
AX8600R Software Manual

Configuration Guide Vol. 1
For Version 12.1

AX86R-S001X

Alaxala

■ Relevant products

This manual applies to the models in the AX8600R series of devices. It also describes the functionality of version 12.1 of the software for the AX8600R series of devices.

■ 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

Cisco is a registered trademark of Cisco Systems, Inc. in the United States and other countries.

Ethernet is a registered trademark of Xerox Corporation.

IPX is a trademark of Novell, Inc.

sFlow is a registered trademark of InMon Corporation in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company and product names in this document are trademarks or registered trademarks of their respective owners.

■ Reading and storing this manual

Before you use the equipment, carefully read the manual and make sure that you understand all safety precautions.

After reading the manual, keep it in a convenient place for easy reference.

■ Notes

Information in this document is subject to change without notice.

■ Editions history

August 2013 (Edition 1) AX86R-S001X

■ Copyright

All Rights Reserved, Copyright(C), 2012, 2013, ALAXALA Networks, Corp.

Preface

Applicable products and software versions

This manual applies to the models in the AX8600R series of devices. It also describes the functionality of version 12.1 of the software for the AX8600R series of devices.

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

Corrections to 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 Device.

Readers must have an understanding of the following:

- The basics of network system management

Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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

- **Unpacking the Device and the basic settings for initial installation**

Quick Start Guide
 (AX86R-Q001X)

- **Determining the hardware setup requirements and how to handle the hardware**

Hardware Instruction Manual
 (AX86R-H001X)

- **Understanding the software functions, configuration settings, and operation commands**

▽ First, see the following guides to check the functions or capacity limits.

- | | | |
|---|---|--|
| <ul style="list-style-type: none"> - Capacity limits - Basic operations (e.g. logging in) - Ethernet | <ul style="list-style-type: none"> - Filters and QoS - Network management | <ul style="list-style-type: none"> - IP packet forwarding - Unicast routing - Multicast routing |
|---|---|--|

Configuration Guide Vol. 1
 (AX86R-S001X)

Configuration Guide Vol. 2
 (AX86R-S002X)

Configuration Guide Vol. 3
 (AX86R-S003X)

▽ If necessary, see the following references.

- **Learning the syntax of commands and the details of command parameters**

Configuration Command Reference Vol. 1
 (AX86R-S004X)

Configuration Command Reference Vol. 2
 (AX86R-S005X)

Configuration Command Reference Vol. 3
 (AX86R-S006X)

Operation Command Reference Vol. 1
 (AX86R-S007X)

Operation Command Reference Vol. 2
 (AX86R-S008X)

Operation Command Reference Vol. 3
 (AX86R-S009X)

- **Understanding system messages and logs**

Message and Log Reference
 (AX86R-S010X)

- **Understanding MIBs**

MIB Reference
 (AX86R-S011X)

- **How to troubleshoot when a problem occurs**

Troubleshooting Guide
 (AX86R-T001X)

Conventions: The terms "Device" and "device"

The term Device (upper-case "D") is an abbreviation for the following:

AX8600R series device

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

Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit

BEQ	Best Effort Queueing
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)
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CC	Continuity Check
CCM	Continuity Check Message
CFM	Connectivity Fault Management
CFP	C Form-factor Pluggable
CIDR	Classless Inter-Domain Routing
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
E-mail	Electronic mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ETH-AIS	Ethernet Alarm Indicator Signal
ETH-LCK	Ethernet Locked Signal
FAN	Fan Unit
FCS	Frame Check Sequence
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
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ	Low Latency Queueing
LSA	Link State Advertisement
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEG	Maintenance Entity Group
MEP	Maintenance association End Point/Maintenance entity group End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MP	Maintenance Point

MRU	Maximum Receive Unit
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NBMA	Non-Broadcast Multiple-Access
NDP	Neighbor Discovery Protocol
NIF	Network Interface
NLA ID	Next-Level Aggregation Identifier
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PA	Protocol Accelerator
packet/s	packets per second (can also appear as pps)
PAD	PADding
PC	Personal Computer
PDU	Protocol Data Unit
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PQ	Priority Queueing
PRU	Packet Routing Unit
PS	Power Supply
PSINPUT	Power Supply Input
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RR	Round Robin
RQ	ReQuest
SA	Source Address
SD	Secure Digital
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Small Form factor Pluggable Plus
SFU	Switch Fabric Unit
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
uRPF	unicast Reverse Path Forwarding
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
RRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

WFQ	Weighted Fair Queueing
WWW	World-Wide Web

Conventions: KB, MB, GB, and TB

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

Contents

Preface	i
Applicable products and software versions	i
Corrections to the manual	i
Intended readers	i
Manual URL	i
Reading sequence of the manuals	i
Conventions: The terms "Device" and "device"	ii
Abbreviations used in the manual	ii
Conventions: KB, MB, GB, and TB	v

PART 1: Overview and Capacity Limits of the Device

1. Overview of the Device	1
1.1 Device overview	2
1.2 Device features	3
2. Device Configuration	7
2.1 Range of Device models	8
2.1.1 External view	8
2.2 Device components	10
2.2.1 Hardware	10
2.2.2 Software	12
3. Capacity Limit	13
3.1 Hardware installation capacities	14
3.1.1 Maximum number of ports that can be handled	14
3.1.2 Maximum installable number of components	14
3.2 Capacity limits	16
3.2.1 Number of table entries	16
3.2.2 Route allocation pattern	18
3.2.3 Link aggregation	19
3.2.4 Filters and QoS	19
3.2.5 Network management	21
3.2.6 IP interfaces and IP packet forwarding	23
3.2.7 Unicast routing	28
3.2.8 Multicast routing	33

PART 2: Operation Management

4. Starting the Device and Logging In	37
4.1 Operation terminal-based management	38
4.1.1 Connection topology of operation terminals	38
4.1.2 Operation terminals	39
4.1.3 Overview of operation management functionality	40
4.2 Starting the device	42
4.2.1 Workflow from starting to stopping a device	42
4.2.2 Start procedures	42
4.2.3 Stop procedure	43
4.3 Login and logout	44

5. Command Operations	45
5.1 Command input mode	46
5.1.1 List of operation commands	46
5.1.2 Command input modes	46
5.2 CLI operations	48
5.2.1 Command line completion	48
5.2.2 Help functionality	48
5.2.3 Entry-error location detection functionality	48
5.2.4 Abbreviated-command execution	49
5.2.5 History functionality	49
5.2.6 Pipe functionality	51
5.2.7 Redirection	51
5.2.8 Paging	51
5.2.9 Customizing CLI settings	51
5.3 Notes on CLI operation	53
5.3.1 If an operation terminal crashes after logging in	53
5.3.2 If you are logged out while operating CLI special keys	53
5.3.3 If you access the files in a standby system	53
6. Configuration	55
6.1 Overview of configuration	56
6.1.1 Configuration at startup	56
6.1.2 Configuration during operation	57
6.1.3 Workflow when editing a running configuration	57
6.1.4 Mode transition when configurations are edited	59
6.1.5 Configuration during initial deployment	60
6.1.6 Lists of configuration commands and operation commands	60
6.2 Configuration editing procedures	63
6.2.1 Starting configuration editing	63
6.2.2 Displaying and checking configuration entries	63
6.2.3 Configuring the commit mode for the configuration	65
6.2.4 Adding, changing, and deleting configuration entries	66
6.2.5 Applying the edited settings to the running configuration	67
6.2.6 Saving configuration entries to a file	68
6.2.7 Applying settings from a configuration file	70
6.2.8 Ending configuration editing	71
6.2.9 Notes on configuration editing	72
6.3 Template operations	73
6.3.1 Overview of Template	73
6.3.2 Creating a template	74
6.3.3 Editing a template	76
6.3.4 Applying a template	78
6.3.5 Using template parameters	79
6.3.6 Special usage of Template	82
6.4 Configuration operations	84
6.4.1 Backing up configurations	84
6.4.2 Copying backup configuration files to the Device	84
6.4.3 Transferring files using the ftp command	85
6.4.4 Transferring files using a memory card	86
7. Remote Login	89
7.1 Description	90
7.1.1 Connecting to the management port	90
7.1.2 Connecting to the communication port	90
7.1.3 Dial-up IP connection	90

7.2	Configuration	94
7.2.1	List of configuration commands	94
7.2.2	Configuring the management port	95
7.2.3	Assigning an IP address to the Device	96
7.2.4	Permitting login by using the Telnet protocol	96
7.2.5	Permitting login by using FTP	97
7.2.6	Permitting login from VRFs by using the Telnet protocol	97
7.2.7	Permitting login from VRFs by using FTP	98
7.3	Operation	99
7.3.1	List of operation commands	99
7.3.2	Checking communication between a remote operation terminal and the Device	100
8.	Login Security and RADIUS or TACACS+	101
8.1	Configuring login security	102
8.1.1	Lists of configuration commands and operation commands	102
8.1.2	Overview of login control	103
8.1.3	Creating and deleting a login user	103
8.1.4	Configuring and changing a login user's password	104
8.1.5	Configuring and changing a password for switching to administrator mode	105
8.1.6	Permitting login from a remote operation terminal	106
8.1.7	Configuring the maximum number of concurrent users	106
8.1.8	Configuring the IP addresses of remote operation terminals permitted to log in	107
8.1.9	Configuring login banners	108
8.1.10	Permitting login from a remote operation terminal when using VRF	109
8.1.11	Configuring the IP address that permits login from a remote operation terminal when using VRF	110
8.2	Description of RADIUS and TACACS+	113
8.2.1	Overview of RADIUS and TACACS+	113
8.2.2	Scope of RADIUS or TACACS+ implementation	113
8.2.3	Authentication using RADIUS or TACACS+	119
8.2.4	RADIUS or TACACS+ and local command authorization	123
8.2.5	RADIUS and TACACS+ accounting	133
8.2.6	Connecting with RADIUS or TACACS+	135
8.3	RADIUS and TACACS+ configurations	137
8.3.1	List of configuration commands	137
8.3.2	Configuring RADIUS authentication	137
8.3.3	Configuring TACACS+ authentication	138
8.3.4	Configuring RADIUS or TACACS+ and local command authorization	140
8.3.5	Configuring RADIUS or TACACS+ login-logout accounting	141
8.3.6	Configuring TACACS+ command accounting	142
9.	Time Settings, NTP, and SNTP	145
9.1	Description	146
9.1.1	Overview	146
9.1.2	Notes on time settings, NTP, and SNTP	146
9.2	Time settings	147
9.2.1	Lists of configuration commands and operation commands	147
9.2.2	System clock settings	147
9.2.3	Daylight savings time settings	147
9.3	NTP configuration	150
9.3.1	List of configuration commands	150
9.3.2	Synchronizing a device with the time server by NTP	150
9.3.3	Synchronizing a device with an NTP server	151
9.3.4	Configuring NTP authentication	151
9.3.5	Using NTP functionality to synchronize the Device on a VRF	151
9.4	SNTP configuration	153

9.4.1	List of configuration commands	153
9.4.2	Synchronizing a device with the time server by SNTP	153
9.4.3	Configuring SNTP authentication	154
9.4.4	Using SNTP functionality to synchronize the Device on a VRF	154
9.5	Operation	155
9.5.1	List of operation commands	155
9.5.2	Checking the time, NTP status, and SNTP status	155
10.	Host Names and DNS	157
10.1	Description	158
10.1.1	Overview	158
10.1.2	Notes on host names and DNS	158
10.2	Configuration	159
10.2.1	List of configuration commands	159
10.2.2	Configuring host names	159
10.2.3	Configuring DNS settings	159
11.	Device Management	161
11.1	System operation panel	162
11.1.1	Startup messages	162
11.1.2	Menu structure	164
11.1.3	Displaying port information	165
11.1.4	Displaying CPU usage rate	166
11.1.5	Displaying memory usage rate	167
11.1.6	Displaying the version	168
11.1.7	Displaying temperature information	172
11.1.8	Replacing boards	173
11.1.9	Stop procedure	176
11.1.10	Displaying a failure	176
11.2	Configuring the device resources	179
11.2.1	Lists of configuration commands and operation commands	179
11.2.2	Specifying the table entry allocation pattern	179
11.3	Checking the Device	180
11.3.1	Lists of configuration commands and operation commands	180
11.3.2	Checking the software version	181
11.3.3	Checking the device status	182
11.3.4	Checking the internal flash memory	185
11.3.5	Checking the memory card	186
11.3.6	Monitoring temperatures	186
11.3.7	Monitoring fan units	188
11.4	Managing SFU, PRU, and NIF	190
11.4.1	Lists of configuration commands and operation commands	190
11.4.2	Disabling a board	190
11.4.3	Configuring PRU startup priorities	191
11.4.4	Checking the SFU status	191
11.4.5	Checking the PRU status	191
11.4.6	Checking the NIF status	192
11.4.7	Configuration when a NIF is replaced	192
11.5	Backing up and restoring operating information	194
11.5.1	List of operation commands	194
11.5.2	Procedure for BCUs in a duplex configuration	194
11.5.3	Procedure for a BCU in a single configuration	194
11.6	Failure recovery	196
11.6.1	Type of problem and recovery processing	196

12. Software Management	199
12.1 Description of software updates	200
12.1.1 Overview	200
12.1.2 Targets of software updates	200
12.1.3 Update and application triggers	200
12.1.4 Non-stop software upgrade	201
12.1.5 Notes on updating software	202
12.2 Operations to update software	203
12.2.1 List of operation commands	203
12.2.2 Preparing an update file	203
12.2.3 Executing the update command	203
12.2.4 Updating SFU, PRU, and NIF	204
12.2.5 Checking after updates	204
12.2.6 Notes on performing updates	205
13. Device Redundancy	207
13.1 Description of the BCU duplex configuration	208
13.1.1 Overview	208
13.1.2 Operation	208
13.1.3 Synchronizing user setting information and usage information	209
13.1.4 System switchover	209
13.1.5 Notes on using the BCU duplex configuration	211
13.2 Operation for the BCU duplex configuration	212
13.2.1 List of operation commands	212
13.2.2 Checking the status of the standby BCU	212
13.2.3 Restarting a BCU	212
13.2.4 Replacing a BCU	212
13.2.5 Synchronizing the user setting information and usage information	212
13.2.6 Performing system switchover	213
13.3 Description of SFU redundancy	214
13.3.1 Device configuration when there is redundancy	214
13.3.2 How a redundant configuration operates	214
13.3.3 SFU operation when a failure occurs	214
13.4 Operation for SFU redundancy	216
13.4.1 List of operation commands	216
13.4.2 Checking the SFU status	216
13.5 Description of power supply unit (PS) redundancy	217
13.5.1 Overview	217
13.5.2 Redundant power supply units	217
13.5.3 Redundant power feeds	217
13.5.4 Supply power management	218
13.6 PS (power supply unit) redundancy configuration	221
13.6.1 List of configuration commands	221
13.6.2 Configuring the redundant power supply unit	221
13.6.3 Configuring the redundant power feed	221
13.7 Operation for PS (power supply unit) redundancy	222
13.7.1 List of operation commands	222
13.7.2 Checking the PS status	222
13.7.3 Checking the supply power	223
14. System Message Output and Log Management	225
14.1 Description	226
14.1.1 Outputting messages	226
14.1.2 Storing logs	226
14.2 Configuration	227

14.2.1	List of configuration commands	227
14.2.2	Configuring the minimum number of operation log entries to be stored	227
14.2.3	Configuring syslog output	228
14.2.4	Configuring email output	228
14.2.5	Controlling message output	228
14.3	Operation	231
14.3.1	List of operation commands	231
14.3.2	Viewing and deleting log entries	231
15.	SNMP	233
15.1	Description	234
15.1.1	Overview of SNMP	234
15.1.2	MIB overview	237
15.1.3	SNMPv1 and SNMPv2C operations	239
15.1.4	SNMPv3 operation	244
15.1.5	Traps	247
15.1.6	Informs	249
15.1.7	IP addresses used for SNMP	250
15.1.8	RMON MIB	250
15.1.9	Notes on connecting to an SNMP manager	251
15.2	Configuration	252
15.2.1	List of configuration commands	252
15.2.2	Configuring MIB access permissions in SNMPv1 and SNMPv2C	252
15.2.3	Configuring MIB accesses in SNMPv3	253
15.2.4	Configuring the sending of traps in SNMPv1 and SNMPv2C	253
15.2.5	Configuring the sending of traps in SNMPv3	254
15.2.6	Configuring the sending of informs in SNMPv2C	254
15.2.7	Suppressing link traps	255
15.2.8	Configuring control information for the RMON Ethernet history group	255
15.2.9	Threshold check for specific MIB values by RMON	256
15.2.10	Configuring permissions for accessing MIBs from VRF in SNMPv1 and SNMPv2C	257
15.2.11	Configuring permissions for accessing MIBs from VRF in SNMPv3	257
15.2.12	Configuring settings for sending traps to a VRF in SNMPv1 and SNMPv2C	258
15.2.13	Configuring settings for sending traps to a VRF in SNMPv3	258
15.2.14	Configuring settings for sending informs to a VRF in SNMPv2C	259
15.3	Operation	260
15.3.1	List of operation commands	260
15.3.2	Checking communication with SNMP managers	260

PART 3: Network Interfaces

16.	Ethernet	263
16.1	Description of information common to all Ethernet interfaces	264
16.1.1	Network configuration example	264
16.1.2	Physical interfaces	264
16.1.3	MAC sublayer control	265
16.1.4	VLAN Tag	266
16.1.5	MAC address of the Device	267
16.2	Configuration common to all Ethernet interfaces	268
16.2.1	List of configuration commands	268
16.2.2	Configuring multiple interfaces by a single command	268
16.2.3	Shutting down an Ethernet interface	268
16.2.4	Configuring jumbo frames	269
16.2.5	Configuring the link-down detection timer	270

16.2.6	Configuring the link-up detection timer	271
16.2.7	Configuring the notification of a frame sending or reception error	271
16.3	Operations common to all Ethernet interfaces	273
16.3.1	List of operation commands	273
16.3.2	Checking the Ethernet operating status	273
16.4	Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces	274
16.4.1	Functionality	274
16.4.2	SFP for 10BASE-T/100BASE-TX/1000BASE-T	281
16.5	Configuration of 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces	282
16.5.1	Configuring ports	282
16.5.2	Configuring flow control	283
16.5.3	Configuring AUTO-MDI/MDI-X	283
16.6	Description of the 1000BASE-X interface	284
16.6.1	Functionality	284
16.7	Configuration of the 1000BASE-X interface	287
16.7.1	Configuring ports	287
16.7.2	Configuring flow control	287
16.8	Description of the 10GBASE-R interface	289
16.8.1	Functionality	289
16.9	Configuration of the 10GBASE-R interface	291
16.9.1	Configuring flow control	291
16.10	Description of 100GBASE-R	292
16.10.1	Functionality	292
16.11	Configuration of the 100GBASE-R interface	293
16.11.1	Configuring flow control	293
17	Link Aggregation	295
17.1	Description of the link aggregation basic functionality	296
17.1.1	Overview	296
17.1.2	Link aggregation configuration	296
17.1.3	Supported specifications	297
17.1.4	MAC address of the channel group	298
17.1.5	Port allocation for sending frames	298
17.1.6	Notes on using link aggregation	299
17.2	Configuration of the link aggregation basic functionality	300
17.2.1	List of configuration commands	300
17.2.2	Configuring static link aggregation	300
17.2.3	Configuring LACP link aggregation	300
17.2.4	Configuring a port channel interface	301
17.2.5	Configuring the allocation method	302
17.2.6	Deleting a channel group	302
17.3	Description of the link aggregation extended functionality	304
17.3.1	Standby link functionality	304
17.3.2	Port detachment restriction functionality	305
17.3.3	Mixed-speed mode	305
17.3.4	Switch back suppression	306
17.4	Configuration of the link aggregation extended functionality	308
17.4.1	List of configuration commands	308
17.4.2	Configuring the standby link functionality	308
17.4.3	Configuring the port detachment restriction functionality	309
17.4.4	Configuring mixed-speed mode	309
17.4.5	Configuring the switch back suppression	310
17.5	Operation for link aggregation	311
17.5.1	List of operation commands	311
17.5.2	Checking the link aggregation status	311

18. IP Interfaces	313
18.1 Description	314
18.1.1 Overview	314
18.1.2 Subinterface	314
18.1.3 Example of a network configuration	314
18.1.4 Specifications for IP interface operation	316
18.1.5 TPID value of VLAN tag	319
18.2 Configuration	320
18.2.1 List of configuration commands	320
18.2.2 Configuring an IP interface	320
18.2.3 Deleting an IP interface	322
18.2.4 Shutting down a subinterface	323
18.2.5 Configuring the TPID value of a VLAN tag	323
18.3 Operation	325
18.3.1 List of operation commands	325
18.3.2 Checking the status and statistics of the IP interface	325
Appendix	327
A Relevant standards	328
A.1 TELNET/FTP	328
A.2 RADIUS or TACACS+	328
A.3 NTP	328
A.4 SNTP	328
A.5 DNS	328
A.6 SYSLOG	329
A.7 SNMP	329
A.8 Ethernet	331
A.9 Link aggregation	331
A.10 VLAN	331
B Acknowledgments	332
Index	335

Chapter

1. Overview of the Device

This chapter describes the features of the Device.

- 1.1 Device overview
- 1.2 Device features

1.1 Device overview

Telecom carriers' commercial networks, including NGNs (Next Generation Networks), are playing an increasingly important role as social infrastructure that provides telecommunication services essential to social activities. Such services include IP telephony, Internet connections, enterprise intraoffice communications, and mobile communications. In particular, in recent years, the amount of traffic in some telecommunication services has increased remarkably, requiring networks to have larger capacity and higher speed.

In addition, communication data flowing through these networks contains a mixture of various kinds of data with different social priorities such as mission-critical data that affects company profits and privately viewed streaming videos. For this reason, high-level network manageability is demanded: for example, to ensure security against information leakage and illegal access, and to appropriately control traffic so that it is kept within the network processing capacity.

This Device is a router product that provides flexible options for building a highly reliable, highly available, and highly scalable telecommunication network foundation essential to achieving a mission-critical IT infrastructure.

Product concepts

The Device is a chassis-type router provided with large capacity, high speed, and high density accommodation capacity. The Device also incorporates the carrier-grade technology developed by ALAXALA Networks Corporation to achieve its guaranteed network concept.

The Device delivers the following functionality:

- Implements 100 gigabit Ethernet and link aggregation that provide sufficient network capacity to meet increased traffic demands.
- Enables implementation of a variety of flexible networks, by providing features such as cutting-edge IPv6 and multicast capabilities, and routing protocols such as OSPF and BGP4 used by large-scale networks.
- Enables implementation of highly reliable and highly available networks by supporting hardware redundancy inside the Device and various types of network redundancy functionality.
- Adopts a distributed engine system that makes the system capacity of the Device scalable. Also adopts a micro line card structure that can accommodate a maximum of four types of network interface cards in the distributed engine to achieve expandability without waste of space.
- Provides a guaranteed network to protect the entire range of traffic handled within a telecommunication carrier network (such as company transaction data, IP telephony data, teleconferencing, and video streaming) according to priorities using QoS technology and other functionality.
- Safeguards networks by security functionality such as high-performance filtering.

1.2 Device features

(1) High-performance architecture

- 100 gigabit Ethernet support
 - 100 gigabit Ethernet non-blocking forwarding
- Employs a distributed engine system and switching fabric system ideal for increasingly-large capacity.

(2) Compact design and high density

- Front intake and rear exhaust air flow
 - Employs an airflow system with a front intake and rear exhaust in a compact chassis.
 - Contributes to greater space efficiency and cooling efficiency of the facility and server room.
- Efficient handling of low-speed and high-speed lines
 - Employs a micro line card structure that efficiently consolidates and handles different interfaces, including 1 gigabit Ethernet used in existing facilities and 10 gigabit Ethernet used for future expansion and increased capacity.
 - Because the Device can be expanded with network interface cards of 1/4 slot size (single half size), power usage of idle ports can be reduced and capital investment efficiency can be increased even for gradual increases in capacity.

(3) High reliability for configuring mission-critical networks

- High product quality
 - High reliability assured through exacting component selection and strict design and testing standards
 - Stable routing processing based on software used successfully by communication carriers and ISPs
- FT architecture for high reliability as a stand-alone device
 - Configuration of a fault-tolerant network (FTN) through the redundancy of internal device power, CPU parts, and packet forwarding parts
- Variety of redundant network configurations
 - Fast Reroute

Link aggregation (IEEE compliance), hot standby (VRRP), static polling[#], and other functionality
 - Load balancing

Equal traffic balancing at the IP level based on OSPF equal-cost multipath routing

[#]

Monitoring functionality that polls a node on a specified path to check its reachability, and dynamically selects a new route in conjunction with static routing
- Comes with functionality to prevent software high load.
 - Protects software from a DoS attack and other issues due to the rate limit or priority control of packets processed with software and achieves stable operations of routing processing.

(4) *Guaranteed communication quality by using powerful hardware-based QoS functionality*

- High-performance hardware-based QoS processing
- Precise QoS control by specification of detailed parameters (L2, L3, and L4 headers)
- Wide range of QoS control functionality
 - IP-QoS (for example: Diff-Serv, bandwidth control, priority control, drop control, etc.)

(5) *Proven routing functionality*

- Stable and sophisticated routing
 - Inheritance of proven routing software
 - A variety of routing protocols (compatible with static, RIP, RIPng, OSPF, OSPFv3, BGP4, BGP4+, PIM-SM/PIM-SSM, IGMP, MLD, and VRF) enable a diverse, flexible, and highly-reliable network.
- Scalable routing functionality
 - Full route support with IPv4/IPv6 dual stack
 - High-speed routing processing that supports large-scale networks
 - Multiple routing sessions are also supported by VRF, etc.

(6) *Robust security*

- Advanced and fine-grained packet filtering
 - Hardware-based high-performance filtering processes
 - L2, L3, and L4 headers can be specified as filtering conditions.
- uRPF support
 - Supports uRPF for detecting and dropping invalid senders by using a routing table.
- Device user account control
 - RADIUS or TACACS+-based device login password authentication
 - Executable commands can be limited for each user.

(7) *Advanced network management, maintenance, and operation*

- Offers IPv4/v6 Dual Stack and full network management functionality for IPv6 environments, including SNMP over IPv6.
- In addition to the basic MIB-II, supports a wide range of MIBs including IPv6 MIB and RMON.
- Supports port mirroring to monitor and analyze traffic (through both receiving and sending ports).
- Capable of analyzing traffic characteristics using sFlow and the sFlow-MIB.
- Online maintenance

Command-free expansion and exchange of boards, power supplies, and fans. Support for non-stop software upgrade.
- Supports SD memory cards.

Enables users to easily back up the configuration and save error information.
- The Ethernet ports, console port, and the memory card slot are all on the front panel.
- Employs a system operation panel.

Various types of information can be displayed and operation instructions can be performed without using a console terminal.

- Supports the Ethernet Connectivity Fault Management (CFM) functionality and Link Layer Discovery Protocol (LLDP) for network maintenance and management.
- Advanced configuration management
 - Supports full configuration management functionalities, including Template, Merge, Rollback, and commit mode.

(8) Power saving

- Low power consumption-oriented architecture design and part selection
 - This helps to reduce the total cost of ownership (TCO) after installation.
- Visualization of power consumption information
 - Power consumption is displayed with an operation command.

Chapter

2. Device Configuration

This chapter describes the appearance and components for the Device.

- 2.1 Range of Device models
- 2.2 Device components

2.1 Range of Device models

The AX8600R series has the following models:

- AX8616R
- AX8632R

The AX8600R series consists of the basic control unit (BCU), switch fabric unit (SFU), packet routing unit (PRU), network interface board (NIF), power supply unit (PS), power input unit (PSINPUT), chassis, fan unit (FAN), and other components.

AX8616R is a model with redundant BCUs, SFUs, and PSs, 4 PRU slots, and 16 NIF slots.

AX8632R is a model with redundant BCUs, SFUs, and PSs, 8 PRU slots, and 32 NIF slots.

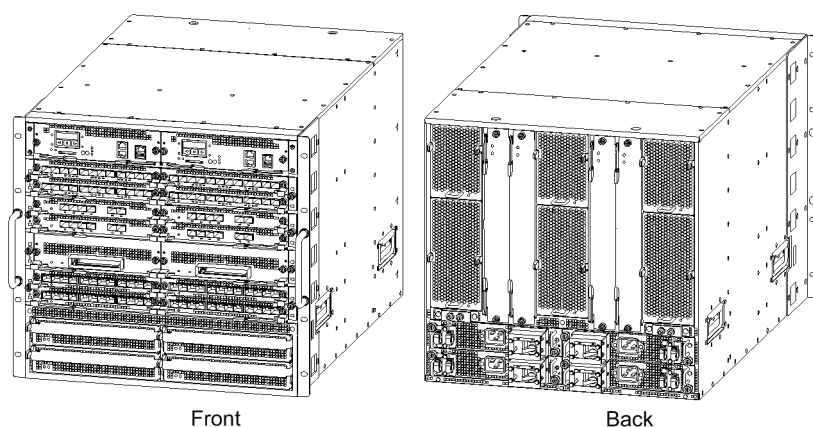
For both AX8616R and AX8632R, a BCU, SFU, PRU, NIF, PS, or FAN can be replaced while the power is on. In addition, if the BCU, SFU, or PS is in a redundant configuration, it can be replaced without stopping communications.

2.1.1 External view

External views of the models are shown below.

(1) AX8616R

Figure 2-1: AX8616R model



- Implemented position

BCU 1	BCU 2
NIF 1	NIF 2
NIF 3	NIF 4
NIF 5	NIF 6
NIF 7	NIF 8
NIF 9	NIF 10
NIF 11	NIF 12
NIF 13	NIF 14
NIF 15	NIF 16
PS 1	PS 2
PS 3	PS 4

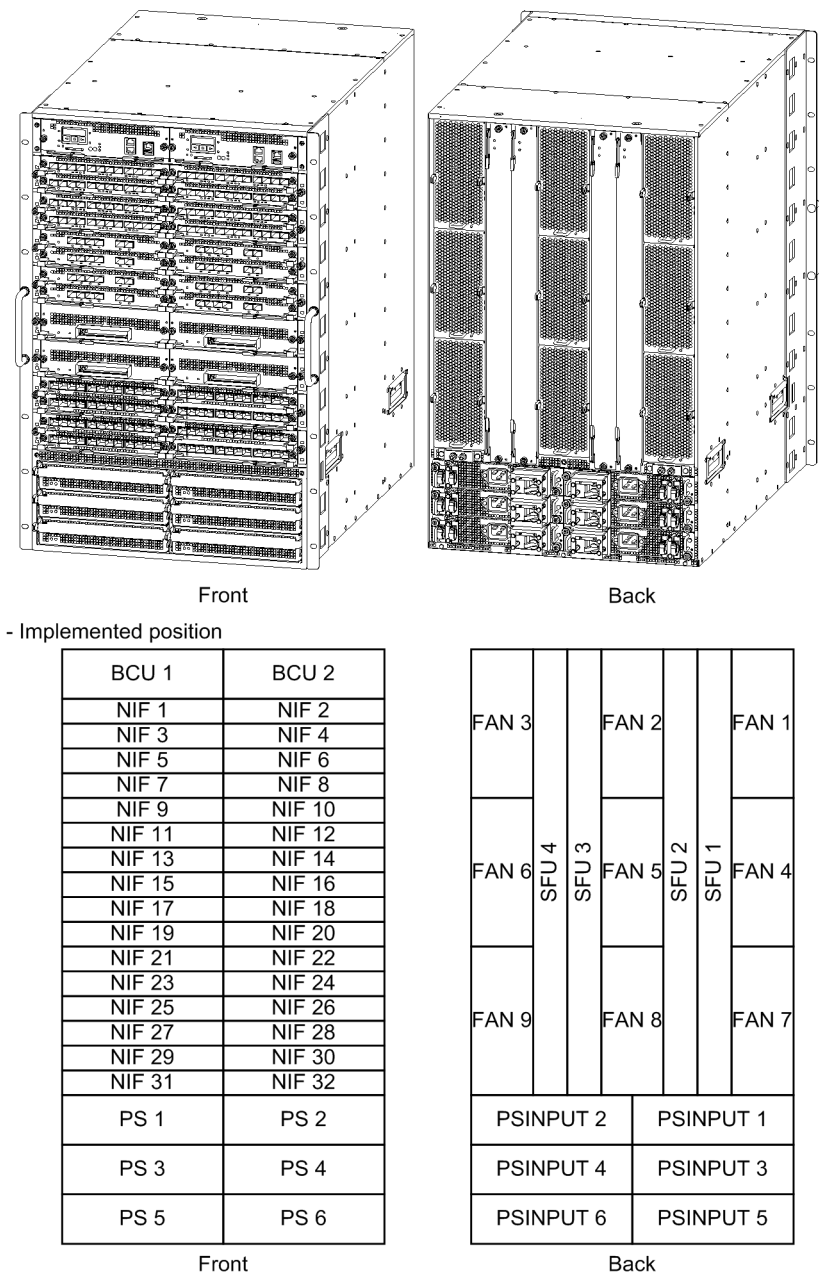
Front

FAN 3		FAN 2		FAN 1
	SFU 4	SFU 3	SFU 2	SFU 1
FAN 6		FAN 5		FAN 4
PSINPUT 2		PSINPUT 1		
PSINPUT 4		PSINPUT 3		

Back

(2) AX8632R

Figure 2-2: AX8632R model

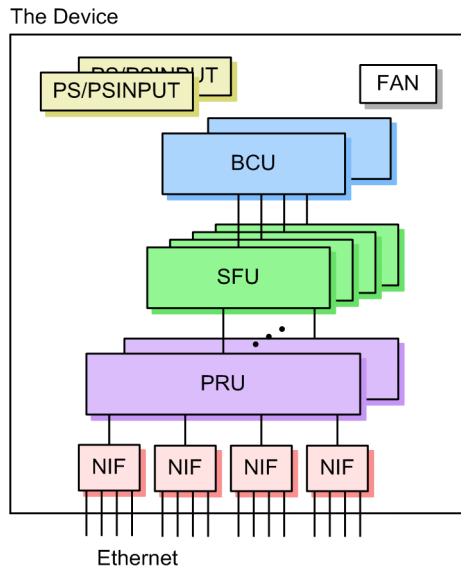


2.2 Device components

2.2.1 Hardware

The Device consists of a PS, PSINPUT, FAN, BCU, SFU, PRU, and NIF. The following figure shows the hardware configuration.

Figure 2-3: Hardware configuration



(1) PS (power supply unit) and PSINPUT (power input unit)

PS and PSINPUT generate DC power for use within the Device from an external power supply. The PS is a power supply unit and PSINPUT is a power supply input unit. Each has an AC power supply and a DC power supply.

Table 2-1: List of PSs

Abbreviation	Basic specifications
PS-A21	AC power supply 100 or 200 V AC system
PS-D21	DC power supply -48 V DC system

Table 2-2: List of PSINPUTs

Abbreviation	Basic specifications
PSIN-A21	AC power supply input unit 100 or 200 V AC system For PSINPUT1, 3, and 5
PSIN-A22	AC power supply input unit 100 or 200 V AC system For PSINPUT2, 4, and 6
PSIN-D21	DC power supply input unit -48 V DC system For PSINPUT1, 3, and 5

Abbreviation	Basic specifications
PSIN-D22	DC power supply input unit -48 V DC system For PSINPUT2, 4, and 6

(2) FAN

FAN is a fan unit for cooling the inside of the Device.

Table 2-3: List of fan units

Abbreviation	Basic specifications
FAN-21	Fan unit for AX8616R
FAN-22	Fan unit for AX8616R or AX8632R

(3) BCU (Basic Control Unit)

BCU manages the entire Device and processes routing protocols. This part is common to all the Devices.

Table 2-4: List of BCUs

Abbreviation	Basic specifications
BCU-1R	Basic control unit 16-GB memory

(4) SFU (Switch Fabric Unit)

SFU performs high-speed packet transmission and reception between PRUs.

Table 2-5: List of SFUs

Abbreviation	Basic specifications
SFU-M1	Switch fabric unit for AX8616R
SFU-L1	Switch fabric unit for AX8632R

(5) PRU (Packet Routing Unit)

PRU achieves high-speed IP forwarding and QoS by performing operations such as routing, filtering, and QoS control through hardware.

Table 2-6: List of PRUs

Abbreviation	Basic specifications
PRU-1A	Packet routing processor 1A

(6) NIF (Network Interface Board)

NIF is an interface control board supporting various media types and processes the physical layer. There are several types of NIF.

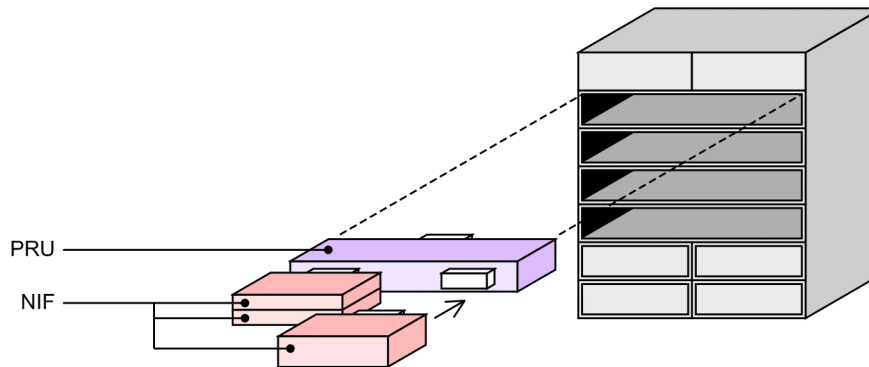
Table 2-7: List of NIFs

Abbreviation	Basic specifications	Size
NL1G-12T	10/100/1000-Mbit/s Ethernet 12 lines	Single half
NL1G-12S	1-Gbit/s Ethernet 12 lines SFP	Single half

Abbreviation	Basic specifications	Size
NLXG-6RS	10-Gbit/s Ethernet 6 lines SFP+	Single half
NMCG-1C	100-Gbit/s Ethernet 1 line CFP	Single full

A PRU has slots to for installing NIFs. A maximum of four single half-size NIFs or a maximum of two single full-size NIFs can be installed in one PRU. Note that both types of NIFs (single full-size NIF and single half-size NIF) can be installed together in one PRU. The following figure shows an image of PRU and NIF installation.

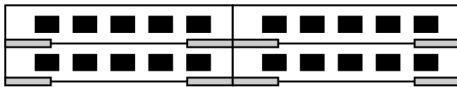
Figure 2-4: Image of PRU and NIF installation



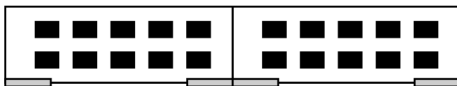
The following figure shows the NIF installation configuration.

Figure 2-5: NIF installation configuration

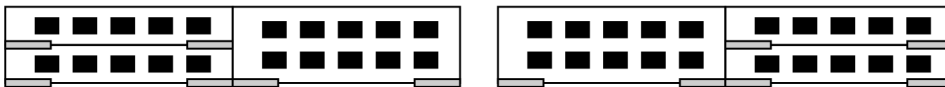
(a) Four single half-size NIFs are mounted



(b) Two single full-size NIFs are mounted



(c) Single half-size and full-size NIFs are mounted together



2.2.2 Software

The following table describes the Device software.

Table 2-8: List of software (basic software)

Abbreviation	Functionality
OS-R/OS-RE	Ethernet, IPv4/IPv6 packet forwarding, unicast routing, multicast routing, filters, QoS, network management functionality, operation management functionality, and other functionality. (This includes encryption functionality.)

Chapter

3. Capacity Limit

This chapter describes the capacity limits for the Device.

- 3.1 Hardware installation capacities
- 3.2 Capacity limits

3.1 Hardware installation capacities

3.1.1 Maximum number of ports that can be handled

The following table describes the maximum number of ports that each model can handle.

Table 3-1: Maximum number of ports that can be handled

Model name	Ethernet			
	100GBASE-R	10GBASE-R	1000BASE-X	10/100/1000BASE-T
AX8616R	8	96	192	192
AX8632R	16	192	384	384

3.1.2 Maximum installable number of components

(1) Installable number of components

The following table describes the maximum number of components that can be installed in each model, including optional devices.

Table 3-2: Maximum installable number of components

Hardware component	AX8616R	AX8632R
BCU	2	2
SFU	4	4
PRU	4	8
NIF (Single full) [#]	8	16
NIF (Single half) [#]	16	32
FAN	6	9
PS/PSINPUT (AC power supply)	4	6
PS/PSINPUT (DC power supply)	4	6
Memory card (SD type)	1/BCU	1/BCU

#

Maximum number of components that can be installed when NIFs of the same type are installed.

(2) Maximum installable number of NIFs

The maximum number of NIFs that can be installed depends on the NIF type. The table below describes the maximum number of NIFs that can be installed in a device per NIF type. Note that values in the table indicate the maximum number of NIFs that can be installed when NIFs of the same type are installed.

Table 3-3: Maximum installable number of NIFs by type, per device

NIF type	Size	AX8616R	AX8632R
NL1G-12T	Single half	16	32
NL1G-12S	Single half	16	32

NIF type	Size	AX8616R	AX8632R
NLXG-6RS	Single half	16	32
NMCG-1C	Single full	8	16

3.2 Capacity limits

3.2.1 Number of table entries

(1) Overview

In this section, the term "number of table entries" refers to the number of routes and the number of filter entries and QoS flow entries.

This Device can be used to select the allocation pattern for the appropriate number of table entries according to the network configuration. You can change an allocation pattern by using configuration commands.

Some route-type and flow-type entry allocation patterns are provided. The following table describes the route-type and flow-type.

Table 3-4: Descriptions of route-type and flow-type table entries

Item	Description
Route-type table entry	IPv4 unicast route IPv4 multicast route IPv6 unicast route IPv6 multicast route ARP NDP
Flow-type table entry	Filter entry QoS flow entry

(2) Hardware profile

In this Device, the hardware profile specifies how the table entries are used to operate the device. You can set the hardware profile to be used by using configuration commands. The following table describes the hardware profile type and supported BCU and PRU.

Table 3-5: Hardware profile type

Hardware profile	Supported BCU	Supported PRU
router-1	BCU-1R	PRU-1A

(3) Allocation patterns

The following tables describe the allocation patterns.

Table 3-6: Allocation patterns for route-type table entries

Pattern name	Meaning
default [#]	A mix of all entry types
ipv4-uni	Priority given to IPv4 unicast (IPv4 unicast main, no multicast and no IPv6)
ipv6-uni	Priority given to IPv6 unicast (IPv6 unicast main, no multicast)

[#]: Default pattern

Table 3-7: Allocation patterns for flow-type table entries

Pattern name	Meaning
default [#]	Equal priority given to filters and QoS

Pattern name	Meaning
filter	Priority given to filters
filter-only	Filter only
qos	Priority given to QoS flow
qos-only	QoS flow only

#: Default pattern

(4) Relationship between a hardware profile and an allocation pattern

The subsection below describes the numbers of route-type table entries and flow-type table entries by hardware profile. When using the VRF functionality, the maximum number of entries is equal to the total number of entries for all VRFs.

(a) router-1

The following table describes the number of route-type table entries for hardware profile router-1.

Table 3-8: Number of route-type table entries for router-1

Pattern name	IPv4 unicast route ^{#1}	IPv4 multicast route	IPv6 unicast route ^{#2}	IPv6 multicast route	ARP	NDP
default	1015808	8000	425984	8000	120000	120000
ipv4-uni	1998848	0	0	0	120000	120000
ipv6-uni	32768	0	983040	0	120000	120000

#1: The following information is included in the number of IPv4 unicast routes:

- Active routes combining RIP, OSPF, BGP4 and static routes
- Active extranet routes imported from other VRFs (including the global network)
- *number-of-IPv4-addresses-configured-for-an-interface* x 2: host routes of directly connected routes, subnet routes
- Number of ARP entries
- If a loopback interface is specified, one route is added.
If a loopback interface is used with VRF, one route is added for each VRF.
- If RIP version 2 is used, one route is added.
If RIP version 2 is used with VRF, one route is added for each VRF.
- If OSPF is used, two routes are added.
If OSPF is used with VRF, two routes are added for each VRF.
- If accept mode was set with VRRP and the state changed to the master state, one route is added.
- In all other cases, four routes are used as fixed device information.
If VRF is used, one route is used as fixed device information for each VRF.

#2: The following information is included in the number of IPv6 unicast routes:

- Number of active routes combining RIPng, OSPFv3, BGP4+, and static routes
- *number-of-IPv6-addresses-configured-for-an-interface* x 2 +

number-of-IPv6-link-local-addresses: host routes (global and link local) of directly connected routes, subnet routes (global).

- Number of NDP entries
- If a loopback interface is specified, one route is added.
If a loopback interface is used with VRF, one route is added for each VRF.
- If accept mode was set with VRRP and the state changed to the master state, one route is added.
- In all other cases, one route is used as fixed device information.
If VRF is used, one route is used as fixed device information for each VRF.

The table below describes the number of flow-type table entries for hardware profile `router-1`. For details about the flow detection mode, see *1.1.3 Flow detection mode* in the manual *Configuration Guide Vol. 2 For Version 12.1* or *3.1.3 Flow detection mode* in the manual *Configuration Guide Vol. 2 For Version 12.1*.

