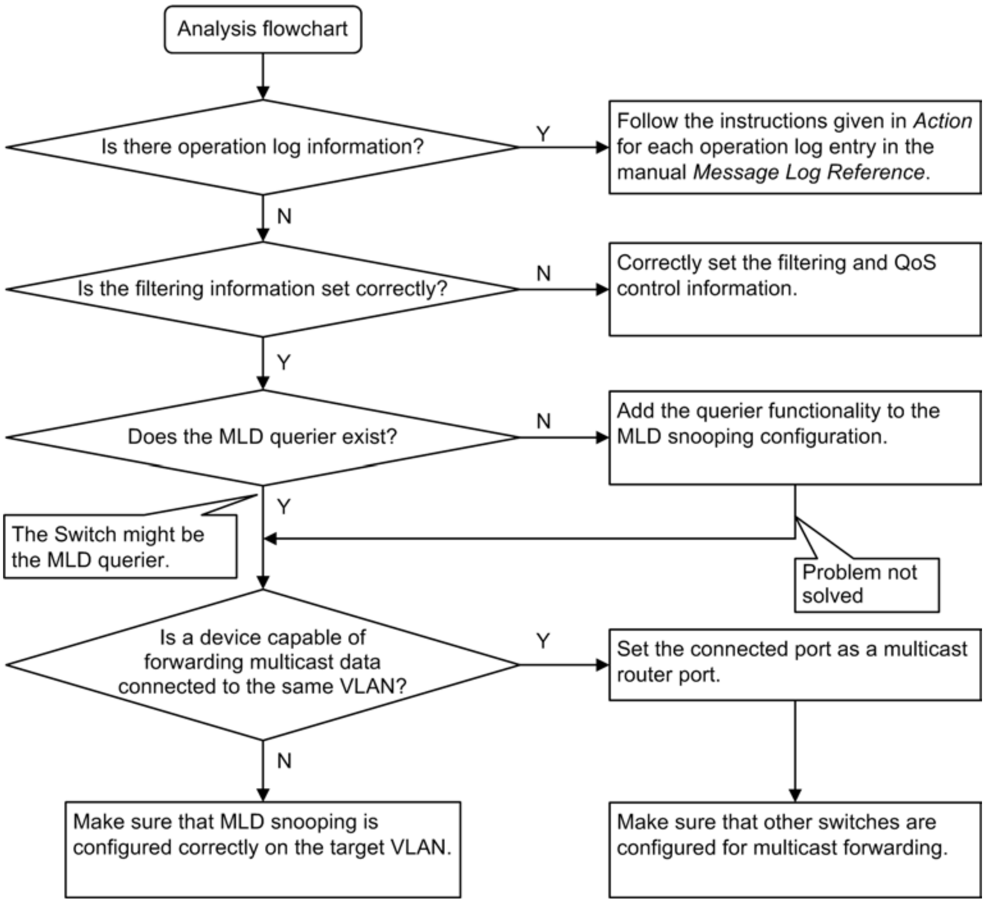

Analysis flowchart
Is there operation log information?
Y
Follow the instructions given in *Action* for each operation log entry in the manual *Message Log Reference*.
N
Is the filtering information set correctly?
N
Correctly set the filtering and QoS control information.
Y
Does the MLD querier exist?
N
Add the querier functionality to the MLD snooping configuration.
The Switch might be the MLD querier.
Y
Problem not solved
Is a device capable of forwarding multicast data connected to the same VLAN?
Y
Set the connected port as a multicast router port.
N
Make sure that MLD snooping is configured correctly on the target VLAN.
Make sure that other switches are configured for multicast forwarding.

Table 3-24 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 filtering and QoS control are configured correctly.	Certain packets might have been discarded by filtering, or packets might have been discarded by the shaper of QoS control. Make sure that the setting conditions for filtering 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 *3.13.1 Checking the filtering and QoS control configuration information*.

No.	Items to check and commands	Action

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: fe80::200:87ff:fe10:1959`[#]
		(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 3001`
		
		`Date 14.11.08 05:21:51 PM UTC`
		`VLAN counts: 3`
		`VLAN 3001:`
		`  IP Address:   Querier: enable`
		`  MLD querying system:`
		`  Querier version: v1`
		`  Port (1): 0/12`
		`  Mrouter-port: 0/12`
		`  Group counts: 1`

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 3001`
		
		`Date 14.11.08 05:22:10 PM UTC`
		`Total Groups: 3`
		`VLAN counts: 3`
		`VLAN 3001 Group counts: 1`
		`  Group Address              MAC Address      Version   Mode`
		`   ff80:0:0:0:0:0:99:a0a        3333.0099.0a0a   v1         -`
		`     Port-list: 0/12`

#: 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:

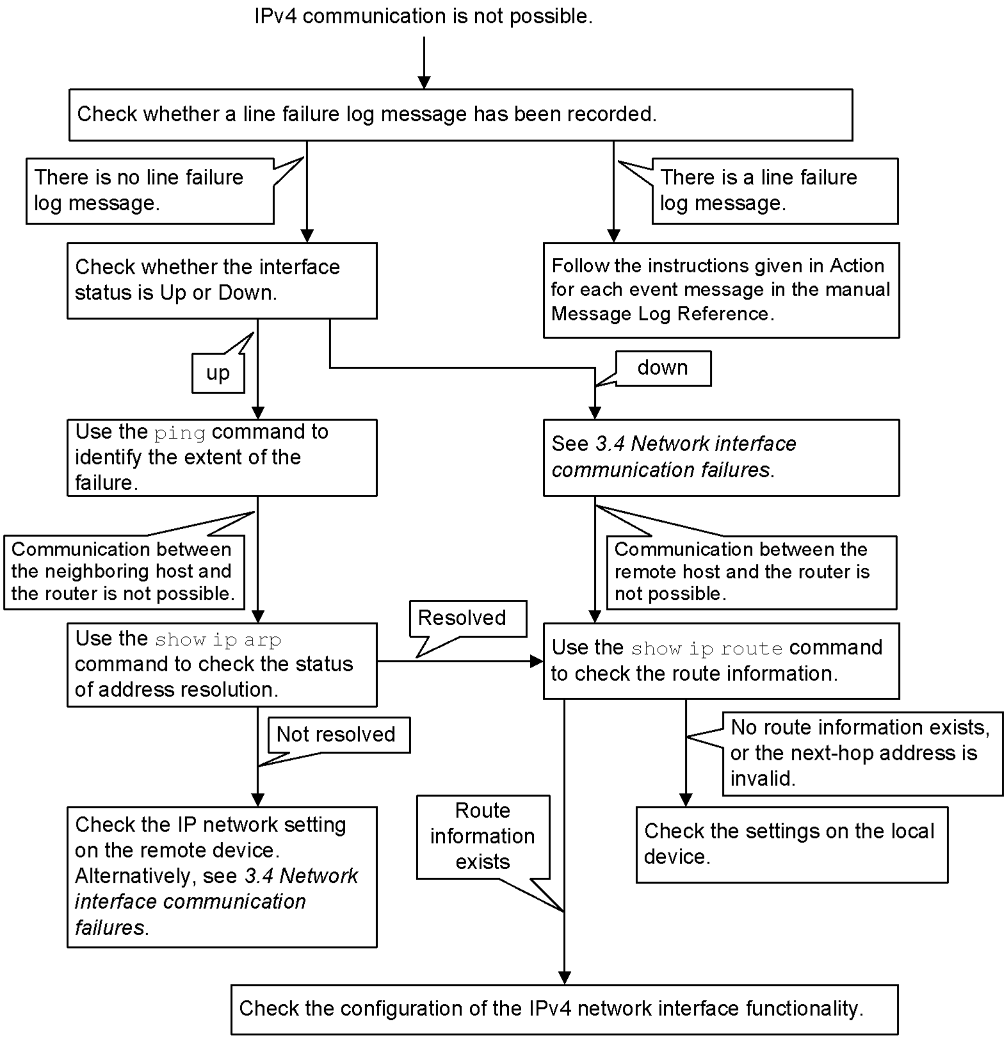
1. A configuration related to IP communication is changed.
2. The network configuration is changed.
3. A network device fails.