Table 3-9: Numbers of flow-type table entries for router-1 (by PRU)

Flow detection mode	Pattern name	Filter	QoS flow
Quantity-oriented mode	default	64000	64000
	filter	96000	32000
	filter-only	128000	--
	qos	30000	96000
	qos-only	--	128000
Condition-oriented mode	default	32000	32000
	filter	48000	16000
	filter-only	64000	--
	qos	15000	48000
	qos-only	--	64000

Legend: --: Not applicable

3.2.2 Route allocation pattern

The following subsection describes capacity limits according to route allocation patterns by hardware profile.

(1) Route allocation patterns for hardware profile router-1*Table 3-10: Route allocation patterns for hardware profile router-1 (1/2)*

Route allocation pattern	IPv4 unicast					IPv4 multicast		Number of IPv4 interfaces
	Maximum number of route entries		Maximum number of route entries by protocol			PIM-SM/PIM-SSM		
	Total active and inactive	Active	RIP+OSPF	BGP	Static	Amount of (S,G) multicast routing information	Number of interfaces	
default	4063232	1015808	100000	4063232	262144	8000	4096	16380
ipv4-uni	7995392	1998848	100000	7995392	262144	--	--	16380
ipv6-uni	131072	32768	30000	131072	32768	--	--	16380

Table 3-11: Route allocation patterns for hardware profile router-1 (2/2)

Route allocati on pattern	IPv6 unicast					IPv6 multicast		Nume r of IPv6 interfa ces
	Maximum number of route entries		Maximum number of route entries for each protocol			PIM-SM/PIM-SSM		
	Total active and inactive	Active	RIPng+ OSPFv3	BGP4+	Static	Amoun t of (S,G) multic ast routing inform ation	Nume r of interfa ces	
default	1703936	425984	100000	1703936	262144	8000	4096	16380
ipv4-uni	--	--	--	--	--	--	--	16380
ipv6-uni	3932160	983040	100000	3932160	262144	--	--	16380

Legend: --: Not applicable

3.2.3 Link aggregation

The following table describes the capacity limits for link aggregation that can be configured.

Table 3-12: Capacity limits for link aggregation

Model	Maximum number of channel groups per device	Maximum number of ports per channel group
AX8616R	192	16
AX8632R	384	16

3.2.4 Filters and QoS**(1) Filters and QoS flow**

This subsection describes the capacity limits for filters and QoS flow. The number of entries here is the number after you convert the list set by the configurations (`access-list` and

qos-flow-list) to a format (entry) used within the device.

(a) Number of filter entries and QoS flow entries

The following table describes the maximum number of filter entries and QoS flow entries.

Table 3-13: Number of filter entries and QoS flow entries

Model	Maximum number of filter entries		Maximum number of QoS flow entries	
	Per PRU	Per device	Per PRU	Per device
AX8616R	128000	512000	128000	512000
AX8632R	128000	1024000	128000	1024000

You use configuration commands to configure the flow control, and the number of entries used varies depending on the flow detection condition parameters configured in the list. The following table describes the flow detection condition parameters that use multiple entries.

Table 3-14: Flow detection conditions that use multiple entries

Flow detection condition parameters that use multiple entries	Examples of calculating the number of entries to use
Destination IPv4 address range specification, source IPv4 address range specification, and destination IPv6 address range specification	<p>The number of entries is determined by whether the specified IP address is separated by several subnets.</p> <p>For example, if 192.168.0.1 to 192.168.0.4 are specified for the destination IPv4 address, it is separated into the following three subnets, so there are three entries.</p> <ul style="list-style-type: none"> • 192.168.0.1/32 • 192.168.0.2/31 • 192.168.0.4/32
Destination port number range specification, and source port number range specification	<p>The number of entries is determined by whether the specified value can be divided into several values when separated by a maximum 16-bit mask.</p> <p>For example, if 135 to 140 are specified as the destination port number, it is separated into the following three areas, so there are three entries.</p> <ul style="list-style-type: none"> • 135/16:0000 0000 1000 0111 (binary expression) • 136/14:0000 0000 1000 10xx (binary expression) • 140/16:0000 0000 1000 1100 (binary expression)
TCP session maintenance (packet detection with the ack flag ON or the rst flag ON)	Two entries are used.
IP length upper or lower limit specification	<p>The number of entries is determined by whether the specified IP length can be divided into several values when separated by a maximum 16-bit mask.</p> <p>For example, if the upper limit is specified to 10, it is separated into the following three areas with the range of 0 to 10, so there are three entries.</p> <ul style="list-style-type: none"> • 0-7/13:0000 0000 0000 0xxx (binary expression) • 8-9/15:0000 0000 0000 100x (binary expression) • 10/16:0000 0000 0000 1010 (binary expression)

If the above flow detection conditions are specified in a multiple-to-one list, the value in which the number of entries used in each flow detection condition is multiplied becomes the number of entries used in one list.

If one of the above flow detection conditions is specified in one list, the number of entries used in the specified flow detection condition becomes the number of entries used in one list.

If two or more are specified, the value in which the number of entries used in each flow detection condition is multiplied becomes the number of entries used in one list.

If the above flow detection conditions are not specified, the number of entries used in one list becomes one entry.

(b) Number of policer entries

When QoS flow with a specified policer entry is applied to an interface, the policer entry is used up. The following table describes the maximum number of policer entries.

Table 3-15: Maximum number of policer entries

Model	Maximum number of entries on the receiving side		Maximum number of entries on the sending side	
	Per PRU	Per device	Per PRU	Per device
AX8616R	64000	256000	64000	256000
AX8632R	64000	512000	64000	512000

The number of entries used by one policer entry varies depending on the content of the bandwidth monitoring functionality specified in the policer entry. The following table describes the numbers of policer entries used for one policer entry.

Table 3-16: Number of policer entries used by one policer entry

Bandwidth monitoring functionality specified in one policer entry	Number of entries used
Maximum bandwidth monitoring only	1
Minimum bandwidth monitoring only	1
Both maximum and minimum bandwidth monitoring	2

3.2.5 Network management

(1) CFM

The following table describes the capacity limits for CFM.

Table 3-17: Capacity limits for CFM

Model	Number of domains	Number of MAs	Number of MEPs	Total number of CFM ports ^{#1, #2}	Total number of remote MEPs ^{#2, #3}
All models of the AX8600R series	8/device	16380/device	16380/device	16380/device	49152/device

#1

The total number of CFM ports is the total number of interfaces sending CFM frames. You can check the total number of CFM ports by using the `show cfm summary` operation command.

#2

The total number of CFM ports and the total number of remote MEPs are governed by the capacity limits when using the default CCM transmission interval. The capacity limits of the total number of CFM ports and total number of remote MEPs change if you change the CCM transmission interval. The following table describes the capacity limits for total CFM ports

and total remote MEPs according to the set CCM transmission interval.

Table 3-18: Capacity limits based on CCM transmission interval

Model	Interval for sending CCMs	Total number of CFM ports	Total number of remote MEPs
All models of the AX8600R series	1 minute or longer	16380	49152
	10 seconds	4096	12288
	1 second	1024	1024

#3

The total number of remote MEPs is the total number of MEPs on other devices. This affects the CCM receiving performance from MEPs. You can check the total number of remote MEPs by using the `show cfm remote-mep` operation command.

Table 3-19: Capacity limits for CFM physical ports and channel groups

Model	Total number of physical ports and channel groups to which MEPs can be assigned [#]
All models of the AX8600R series	All ports

#

Multiple MEPs can be assigned to the same port. For channel groups, one channel group is counted as one port.

Table 3-20: Capacity limits for the CFM database

Model	Number of MEP CCM database entries	Number of linktrace database entries [#]
All models of the AX8600R series (IEEE 802.1ag)	63/MEP	2048/device
All models of the AX8600R series (ITU-T Y.1731)	49152/device	2048/device

#

If information for 256 devices is stored per route, the database can store information for a maximum of eight routes (2048/256 devices = 8 routes).

(2) LLDP

The following table describes the capacity limits for LLDP.

Table 3-21: Capacity limits for LLDP

Model	LLDP neighboring device information [#]
All models of the AX8600R series	Same as the number of ports that can be handled

#

The LLDP neighboring device information is the information of the neighboring devices that are managed by LLDP and are connected to the Device.

3.2.6 IP interfaces and IP packet forwarding

(1) Number of IP interfaces

An interface with a configured IPv4 or IPv6 address is called an IP interface. The following interfaces can be configured with an IP address on this Device:

- Ethernet interface
- Ethernet subinterface
- Port channel interface
- Port channel subinterface
- Management port
- Serial connection port (AUX)
- Loopback interface

The table below describes the maximum number of IP interfaces that can be used with the Device. IPv4 and IPv6 addresses can be used on the same interface as well as separately on different interfaces.

Table 3-22: Maximum number of IP interfaces

IP interface type	Number of IP interfaces
Ethernet interface	16380 ^{#1}
Ethernet subinterface	
Port channel interface	
Port channel subinterface	
Management port	1
Serial connection port (AUX) ^{#2}	1
Loopback interface ^{#3}	1025

#1

This is the total number of Ethernet interfaces, Ethernet subinterfaces, port channel interfaces, and port channel subinterfaces. However, the total number of Ethernet subinterfaces, port channel interfaces, and port channel subinterfaces is 16000.

#2

Only IPv4 addresses can be assigned.

#3

One can be assigned for each global network or VRF.

(2) Maximum number of multihomed subnets

In a multihomed connection, multiple IPv4 or IPv6 addresses can be assigned to the same interface.

(a) For IPv4

The following table describes the maximum number of multihomed subnets for IPv4. The values indicated here are the number of addresses that can be assigned to one interface in the configuration.

Table 3-23: Maximum number of multihomed subnets (for IPv4)

IP interface type	Number of multihomed subnets
Ethernet interface	256
Ethernet subinterface	256
Port channel interface	256
Port channel subinterface	256
Management port	1
Serial connection port (AUX)	1
Loopback interface	1

(b) For IPv6

The table below describes the maximum number of multihomed subnets for IPv6. The values indicated here are the number of addresses that can be assigned to one interface in the configuration.

Table 3-24: Maximum number of multihomed subnets (for IPv6)

IP interface type	Number of multihomed subnets
Ethernet interface	7
Ethernet subinterface	7
Port channel interface	7
Port channel subinterface	7
Management port	7
Loopback interface	1

(3) Maximum number of IP addresses**(a) IPv4 address**

The following table describes the maximum number of IPv4 addresses that can be assigned per device in the configuration.

Table 3-25: Maximum number of IPv4 addresses that can be assigned per device in the configuration

IP interface type	Number of IPv4 addresses
Ethernet interface	16672 [#]
Ethernet subinterface	
Port channel interface	
Port channel subinterface	
Management port	1
Serial connection port (AUX)	1
Loopback interface	1025

#

This is the total number of Ethernet interfaces, Ethernet subinterfaces, port channel interfaces, and port channel subinterfaces. However, the total number of Ethernet subinterfaces, port channel interfaces, and port channel subinterfaces is 16000.

(b) IPv6 address

The table below describes the maximum number of IPv6 addresses that can be assigned per device in the configuration. The values indicated here include the number of IPv6 link-local addresses assigned in the configuration.

Table 3-26: Maximum number of IPv6 addresses that can be assigned per device in the configuration

IP interface type	Number of IPv6 addresses
Ethernet interface	16672 [#]
Ethernet subinterface	
Port channel interface	
Port channel subinterface	
Management port	7
Loopback interface	1025

#

This is the total number of Ethernet interfaces, Ethernet subinterfaces, port channel interfaces, and port channel subinterfaces. However, the total number of Ethernet subinterfaces, port channel interfaces, and port channel subinterfaces is 16000.

An interface must always be assigned one IPv6 link-local address. When an IPv6 global address is assigned to an interface in the configuration, an IPv6 link-local address is assigned automatically to the interface. In addition to a link-local address, the address `::1/128` is assigned automatically to the loopback interface. For that reason, the maximum numbers of IPv6 addresses actually set for a device are as shown in the following table.

Table 3-27: Maximum number of IPv6 addresses assigned for a device

IP interface type	Number of IPv6 addresses assigned in the configuration	Number of automatically assigned IPv6 addresses	Total
Ethernet interface	16672 [#]	16380 [#]	33052 [#]
Ethernet subinterface			
Port channel interface			
Port channel subinterface			
Management port	7	1	8
Loopback interface	1025	2050	3075

#

This is the total number of Ethernet interfaces, Ethernet subinterfaces, port channel interfaces, and port channel subinterfaces.

(4) Maximum number of remote devices

The following describes the maximum number of remote devices with which the Device can

communicate.

(a) Number of ARP entries

For IPv4, the hardware address corresponding to the destination address of the packet to be sent is determined by the ARP. The maximum number of remote devices is determined by the number of ARP entries. An ARP entry can be registered as a static entry by using a configuration command. The following table describes the maximum number of static ARP entries that can be set in the configuration.

Table 3-28: Maximum number of static ARP entries that can be set per device in the configuration

Model	Maximum number of static ARP entries
All models of the AX8600R series	65535

For details about the maximum number of ARP entries allowed by the Device, see *Table 3-8: Number of route-type table entries for router-1*. Note that the maximum number of ARP entries includes the number of static ARP entries.

(b) Number of NDP entries

For IPv6, NDP address resolution determines a hardware address that corresponds to the destination address of a packet to be sent. The maximum number of remote devices is determined by the number of NDP entries. An NDP entry can be registered as a static entry by using a configuration command. The following table describes the maximum number of static NDP entries that can be set in the configuration.

Table 3-29: Maximum number of static NDP entries that can be set per device in the configuration

Model	Maximum number of static NDP entries
All models of the AX8600R series	65535

For details about the maximum number of NDP entries allowed by the Device, see *Table 3-8: Number of route-type table entries for router-1*. Note that the maximum number of NDP entries includes the number of static NDP entries.

(c) Maximum number of RA interfaces

Using RA, terminals generate addresses based on the IPv6 address information received from the router. The following table describes the maximum number of interfaces and the maximum number of prefixes for the Device.

Table 3-30: Maximum number of interfaces and maximum number of prefixes for RA

Model	Maximum number of interfaces	Maximum number of prefixes	
		Per interface	Per device
All models of the AX8600R series	16380	7	32760

(5) VRF

The table below describes the number of VRFs that can be set. Note that the global network is not included in the number.

Table 3-31: Number of VRFs that can be set

Model	Number of VRFs that can be set
All models of the AX8600R series	1024

(6) Policy-based routing

The following table describes the capacity limits for policy-based routing.

Table 3-32: Number of entries for policy-based routing per device

Item	Number of entries
Number of entries in the access list for which policy-based routing is specified	Included in the maximum number of filter entries in <i>Table 3-13: Number of filter entries and QoS flow entries</i> . ^{#1}
Number of IPv4 policy-based routing lists	4096 ^{#2}
Number of IPv6 policy-based routing lists	4096 ^{#2}
Maximum number of next hops per policy-based routing list	8

#1

For details on how to calculate the number of entries, see *3.2.4 Filters and QoS*.

#2

The same policy-based routing list can be specified for multiple access lists. In this case, the number of policy-based routing lists to be used is calculated as one list.

(7) DHCP/BOOTP relay agent

The following table describes the capacity limits for a DHCP/BOOTP relay agent.

Table 3-33: Capacity limits for a DHCP/BOOTP relay agent

Item	Capacity limits
Number of client connection interfaces	16383
Number of clients	65532
Number of assigned addresses	65532
Number of servers	4096
Number of servers (per global network)	16
Number of servers (per VRF)	16
Number of servers (per interface)	16

(8) DHCPv6 relay agent

The following table describes the capacity limits for a DHCPv6 relay agent.

Table 3-34: Capacity limits for a DHCPv6 relay agent

Item	Capacity limits
Number of client connection interfaces	16383
Number of clients	131064
Number of assigned addresses (total of IA_NA, IA_TA, and IA_PD)	131064
Number of servers	4096
Number of servers (per global network)	4096
Number of servers (per interface)	16

Item	Capacity limits
Number of automatically generated static routes	131064

(9) VRRP

The following table describes the capacity limits for VRRP.

Table 3-35: Capacity limits for VRRP

Model	Maximum number of virtual routers	
	Per interface	Per device
All models of the AX8600R series	255 [#]	255 [#]

[#]: Total IPv4 and IPv6 virtual routers

Table 3-36: Capacity limits for VRRP (when using group switching)

Model	Maximum number of virtual routers		Maximum number of groups	Maximum number of follower virtual routers per group
	Per interface	Per device		
All models of the AX8600R series	255 [#]	16380 [#]	255	16379

[#]: The maximum number of IPv4 and IPv6 virtual routers is 255. However, by creating a follower virtual router with the use of group switching, it is possible to operate 16380 virtual routers.

3.2.7 Unicast routing**(1) Maximum number of neighboring routers**

The following table describes the definition of the maximum number of neighboring routers for each routing protocol.

Table 3-37: Definitions of maximum number of neighboring routers

Routing protocol	Definition of the maximum number of neighboring routers
Static routing	Number of next hop addresses
RIP, RIPng	Number of RIP or RIPng routers on a RIP- or RIPng-enabled network of the Device
OSPF, OSPFv3	If the Device is a designated OSPF or OSPFv3 router (DR or BDR), this is the number of all other OSPF or OSPFv3 routers on the network. If the Device is not a designated OSPF or OSPFv3 router, it is the number of designated routers (DR, BDR) on the network.
BGP4, BGP4+	Number of BGP4 or BGP4+ peers

The following table describes the maximum number of neighboring routers.

Table 3-38: Maximum number of neighboring routers

Routing protocol	Maximum number of neighboring routers
Static routing (total number of IPv4 and IPv6)	32760 [#]
RIP	200

Routing protocol	Maximum number of neighboring routers
RIPng	200
OSPF	250
OSPFv3	125
BGP4	500
BGP4+	500
Total number of neighboring routers for RIP, RIPng, OSPF, OSPFv3, BGP4, and BGP4+	512

#

The number of neighboring routers that can be monitored by the dynamic monitoring functionality is limited by the polling interval. The following table describes the details.

Table 3-39: Maximum number of neighboring routers that support the dynamic monitoring functionality for static routes

Polling interval	Maximum number of neighboring routers that support the dynamic monitoring functionality
1 second	240
5 seconds	1200

(2) Relationship between the number of route entries and the maximum number of neighboring routers

The following table describes the relationship between the maximum number of route entries and the maximum number of neighboring routers.

Table 3-40: Relationship between the number of route entries and the maximum number of neighboring routers

Routing protocol	Number of route entries ^{#1}	Maximum number of neighboring routers ^{#2}
RIP	2000	100
	10000	20
RIPng	2000	100
	10000	20
OSPF ^{#3, #4}	1000	250
	5000	50
	10000	25
	100000	3
OSPFv3 ^{#3, #5}	1000	125
	5000	25
	10000	12
	100000	3

Routing protocol	Number of route entries ^{#1}	Maximum number of neighboring routers ^{#2}
BGP4	#6	500
BGP4+	#6	500

#1

The number of route entries includes alternate routes.

#2

If all the routing protocols (RIP, RIPng, OSPF, OSPFv3, BGP4, and BGP4+) are used in conjunction, the maximum number of neighboring routers for each protocol is $1/n$, where n is the number of routing protocols being used. For example, when BGP4 and BGP4+ are not used and OSPF (1000 routes) and OSPFv3 (1000 routes) are used together, the maximum number of neighboring routers is 1/2, and 125 with OSPF and 62 with OSPFv3.

#3

The maximum number of OSPF/OSPFv3 route entries is equivalent to the number of LSAs.

#4

If OSPF is used on VRFs, the maximum number of neighboring routers in the device is 250. Make sure that the total number of neighboring routers (calculated by multiplying the number of LSAs in each VRF by the number of neighboring routers) does not exceed 250000.

#5

If OSPFv3 is used on VRFs, the maximum number of neighboring routers in the device is 125. Make sure that the total number of neighboring routers (calculated by multiplying the number of LSAs in each VRF by the number of neighboring routers) does not exceed 125000.

#6

See *Table 3-10: Route allocation patterns for hardware profile router-1 (1/2)* and *Table 3-11: Route allocation patterns for hardware profile router-1 (2/2)*.

(3) Maximum number of configuration settings for the Device

The table below describes the maximum number of route configurations that can be set for each routing protocol.

The numbers shown in this table are the maximum numbers that can be specified by the configuration. Make sure to stay within all capacity limits shown in this chapter during operation.

Table 3-41: Maximum number of configurations that can be set

Category	Configuration command	Definition of "maximum number"	Maximum number of settings
IPv4 summarized route	ip summary-address	Number of lines	1024
IPv6 summarized route	ipv6 summary-address	Number of lines	1024
IPv4 static	ip route	Number of lines	1048576
IPv6 static	ipv6 route	Number of lines	1048576
RIP	network	Number of lines	256
	ip rip authentication key	Number of lines	512

Category	Configuration command	Definition of "maximum number"	Maximum number of settings
OSPF	area range	Number of lines	1024
	area virtual-link	Total number of lines when the authentication-key and message-digest-key parameters are set	512
	ip ospf authentication-key ip ospf message-digest-key	Total number of lines for each command	512
	network	Number of lines	512
	router ospf	Number of lines	256
OSPFv3	area range	Number of lines	1024
	ipv6 router ospf	Number of lines	128
BGP4	network	Number of lines	1024
BGP4+	network	Number of lines	1024
Route filtering	distribute-list in (RIP) distribute-list out (RIP) redistribute (RIP)	Total number of lines for each command	2048
	distribute-list in (OSPF) distribute-list out (OSPF) redistribute (OSPF)	Total number of lines for each command	2048
	distribute-list in (BGP4) distribute-list out (BGP4) redistribute (BGP4)	Total number of lines for each command	2048
	distribute-list in (RIPng) distribute-list out (RIPng) redistribute (RIPng)	Total number of lines for each command	2048
	distribute-list in (OSPFv3) distribute-list out (OSPFv3) redistribute (OSPFv3)	Total number of lines for each command	1024
	distribute-list in (BGP4+) distribute-list out (BGP4+) redistribute (BGP4+)	Total number of lines for each command	2048
	ip as-path access-list	Number of setting <id> types	1024
		Number of lines	4096
	ip community-list	Number of setting <id> types	512
		Number of lines with the standard setting	1024
		Number of lines with the expanded setting	1024
	ip prefix-list	Number of setting <id> types	2048
		Number of lines	8192
	ipv6 prefix-list	Number of setting <id> types	2048

3. Capacity Limit

Category	Configuration command	Definition of "maximum number"	Maximum number of settings
		Number of lines	8192
	neighbor in (BGP4) neighbor out (BGP4)	Total number of lines with the <ipv4 address> setting	1024
		Total number of lines with the <peer group> setting	1024
	neighbor in (BGP4+) neighbor out (BGP4+)	Total number of lines with the <ipv6 address> setting	1024
		Total number of lines with the <peer group> setting	1024
	route-map	Number of setting <id> types	1024
		Number of <id> and <seq> combinations	4096
	match as-path	Total number of parameters specified for each line	4096
	match community	Total number of parameters specified for each line	4096
	match interface	Total number of parameters specified for each line	2048
	match ip address match ipv6 address	Total number of parameters specified for each line	4096
	match ip route-source match ipv6 route-source	Total number of parameters specified for each line	2048
	match origin	Number of lines	2048
	match protocol	Total number of parameters specified for each line	4096
	match route-type	Number of lines	2048
	match tag	Total number of parameters specified for each line	2048
	match vrf	Total number of parameters specified for each line	4096
	set as-path prepend count set distance set local-preference set metric set metric-type set origin set tag	Number of <id> and <seq> combinations for a route-map filter on which any one of these parameters is specified	4096
	set community	Total number of parameters specified for each line	2048
	set community-delete	Total number of parameters specified for each line	2048

3.2.8 Multicast routing

This subsection describes the capacity limits for IPv4 and IPv6 multicast. If IPv4 or IPv6 multicast is used on multiple VRFs, you must include the total number of all VRFs and the global network within the capacity limitations.

(1) Capacity limits for multicast

The following table describes the capacity limits for IPv4 and IPv6 multicast.

Table 3-42: Capacity limits for multicast

Item	Maximum number	
	IPv4 multicast	IPv6 multicast
PIM-SM and PIM-SSM multicast interfaces	512/device	512/device
IGMP and MLD operating interfaces	4095/device	4095/device
Multicast senders	256/group 4000/device	256/group 4000/device
Downstream interfaces for all multicast forwarding entries ^{#1}	560000/device	
Amount of PIM-SM or PIM-SSM multicast routing information (total of (S,G) multicast routing information and (*,G) multicast routing information) <ul style="list-style-type: none"> S: Source address G: Group address 	8000/device	8000/device
PIM-SM or PIM-SSM multicast forwarding entries ^{#2} (total of multicast forwarding entries and negative cache entries)	8000/device	8000/device
IGMP and MLD multicast group members ^{#3, #4}	256/interface 32768/device	256/interface 32768/device
Source addresses per group address with IGMP and MLD	256/group address	256/group address

#1

The total number of downstream interfaces in all the multicast forwarding entries is the total of downstream interfaces for IPv4 multicast and for IPv6 multicast. Note that the maximum number becomes equal to or less than 560000 depending on the configuration and the usage status of entries.

#2

Multicast forwarding entries refer to IPv4 and IPv6 multicast routes described in 3.2.1 *Number of table entries*.

#3

The number of multicast group members indicates the maximum number of received IGMP Report messages and MLD Report messages.

#4

The number of multicast group members per device refers to the total number of multicast groups joined through all interfaces.

(2) Capacity limits related to PIM-SM

The following table describes the capacity limits related to PIM-SM.

Table 3-43: Capacity limits related to PIM-SM

Item	Maximum number	
	IPv4 multicast	IPv6 multicast
Neighboring routers	256/interface 512/device	256/interface 512/device
Rendezvous point candidates	2/group address	2/group address
Group addresses that can be assigned to rendezvous points per device [#]	128/network (VPN) 512/device	128/network (VPN) 512/device
Group addresses that can be assigned to rendezvous points per network (VPN)	128/network (VPN) 512/device	128/network (VPN) 512/device
Bootstrap router candidates	512/device	512/device
Static rendezvous point router addresses	16/network (VPN) 512/device	16/network (VPN) 512/device
Configurations of multicast server virtual connection functionalities	--	128/interface 256/device

Legend: --: Not applicable

#

If a rendezvous point is set without specifying any group address, the default group address (224.0.0.0/4 for IPv4 and ff00::/8 for IPv6) is set. When a rendezvous point is set for a global network and VRF, the default group address is also used as a group address.

(3) Capacity limits related to IGMP and MLD

The following table describes the capacity limits related to IGMP and MLD.

Table 3-44: Capacity limits related to IGMP and MLD

Item	Maximum number	
	IPv4 multicast	IPv6 multicast
Static group members ^{#1}	256/interface 4000/device	256/interface 4000/device
Configurations of PIM-SSM Link Operation in IGMP and MLD (source address and group address pairs) ^{#2}	1024/device	1024/device
Record information that can be processed per Report message with IGMPv3 and MLDv2 ^{#3}	32 records/message 32 sources/record	32 records/message 32 sources/record

#1

The number of static group members is the total number of multicast groups that members statically join through each multicast interface. When a member statically joins the same multicast group through multiple interfaces, the number of static group members is not one, but the number of interfaces through which the relevant member statically joins the multicast group.

#2

The number of settings changes depending on the value obtained by combining the number of interfaces used for multicast and the number of multicast group members. Use PIM-SSM Link Operation in IGMP and MLD within the ranges described in *Table 3-45: Number of settings for PIM-SSM Link Operation in IGMP and MLD for the number of used interfaces* and *Table 3-46: Number of settings for PIM-SSM Link Operation in IGMP and MLD for the total of multicast group members*.

Note that the total number of multicast group members is the number of dynamic group members and static group members combined. When a member joins the same group address through different interfaces, the number of multicast group members is not one, but the number of interfaces through which the relevant member joins the group address.

#3

A maximum of 256 sources can be processed in one IGMPv3 Report message. A record that does not contain source information is also counted as one source.

When PIM-SSM Link Operation in IGMP is configured, the number of source addresses defined in the EXCLUDE Record that matches that setting is counted. If there are multiple EXCLUDE Records in the received IGMPv3 Report message, and if more than 256 sources were added in the setting for PIM-SSM Link Operation in IGMP, no multicast routing information will be created for any subsequent EXCLUDE Records in that message that match the link operation setting. Note that this also applies to MLD.

Table 3-45: Number of settings for PIM-SSM Link Operation in IGMP and MLD for the number of used interfaces

Number of used interfaces	Number of settings for PIM-SSM Link Operation in IGMP and MLD
256	1024
512	512
1024	256
4095	64

Table 3-46: Number of settings for PIM-SSM Link Operation in IGMP and MLD for the total of multicast group members

Total number of multicast group members	Number of settings for PIM-SSM Link Operation in IGMP and MLD
64	1024
128	512
256	256
512	128
1024	64
2048	32
4096	16
8192	8

(4) Capacity limits related to VRF

The following table describes the capacity limits when using the multicast routing functionality with VRF.

Table 3-47: Capacity limits related to VRF

Item	Maximum number	
	IPv4 multicast	IPv6 multicast
VRFs to which multicast can be set	512/device	512/device
Multicast filters for a multicast extranet [#]	1024/device	1024/device
Route-map filters to be used for a multicast extranet	512/device	512/device

#

This is the total number of group addresses within access lists specified by all route-map filters.

(5) Notes on multicast packet senders

Some multicast packet sender has the special property of sending multicast packets as burst traffic. Caution must be exercised if the multicast packets received from a sender with this property are distributed via multicast.

The number of interfaces capable of multicast operation varies depending on the type of network interface board (NIF) handling the multicast receivers' lines. The table below describes the numbers of interfaces capable of multicast transmission. When IPv4 multicast and IPv6 multicast are used together, the number of interfaces is the total of interfaces for IPv4 multicast and for IPv6 multicast.

Table 3-48: Number of interfaces capable of multicast transmission

NIF type	Number of interfaces capable of multicast transmission (recommended value [#])
NL1G-12T	64 interfaces per port
NL1G-12S	64 interfaces per port
NLXG-6RS	64 interfaces per port
NMCG-1C	1024 interfaces per port

#

The recommended values are calculated assuming as follows. A sender has the special property of sending multicast packets as eight bursts (the property of temporarily storing multicast packets amounting to eight packets, and then continuously sending them to the network). If the number of bursts is larger, some multicast packets might be discarded. In such a case, the number of interfaces to which multicast is set must be reduced.

Chapter

4. Starting the Device and Logging In

This chapter provides overviews of operation terminals required to operate the Device and operation management, and describes how to start and stop the Device, and how to log in and log out.

- 4.1 Operation terminal-based management
- 4.2 Starting the device
- 4.3 Login and logout

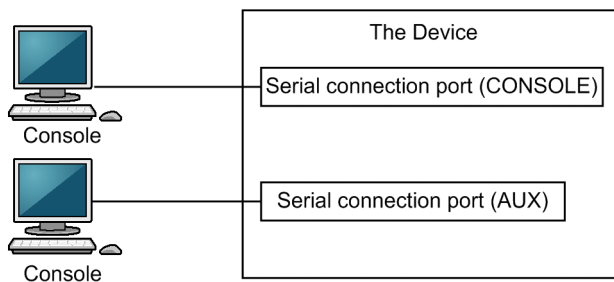
4.1 Operation terminal-based management

A console or remote operation terminal is required to operate the Device. A console is a terminal connected via RS232C, and a remote operation terminal is a terminal connected via an IP network. The Device also supports network management by an SNMP manager over an IP network. A terminal such as a console or remote operation terminal that performs the operation management of the Device is called an operation terminal.

4.1.1 Connection topology of operation terminals

A console is connected to the serial connection port (CONSOLE) of the Device. It can also be connected to the serial connection port (AUX) of the Device. The figure below shows the connection topology of the console.

Figure 4-1: Console connections

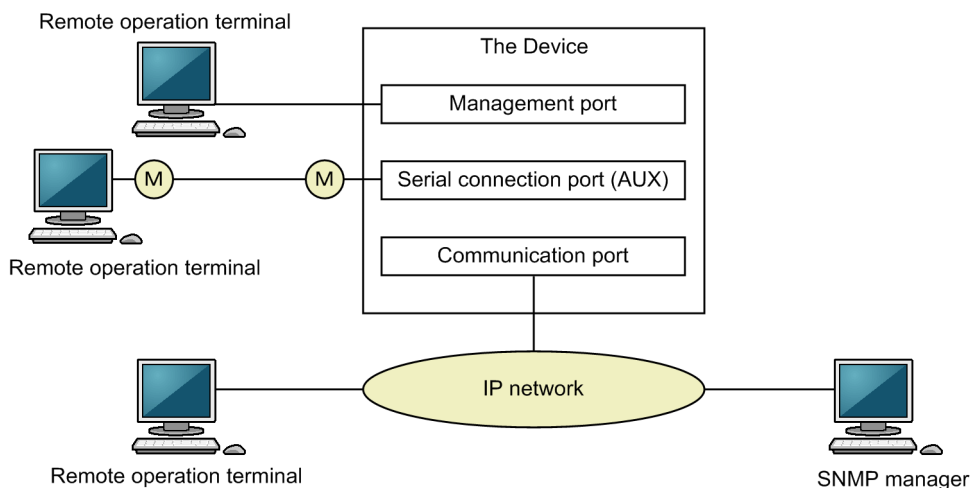


A remote operation terminal can employ the three connection topologies described below.

- Connection via a management port
- Connection via an IP network to which a communication port is connected
- IP-connection to a serial connection port (AUX) by dial-up

The figure below shows the connection topology of remote operation terminals.

Figure 4-2: Remote operation terminal connections



Legend: (M) : Modem

(1) Serial connection port (CONSOLE)

The serial connection port (CONSOLE) is for console connections. Because you can log in via this

port without performing any configuration settings, you can log in to the device from this port during initial deployment, and then enter the initial settings.

(2) Serial connection port (AUX)

The serial connection port (AUX) is for console connections. Because you can log in via this port without specifying any configuration settings, you can log in to the device from this port during initial deployment, and then specify the initial settings. Rom and Boot states are not displayed during connection from the serial connection port (AUX).

(3) Management port

Using the management port, you can log in to the Device from a remote operation terminal or manage the network via an SNMP manager. To log in to the Device via this port using Telnet or FTP, you must first register the IP address of the Device and permit remote access using configuration commands.

(4) Communication port

The communication port enables the same operations as a management port.

(5) Dial-up IP connection to serial connection port (AUX)

The dial-up IP connection enables the same operation as when a remote operation terminal is connected via a management port. For details about how to set the Device and modem for this connection, see 7.1.3 *Dial-up IP connection*.

4.1.2 Operation terminals

The following table describes the difference in scope in the operation management of a console and remote operation terminal.

Table 4-1: Difference in scope in the operation management of a console and remote operation terminal

Operation functionality	Console	Remote operation terminal
Remote login	Not supported	Supported
Login from the Device to an operation terminal	Not supported	Supported
Access control	None	Yes
Command input	Supported	Supported
File transfer protocol	None	FTP
IP communication	Not supported	IPv4 and IPv6
SNMP manager connection	Not supported	Supported
Configuration settings	Not required	Required

(1) Console

The console connects via RS232C and runs general communications software. To enable communication between the console and the Device, make sure that the following standard VT-100 settings (Device defaults) are defined in the communication software:

- Communication speed: 9600 bit/s
- Data size: 8 bits
- Parity bit: None
- Stop bit: 1 bit

- Flow control: None

If you want to use the console with a communication speed other than 9600 bit/s (1200, 2400, 4800, or 19200 bit/s) in connection of a serial connection port (CONSOLE), change the communication speed on the Device side using the `speed` configuration command. The new setting takes effect after you log out from the console.

For connection of a serial connection port (AUX), the communication speed is fixed at 9600 bit/s.

Figure 4-3: Example of setting the communication speed during console connection

```
(config)# line console 0
(config-line)# speed 19200
```

Note:

Keep the following in mind when using the console.

- When you log in from the console, the Device automatically acquires and sets the screen size using the VT-100 control characters. If the console does not support VT-100 emulation, the screen size cannot be obtained or set. Invalid character strings might appear or the first CLI prompt might be displayed incorrectly.

Note that the same problem occurs when you press a key as soon as you log in. This is because display results cannot be acquired for VT-100 control characters. If this happens, log in again.

- The communication speed settings are enabled after logging out. Change the communication speed settings of the communication terminal and communication software you are using after logging out from the console. Until they are changed, some characters are displayed incorrectly (e.g. login prompt).
- If the communication speed is set to settings other than 9600 bit/s, invalid characters appear after starting (or restarting) the device until the new configuration is enabled in the system.

(2) Remote operation terminal

Remote operation terminals connect to the Device via an IP network and perform command operations. Any terminal that has Telnet client functionality can be used as a remote operation terminal.

Note:

The Telnet server in the Device recognizes `CR` as the line feed code. Some clients send `CR` and `LF` as the line feed code. If you connect to a device from this type of terminal, problems will occur: Blank lines might appear, or nothing happens when you press the `y` or `n` key in response to a prompt. If this is the case, check the client settings.

4.1.3 Overview of operation management functionality

To begin using the Device, complete the setup tasks and then power on the Device. From an operation terminal connected to the Device, you can execute operation commands and configuration commands to check the device status or to change the configuration as the connected network changes. The following table describes the Device management operations you can perform.

Table 4-2: Operation management functionality

Operation functionality	Overview
Command input	Accepts input from the command line.
Login control	Blocks unauthorized access and performs password checks.

Operation functionality	Overview
Configuration editing	Sets the running configuration.
Network commands	Supports remote operation commands.
Logs and statistics	Shows information such as past failures and statistics about line usage.
LED display and fault reporting	Shows the status of the Device using LEDs.
MIB information gathering	Manages the network via an SNMP manager.
Device maintenance	Provides commands such as displaying statuses for maintaining the device, and line diagnostics for tracking device and network failures.
Memory card tools	Performs tasks such as formatting memory cards.

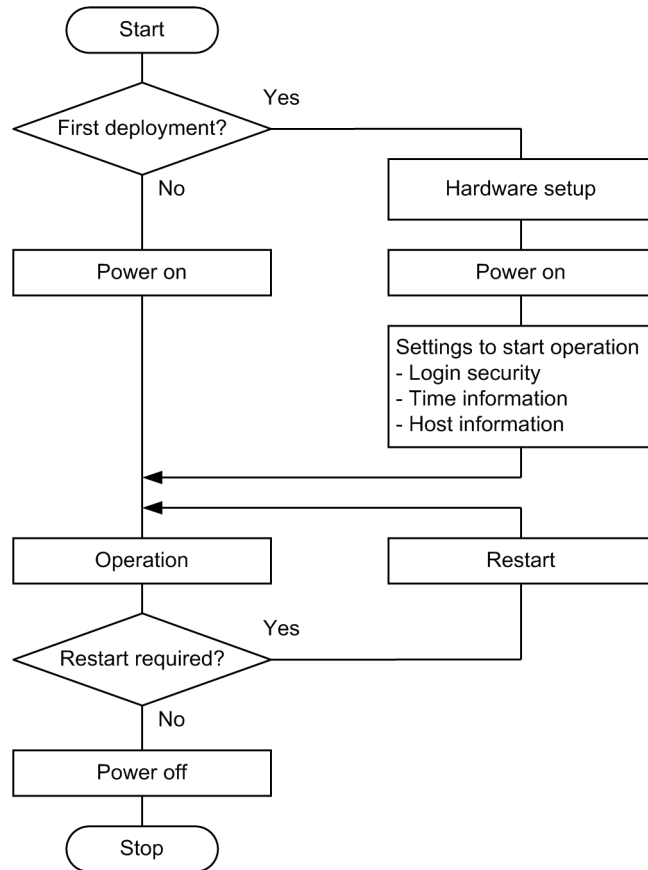
4.2 Starting the device

This section describes how to start and stop the Device.

4.2.1 Workflow from starting to stopping a device

The figure below shows the workflow from starting to stopping the Device. For details on how to set up the hardware, see the *Hardware Instruction Manual*.

Figure 4-4: Workflow from starting to stopping the Device



4.2.2 Start procedures

The following table describes the procedures for starting and restarting the Device.

Table 4-3: Start and restart procedures

Start method	Description	Procedure
Power on	Starts the Device from the powered-off status.	Turn the power switch on.
Manual restart	Resets the Device after a failure. The time required for a restart varies depending on the board.	Press the RESET button.
Command restart	Resets the Device after a failure.	Execute the <code>reload</code> command.

Start method	Description	Procedure
Default restart	<p>Restarts the Device if you cannot log in because you forgot your password, or if you cannot execute commands from the console for some reason such as an error in configuring command authorization. During a default restart, none of the following operations is performed: login authentication by password, authentication when changing to administrator mode (by the <code>enable</code> command), RADIUS or TACACS+ authentication, and command authorization. Even if the user account <code>operator</code> is not set in the configuration, you can log in as the user <code>operator</code>.# Take care when starting the Device by a default restart because the security level lowers in the above case.</p> <p>Note that a default restart does not change the configuration.</p> <p>The new password set at a default restart takes effect after the Device is restarted.</p> <p>Before executing a default restart, make sure that you stop the Device from the system operation panel. For details on how to stop the Device from the system operation panel, see <i>11.1.9 Stop procedure</i>.</p> <p>In a BCU duplex configuration, execute a default restart for the BCU in both the active and standby systems. Execute the default restart on the active system first, and then the standby system.</p>	Push and hold the RESET button for at least five seconds.

#

If you log in to the Device by using the user `operator` when the user account `operator` is not set in the configuration, login is processed with the following common user information:

- User name: `remote_user`
- Home directory: `/usr/home/share`

If the STATUS lamp turns red when you start or restart the Device, see the *Troubleshooting Guide*. For details about the LED lamp indications, see the *Hardware Instruction Manual*.

The Device boots from the memory card if you start or restart the Device from an inserted memory card that contains the software image file `k.img`. When you use this method, the configuration information reverts to the factory defaults and you cannot save your own settings. Avoid using this method under normal circumstances.

4.2.3 Stop procedure

Powering off the Device while files are being accessed might corrupt the files. Make sure that no users are logged in before you power off the Device. We recommend that you first stop the device by using the `reload stop` operation command, and then turn off the power.

4.3 Login and logout

This section describes login and logout procedures.

(1) Login

When the device starts, a login page appears. Enter your user name and password. If authentication is successful, a command prompt appears. If authentication fails, the message `Login incorrect` appears and you cannot log in. The figure below shows the login page.

When you first install the Device, you can log in with the user name `operator`, without needing a password.

Figure 4-5: Login page

```
login: operator
Password: *****                                <-1
Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.
>                                                    <-2
```

1. If no password is set or you start the device by a default restart, this part is not displayed. The actual input characters in the password are not shown.
2. The command prompt appears. However, when the device is started by a default restart, the following message is displayed before the command prompt appears:

```
*****
* WARNING!                                     *
* A default restart was performed on the device.   *
* The security level of the device has been lowered.*
*****
```

(2) logout

To log out after completing operations via the CLI, execute the `logout` command or the `exit` command. The figure below shows the logout page.

Figure 4-6: Logout page

```
> logout
login:
```

(3) Auto-logout

You are automatically logged out if there is no key input for a set duration (default: 60 minutes). You can change the auto-logout time using the `username` configuration command or the `set exec-timeout` operation command.

Chapter

5. Command Operations

This chapter describes how to specify commands on the Device.

- 5.1 Command input mode
- 5.2 CLI operations
- 5.3 Notes on CLI operation

5.1 Command input mode

5.1.1 List of operation commands

The following table describes the operation commands for input mode transitions and utilities.

Table 5-1: List of operation commands

Command name	Description
enable	Changes the command input mode from user mode to administrator mode.
disable	Changes the command input mode from administrator mode to user mode.
quit	Ends the current command input mode.
exit	Ends the current command input mode.
logout	Logs out from the device.
configure (configure terminal)	Changes the command input mode from administrator mode to configuration command mode, and starts configuration editing.
diff [#]	Compares two specified files and displays their differences.
grep [#]	Retrieves a specified file and outputs lines containing a specified pattern.
more [#]	Shows one page of the contents of a specified file.
less [#]	Shows one page of the contents of a specified file.
tail [#]	Outputs the contents of a specified file from a specified point.
hexdump [#]	Shows a hexadecimal dump.

[#]

See 9. *Utilities* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

5.1.2 Command input modes

To change the configuration or check the status of the Device, you must move to the appropriate command input mode, and then enter a configuration command or operation command. From the CLI prompt, you can tell which command input mode you are in.

The following table describes the correspondences between command input modes and CLI prompts.

Table 5-2: Correspondences between command input modes and CLI prompts

Command input modes	Executable command	Prompt
User mode	Operation commands (Some commands, such as the <code>configure</code> command, can only be executed in administrator mode.)	>
Administrator mode		#
Configuration command mode	Configuration commands [#]	(config) #

[#]

You can execute an operation command while editing a configuration entry without changing the command input mode to administrator mode by using commands such as the `quit` command and the `exit` command. To do so, enter the operation command preceded by a

dollar sign (\$).