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 3-4 Analysis flowchart


IPv4 communication is not possible.
Check whether a line failure log message has been recorded.
There is no line failure log message.
There is a line failure log message.
Check whether the interface status is Up or Down.
Follow the instructions given in Action for each event message in the manual Message Log Reference.
up
down
Use the ping command to identify the extent of the failure.
See 3.4 Network interface communication failures.
Communication between the neighboring host and the router is not possible.
Communication between the remote host and the router is not possible.
Resolved
Use the show ip arp command to check the status of address resolution.
Use the show ip route command to check the route information.
Not resolved
No route information exists, or the next-hop address is invalid.
Check the IP network setting on the remote device. Alternatively, see 3.4 Network interface communication failures.
Route information exists
Check the settings on the local device.
Check the configuration of the IPv4 network interface functionality.

(1) Checking the device failure log

One probable cause of disabled communication is a line failure (or damage). The following describes the procedure for displaying the messages that indicate a hardware failure. You can find these messages in the device failure log displayed by the Switch.

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

1. Log in to the Switch.
2. Use the `show critical-logging` operation command to display the device failure log.
3. Each entry in the device failure log indicates the date and time that a failure occurred. Check whether a device failure log entry was displayed for the date and time that communication was disabled.
4. For details about the failure and corrective action for the device failure log entry described above, see the *Message Log Reference*, and then follow the instructions given in the manual.
5. If a Switch failure 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 the 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.

(6) Checking the unicast routing information

You need to check the route 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 route information obtained by the Switch.
3. If the route information obtained by the Switch contains route 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.

   - Filter functionality

     See *(7) Checking the filtering and QoS configuration information*.

(7) Checking the filtering and QoS configuration information

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

Make sure that the setting conditions for filtering 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 *3.13.1 Checking the filtering and QoS control configuration information*.

3.7 Layer 2 authentication communication failures

3.7.1 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 3-25 Failure analysis method for IEEE802.1X

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 exists, 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 VLAN-based authentication (dynamic): ● Make sure the MAC address on the authentication terminal has not been registered with the `mac-address` configuration command. ● Make sure `aaa authentication network default group radius` has been set in a configuration command. ● 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 following reasons. Check for problems. (1) The user ID or password has not been registered on the authentication server. The user ID or password is entered incorrectly. ● If `The number of supplicants on the switch is full` is displayed: Authentication failed because the maximum number of supplicants for the device was exceeded. ● If `The number of supplicants on the interface is full` is displayed: Authentication failed because the maximum number of supplicants for the interface was exceeded. ● If `Failed to authenticate the supplicant because it could not be registered to mac-address-table.` is displayed: Authentication was successful, but an attempt to set the MAC address table for the hardware failed. See the appropriate location in the *Message Log Reference*, and take the action described in *Action*. ● If the authentication mode is set to VLAN-based authentication (dynamic) and `Failed to assign VLAN.` is displayed: Authentication by the RADIUS server was successful, but VLAN allocation failed. ● If `Failed to authenticate the supplicant because it could not be registered to MAC VLAN.` is displayed: Authentication was successful, but an attempt to set the MAC VLAN table for the hardware failed. See the appropriate location in the *Message 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) or VLAN-based authentication (dynamic), go to No. *7*. For all other cases, see the RADIUS server log to check whether authentication failed.

No.	Items to check and commands	Action
7	Execute the `show dot1x logging` operation command, and check whether dynamic allocation in VLAN-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)` [port-based authentication (dynamic)][VLAN-based authentication (dynamic)] 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. ● `(Reason: Tunnel-Type Attribute is not VLAN(13)` [port-based authentication (dynamic)][VLAN-based authentication (dynamic)] 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)` [port-based authentication (dynamic)][VLAN-based authentication (dynamic)] 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))` [port-based authentication (dynamic)][VLAN-based authentication (dynamic)] 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: No Tunnel-Private-Group-ID Attribute)` [port-based authentication (dynamic)][VLAN-based authentication (dynamic)] Dynamic allocation has failed because the `Tunnel-Private-Group-ID` attribute is not set for the RADIUS attribute of the RADIUS server. Set the `Tunnel-Private-Group-ID` attribute for the RADIUS attribute of the RADIUS server.

No.	Items to check and commands	Action
		● (Reason: Invalid Tunnel-Private-Group-ID Attribute) [port-based authentication (dynamic)][VLAN-based authentication (dynamic)] 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) For port-based authentication (dynamic): 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 for the RADIUS attribute of the RADIUS server matches the VLAN ID of the authenticating port specified by using the switchport mac vlan#1 configuration command. 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 VLAN ID is not set to radius-vlan) For VLAN-based authentication (dynamic): The VLAN ID specified for the Tunnel-Private-Group-ID attribute of the RADIUS attribute of the RADIUS server is not enabled for VLAN-based authentication (dynamic). Correct the configuration so that the VLAN ID specified for the Tunnel-Private-Group-ID attribute for the RADIUS attribute of the RADIUS server matches the VLAN ID specified by the dot1x vlan dynamic radius-vlan configuration command for VLAN-based authentication (dynamic). 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 apply, see the RADIUS server log to check whether authentication has failed.
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.	For port-based authentication (static): ● 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 of the authentication IPv4 access list name for the Switch.

#1

If the switchport mac vlan configuration command has not been set, check whether the VLAN ID for the RADIUS server has been set using the vlan configuration command with "mac-based" specified.

#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 the item in the table does not apply, see *3.5 Layer 2 network communication failures*.

Table 3-26 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.

3.7.2 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 3-27 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 mode, go to No. *5*. ● If the login page appears in RADIUS authentication mode, 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.	[Fixed VLAN mode] [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*.

No.	Items to check and commands	Action
4	Check the setting of the authentication IPv4 access list.	[Fixed VLAN mode] [Dynamic VLAN mode] ● 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 filtering conditions in the authentication IPv4 access list are also set in the standard access list. ● Make sure a filtering 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 filtering 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*.
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] ● Make sure the VLAN ID of the RADIUS server matches the VLAN ID of the authenticating port specified in the `switchport mac vlan`[#1] configuration command. ● 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.

No.	Items to check and commands	Action
		[Legacy mode] ● Make sure the VLAN ID of the RADIUS server matches the VLAN ID specified in the `web-authentication vlan` configuration command and in the `switchport mac vlan` command for the port connected to the terminal to be authenticated. ● 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*.
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 *Operation Command Reference*).
		[Fixed VLAN mode] [Dynamic VLAN mode] ● 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.
		Common to Web authentication ● 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

If the `switchport mac vlan` configuration command has not been set, check whether the VLAN ID for the RADIUS server has been set by using the `vlan` configuration command with `mac-based` specified.

#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 3-28 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 ● web-authentication static-vlan max-user ● authentication arp-relay ● authentication ip access-group ● web-authentication redirect enable ● web-authentication redirect-mode [Dynamic VLAN mode] ● web-authentication port ● web-authentication max-user ● authentication arp-relay ● authentication ip access-group ● web-authentication redirect enable ● web-authentication redirect-mode [Legacy mode] ● web-authentication max-user ● web-authentication vlan
2	Check the IP address settings for the VLAN interfaces.	[Fixed VLAN mode] Make sure the IP address for the VLAN interface is set correctly. [Dynamic VLAN mode] [Legacy mode] Make sure the IP addresses for the following VLAN interfaces are set correctly: ● Pre-authentication VLAN ● Post-authentication VLAN
3	Configuring the DHCP server	If a DHCP server is used, see *(1) Communication failures occurring when the DHCP server is used*3.7.2(1).

No.	Items to check and commands	Action
4	Check the filtering configuration.	Certain packets might have been discarded by filtering or packets might have been discarded by the shaper of QoS control. Make sure that the setting conditions for filtering 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 *3.13.1 Checking the filtering and QoS control configuration information*.
5	Setting the authentication IPv4 access list	[Fixed VLAN mode] [Dynamic VLAN mode] Make sure that the filtering 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	[Fixed VLAN mode] [Dynamic VLAN mode] Make sure that the `authentication arp-relay` configuration command is set correctly so that unauthenticated terminals can send ARP packets to devices outside the Switch.

(1) 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. You might have checked the client and server settings (such as network card settings and cable connections) and concluded that cause 3 applies. For example, the configuration and network configuration are correct, but IP communication is not possible due to disabled allocation of IP addresses to clients. In such a case, see *(b) Checking the operation log and interface* through to *(d) Checking the filtering and QoS configuration information* for details.