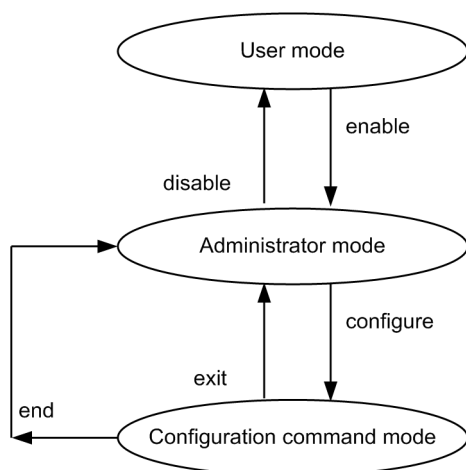
<Example>

To execute the `show ip arp` operation command in configuration command mode:

```
(config)# $show ip arp
```

The following figure shows an overview of mode transitions.

Figure 5-1: Overview of mode transitions



Legend:

→ : Direction of mode transition

In the following cases, letters appear in front of the CLI prompt to show you where you are:

1. When you set a host name using the `hostname` configuration command, the first 20 characters of the host name appear in the prompt.
2. If the edited configuration has not been saved in the startup configuration or if there is a difference between the changed startup configuration and the configuration being edited, an exclamation mark (!) appears in front of the prompt.

The following figure shows an example of displaying prompts in these two cases.

Figure 5-2: Example of displaying prompts

```

> enable
# configure
(config)# hostname "OFFICE1"
!OFFICE1(config)# save
OFFICE1(config)# quit
OFFICE1# quit
OFFICE1>
  
```

5.2 CLI operations

5.2.1 Command line completion

By pressing the **Tab** key on the command line, you can complete a partially entered command name or file name, which simplifies command input. The following figure shows an example of simplified command input using this functionality.

Figure 5-3: Simplified command input using entry completion

```
(config)# in[Tab]
(config)# interface
```

When you press the **Tab** key here, a list of parameters and file names that can be specified appears. The following figure shows an example of displaying parameters and file names by using command line completion.

Figure 5-4: Example of displaying parameters and file names by using command line completion

```
(config)# interface [Tab]
async                loopback                port-channel
gigabitethernet      mgmt                    range
hundredgigabitethernet null                tengigabitethernet
(config)# interface
```

5.2.2 Help functionality

By typing a question mark (?) on the command line, you can search for a specifiable command or parameter. You can also find out what the command or parameter means. The following figure shows an example of the Help display when you enter a question mark.

Figure 5-5: Example of Help display by entering a question mark

```
> show port ?
<port list>  <nif no.>/<port no.> ex."1/2", "2/1-5", "3/1,4/1", "**/*"
statistics   Display the statistics information list of ports
transceiver  Display the transceiver information list of ports
<cr>
> show port
```

If you type a question mark in a parameter without entering a preceding space, command line completion will activate. To use a question mark (?) in a command parameter, press **Ctrl + V**, and then enter the question mark.

5.2.3 Entry-error location detection functionality

If you enter a command or parameter incorrectly, the error is marked by a caret (^) and an error message appears on the next line. For details on error messages, see *Error messages displayed by the entry-error location detection functionality* in the manual *Operation Command Reference Vol. 1 For Version 12.1*. This functionality also works when the **Tab** key is pressed or a question mark (?) is typed.

Check and re-enter the command or parameter, referring to the location marked by ^ and error message. The following figures show an example of entry-error location detection.

Figure 5-6: Display example for a spelling mistake

```
(config)# interface gigabitehnternet 1/1
interface gigabitehnternet 1/1
                        ^
% The command or parameter at the ^ marker is invalid.
(config)#
```


Figure 5-7: Display example for a missing parameter

```
(config)# interface gigabitethernet 1/1
(config-if)# speed
speed
^
% The command at the ^ marker is invalid.
(config-if)#
```

5.2.4 Abbreviated-command execution

A command or parameter entered in abbreviated form will be executed if the entered characters are identified as a unique command or parameter. The following figure shows an example of abbreviated-command execution.

Figure 5-8: Example of abbreviated-command execution (show netstat interface command)

```
> sh nets in [Enter]
Date 20XX/07/19 12:00:00 UTC
Name      Mtu    Network  Address      Ipkts Ierrs   Opkts Oerrs  Colls
Eth1/2    1500   192.168/24  192.168.0.60  3896   2       2602    0      0
>
```

The configuration commands that can be executed in abbreviated form differ depending on configuration modes.

Configuration command `show`:

Can be executed in abbreviated form in all configuration modes.

Configuration commands `commit`, `end`, `quit`, `exit`, `rollback`, `save`, `status`, and `top`:

Can be executed in abbreviated form only in global configuration mode or in the submode (level 2) to which the state shifts after execution of the `template` command. If these commands are executed in other modes, an entry error occurs.

Configuration command `end-template`:

Can be executed in abbreviated form only in the submode (level 2) to which the state shifts after execution of the `template` command. If these commands are executed in other modes, an entry error occurs.

Configuration commands `delete`, `insert`, and `replace`:

Can be executed in abbreviated form in the submode (level 2) to which the state shifts after execution of the `template` command and in the subsequent modes. If these commands are executed in other modes, an entry error occurs.

Other configuration commands in all modes:

Can be executed in abbreviated form if they can be uniquely identified in each mode.

Parameters following a parameter containing an asterisk (*) cannot be abbreviated.

5.2.5 History functionality

The history functionality allows you to easily re-execute a command entered in the past, and to change part of the command before execution. The following figure shows some examples of using the history functionality.

Figure 5-9: Simplified command input using the history functionality

```
> ping 192.168.0.1 numeric count 1 <-1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.329 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
```

```

round-trip min/avg/max = 1.329/1.329/1.329 ms
>
> ping 192.168.0.1 numeric count 1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.225 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.225/1.225/1.225 ms
>
> ping 192.168.0.2 numeric count 1
PING 192.168.0.2 (192.168.0.2): 56 data bytes

--- 192.168.0.2 PING Statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
>

```

1. Execute the `ping` command on 192.168.0.1.
2. Press the up arrow key (↑) to call the preceding command.
In this example, pressing the up arrow key once displays the line `ping 192.168.0.1 numeric count 1`. Simply press the **Enter** key to re-execute this command.
3. Execute the `ping` command on 192.168.0.1.
4. Press the up arrow key (↑) to call the preceding command, and then use the left arrow key (←) and the **Backspace** key to edit the command string.
In this example, pressing the up arrow key (↑) once displays the line `ping 192.168.0.1 numeric count 1`. Change 1 in the IP address to 2, and then press the **Enter** key.
5. Execute the `ping` command on 192.168.0.2.

Using the history functionality and the character strings in the table below, you can call or change a previously executed command string, and then execute the command. Command string conversion is not supported for configuration commands.

Table 5-3: Characters supported by command string conversion

Specification	Description
!!	Calls and executes the last executed command.
!n	Calls and executes the command that has history number <i>n</i> [#] .
!-n	Calls and executes the <i>n</i> th previous command.
!str	Calls and executes the last executed command beginning with the character string <i>str</i> .
^str1^str2	Executes the last executed command, replacing <i>str1</i> with <i>str2</i> .

#

The array number displayed by the `show history` operation command.

After you call a previously executed command, and then edit the command string or delete the command using the **Backspace** key or the **Ctrl + C** keys, you can call the command again and edit or erase its history.

Notes

Depending on the communication software you are using, the arrow keys (↑, ↓, ←, →) might not call a command. If so, check the settings in your communication software manual.

5.2.6 Pipe functionality

Using a pipe, you can pass command execution results to another command. Passing the results to the `grep` command can make them easier to understand. *Figure 5-10: Result of executing the `show sessions` command* shows the result of executing the `show sessions` command.

Figure 5-11: Filtering the execution result of the `show sessions` command by using the `grep` command shows the result of filtering the execution result of the `show sessions` command by using the `grep` command.

Figure 5-10: Result of executing the `show sessions` command

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
operator console ----- 0   Jan  6 14:16
operator aux      ----- 1   Jan  6 14:16 (ppp0:200.10.10.1)
operator tty0     ----- 2   Jan  6 14:16 (192.168.3.7)
operator tty1     admin  3   Jan  6 14:16 (192.168.3.7)
```

Figure 5-11: Filtering the execution result of the `show sessions` command by using the `grep` command

```
> show sessions | grep admin
operator tty1     admin  3   Jan  6 14:16 (192.168.3.7)
>
```

5.2.7 Redirection

Using redirection, you can output command execution results to a file. The following figure shows an example of outputting the execution result of the `show ip interface` command to a file.

Figure 5-12: Execution result of the `show ip interface` command output to a file

```
> show ip interface > show_interface.log
>
```

5.2.8 Paging

If paging is effective, when the command execution result information you want to view extends outside the viewable area, you can scroll through the information page by page, by keyboard input. Paging is not performed when redirection is used. Paging can be enabled or disabled by executing the `username` configuration command or the `set terminal pager` operation command.

5.2.9 Customizing CLI settings

The behavior of part of the auto-logout and CLI functionality can be customized on a user basis as CLI environment information. The following table describes the CLI functionality and CLI environment information that can be customized.

Table 5-4: Customizable CLI functionality and CLI environment information

Functionality	Customizable contents and defaults
Auto-logout	Time until the user is automatically logged out. Default: 60 minutes
Paging	Whether to enable paging. Default: Paging enabled
Help functionality	List of commands displayed in Help messages. Default: When you display a Help message for operation commands, a list of all specifiable operation commands appears.

This CLI environment information can be set for each user by executing the `username` configuration command. Alternatively, you can temporarily change operation in the target session

by using the following operation commands:

- `set exec-timeout`
- `set terminal pager`
- `set terminal help`

If you set the CLI environment information by using the configuration command, log out once and then log in again to enable the setting. Note that if you temporarily change the operation by using operation commands, you cannot view the setting status. In that case, check the operating status of each functionality.

5.3 Notes on CLI operation

5.3.1 If an operation terminal crashes after logging in

If an operation terminal crashes, the user's login status is sometimes retained in the Device. If this occurs, either wait for the user to be automatically logged out, or log in again and delete the login user by using the `killuser` operation command.

5.3.2 If you are logged out while operating CLI special keys

Pressing **Ctrl + C** keys, **Ctrl + Z** keys or **Ctrl + ** keys might cause you to log out. In such a case, log in again.

5.3.3 If you access the files in a standby system

When accessing files below the `/standby` directory, pay attention to the following points:

- Command line completion cannot be used.
- Do not use the `cd` operation command to move to directories below the `/standby` directory.
- Accessing the files takes longer than accessing files in an active system.

Chapter

6. Configuration

The configuration and operating conditions of the Device must be set to match the network environment. This chapter describes what you need to know when setting the configuration.

- 6.1 Overview of configuration
- 6.2 Configuration editing procedures
- 6.3 Template operations
- 6.4 Configuration operations

6.1 Overview of configuration

Both at deployment and during operation, the administrator will need to perform configuration settings relating to the connected network and the operating conditions of the Device.

6.1.1 Configuration at startup

When you power on the Device, the startup configuration file in internal memory is read and operation commences according to the file contents. The configuration used during operation is referred to as the running configuration.

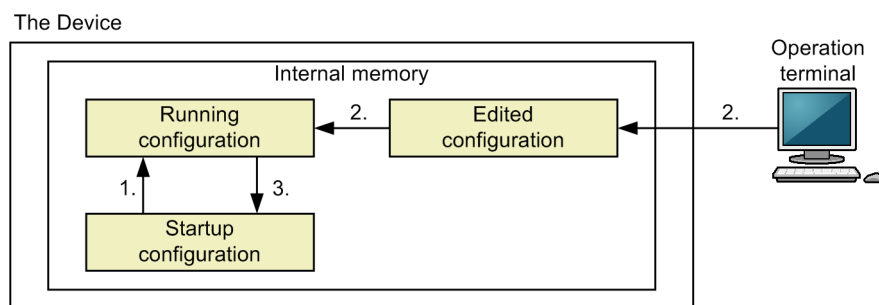
You cannot directly edit the startup configuration. It is updated automatically when you edit the configuration and then execute the `save` command or the `commit` command.

The Device provides two methods for applying an edited configuration to a running configuration. You can select between these two methods by using the commit mode setting. The following describes how to apply the edited configuration for each mode.

(1) Auto-applied commit mode

The edited settings are immediately applied to the running configuration. The following figure shows an overview of the configuration at startup and during operation.

Figure 6-1: Overview of the configuration at startup and during operation (auto-applied commit mode)

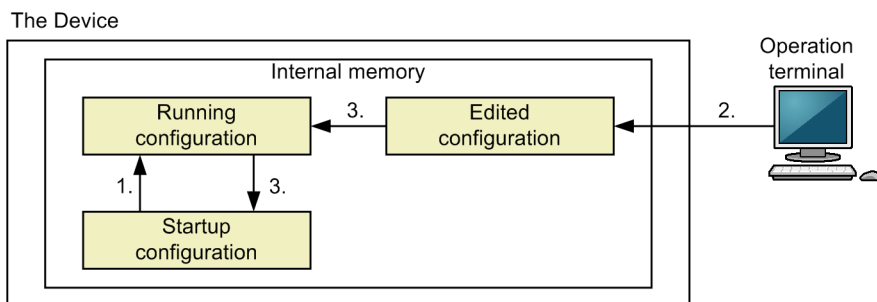


1. Start the Device. The startup configuration is read from the Device's internal memory and loaded as a running configuration.
Operation starts based on the settings of the running configuration.
2. Edit the configuration. The edited settings are immediately applied to the running configuration.
3. Execute the `save` command. The changed running configuration is saved as the startup configuration.

(2) Manual commit mode

The edited settings are not immediately applied to the running configuration. When the `commit` command is executed, the edited settings are collectively applied to the running configuration and then it is saved as the startup configuration. The following figure shows an overview of the configuration at startup and during operation.

Figure 6-2: Overview of the configuration at startup and during operation (manual commit mode)



1. Start the Device. The startup configuration is read from the Device's internal memory and loaded as the running configuration.
Operation starts based on the settings of the running configuration.
2. Edit the configuration. The edited settings are not immediately applied to the running configuration.
3. Execute the `commit` command. The edited settings are applied to the running configuration, and then the running configuration is saved as the startup configuration.

6.1.2 Configuration during operation

When the configuration is edited during operation, if auto-applied commit mode is selected for the commit mode, the edited settings are immediately applied to the running configuration. By executing the `save` command, you can save the changed running configuration as the startup configuration in the Device's internal memory. In manual commit mode, the edited settings are not immediately applied to the running configuration. By executing the `commit` command, you can collectively apply the edited settings to the running configuration and save the running configuration as the startup configuration.

Note that the edited contents will be lost if you restart a device without first saving the running configuration.

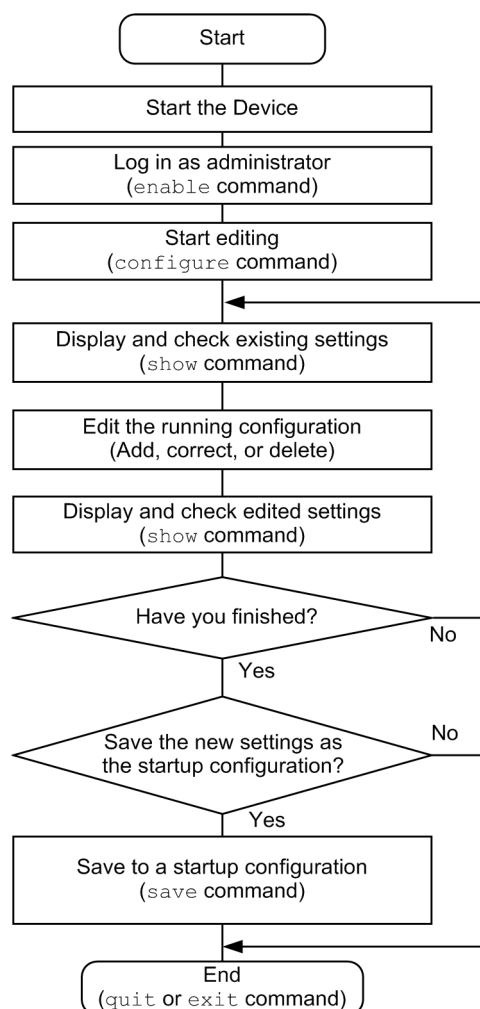
6.1.3 Workflow when editing a running configuration

You will need to edit the running configuration at initial deployment and after changing the network configuration. Editing at deployment must be performed on the console.

(1) Flow in auto-applied commit mode

The figure below shows the flow of editing the running configuration in auto-applied commit mode. After you start editing by executing the `configure` command, execute the `status` command to make sure that auto-applied commit mode is selected for the commit mode.

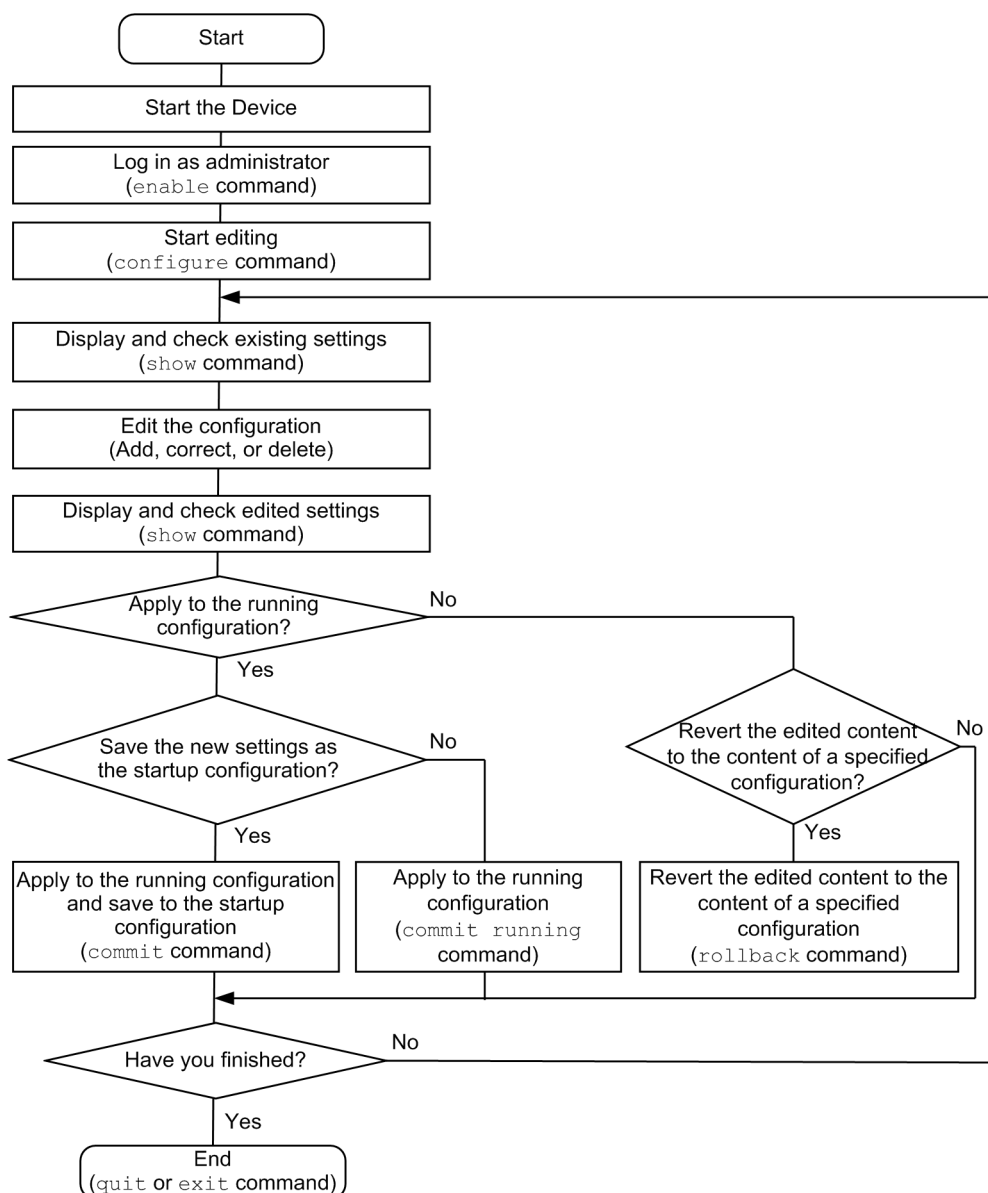
Figure 6-3: Flow of editing the running configuration (auto-applied commit mode)



(2) Flow in manual commit mode

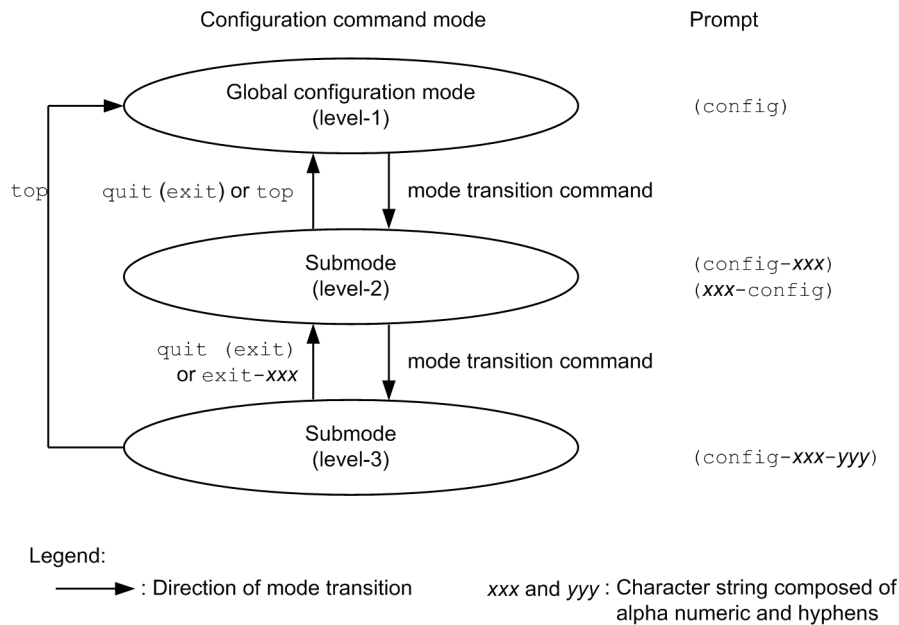
The figure below shows the flow of editing the running configuration in manual commit mode. After you start editing by executing the `configure` command, execute the `status` command to make sure that manual commit mode is selected for the commit mode.

Figure 6-4: Flow of editing the running configuration (manual commit mode)



6.1.4 Mode transition when configurations are edited

Edit configurations in the appropriate executable configuration command mode. To edit a submode configuration, you must first switch from global configuration mode to the submode by using a mode transition command. You can then execute the required configuration commands. The following figure shows an overview of transitions between modes when configurations are edited.

Figure 6-5: Overview of transitions between modes when configurations are edited

6.1.5 Configuration during initial deployment

The Device automatically generates the following configurations during initial deployment:

- **Physical interfaces**
Generates the configuration of each physical interface according to the installation position and type of the NIF board installed in the Device. By default, physical interfaces are in the shutdown state.
- **Default account**
Generates a default account configuration for default operating user during initial deployment.
- **Hardware profile**
Generates a hardware profile configuration according to the BCU or PRU installed in the Device.
- **Flow detection mode for filters and QoS**
Generates a configuration for the flow detection mode for filters and QoS according to the BCU or PRU installed in the Device.
- **Allocation pattern for table entries**
Generates a configuration for allocation patterns of route-type table entries and flow-type table entries according to the BCU or PRU installed in the Device.

6.1.6 Lists of configuration commands and operation commands

The table below describes the configuration commands for configuration setting, editing, and operation.

Table 6-1: List of configuration commands

Command name	Description
apply-template	Applies the configuration commands set to the template to the configuration being edited.

Command name	Description
commit	Applies the edited configuration settings to the running configuration and then saves it as the startup configuration.
configuration commit-mode	Sets the commit mode for the configuration.
delete	Deletes configuration commands set to the template.
end	Ends configuration command mode and returns to administrator mode.
end-template	Ends template mode and returns to global configuration mode.
insert	Inserts a configuration command into a desired location in the template. After this command is executed, the mode shifts to insert mode.
load	Applies the specified configuration file to the configuration being edited. Depending on the contents of the specified file, you can configure, modify, or delete the configuration.
quit (exit)	Returns to the previous mode. If you are editing a configuration in global configuration mode, the command ends configuration mode and returns you to administrator mode.
replace	Overwrites configuration commands set to the template. After this command is executed, the mode shifts to replace mode.
rollback	Restores the contents of the configuration being edited to the contents of the specified configuration.
save	Saves the edited configuration to the startup configuration file or to a backup configuration file.
show	Shows the configuration being edited.
status	Shows the status of the configuration being edited.
template	Creates a configuration command template.
top	Returns to global configuration mode from the submenu.

The following table describes the operation commands relating to configuration editing and operation.

Table 6-2: List of operation commands

Command name	Description
show running-config	Shows the running configuration.
show startup-config	Shows the startup configuration.
copy	Copies a configuration.
erase configuration	Resets a running configuration to the defaults.
show file	Shows the contents and line numbers of a local or remote server file.
cd	Changes the directory.
pwd	Shows the path to the current directory.
ls	Lists files and directories.
dir	Lists files, used for the Device, that were deleted in a way that allows them to be recovered.
cat	Shows the contents of a specified file.

6. Configuration

Command name	Description
cp	Copies a file.
mkdir	Creates a new directory.
mv	Moves or renames a file.
rm	Deletes a specified file.
rmdir	Deletes a specified directory.
delete	Deletes files, used for the Device, in a way that allows them to be recovered.
undelete	Recovers files, used by the Device, that were deleted in a way that allows them to be recovered.
squeeze	Completely erases files, used by the Device, that were deleted in a way that allows them to be recovered.

6.2 Configuration editing procedures

6.2.1 Starting configuration editing

To edit a configuration, first execute the `enable` command to switch to administrator mode. Then enter the `configure` command or the `configure terminal` command. The prompt changes to `(config)#`, allowing you to edit the configuration. The following figure shows an example of starting editing of a configuration.

Figure 6-6: Example of starting editing of a configuration

```
> enable                <-1
# configure             <-2
(config)#
```

1. Execute the `enable` command to enter administrator mode.
2. Start configuration editing.

6.2.2 Displaying and checking configuration entries

(1) Displaying and checking the running configuration or startup configuration

You can display and check the running configuration or the startup configuration file by using the `show running-config` operation command and the `show startup-config` operation command in administrator mode. The following figure shows an example of displaying a running configuration.

Figure 6-7: Example of displaying a running configuration

```
OFFICE01# show running-config                <-1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
interface gigabitethernet 1/1
    shutdown
!
interface gigabitethernet 1/2
    shutdown
!
OFFICE01#
```

1. Display the running configuration.

(2) Displaying and checking the configuration being edited

Using the `show` command in configuration command mode, you can display and check the configuration being edited. *Figure 6-8: Displaying all the contents of the configuration being edited* to *Figure 6-11: Displaying information on the specified interface in interface mode* show examples of displaying configurations.

Figure 6-8: Displaying all the contents of the configuration being edited

```
OFFICE01(config)# show                      <-1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
interface gigabitethernet 1/1
    shutdown
!
interface gigabitethernet 1/2
    shutdown
!
```

```
OFFICE01(config)#
```

1. Display all the contents of the configuration being edited when no parameter is specified.

Figure 6-9: Displaying information on all configured interfaces

```
OFFICE01(config)# show interface gigabitethernet <-1
interface gigabitethernet 1/1
shutdown
!
interface gigabitethernet 1/2
shutdown
!
OFFICE01(config)#
```

1. Display all the configured interfaces in the configuration being edited.

Figure 6-10: Displaying information on the specified interface

```
OFFICE01(config)# show interface gigabitethernet 1/1 <-1
interface gigabitethernet 1/1
shutdown
!
OFFICE01(config)#
```

1. Display gigabit Ethernet interface 1/1 in the configuration being edited.

Figure 6-11: Displaying information on the specified interface in interface mode

```
OFFICE01(config)# interface gigabitethernet 1/1
OFFICE01(config-if)# show <-1
interface gigabitethernet 1/1
shutdown
!
OFFICE01(config-if)#
```

1. Display gigabit Ethernet interface 1/1 in the configuration being edited.

(3) Checking the differences between the configuration being edited and the running configuration

If a configuration is edited while manual commit mode is selected for the commit mode, differences occur between that configuration and the running configuration. The following figure shows an example of checking the differences between the configuration being edited and the running configuration.

Figure 6-12: Example of checking the differences between the configuration being edited and the running configuration

```
OFFICE01(config)# show > edit-config <-1
OFFICE01(config)# quit
The changes to the configuration have not been saved.
Do you want to exit configure mode without saving the changes? (y/n): y
OFFICE01# show running-config > running-config <-2
OFFICE01# diff running-config edit-config <-3
1c1
< #Last modified by operator at Fri Nov 16 12:00:00 20XX UTC with version XX.XX
---
> #Last modified by operator at Fri Nov 16 12:00:01 20XX UTC with version XX.XX
8a9
> speed 1000
```


1. Output all the contents of the configuration being edited to a file.
2. Output all the contents of the running configuration to a file.
3. Output the differences between the configuration being edited and the running configuration.
You can check the changes made from the running configuration.

6.2.3 Configuring the commit mode for the configuration

(1) Checking the commit mode

Before editing the configuration, you must check the commit mode set for the configuration. The following figure shows an example of checking the commit mode.

Figure 6-13: Example of checking the commit mode

```
# configure
(config)# status <-1
File name       : running-config
Commit mode     : Auto commit <-2
Last modified time : Thu Oct 11 12:00:00 20XX UTC by operator (not modified)
Buffer          : Total XXXXXXXXXX Bytes
                  Available XXXXXXXXXX Bytes (XXXX%)
                  Fragments XX Bytes (XXXX%)
Login user      : USER operator LOGIN Fri Oct 12 12:00:00 20XX UTC edit
(config)#
```

1. Execute the `status` command in configuration command mode.
2. When information about the configuration being edited appears, check the content of `Commit mode`. If `Auto commit` is displayed, auto-applied commit mode is currently active. If `Manual commit` is displayed, manual commit mode is currently active.

(2) Setting the commit mode

You must set the commit mode for the configuration. The following figure shows a setting example of changing the commit mode from auto-applied commit mode to manual commit mode.

Figure 6-14: Setting example of changing the commit mode from auto-applied commit mode to manual commit mode

```
(config)# configuration commit-mode manual <-1
!(config)#
```

1. Set the commit mode to manual commit mode. The manual commit mode setting is immediately applied to the running configuration. Therefore, when the setting is made, the mode shifts to manual commit mode.

The following figure shows a setting example of changing the commit mode from manual commit mode to auto-applied commit mode.

Figure 6-15: Setting example of changing the commit mode from manual commit mode to auto-applied commit mode

```
(config)# no configuration commit-mode <-1
!(config)# commit <-2
A commit of the configuration finished successfully.
(config)#
```

1. Delete the manual commit mode setting.
2. Apply the operation in step 1 to the running configuration by using the `commit` command and then save the configuration as the startup configuration. When execution of the `commit` command finishes, the mode shifts to auto-applied commit mode.

6.2.4 Adding, changing, and deleting configuration entries

(1) Configuration command input

Configuration commands are used for editing configuration entries. You can also negate a configuration command by specifying `no` at the beginning. The following figure shows an example of editing a configuration.

Figure 6-16: Example of editing a configuration

```
(config)# interface gigabitethernet 1/1      <-1
(config-if)# description "PORT001"          <-2
(config-if)# exit
(config)#
(config)# interface gigabitethernet 1/1      <-3
(config-if)# no description                  <-4
(config-if)# exit
(config)#
```

1. Change the mode to gigabit Ethernet interface 1/1.
2. Set supplementary information.
3. Change the mode to gigabit Ethernet interface 1/1.
4. Delete supplementary information.

To disable functionality by using configuration commands, specify `no` at the beginning of the command string. To reinstate the functionality, enter the same command without the preceding `no`. The following figure shows an example of disabling and reinstating functionality.

Figure 6-17: Example of disabling and reinstating functionality

```
(config)# no ip domain lookup                <-1
(config)# ip domain name router.example.com  <-2
(config)# ip name-server 192.0.2.1           <-3
(config)# ip domain lookup                   <-4
```

1. Disable the DNS resolver functionality.
2. Set the domain name as `router.example.com`.
3. Set the address for the name server to `192.0.2.1`.
4. Activate the DNS resolver functionality.

(2) Command syntax check

When you enter a configuration command, the system immediately checks whether the input configuration contains any errors. If there are no errors, the prompt shown in the figure below appears, ready for command input. Note that the timing of applying the entered command varies depending on the commit mode of the configuration.

Figure 6-18: Output for a correct configuration

```
(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"
(config-if)#
```

If an error is found in the edited configuration, an error message indicating the nature of the error appears in the line below the entered command, as shown in the figure below. In this case, the edited configuration does not take effect. Correct the error and re-enter the configuration command.

Figure 6-19: Error message output for an incorrect configuration

```
(config)# interface tengigabitethernet 1/1
(config-if)# description
description
```

```

      ^
% The command at the ^ maker is invalid.
(config-if)#

```

6.2.5 Applying the edited settings to the running configuration

(1) Auto-applied commit mode

If auto-applied commit mode is selected for the commit mode of the configuration, the edited settings of the configuration are immediately applied to the running configuration. The following figure shows an example of applying the settings to the running configuration in auto-applied commit mode.

Figure 6-20: Example of applying the settings to the running configuration (auto-applied commit mode)

```

(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"                <-1
!(config-if)# exit
!(config)#

```

1. Edit the configuration. When execution of the command finishes, the settings are applied to the running configuration.

(2) Manual commit mode

When the commit mode of the configuration is manual commit mode, by executing the `commit` command, the edited settings of the configuration are collectively applied to the running configuration and the changed running configuration is saved as the startup configuration. The following figure shows an example of applying the settings to the running configuration in manual commit mode.

Figure 6-21: Example of applying the settings to the running configuration (manual commit mode)

```

(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"                <-1
!(config-if)# exit
!(config)# commit                                <-2
A commit of the configuration finished successfully.
(config)#

```

1. Edit the configuration. When execution of the command finishes, the settings are not yet applied to the running configuration.
2. Execute the `commit` command. The edited settings are collectively applied to the running configuration, which is then saved as the startup configuration.

If you want to discard the edited settings and restore the settings of the specified configuration after editing the configuration, use the `rollback` command. The following figure shows an example of restoring the previous settings of the configuration.

Figure 6-22: Example of restoring the previous settings of the configuration

```

(config)# interface gigabitethernet 1/1
(config-if)# description "PORT001"                <-1
!(config-if)# exit
!(config)# rollback running                        <-2
The configuration being edited will be discarded.
Do you want to roll back the configuration? (y/n): y
A rollback of the configuration finished successfully.
(config)#

```

1. Edit the configuration. When execution of the command finishes, the settings are not yet applied to the running configuration.

2. Execute the `rollback` command. The settings of the specified configuration (the running configuration in this example) are restored to replace the settings of the edited configuration.

6.2.6 Saving configuration entries to a file

(1) Saving to the startup configuration file

Using the `save` command or the `commit` command, you can save the edited configuration to the startup configuration file.

The following figure shows an example of saving configuration entries in auto-applied commit mode.

Figure 6-23: Example of saving configuration entries (auto-applied commit mode)

```
# configure <-1
(config)#
:
: <-2
:
!(config)# save <-3
(config)#
```

1. Start configuration editing.
2. Edit the configuration.
3. Save to the startup configuration file.

The following figure shows an example of saving configuration entries in manual commit mode.

Figure 6-24: Example of saving configuration entries (manual commit mode)

```
# configure <-1
(config)#
:
: <-2
:
!(config)# commit <-3
A commit of the configuration finished successfully.
(config)#
```

1. Start configuration editing.
2. Edit the configuration.
3. Execute the `commit` command. The edited settings are collectively applied to the running configuration and then it is saved as the startup configuration.

(2) Partially saving to a configuration file in global configuration mode

When a command name is specified for the `subset` parameter in the `save` command, among the configuration entries being edited, the configuration entries with the specified command name are saved to a file. The following figure shows an example of saving the configuration entries with the specified command name to a file.

Figure 6-25: Example of saving the configuration entries with the specified command name to a file

```
(config)# show <-1
:
:
:
interface gigabitethernet 1/1
description "PORT001"
!
interface gigabitethernet 1/2
description " PORT002"
```

```

!
:
:
:
(config)# save /usr/home/operator/tmp.cnf subset interface gigabitethernet
<-2
Do you want to save the configuration in the file /usr/home/operator/tmp.cnf? (y/
n): y
(config)# exit
#cat /usr/home/operator/tmp.cnf <-3
interface gigabitethernet 1/1
    description "PORT001"
!
interface gigabitethernet 1/2
    description "PORT002"
!
:
:
:
# configure
(config)# save /usr/home/operator/tmp2.cnf subset interface gigabitethernet 1/1
<-4
Do you want to save the configuration in the file /usr/home/operator/tmp2.cnf?
(y/n): y
(config)# exit
# cat /usr/home/operator/tmp2.cnf <-5
interface gigabitethernet 1/1
    description "PORT001"
!
#

```

1. Check the configuration entries being edited.
2. Among the configuration entries being edited, save the configuration entries for all the already configured gigabit Ethernet interfaces into /usr/home/operator/tmp.cnf.
3. Display the contents of the saved file.
4. Among the configuration entries being edited, save the configuration entries for the already configured gigabit Ethernet interface 1/1 into /usr/home/operator/tmp2.cnf.
5. Display the contents of the saved file.

(3) Partially saving to the configuration file in a submode

When the `save` command is executed with a file name and the `subset` parameter specified in a submode, among the configuration entries being edited, the configuration entries in the relevant mode and subsequent modes are saved to a file. The following figure shows an example of executing the `save` command in a submode.

Figure 6-26: Example of executing the save command in a submode

```

(config)# interface gigabitethernet 1/1
(config-if)# show <-1
interface gigabitethernet 1/1
    description "PORT001"
!
(config-if)# save /usr/home/operator/tmp.cnf subset <-2
Do you want to save the configuration in the file /usr/home/operator/tmp.cnf? (y/
n): y
(config)# exit
#cat /usr/home/operator/tmp.cnf <-3
interface gigabitethernet 1/1
    description "PORT001"
!
#

```

1. Check the configuration entries for gigabit Ethernet interface 1/1.
2. Save the configuration entries for gigabit Ethernet interface 1/1 into `/usr/home/operator/tmp.cnf`.
3. Display the contents of the saved file.

6.2.7 Applying settings from a configuration file

By using the load command, you can apply the settings of the specified configuration file to the configuration being edited. The following figures show an example of merging the specified configuration file into the configuration being edited.

Figure 6-27: Example of merging (adding) a configuration file

```
(config)# show <-1
:
:
:
interface gigabitethernet 1/1
!
:
:
:
(config)# exit
# cat /usr/home/operator/tmp.cnf <-2
interface gigabitethernet 1/1
shutdown
description "PORT001"
speed 1000
no shutdown
!
# configure
(config)# load merge /usr/home/operator/tmp.cnf <-3
Do you want to apply the specified configuration file to the configuration being
edited? (y/n): y
!(config)# show <-4
:
:
:
interface gigabitethernet 1/1
description "PORT001"
speed 1000
!
!(config)#
```

1. Check the configuration being edited.
2. Check the configuration file to be merged `/usr/home/operator/tmp.cnf`. (This file contains the settings to be added to the configuration being edited.)
3. Merge (add) `/usr/home/operator/tmp.cnf` into the configuration being edited.
4. Check the configuration being edited into which the specified file has been completely merged.

Figure 6-28: Example of merging (deleting) a configuration file

```
# show running-config <-1
:
:
:
interface gigabitethernet 1/1
description "PORT001"
speed 1000
```

```

:
:
:
# cat /usr/home/operator/tmp2.cnf <-2
interface gigabitethernet 1/1
shutdown
no description
no speed
no shutdown
!
# configure
(config)# load merge /usr/home/operator/tmp2.cnf <-3
Do you want to apply the specified configuration file to the configuration being
edited? (y/n): y
!(config)# show <-4
:
:
:
interface gigabitethernet 1/1
!
:
:
:
!(config)#

```

1. Check the configuration being edited.
2. Check the configuration file to be merged `/usr/home/operator/tmp2.cnf`. (This file contains the settings to be deleted from the configuration being edited.)
3. Merge `/usr/home/operator/tmp2.cnf` into the configuration being edited. (The settings of this file are deleted from the configuration being edited.)
4. Check the configuration being edited into which the specified file has been completely merged.

6.2.8 Ending configuration editing

(1) Ending configuration editing after saving the edited settings

After saving the edited settings into the startup configuration file by using the `save` or `commit` command, execute the `quit` or `exit` command in global configuration mode.

The following figure shows an example of ending configuration editing in auto-applied commit mode.

Figure 6-29: Example of ending configuration editing (auto-applied commit mode)

```

!(config)# save
(config)# quit <-1

```

1. End configuration editing.

The following figure shows an example of ending configuration editing in manual commit mode.

Figure 6-30: Example of ending configuration editing (manual commit mode)

```

!(config)# commit
A commit of the configuration finished successfully.
(config)# quit <-1

```

1. End configuration editing.

(2) Ending configuration editing without saving the edited settings

After editing the configuration, if you do not execute the `save` or `commit` command but you execute the `quit` or `exit` command to end configuration editing, a confirmation message appears. To exit

configuration command mode without saving the edited settings to the startup configuration file, enter *y*. If you type any other letter, you will remain in configuration command mode. The following figure shows an example of ending configuration editing without saving the edited settings.

Figure 6-31: Example of ending configuration editing without saving the edited settings

```
# configure <-1
(config)#
:
: <-2
:
!(config)# quit
The changes to the configuration have not been saved.
Do you want to exit configure mode without saving the changes? (y/n): y <-3
!#
```

1. Start configuration editing.
2. Edit the configuration.
3. A confirmation message appears.

6.2.9 Notes on configuration editing

(1) Limits on the number of configuration commands

Because user configurations are stored in memory, the number of commands you can enter in configuration entries depends on the amount of available memory. If there is insufficient memory for the entries, or if the number of entries you have edited exceeds the device capacity, either of the following messages appears: The maximum number of entries are already configured. Configuration memory is insufficient. (entry = *<entry-name>*) or The maximum number of entries are already configured. (failed entry = *<entry-name>*). If such a message appears, check whether any unnecessary entries exist.

(2) Copying and pasting configuration entries

You can copy and paste configuration entries a maximum of 1000 characters per line, and less than 4000 characters total (including spaces and line feed codes) per operation. Note that the configurations will not be set correctly if you attempt to paste 4000 characters or more at one time.

If the configuration entries exceed 4000 characters, copy and paste them in multiple operations, each time keeping the number of characters to no more than 1000 per line and less than 4000 total.

6.3 Template operations

This section describes how to use a template to edit the configuration.

6.3.1 Overview of Template

(1) Overview of Template

The features of Template are as follows:

- A series of configuration commands to be repeatedly executed can be registered and created as a template. After creating a template, you can delete, insert, or modify a configuration command to re-edit the template. Also, you can repeatedly apply a created template to the Device.
- Any parameters of a configuration command to be registered in a template can be set as a replaceable string (hereafter called template parameters). You can specify strings to replace the template parameters when the template is applied to the Device.
- The configuration commands registered in a template can be set to the Device in the order they were entered. For example, to change interface information, you can reproduce a series of actions within a template, from temporarily stopping the interface, to changing the settings, and resuming the interface.

For Template, create a template where configuration commands are registered. Then, apply the settings registered in the template to the configuration being edited. These steps resemble creating a script and executing it.

The following figure shows an example of creating a template.

Figure 6-32: Example of creating a template

```
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT
(config-if-TPL)# shutdown
(config-if-TPL)# speed 1000
(config-if-TPL)# no shutdown
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config-TPL)# end-template
(config)#
```

The template here is named as `EtherDEF`. The configuration commands entered in template mode are registered in the template `EtherDEF`. Note that at the time a template is created, the configuration commands registered in it are not applied to the configuration being edited. To apply the settings of the template to the configuration being edited, use the `apply-template` command. The following figure shows an example of applying a template.

Figure 6-33: Example of applying a template

```
(config)# show interface gigabitethernet 1/1          <-1
interface gigabitethernet 1/1
!
(config)# apply-template EtherDEF 1/1                 <-2
(config)# show interface gigabitethernet 1/1          <-3
interface gigabitethernet 1/1
  speed 1000
```

```
!
(config)#
```

1. Check the configuration for gigabit Ethernet interface 1/1.
2. Apply the template `EtherDEF` to gigabit Ethernet interface 1/1.
3. Check the configuration for gigabit Ethernet interface 1/1 to see that the contents of the template `EtherDEF` are applied.

(2) Template position

A template is positioned as part of a configuration and set within a configuration. The following figure shows an example of the configuration structure.

Figure 6-34: Configuration structure

```
(config)# show
:
:
:
template EtherDEF $PORT          - |
  interface gigabitethernet $PORT  |
  shutdown                        |
  speed 1000                       | <-1
  no shutdown                      |
  end-template                     |
!                                  - |
(config)#
```

1. This part is a template.

6.3.2 Creating a template

(1) Creating a template and ending template editing

To create a template, use the `template` command in global configuration mode. When you execute the `template` command, the mode shifts to the mode for editing a template (called template mode) and you can register configuration commands in a template. At this time, `-TPL` (which indicates template mode) is added to the prompt. The following figure shows an example of creating a template.

Figure 6-35: Example of creating a template

```
(config)# template EtherDEF $PORT
(config-TPL)# show
template EtherDEF $PORT
  end-template
!
(config-TPL)#
```

To end template editing, use any of the commands shown in the following table.

Table 6-3: Commands that end template editing

Command name	Description
<code>end</code>	Ends template mode and enters administrator mode.
<code>end-template</code>	Ends template mode and enters global configuration mode.
<code>quit (exit)</code>	If in config-TPL mode, ends template mode and enters global configuration mode. If not in config-TPL mode, moves one level upward.
<code>top</code>	Ends template mode and enters global configuration mode.

The `end-template` command is automatically registered in the template. Therefore, even if template mode is ended by a command other than the `end-template` command, the `end-template` command is registered in the template. The following figure shows an example of ending template editing.

Figure 6-36: Example of ending template editing

```
(config-TPL)# end-template
(config)#
```

(2) Registering configuration commands in a template

You can register configuration commands for setting a configuration and for deleting a configuration in a template. The following figure shows an example of registering configuration commands in a template.

Figure 6-37: Example of registering configuration commands in a template

```
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT          <-1
(config-if-TPL)# shutdown                               <-1
(config-if-TPL)# speed 1000                             <-1
(config-if-TPL)# no shutdown                            <-2
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config-TPL)#
```

1. Register a configuration command for setting a configuration in the template.
2. Register a configuration command for deleting a configuration in the template.

Template provides the modes that are similar to the modes for normal configuration editing. Mode transition occurs in the same way. At this time, `-TPL` (which indicates template mode) is added to the prompt in every mode. The following figure shows an example of template mode transition.

Figure 6-38: Example of template mode transition

```
(config)# interface gigabitethernet 1/1                <-1
(config-if)#                                           <-1
(config-if)# exit
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT          <-2
(config-if-TPL)#                                       <-2
```

1. Mode transition during normal configuration editing.
2. Mode transition during template editing. Mode transition occurs in the same way as during normal configuration editing. `-TPL` (which indicates template mode) is added to the prompt.

In template mode, configuration commands are registered in a template in the order they were entered. The following figure shows an example of registering commands in the template in the order they were entered.

Figure 6-39: Example of registering commands in the template in the order they were entered

```
(config)# template EtherDEF $PORT
(config-TPL)# interface gigabitethernet $PORT          <-1
(config-if-TPL)# shutdown                               <-1
```

```

(config-if-TPL)# speed 1000                <-1
(config-if-TPL)# no shutdown                <-1
(config-if-TPL)# exit
(config-TPL)# show                          <-2
template EtherDEF $PORT
    interface gigabitethernet $PORT        <-3
        shutdown                          <-3
        speed 1000                        <-3
        no shutdown                       <-3
    end-template
!
(config-TPL)#

```

1. Register a configuration command in the template.
2. Use the `show` command to check the contents of the template.
3. The configuration commands are registered in the order they were entered.

6.3.3 Editing a template

(1) Re-registering (overwriting) a command in the template

When a configuration command is entered that is the same as one registered in the template and has the same parameters, the registered command is overwritten. In this case, the current position of the relevant command in order of registration is not changed.

If a configuration command is entered that is the same as one registered in the template but has a different parameter, the newly entered configuration command is registered as a different command.

If the entered command accompanies mode transition, the mode shifts to the relevant mode. Note that a command entered after mode transition is registered as a new command at the end of the relevant mode.

The following figure shows an example of re-registering a command that accompanies mode transition.

Figure 6-40: Example of re-registering a command

```

(config-TPL)# show
template EtherDEF $PORT
    interface gigabitethernet $PORT
        shutdown
        speed 1000
        no shutdown
    end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT <-1
(config-if-TPL)# speed auto                  <-2
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT
    interface gigabitethernet $PORT
        shutdown
        speed 1000
        no shutdown
        speed auto                          <-3
    end-template
!
(config-TPL)#

```

1. Change the mode to gigabit Ethernet interface `$PORT` that is already registered in the template.
2. Enter a configuration command that is the same as the configuration command registered in

the template (speed command) but has a different parameter.

3. The entered command is registered as a new command at the end of gigabit Ethernet interface \$PORT. (This command is not written over the already registered speed 1000.)

(2) Deleting a command in the template

To delete a configuration command registered in the template, use the delete command. The following figure shows an example of using the delete command.

Figure 6-41: Example of using the delete command

```
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT          <-1
(config-if-TPL)# delete speed 1000                     <-2
(config-if-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT                      <-3
    shutdown
    no shutdown
  end-template
!
(config-if-TPL)#
```

1. Shift to the mode for the command to be deleted.
2. Specify the command to be deleted for the delete command.
3. speed 1000 has been deleted.

(3) Inserting a command in the template

To insert a configuration command in a desired position in the template, use the insert command. The following figure shows an example of using the insert command.

Figure 6-42: Example of using the insert command

```
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    no shutdown
  end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT          <-2
(config-if-TPL)# insert speed 1000                     <-3
(config-if-TPL-INS)# no shutdown                       <-4
(config-if-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000                                          <-5
    no shutdown
  end-template
!
(config-if-TPL)#
```

1. Insert a command is in this position.

2. Shift to the mode for the command to be inserted.
3. Specify the command to be inserted for the `insert` command.
4. `-INS` is added after the prompt. Here, enter `no shutdown` that is put in the insert position.
5. `speed 1000` has been inserted before `no shutdown`.

(4) Correcting a command in the template

To correct a configuration command or parameter registered in the template, use the `replace` command. The following figure shows an example of using the `replace` command.

Figure 6-43: Example of using the replace command

```
(config-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000                                <-1
    no shutdown
  end-template
!
(config-TPL)#
(config-TPL)# interface gigabitethernet $PORT  <-2
(config-if-TPL)# replace speed auto           <-3
(config-if-TPL-REP)# speed 1000               <-4
(config-if-TPL)# show
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed auto                                <-5
    no shutdown
  end-template
!
(config-if-TPL)#
```

1. Change the parameter in the `speed` command from `1000` to `auto`.
2. Shift to the mode for the command to be changed.
3. Specify the command after change for the `replace` command.
4. `-REP` is added after the prompt. Here, enter the command before the change.
5. The parameter has been changed.

6.3.4 Applying a template

To apply the configuration commands registered in the template to the configuration being edited, execute the `apply-template` command in global command mode.

When the `apply-template` command is executed, the configuration commands registered in the template are set from the first line, one after another. Therefore, register the configuration commands whose setting order is predetermined in the template in the correct order. The following figure shows an example of applying a template to the configuration being edited.

Figure 6-44: Example of applying a template to the configuration being edited

```
(config)# show template
template EtherDEF $PORT
  interface gigabitethernet $PORT
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config)# apply-template EtherDEF 1/1
(config)#
```



Command execution example

```
(config)# interface gigabitethernet 1/1
(config-if)# shutdown
(config-if)# speed 1000
(config-if)# no shutdown
(config-if)# exit
(config)#
```

Because the configuration commands are applied from top to end in sequence to the configuration being edited, the configuration commands have been virtually set in the order shown by the command execution image in this figure.

6.3.5 Using template parameters

(1) Overview of template parameters

Arbitrary parameters for a configuration command to be registered in a template can be set to a template as template parameters. A template parameter is a replaceable string. If you set some parameter as a template parameter when registering configuration commands in a template, you can specify a numeric value or string to that template parameter when applying the template to the configuration being edited by using the `apply-template` command.

The format for template parameters is a string made up of a dollar sign (\$) and a string of 31 characters or less. Set `$PORT`, for example.

You can use a template parameter for an arbitrary parameter (a parameter surrounded by angle brackets (< >)) for a configuration command. When creating a new template, set all the template parameters to be used for the template. To change the template parameter to be used, use the `change-parameter` parameter in the `template` command.

Note that only the template parameters set by the `template` command can be used for the configuration commands registered in the template. The following figure shows an example of using template parameters when creating a template.

Figure 6-45: Example of using template parameters when creating a template

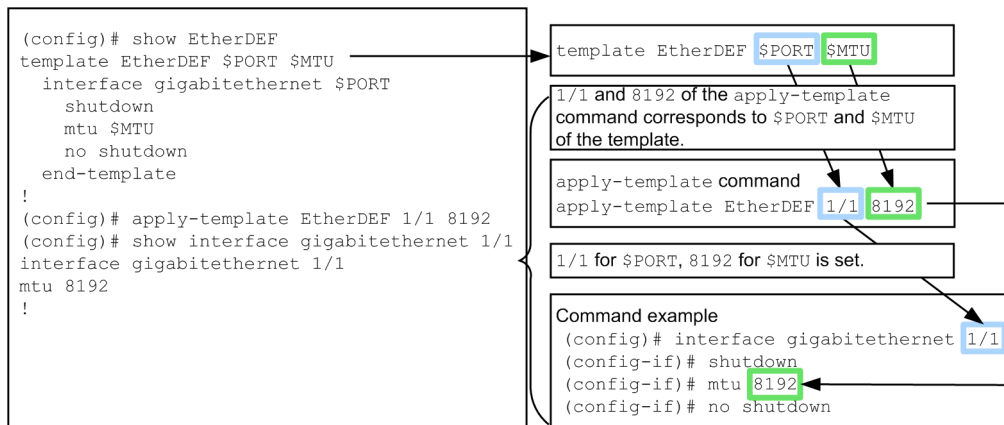
```
(config)# template EtherDEF $PORT $MTU                                <-1
(config-TPL)# interface gigabitethernet $PORT                        <-2
(config-if-TPL)# shutdown
(config-if-TPL)# mtu $MTU                                           <-2
(config-if-TPL)# no shutdown
(config-if-TPL)# exit
(config-TPL)# show
template EtherDEF $PORT $MTU
  interface gigabitethernet $PORT
    shutdown
    mtu $MTU
    no shutdown
  end-template
```

```
!
(config-TPL)#
```

1. Set template parameters when creating a new template.
2. The template parameters set in step 1 can be used as a command parameter. (Any template parameter not set in step 1 cannot be used.)

For the template parameters set in the template, the values that are entered when the `apply-template` command is executed are specified. The following figure shows an example of specifying template parameters.

Figure 6-46: Example of specifying template parameters



In this figure, two template parameters are used in the template, in the order of `$PORT` and `$MTU`. If you enter `1/1` and then `8192` when executing the `apply-template` command, the template is applied to the configuration being edited with `1/1` specified for `$PORT` and `8192` specified for `$MTU`.

By treating arbitrary parameters as template parameters, you can do the following:

- A single template can be used repeatedly. For example, if you set `<nif no.>/<port no.>` as a template parameter while creating a template to be set to an interface, you can make the template applicable to any Ethernet interface.
- When the format of the template parameter to be set is `$<parameter>#<index>`, the same configuration command can be registered in multiple locations.
- When a parameter for which multiple values cannot be specified is set as a template parameter, sequential numeric values (for example, `192.0.2.1`, `192.0.2.2`, ...) can be specified for the template parameter by, for example, using external script functionality.

(2) Registering the same configuration command

To register an identical configuration command to a template, specify the template parameter in the format `$<parameter>#<index>`. By doing so, you can register an identical command as another command because its `<index>` is different. Note that when the `apply-template` command is executed, only the part `$<parameter>` in `$<parameter>#<index>` is applied to the configuration being edited. The following figure shows an example of a template using `$<parameter>#<index>`.

Figure 6-47: Example of a template using `$<parameter>#<index>`

```
(config)# show template
template LacpSet $PORT $LA_ID
  interface range gigabitethernet $PORT#1 <-1
    shutdown
    channel-group $LA_ID mode active
  lacp system-priority 100
  interface port-channel $LA_ID
```



```

    channel-group lacp system-priority 50
interface range gigabitethernet $PORT#2          <-1
    no shutdown
end-template
!
(config)#

```

1. When the template is applied to a configuration by the `apply-template` command, `$PORT#1` and `PORT#2` are the same command because an entered value is specified for `$PORT`. However, because their names are different in the template, they can be registered in several locations.

The following figure shows an example of applying this template to the configuration being edited.

Figure 6-48: Example of applying a template using \$<parameter>#<index>

```

(config)# apply-template LacpSet 1/1 10
(config)# show
:
:
:
lacp system-priority 100
!
interface port-channel 10
    channel-group lacp system-priority 50
!
interface gigabitethernet 1/1
    channel-group 10 mode active
!
(config)#

```

In this figure, the configuration commands are applied in the following order:

1. interface gigabitethernet 1/1
2. shutdown
3. channel-group 10 mode active
4. exit
5. lacp system-priority 100
6. interface port-channel 10
7. channel-group lacp system-priority 50
8. interface gigabitethernet 1/1
9. no shutdown
10. !

(3) Changing a template parameter

To add, change, or delete a template parameter that can be used for templates, use the `change-parameter` parameter in the `template` command. When the `change-parameter` parameter is used, the relevant template parameter set by the `template` command is overwritten. The following figure shows an example of changing a template parameter.

Figure 6-49: Example of changing a template parameter

```

(config)# show EtherDEF
template EtherDEF $PORT
:
:
:
(config)# template EtherDEF change-parameter $PORT $MTU      <-1
(config-TPL)# show
template EtherDEF $PORT $MTU                                  <-2

```

```

:
:
:
(config-TPL)#

```

1. By using the `change-parameter` parameter in the `template` command, change the current template parameter to `$PORT $MTU`.
2. `$MTU` has been added as a usable template parameter.

6.3.6 Special usage of Template

(1) Command that can set multiple items for a parameter

When you register a configuration command that can set multiple items for a parameter in a template, the contents of a parameter that you enter are registered in the template without change. For example, if you enter a command with multiple interfaces specified in it, the settings that you enter are registered without change in a template. When you apply the template by using the `apply-template` command, the template is divided into parts for each interface. The following figure shows an example of a template in which multiple interfaces are specified.

Figure 6-50: Example of a template in which multiple interfaces are specified

```

(config)# show template
template EtherDEF
  interface range gigabitethernet 1/1-2          <-1
    shutdown
    speed 1000
    no shutdown
  end-template
!
(config)#

```

1. The entered commands and parameters are registered in the template without change.

The following figure shows an example of applying this template to the configuration being edited.

Figure 6-51: Example of applying a template in which multiple interfaces are specified

```

(config)# apply-template EtherDEF                <-1
(config)# show interface range gigabitethernet 1/1-2
interface gigabitethernet 1/1                    <-2
  speed 1000
!
interface gigabitethernet 1/2                    <-2
  speed 1000
!

```

1. Apply the template.
2. A divided part of the template corresponding to the interface has been applied to the configuration.

(2) Using template parameters for special parameters

The following table describes how to set template parameters for special parameters in template mode and how to specify values for such template parameters when executing the `apply-template` command.

Table 6-4: Examples of setting template parameters for special parameters and specifying values for such template parameters

Parameter	Template parameter	
	Sample code	Value specification example
<nif no.>/<port no.>	interface gigabitethernet \$PORT	\$PORT:1/1
<interface id list>	monitor session 1 source interface add gigabitethernet \$PORTS	\$PORTS:1/1-2
	monitor session 1 source interface add gigabitethernet \$PORTS1, gigabitethernet \$PORTS2	\$PORTS1:1/1-2 \$PORTS2:2/5
Specification of multiple interfaces	interface range gigabitethernet \$PORTS	\$PORTS:1/1-2
	interface range gigabitethernet \$PORTS1,gigabitethernet \$PORTS2	\$PORTS1:1/1-2 \$PORTS2:2/5
Specification of subinterfaces	interface gigabitethernet \$PORT.\$SUB_INDEX	\$PORT:1/1 \$SUB_INDEX:1
	interface port-channel \$LA_ID.\$SUB_INDEX	\$LA_ID:1 \$SUB_INDEX:1

(3) Special command

When you register in a template a configuration command in which data to be encoded is specified, the encoded data is registered in the template as in the case of normal configuration settings. The following figure shows an example of registering the `banner` command with the template.

Figure 6-52: Example of registering the banner command with the template

```
(config)# template set_banner
(config-TPL)# banner login plain-text          <-1
--- Press CTRL+D or only '.' line to end ---
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.                        <-2
.
(config-TPL)# show
template set_banner
  banner login encode
"V2FybmluZyEhISBXYXJuaW5nISEhIFdhcm5pbmchISEKVHpcyBpcyBvdXIgc3lzdGVtLiBZb3Ugc2
hvdWxkIG5vdCBsb2dpci4KUGx1YXNlIGNsb3NlIGNvbm5lY3Rpb24uCg=="
                                           <-3
!
(config-TPL)#
```

1. Register the `banner` command with the template.
2. Enter a login message.
3. The encoded result has been registered in the template.

6.4 Configuration operations

This section describes operations such as configuration backups and file transfers.

6.4.1 Backing up configurations

Using the `copy` operation command, you can back up a configuration to a remote server or to the Device itself. Note that when saving a backup configuration file to the Device, you cannot specify the directory for the startup configuration file (`/config`). Create your own backup configuration files in your home directory.

You can back up both the startup configuration and running configuration. When you edit a configuration during operation but do not save it, even if you back up the startup configuration, the contents of the backed-up configuration file differ from those of the running configuration or the configuration being edited. The following figures show examples of backing up both configurations.

Figure 6-53: Example of backing up the startup configuration

```
> enable
# copy startup-config ftp://staff@[2001:db8::1]/backup.cnf
Are you sure you want to copy the configuration file to ftp://staff@[2001:db8::1]/
backup.cnf? (y/n): y

Authentication for 2001:db8::1.
User: staff
Password: xxx                                <-1
transferring...

Data transfer succeeded.
#
```

1. Enter the password stored on the remote server for the user account `staff`.

Figure 6-54: Example of backing up the running configuration

```
> enable
# copy running-config ftp://staff@[2001:db8::1]/backup.cnf
Are you sure you want to copy the configuration file to ftp://staff@[2001:db8::1]/
backup.cnf? (y/n): y

Authentication for 2001:db8::1.
User: staff
Password: xxx                                <-1
transferring...

Data transfer succeeded.
#
```

1. Enter the password stored on the remote server for the user account `staff`.

6.4.2 Copying backup configuration files to the Device

Use the `copy` operation command to apply the backup configuration file to the startup configuration. The following figure shows an application example.

Figure 6-55: Example of applying a backup configuration file to the startup configuration

```
> enable
# copy ftp://staff@[2001:db8::1]/backup.cnf startup-config
User account information is set in the configuration file.
The home directory of any deleted users will be deleted.
Are you sure you want to copy the configuration file to startup-config? (y/n): y
```

```

Authentication for 2001:db8::1.
User: staff
Password: xxx
transferring...
Data transfer succeeded.
#

```

1. Enter the password stored on the remote server for the user account `staff`.

6.4.3 Transferring files using the ftp command

Use the `ftp` command to transfer files between the Device and a remote operation terminal.

(1) Transferring a backup configuration file to the Device

After transferring the backup configuration file to your home directory on a Device (`/usr/home/operator`), copy it to the startup configuration by using the `copy` operation command. The following figure shows an example of transferring a backup configuration file to the Device by using the `ftp` command.

Figure 6-56: Example of transferring a backup configuration file to the Device (ftp command)

```

> cd /usr/home/operator
> ftp 192.0.2.1
Connect to 192.0.2.1.
220 FTP server (Version wn-2.4(4) Wed Jan 1 12:00:00 JST 20XX) ready.
Name (192.0.2.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> get backup.cnf
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodbye
> enable
# copy /usr/home/operator/backup.cnf startup-config
User account information is set in the configuration file.
The home directory of any deleted users will be deleted.
Are you sure you want to copy the configuration file to startup-config? (y/n): y
#

```

1. Transfer the backup configuration file.
2. Copy the backup configuration file (`backup.cnf`) to the startup configuration.
3. A confirmation message asking whether you want to replace the existing startup configuration appears.

(2) Transferring a backup configuration file to a remote operation terminal

The following figure shows an example of transferring a backup configuration file stored in the Device to a remote operation terminal.

Figure 6-57: Example of transferring a backup configuration file to a remote operation terminal

```

> cd /usr/home/operator
> enable

```

```

# copy running-config backup.cnf                                <-1
Are you sure you want to copy the configuration file to /usr/home/operator/
backup.cnf? (y/n): y
# exit
> ftp 192.0.2.1
Connect to 192.0.2.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 12:00:00 JST 20XX) ready.
Name (192.0.2.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> put backup.cnf                                            <-2
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodbye
>

```

1. Copy the running configuration to the backup configuration file.
2. Transfer the backup configuration file.

6.4.4 Transferring files using a memory card

Use the `cp` command to transfer files to a memory card.

(1) Transferring a backup configuration file to the Device

After transferring the backup configuration file from a memory card to your home directory (`/usr/home/operator`), copy it to the startup configuration by using the `copy` operation command. The following figure shows an example of transferring a backup configuration file to the Device by using the `cp` command.

Figure 6-58: Example of transferring a backup configuration file on a memory card to the Device (cp command)

```

> cd /usr/home/operator
> cp mc-file backup.cnf backup.cnf                                <-1
> enable
# copy /usr/home/operator/backup.cnf startup-config              <-2
User account information is set in the configuration file.
The home directory of any deleted users will be deleted.
Are you sure you want to copy the configuration file to startup-config? (y/n): y
                                                                    <-3
#

```

1. Transfer the backup configuration file from the memory card.
2. Copy the backup configuration file (`backup.cnf`) to the startup configuration.
3. A confirmation message asking whether you want to replace the existing startup configuration appears.

(2) Transferring a backup configuration file to a memory card

The following figure shows an example of transferring a backup configuration file stored in the Device to a memory card.

Figure 6-59: Example of transferring a backup configuration file to a memory card

```

> cd /usr/home/operator
> enable
# copy running-config backup.cnf                                <-1

```

```
Are you sure you want to copy the configuration file to /usr/home/operator/  
backup.cnf? (y/n): y  
# exit  
> cp backup.cnf mc-file backup.cnf                                <-2  
>
```

1. Copy the running configuration to the backup configuration file.
2. Transfer the backup configuration file to the memory card.

Chapter

7. Remote Login

This chapter describes remote access to the Device from a remote operation terminal.

- 7.1 Description
- 7.2 Configuration
- 7.3 Operation

7.1 Description

7.1.1 Connecting to the management port

This subsection describes the management port.

(1) Management port functional specifications

The management port provides an interface for connecting to a remote operation terminal. The following table describes the functional specifications of the management port.

Table 7-1: Management port functional specifications

Functionality	Specifications
Interface type	10BASE-T, 100BASE-TX, and 1000BASE-T
Auto-negotiation	Supported
AUTO-MDI/MDI-X	Supported
MAC and LLC sublayer control frames	Ethernet V2 format
Supported protocol	IPv4 and IPv6

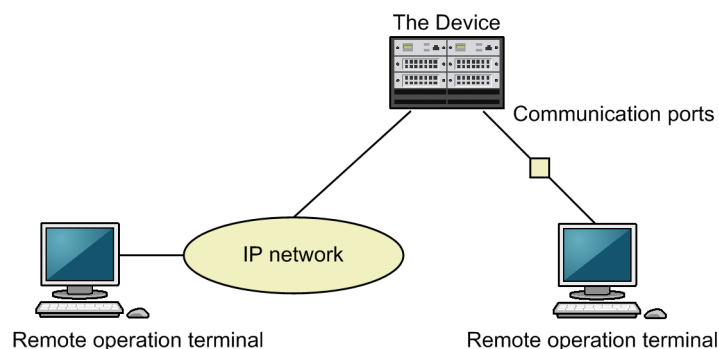
(2) Notes on using the management port

The management port is an interface mainly intended for remote operation. You can communicate from the management port through a NIF, but we do not recommend this operation.

7.1.2 Connecting to the communication port

To log in to the Device from a remote terminal via the communication port, you must first configure the connection in the Device, including setting its IP address. At initial deployment, no IP addresses or other settings are defined. Log in from the console to set up the connection.

Figure 7-1: Login to the Device from a remote operation terminal



7.1.3 Dial-up IP connection

This subsection describes how to connect a remote operation terminal to the serial connection port (AUX) via a dial-up IP connection.

(1) Setting the Device

(a) Preparing the modem

Configure the modem to answer automatically. Use straight cables to connect to the modem, or connect the modem to an AT-compatible machine. The Device cannot be used to configure the modem, so to specify these settings, use the PC to which the modem is connected.

Referring to the documentation included with the modem, use AT commands to configure the modem as specified in the table below. If the modem supports extended AT commands, the commands to be used might differ from those shown in the examples below.

Table 7-2: Modem settings

Configuration items	Description	Example (Hayes-compatible AT commands used)
CD signal state	The CD signal is usually set to off. It switches on when the modem receives a carrier from the remote modem.	AT&C1
DTR signal state	The modem is initialized when the DTR signal changes from on to off.	AT&D3
Command echo	No command entered is output to the DTE.	ATE0
Flow control	Flow control between the DTE and DCE is configured. <ul style="list-style-type: none"> • Enable RTS-CTS flow control. • Disable XON-XOFF flow control. 	AT&K3
Result code	No result code is output to the DTE.	ATQ1
Automatic answering	The number of rings is specified before answering automatically.	ATS0=2
Setting at reset	The settings are loaded from the modem's non-volatile memory.	AT&Y0
Save settings	The settings are saved in the modem's non-volatile memory.	AT&W0

If command echo is set so that no command is output to the DTE, no character appears when a command is entered. When the modem configuration is complete, save the settings in the modem. After saving the settings, display and check them.

Example: Using a Hayes-compatible AT command to configure a modem to answer automatically

```
AT&F&C1&D3E0&K3Q1S0=2&W0&Y0&V
```

Serial connection (with a modem) uses communication software to dial numbers. For details about dialing, see the appropriate documentation included with the communication software you are using. You can use AT commands from a terminal to dial numbers. If the communication software you are using does not have dialing capability, use appropriate AT commands to dial numbers. For details about how to dial numbers by using AT commands, see the documentation for the modem.

Examples: Using Hayes-compatible AT commands for dialing numbers

- Using a public line to tone dial 123-4567

```
AT&FE0&S1S0=0S2=255TD123-4567
```

- Using a PBX to tone dial 123-4567

```
AT&FX3E0&S1S0=0S2=255TD123-4567
```

- Using a PBX to tone dial 0, wait for a few seconds, and then dial 123-4567

```
AT&FX3E0&S1S0=0S2=255TD0,123-4567
```

Connect the configured modem to the AUX port of the Device.

(b) Configuration settings

Set the IP addresses used by the Device and remote operation terminal. The interface to be configured is `async`.

The command examples in the figure below assume that the IP address used by the Device is

10.0.0.1 and the one used by the remote operation terminal is 10.0.0.2.

Figure 7-2: Example of setting a configuration relating to async

```
(config)# interface async 1
(config-if)# ip address 10.0.0.1 255.255.255.0
(config-if)# peer default ip address 10.0.0.2
```

(2) Setting the remote operation terminal

(a) Preparing the modem

For details about how to set the modem to use it on the operation terminal connected to the Device via a dial-up IP connection, see the documentation for the modem.

(b) Setting the connection software

Install software for dial-up IP connections on the operation terminal to be connected to the Device via a dial-up IP connection, and then configure the terminal as shown in the following table.

Table 7-3: Dial-up IP connection settings

Configuration items	Description
Server type	PPP
Internet protocol (TCP/IP)	TCP/IP
IP address	Obtains the IP address automatically.
DNS server address	Obtains the address of the DNS server automatically.
Authentication method	Does not encrypt passwords (PAP).
Phone number	Phone number used by the modem that is to be connected to the Device

(c) User name and password for authentication

As the user name and password used for authentication of the dial-up IP connection, use the user name and password used to log in to the Device. Note that if authentication is performed based on a user name with no password, the entered password is ignored.

(3) Line connection and login

(a) Line connection

Use the connection software to dial.

(b) Checking the connection

If the dial-up IP connection is successfully established, an IP address is assigned. You can use the `ping` command or similar to check whether it is possible to communicate with the destination address.

If the `show sessions` command is used on the Device while a dial-up IP connection is correctly performed, the user is displayed as if the user logged in from the AUX port and the IP address used by the operation terminal is also displayed.

Figure 7-3: Example of executing the show sessions command

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
gilbert console ----- 0 Jan 6 14:16
john aux ----- 1 Jan 6 14:16 (ppp0:10.0.0.1) <-1
```

1. Make sure that `aux` is displayed. The IP address (10.0.0.1) assigned to the operation terminal is also displayed.

(c) Login

You can now use the remote operation terminal (for remote login).

(4) Line disconnection

A dial-up IP connection is disconnected when one of the following events occurs:

- A disconnection request is issued from the operation terminal
- The user[#] is forced to log out by the `killuser` command from another logged-in user.
- Line failure
- A command related to the `interface async` configuration command is changed or deleted.

#

This is the user logging in via the AUX port.

Notes

If a dial-up IP connection is disconnected, it might take some time before you can reconnect. In such a case, wait 300 seconds or so before trying to reconnect.

7.2 Configuration

7.2.1 List of configuration commands

The following table describes the configuration commands for the management port.

Table 7-4: List of configuration commands

Command name	Description
description	Sets supplementary information.
duplex	Sets duplex for the management port.
interface mgmt	Specifies the configuration of the management port.
ip routing	Enables or disables IPv4 Layer 3 forwarding in the management port.
ipv6 routing	Enables or disables IPv6 Layer 3 forwarding in the management port.
shutdown	Places the management port in the shutdown state.
speed	Sets the line speed of a management port.
ip address ^{#1}	Specifies the IPv4 address of the management port.
ipv6 address ^{#2}	Specifies the IPv6 address of the management port.
ipv6 enable ^{#2}	Enables the IPv6 functionality of the management port. This command automatically creates a link-local address.

#1

See 2. *IPv4, ARP, and ICMP* in the manual *Configuration Command Reference Vol. 3 For Version 12.1*.

#2

See 3. *IPv6, NDP, and ICMPv6* in the manual *Configuration Command Reference Vol. 3 For Version 12.1*.

The following table describes the configuration commands relating to connection and remote operation for an operation terminal.

Table 7-5: List of configuration commands

Command name	Description
ftp-server	Permits access from remote operation terminals using FTP.
line console	Sets parameters for the console (RS232C).
line vty	Permits Telnet remote access to a device.
speed	Sets the communication speed of the console (RS232C).
transport input	Regulates access from a remote operation terminal using the various protocols.

For the configuration commands related to setting up IPv4 and IPv6 interfaces, see 2. *Settings and Operation for IP, ARP, and ICMP* in the manual *Configuration Guide Vol. 3 For Version 12.1* or 4. *Settings and Operation for IPv6, NDP, and ICMPv6* in the manual *Configuration Guide Vol. 3 For Version 12.1*.

7.2.2 Configuring the management port

(1) Shutting down the management port

Points to note

Configuring the management port might require you to execute multiple commands. In such a case, if the management port enters a link-up state before the configuration is complete, the Device cannot communicate as expected. Therefore, we recommend that you shut down the management port first, and then after the configuration is complete, exit the management port from the shutdown state.

Command examples

1. **(config)# interface mgmt 0**
Specifies that the management port is to be configured.
2. **(config-if)# shutdown**
Shuts down the management port.
3. **(config-if)# *******
Specifies a configuration for the management port.
4. **(config-if)# no shutdown**
Exits the management port from the shutdown state.

Related information

To stop operation of the management port, you can use the `inactivate` operation command. If the `inactivate` command is used to set the management port to an inactive state and then the Device is restarted, the management port enters an active state. If the management port is shut down, it remains in a disabled state even if the Device is restarted. To activate the management port, set `no shutdown` in the configuration to exit the port from the shutdown state.

(2) Specifying an IPv4 address

Points to note

The example below shows how to specify an IPv4 address in the management port. To specify an IPv4 address, you need to switch to interface configuration command mode.

Command examples

1. **(config)# interface mgmt 0**
Switches the management port to interface configuration command mode.
2. **(config-if)# ip address 192.168.1.1 255.255.255.0**
Sets the IPv4 address 192.168.1.1 and the subnet mask 255.255.255.0 for the management port.

(3) Specifying an IPv6 address

Points to note

The example below shows how to specify an IPv6 address in the management port. Use the `ipv6 enable` command to enable the IPv6 functionality. If the `ipv6 enable` command is not set, IPv6 configuration is not enabled.

Command examples

1. **(config)# interface mgmt 0**

Switches the management port to interface configuration command mode.

2. **(config-if)# ipv6 enable**

Allows the use of an IPv6 address for the management port.

3. **(config-if)# ipv6 address 2001:db8::1/64**

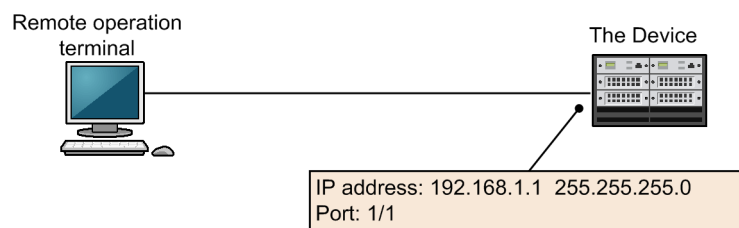
Sets the IPv6 address 2001:db8::1 and the prefix length 64 for the management port.

7.2.3 Assigning an IP address to the Device

Points to note

To access the Device from a remote operation terminal, you must first set an IP address in the interface that the terminal connects to.

Figure 7-4: Example of connecting with a remote operation terminal



Command examples

1. **(config)# interface gigabitethernet 1/1**

Switches to the configuration command mode for port 1/1.

2. **(config-if)# ip address 192.168.1.1 255.255.255.0**

(config-if)# exit

Sets the IPv4 address 192.168.1.1 and the subnet mask 255.255.255.0 for the port 1/1 Ethernet interface.

7.2.4 Permitting login by using the Telnet protocol

Points to note

The device's IP address must be assigned before you can use this procedure.

Set the `line vty` configuration command that allows remote login to the Device via the Telnet protocol.

If remote login has not been configured, you can log in only from the console.

Command examples

1. `(config)# line vty 0 2`
`(config-line)#`

Permits remote access to the Device from a remote operation terminal by using the Telnet protocol. Also, limits the number of concurrent remote logins to a maximum of three users.

7.2.5 Permitting login by using FTP

Points to note

The device's IP address must be assigned before you can use this procedure.

Set the `ftp-server` configuration command that allows remote access to the Device from a remote operation terminal via FTP.

If this configuration is not set, users cannot access the Device by using FTP.

Command examples

1. `(config)# ftp-server`

Permits remote access to the Device from a remote operation terminal by using FTP.

7.2.6 Permitting login from VRFs by using the Telnet protocol

(1) Permitting users to log in from all VRFs including the global network via Telnet

Points to note

To permit access from all VRFs, set the `vrf all` parameter of the `transport input` configuration command. If this `vrf all` parameter is not set, only access from the global network is allowed.

Command examples

1. `(config)# line vty 0 2`
`(config-line)#`

Permits remote access to the Device from a remote operation terminal by using the Telnet protocol. Also, limits the number of concurrent remote logins to a maximum of three users.

2. `(config-line)# transport input vrf all telnet`
`(config-line)#`

Permits remote access to the Device from remote operation terminals on all VRFs including the global access via the Telnet protocol.

(2) Permitting login from a specified VRF by using the Telnet protocol

Points to note

To permit access from a specified VRF, set the VRF ID to the `vrf` parameter of the `transport input` configuration command. If this `vrf` parameter is not set, only access from the global network is allowed.

Command examples

1. `(config)# line vty 0 2`
`(config-line)#`

Permits remote access to the Device from a remote operation terminal by using the Telnet protocol. Also, limits the number of concurrent remote logins to a maximum of three users.

2. **(config-line)# transport input vrf 2 telnet**
(config-line)#

On VRF2, permits remote access to the Device from a remote operation terminal via the Telnet protocol. The global network is excluded.

7.2.7 Permitting login from VRFs by using FTP

(1) Permitting users to log in from all VRFs including the global network via FTP

Points to note

To permit access from all VRFs, set the `vrf all` parameter of the `ftp-server` configuration command. If this `vrf all` parameter is not set, only access from the global network is allowed.

Command examples

1. **(config)# ftp-server vrf all**

Permits remote access to the Device from remote operation terminals on all VRFs including global access via FTP.

(2) Permitting login from a specified VRF by using FTP

Points to note

To permit access from a specific VRF, set the VRF ID to the `vrf` parameter of the `ftp-server` configuration command. If this `vrf` parameter is not set, only access from the global network is allowed.

Command examples

1. **(config)# ftp-server vrf 2**

On VRF2, permits remote access to the Device from a remote operation terminal via FTP. The global network is excluded.

7.3 Operation

7.3.1 List of operation commands

The following table describes the operation commands for the management port.

Table 7-6: List of operation commands

Command name	Description
show ip interface ^{#1}	Shows the status of IPv4 interfaces.
show ip arp ^{#1}	Shows the information in the ARP entries.
clear arp-cache ^{#1}	Deletes dynamic ARP information.
clear ip duplicate-address ^{#1}	Removes the suppressed state of communication for the address whose duplication was detected by Address Conflict Detection.
ping ^{#1}	Performs an IPv4 echo test.
show ipv6 interface ^{#2}	Shows the status of the IPv6 interface.
show ipv6 neighbors ^{#2}	Shows NDP information.
clear ipv6 neighbors ^{#2}	Clears dynamic NDP information.
clear ipv6 duplicate-address ^{#2}	Removes the suppressed state of communication for the address whose duplication was detected by Duplicate Address Detection.
ping ipv6 ^{#2}	Performs an ICMPv6 echo test.

#1

See 2. *IPv4, ARP, and ICMP* in the manual *Operation Command Reference Vol. 3 For Version 12.1*.

#2

See 3. *IPv6, NDP, and ICMPv6* in the manual *Operation Command Reference Vol. 3 For Version 12.1*.

The following table describes the operation commands relating to connection and remote operation for an operation terminal.

Table 7-7: List of operation commands

Command name	Description
set exec-timeout	Specifies the length of time until the user is automatically logged out.
set terminal help	Selects the type of command help messages to be displayed.
set terminal pager	Enables or disables paging.
show history	Shows a log of operation commands executed in the past. (No log is displayed for configuration commands.)
telnet	Connects a virtual terminal via Telnet to the remote operation terminal that has the specified IP address.
ftp	Transfers files between the Device and a remote terminal connected by using TCP/IP.
tftp	Transfers files between the Device and a remote terminal connected by using UDP.

7.3.2 Checking communication between a remote operation terminal and the Device

You can check that the Device and remote operation terminal are communicating by using the `ping` or `ping ipv6` operation command. For details see 2. *Settings and Operation for IP, ARP, and ICMP* in the manual *Configuration Guide Vol. 3 For Version 12.1* or 4. *Settings and Operation for IPv6, NDP, and ICMPv6* in the manual *Configuration Guide Vol. 3 For Version 12.1*.

Chapter

8. Login Security and RADIUS or TACACS+

This chapter describes login control, login security, accounting, and RADIUS and TACACS+ application functionality in the Device.

- 8.1 Configuring login security
- 8.2 Description of RADIUS and TACACS+
- 8.3 RADIUS and TACACS+ configurations

8.1 Configuring login security

8.1.1 Lists of configuration commands and operation commands

The following table describes the configuration commands for login security.

Table 8-1: List of configuration commands

Command name	Description
aaa authentication enable	Specifies the authentication method to be used when changing to administrator mode (by the <code>enable</code> command).
aaa authentication enable attribute-user-per-method	Changes the user name attributes used in authentication when changing to administrator mode (by the <code>enable</code> command).
aaa authentication enable end-by-reject	Terminates authentication if an attempt to change to administrator mode (by the <code>enable</code> command) is denied.
aaa authentication login	Specifies the authentication method to be used at remote login.
aaa authentication login console	Applies the authentication method specified by the <code>aaa authentication login</code> command when the user logs in from the console (RS232C) and the AUX port.
aaa authentication login end-by-reject	Terminates authentication if login authentication is denied.
aaa authorization commands	Specifies that command authorization is to be performed by a RADIUS or TACACS+ server.
aaa authorization commands console	Applies the command authorization specified by the <code>aaa authorization commands</code> command when the user logs in from the console (RS232C) and the AUX port.
banner	Defines the messages to be displayed before and after the user logs in.
commands exec	Adds a command string to a command list used when local (configuration-based) command authorization is enabled.
enable password	Sets the password to be used for changing to administrator mode (by the <code>enable</code> command).
ip access-group	Sets an access list that specifies the IPv4 addresses of remote operation terminals for which remote login to the Device is permitted or denied.
ipv6 access-class	Sets an access list that specifies the IPv6 addresses of remote operation terminals for which remote login to the Device is permitted or denied.
parser view	Generates a command list used when local (configuration-based) command authorization is enabled.
username	Creates a user account to log in to the Device and sets a password for the user account. Sets for a specified user a command list or command class used in local (configuration-based) command authorization.

The following table describes the operation commands for login security.

Table 8-2: List of operation commands

Command name	Description
show users	Shows the user account set by the <code>username</code> configuration command.
make hidden-password	Creates a hashed password string to be set to the <code>username</code> and <code>enable password</code> configuration commands.

Command name	Description
show sessions (who)	Shows the users currently logged in to the Device.
show whoami (who am i)	Shows only the user, logged in to the Device, who executed this command.
killuser	Forcibly logs out a login user.

8.1.2 Overview of login control

The Device supports local login via a serial connection, and remote login using Telnet over an IPv4 or IPv6 network.

The following controls are implemented in the Device when a user logs in and during a user session:

1. To prevent unauthorized access, a password check is performed at login, and restrictions based on the user ID are placed on the range of commands that the user can execute.
2. Multiple terminals can log in to a Device concurrently.
3. The maximum number of users who can log in concurrently is 16. You can reduce this limit by using the `line vty` configuration command.
4. You can limit the IPv4 and IPv6 addresses permitted to access the Device by using the `ip access-list standard`, `ipv6 access-list`, `ip access-group`, and `ipv6 access-class` configuration commands.
5. You can limit the protocols used to access the Device (Telnet and FTP) by using the `transport input` and `ftp-server` configuration commands.
6. You can limit the IPv4 and IPv6 addresses permitted to access the Device in a VRF configuration by using the `ip access-list standard`, `ipv6 access-list`, `ip access-group`, and `ipv6 access-class` configuration commands.
7. You can limit the protocols (Telnet and FTP) used to access the Device in a VRF configuration by using the `transport input` and `ftp-server` configuration commands.
8. Command execution results appear only on the terminal where the command was executed. Operation messages appear on all login terminals.
9. Entered commands, response messages, and operation messages are recorded as an operation log. The operation log can be viewed by using the `show logging operation` command.
10. The user is automatically logged out if there is no key input for a specified period (default: 60 minutes).
11. You can forcibly log out a user using the `killuser` operation command.

8.1.3 Creating and deleting a login user

To create a user account for logging in to the Device, use the `username` configuration command. The following figure shows an example.

Figure 8-1: Creating a user named newuser (entering a password)

```
(config)# username newuser password input
New password:***** <-1
Retype new password:***** <-2
(config)#
```

1. Enter the user's password (the actual input characters are not shown).
2. Enter the user's password again for confirmation (the actual input characters are not shown).

The entered password is automatically hashed and set to the configuration. If you press the **Enter**

key without entering any password, a login user with no password is created.

When creating a login user, you can also specify a hashed password created by using the `make hidden-password` operation command. The following figure shows an example of creating a login user by specifying a hashed password.

Figure 8-2: Creating a user named newstaff (specifying a hashed password)

```
> make hidden-password                                <-1
Input password:*****                                <-2
Retype password:*****                                <-3

A password was created. Set it in the configuration.
"$6$pRo7aJE ... 3ewCiDAwB1"                            <-4
> enable
# configure
(config)# username newstaff password hidden "$6$pRo7aJE ... 3ewCiDAwB1" <-5
(config)#
```

1. Execute the `make hidden-password` operation command.
2. Enter the user's password (the actual input characters are not shown).
3. Enter the user's password again for confirmation (the actual input characters are not shown).
4. A hashed password string is created.
5. Specify the hashed password string created by using the `make hidden-password` command.

If you specify double quotation marks (") after `hidden`, a login user with no password is created.

You can use the `show users` operation command to check the created login user.

Delete login users that are not used anymore from the configuration. The following figure shows an example of deleting a login user.

Figure 8-3: Deleting the user newuser

```
(config)# no username newuser
Do you want to delete the user account newuser? (y/n): y    <-1
(config)#
```

1. If you enter `y`, the specified login user is deleted.

If you do not intend to use the pre-defined login user (`username operator 100 password hidden ""`), to prevent any security risk, we recommend that you delete that account after you create a new login user.

If a login user is deleted, that user's home directory is also deleted. Therefore, save the files you want to keep into the `/usr/home/share` directory or create a backup copy of them externally before deleting the login user. Note that any user can write and read files in the `/usr/home/share` directory. Be careful about file management.

Also, by using the `aaa authentication login` configuration command, you can implement RADIUS or TACACS+ authentication. For details about configuration setting examples, see [8.3.2 Configuring RADIUS authentication](#) and [8.3.3 Configuring TACACS+ authentication](#).

8.1.4 Configuring and changing a login user's password

To set or change a login user's password, use the `username` configuration command. The following figure shows a password setting example.

Figure 8-4: Setting and changing a password for the user newuser (entering a password)

```
(config)# username newuser password input
New password:*****                                     <-1
Retype new password:*****                               <-2
(config)#
```


1. Enter the user's password (the actual input characters are not shown).
2. Enter the user's password again for confirmation (the actual input characters are not shown).