(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 filtering and QoS 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 filtering functionality or packets might have been discarded by the shaper of the QoS functionality. Therefore, on the Switch and relay device between the client and server, check in the system configuration whether the setting conditions for the filtering functionality and QoS control in the configuration are correct and whether the shaper is used appropriately. For details about the procedure, see *3.13.1 Checking the filtering 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*.

3.7.3 Communication failures occurring when MAC-based authentication is used

If communication is not possible when IMAC-based authentication 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 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 mode is not possible, go to No. *2*. ● If authentication in RADIUS authentication mode 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 check the information for the operation.

No.	Items to check and commands	Action
		[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] [Legacy 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. [Dynamic VLAN mode] ● Make sure the VLAN ID of the RADIUS server matches the VLAN ID of the authenticating port specified in the `switchport mac vlan`[#1] configuration command. ● 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.
		[Legacy mode] ● Make sure the VLAN ID of the RADIUS server matches the VLAN ID specified in the `mac-authentication vlan` configuration command and in the `switchport mac vlan` command for the port connected to the terminal to be authenticated. ● 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*.

No.	Items to check and commands	Action
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.	[Fixed VLAN mode] [Dynamic VLAN mode] ● 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 filtering 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 filtering 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 *Operation Command Reference*. [Fixed VLAN mode] [Dynamic VLAN mode] ● 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.
		Common to MAC-based authentication ● 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

If the switchport mac vlan configuration command has not been set, check whether the VLAN ID for the RADIUS server has been set using the vlan configuration command with mac-based specified.

#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 3-30 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 static-vlan max-user ● mac-authentication vlan-check ● authentication arp-relay ● authentication ip access-group [Dynamic VLAN mode] ● mac-authentication port ● mac-authentication max-user ● authentication arp-relay ● authentication ip access-group [Legacy mode] ● mac-authentication max-user ● mac-authentication vlan

No.	Items to check and commands	Action
2	VLAN interface setting	[Fixed VLAN mode] Make sure the IP address for the VLAN interface is set correctly. [Dynamic VLAN mode] [Legacy mode] Make sure the IP addresses for the following VLAN interfaces are set correctly: ● Pre-authentication VLAN ● Post-authentication VLAN
3	Check the filtering configuration.	Certain packets might have been discarded by filtering or packets might have been discarded by the shaper of QoS control. Make sure that the setting conditions for filtering 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 *3.13.1 Checking the filtering and QoS control configuration information*.
4	Setting the authentication IPv4 access list	[Fixed VLAN mode] [Dynamic VLAN mode] Make sure that the filtering 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	[Fixed VLAN mode] [Dynamic VLAN mode] Make sure that the `authentication arp-relay` configuration command is set correctly so that unauthenticated terminals can send ARP packets to devices outside the Switch.

3.7.4 Communication failures occurring when secure Wake-on-LAN is used [OP-WOL]

If a failure occurs when secure Wake-on-LAN.1X 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 3-31 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, continue with No. 2.
		If the user authentication page appears: ● If user authentication is not possible, continue with No. *3*. ● If user authentication is possible: If `Not available` appears on the page used for selecting the terminal and sending the `startup` command, continue with No. *5*. If startup of the terminal cannot be confirmed after the `startup` command is sent, continue with No. *6*.

No.	Items to check and commands	Action
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-authenticaion 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-authenticaion 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.
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, continue with No. *7*.
7	Use the `show wol-device name` operation command to check the information displayed for `Alive` for the terminal.	● If `no-check` 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*.

No.	Items to check and commands	Action
8	If the startup check is enabled, check the IP address information.	● For a DHCP client: Make sure that `dhcp` is registered and 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. ● If the IP address information is correct, continue with 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.

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

3.8.1 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 3-32 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: Continue with No. *2*. ● Pair information is displayed: - If the `Status` information for the port displayed using the `show switchport backup` operation command does not change immediately after the physical port enters the link-down status, continue with No. *3*. - If automatic preemption or timer preemption is not possible after the primary port enters the link-up status, continue with 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 `select switchport backup interface` 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 Spanning Tree is running on the upstream switch of the primary port.	When Spanning Tree 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 Spanning Tree 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: Continue with No. *7*. Reception is not possible: Continue with 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 it 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 1,024. ● 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 SNMP communication failures

3.9.1 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

#
```

3.9.2 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

#
```

3.10 Communication failures in the neighboring device management functionality

3.10.1 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 3-33 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, *3.4 Network interface communication failures*.