The entered password is automatically hashed and set to the configuration. If you press the **Enter** key without entering any password, a login user with no password is created.

When setting or changing the password, you can also specify a hashed password created by using the `make hidden-password` operation command. The following figure shows an example of setting a password by specifying a hashed password.

Figure 8-5: Setting and changing a password for the user newstaff (specifying a hashed password)

```
> make hidden-password                                <-1
Input password:*****                                <-2
Retype password:*****                                <-3

A password was created. Set it in the configuration.
"$6$pRo7aJE ... 3ewCiDAwB1"                            <-4
> enable
# configure
(config)# username newstaff password hidden "$6$pRo7aJE ... 3ewCiDAwB1" <-5
(config)#
```

1. Execute the `make hidden-password` operation command.
2. Enter the user's password (the actual input characters are not shown).
3. Enter the user's password again for confirmation (the actual input characters are not shown).
4. A hashed password string is created.
5. Specify the hashed password string created by using the `make hidden-password` command.

If double quotation marks (") are specified after `hidden`, a login user with no password is created.

8.1.5 Configuring and changing a password for switching to administrator mode

To execute configuration commands, you must switch to administrator mode by using the `enable` command. Because the Device has no pre-defined passwords, executing the `enable` command at first deployment will place you in administrator mode without authentication.

However, from the viewpoint of security, we do not recommend that every user be allowed to change to administrator mode without password authentication in normal operation. Thus, set and change a password for changing to administrator mode by using the `enable password` configuration command. The following figure shows a password setting example.

Figure 8-6: Setting and changing a password for switching to administrator mode (entering a password)

```
(config)# enable password input
New password:*****                                <-1
Retype new password:*****                            <-2
(config)#
```

1. Enter the user's password (the actual input characters are not shown).
2. Enter the user's password again for confirmation (the actual input characters are not shown).

The entered password is automatically hashed and set to the configuration. If you press the **Enter** key without entering any password, no password is required.

When setting or changing the password, you can also specify a hashed password created by using

the `make hidden-password` operation command. The following figure shows an example of setting a password by specifying a hashed password.

Figure 8-7: Setting and changing a password for switching to administrator mode (specifying a hashed password)

```
> make hidden-password                                <-1
Input password:*****                                <-2
Retype password:*****                               <-3

A password was created. Set it in the configuration.
"$6$pRo7aJE ... 3ewCiDAwB1"                          <-4
> enable
# configure
(config)# enable password hidden "$6$pRo7aJE ... 3ewCiDAwB1" <-5
(config)#
```

1. Execute the `make hidden-password` operation command.
2. Enter the user's password (the actual input characters are not shown).
3. Enter the user's password again for confirmation (the actual input characters are not shown).
4. A hashed password string is created.
5. Specify the hashed password string created by using the `make hidden-password` command.

Using the `aaa authentication enable` configuration command, you can implement authentication using a RADIUS or TACACS+ server. For details about configuration setting examples, see 8.3.2 *Configuring RADIUS authentication* and 8.3.3 *Configuring TACACS+ authentication*.

8.1.6 Permitting login from a remote operation terminal

Using the `line vty` configuration command, you can enable login to the Device from a remote operation terminal. If remote login has not been configured, you can log in only from the console. The following figure shows an example of configuring permission for login from a remote operation terminal.

Figure 8-8: Example of configuring permission for login from a remote operation terminal

```
(config)# line vty 0 2
(config-line)#
```

To permit access to the Device from a remote operation terminal using FTP, you must set the `ftp-server` configuration command. If you omit this setting, users cannot access the Device by FTP.

Figure 8-9: Example of configuring permission for FTP access

```
(config)# ftp-server
(config)#
```

8.1.7 Configuring the maximum number of concurrent users

Using the `line vty` configuration command, you can enable login to the Device from a remote operation terminal. The value of the `<num>` parameter of the `line vty` command limits the number of remote users who can log in concurrently. Regardless of this setting, login from the console is always possible. The following setting example allows no more than two users to be logged in concurrently.

Figure 8-10: Example of setting the maximum number of concurrent users

```
(config)# line vty 0 1
(config-line)#
```

Device behavior in regard to concurrent users is as follows:

- Multiple users attempting to log in at the same time might not succeed, even if the number of concurrent users is equal to or less than the maximum.
- If you change the maximum number of concurrent users, current user sessions will not be terminated.

8.1.8 Configuring the IP addresses of remote operation terminals permitted to log in

By setting their IP addresses, you can specify which remote operation terminals are allowed to log in to the Device. After configuring settings, check whether other remote operation terminals are denied login to the Device.

Points to note

To permit access to the Device from only specified remote operation terminals, you must register their IP addresses in advance using the `ip access-list standard`, `ipv6 access-list`, `ip access-group`, or `ipv6 access-class` configuration command. You can register a maximum of 128 IPv4 addresses and subnet masks, or IPv6 addresses and prefixes. If you omit this setup, all remote operation terminals will be able to access the Device. If access is attempted from a terminal that does not have access permission (a terminal not registered in the configuration entry), the message with message type ACCESS and message ID 06000001 indicating the access attempt will appear on other login terminals. If you change the IP addresses that are permitted to access, current user sessions will not be terminated.

Command examples (IPv4)

1.

```
(config)# ip access-list standard REMOTE
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit
```

Sets an access list (REMOTE) that permits login only from the network IP address 192.168.0.0/24.

2.

```
(config)# line vty 0 2
(config-line)# ip access-group REMOTE in
(config-line)#
```

Moves to line mode, applies the access list REMOTE, and permits login only from the network IP address 192.168.0.0/24.

Command examples (IPv6)

1.

```
(config)# ipv6 access-list REMOTE6
(config-ipv6-nacl)# permit ipv6 2001:db8:811:ff01::/64 any
(config-ipv6-nacl)# exit
```

Sets an access list (REMOTE6) that permits login only from the network IP address 2001:db8:811:ff01::/64.

2.

```
(config)# line vty 0 2
(config-line)# ipv6 access-class REMOTE6 in
(config-line)#
```

Moves to line mode, applies the access list `REMOTE6`, and permits login only from the network IP address `2001:db8:811::ff01::/64`.

8.1.9 Configuring login banners

By setting login banners with the `banner` configuration command, you can display messages before and after a user logs in to the Device from the console, or from a Telnet or FTP client running on a remote operation terminal.

Points to note

The following pre-login message can be presented when a Telnet or FTP client running on a remote operation terminal connects to the Device over the network:

```
#####
Only Administrators can connect.
The Administrator's phone number is xxx-xxxx-xxxx.
#####
```

Command examples

- ```
1. (config)# banner login plain-text
```

```
--- Press CTRL+D or only '.' line to end ---
```

#####

Only Administrators can connect.

The Administrator's phone number is xxx-xxxx-xxxx.

#####

•

Enter the pre-login screen message.

After typing the message, enter a line containing a period (.) only, or press the **Ctrl + D** keys.

2. (config)# show banner

**banner login encode**[illegible]

The message you entered is encoded automatically.

- ```
3. (config)# show banner login plain-text
```

#####

Only Administrators can connect.

The Administrator's phone number is xxx-xxxx-xxxx.

#####

```
(config)#
```

To check the banner message in text format, specify the `plain-text` parameter in the `show banner login` command.

When you finish setting the login banner, connect to the Device from the Telnet or FTP client of a remote terminal. After a connection is established, a message appears on the client.

Figure 8-11: Example of connecting to the Device from a remote operation terminal (connecting through Telnet)

```
> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

#####
Only Administrators can connect.
The Administrator's phone number is xxx-xxxx-xxxx.
#####
login:
```

Figure 8-12: Example of connecting to the Device from a remote operation terminal (connecting through FTP)

```
> ftp 10.10.10.10
Connected to 10.10.10.10.
220-
#####
Only Administrators can connect.
The Administrator's phone number is xxx-xxxx-xxxx.
#####
220 10.10.10.10 FTP server ready.
Name (10.10.10.10:staff):
```

8.1.10 Permitting login from a remote operation terminal when using VRF

Using the `line vty` configuration command, you can enable login to the Device from a remote operation terminal. Set the `vrf` parameter of the `transport input` configuration command to permit access from VRFs. If this `vrf` parameter is not set, only access from the global network is allowed.

The following figure shows how to permit remote access to the Device from remote operation terminals on all VRFs including the global access via the Telnet protocol.

Figure 8-13: Setting example of permitting login from remote operation terminals on all VRFs including the global network

```
(config)# line vty 0 2
(config-line)# transport input vrf all telnet
(config-line)#
```

The figure below shows how to permit remote access to the Device from remote operation terminals on a specified VRF via the Telnet protocol. The global network is excluded.

Figure 8-14: Setting example of permitting login from remote operation terminals on VRF 2

```
(config)# line vty 0 2
(config-line)# transport input vrf 2 telnet
(config-line)#
```

To permit access to the Device from a remote operation terminal using FTP, you must set the `ftp-server` configuration command. To permit access from VRFs, set the `vrf` parameter. If this `vrf` parameter is not set, only access from the global network is allowed.

The following figure shows how to permit remote access to the Device from remote operation terminals on all VRFs including the global access via FTP.

Figure 8-15: Setting example of permitting access from remote operation terminals on all VRFs including the global network via FTP

```
(config)# ftp-server vrf all
(config)#
```

The figure below shows how to permit remote access to the Device from remote operation terminals on a specified VRF via FTP. The global network is excluded.

Figure 8-16: Setting example of permitting access from remote operation terminals on VRF 2 via FTP

```
(config)# ftp-server vrf 2
(config)#
```

8.1.11 Configuring the IP address that permits login from a remote operation terminal when using VRF

By setting their IP addresses in an access list, you can specify which remote operation terminals are allowed to log in to the Device.

As a rule, access lists are individually set to the global network and each VRF. An access list can also be set to all VRFs including the global network. Although these configurations can be used in combination, the last access list is implicitly discarded when using multiple access lists.

How access lists are applied to the access source VRFs (that is, the application range of access lists) depends on the relationship between the access sources and the locations where access lists are set. As an example, the following table describes how an applied access list will change depending on where access lists are set when the Device is accessed from the global network, VRF 10 and VRF 20. (Entries in parentheses show which access list is applied.)

Table 8-3: Application range of access lists

Access list location	Access source VRF		
	Global network	VRF 10	VRF 20
• global	(global)	--	--
• global • VRF 10	(global)	(VRF 10)	--
• global • VRF 10 • VRF ALL	(global) [#] After functionality applied (VRF ALL)	(VRF 10) [#] After functionality applied (VRF ALL)	(VRF ALL)

Legend

--: No access list is applied. Therefore, access is not restricted.

global: Global network

VRF 10: VRF 10

VRF ALL: All VRFs including the global network

#

Individually set access lists are applied with a higher priority than access lists set as VRF ALL. When using multiple access lists, individually set access lists will not be implicitly discarded. If no individually set access list satisfies the conditions, the access list set as VRF ALL is applied. If the access lists set as VRF ALL does not satisfy the conditions either, access is restricted due to the implicit discard.

After configuring settings, check whether other remote operation terminals are denied login to the

Device.

Points to note

Use an access list to permit access to the Device from specific remote operation terminals. To do so, you must register their IP addresses in advance by using the `ip access-list standard`, `ipv6 access-list`, `ip access-group`, and `ipv6 access-class` configuration commands. You can register a maximum of 128 IPv4 addresses and subnet masks, or IPv6 addresses and prefixes. If you omit this configuration, all remote operation terminals will be able to access the Device. If access is attempted from a terminal that does not have access permission (a terminal not registered in the configuration entry), the message with message type ACCESS and message ID 06000001 indicating the access attempt will appear on other login terminals.

A configuration example is shown below. First, restrict login from remote operation terminals on all VRFs including the global network. Next, permit login from the global network and specified VRFs. After this, login is permitted only from specified networks.

Command examples

1.

```
(config)# ip access-list standard REMOTE_VRFALL
(config-std-nacl)# deny any
(config-std-nacl)# exit
```

Set an access list (REMOTE_VRFALL) that is to be applied for all VRFs including the global network and restricts login to the Device.

2.

```
(config)# ip access-list standard REMOTE_GLOBAL
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit
```

Sets an access list (REMOTE_GLOBAL) that is to be applied for the global network and permits login only from the network 192.168.0.0/24.

3.

```
(config)# ip access-list standard REMOTE_VRF10
(config-std-nacl)# permit 10.10.10.0 0.0.0.255
(config-std-nacl)# exit
```

Sets an access list (REMOTE_VRF10) that is to be applied for VRF 10 and permits login only from the network 10.10.10.0/24.

4.

```
(config)# line vty 0 2
(config-line)# ip access-group REMOTE_VRFALL vrf all in
(config-line)# ip access-group REMOTE_GLOBAL in
(config-line)# ip access-group REMOTE_VRF10 vrf 10 in
(config-line)#
```

Moves to line mode, applies the access list REMOTE_VRFALL to all VRFs including the global network, the access list REMOTE_GLOBAL to the global network, and the access list REMOTE_VRF10 to VRF 10.

For the global network, login only from the remote operation terminals in the network 192.168.0.0/24 is permitted.

For VRF 10, login only from the remote operation terminals in the network 10.10.10.0/24 is permitted.

For the other VRFs, login to the Device is restricted.

8.2 Description of RADIUS and TACACS+

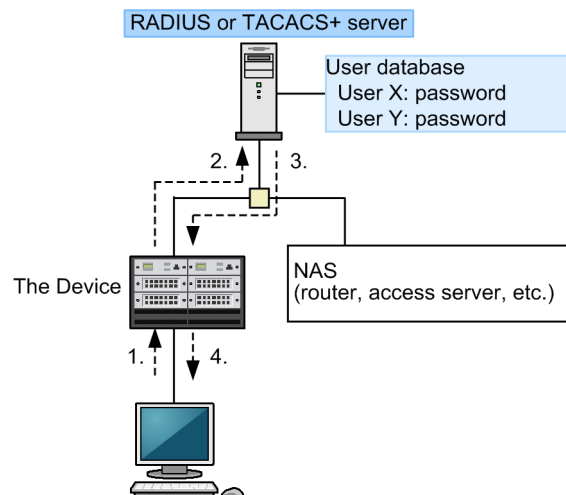
8.2.1 Overview of RADIUS and TACACS+

RADIUS (Remote Authentication Dial In User Service) and TACACS+ (Terminal Access Controller Access Control System Plus) are protocols that provide authentication, authorization, and accounting services to a Network Access Server (NAS). A NAS is a device such as a remote access server or router that acts as a RADIUS or TACACS+ client. A NAS device requests services such as user authentication, command authorization, and accounting from the configured RADIUS or TACACS+ server. The server responds to service requests based on the data in its management information database. The Device supports NAS functionality.

When RADIUS or TACACS+ is implemented, authentication information such as user passwords used by the NAS devices, command authorization information, and accounting information can be centrally managed by one RADIUS or TACACS+ server. The Device can request user authentication, authorization, and accounting services from a RADIUS or TACACS+ server.

The following figure shows the flow of RADIUS or TACACS+ authentication.

Figure 8-17: Flow of RADIUS or TACACS+ authentication



1. User X accesses the Device via Telnet from a remote operation terminal.
2. The Device requests authentication to the RADIUS or TACACS+ server specified by the configuration.
3. The RADIUS or TACACS+ server authenticates user X based on the user database and notifies the Device that user X has been authenticated.
4. The Device permits Telnet access from user X's remote operation terminal based on the RADIUS or TACACS+ authentication.

If command authorization is set in the configuration, the Device permits or restricts an operation command executed by the user according to the command list set in the RADIUS or TACACS+ server.

8.2.2 Scope of RADIUS or TACACS+ implementation

The Device uses RADIUS or TACACS+ for login authentication from an operation terminal, authentication when changing to administrator mode (by the `enable` command), command authorization, and accounting. The functionality supported by RADIUS and TACACS+ is listed below.

(1) Functionality supported by RADIUS and TACACS+

RADIUS or TACACS+ authentication can be used for the following operations:

- Telnet access from a remote operation terminal (IPv4/IPv6)
- FTP access from a remote operation terminal (IPv4/IPv6)
- Login from the console (RS232C) or the AUX port
- Transition to administrator mode (by the `enable` command)

RADIUS or TACACS+ command authorization can be used for the following operations:

- Telnet access from a remote operation terminal (IPv4/IPv6)
- Login from the console (RS232C) or the AUX port

RADIUS or TACACS+ accounting can be used for the following operations:

- Telnet login-logout from a remote operation terminal (IPv4/IPv6)
- FTP login-logout from a remote operation terminal (IPv4/IPv6)
- Login and logout from the console (RS232C) or the AUX port
- Command input using the CLI (supported only for TACACS+)
- Command input on the system operation panel (supported only for TACACS+)

(2) Scope of RADIUS implementation

The Device supports the following NAS functionality for communication with a RADIUS server:

Table 8-4: Scope of RADIUS support

Category	Description
Documentation	Limited to NAS-related functionality only.
Packet type	<p>Support for the following packet types used in login authentication, authentication when changing to administrator mode (by the <code>enable</code> command), and command authorization:</p> <ul style="list-style-type: none"> • Access-Request (send) • Access-Accept (receive) • Access-Reject (receive) <p>Support for the following accounting packet types:</p> <ul style="list-style-type: none"> • Accounting-Request (send) • Accounting-Response (receive)

Category	Description
Attribute	<p>Support for the following attributes used in login authentication and authentication when changing to administrator mode (by the <code>enable</code> command):</p> <ul style="list-style-type: none"> • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-IPv6-Address • NAS-Identifier • Reply-Message <p>Support for the following command authorization attributes:</p> <ul style="list-style-type: none"> • Class • Vendor-Specific (Vendor-ID = 21839) <p>Support for the following accounting attributes:</p> <ul style="list-style-type: none"> • User-Name • NAS-IP-Address • NAS-IPv6-Address • NAS-Port • NAS-Port-Type • Service-Type • Calling-Station-Id • Acct-Status-Type • Acct-Delay-Time • Acct-Session-Id • Acct-Authentic • Acct-Session-Time

(a) Description of supported RADIUS attributes

The table below describes the RADIUS attributes used in authentication, command authorization, and accounting.

To perform command authorization using a RADIUS server, you must set up the server in advance so that it returns a Class or Vendor-Specific attribute when a user is authenticated. Set vendor-specific attributes in a `dictionary` file or other configuration file to register them with the RADIUS server. For details about command authorization, see *8.2.4 RADIUS or TACACS+ and local command authorization*.

Table 8-5: Supported RADIUS attributes

Attribute name	Attribute value	Packet type	Description
User-Name	1	Access-Request Accounting-Request	The name of the user being authenticated. Sends the login user name when login authentication is performed. Following <i>Table 8-10: User name attributes to be set</i> sends the user name when authentication is performed to go into administrator mode (by the <code>enable</code> command).
User-Password	2	Access-Request	The password of the user being authenticated, sent in encrypted form
Service-Type	6	Access-Request Accounting-Request	Login (value = 1). Administrative (value = 6; used only for Access-Request packet type). Ignored when attached to Access-Accept or Access-Reject.

Attribute name	Attribute value	Packet type	Description
NAS-IP-Address	4	Access-Request Accounting-Request	The IP address of the Device. Indicates the local address if the local address is specified. Indicates the IP address of the requesting interface if the local address is not specified.
NAS-IPv6-Address	95	Access-Request Accounting-Request	The IPv6 address of the Device Indicates the local address if the local address is specified. Indicates the IPv6 address of the requesting interface if the local address is not specified. If communicating with IPv6 link-local addresses, the IPv6 link-local address of the requesting interface is set, regardless of the local address setting.
NAS-Identifier	32	Access-Request Accounting-Request	The device name of the Device. This is not attached if a device name was not set.
Reply-Message	18	Access-Accept Access-Reject Accounting-Response	A message from the server. Output as an operation log entry if attached.
Class	25	Access-Accept	The login class; used in command authorization.
Vendor-Specific	26	Access-Accept	A login list; used in command authorization.
NAS-Port	5	Accounting-Request	The port number of the NAS device to which the user is connected. The Device stores the tty port number, or 100 for FTP connection.
NAS-Port-Type	61	Accounting-Request	The method of connection to the NAS device. The Device stores <code>Virtual</code> (5) for access via Telnet and FTP, and <code>Async</code> (0) for access from the console and the AUX port connection.
Calling-Station-Id	31	Accounting-Request	The user's ID. The Device stores clients' IPv4 and IPv6 addresses for access via Telnet and FTP, <code>console</code> for access from the console, and <code>aux</code> for access from the AUX port.
Acct-Status-Type	40	Accounting-Request	The timing at which the Accounting-Request was sent. The Device stores <code>Start</code> (1) if sent at login, or <code>Stop</code> (2) if sent at logout.
Acct-Delay-Time	41	Accounting-Request	The length of time (in seconds) taken to send the Accounting-Request after an event requiring this attribute to be sent has occurred.
Acct-Session-Id	44	Accounting-Request	A character string for identifying the session. The Device stores the session's process ID.
Acct-Authentic	45	Accounting-Request	The manner in which the user was authenticated. The Device stores three authentication types: <code>RADIUS</code> (1), <code>Local</code> (2), or <code>Remote</code> (3).

Attribute name	Attribute value	Packet type	Description
Acct-Session-Time	46	Accounting-Request (only when Acct-Status-Type is Stop)	The length of time (in seconds) that the user received the service. The Device stores the time (in seconds) from successful login until logout.

- Access-Request packet

No attributes other than those listed above are attached to Access-Request packets sent by the Device.

- Access-Accept, Access-Reject, and Accounting-Response packets

Attributes other than those listed above are ignored by the Device if attached to the packet.

(3) Scope of TACACS+ implementation

The Device supports the following NAS functionality for communication with a TACACS+ server:

Table 8-6: Scope of TACACS+ implementation

Category		Description
Packet type		Support for the following packet types used in login authentication and authentication when changing to administrator mode (by the <code>enable</code> command): <ul style="list-style-type: none"> • Authentication Start (send) • Authentication Reply (receive) • Authentication Continue (send) Support for the following command authorization packet types: <ul style="list-style-type: none"> • Authorization Request (send) • Authorization Response (receive) Support for the following accounting packet types: <ul style="list-style-type: none"> • Accounting Request (send) • Accounting Reply (receive)
Login authentication	Attribute	<ul style="list-style-type: none"> • User • Password • priv-lvl
Authentication when changing to administrator mode (by the <code>enable</code> command)		
Command authorization	service	<ul style="list-style-type: none"> • taclogin
	Attribute	<ul style="list-style-type: none"> • class • allow-commands • deny-commands
Accounting	flag	<ul style="list-style-type: none"> • TAC_PLUS_ACCT_FLAG_START • TAC_PLUS_ACCT_FLAG_STOP
	Attribute	<ul style="list-style-type: none"> • task_id • start_time • stop_time • elapsed_time • timezone • service • priv-lvl • cmd

(a) Description of supported TACACS+ attributes

The table below describes the TACACS+ attributes used in authentication, command authorization, and accounting.

To perform command authorization using a TACACS+ server, you must set up the server in advance so that it returns a class attribute or an allow-commands or deny-commands attribute with the requested service when a user is authenticated. For details about command authorization, see *8.2.4 RADIUS or TACACS+ and local command authorization*.

Table 8-7: Supported TACACS+ attributes

Service	Attribute	Description
-	User	The name of the user being authenticated. Sends the login user name when login authentication is performed. Following <i>Table 8-10: User name attributes to be set</i> , sends the user name when authentication is performed to go into administrator mode (by the <code>enable</code> command).
	Password	The password of the user being authenticated, sent in encrypted form
	priv-lvl	The privilege level of the user being authenticated. 1 is used for login authentication. 15 is used for authentication when changing to administrator mode (by the <code>enable</code> command).
taclogin	class	Command class
	allow-commands	Authorized command list
	deny-commands	Unauthorized command list

Legend: --: Not applicable

The following table describes the TACACS+ flags for accounting services.

Table 8-8: TACACS+ accounting flags

Flag	Description
TAC_PLUS_ACCT_FLAG_START	Indicates accounting START packets. However, if <code>stop-only</code> is specified as the trigger of accounting in the <code>aaa</code> configuration entry, no accounting START packets will be sent.
TAC_PLUS_ACCT_FLAG_STOP	Indicates accounting STOP packets. However, if <code>stop-only</code> is specified as the trigger of accounting in the <code>aaa</code> configuration entry, only accounting STOP packets will be sent.

The following table describes the values of the TACACS+ attribute-value pairs used for accounting.

Table 8-9: TACACS+ accounting attribute-value pairs

Attribute	Value
task_id	The ID assigned to the event. The Device stores process IDs for accounting events.
start_time	The time at which the event started. The Device stores the times at which each accounting event was started. This attribute is stored when the following events occur: <ul style="list-style-type: none"> If <code>start-stop</code> is specified as the trigger of accounting: When the user logs in, and before a command is executed If <code>stop-only</code> is specified as the trigger of accounting: Before a command is executed

Attribute	Value
stop_time	The time at which the event ended. The Device stores the times at which each accounting event ended. This attribute is stored when the following events occur: <ul style="list-style-type: none"> If <code>start-stop</code> is specified as the trigger of accounting: When the user logs out, and after a command is executed If <code>stop-only</code> is specified as the trigger of accounting: When the user logs out
elapsed_time	The elapsed time (in seconds) after the event started. The Device stores the length of time (in seconds) from the start to the end of accounting events. This attribute is stored when the following events occur: <ul style="list-style-type: none"> If <code>start-stop</code> is specified as the trigger of accounting: When the user logs out, and after a command is executed If <code>stop-only</code> is specified as the trigger of accounting: When the user logs out
timezone	A string representing the time zone
service	The character string <code>shell</code>
priv-lvl	Privilege level 1 if using an operation command when setting up command accounting, or level 15 if using a configuration command
cmd	The command string (maximum 250 characters) entered when setting up command accounting

8.2.3 Authentication using RADIUS or TACACS+

This section describes authentication methods when using RADIUS or TACACS+.

(1) *Selecting the authentication service*

You can specify multiple services for login authentication and for authentication when changing to administrator mode (by the `enable` command). Specifiable services cover RADIUS and TACACS+ authentication, and login security functionality implemented in the Device by the `adduser` and `password` configuration commands.

These authentication methods can be specified singly or in combination. When multiple authentication methods are specified, the configuration command with `end-by-reject` set (see below) can change the behavior of the authentication service performed when the first-specified authentication method fails.

For login authentication

```
aaa authentication login end-by-reject
```

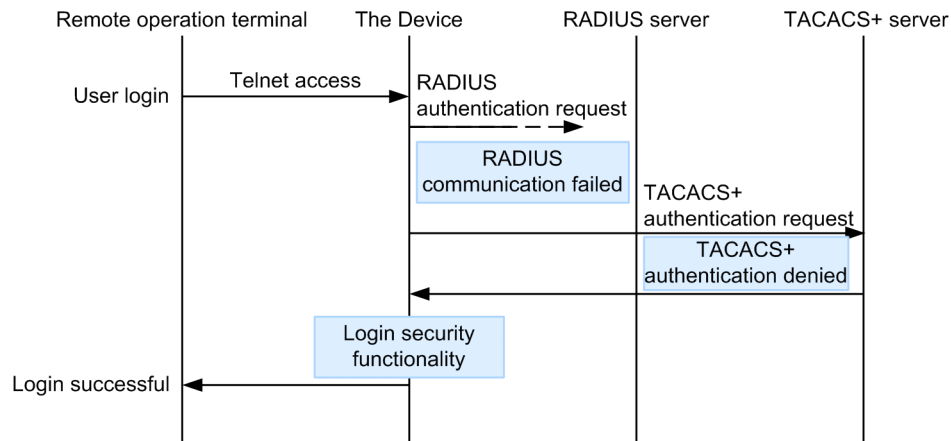
For authentication when changing to administrator mode (by the `enable` command)

```
aaa authentication enable end-by-reject
```

(a) **When end-by-reject is not set**

The following explains how an authentication service is selected when `end-by-reject` is not set. If authentication fails when using the first specified method when `end-by-reject` is not set, authentication can be performed using the next specified method regardless of the reason of failure.

As an example, the figure below shows the sequence in which authentication is performed when RADIUS, TACACS+, and individual login security methods are specified and performed in that order. The authentication results are as follows: The RADIUS server cannot communicate, the TACACS+ server denies authentication, and authentication succeeds through the login security functionality.

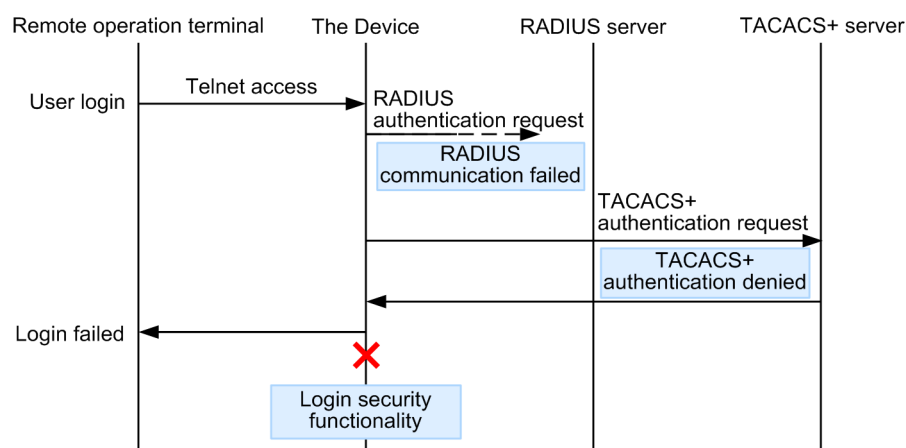
Figure 8-18: Sequence of authentication (without end-by-reject specified)

In this figure, the user accesses the Device via Telnet from a remote operation terminal, and the Device requests the RADIUS server to perform authentication. If the RADIUS authentication fails due to a communication failure, the Device requests the TACACS+ server to perform authentication. If TACACS+ authentication fails because the TACACS+ server denied the request, the Device performs authentication using the local login security functionality. At this point, authentication is successful and the user is able to log in to the Device.

(b) When end-by-reject is set

The following explains how an authentication service is selected when `end-by-reject` is set. If authentication fails when using the first specified method when `end-by-reject` is set, authentication is not performed using the next specified method. The entire authentication process is terminated at the first denial and is treated as a failure. The next authentication is performed only when authentication failed due to an abnormality such as communication failure.

As an example, the figure below shows the sequence in which authentication is performed when RADIUS, TACACS+, and individual login security methods are specified and performed in that order. The authentication results are as follows: The RADIUS server cannot communicate, and the TACACS+ server denies authentication.

Figure 8-19: Sequence of authentication (with end-by-reject specified)

In this figure, the user accesses the Device via Telnet from a remote operation terminal, and the Device requests the RADIUS server to perform authentication. If the RADIUS authentication fails due to a communication failure, the Device requests the TACACS+ server to perform authentication. The entire authentication process fails when authentication is denied by the TACACS+ server. The login security functionality of the Device that is specified as the next

method is not performed. As a result, the user fails to log in to the Device.

(2) Selecting the RADIUS or TACACS+ server

You can specify a maximum of four RADIUS servers and four TACACS+ servers. If one server is unreachable and its authentication service is unavailable, each of the other servers is attempted in turn.

When the RADIUS or TACACS+ servers are specified by host name and multiple addresses can be resolved, a single address is determined in order of priority and that server is communicated with.

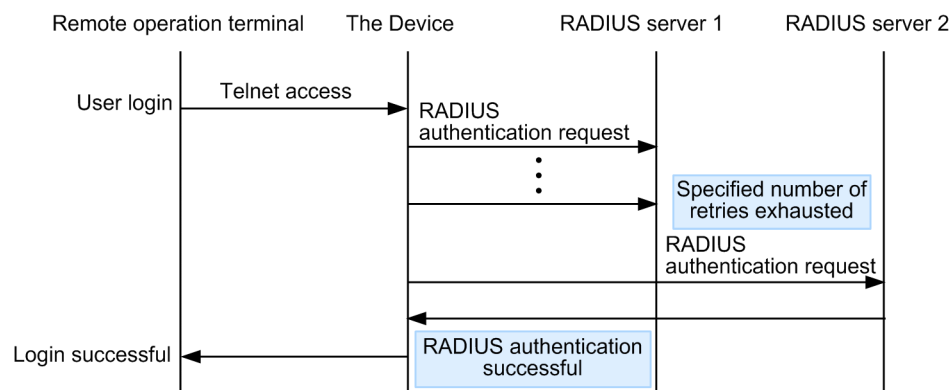
For details about order of priority, see *10.1 Description*.

Notes

If you are using a DNS server to resolve host names, communication with the server can take a long time. For this reason, we recommend that you specify the RADIUS or TACACS+ servers by IP address.

You can set a timeout period after which a RADIUS or TACACS+ server is judged unreachable. The default is five seconds. If a RADIUS server times out, another attempt is made to connect to it. You can set the maximum number of connection retries that the server makes with each server (three by default). Thus, the maximum length of time until RADIUS login authentication is deemed unavailable is given by the equation: $(\text{timeout-period}) \times (\text{number-of-retries}) \times (\text{number-of-configured-RADIUS-servers})$. If a TACACS+ server times out, reconnecting to the TACACS+ server is not attempted. Thus, the maximum length of time until TACACS+ login authentication is deemed unavailable is given by the equation: $(\text{timeout-period}) \times (\text{number-of-configured-TACACS+-servers})$. The following figure shows the RADIUS server selection sequence.

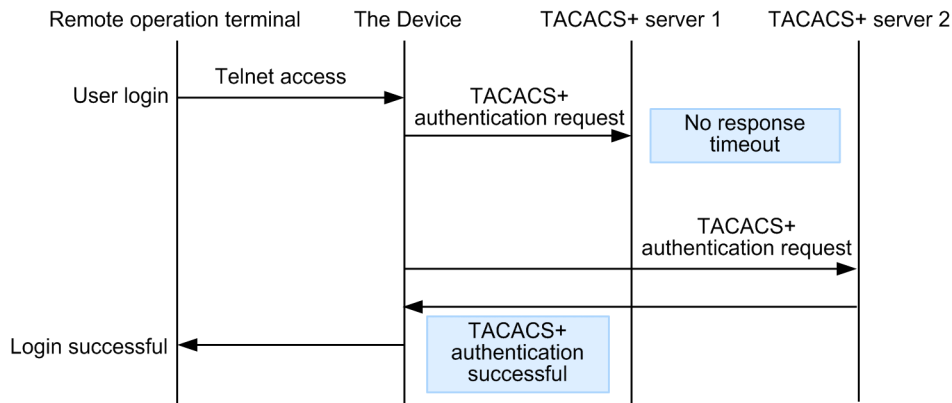
Figure 8-20: RADIUS server selection sequence



In this figure, the user accesses the Device via Telnet from a remote operation terminal, and the Device requests RADIUS server 1 to perform authentication. If RADIUS server 1 is unreachable, the RADIUS authentication request is sent to RADIUS server 2. At this point, authentication is successful and the user is able to log in to the Device.

The following figure shows the TACACS+ server selection sequence.

Figure 8-21: TACACS+ server selection sequence



In this figure, the user accesses the Device via Telnet from a remote operation terminal, and the Device requests TACACS+ server 1 to perform authentication. If TACACS+ server 1 is unreachable, the TACACS+ authentication request is sent to TACACS+ server 2. At this point, authentication is successful and the user is able to log in to the Device.

(3) Registering information with a RADIUS or TACACS+ server

(a) For login authentication

Register the user name and password with the RADIUS or TACACS+ server. A user name can be registered in either of two ways:

- User name already registered in the Device by the `username` configuration command
Login processing is based on the user information registered in the Device.
- Unregistered user name
Login processing is based on the following common user information:
 - User name: `remote_user`
 - Home directory: `/usr/home/share`

Note the following when an unregistered user logs in:

- File management
All created files are managed under `remote_user`, which means that other users will be able to read and write to them. Manage files carefully, for example by storing important files outside the network by FTP or other means.

(b) For authentication when changing to administrator mode (`enable` command)

Register the following user information for changing to administrator mode (by the `enable` command):

- User name

The Device sends the user names shown in the table below to the server as user name attributes. The user names to be sent can be changed using configuration commands. Register the corresponding user names with the server.

Table 8-10: User name attributes to be set

Command name	User name	
	RADIUS authentication	TACACS+ authentication
Not set	admin	admin

Command name	User name	
	RADIUS authentication	TACACS+ authentication
aaa authentication enable attribute-user-per-method	\$enab15\$	Login user name

- Privilege level

The privilege level is fixed at 15.

However, some servers use specific names (e.g. \$enab15\$) regardless of the sent user name attributes, and in some cases, privilege level registration is not necessary. For details, see your server documentation.

8.2.4 RADIUS or TACACS+ and local command authorization

This section describes command authorization using RADIUS or TACACS+ and local (configuration-based) command authorization.

(1) Overview of command authorization

You can limit the types of operation commands available to a login user who has been authenticated by a RADIUS server, TACACS+ server, or local password. This is known as command authorization. The operation commands that the user is allowed to use are controlled according to a command class or command lists obtained from the RADIUS or TACACS+ server or set in the local configuration. Operation commands that the user is not allowed to use do not appear among the character strings presented by command line completion. When a partially entered operation command contains a parameter with a value or character string, such as *<option>* or *<Host Name>*, the parameter part does not appear among the displayed entry completion strings.

Figure 8-22: RADIUS or TACACS+ login authentication and command authorization

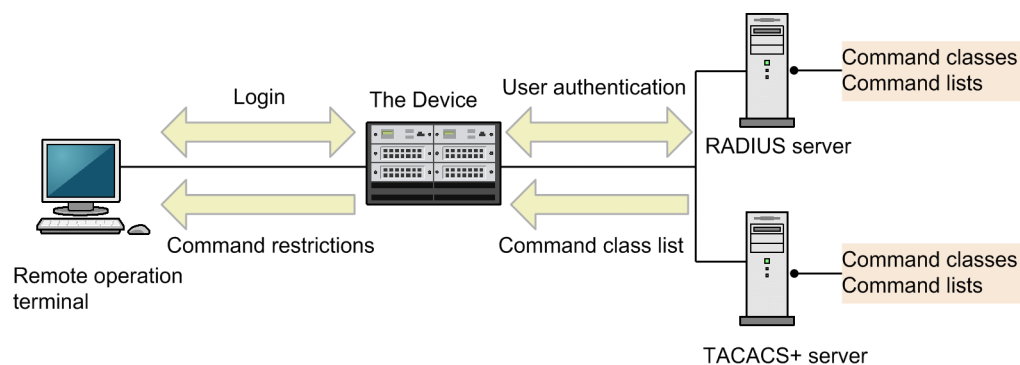
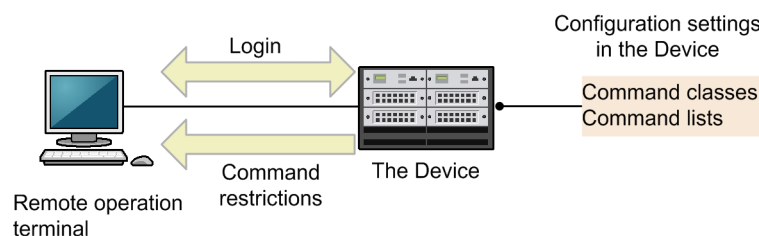


Figure 8-23: Local login authentication and command authorization



When command authorization is configured in the `aaa` configuration entries and RADIUS or TACACS+ authorization is specified, the command lists for the user are retrieved from the server concurrently with login authentication. If local command authorization is specified, the command lists set in the configuration entries are obtained concurrently with the login authentication. The

Device permits or denies operation commands entered by the login user according to these command lists.

Figure 8-24: RADIUS/TACACS+Sequence of RADIUS or TACACS+ command authorization

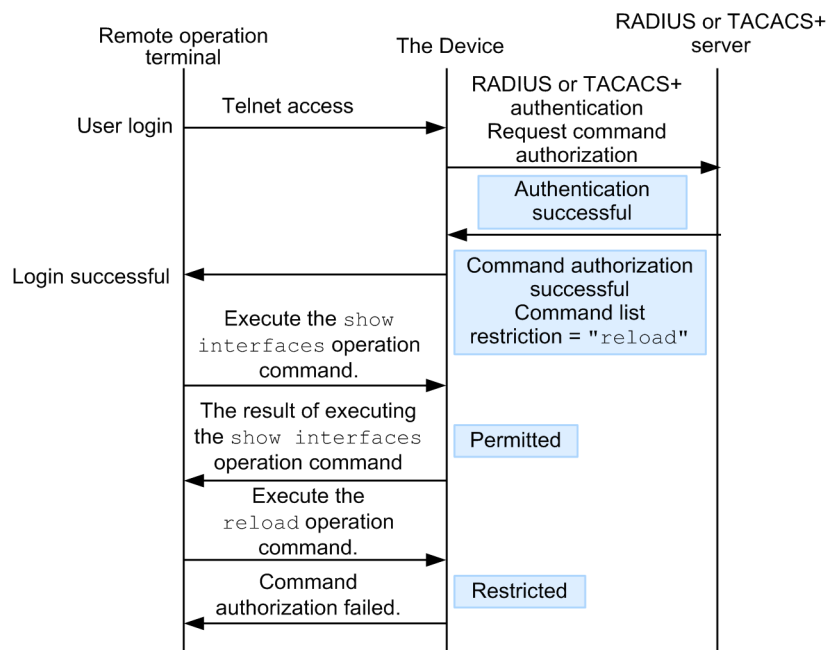
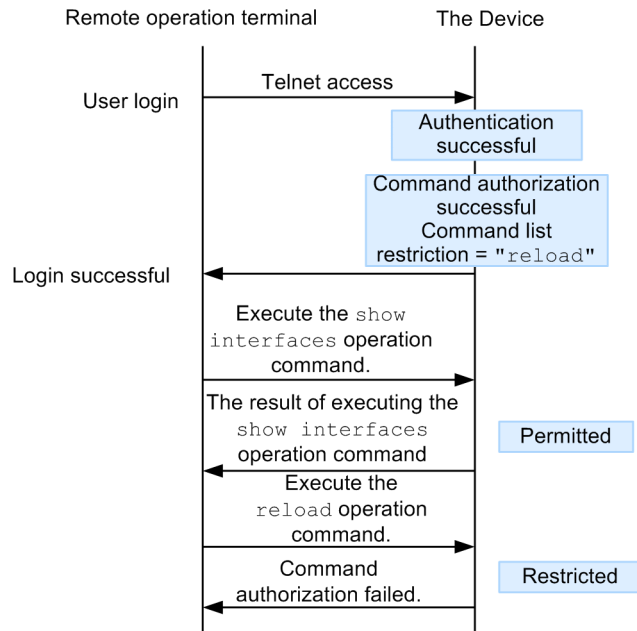


Figure 8-25: Sequence of local command authorization



In *Figure 8-24: RADIUS/TACACS+Sequence of RADIUS or TACACS+ command authorization*, the user accesses the Device via Telnet from a terminal, and the Device requests the RADIUS or TACACS+ server to perform authentication and command authorization. Authentication succeeds, the associated command lists are retrieved from the server, and the user logs in to the Device.

In *Figure 8-25: Sequence of local command authorization*, the user accesses the Device via Telnet from a remote operation terminal and the Device performs local authentication. Authentication succeeds, the associated command lists are obtained from the local configuration,

and the user logs in to the Device.

After login, the user can execute operation commands such as `show interfaces` on the Device. The `reload` operation command cannot be executed, however, because it is included in the unauthorized command list.

Note:

Any changes you make to a command list on the RADIUS or TACACS+ server, or to a locally configured command list, apply after the next login authentication.

(2) Setup procedures for RADIUS or TACACS+ and local command authorization

To use RADIUS or TACACS+ command authorization, set up a RADIUS or TACACS+ server and the Device as follows:

1. Decide your policies for restricting command execution.
For each user, decide which operation commands to restrict or permit.
2. Create command lists.
In addition to specifying a command class, you can set up separate lists of authorized commands and unauthorized commands.
3. Set up a RADIUS or TACACS+ server.
On the RADIUS or TACACS+ remote authentication server, perform the settings for authorizing commands based on your command restriction policies.
4. Set up remote authentication on the Device.
Set the RADIUS or TACACS+ server configuration and the `aaa` configuration on the Device.
5. Test the command authorization to make sure it works.
Log in to the Device from a remote operation terminal that is set up for RADIUS or TACACS+ authentication, and make sure that entered commands are permitted or denied correctly.

To use local command authorization, set up the Device as follows:

1. Decide your policies for restricting command execution.
For each user, decide which operation commands to restrict or permit.
2. Create command lists.
You can specify a command class, or you can enter authorized and unauthorized commands in separate command lists. Configure each command list based on your command restriction policies.
There is no need to create any command lists if you are using command classes only.
3. Assign a command class or command lists to each user.
Set the `username` configuration command to assign a command class or command lists to each user.
Then, set the `aaa` configuration.
4. Test the command authorization to make sure it works.
Log in to the Device by local authentication, and check that commands are permitted or denied correctly.

(3) Deciding your command restriction policies

For each user, decide which operation commands to restrict or permit. This means that each user,

once logged in, will be allowed to use some commands but not others. For details about setting command restriction policies, see (5) *Settings required for RADIUS or TACACS+ and local command authorization*.