No.	Items to check and commands	Action
5	Execute the `show lldp` operation command, and check the number of neighboring device information items on the port to which the neighboring device is connected.	● If `0` is displayed for `Neighbor Counts`, check No. *1* through No. *5* on the neighboring device. If the number of neighboring device information items is also 0 on the neighboring device, the connection between the devices might be incorrect. Check the connection. ● Certain packets might have been discarded by filtering or packets might have been discarded by the shaper of QoS control. Make sure that the setting conditions for filtering 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 *3.13.1 Checking the filtering and QoS control configuration information*.

3.11 NTP communication failures

3.11.1 Time information cannot be acquired from the NTP server

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

Table 3-34 NTP failure analysis method

No.	Items to check and commands	Action
1	Use the `show clock` operation command to make sure that the time zone is set.	If the time zone is set in the information displayed by the command, go to No. *2*.
		If the time zone is not set in the information displayed by the command, set the time zone.
2	Use the `show ntp-client` operation command to check the information acquired 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.

3.12 Communication failures in the IEEE 802.3ah/UDLD functionality

3.12.1 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 3-35 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`, continue with 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 filtering and QoS control configurations.	● The control frames (`slow-protocol`) used for the IEEE 802.3ah/UDLD functionality might have been discarded by filtering or QoS control. For details about the procedure, see *3.13.1 Checking the filtering 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

3.13 Communication failures in filtering and QoS configurations

3.13.1 Checking the filtering 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 filtering or by the shaper of QoS control.

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

(1) Checking whether packets have been discarded by filtering

1. Log in to the Switch.
2. Execute the operation command `show access-filter`, and check the filtering conditions in the access list applied to the interface, the number of packets that match the filtering conditions, and the number of packets discarded by a filter entry for implicit discard.
3. Compare the filtering 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 filtering conditions, the packets might have been discarded implicitly.
4. Check whether the setting conditions in the filtering configuration are correct.

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

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.

3.14 Port mirroring failures

3.14.1 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 filtering functionality for the mirror port.

3.15 Power saving functionality failures

3.15.1 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 3-36 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: [AX1250S] [AX1240S] 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 with 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 with 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 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 (RS-232C), the LEDs do not light with 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.

3.15.2 Power saving functionality scheduling is disabled

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

Table 3-37 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. [AX1250S] [AX1240S]	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. [AX1250S] [AX1240S]	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. [AX1250S] [AX1240S]	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 suppression mode is set after the sleep mode is canceled. To resume schedule-enabled mode after canceling sleep mode, execute the set power-control schedule enable operation command.

3.16 Failures occurring when long-life solution is supported

3.16.1 Correct date not displayed in temperature history

If the execution result of the `show environment temperature-logging` operation command does not contain the collection date or time, one of the following events may have occurred.

1. An attempt to restart the Switch was made, for example, by turning it off and on while saving temperature history information to internal flash memory, and the information could not be saved.
2. The time setting in the Switch was changed and the collection time is now earlier than the previous history information time.

You can continue to use the Switch, since the collection of temperature history information is continued.

4. Obtaining Failure Information

This chapter mainly describes how to obtain failure information.

4.1 Obtaining failure information

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

It might take tens of minutes for the `show tech-support` command to display information. As described below, we recommend that you either save the information on 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 it via FTP.

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

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

The file with 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 before executing the `show tech-support ramdisk` 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 by using 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 13.11.08 10:19:31 AM UTC
    File Date                    Size Name
    2008/11/13 10:15:00 AM       1,265 showtech.txt

>
```

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

```
>show mc

Date 13.11.08 10:19:51 AM UTC
    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.

```
> show mc-file

Date 13.11.08 10:20:53 AM UTC
    File Date               Size Name
    2008/11/13 10:20       1,265 showtech.txt


>
```

4.3 Transferring files via FTP

Failure information copied from 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, click the **Start** menu, choose **All Programs** and then **Accessories**, and then click **Command Prompt**.)

The following figure shows an example for transferring a file to the `C:¥TEMP` directory on a PC   when the IP address of the Switch is 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 AX1200 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.