A command restriction policy applies only to operation commands. It does not apply to undocumented debugging commands (such as the `ps` command) that are always unauthorized. (If you ever need to set permission for debugging commands, specify `root` as the unrestricted command class described below.) The `logout`, `exit`, `quit`, `disable`, `set terminal`, `show whoami`, `who am i` commands are always permitted.

The following policies are pre-defined in the Device. By selecting one of these standard command classes, you can set the command restrictions associated with that class.

Table 8-11: Command classes

Command class	Authorized command	Unauthorized command
<code>root</code> Unrestricted access to all commands	All commands (including undocumented debugging commands) with no authorization required	None
<code>allcommand</code> Unrestricted access to all operation commands	All operation commands "all"	None (except undocumented debugging commands)
<code>noconfig</code> No configuration changes permitted (no authority to execute configuration commands)	Operation commands except those in the next column	"config, copy, erase configuration"
<code>noenable</code> No commands requiring administrator privilege permitted	Operation commands except those in the next column	"enable"

In addition to specifying a command class, you can specify an authorized command list and unauthorized command list.

(4) Setting command lists

In addition to specifying a command class, you can set up separate lists of authorized commands and unauthorized commands. When entering commands in each list, be aware of any spaces required in the command strings and separate each command with a comma (,). To create a command list for local command authorization, specify each command in a separate `commands exec` configuration command. The entered commands, linked with commas (,), are used on the Device as a command list.

It is determined whether any of the command strings in the command lists match the initial character string of the command entered by the user (match beginning). As a special character, you can specify `all` in a command list, which means all operation commands.

When an entered command matches commands in both the authorized command list and unauthorized command list, the resultant action is determined by the matched command that has the greater number of characters (where `all` counts as one character). If both command lists contain the same command string, the input command is taken to be authorized.

If you specify command classes as well as lists of authorized and unauthorized commands, the command lists associated with each command class (the entries enclosed in double quotation marks (") in *Table 8-11: Command classes*) and the specified lists of authorized and unauthorized commands are all subject to judgment. Also, if you specify the `root` command class, this will invalidate the authorized/unauthorized command class settings, allowing the user to execute all commands including undocumented debugging commands (such as the `ps` command).

The following seven examples show which commands will be permitted or restricted on the Device according to the command lists set in each case.

Example 1

If you set only an authorized command list, the user is authorized to execute only the commands in that list.

Table 8-12: Command list example 1

Command list	Input by user	Judgment
Authorized command list = "show ,ping" Unauthorized command list: None set	show ip arp	Allow
	ping ipv6 ::1	Allow
	reload	Deny

Example 2

If an entered command matches commands in both the authorized command list and unauthorized command list, the judgment is determined by the matched command that has the greater number of characters (where `all` counts as one character).

Table 8-13: Command list example 2

Command list	Input by user	Judgment
Authorized command list = "show ,ping ipv6" Unauthorized command list = "show ip,ping"	show system	Allow
	show ipv6 neighbors	Deny
	ping ipv6 ::1	Allow
	ping 10.10.10.10	Deny

Example 3

If you set both authorized and unauthorized command lists, entered commands that match neither list are taken to be authorized.

Table 8-14: Command list example 3

Command list	Input by user	Judgment
Authorized command list = "show" Unauthorized command list = "reload"	ping 10.10.10.10	Allow
	reload	Deny

Example 4

If the same command string appears in both the authorized and unauthorized command lists, the command is taken to be authorized.

Table 8-15: Command list example 4

Command list	Input by user	Judgment
Authorized command list = "show" Unauthorized command list = "show ,ping"	show system	Allow
	ping ipv6 ::1	Deny

Example 5

If you do not set any command lists, all entered commands except `logout` and some others are denied.

Table 8-16: Command list example 5

Command list	Input by user	Judgment
Authorized command list: None set Unauthorized command list: None set	All commands	Deny
	logout, exit, quit, disable, set terminal, show whoami, who am i	Allow

Example 6

The `root` command class allows all commands to be executed with no authorization required. If you specify `root`, the authorized/unauthorized command class settings are invalidated, and the user can execute all commands including undocumented debugging commands (such as the `ps` command).

Table 8-17: Command list example 6

Command list	Input by user	Judgment
Command class = "root"	All commands (including undocumented debugging commands)	Allow

Example 7

If you set only an unauthorized command list, the user is authorized to execute all operation commands that do not match those in the list.

Table 8-18: Command list example 7

Command list	Input by user	Judgment
Authorized command list: None set Unauthorized command list = "reload"	All operation commands except <code>reload</code>	Allow
	<code>reload</code>	Deny

To illustrate how command authorization is implemented, assume that the following command restriction policies have been decided:

Table 8-19: Examples of command restriction policies

User name	Command class	Authorized command	Unauthorized command
staff	allcommand	All operation commands	None
guest	None	All operation commands except those in the next column	<code>reload...#</code> <code>inactivate...#</code> <code>enable...#</code>
test	None	<code>show ip...#</code> (<code>show ipv6...</code> is unauthorized)	All operation commands except those in the previous column

#: The ellipsis (...) represents a parameter (for example, `show ip...` might represent `show ip arp`).

(5) Settings required for RADIUS or TACACS+ and local command authorization

Based on the example command restriction policies determined in *Table 8-19: Examples of command restriction policies*, enter settings on the RADIUS or TACACS+ remote authentication server, additional to the usual login authentication settings, to implement command restrictions based on the attribute values described in the table below.

Note that if command authorization has not been configured on the server side, after authentication and successful login from a remote terminal you will not be authorized to execute any commands except `logout`, `exit`, `quit`, `disable`, `set terminal`, `show whoami`, and `who am i`. In this case, log in from the console.

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

■ When using RADIUS servers

To implement command authorization with a RADIUS server, set up the server so that the following attributes will be returned at authentication.

Table 8-20: RADIUS setup attributes

Attribute	Vendor-specific attribute	Code
25 Class	--	Class Specify one of the following strings: <code>root</code> , <code>allcommand</code> , <code>noconfig</code> , or <code>noenable</code>
26 Vendor-Specific Vendor-Id: 21839	ALAXALA-Allow-Commands Vendor type: 101	Authorized command list Specify the initial string of each of the authorized commands to be matched, separated by commas (,). Spaces are also matched. Use "all" to specify every operation command. When an authorized command list alone is set, all commands other than those in the list are prohibited. Example: <code>ALAXALA-Allow-Commands="show ,ping ,telnet"</code>
	ALAXALA-Deny-Commands Vendor type: 102	Unauthorized command list Specify the initial string of each of the unauthorized commands to be matched, separated by commas (,). Spaces are also matched. Use "all" to specify every operation command. When an unauthorized command list alone is set, all commands other than those in the list are permitted. Example: <code>ALAXALA-Deny-Commands="enable, reload, inactivate"</code>

Legend: --: Not applicable

Set these vendor-specific attributes in a `dictionary` file or other configuration file to register them with the RADIUS server.

Figure 8-26: Example of registering vendor-specific attributes in a dictionary file for a RADIUS server

```

VENDOR      ALAXALA      21839
ATTRIBUTE   ALAXALA-Allow-Commands 101      string  ALAXALA
ATTRIBUTE   ALAXALA-Deny-Commands  102      string  ALAXALA

```

The following figure shows an example of implementing the policies determined in Table 8-19: *Examples of command restriction policies* in a typical RADIUS server.

Figure 8-27: Example of RADIUS server setup

```

staff Password = "*****"
      Class = "allcommand" <-1

guest Password = "*****"
      Alaxala-Deny-Commands = "enable, reload, inactivate" <-2

```

```
test Password = "*****"
Alaxala-Allow-Commands = "show ip " <-3
```

Note: The asterisks (*****) represent the user password.

1. The `allcommand` class permits all operation commands.
2. Prohibits commands beginning with `enable`, `reload`, or `inactivate`.

Because `allow-commands` is not specified, all other commands are permitted.

3. Spaces are meaningful.

Because `show ip` is followed by a space, commands such as `show ip arp` are permitted, but commands such as `show ipv6 neighbors` are not.

All other commands are prohibited.

Notes

- When multiple `Class` entries are received on the Device the first entry is recognized and subsequent entries are ignored.

Figure 8-28: Example of setting multiple Class entries

```
Class = "noenable" <-1
Class = "allcommand"
```

1. Only the first `noenable` is valid.

- When multiple class names are registered in the `Class` entry on the Device, the first class name is recognized and subsequent class names are ignored. For example, if you enter `class="noenable,allcommand"`, only `noenable` will be valid.
- When multiple entries are received with the `ALAXALA-Deny-Commands` attribute or `ALAXALA-Allow-Commands` attribute, a maximum of 1024 characters are recognized, including commas (,) and spaces. Subsequent characters are ignored. Also, if you specify multiple entries for the same attribute as in the example below, a comma (,) will be automatically placed in front of each entry on receipt of the second and subsequent entries on the Device.

Figure 8-29: Example of setting multiple Deny-Commands entries

```
ALAXALA-Deny-Commands = "inactivate, reload" <-1
ALAXALA-Deny-Commands = "activate, test, ....." <-1
```

1. The Device can recognize the underlined parts up to a total of 1024 characters.

As shown in the figure below, when the above `Deny-Commands` entries are received, a comma (,) is automatically placed in front of the `activate` command which is the first command in the second entry.

```
Deny-Commands =
"inactivate, reload, activate, test, ....."
```

■ When using TACACS+ servers

To implement command authorization with a TACACS+ server, set attribute-value pairs as shown below.

Table 8-21: TACACS+ setup attributes

Service	Attribute	Code
taclogin	class	Command class Specify one of the following strings: root, allcommand, noconfig, or noenable
	allow-commands	Authorized command list Specify the initial string of each of the authorized commands to be matched, separated by commas (,). Spaces are also matched. Use "all" to specify every operation command. When an authorized command list alone is set, all commands other than those in the list are prohibited. Example: allow-commands="show ,ping ,telnet "
	deny-commands	Unauthorized command list Specify the initial string of each of the unauthorized commands to be matched, separated by commas (,). Spaces are also matched. Use "all" to specify every operation command. When an unauthorized command list alone is set, all commands other than those in the list are permitted. Example: deny-commands="enable, reload, inactivate"

The following figure shows an example of implementing the policies determined in Table 8-19: *Examples of command restriction policies* in a typical TACACS+ server.

Figure 8-30: Example of TACACS+ server setup

```

user=staff {
    login = cleartext "*****"
    service = taclogin {
        class = "allcommand"
    }
}

user=guest {
    login = cleartext "*****"
    service = taclogin {
        deny-commands = "enable, reload, inactivate"
    }
}

user=test {
    login = cleartext "*****"
    service = taclogin {
        allow-commands = "show ip "
    }
}

```

<-1

<-2

<-3

Note: The asterisks (*****) represent the user password.

1. Sets taclogin as the service name.
The allcommand class permits all operation commands.
2. Prohibits commands beginning with enable, reload, or inactivate.
Because allow-commands is not specified, all other commands are permitted.
3. Spaces are meaningful.
Because show ip is followed by a space, commands such as show ip arp are permitted, but commands such as show ipv6 neighbors are not.
All other commands are prohibited.

Notes

- When multiple class names are registered in the `class` entry on the Device, the first class name is recognized and subsequent class names are ignored. For example, if you enter `class="noenable,allcommand"`, only `noenable` will be valid.
 - For each of the deny-commands and allow-commands attributes, a maximum of 1024 characters are recognized, including commas (,) and spaces. Subsequent characters are ignored.
- When using local command authorization

The following figure shows an example of implementing the policies determined in *Table 8-19: Examples of command restriction policies* by using the local command authorization.

Figure 8-31: Example of setting the configuration

```
username guest 100 password hidden "$6$IV8Zku9 ... yHwVYBogw0"
username guest view guest_view
username staff 101 password hidden "$6$sIn064g ... o1jy7xbHj."
username staff view-class allcommand                                <-1
username test 102 password hidden "$6$ijRqkU2j ... 8qdMXxFk0"
username test view test_view
!
parser view guest_view
  commands exec exclude all "enable"                                <-2
  commands exec exclude all "inactivate"                            <-2
  commands exec exclude all "reload"                                <-2
!
parser view test_view
  commands exec include all "show ip "                                <-3
!
aaa authentication login default local
aaa authorization commands default local
```

1. Assigns the `allcommand` class to the user `staff`, permitting all operation commands.
2. Prohibits commands beginning with `enable`, `inactivate`, or `reload`.

Because `commands exec include` is not specified, all other commands are permitted.

3. Spaces are meaningful.

Because `show ip` is followed by a space, commands such as `show ip arp` are permitted, but commands such as `show ipv6 neighbors` are not.

All other commands are prohibited.

(a) Testing the setup

After the setting is complete, log in to the Device from a remote operation terminal by using RADIUS or TACACS+ or local command authorization. After you log in, execute the `show whoami` command to make sure that the command lists are set, and then execute one or two commands to make sure they are permitted or denied correctly.

Figure 8-32: Example of login and testing by the user "staff"

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
staff ttyp0 ----- 2 Jan 6 14:17 (10.10.10.10)

Home-directory: /usr/home/staff
Authentication: TACACS+ (Server 192.168.10.1)
Class: allcommand
  Allow: "all"
  Deny : -----
Command-list: -----
>
```

```
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> /bin/date
The command is not authorized by the RADIUS/TACACS+ server or the configuration.
>
```

Figure 8-33: Example of login and testing by the user "guest"

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
guest ttyp0 ----- 2 Jan 6 14:17 (10.10.10.20)

Home-directory: /usr/home/guest
Authentication: RADIUS (Server 192.168.10.1)
Class: -----
Command-list:
    Allow: -----
    Deny : "enable,reload,inactivate"

>
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> reload
The command is not authorized by the RADIUS/TACACS+ server or the configuration.
>
```

Figure 8-34: Example of login and testing by the user "test"

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
test ttyp0 ----- 2 Jan 6 14:17 (10.10.10.30)

Home-directory: /usr/home/test
Authentication: LOCAL
Class: -----
Command-list:
    Allow: "show ip "
    Deny : -----

>
> show ip arp <-1
> show ipv6 neighbors
The command is not authorized by the RADIUS/TACACS+ server or the configuration.
>
```

1. The command is executed.

8.2.5 RADIUS and TACACS+ accounting

This section describes RADIUS and TACACS+ accounting methods.

(1) Setting up accounting

By configuring accounting in the RADIUS or TACACS+ configuration and in the `aaa accounting` configuration, you can set up the Device to send accounting information to the RADIUS or TACACS+ server whenever a user logs in or logs out from the Device by using a remote operation terminal. Accounting information will also be sent to the TACACS+ server at every command input to the Device.

Two types of accounting can be configured: login accounting for sending login and logout events to the server, and command accounting for sending command input events. Command accounting is supported only by TACACS+.

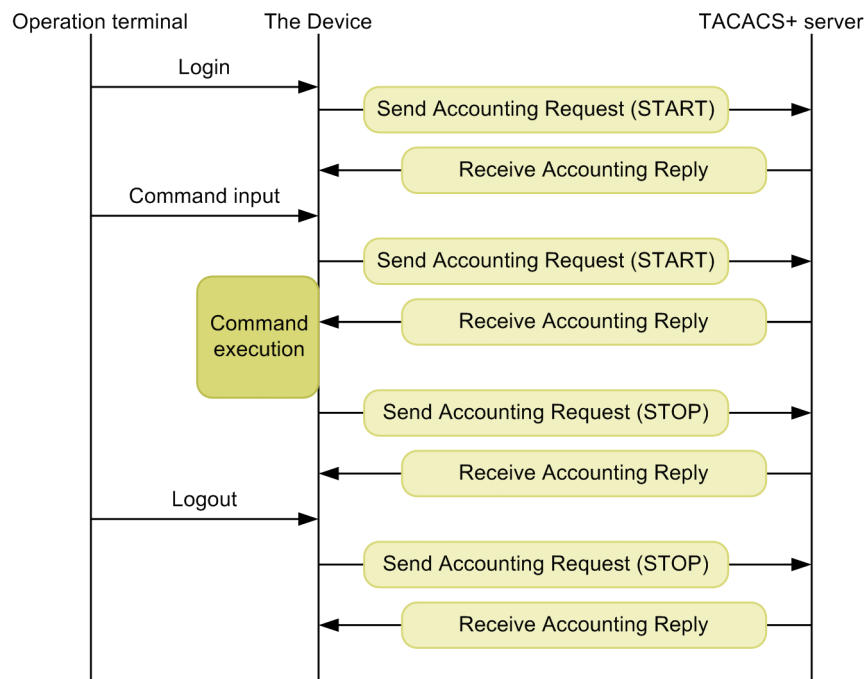
For each type of accounting, you can select either a mode (`start-stop`) that sends both START and STOP accounting notices, or a mode (`stop-only`) that sends STOP notices only. For command accounting, you can choose to report all entered commands or only configuration commands. Normally, records are sent to each RADIUS or TACACS+ server in turn, as long as each server is available and until accounting is successful, but you can also choose a mode (`broadcast`) to

broadcast accounting records to all the servers regardless of success or failure.

(2) Accounting flow

The following figure shows the processing sequence when the system is configured to send accounting notices to a TACACS+ server in START-STOP transmission mode for both login accounting and command accounting.

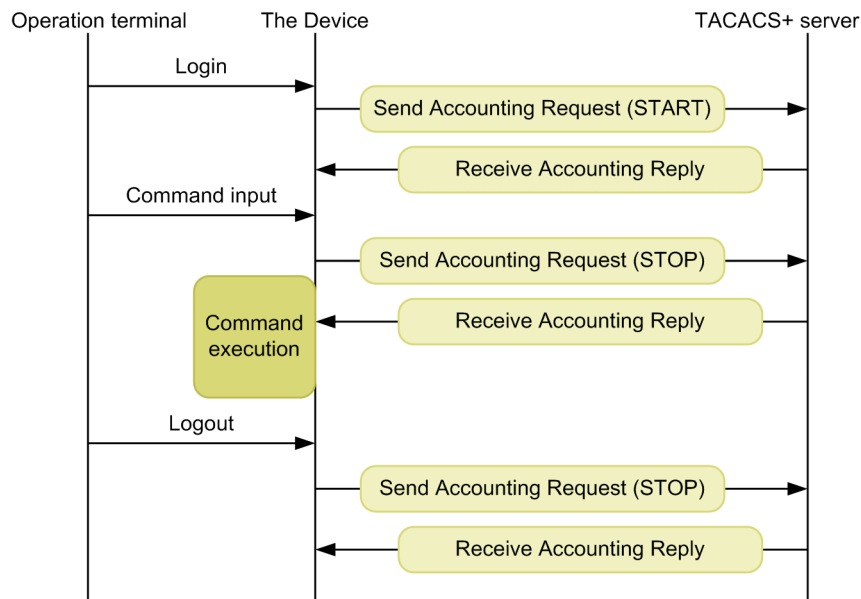
Figure 8-35: TACACS+ accounting sequence (login and command accounting in START-STOP transmission mode)



In this figure, when a user successfully logs in from a remote operation terminal, accounting information such as user data and timestamps is sent from the Device to the TACACS+ server. In addition, command accounting information is forwarded before and after every command executed by the user. Finally, when the user logs out, information such as the duration of the session is sent.

The following figure shows the processing sequence when the system is configured to send accounting notices to a TACACS+ server in START-STOP transmission mode for login accounting, and in STOP-ONLY transmission mode for command accounting.

Figure 8-36: TACACS+ accounting sequence (login accounting in START-STOP transmission mode; command accounting in STOP-ONLY transmission mode)



The login-logout accounting behavior here is the same as the example in *Figure 8-35: TACACS+ accounting sequence (login and command accounting in START-STOP transmission mode)*, but because STOP-ONLY transmission mode is specified for command accounting, command-related accounting information is sent from the Device to the TACACS+ server before command execution only.

(3) Notes

When you configure accounting in the RADIUS or TACACS+ configuration and in the `aaa accounting` configuration, or change the IPv4 device address in the `interface loopback` configuration, accounting events being sent or received, unsent events, and statistics are cleared and the accounting sequence follows the new settings.

If numerous users are entering commands and logging in and out in succession, some accounting events might not be logged due to the large volume of generated events.

To avoid overloading the Device, servers, and network with a large volume of accounting events, we recommend that you set STOP-ONLY transmission mode for command accounting. Take care not to specify a RADIUS or TACACS+ server that is likely to be unreachable.

If you clear the accounting statistics using the `clear accounting` operation command, the service will recommence recording statistics about accounting events sent to the servers only when the accounting events that were being sent to a server when the `clear accounting` command was executed have been successfully transmitted.

If you are using a DNS server to resolve host names, communication with the server can take a long time. For this reason, we recommend that you specify the RADIUS and TACACS+ servers by IP address.

8.2.6 Connecting with RADIUS or TACACS+

(1) Connecting to RADIUS servers

(a) Device identification on the RADIUS server side

RADIUS protocol states that the source IP address of the request packet must be used as the key for identifying the NAS. The Device uses the following types of address as the source IP address of a request packet:

- If a local address is set by the `interface loopback 0` configuration command, the local address is used as the source IP address.
- If a local address is not set, the IP address of the sending interface is used.

Therefore, if the local address is set, that IP address must be used to register the Device with the RADIUS server. By setting the local address, the RADIUS server will be able to reliably identify the Device from the registered information, if the interface for communicating with the RADIUS server were unidentifiable.

(b) RADIUS server messages

In some cases, the RADIUS server attaches a Reply-Message attribute to a response and sends a message to the requestor. The Device outputs the contents of the Reply-Message attribute to an operation log. If authentication by the RADIUS server fails, check this operation log.

(c) Port number of the RADIUS server

Port 1812 is assigned to the RADIUS authentication service in RFC 2865. Unless otherwise specified, the Device uses port 1812 in requests sent to a RADIUS server. However, some RADIUS servers still use port 1645, which was used in early implementations. For a RADIUS server of this type, specify 1645 in the `auth-port` parameter of the `radius-server host` configuration. Because you can specify any value from 1 to 65535 in the `auth-port` parameter, the RADIUS server is supported regardless of the specified port.

(2) Connecting with a TACACS+ server

(a) TACACS+ server setup

- Take care with the service and attribute name settings when connecting the Device with a TACACS+ server. For TACACS+ server attributes, see *8.2.4 RADIUS or TACACS+ and local command authorization*.
- If a local address is set by the `interface loopback 0` configuration command, the local address is used as the source IP address.

8.3 RADIUS and TACACS+ configurations

8.3.1 List of configuration commands

The following tables describe the configuration commands for RADIUS, TACACS+, and accounting.

Table 8-22: List of configuration commands (RADIUS)

Command name	Description
radius-server host	Sets a RADIUS server for authentication, authorization, and accounting purposes.
radius-server key	Sets a RADIUS server key for authentication, authorization, and accounting purposes.
radius-server retransmit	Sets the maximum number of retransmissions to a RADIUS server used for authentication, authorization, and accounting purposes.
radius-server timeout	Sets a response timeout value for a RADIUS server used for authentication, authorization, and accounting purposes.

Table 8-23: List of configuration commands (TACACS+)

Command name	Description
tacacs-server host	Sets a TACACS+ server for authentication, authorization, and accounting purposes.
tacacs-server key	Sets a shared private key for communication with a TACACS+ server used for authentication, authorization, and accounting purposes.
tacacs-server timeout	Sets a response timeout value for a TACACS+ server used for authentication, authorization, and accounting purposes.

Table 8-24: List of configuration commands (accounting)

Command name	Description
aaa accounting commands	Enables command accounting.
aaa accounting exec	Enables login-logout accounting.

8.3.2 Configuring RADIUS authentication

(1) Example of configuring login authentication

Points to note

The example below shows how to configure RADIUS authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the RADIUS server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

The usual setup for remote access must be completed in advance.

Command examples

1. **(config)# aaa authentication login default group radius local**
Sets RADIUS authentication and local authentication, in that order, as the authentication methods to be used when a user logs in.

2. **(config)# aaa authentication login end-by-reject**

Configures the settings so that the whole authentication process ends when denied by RADIUS authentication and no local authentication is performed.

3. **(config)# radius-server host 192.168.10.1 key "039fk11f84kxm3"**

Sets IP address 192.168.10.1 as the server to be used for RADIUS authentication and a shared key for communication with the server.

(2) Example of configuring authentication for changing to administrator mode (enable command)

Points to note

The example below shows how to configure RADIUS authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the RADIUS server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

Also specify settings so that \$enab15\$ is sent as the user name attribute for RADIUS authentication.

Command examples

1. **(config)# aaa authentication enable default group radius enable**

Sets RADIUS authentication and local authentication, in that order, as the authentication methods to be used when the user changes to administrator mode (by the `enable` command).

2. **(config)# aaa authentication enable end-by-reject**

Configures the settings so that the whole authentication process ends when denied by RADIUS authentication and no local authentication is performed.

3. **(config)# aaa authentication enable attribute-user-per-method**

Configure a setting so that \$enab15\$ is sent as the user name attribute for RADIUS authentication.

4. **(config)# radius-server host 192.168.10.1 key "039fk11f84kxm3"**

Sets IP address 192.168.10.1 as the server to be used for RADIUS authentication and a shared key for communication with the server.

8.3.3 Configuring TACACS+ authentication

(1) Example of configuring login authentication

Points to note

The example below shows how to configure TACACS+ authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the TACACS+ server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

The usual setup for remote access must be completed in advance.

Command examples

1. **(config)# aaa authentication login default group tacacs+ local**
Sets TACACS+ authentication and local authentication, in that order, as the authentication methods to be used when a user logs in.
2. **(config)# aaa authentication login end-by-reject**
Configures the settings so that the whole authentication process ends when denied by TACACS+ authentication and no local authentication is performed.
3. **(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"**
Sets IP address 192.168.10.1 as the server to be used for TACACS+ authentication and a shared key for communication with the server.

(2) Example of configuring authentication for changing to administrator mode (enable command)

Points to note

The example below shows how to configure TACACS+ authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the TACACS+ server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

Also set the login user name to be sent as the user name attribute when performing TACACS+ authentication.

Command examples

1. **(config)# aaa authentication enable default group tacacs+ enable**
Sets TACACS+ authentication and local authentication, in that order, as the authentication methods to be used when the user changes to administrator mode (by the `enable` command).
2. **(config)# aaa authentication enable end-by-reject**
Configures the settings so that the whole authentication process ends when denied by TACACS+ authentication and no local authentication is performed.
3. **(config)# aaa authentication enable attribute-user-per-method**
Sets the login user name to be sent as the user name attribute when performing TACACS+ authentication.
4. **(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"**
Sets IP address 192.168.10.1 as the server to be used for TACACS+ authentication and a shared key for communication with the server.

8.3.4 Configuring RADIUS or TACACS+ and local command authorization

(1) Example of configuring RADIUS command authorization

Points to note

The example below shows how to configure command authorization using a RADIUS server.

Before performing this procedure, complete the setup for using RADIUS authentication.

Command examples

1. **(config)# aaa authentication login default group radius local**
(config)# radius-server host 192.168.10.1 key "RaD#001"

Configures RADIUS authentication as a prerequisite step.

2. **(config)# aaa authorization commands default group radius**

Performs command authorization using a RADIUS server.

Notes

If command authorization has been configured as described above, but has not been set up on the RADIUS server side, all commands will be prohibited when the RADIUS-authenticated user logs in. If you are unable to execute any commands, because a setup task has been omitted, for example, log in from the console and complete the required setup. If command authorization has also been implemented on the console by the `aaa authorization commands console` configuration command, perform a default restart and then log in.

(2) Example of configuring TACACS+ command authorization

Points to note

The example below shows how to configure command authorization using a TACACS+ server.

Before performing this procedure, complete the setup for using TACACS+ authentication.

Command examples

1. **(config)# aaa authentication login default group tacacs+ local**
(config)# tacacs-server host 192.168.10.1 key "TaC#001"

Configures authentication by a TACACS+ server as a prerequisite step.

2. **(config)# aaa authorization commands default group tacacs+**

Performs command authorization using a TACACS+ server.

Notes

If command authorization has been configured as described above, but has not been set up on the TACACS+ server side, all commands will be prohibited when the TACACS+-authenticated user logs in. If you are unable to execute any commands, because a setup task has been omitted, for example, log in from the console and complete the required setup. If command authorization has also been implemented on the console by the `aaa authorization commands console` configuration command, perform a default restart and then log in.

(3) Example of configuring local command authorization**Points to note**

The example below shows how to configure local command authorization.

Before performing this procedure, set the user name and the associated command class (username view-class) or command lists (username view, parser view, or commands exec).

Also, change the settings so that local password authentication can be used.

Command examples

1.

```
(config)# parser view Local_001
(config-view)# commands exec include all "show"
(config-view)# commands exec exclude all "reload"
```

Creates the command lists to be used for local authorization.

There is no need to create any command lists if you are using command classes only.

2.

```
(config)# username user001 view Local_001
(config)# username user001 view-class noenable
```

Assigns a command class or command lists to the specified user.

Both a command class and command lists can be used together.

3.

```
(config)# aaa authentication login default local
```

Configures local password authentication.

4.

```
(config)# aaa authorization commands default local
```

Performs command authorization using local authentication.

Notes

Be aware that local command authorization applies to all users who log in with local authentication. Configure local authorization carefully so that security is not compromised.

If no command class or command list has been set for a user, no commands will be permitted or executable by that user.

If you are unable to execute any commands, because a setup task has been omitted, for example, log in from the console and complete the required setup. If command authorization has also been implemented on the console by the `aaa authorization commands console` configuration command, perform a default restart and then log in.

8.3.5 Configuring RADIUS or TACACS+ login-logout accounting**(1) Example of configuring RADIUS login-logout accounting****Points to note**

The example below shows how to configure RADIUS login-logout accounting. Before you begin, complete the setup on the RADIUS server host to which the accounting records will be sent.

Command examples

1. **(config)# radius-server host 192.168.10.1 key "RaD#001"**
Configures the RADIUS server as a prerequisite step.
2. **(config)# aaa accounting exec default start-stop group radius**
Configures login-logout accounting.

Notes

If you set `aaa accounting exec` when the `radius-server` configuration is not set, the system message (message type: ACCESS, message ID: 27000013) will appear whenever a user logs in or logs out. Make sure that you configure the destination RADIUS server first.

(2) Example of configuring TACACS+ login-logout accounting

Points to note

The example below shows how to configure TACACS+ login-logout accounting. Before you begin, complete the setup on the TACACS+ server host to which the accounting records will be sent.

Command examples

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
Configures the TACACS+ server as a prerequisite step.
2. **(config)# aaa accounting exec default start-stop group tacacs+**
Configures login-logout accounting.

Notes

If you set `aaa accounting exec` when the `tacacs-server` configuration is not set, a system message (message type: ACCESS, message ID: 27000013) will appear whenever a user logs in or logs out. Make sure that you configure the destination TACACS+ server first.

8.3.6 Configuring TACACS+ command accounting

(1) Example of configuring TACACS+ command accounting

Points to note

The example below shows how to configure TACACS+ command accounting.

Before you begin, complete the setup on the TACACS+ server host to which the accounting records will be sent.

Command examples

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
Configures the TACACS+ server as a prerequisite step.
2. **(config)# aaa accounting commands 0-15 default start-stop group tacacs+**
Configures command accounting.

Notes

If you set `aaa accounting` commands when the `tacacs-server` configuration is not set, a system message (message type: ACCESS, message ID: 27000013) will appear whenever a user executes a command. Make sure that you configure the destination TACACS+ server first.

Chapter

9. Time Settings, NTP, and SNTP

This chapter describes time settings, NTP, and SNTP.

- 9.1 Description
- 9.2 Time settings
- 9.3 NTP configuration
- 9.4 SNTP configuration
- 9.5 Operation

9.1 Description

9.1.1 Overview

Set the clock time at first deployment of the Device. Time information is used in the Device's log entries and in timestamps when files are created. Set the correct time when you begin using the Device. You can set the time using the `set clock` operation command.

You can also use Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to synchronize the times with an NTP server or SNTP server on the network. The features of NTP and SNTP in the Device are as follows:

Features of NTP

- Times can be synchronized with high accuracy by referencing multiple NTP servers.
- Times can be automatically adjusted by calculating time accuracy based on past synchronization information.
- Times can be corrected between multiple NTP servers by configuring symmetric active/passive mode

Features of SNTP

- Time synchronization using IPv6 is supported.
- The design is simple, and does not require time information calculations like NTP
- A maximum of 4096 inquiries about time information from SNTP clients can be handled.

If the Device uses NTP or SNTP client functionality, the Device can be synchronized with an NTP or SNTP server. If the Device uses NTP or SNTP server functionality, NTP or SNTP clients can be synchronized with the Device.

9.1.2 Notes on time settings, NTP, and SNTP

- If the time is changed, the CPU usage statistics displayed by the `show cpu` operation command are cleared to zero.
- The daylight savings time setting is also effective for past times in a day.
- NTP and SNTP cannot be set at the same time.

9.2 Time settings

9.2.1 Lists of configuration commands and operation commands

The following table describes the configuration commands for time settings.

Table 9-1: List of configuration commands

Command name	Description
clock summer-time	Sets the clock for daylight savings time.
clock timezone	Sets the time zone.

The following table describes the operation commands for time settings.

Table 9-2: List of operation commands

Command name	Description
set clock	Sets and shows the local date and time.

9.2.2 System clock settings

The following describes an example of setting Japan time (time zone: JST, offset from UTC: +9).

Points to note

To set the Device's system clock, you must set the time zone in advance by using the `clock timezone` configuration command.

Command examples

1. **(config)# clock timezone JST +9**

Sets the JST time zone and an offset of +9 from UTC.

2. **(config)# save**
(config)# exit

In auto-applied commit mode, use the `save` command to save the settings into the startup configuration. In manual commit mode, use the `commit` command to apply the settings to the running configuration and save it as the startup configuration.

Then, configuration command mode switches to administrator mode.

3. **# set clock 1303221530**
Fri Mar 22 15:30:00 JST 2013

Sets the clock to 15:30 JST on March 22, 2013.

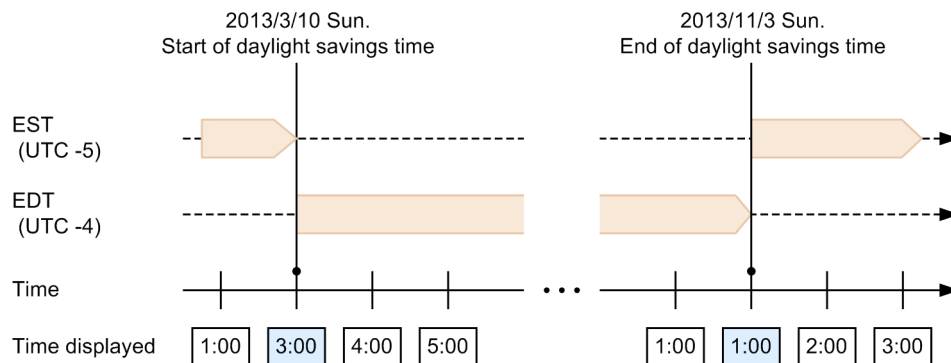
9.2.3 Daylight savings time settings


Not only standard time but also daylight savings time can be set for the time zone. For the daylight savings time settings, you can specify a daylight savings time period and the time difference from the standard time. The standard time specified by the `clock timezone` configuration command is used as a reference time for the time of day to change to daylight savings time.

For example, to apply U.S. Eastern Daylight Time (EDT) to the Eastern Standard Time (EST) time zone in the United States, set the period for applying Eastern Daylight Time (from 2:00 a.m. on the

second Sunday in March to 2:00 a.m. on the first Sunday in November) as daylight savings time with one-hour time difference. In this case, as the start of daylight savings time, set the clock ahead one hour at 2:00 a.m. EST on the second Sunday in March. In addition, as the end of daylight savings time, set the clock back one hour at 2:00 a.m. EDT on the first Sunday in November. The following figure shows an example of daylight savings time application.

Figure 9-1: Example of applying daylight savings time








Legend:  : The time zone applied to the Device.

To set daylight savings time, specify the start and end of the daylight savings time period, in weeks. For that reason, each of the actual start and end dates is determined by the first day of the week in the specified month. For example, if the first day of the week is Wednesday and there are 30 days in the relevant month, the correspondence between the week and the date is as follows:

Figure 9-2: Correspondence between the week and the date (when the first day of the week is Wednesday)

Day	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Sun.
Date			1	2	3	4	5
	6	7	8	9	10	11	12
	13	14	15	16	17	18	19
	20	21	22	23	24	25	26
	27	28	29	30			

Legend:  : 1st week  : 2nd week  : 3rd week
 : 4th week  : 5th week

In this example, the first week is 1st-7th, the second week is 8th-14th, the third week is 15th-21st, the fourth week is 22nd-28th, and the fifth week is 29th-30th. If the fifth week is set and the specified day of the week does not exist in that week, daylight savings time starts or ends on the specified day of the week in the fourth week.

Points to note

To set daylight savings time, you must set an offset from the time zone by using the `clock summer-time` configuration command.

Command examples

1. `(config)# clock timezone EST -5`

Sets the EST time zone and an offset of -5 from UTC.

2. **(config)# clock summer-time EDT recurring 3 2 sun 0200 11 1 sun 0200 offset 60**

Sets EDT for a period between 2:00 a.m. on the second Sunday in March and 2:00 a.m. on the first Sunday in November. During the daylight savings time period, puts the clock 60 minutes ahead of EST.

3. **(config)# save**
(config)# exit

In auto-applied commit mode, saves the settings into the startup configuration by using the `save` command. In manual commit mode, use the `commit` command to apply the settings to the running configuration and save it as the startup configuration.

Then, configuration command mode switches to administrator mode.

4. **# show clock**
Fri Mar 22 15:30:00 EDT 2013

Shows the time of day. Because March 22, 2013 is in the daylight savings time period, the clock is set one hour ahead of EST. Also, the name of the time zone is EDT.

9.3 NTP configuration

9.3.1 List of configuration commands

The following table describes the configuration commands for NTP.

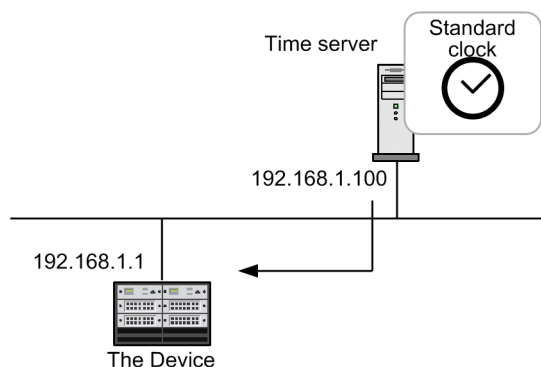
Table 9-3: List of configuration commands

Command name	Description
ntp access-group	Creates an access group that can be permitted or denied access to NTP services by means of an IPv4 address filter.
ntp authenticate	Enables the NTP authentication functionality.
ntp authentication-key	Sets an authentication key.
ntp broadcast	Broadcasts NTP packets to each interface and synchronizes other devices with the Device.
ntp broadcast client	Specifies the setting for accepting NTP broadcast messages from devices on the connected subnet.
ntp broadcastdelay	Specifies the estimated latency (time delay) between the NTP broadcast server sending time information and the Device.
ntp master	Designates the device as a local time server.
ntp peer	Sets NTP server symmetric active/passive mode.
ntp server	Sets client/server mode and specifies client mode for an NTP server.
ntp trusted-key	Sets a key number to perform authentication for security purposes when synchronizing with other devices.

9.3.2 Synchronizing a device with the time server by NTP

Using NTP, synchronize the system clock of the Device with a time server.

Figure 9-3: NTP configuration example (synchronization with a time server)



Points to note

When multiple time servers are configured in the network, the `prefer` parameter of the `ntp server` command selects the time server for synchronizing the system clock of the Device. If you omit the `prefer` parameter, the selected time server will be the one with the least `stratum` value, or a randomly selected time server if they all have the same `stratum` value.

Command examples

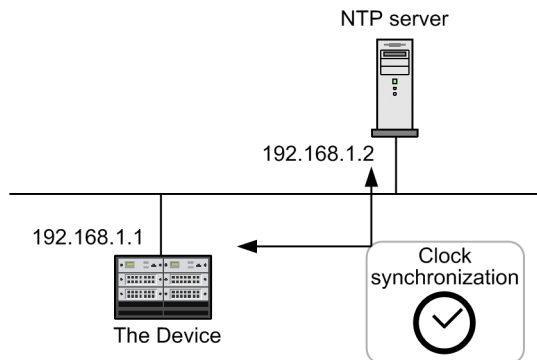
1. **(config)# ntp server 192.168.1.100**

Synchronizes the Device with the time server whose IPv4 address is 192.168.1.100.

9.3.3 Synchronizing a device with an NTP server

Using NTP, synchronize the system clock of the Device with the NTP server, adjusting both time settings.

Figure 9-4: NTP configuration example (synchronization with an NTP server)



Points to note

To synchronize the Device with multiple NTP servers, you must configure multiple settings using the `ntp peer` command.

When multiple NTP servers are configured in the network, the `prefer` parameter of the `ntp peer` command selects the NTP server to be used for synchronizing the Device's system clock. If you omit the `prefer` parameter, the selected NTP server will be the one with the least `stratum` value, or a randomly selected NTP server if they all have the same `stratum` value.

Command examples

1. `(config)# ntp peer 192.168.1.2`

Establishes a peer relationship with the NTP server whose IPv4 address is 192.168.1.2.

9.3.4 Configuring NTP authentication

Points to note

To synchronize the device's clock with other devices using NTP, configure authentication for security purposes.

Command examples

1. `(config)# ntp authenticate`
Enables the NTP authentication functionality.
2. `(config)# ntp authentication-key 1 md5 NtP#001`
Sets NtP#001 in key number 1 as the NTP authentication key.
3. `(config)# ntp trusted-key 1`
Specifies key number 1 for NTP authentication.

9.3.5 Using NTP functionality to synchronize the Device on a VRF

Use the NTP functionality to synchronize time with NTP servers and NTP clients on VRFs.

Points to note

Using the NTP functionality, synchronize the Device system clock with a given NTP server on a VRF. Once the Device's system clock is synchronized to an NTP server, the time of the Device's system clock time can be distributed to multiple NTP clients on all VRFs including the global network.

If the clock-source NTP server and NTP clients are on different VRFs, notify the NTP clients of the referred-to host of the Device as the local time server.

Command examples

1. **(config)# ntp server vrf 10 192.168.1.100**

Synchronizes the Device's system clock to the NTP server with the IPv4 address 192.168.1.100 on VRF 10. The configuration is client/server mode.

2. **(config)# ntp peer vrf 10 192.168.1.100**

Synchronizes the Device's system clock to the NTP server with the IPv4 address 192.168.1.100 on VRF 10. The configuration is symmetric active/passive mode

3. **(config)# ntp broadcast client**

Synchronizes the Device's system clock using NTP broadcast messages. Receives NTP broadcast messages from the NTP server to all subnets within all VRFs including the global network.

4. **(config)# interface gigabitethernet 1/3**

(config-if)# vrf forwarding 20

(config-if)# ip address 192.168.10.1 255.255.255.0

(config-if)# ntp broadcast

Sets NTP broadcasting to the interface with the specified VRF. Once the Device's clock is synchronized to the NTP server, sends NTP broadcast packets to the network of VRF 20, IPv4 address 192.168.10.0, subnet mask 255.255.255.0.

9.4 SNTP configuration

9.4.1 List of configuration commands

The following table describes the configuration commands for SNTP.

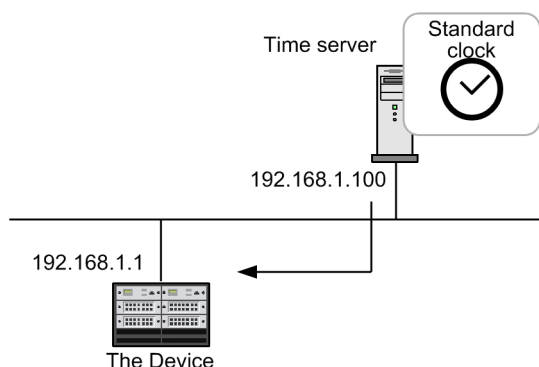
Table 9-4: List of configuration commands

Command name	Description
sntp access-group	Creates an access group that can be permitted or denied access to SNTP services by means of an address filter.
sntp authenticate	Enables the SNTP authentication functionality.
sntp authentication-key	Sets an authentication key.
sntp broadcast	Specifies the transmission of SNTP packets on each interface through broadcast or multicast so that other devices can be synchronized with the Device.
sntp broadcast client	Specifies the setting for accepting SNTP broadcast or multicast messages from devices on the connected subnet.
sntp broadcastdelay	Specifies the estimated latency (time delay) between the SNTP broadcast server or SNTP multicast server sending time information and the Device.
sntp broadcast send-interval	Specifies the sending interval for distributing time information to SNTP clients through broadcast or multicast.
sntp client interval	Specifies the time interval of requesting time information to the SNTP server.
sntp master	Designates the device as a local time server.
sntp server	Sets client/server mode and specifies client mode for an SNTP server.
sntp trusted-key	Sets a key number to perform authentication for security purposes when synchronizing with other devices.

9.4.2 Synchronizing a device with the time server by SNTP

Using SNTP, synchronize the system clock of the Device with a time server.

Figure 9-5: SNTP configuration example (synchronization with a time server)



Command examples

1. (config)# sntp server 192.168.1.100

Synchronizes the Device with the time server whose IPv4 address is 192.168.1.100.

9.4.3 Configuring SNTP authentication

Points to note

To synchronize the device's clock with other devices using SNTP, configure authentication for security purposes.

Command examples

1. **(config)# sntp authenticate**
Enables the SNTP authentication functionality.
2. **(config)# sntp authentication-key 1 md5 Sntp#001**
Sets Sntp#001 in key number 1 as the SNTP authentication key.
3. **(config)# sntp trusted-key 1**
Specifies key number 1 for SNTP authentication.

9.4.4 Using SNTP functionality to synchronize the Device on a VRF

Use the SNTP functionality to synchronize time with SNTP servers and SNTP clients on VRFs.

Points to note

Using the SNTP functionality, synchronize the Device's system clock with a given SNTP server on a VRF. Once the Device's system clock is synchronized to an SNTP server, the time of the Device's system clock can be distributed to multiple SNTP clients on all VRFs including the global network.

If the clock-source SNTP server and SNTP clients are on different VRFs, notify the SNTP clients of the referenced host of the Device as the local time server.

Command examples

1. **(config)# sntp server vrf 10 192.168.1.100**
Synchronizes the Device's system clock to the SNTP server with the IPv4 address 192.168.1.100 on VRF 10. The configuration is client/server mode.
2. **(config)# sntp broadcast client**
Synchronizes the Device's system clock using SNTP broadcast messages. Receives SNTP broadcast messages from the SNTP server to all subnets within all VRFs including the global network.
3. **(config)# interface gigabitethernet 1/4**
(config-if)# vrf forwarding 20
(config-if)# ip address 192.168.10.1 255.255.255.0
(config-if)# sntp broadcast ip
Sets SNTP broadcasting to the interface with the specified VRF. Once the Device's clock is synchronized to the SNTP server, sends SNTP broadcast packets to the network of VRF 20, IPv4 address 192.168.10.0, subnet mask 255.255.255.0.

9.5 Operation

9.5.1 List of operation commands

The following table describes the operation commands for time settings, NTP, and SNTP.

Table 9-5: List of operation commands

Command name	Description
show clock	Shows the current date and time.
show ntp associations	Shows the activity status of the connected NTP server.
restart ntp	Restarts the local NTP server.
set clock sntp	Manually synchronizes the clock with the SNTP server.
show sntp status	Shows the activity status of the connected SNTP server.
restart sntp	Restarts the local SNTP server.

9.5.2 Checking the time, NTP status, and SNTP status

(1) Checking the time

Using the `show clock` command, you can check the time information set in the Device. An example is shown below:

Figure 9-6: Checking the time settings

```
> show clock
Wed Mar 22 15:30:00 UTC 20XX
>
```

(2) Checking the operating status of NTP

If the Device's system clock is synchronized with an NTP server on the network by NTP, you can check the operating status of the NTP server with which the Device is currently synchronized by using the `show ntp associations` command. An example is shown below:

Figure 9-7: Checking the activity status of the NTP server

```
> show ntp associations
Date 20XX/05/01 12:00:00 UTC
  remote      refid      st t when poll reach  delay  offset  disp
=====
*timesvr     192.168.1.100      3 u   1   64  377    0.89   -2.827   0.27
>
```

(3) Checking the operating status of SNTP

If the Device's system clock is synchronized with an SNTP server on the network by SNTP, you can check the operating status of the SNTP server with which the Device is currently synchronized by using the `show sntp status` command. An example is shown below:

Figure 9-8: Checking the activity status of the SNTP server

```
> show sntp status
Date 20XX/05/01 12:00:00 UTC
Last SNTP Status
Current server: 192.168.1.100 VRF 30
Status:synchronize
Mode : Unicast, Lapsed time : 14(s), Offset : 1(s)
Poll interval: 16
Configured SNTP Status
  SNTP server 2001:db8::1 priority 50
>
```

9. Time Settings, NTP, and SNTP

```
SNTP server 2001:db5::100 VRF 10 priority 20
*SNTP server 192.168.1.100 VRF 30 priority 10
SNTP broadcast 192.168.2.255 VRF 20
>
```

Chapter

10. Host Names and DNS

This chapter describes host names and the Domain Name System (DNS), and describes how to use them.

10.1 Description

10.2 Configuration

10.1 Description

10.1.1 Overview

Host name information for identifying other devices on the network can be set in the Device. This information can be used to specify another networked device when configuring the Device to perform logging, for example. You can set host name information in the Device by using either of the following methods:

- Specify host names individually using the `ip host` or `ipv6 host` configuration command.
- Query the DNS server on the network using the DNS resolver functionality.

When setting host names by using the `ip host` or `ipv6 host` configuration command, you must explicitly associate an IP address with each host name to be used. When using the DNS resolver, there is no need to map IP addresses with referenced host names because the Device looks them up by querying the DNS server.

If you set a host name by using the `ip host` or `ipv6 host` configuration command and also use the DNS resolver, the host name set in the configuration command takes priority. If you set the same host name for IPv4 and IPv6 by using `ip host` and `ipv6 host`, IPv4 takes priority. If the DNS resolver functionality makes inquiries about the host names set for both IPv4 and IPv6, IPv6 takes priority.

The DNS resolver functionality provided by the Device complies with RFC 1034 and RFC 1035.

10.1.2 Notes on host names and DNS

If the DNS server IP address is not correctly set in the Device or if the reverse lookup functionality (functionality for using an IP address to search for a host name) does not work for the DNS server, it takes time to detect that communication with the DNS server or reverse lookup is not possible. In this case, the Device operation might be affected. For example, it takes a long time until the login prompt appears during a remote connection to the Device via Telnet.

You can check the status of connections with the DNS server by using the `nslookup` operation command. Note that you can disable the reverse lookup functionality by using the `no ip domain reverse-lookup` configuration command.

10.2 Configuration

10.2.1 List of configuration commands

The following table describes the configuration commands for host names and the DNS.

Table 10-1: List of configuration commands

Command name	Description
ip domain lookup	Disables or enables the DNS resolver functionality.
ip domain name	Sets the domain name to be used by the DNS resolver.
ip host	Sets host name information mapped to an IPv4 address.
ip name-server	Sets the name server referenced by the DNS resolver.
ipv6 host	Sets host name information mapped to an IPv6 address.

10.2.2 Configuring host names

(1) Mapping a host name to an IPv4 address

Points to note

The example below shows how to map a host name to an IPv4 address.

Command examples

1. **(config)# ip host WORKPC1 192.168.0.1**

Maps the host name WORKPC1 to the device whose IPv4 address is 192.168.0.1.

(2) Mapping a host name to an IPv6 address

Points to note

The example below shows how to map a host name to an IPv6 address.

Command examples

1. **(config)# ipv6 host WORKPC2 2001:db8:10::100**

Maps the host name WORKPC2 to the device whose IPv6 address is 2001:db8:10::100.

10.2.3 Configuring DNS settings

(1) DNS resolver setting

Points to note

The example below shows how to set the domain name to be used by the DNS resolver, and the name server that the DNS resolver looks up. Because the DNS resolver functionality is enabled by default, it works as soon as the name server has been set. Note that queries to the name servers are sent in the specified order.

Command examples

1. **(config)# ip domain name router.example.com**

Set the domain name as router.example.com.

2. **(config)# ip name-server 192.168.0.1**

Sets 192.168.0.1 for the name server. When referencing host name information, the Device queries this name server first.

3. **(config)# ip name-server 2001:db8::1**

Sets 2001:db8::1 for the name server. The Device queries this name server if the Device cannot query the name server whose address is 192.168.0.1.

4. **(config)# ip name-server 192.168.0.2**

Sets 192.168.0.2 for the name server. The Device queries this name server if the Device cannot query the name servers whose addresses are 192.168.0.1 and 2001:db8::1.

(2) Disabling the DNS resolver

Points to note

The example below shows how to disable the DNS resolver functionality.

Command examples

1. **(config)# no ip domain lookup**

Disables the DNS resolver functionality.

Chapter

11. Device Management

This chapter describes all aspects of managing the Device.

- 11.1 System operation panel
- 11.2 Configuring the device resources
- 11.3 Checking the Device
- 11.4 Managing SFU, PRU, and NIF
- 11.5 Backing up and restoring operating information
- 11.6 Failure recovery

11.1 System operation panel

The system operation panel incorporated in a BCU can display device information, operation instructions, and failure information.

The system operation panel is provided with a 16-digit, two-line LCD and three operation keys: the **BACK** key (◀), **ENTR** key (■), and **FWRD** key (▶). In addition to being able to display information about a failure occurring in the Device, the system operation panel can display device information, operation instructions, and failure information when you operate its keys and move through a hierarchical menu.

As basic operations of the system operation panel, use the **BACK** key and the **FWRD** key to move to and select an item, and use the **ENTR** key to apply the selection. For example, if you want to inactivate a board, in **Main Menu**, select **ACTION** and press the **ENTR** key. Then, in **ACTION**, select **INACT** and press the **ENTR** key.

When you perform a key operation in the system operation panel, the LCD is turned on. Also when failure information is displayed, the LCD is automatically turned on. If you do not perform a key operation for 60 seconds and there is no failure information displayed, the LCD is turned off.

11.1.1 Startup messages

(1) POST message

In the Device, BCU performs a self-diagnosis test (hardware diagnosis) at startup. At this time, a POST (Power On Self Test) message appears on the LCD, indicating the progress of the initial diagnosis of the Device.

Figure 11-1: Example of a displayed POST message



Table 11-1: Items displayed in a POST message

Displayed location	Displayed information
Top	POST code
Bottom	(Empty line)

(2) BOOT message

When BCU completes a self-diagnosis test, the Device starts. At this time, a message appears on the LCD, indicating the startup status of the Device.

Figure 11-2: Example of a displayed BOOT message



Table 11-2: Items displayed in a BOOT message


Displayed location	Displayed information
Top	BOOT status message

Displayed location	Displayed information
Bottom	(Empty line)

(3) Stop message

If an anomaly is detected during initial diagnosis at startup, a BCU failure occurs, or the user stops BCU through command operation, a message appears on the LCD, indicating that the Device is stopped.

Figure 11-3: Example of a displayed stop message



[BOOT] HALT

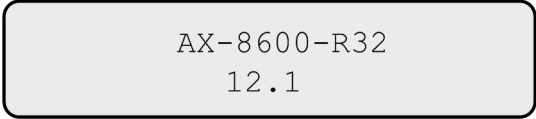
Table 11-3: Items displayed in a stop message

Displayed location	Displayed information
Top	Stop status message (1st half)
Bottom	Stop status message (2nd half) No message might be displayed.

(4) Idle state

When the Device has started completely, the LCD displays the model and software version. This state is called an idle state.

Figure 11-4: Example of a displayed idle state



AX-8600-R32
12.1

Table 11-4: Items displayed for the idle state

Displayed location	Displayed information
Top	Device model
Bottom	Software version

If the identification name has been set by the `hostname` configuration command, after the device model and software version are displayed for five seconds, the device identification name is displayed on the bottom line of the LCD.

Figure 11-5: Example of a displayed device identification name



east-01

Table 11-5: Items displayed for the device identification name

Displayed location	Displayed information
Top	(Empty line)
Bottom	Device identification name If the name is 17 or more characters, the name is displayed by scrolling one character at a time to the left. After the last character is displayed, the display starts from the first character again.

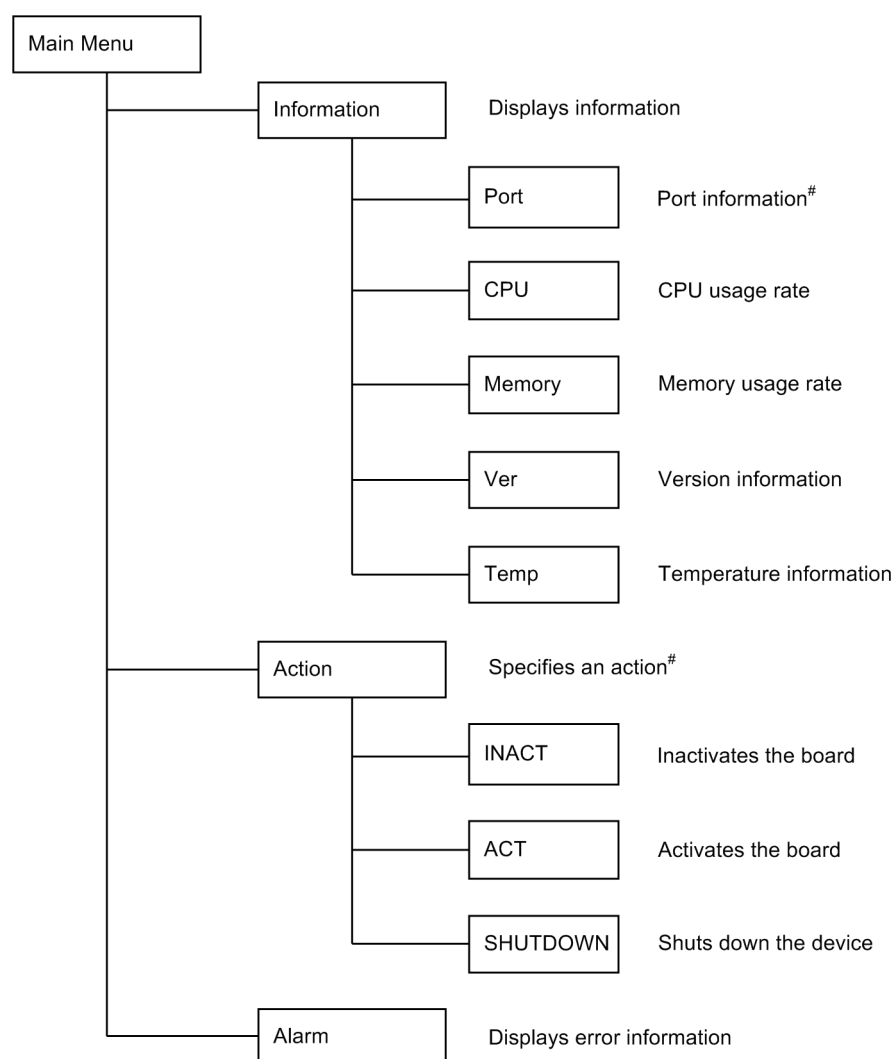
11.1.2 Menu structure

The figure below shows the menu structure under **Main Menu**.

To return to the upper level menu, select the up arrow (↑) by using the **BACK** key and the **FWRD** key and then press the **ENTR** key. To return to **Main Menu**, select x by using the **BACK** key and the **FWRD** key and then press the **ENTR** key. Note that after a certain period of time passes without key operation, the display returns to **Main Menu**.

If you do not perform a key operation for 30 seconds after **Main Menu** is displayed, the idle state display appears.

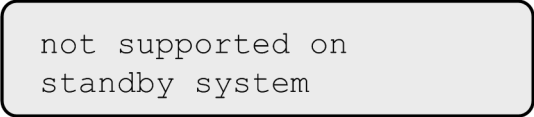
Figure 11-6: Menu structure



#: This item cannot be operated by the standby BCU.

If an item in a menu that is not operable by the standby BCU is selected, `not supported on standby system` is displayed for three seconds, and **Main Menu** automatically appears again.

Figure 11-7: Display when a menu item inoperable by the standby BCU is selected




```
not supported on
standby system
```

11.1.3 Displaying port information

The display of port information shows the status of the interface that has the selected port number. In **INFORMATION**, select **Port** and press the **ENTR** key to display the screen for selecting a NIF number.

If there is no active NIF, `No Active NIF` is displayed for three seconds, and then **Main Menu** automatically appears again.

Figure 11-8: Display when there is no active NIF




```
No Active NIF
```

(1) NIF number selection

In the screen for selecting a NIF number of the port to be displayed, press the **FWRD** key to display the selectable NIF numbers in ascending order. If a NIF is not active, its NIF number is skipped. If you press the **BACK** key, the selectable NIF numbers are displayed in reverse order of the numbers displayed when you press the **FWRD** key. Select the NIF number of the port whose information you want to display and apply the selection by pressing the **ENTR** key. Information about that port is displayed.

Figure 11-9: Example of a displayed NIF number selection



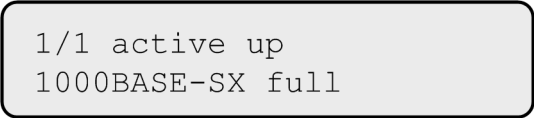
```
Which NIF?
NIF No.  < 01 >
```

(2) Port information display

The display of port information shows the status of a physical interface. Press the **FWRD** key to display the information of the next port. Press the **BACK** key to display the port information in reverse order (backward). If there are multiple active NIFs, you can display the desired port information by using the **FWRD** and **BACK** keys to skip NIFs.

To return to **Main Menu**, press the **ENTR** key. Note that if you do not perform a key operation for 30 seconds, **Main Menu** automatically appears again.

Figure 11-10: Example of displayed port information



```
1/1 active up
1000BASE-SX full
```

Table 11-6: Items displayed for the port information

Category	Model name	Meaning
Port installed position	<nif no.>/<port no.>	<nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Port status	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Initializing or waiting for negotiation to be established
	fault	Failed
	inactive	Stopped by an operation command
	disable	Stopped by a configuration command
	standby	Standby state activated by the standby link functionality of link aggregation
	suspend	Suspension of port startup associated with a shortage of operating SFUs or with PRU initialization
	unused	Unused (no configuration)
	mismatch	Mismatch between a installed NIF and configuration
Line speed	For details about the line speed, see the display item <i>Speed</i> of the <code>show port</code> operation command.	
Full duplex or half duplex	For details about full duplex and half duplex, see the display item <i>Duplex</i> of the <code>show port</code> operation command.	

11.1.4 Displaying CPU usage rate

You can display the CPU usage rates of the BCU-CPU, PA, and PRU-CPU. In **INFORMATION**, select **CPU** and press the **ENTR** key to display a CPU usage rate.

(1) CPU type selection

While a CPU usage rate is displayed, press the **FWRD** key to display the CPU types, one at a time, in the following order: BCU-CPU, PA, and PRU-CPU (PRU number). If you press the **BACK** key, the CPU types are displayed in reverse order of the types displayed when you press the **FWRD** key.

(2) CPU usage rate

A CPU usage rate is displayed in a horizontal bar graph in increments of 2%. The displayed graph is updated to the latest information every five seconds.

To return to **Main Menu**, press the **ENTR** key. Note that if you do not perform a key operation for one hour, **Main Menu** automatically appears again.

Figure 11-11: Example of displaying the CPU usage rate



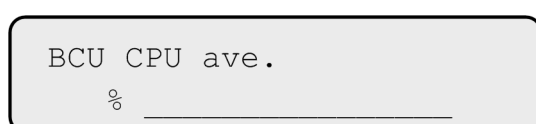
Table 11-7: Items displayed for the CPU usage rate

Display items	Displayed information
BCU CPU ave.	Average value (%) for the CPU usage rate of the BCU-CPU obtained through aggregation of data for one second Displays information about the local system.
PA ave.	Average value (%) for the CPU usage rate of the PA obtained through aggregation of data for one second Displays information about the local system.
PRU<pru no.> CPU ave.	Average value (%) for the CPU usage rate of the PRU-CPU obtained through aggregation of data for one second <pru no.>: PRU number

Initialize is displayed in the bottom line of the LCD in any of the following cases: When a CPU usage rate is displayed, the PRU has not yet started completely or the first CPU usage rate measurement has not yet been completed. In addition, when the operating status of the PRU is not active, the operating status of the PRU is displayed in the bottom line of the LCD.

If a CPU usage rate cannot be obtained, no value is displayed. In the next update, a CPU usage rate is obtained again.

Figure 11-12: Display when a CPU usage rate fails to be obtained



11.1.5 Displaying memory usage rate

You can display the memory usage rates of the BCU-CPU, PA, and PRU-CPU. In **INFORMATION**, select **Memory** and press the **ENTR** key to display a memory usage rate.

(1) CPU type selection

While a memory usage rate is displayed, press the **FWRD** key to display the CPU types, one at a time, in the following order: BCU-CPU, PA, and PRU-CPU (PRU number). If you press the **BACK** key, the CPU types are displayed in reverse order of the types displayed when you press the **FWRD** key.

(2) Memory usage rate

A memory usage rate is displayed in a horizontal bar graph in increments of 2%. The displayed graph is updated to the latest every five seconds. When the memory usage rate for the BCU-CPU or PRU-CPU is displayed, the CPU type is displayed at the top by scrolling.

To return to **Main Menu**, press the **ENTR** key. Note that if you do not perform a key operation for one hour, **Main Menu** automatically appears again.

Figure 11-13: Example of displaying the memory usage rate



Table 11-8: Items displayed for the memory usage rate

Display items	Displayed information
BCU memory usage	Usage rate (%) of the memory installed in the BCU-CPU Displays information about the local system.

Display items	Displayed information
PA memory usage	Usage rate (%) of the memory installed in the PA Displays information about the local system.
PRU<pru no.> memory usage	Usage rate (%) of the memory installed in the PRU-CPU <pru no.>: PRU number

If the operating status of the PRU is not active when the usage rate of a memory is displayed, the operating status of the PRU is displayed in the bottom line of the LCD.

11.1.6 Displaying the version

You can display information about the Device software and the installed boards (model, serial information, and operating time). In **INFORMATION**, select **ver** and press the **ENTR** key to display the version.

(1) Selecting a display target

If you press the **FWRD** key while the version is displayed, display targets are shown in the order below. If you press the **BACK** key, the display targets are shown in reverse order of the display targets shown when you press the **FWRD** key

1. Model
2. Software
3. BCU (BCU number)
4. SFU (SFU number)
5. PRU (PRU number)
6. NIF (NIF number)
7. Power supply unit (power supply unit slot number)
8. Fan unit (fan unit slot number)

For the standby BCU, the display of items from 4. SFU to 8. Fan unit is skipped.

(2) Displaying the version

When you select a display target, its model is displayed first. In this state, press the **ENTR** key to change the display to the following order: serial information and operating time. If you press the **FWRD** key while a model, serial information, or operating time is displayed, the model of the next display target is displayed. If you press the **BACK** key, the targets are displayed in reverse order of the targets displayed when you press the **FWRD** key.

To return to **Main Menu**, press the **ENTR** key while the operating time is displayed (serial information will be displayed if the display target is a model or software). Note that if you do not perform a key operation for 30 seconds, **Main Menu** automatically appears again.

Table 11-9: List of display items when the version is displayed

Display target	Model	Serial information	Operating time
Model	Device model	Device serial information	--
Software	Software model	Software version	--
Board	BCU model	BCU serial information	BCU operating time
	SFU model	SFU serial information	SFU operating time
	PRU model	PRU serial information	PRU operating time
	NIF model	NIF serial information	NIF operating time

Display target	Model	Serial information	Operating time
Power supply unit	Power supply unit model	Power supply unit serial information	Power supply unit operating time
Fan unit	Fan unit model	Fan unit serial information	Fan unit operating time

Legend: --: Not applicable

(a) Model

Figure 11-14: Example of displaying the model

MODEL
AX-8600-R32

Table 11-10: Items displayed for the model

Displayed location	Displayed information
Top	Fixed as MODEL.
Bottom	Device model

Figure 11-15: Example of displaying the software model

OS-RE
AX-P8600-R2

Table 11-11: Items displayed for the software model

Displayed location	Displayed information
Top	Software abbreviation
Bottom	Software model Displays information about the local system.

Figure 11-16: Example of displaying the board model (NIF)

[1]NL1G-12T
AX-F8600-711T

Table 11-12: Items displayed for the board model

Displayed location	Displayed information
Top	[board-installed-slot-number] + abbreviated-name-of-the-board When the operating status of the board is displayed at the bottom, the abbreviated name of the board is not displayed.
Bottom	Board model [#]

[#]: The details to be displayed for each model vary depending on the operating status of the board, power supply unit, or fan unit. The following table describes model display conditions by operating status.

Table 11-13: Model display conditions by operating status of the board, power supply unit, or fan unit

Operating status of the board, power supply unit, or fan unit	BCU	SFU	PRU	NIF	Power supply unit	Fan unit
active	Y	Y	Y	Y	Y	Y
standby	Y	--	--	--	--	--
initialize	Y	Y	Y	Y	--	--
disable (board installed)	--	Y	Y	Y	--	--
disable (board not installed)	--	N	N	N	--	--
inactive	Y	Y	Y	Y	--	--
notconnect	N	N	N	N	N	N
fault	Y	Y	Y	Y	Y [#]	Y [#]
power shortage	--	--	Y	Y	--	--
notsupport	N	N	N	N	N	N
connect	--	--	--	--	N	--
unknown	--	N	N	N	--	--

Legend: Y: Displays the board model; N: Displays the operating status of the board, power supply unit, or fan unit; --: Not applicable

#: If a hardware failure occurs, the model and abbreviated name might be unobtainable.

(b) Serial information

Figure 11-17: Example of displaying the software version

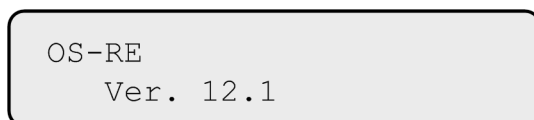


Table 11-14: Items displayed for the software version

Displayed location	Displayed information
Top	Software abbreviation
Bottom	Software version Displays information about the local system.

Figure 11-18: Example of displayed serial information



Table 11-15: Items displayed in the serial information

Displayed location	Displayed information
Top	Fixed as SI.

Displayed location	Displayed information
Bottom	Serial information [#] Information is displayed by scrolling one character at a time to the left. After the last character is displayed, the display starts from the first character again.

[#]: The details to be displayed for serial information vary depending on the operating status of the board, power supply unit, or fan unit. The following table describes serial information display conditions by operating status.

Table 11-16: Serial information display conditions by operating status of the board, power supply unit, or fan unit

Operating status of the board, power supply unit, or fan unit	BCU	SFU	PRU	NIF	Power supply unit	Fan unit
active	Y	Y	Y	Y	Y	Y
standby	Y	--	--	--	--	--
initialize	Y	Y	Y	Y	--	--
disable (board installed)	--	Y	Y	Y	--	--
disable (board not installed)	--	N	N	N	--	--
inactive	Y	Y	Y	Y	--	--
notconnect	N	N	N	N	N	N
fault	Y	Y	Y	Y	Y [#]	Y [#]
power shortage	--	--	Y	Y	--	--
notsupport	Y	Y	Y	Y	Y	Y
connect	--	--	--	--	N	--
unknown	--	N	N	N	--	--

Legend: Y: Displays serial information; N: Displays the operating status of the board, power supply unit, or fan unit; --: Not applicable

[#]: If a hardware failure occurs, the serial information might be unobtainable.

(c) Operating time

Two types of operating times are alternately displayed every five seconds: `Runtime Total` (total operating time) and `Runtime Caution` (total operating time in the caution status in which the inlet temperature is high).

Figure 11-19: Example of displaying the operating time

Runtime Total 120 days 8 hours

Table 11-17: Items displayed for the operating time

Displayed location	Displayed information
Top	Runtime Total: Cumulative operating time Runtime Caution: Cumulative operating time in the caution status in which the inlet temperature is high

Displayed location	Displayed information
Bottom	The operating time of the type indicated at the top (days: days and hours: hours) [#]

[#]: The details to be displayed for operating time vary depending on the operating status of the board, power supply unit, or fan unit. The following table describes operating time display conditions by operating status.

Table 11-18: Operating time display conditions by operating status of the board, power supply unit, or fan unit

Operating status of the board, power supply unit, or fan unit	BCU	SFU	PRU	NIF	Power supply unit	Fan unit
active	Y	Y	Y	Y	Y	Y
standby	Y	--	--	--	--	--
initialize	Y	N	N	N	--	--
disable (board installed)	--	N	N	N	--	--
disable (board not installed)	--	N	N	N	--	--
inactive	N	N	N	N	--	--
notconnect	N	N	N	N	N	N
fault	N	N	N	N	N	N
power shortage	--	--	N	N	--	--
notsupport	N	N	N	N	N	N
connect	--	--	--	--	N	--
unknown	--	N	N	N	--	--

Legend: Y: Displays the operating time; N: Displays the operating status of the board, power supply unit, or fan unit; --: Not applicable

11.1.7 Displaying temperature information

You can display the inlet temperature of the BCU. In **INFORMATION**, select **Temp** and press the **ENTR** key to display temperature information.

(1) Temperature

The inlet temperature (centigrade) and temperature status of BCU are displayed. The displayed details do not change even if you press the **FWRD** or **BACK** key.

To return to **Main Menu**, press the **ENTR** key. Note that if you do not perform a key operation for 30 seconds, **Main Menu** automatically appears again.

Figure 11-20: Example of displayed temperature information

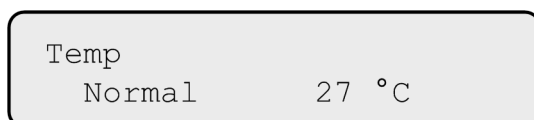


Table 11-19: Items displayed in the temperature information

Displayed location	Displayed information
Top	Fixed as Temp.

Displayed location	Displayed information
Bottom	Temperature status [#] <ul style="list-style-type: none"> • Normal: Normal • Caution: High or low temperature caution • Critical: High temperature warning • Fault: Stop due to high temperature Displays information about the local system.
	BCU inlet temperature (centigrade)

[#]: For details about the temperature status, see *11.3.6 Monitoring temperatures*.

11.1.8 Replacing boards

With the power turned on, you can instruct board replacement from the system operation panel. The following boards are replaceable:

- Standby BCU
- SFU
- PRU
- NIF

The following provides an overview of the procedure for replacing boards while the power is turned on:

1. Select and execute **INACT** in the system operation panel to inactivate the board.
2. Remove the board inactivated in step 1.
3. Install a replacement board.
4. Select and execute **ACT** in the system operation panel to activate the board.

For details about how to replace boards, see the *Hardware Instruction Manual*.

(1) **Selecting a board to be inactivated or activated**

To inactivate a board:

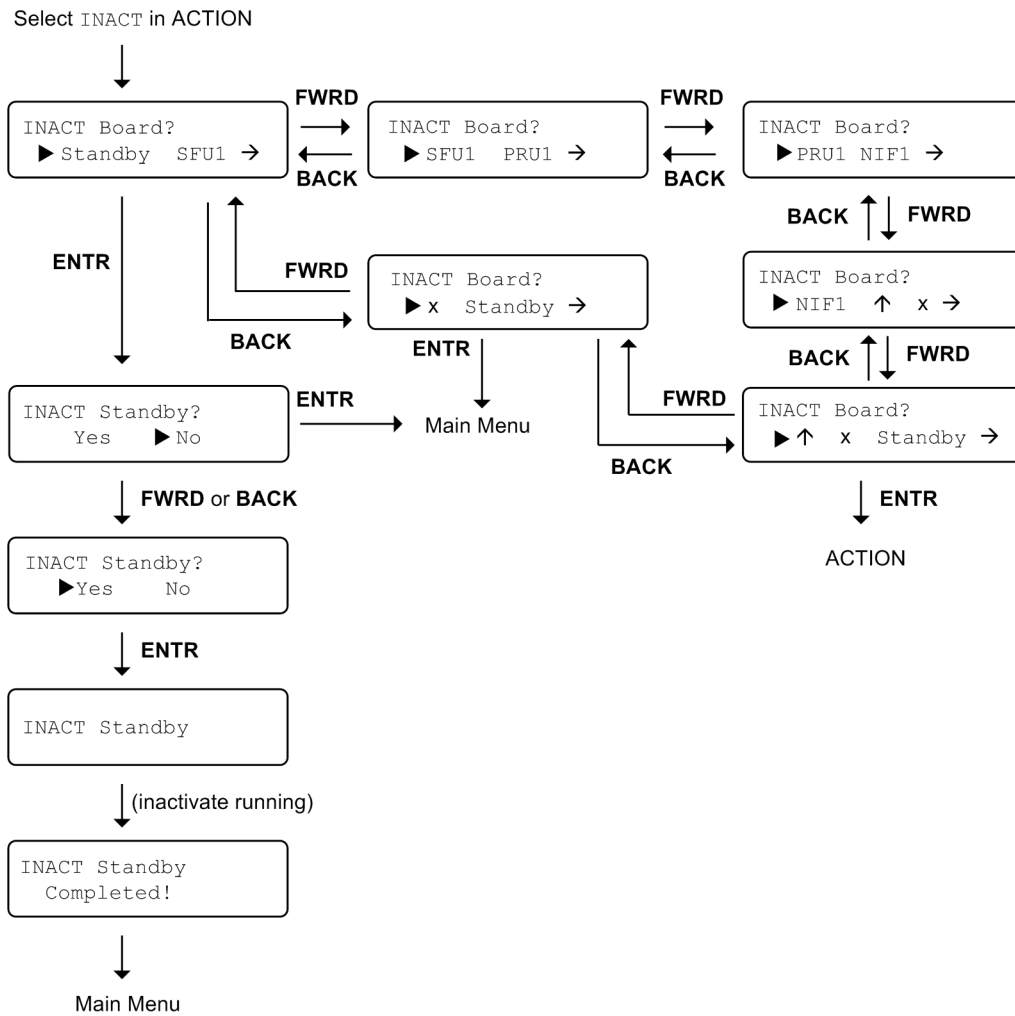
In **ACTION**, select **INACT** and press the **ENTR** key to display the screen for selecting the board to be inactivated.

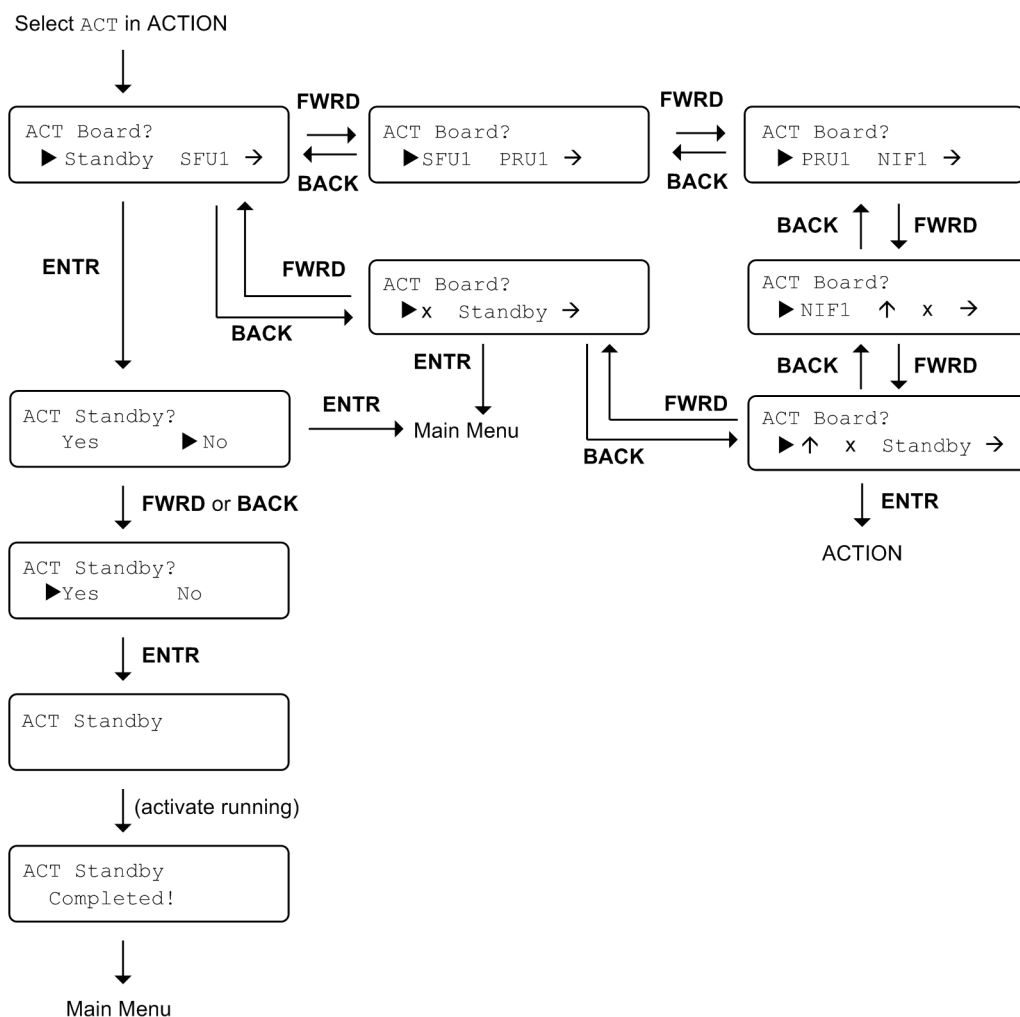
To activate a board:

In **ACTION**, select **ACT** and press the **ENTR** key to display the screen for selecting the board to be activated.

(2) **Suppression of the display of other information**

During instructions for board replacement, failure information is not displayed.

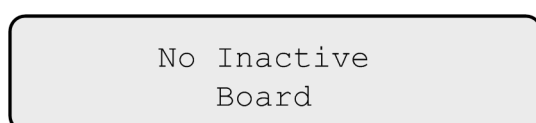
(3) Inactivating a board*Figure 11-21: Procedure for inactivating a board*

(4) Activating a board*Figure 11-22: Procedure for activating a board***(5) Display when there is no board to be inactivated or activated**

If no board can be inactivated when you select **INACT** from **ACTION**, **No Active Board** is displayed for three seconds and then **Main Menu** automatically appears again.

Figure 11-23: Display when there is no board to be inactivated

If there is no board that can be activated when **ACT** is selected in **ACTION**, **No Inactive Board** is displayed for three seconds and then **Main Menu** automatically appears again.

Figure 11-24: Display when there is no board to be activated

11.1.9 Stop procedure

You can send an instruction to stop the Device from the system operation panel. To restart the Device after you stop it from the system operation panel, turn the power switch off once and then turn the power switch on.

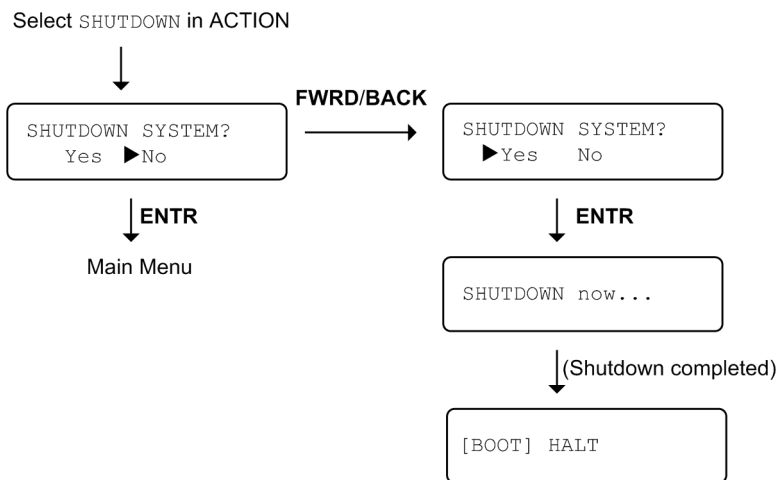
In **ACTION**, select **SHUTDOWN** and press the **ENTR** key to display the screen for confirming that the Device has stopped.

(1) Suppression of the display of other information

During instructions for stopping the Device, failure information is not displayed.

(2) Operating the system operation panel to stop the Device

Figure 11-25: Operation procedure for stopping the Device



11.1.10 Displaying a failure

If a failure occurs in the Device or if **Alarm** is selected in **Main Menu** during the occurrence of a Device failure, the system operation panel displays the failure to help identify the failed area or functionality. When **SYSTEM1 LED** on a BCU is lit red, the failure display indicates that a device failure occurred. When **SYSTEM1 LED** on a BCU is flashing green, the failure display indicates that a partial device failure occurred.

Among the output system messages, the failure display shows messages related to failures that require action (event level S1 to S4). At that time, a failure is displayed with priority given to a smaller event level number.

When all the failed areas have been recovered, the failure display automatically disappears and **SYSTEM1 LED** is lit green again.

(1) Failure display

When a failure occurs, the LCD is turned on to display a message type and message ID together with an event level. To display the message text regarding the failure, press the **ENTR** key. To display **Main Menu**, press the **ENTR** key again. The message text moves to the left and is displayed repeatedly.

Figure 11-26: Example of displayed failure information (a hardware failure was detected in a NIF)

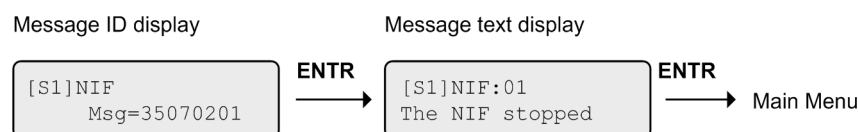


Table 11-20: Items displayed for the message ID

Displayed location	Displayed information
Top	[Sx] : Event level (x: Event level number)
	Message type
Bottom	Message ID

Table 11-21: Items displayed in the message text

Displayed location	Displayed information
Top	[Sx] : Event level (x: Event level number)
	Message type detailed information
Bottom	Message text If the name is 17 or more characters, the name is displayed by scrolling one character at a time to the left. After the last character is displayed, the display starts from the first character again.

(2) Menu display while a failure is displayed

If you want to display **Main Menu** to view device information or specify operation instructions while a failure is displayed, press the **ENTR** key twice in the message ID display, or press the **ENTR** key once in the message text display.

In any of the following cases, the display state returns from the menu display to the failure display:

- If a failure occurs in a state other than when you are specifying operation instructions
- If the Device does not recover from the failure after 10 seconds have passed since **Main Menu** was displayed
- If **Alarm** is selected in **Main Menu**

(3) Relationship with the display of other information


Even though other information is displayed, a failure is displayed first when it occurs. However, while you are specifying operation instructions, a failure is not displayed if it occurs. The failure is displayed after you finish specifying the operation instructions.

(4) Failure display when multiple faults occur

If only one fault occurs, the event level is displayed between square brackets ([]). If multiple faults occur, the event level is displayed between double square brackets ([[]]).

If multiple faults occur, pressing the **FWRD** or **BACK** key switches the display of failure details in ascending order of the faults' event level numbers (if the levels are the same, the order is the order of occurrence) while the display mode is sustained. For example, if a message ID is displayed, other message IDs are displayed, and if message text is displayed, other message text is displayed. If the displayed fault is not a fault with the smallest event level number (for the same event level, the oldest fault), the fault is displayed for 30 seconds, and then the failure display returns to the display of the fault that has the smallest event level number and is the oldest.

Figure 11-27: Failure display when multiple faults occur



```
[ [S1] ] NIF
Msg=35070201
```

(5) Display when there is no failure

If there is no failure when Alarm is selected in **Main Menu**, No Error is displayed for three seconds and then **Main Menu** automatically appears again.

Figure 11-28: Display when there is no failure



11.2 Configuring the device resources

11.2.1 Lists of configuration commands and operation commands

The following table describes the configuration commands for the device resource setting.

Table 11-22: List of configuration commands

Command name	Description
flow-table allocation	Sets the allocation pattern for the number of entries in a flow-type table for the Device.
forwarding-table allocation	Sets the allocation pattern for the number of entries in a route-type table for the Device.

The following table describes the operation commands for the device resource setting.

Table 11-23: List of operation commands

Command name	Description
show pru resources	Shows the operation status and resource usage status of PRUs.

11.2.2 Specifying the table entry allocation pattern

The Device has two types of table entry allocation patterns, route-type table entry allocation and flow-type table entry allocation. You can specify the settings for these two patterns by using the `forwarding-table allocation` configuration command and the `flow-table allocation` configuration command respectively.

You can check information about each allocation pattern and about the number of entries in each table by using the `show pru resources` operation command.

(1) Route-type table entry settings

Points to note

The initial status of a route-type table entry is `default`. After completing the setting, restart all the PRUs to apply the specified route-type table entry allocation pattern.

Command examples

1. **(config)# forwarding-table allocation ipv4-uni**

Enters global configuration mode and sets the route-type table entry allocation pattern as priority given to IPv4 unicast.

(2) Flow-type table entry settings

Points to note

The initial status of a flow-type table entry is `default`. After completing the setting, restart all the PRUs to apply the specified flow-type table entry allocation pattern.

Command examples

1. **(config)# flow-table allocation filter**

Enters global configuration mode and sets the flow-type table entry allocation pattern as priority given to filters.

11.3 Checking the Device

11.3.1 Lists of configuration commands and operation commands

The following tables describe the configuration commands and operation commands for checking the device.

Table 11-24: List of configuration commands (identification name setting)

Command name	Description
hostname	Sets the identification name of a Device.

Table 11-25: List of configuration commands (device operation setting)

Command name	Description
system fan mode	Sets the operating mode of the fan.
system high-temperature-action	Sets the operating mode of a BCU when the inlet temperature of the BCU exceeds the guaranteed operating range.
system temperature-warning-level	Outputs a temperature warning system message when the inlet temperature of the Device reaches or exceeds the specified temperature. Also outputs a temperature recovery system message when the inlet temperature of the Device drops by 3 degrees Celsius or more after reaching or exceeding the specified temperature.
system temperature-warning-level average	Outputs a system message when the average inlet temperature of the Device reaches or exceeds the specified temperature.

Table 11-26: List of operation commands (checking the software version and device status)

Command name	Description
show version	Shows version information and information about the installed boards.
show system	Shows the operating status of the device.
show environment	Shows information about the device's environment.
reload	Restarts the device, and collects the log data at that time. During normal operation, a BCU memory dump is collected.
show tech-support	Shows information about the status of the hardware and software required for technical support.
show power	Shows the elapsed time of the device and the power consumption and cumulative power consumption of each board.

Table 11-27: List of operation commands (checking the internal flash memory and memory card)

Command name	Description
show mc [#]	Shows the usage status of the memory card.
format mc [#]	Formats the memory card for use by the Device.
show flash [#]	Shows internal flash memory usage.

#

See 12. *Checking Internal Memory and Memory Cards* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

Table 11-28: List of operation commands (checking resource information and dump information)

Command name	Description
show cpu ^{#1}	Shows CPU usage.
show processes ^{#1}	Shows information about processes being executed on the device.
show memory ^{#1}	Shows the installed capacity, used capacity, and free capacity of the physical memory of the Device.
df ^{#1}	Shows the available disk space.
du ^{#1}	Shows the amount of space being used by the files in a directory.
erase dumpfile ^{#2}	Erases dump files on the dump file storage directory or core files on the core file storage directory.
show dumpfile ^{#2}	Shows a list of dump files on the dump file storage directory or core files on the core file storage directory.

#1

See 13. *Resource Information* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

#2

See 14. *Dump Information* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

11.3.2 Checking the software version

By using the `show version` operation command, you can check version information and information about the installed boards. The version information shows the version of the currently running software. If software is updated but the new software is not applied to operation, the installed version is shown between parentheses (). An example is shown below.

Figure 11-29: Checking the software version