Appendix

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

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

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

For details on the displayed information, see the manual *Operation Command Reference*. For details about each command in this table in which the Description column contains "OAN", see the appropriate OAN manual.

[Note]

The manual *Operation Command Reference* does not cover part of the information displayed by the `show tech-support` command. This type of information is not made public because it contains internal information of the Switch (available with a command in this table in which the Description column contains "Internal Switch information").

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

Table A-1 Detailed display contents

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

No.	Command (displayed)	Description	No parameter specified
15	`show mc-file`	Memory card files information	Y
16	`show ramdisk-file`	RAMDISK files information	Y
17	`show mc`	Amount of MC used	Y
18	`show ramdisk`	Amount of RAMDISK used	Y
19	`show critical-logging summary`	Device failure logs	Y
20	`show critical-logging`	Detailed switch failure log information	Y
21	`show logging`	Operation log information	Y
22	`show cpu (days/hours)`	CPU usage (per day, per hour)	Y
23	`show cpu (minutes/seconds)`	CPU usage (per minute, per second)	Y
24	`show memory summary`	Memory usage of the device	Y
25	`show interfaces`	Detailed statistics for ports	Y
26	`show port`	Port information	Y
27	`show port statistics`	Port statistics	Y
28	`show port protocol`	Protocol information for ports	Y
29	`show port transceiver`	Port transceiver information	Y
30	`show power inline`	PoE information	Y
31	`show channel-group summary`	Link aggregation information	Y
32	`show channel-group detail`	Detailed link aggregation information	Y
33	`show channel-group statistics`	Link aggregation statistics	Y
34	`show channel-group statistics lacp`	LACP statistics for link aggregation	Y
35	`show mac-address-table`	MAC address table information	Y
36	`show mac-address-table learning-counter`	Number of learnt addresses in the MAC address table	Y
37	`show vlan summary`	VLAN information	Y
38	`show vlan detail`	Detailed VLAN information	Y
39	`show vlan mac-vlan`	MAC VLAN information	Y
40	`show spanning-tree detail`	Spanning Tree details	Y

No.	Command (displayed)	Description	No parameter specified
41	`show spanning-tree port-count`	Number of accommodated spanning trees	Y
42	`show spanning-tree statistics`	Spanning Tree statistics	Y
43	`show axrp detail`	Ring Protocol details	Y
44	`show ip dhcp snooping`	DHCP snooping information	Y
45	`show ip dhcp snooping binding`	Binding database information for DHCP snooping	Y
46	`show ip dhcp snooping statistics`	DHCP snooping statistics	Y
47	`show ip arp inspection statistics`	Dynamic ARP inspection statistics	Y
48	`show igmp-snooping`	IGMP snooping information	Y
49	`show igmp-snooping group`	IGMP snooping group information	Y
50	`show igmp-snooping statistics`	IGMP snooping statistics	Y
51	`show mld-snooping`	MLD snooping information	Y
52	`show mld-snooping group`	MLD snooping group information	Y
53	`show mld-snooping statistics`	MLD snooping statistics	Y
54	`show ip interface`	IP interface information	Y
55	`show ip arp`	ARP information	Y
56	`show ip route`	Static route information	Y
57	`show access-filter`	Statistics on filtering	Y
58	`show qos-flow`	QoS control function statistics	Y
59	`show qos queueing`	Output queue statistics for each port	Y
60	`show authentication fail-list`	Information for terminals where Layer 2 authentication has failed	Y
61	`show authentication logging`	Full operation log information for Layer 2 authentication	Y
62	`show dot1x detail`	IEEE 802.1X authentication status information	Y
63	`show dot1x statistics`	IEEE 802.1X statistics	Y
64	`show dot1x logging`	IEEE 802.1X operation log information	Y
65	`show web-authentication`	Web authentication configuration information	Y

No.	Command (displayed)	Description	No parameter specified
66	`show web-authentication html-files detail`	Registered authentication screen file information for Web authentication	Y
67	`show web-authentication user edit`	Internal Web authentication DB contents and changes	Y
68	`show web-authentication user commit`	Internal Web authentication DB contents	Y
69	`show web-authentication login select-option detail`	Detailed authenticated user information for Web authentication	Y
70	`show web-authentication login summary port`	Authenticated user information for Web authentication (port level)	Y
71	`show web-authentication login summary vlan`	Authenticated user information for Web authentication (VLAN level)	Y
72	`show web-authentication logging`	Operation log information for Web authentication	Y
73	`show web-authentication statistics`	Web authentication statistics	Y
74	`show ip dhcp binding`	Binding information for DHCP server information	Y
75	`show ip dhcp conflict`	DHCP-detected conflict IP address information	Y
76	`show ip dhcp server statistics`	Statistics about the DHCP server	Y
77	`show mac-authentication`	MAC authentication configuration information	Y
78	`show mac-authentication login select-option detail`	Detailed authenticated terminal information for MAC authentication	Y
79	`show mac-authentication login summary port`	Authenticated terminal information for MAC authentication (port level)	Y
80	`show mac-authentication login summary vlan`	Authenticated terminal information for MAC authentication (VLAN level)	Y
81	`show mac-authentication logging`	Operation log information for MAC authentication	Y
82	`show mac-authentication statistics`	MAC authentication statistics	Y
83	`show mac-authentication mac-address edit`	Internal MAC authentication DB contents and changes	Y
84	`show mac-authentication mac-address commit`	Internal MAC authentication DB contents	Y
85	`show authentication multi-step`	Authentication terminal information for multistep authentication	Y
86	`show wol`	Secure Wake-on-LAN user information	Y

No.	Command (displayed)	Description	No parameter specified
87	show wol-authentication user edit	Internal DB contents and changes for secure Wake-on-LAN user authentication	Y
88	show wol-authentication user commit	Internal DB contents for secure Wake-on-LAN user authentication	Y
89	show wol-device name edit	Internal DB contents and changes for registering secure Wake-on-LAN terminals where activation commands are sent	Y
90	show wol-device name commit	Internal DB contents for registering secure Wake-on-LAN terminals where activation commands are sent	Y
91	show license	License information	Y
92	show gsrp aware	GSRP aware information	Y
93	show switchport backup	Uplink redundancy information	Y
94	show switchport backup statistics	Statistics of the functionality for sending and receiving flush control frames for uplink redundancy	Y
95	show switchport backup mac-address-table update	MAC address update functionality setting information for uplink redundancy	Y
96	show switchport backup mac-address-table update statistics	MAC address update functionality statistics for uplink redundancy	Y
97	show efmoam	IEEE 802.3ah/OAM functionality information	Y
98	show efmoam statistics	IEEE 802.3ah/OAM functionality statistics	Y
99	show storm-control detail	Storm control information	Y
100	show loop-detection	L2 loop detection information	Y
101	show loop-detection logging	L2 loop detection log information	Y
102	show loop-detection statistics	L2 loop detection statistics	Y
103	show cfm	CFM information	Y
104	show cfm summary	Detailed CFM information (the numbers accommodated MP and CFM ports)	Y
105	show cfm remote-mep	CFM remote MEP information	Y
106	show cfm remote-mep detail	Detailed CFM remote MEP information	Y
107	show cfm fault	CFM CC-detected failure information	Y

No.	Command (displayed)	Description	No parameter specified
108	`show cfm fault detail`	Detailed CFM CC-detected failure information	Y
109	`show cfm l2traceroute-db`	CFM Linktrace database information	Y
110	`show cfm l2traceroute-db detail`	Detailed CFM Linktrace database information	Y
111	`show cfm statistics`	CFM statistics	Y
112	`show lldp detail`	Neighboring device information for the LLDP functionality	Y
113	`show lldp statistics`	LLDP functionality statistics	Y
114	`show auto-config`	OAN: AUTOCONF functionality status information	Y
115	`show auto-config neighbor`	OAN: AUTOCONF functionality neighboring information	Y
116	`show config-lock-status`	OAN: Lock functionality status	Y
117	`show netconf`	OAN: NETCONF functionality status information	Y
118	`show netconf denied-host`	OAN: Access denied status information	Y
119	`show software-update user`	OAN: User list information for software update	Y
120	`show on-api webauth-html-file user`	OAN: User list information for Web authentication login page HTML file replacement	Y
121	`show on-api energy-saving user`	OAN: User list information for power saving configuration	Y
122	`Detail Information`	Internal Switch information	Y

Legend Y: Displayed

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

Index