```
> show version software
Date 20XX/04/01 02:54:45 UTC
BCU1: AX-P8600-R2, OS-RE, Ver.12.1
      BCU-CPU: Ver.12.1
      BCU-CPU Boot ROM: Ver.0.0.2
      PA: Ver.12.1
      PA Boot ROM: Ver.2.1.12
      HDC: Ver.0.3
BCU2: notconnect
SFU1: HDC: Ver.1.18
SFU2: notconnect
SFU3: notconnect
SFU4: notconnect
PRU1: PRU-CPU: Ver.12.1
      PRU-CPU Boot ROM: Ver.2.1.4
      HDC: Ver.0.16
PRU2: notconnect
PRU3: notconnect
PRU4: notconnect
NIF1: HDC: Ver.0.19
NIF2: notconnect
:
NIF16: notconnect
```

>

11.3.3 Checking the device status

(1) Operation status check

By using the `show system operation` command, you can check the following information:

- Information about the device
- Information about fans, power supply units, and boards (BCU, SFU, PRU, and NIF).

An example is shown below.

Figure 11-30: Checking the operation status

```
> show system
Date 20XX/04/01 01:52:01 UTC
System: AX8616R, OS-RE, Ver.12.1, [9896.21]
  Elapsed time: 2 days 04:30
  Name: System
  Contact: Contact
  Location: Location
  Chassis MAC address: 0012.e286.5300
  BCU redundancy status: duplex
  FAN control mode: 1 (normal)
  Temperature warning level: current = 45, average = 45
  High temperature action: stop
  Power redundancy mode: 2 (Power Supply + Input Source)
  System MTU: 1518

Hardware information
  FAN1: active
    Elapsed time: 2 days 04:30
    Lamp: STATUS LED = green
  FAN2: active
    Elapsed time: 2 days 04:30
    Lamp: STATUS LED = green
  FAN3: active
    Elapsed time: 2 days 04:30
    Lamp: STATUS LED = green
  FAN4: active
    Elapsed time: 2 days 04:30
    Lamp: STATUS LED = green
  FAN5: active
    Elapsed time: 2 days 04:30
    Lamp: STATUS LED = green
  FAN6: active
    Elapsed time: 2 days 04:30
    Lamp: STATUS LED = green
  PS1: active
    Elapsed time: 2 days 04:30
  PS2: active
    Elapsed time: 2 days 04:30
  PS3: active
    Elapsed time: 2 days 04:30
  PS4: active
    Elapsed time: 2 days 04:30
  BCU1: active
    Elapsed time: 2 days 04:30
    Boot device: primary
    BCU-CPU: active
      Boot: 20XX/03/29 09:10:46 UTC, power on, fatal error restart 0 time
      Board: clock 2.0GHz, memory 16,068,212KB
    PA: active
      Boot: 20XX/03/29 09:10:46 UTC, power on, fatal error restart 0 time
      Board: clock 1.1GHz, memory 2,097,152KB
    Lamp: STATUS LED = green, ACTIVE LED = green
```

```

        SYSTEM1 LED = green, SYSTEM2 LED = light off
    System operation panel: no error
    Management port: active up
        10BASE-T half(auto), 0012.e286.5301
    Temperature: normal (32 degree C)
    Flash: enabled, 6,153,286KB
    MC: notconnect
BCU2: standby
    Elapsed time: 2 days 04:30
    Boot device: primary
    BCU-CPU: active
        Boot: 20XX/03/29 09:10:53 UTC, power on, fatal error restart 0 time
        Board: clock 2.0GHz, memory 16,068,212KB
    PA: active
        Boot: 20XX/03/29 09:10:53 UTC, power on, fatal error restart 0 time
        Board: clock 1.1GHz, memory 2,097,152KB
    Lamp: STATUS LED = green, ACTIVE LED = green
        SYSTEM1 LED = green, SYSTEM2 LED = light off
    System operation panel: no error
    Management port: unused
    Temperature: normal (32 degree C)
    Flash: enabled, 6,153,286KB
    MC: notconnect
SFU1: active, fatal error restart 0 time
    Elapsed time: 2 days 04:34
    Lamp: STATUS LED = green, ACTIVE LED = green
SFU2: notconnect
SFU3: notconnect
SFU4: notconnect
PRU1: active, fatal error restart 0 time
    Elapsed time: 2 days 04:30
    Boot: 20XX/03/29 09:20:26 UTC
    Board: clock 0.8GHz, memory 3,760,820KB
    Lamp: STATUS LED = green
    Forwarding database management
        Forwarding-table allocation
            Configuration: default
            Current: default
    Flow database management
        Flow-table allocation
            Configuration: default
            Current: default
        Flow detection mode
            Configuration: quantity-oriented
            Current: quantity-oriented
PRU2: notconnect
PRU3: notconnect
PRU4: notconnect
NIF1: active, fatal error restart 0 time
    Elapsed time: 2 days 04:34
    Lamp: STATUS LED = green
NIF2: notconnect
:
NIF16: notconnect
>

```

(2) Checking the environment status

By using the `show environment` operation command, you can check the following information:

- Fan information
- Power supply unit information
- Power usage information
- Inlet temperature of BCU

- Temperature status of each board (BCU, SFU, PRU, and NIF)
- Operating time information of each board (BCU, SFU, PRU, and NIF)

An example is shown below.

Figure 11-31: Checking the environment status

```
> show environment
Date 20XX/03/27 06:16:38 UTC

FAN environment
  FAN1: active, Speed = 2600
  FAN2: active, Speed = high
  FAN3: active, Speed = 2600
  FAN4: active, Speed = high
  FAN5: fault
  FAN6: active, Speed = high
  Mode: 1 (normal)

Power environment
  Input voltage: AC200-240V
  Power redundancy mode: 2 (Power Supply + Input Source)
  Power supply redundancy status
    Power supply: active = 4, required = 1 (Redundant)
    Input source: active = 2(from A) 2(from B), required = 1 (Redundant)
  PS1: active
  PS2: active
  PS3: active
  PS4: active

Power usage
  Total power capacity:                10168.00 W
    Input source A:                    5084.00 W
    Input source B:                    5084.00 W
  Total power allocated:                1477.00 W
  Total power available for additional boards: 8691.00 W
  Power available (Power supply unit redundant case): 6149.00 W
  Power available (Input source redundant case)
    Input source A:                    3607.00 W
    Input source B:                    3607.00 W

Inlet temperature
  BCU1: normal (36 degree C)
  BCU2: normal (36 degree C)

Board temperature
  BCU1: normal
  BCU2: normal
  SFU1: normal
  SFU2: notconnect
  SFU3: notconnect
  SFU4: notconnect
  PRU1: normal
  PRU2: notconnect
  PRU3: notconnect
  PRU4: notconnect
  NIF1: normal
  NIF2: notconnect
  :
  NIF16: notconnect

Accumulated running time
      total          caution          critical
BCU1    2 days 16 hours  1 day  1 hour  0 days  0 hours
BCU2    2 days 16 hours  1 day  1 hour  0 days  0 hours
SFU1    2 days 16 hours  1 day  1 hour  0 days  0 hours
SFU2    notconnect
SFU3    notconnect
```



```

SFU4      notconnect
PRU1       2 days 16 hours      1 day   1 hour      0 days   0 hours
PRU2      notconnect
PRU3      notconnect
PRU4      notconnect
NIF1       2 days 16 hours      1 day   1 hour      0 days   0 hours
NIF2      notconnect
:
NIF16     notconnect
PS1        2 days 16 hours      1 day   1 hour      0 days   0 hours
PS2        2 days 16 hours      1 day   1 hour      0 days   0 hours
PS3        2 days 16 hours      1 day   1 hour      0 days   0 hours
PS4        2 days 16 hours      1 day   1 hour      0 days   0 hours
FAN1       2 days 16 hours      1 day   1 hour      0 days   0 hours
FAN2       2 days 16 hours      1 day   1 hour      0 days   0 hours
:
FAN6       2 days 16 hours      1 day   1 hour      0 days   0 hours
>

```

(3) Checking temperature log data

The temperature-logging parameter of the `show environment` operation command allows you to check inlet temperature logs recorded for a maximum of two years. When the temperature-logging parameter is specified, the average inlet temperature recorded every six hours is displayed. An example is shown below.

Figure 11-32: Checking temperature log data

```

> show environment temperature-logging
Date 20XX/04/01 01:44:40 UTC
BCU1
Date      0:00   6:00  12:00  18:00
20XX/04/01  32.9
20XX/03/31  33.0   33.0   33.0   33.0
20XX/03/30  33.0   33.0   33.0   33.0
20XX/03/29   -     -    33.7   33.0

BCU2
Date      0:00   6:00  12:00  18:00
20XX/04/01  32.9
20XX/03/31  33.0   33.0   33.0   33.0
20XX/03/30  33.0   33.0   33.0   33.0
20XX/03/29   -     -    33.7   33.0
>

```

11.3.4 Checking the internal flash memory

By using the `show flash` operation command, you can check the usage of the internal flash memory. An example is shown below.

Figure 11-33: Checking the internal flash memory

```

> show flash
Date 20XX/04/01 07:09:21 UTC
BCU1 Flash: enabled
      area      used      free      total
user      185,394KB    2,832,550KB    3,017,944KB
config      1,682KB    1,601,538KB    1,603,220KB
dump0       2,816KB     326,416KB     329,232KB
dump1       998KB     1,064,674KB    1,065,672KB
log         11KB      137,207KB     137,218KB
total     190,901KB    5,962,385KB    6,153,286KB
BCU2 Flash: enabled
      area      used      free      total
user      185,394KB    2,832,550KB    3,017,944KB
config      1,682KB    1,601,538KB    1,603,220KB
dump0       2,816KB     326,416KB     329,232KB

```

```

dump1          998KB      1,064,674KB      1,065,672KB
log            11KB       137,207KB       137,218KB
total          190,901KB  5,962,385KB     6,153,286KB
>

```

11.3.5 Checking the memory card

By using the `show mc` operation command, you can check the usage of the memory card. An example is shown below.

Figure 11-34: Checking the memory card

```

> show mc
Date 20XX/04/01 07:20:11 UTC
BCU1 MC: enabled
CID: 00c7000910d06b224734304653415001
used:      189,792KB
free:      3,680,928KB
total:     3,870,720KB
BCU2 MC: -----
>

```

11.3.6 Monitoring temperatures

(1) Inlet temperature monitoring

In this Device, the inlet temperature is monitored for both an active system and a standby system. If the inlet temperature is too low or too high, a system message is output or an SNMP trap is issued. If the inlet temperature reaches the high-temperature stop level, the Device is stopped.

Note that you can reference inlet temperature log data recorded for a maximum of two years.

(2) Inlet temperature monitoring level and operation

The following table describes inlet temperature monitoring levels and operations.

Table 11-29: Monitoring levels and operations

Inlet temperature	Monitoring level	Operating condition level	System operation
Drops to 2 degrees Celsius or lower.	Low temperature caution	caution	Operation is continued. When the operating condition level changes, a system message is output and an SNMP trap is issued.
Rises to 5 degrees Celsius or higher.	Recovered from low temperature caution	normal	
Drops to 40 degrees Celsius or lower.	Recovered from high temperature caution	normal	
Rises to 43 degrees Celsius or higher.	High temperature caution	caution	
Drops to 50 degrees Celsius or lower.	Recovered from high temperature warning	caution	
Rises to 53 degrees Celsius or higher.	High temperature warning	critical	BCU is stopped.#
Rises to 65 degrees Celsius or higher.	Stop due to high temperature	fault	

#: By using the `system high-temperature-action` configuration command, you can set BCU not to stop.

The operations when BCU is stopped because the temperature reaches the high temperature stop level are shown as follows:

For single-configuration BCU:

A system message is output, an SNMP trap is issued, and the Device is stopped. The stopped BCU does not recover automatically.

In a BCU duplex configuration, when the active BCU (BCU 1, for example) is at the high temperature stop level:

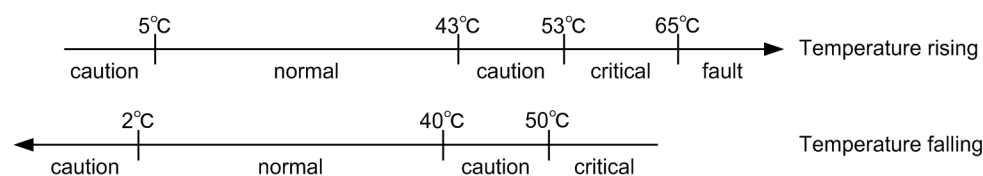
A system message is output, an SNMP trap is issued, and BCU 1 is stopped. After system switchover, BCU 2 becomes an active system and operates as a single-configuration system. The stopped BCU 1 does not recover automatically.

In a BCU duplex configuration, when the standby BCU (BCU 2, for example) is at the high temperature stop level:

A system message is output, an SNMP trap is issued, BCU 2 is stopped, and BCU1 operates as a single-configuration system. The stopped BCU 2 does not recover automatically.

The following figure shows the operating condition levels and temperature values.

Figure 11-35: Operating condition levels and temperature values



(3) Warning according to arbitrary inlet temperature and recovery notification

(a) Monitoring the inlet temperature

If you set the `system temperature-warning-level` configuration command, a system message that gives temperature warning is output when the inlet temperature of the Device reaches or exceeds the specified temperature. In addition, a temperature recovery system message is output when the inlet temperature of the Device drops by 3 degrees Celsius or more after reaching or exceeding the specified temperature. Note that a temperature-warning system message is output after a temperature recovery system message is output.

(b) Monitoring the average inlet temperature

If you set the `system temperature-warning-level average` configuration command, a system message that gives temperature warning is output at 12:00 every day when the average inlet temperature over a number of days specified by the Device reaches or exceeds the specified temperature.

(4) Checking the inlet temperature status

You can check the inlet temperature status from the `Inlet Temperature` item displayed by the `show environment` operation command. In addition, the `temperature-logging` parameter of the `show environment` operation command allows you to check inlet temperature logs recorded for a maximum of two years.

(5) Monitoring the board temperature

In addition to monitoring the inlet temperature, the Device monitors the temperature of each board. The boards targeted for monitoring are the BCU, SFU, PRU, and NIF.

If a board becomes too hot to continue operation, the Device stops the relevant board. The stopped board does not recover automatically even if its temperature drops. The following table describes board temperature monitoring levels and operations.

Table 11-30: Monitoring levels and operations

Monitoring level	Operating condition level	System operation
Recovered from high temperature warning	normal	Continues operation of the relevant board.
High temperature warning detected	critical	
Stop due to high temperature	fault	Outputs a system message, issues an SNMP trap, and stops the relevant board.

(6) Checking the board temperature status

You can check the temperature status of each board from the `Board Temperature` item displayed by the `show environment` operation command.

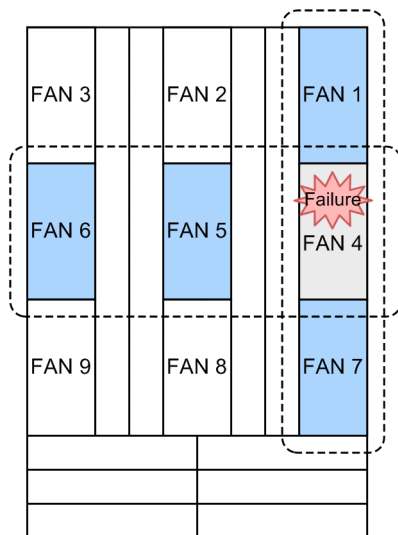
11.3.7 Monitoring fan units

(1) Monitoring fan unit status

A fan unit contains multiple fans, and the Device can contain multiple fan units.

If a fan unit fails during operation (an individual fan fails, or a fan unit fails or is removed), a fan unit failure system message is output and an SNMP trap is issued. When the above occurs, the operation of the Device continues by rotating other fan units installed in the same row and column as the relevant fan unit at high speed. A failed fan unit can be removed or replaced while the Device keeps operating. The following figure shows an example of operation when a fan unit fails.

Figure 11-36: Example of operation when a fan unit fails



Legend: : Fan unit rotating at high speed

When normal operation starts after you replace a faulty fan unit, a system message indicating recovery from fan unit failure is output and an SNMP trap is issued. At the same time, the high-speed rotation of other fan units installed in the same row and column as the relevant fan unit is canceled (only if there is no fan unit failure in the same row and column).

When the fan units are rotated at high speed or when the high-speed rotation is canceled, a system message is output for each of the relevant fan units.

(2) Checking the fan unit status

You can check the fan operating status and rotational speed of each fan unit from the `Fan environment` item displayed by the `show environment` operation command.

11.4 Managing SFU, PRU, and NIF

11.4.1 Lists of configuration commands and operation commands

The following table describes the configuration commands for managing SFUs, PRUs, and NIFs.

Table 11-31: List of configuration commands

Command name	Description
power enable [#]	Changes the status of a board from disabled to active. This command turns off the power to a board if <code>no power enable</code> is specified.
system pru priority [#]	Sets the priority of a PRU to be started when the Device starts.

#

See *10. SFU/PRU/NIF Management* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

The following table describes the operation commands for managing SFUs, PRUs, and NIFs.

Table 11-32: List of operation commands

Command name	Description
show system	Shows the statuses of the SFU and PRU.
show nif [#]	Shows the operating status of NIFs.
clear counters nif [#]	Clears the NIF statistics counter.
activate sfu [#]	Changes the status of a SFU from inactive to active.
inactivate sfu [#]	Changes the status of a SFU from active to inactive. This command also turns off the power to the SFU
activate pru [#]	Changes the status of the PRU from inactive to active.
inactivate pru [#]	Changes the status of the PRU from active to inactive. This command also turns off the power to the PRU.
activate nif [#]	Changes the status of a NIF from inactive to active.
inactivate nif [#]	Changes the status of a NIF from active to inactive. This command also turns off the power to a NIF.

#

See *11. SFU/PRU/NIF Management* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

11.4.2 Disabling a board

By using the `power enable` configuration command, you can disable an unused SFU, PRU, or NIF. The power of the board for which this setting is made will be turned off. In the example below, an SFU is disabled.

Points to note

If this configuration command is used to configure the setting, this state can be continued even after the device restarts.

Command examples

1. **(config)# no power enable sfu 1**

Disables SFU1 in configuration command mode.

11.4.3 Configuring PRU startup priorities

If the power supply does not provide enough power when the Device starts, not all PRUs start. The priority of each PRU to be started in that case must be set using a value from 1 to 255. The lower the set value, the higher the priority. The default priority value is 128.

When the Device starts, PRUs start in descending order of priority. PRUs with the same priority value start in ascending order of PRU numbers. If the power supply is supplying enough power when the Device starts, this priority operation does not apply and all PRUs start. In the example below, the priority of board PRU 1 is set to high and the priority of board PRU 4 is set to low.

Points to note

In order to clarify which PRUs start when the Device starts, set a different priority for each PRU.

This setting applies only when the Device starts. Therefore, we recommend that you configure this setting at the time of initial deployment.

Command examples

1. **(config)# system pru 1 priority 1**
(config)# system pru 4 priority 255

Sets 1 as the priority of PRU 1 and 255 as the priority of PRU 4.

11.4.4 Checking the SFU status

By using the `show system` operation command, you can check the operating status and update status of the SFU. If the relevant SFU has been updated, its update status is displayed. An example is shown below.

Figure 11-37: SFU status check

```
> show system
Date 20XX/12/10 15:11:20 UTC
System: AX8632R, OS-RE, Ver.12.1, [123.1]
:
:
SFU1 : active (restart required), fatal error restart 0 time
      Elapsed time : 2 days 2:30
      Lamp : STATUS LED = green , ACTIVE LED = light off
SFU2 : notconnect
:
SFU4 : active, fatal error restart 0 time
      Elapsed time : 2 days 2:30
      Lamp : STATUS LED = green , ACTIVE LED = light off
>
```

11.4.5 Checking the PRU status

By using the `show system` operation command, you can check the operating status and update status of PRUs. If the relevant PRU has been updated, its update status is displayed. An example is shown below.

Figure 11-38: PRU status check

```
> show system
Date 20XX/12/10 15:11:20 UTC
System: AX8632R, OS-RE, Ver.12.1, [123.1]
:
:
PRU1 : active (restart required), fatal error restart 0 time
:
```

```

PRU2 : notconnect
      :
PRU8 : active, fatal error restart 0 time
      :
>

```

11.4.6 Checking the NIF status

By using the `show nif` operation command, you can check the operating status and update status of NIFs. If the relevant NIF has been updated, its update status is displayed. An example is shown below.

Figure 11-39: NIF status check

```

>show nif 1
Date 20XX/04/01 12:00:00 UTC
NIF1: active(restart required) 12-port 10BASE-T/100BASE-TX/1000BASE-T  retry:0
      Average:103Mbps/24Gbps  Peak:150Mbps at 08:10:30
Port1: active up 1000BASE-T full(auto) 0012.e240.0a04
      Bandwidth:1000000kbps  Average out:20Mbps  Average in:10Mbps
      description: test lab area network
Port2: active up 1000BASE-T full(auto) 0012.e240.0a05
      Bandwidth:1000000kbps  Average out:0Mbps  Average in:0Mbps
      description: computer management floor network
Port3: active up 1000BASE-T full(auto) 0012.e240.0a06
      Bandwidth:1000000kbps  Average out:2Mbps  Average in:1Mbps
      :
      :
>

```

11.4.7 Configuration when a NIF is replaced

If a NIF is installed when there are no port configurations, port configurations corresponding to the installed NIF are automatically created. However, if port configurations already exist and an existing NIF is replaced with a NIF that handles Ethernet types different from the existing ones (10BASE-T/100BASE-TX/1000BASE-T, 1000BASE-X, 10GBASE-R, and 100GBASE-R), port configurations corresponding to the NIF after replacement are not created automatically. For that reason, port configurations do not match the Ethernet types handled by the installed NIF and link-up does not occur for the unmatched ports.

If port configurations corresponding to the NIF after replacement are not created automatically, delete the configurations before replacement for the relevant ports. For ports whose configurations before replacement have been deleted, configurations corresponding to the NIF after replacement are created automatically.

The example below shows automatic creation and deletion of port configurations at the time of NIF replacement. In this example, the NLXG-6RS NIF is replaced by the NL1G-12T NIF.

1. Remove the NIF (NLXG-6RS).
2. Check the configuration.


```

(config)# show
interface tengigabitethernet 1/1
!
interface tengigabitethernet 1/2
!
interface tengigabitethernet 1/3
!
interface tengigabitethernet 1/4
!
interface tengigabitethernet 1/5
!
interface tengigabitethernet 1/6
!

```

Even after the NIF is removed, the port configurations corresponding to it are not deleted.

3. Install the NIF (NL1G-12T).

4. Check the configuration.

```
(config)# show
interface tengigabitethernet 1/1
!
:
:

!
interface tengigabitethernet 1/6
!
interface gigabitethernet 1/7
!
interface gigabitethernet 1/8
!
interface gigabitethernet 1/9
!
interface gigabitethernet 1/10
!
interface gigabitethernet 1/11
!
interface gigabitethernet 1/12
!
```

For ports 1/1 to 1/6, where the 10 gigabit Ethernet interface configurations before replacement exist, configurations corresponding to the NIF after replacement are not created automatically.

For ports 1/7 to 1/12, gigabit Ethernet interface configurations corresponding to the NIF after replacement are created automatically.

5. Delete the configuration for port 1/1.

```
(config)# no interface tengigabitethernet 1/1
```

6. Check the configuration.

```
(config)# show
interface gigabitethernet 1/1
!
interface tengigabitethernet 1/2
!
:
:

!
interface tengigabitethernet 1/6
!
interface gigabitethernet 1/7
!
:
:
```

For port 1/1, whose configuration before replacement has been deleted, a configuration corresponding to the NIF after replacement is created automatically.

11.5 Backing up and restoring operating information

This section describes how to restore operating information after a failure or module replacement.

In a BCU duplex configuration, execute the procedure described in *11.5.2 Procedure for BCUs in a duplex configuration*. To ensure and facilitate backup and restore operations for a single-configuration BCU, execute the procedure described in *11.5.3 Procedure for a BCU in a single configuration*. You can also restore the information manually, but we do not recommend this because the device handles a wide variety of operating information which is complicated to manage and cannot be fully restored.

11.5.1 List of operation commands

The following table describes the operation commands for backup and restore operations.

Table 11-33: List of operation commands

Command name	Description
backup	Saves device information and information about active applications to a memory card or remote FTP server.
restore	Restores the device information saved to a memory card or remote FTP server to the Device.

11.5.2 Procedure for BCUs in a duplex configuration

In the state in which the replacement BCU has been started as the standby system, execute the following commands to synchronize the software version and setting files with the standby system.

- `update software` command
Synchronizes the software version.
- `synchronize` command
Synchronizes other setting files. The targets to be synchronized by this command include configurations.

For details about management information synchronization processing in duplex operation, see *13.1.3 Synchronizing user setting information and usage information*.

If both the active and standby BCUs are replaced in a BCU duplex configuration, restore the Device by using the `restore` command as follows:

1. To avoid system switchover during execution of the `restore` command, inactivate the standby system by using the `inactivate bcu standby` command.
2. Execute the `restore` command in the active system. This makes the active system restart.
3. Activate the standby system by using the `activate bcu standby` command.
4. Synchronize the standby system with the active system by using the `update software` command and the `synchronize` command.

11.5.3 Procedure for a BCU in a single configuration

(1) Backing up information

Create a backup by using the `backup` command at a time when the device is running normally. The `backup` command places the information below, which is required for device operation, in one file, and then saves the file to a memory card or external FTP server.

If any changes are made to the following information, we recommend that you back it up again by

using the `backup` command:

- Files for updating software to the version in current use
- `startup-config`

Note that the `backup` command does not save the following information:

- Operation and statistics logs
- Dump files and other error information saved internally
- Files created or saved by a user in a home directory set for that user account

(2) Restoring information

To restore information from a backup file created by the `backup` command, use the `restore` command.

When you execute the `restore` command, the device software is updated automatically from the software update files stored in the backup file. After the update is complete, the Device restarts automatically. After the restart, the recovered environment is used.

11.6 Failure recovery

Recovery processing is performed automatically when a problem occurs during Device operation. The processing is localized according to the type of problem, minimizing its impact and allowing unaffected sections to continue operating.

11.6.1 Type of problem and recovery processing

Recovery processing differs according to the nature of the problem. The following table describes problem types and recovery processing.

Table 11-34: Problem type and recovery processing

Problem type	Device response	Recovery processing	Areas affected
Error detected at a port	The Device automatically recovers an unlimited number of times.	Reinitialize the affected port.	Communication via the affected port is suspended.
NIF failure	The Device automatically recovers a maximum of three times. ^{#1} If a failure occurs at the three auto-recovery attempt, the device stops. The number of auto-recovery attempts is reset every hour after the Device has started.	Reinitialize the failed NIF.	Communication via all the ports handled by the failed NIF is suspended.
PRU failure	The Device automatically recovers a maximum of three times. ^{#1} If a failure occurs at the third auto-recovery attempt, the device stops. The number of auto-recovery attempts is reset every hour after the Device has started.	Reinitialize the failed PRU.	Communication via all the NIFs installed in the failed PRU is suspended.
SFU failure	The Device automatically recovers a maximum of three times. ^{#1} If a failure occurs at the three auto-recovery attempt, the device stops. The number of auto-recovery attempts is reset every hour after the Device has started.	Reinitialize the failed SFU.	If there is a redundant SFU, communication can be maintained. If there is no active SFU except the failed SFU, communication via all the NIFs is suspended.

Problem type	Device response	Recovery processing	Areas affected
BCU failure	The Device automatically recovers a maximum of six times. ^{#1} If a failure occurs at the sixth auto-recovery attempt, the device stops. The number of auto-recovery attempts are reset after one hour of post recovery operation.	Reinitialize the failed BCU. In a BCU duplex configuration, recovery processing is performed by system switchover.	Communication via all ports on the Device is suspended. In a BCU duplex configuration, communication can be maintained.
Inlet temperature error	The BCU in which an error was detected is stopped. ^{#2}	The stopped BCU does not recover automatically.	Communication via all ports on the Device is suspended.
Power supply unit failure (PS)	Supply of power to the power supply unit in which an error was detected is stopped. If multiple power supply units are installed, operation continues based on power supplied from the remaining power supply units.	The power supply unit in which an error was detected does not recover automatically.	If there is a redundant power supply unit, operation continues. If there is no redundant power supply unit normal operation is not possible when power necessary for device operation ceases to be supplied.
Fan unit failure	All the other fan units installed in the vertical and horizontal directions relative to the fan unit in which a failure was detected start rotating at high speed.	The failed fan unit does not recover automatically.	Communication is not affected. The temperature inside the Device might increase.

#1

Depending on the failure details, the Device does not recover automatically and the failed board is stopped.

#2

If the setting for not stopping BCU is made by the `system high-temperature-action` configuration command, the BCU is not stopped.

Chapter

12. Software Management

This chapter describes software management.

12.1 Description of software updates

12.2 Operations to update software

12.1 Description of software updates

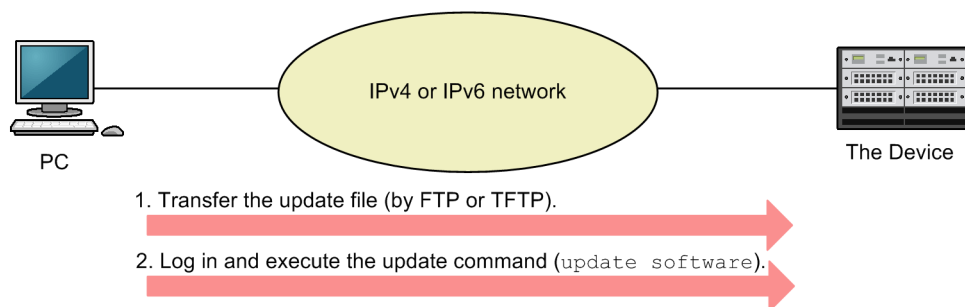
12.1.1 Overview

A software update means changing the software version from the currently used version to a different version. A software update consists of processing to update the software for each board in the Device and processing to apply the updated software to the operating status of the Device. A version can be either upgraded or downgraded.

You can update software by transferring an update file from a remote operation terminal such as a PC or from a memory card, and then executing the `update software` operation command. At board startup and at system switchover between the active and standby systems, the software for the SFUs, PRUs, and NIFs is automatically updated to the same version as the version of the software for the active BCU. When software is updated, the existing configuration is inherited without change.

The following figure shows an overview of a software update using the `update software` operation command.

Figure 12-1: Overview of a software update



12.1.2 Targets of software updates

In a software update, the software for each board in the Device and the software related to hardware control (HDC: Hardware dependent code) are updated. If the software already installed in each board is the same version as the software used for the update, the update is not performed.

The following table describes the targets of software updates.

Table 12-1: Targets of software updates

Board	Target of update
BCU	Software, HDC
SFU	HDC
PRU	Software, HDC
NIF	HDC

12.1.3 Update and application triggers

Software update is triggered by the following two operations:

- Execution of the `update software` operation command
- Board startup

The timings of the software update and of the application of the update vary depending on the update triggers. This subsection describes the update and application timings for each update

trigger.

You can check the software update and application status by using the `show version` operation command and comparing the active version and installed version.

(1) Execution of the update software operation command

If the BCU single configuration is used:

After the software for the BCU is updated, the new software is applied by automatically restarting the Device. At the same time, the software for each board is updated and the new software is applied. You can also specify that automatic restart is not to be performed when the `update software` command is executed.

If the BCU duplex configuration is used:

After the software for the BCUs is updated, the new software is applied to the BCUs by automatically restarting them. You can also specify that automatic restart is not to be performed when the `update software` command is executed.

If the active BCU is the update target, the software for each SFU, PRU, and NIF is also updated. To apply the updated software, restart each board by using operation commands.

For details about the software application trigger, see *12.2 Operations to update software*.

(2) Board startup

During a software update for the SFU, PRU, or NIF triggered by board startup, the software is automatically updated and applied. Therefore, the started board operates on the software whose version is the same as the version of the software on the active BCU.

12.1.4 Non-stop software upgrade

The functionality, non-stop software upgrade, updates software without interrupting communication in a redundant configuration. Communication during an update operation can be maintained by updating the software in the boards one after another while retaining data such as the routing table. The operation at each board is as follows:

BCU

An update is performed with system switchover in a duplex configuration, so that the software and the HDC can be updated while communication is maintained.

SFU

SFUs are restarted one after another in a redundant configuration, so that the HDC can be updated while communication is maintained.

PRU

Using link aggregation over multiple PRUs, PRUs are restarted one after another, so that the software and the HDC can be updated while communication is maintained.

NIF

Using link aggregation over multiple NIFs, NIFs are restarted one after another, so that the HDC can be updated while communication is maintained.

For an update, the version of the software can be both upgraded and downgraded without stopping communication.

The following table describes the conditions for non-stop software upgrade.

Table 12-2: Applicable conditions for non-stop software upgrade

Item	Applicable conditions
Device configuration	The BCUs are in a duplex configuration. The SFUs are in a redundant configuration. Link aggregation over multiple PRUs is used.
	For downgrading, hardware (such as PRU and NIF) not supported by the updated software version is not used.
Supported functionality	Functionality is used that supports Non-Stop Communication at system switchover. For details, see (1) <i>List of functionalities that support Non-Stop Communication at system switchover</i> in 13.1.4 <i>System switchover</i> .
	For downgrading, functionality not supported by the updated software is not used.
Software version	The version is 12.1 or later both before and after an update.
	Both the active and standby BCUs operate on the same version of software before an update.
Configuration	The running configuration and the configuration being edited match the startup configuration.
	The startup configuration for the active BCU matches the startup configuration for the standby BCU.

12.1.5 Notes on updating software

(1) Notes on the power supply

Do not turn off the power during a software update.

(2) Notes on SFUs

If you want to perform non-stop software upgrade, we recommend that you install an adequate number of SFUs that can maintain the performance required by the Device even if one of them stops.

To update the HDC for SFUs, you need to restart SFUs one after another. At this time, depending on the configuration of the installed PRUs and NIFs and on the number of SFUs, the performance might be lower than the performance required by the Device while SFUs are restarted one after another.

(3) Notes on configurations

The configurations stored in the internal flash memory are inherited even after a software update. If there are too many configurations stored, it might take a long time to inherit them.

If there are configurations that are not supported due to downgrading among the inherited configurations, after such unsupported configurations are deleted, the rest of the configurations are used for operation.

12.2 Operations to update software

12.2.1 List of operation commands

The following table describes the operation commands for software management.

Table 12-3: List of operation commands

Command name	Description
update software	Updates the software to the specified software.

12.2.2 Preparing an update file

1. If you have not saved a configuration after editing it online, save it by executing the `save` or `commit` configuration command before an update.

If you do not save a configuration that you edited, the configuration before editing is restored when BCU restarts after completion of an update.

2. Execute the `show flash` command.

Make sure that there is free space (`free`) equal to or larger than the following value in the user area (`user`) of the internal flash memory of BCU1 and BCU2 each:

size-of-update-file - size-of-the-file-/usr/var/update/k.img + 10 MB

3. Transfer the update file to the Device. Using the file name `k.img`, copy the file to the directory (`/usr/var/update`).

There are two ways of transferring the file: by using FTP or by using a memory card. If you use FTP, transfer the file in binary mode.

4. Execute the `ls -l /usr/var/update` command.

Make sure that the file size of `k.img` is equal to the file size of the source file. When you finish checking, go to *12.2.3 Executing the update command*.

12.2.3 Executing the update command

The procedure varies depending on whether the BCU single configuration or BCU duplex configuration is used.

(1) Updating when the BCU single configuration is used

1. Execute the `cd /usr/var/update` command.
2. Execute the `update software k.img active` command.

The version of the software to be installed and the update targets are displayed.

If the BCU is included in the update targets:

After the software is updated, the Device automatically restarts. When the Device restarts, log in again and then go to *12.2.5 Checking after updates*.

If the BCU is not included in the update targets:

You need to manually restart the SFU, PRU, or NIF. Go to *12.2.4 Updating SFU, PRU, and NIF*.

(2) Updating when the BCU duplex configuration is used

1. Execute the `cd /usr/var/update` command.
2. Execute the `update software k.img standby` command.

The version of the software to be installed and the update targets are displayed.

If the BCU is included in the update targets:

After the software is updated, the standby BCU restarts automatically. When the standby BCU restarts, go to step 3.

If the BCU is not included in the update targets:

Execute the `update software k.img active` command.

The version of the software to be installed and the update targets are displayed. After the software is updated, go to step 9.

3. Execute the `show version` command.

Make sure that the standby BCU is running on the updated software.

4. Execute the `show system` command.

In the `Hardware information` field, check the operating status of the standby BCU.

If `configuration discord` is displayed as the operating status:

Execute the `update software k.img active` command.

The version of the software to be installed and the update targets are displayed. After the software is updated, system switchover occurs because the active BCU automatically restarts. After system switchover, log in again and go to step 9.

If `configuration discord` is not displayed as the operating status:

Go to step 5.

5. Execute the `redundancy force-switchover` command.

Manually perform system switchover. After system switchover, log in again to the new active BCU.

6. Execute the `cd /usr/var/update` command.

7. Execute the `show system` command.

In the `Hardware information` field, make sure that `configuration discord` is not displayed as the operating status of the standby BCU.

8. Execute the `update software k.img standby` command.

After the software is updated, the standby BCU restarts automatically.

9. Execute the `show system` command.

In the `Hardware information` field, make sure that the operating status of the standby BCU is `standby`. When you finish checking, go to *12.2.4 Updating SFU, PRU, and NIF*.

12.2.4 Updating SFU, PRU, and NIF

1. After executing the `inactivate` command for all SFUs and PRUs, execute the `activate` command.

All SFUs, PRUs, and NIFs restart. If the applicable conditions for non-stop software upgrade are satisfied at this point, software can be applied without communication interruption by restarting the boards one by one. After all the SFUs, PRUs, and NIFs restart, go to *12.2.5 Checking after updates*.

12.2.5 Checking after updates

The procedure varies depending on whether the BCU single configuration or BCU duplex configuration is used.

(1) Checking when the BCU single configuration is used

1. Execute the `show version` command.

Make sure that the software version for the BCU is the same as the expected version.

(2) Checking when the BCU duplex configuration is used

When the BCU duplex configuration is used, note that the update procedure so far might have caused switching between the active BCU and the standby BCU.

1. Execute the `show version` command.

Make sure that the software version for the active BCU version is the same as the expected version.

2. Execute the `show system` command.

In the `Hardware information` field, make sure that none of the following is displayed as the operating status of the standby BCU:

- `configuration discord`
- `software version discord`

12.2.6 Notes on performing updates

Delete the `k.img` file only when you are instructed to do so by the procedure. If you delete the file without being instructed to do so, you will be unable to restore the file if an abnormal termination occurs.

Chapter

13. Device Redundancy

This chapter describes redundancy configurations of the Device.

- 13.1 Description of the BCU duplex configuration
- 13.2 Operation for the BCU duplex configuration
- 13.3 Description of SFU redundancy
- 13.4 Operation for SFU redundancy
- 13.5 Description of power supply unit (PS) redundancy
- 13.6 PS (power supply unit) redundancy configuration
- 13.7 Operation for PS (power supply unit) redundancy

13.1 Description of the BCU duplex configuration

13.1.1 Overview

(1) Device configuration

To create a duplex configuration for the basic control unit (BCU), install two BCUs in the Device. Each of these two boards operates as either the active BCU or the standby BCU. By creating a duplex configuration for BCU, you can increase reliability in the event of a failure. If a failure occurs in the active BCU, the active BCU and the standby BCU are switched, and the standby BCU starts operation as a new active BCU.

(2) Conditions for creating a duplex configuration

The conditions for operating BCU in a duplex configuration are shown below. If all the conditions are met, system switchover is possible.

- The active BCU is running normally.
- The standby BCU is running normally.
- The configurations for both BCUs are synchronized with one another.

If any of these conditions is not met, a system message is output as a warning. To satisfy all the conditions, take action according to the instruction of the system message.

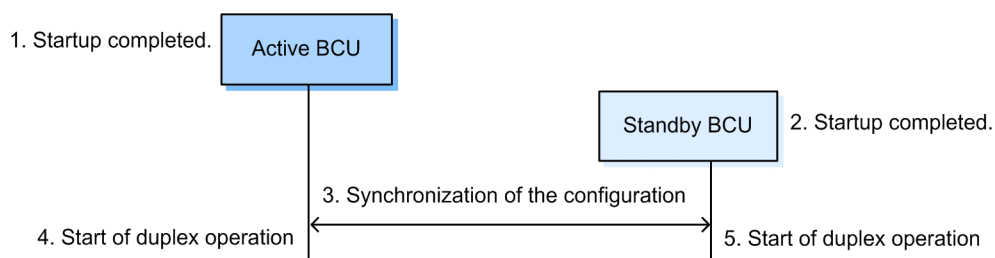
13.1.2 Operation

The Device operates in a single configuration when one BCU is installed in the Device.

When two BCUs are installed, one of them starts as the standby BCU. After that, if the conditions for creating a duplex configuration are met, a system message (message type: BCU, message ID: 01101006) appears and the Device starts operating in a duplex configuration.

Even if two BCUs are installed, the Device operates in a single configuration until startup of the standby BCU is complete. Communication is not affected if the configuration switches between single and duplex configurations. The following figure shows a workflow from the start of operation in a single configuration to operation in a duplex configuration.

Figure 13-1: Operation when starting to operate in a duplex configuration



1. Only the active BCU operates in a single configuration
2. Startup of the standby BCU is complete.
3. Synchronization between the configurations of the active BCU and the standby BCU is complete.
4. A system message appears, indicating that the active BCU has started operating in a duplex configuration.
5. A system message appears, indicating that the standby BCU has started operating in a duplex configuration.

If two BCUs are installed in the Device and then the power of the Device is turned on, BCU1

operates as the active BCU and BCU2 operates as the standby BCU.

13.1.3 Synchronizing user setting information and usage information

The table below describes the user setting information and usage information synchronized between the active BCU and the standby BCU. The synchronized information is also applied to the operation of the standby BCU, so that no conflict occurs after system switchover.

Table 13-1: User setting information and usage information synchronized during operation

User's setting information and usage information	Timing of synchronization
Running configuration and configuration being edited	<ul style="list-style-type: none"> When operation in a duplex configuration starts When the configuration is changed
Startup configuration	<ul style="list-style-type: none"> When the startup configuration is updated by any of the following commands: <ul style="list-style-type: none"> - Configuration command <code>save</code> - Configuration command <code>commit</code> - Operation command <code>copy</code> - Operation command <code>erase configuration</code> When the <code>synchronize</code> operation command is executed
Files created under the home directory	<ul style="list-style-type: none"> When the <code>synchronize</code> operation command is executed (only when the <code>userfile</code> parameter is specified)

13.1.4 System switchover

If the BCUs operate in a duplex configuration in the Device, switching of the active BCU occurs when the `redundancy force-switchover` operation command is executed or when the active BCU fails.

If you use the command to perform system switchover, the system for which the command is executed operates as the standby BCU after the system switchover. If the Device is not ready for system switchover, system switchover by the command is suppressed.

You can check the status of the duplex configuration by using the `show system operation` command. If the Device has not completely started or is not ready for system switchover, do the following:

- Use the `show logging` operation command and take action according to the system message.
- Take action according to the *Troubleshooting Guide*.

Note that system switchover causes all the users accessing the Device through remote connection to log out. At this time, any command being executed by a user accessing the Device through a remote connection is terminated. After system switchover, the user needs to log in to the Device and execute the command again.

(1) List of functionalities that support Non-Stop Communication at system switchover

The table below describes the functionalities that support Non-Stop Communication at system switchover. Because each of the functionalities that support Non-Stop Communication at system switchover operates without stopping when system switchover occurs, communication can be maintained even after system switchover. Functionalities that do not support Non-Stop Communication at system switchover need relearning after system switchover. Therefore, communication is interrupted until the network information is reconfigured.

Table 13-2: Support status of Non-Stop Communication at system switchover

Category	Functionality	Supported
Access to the Device	Telnet and FTP	N

Category	Functionality	Supported
Network interfaces	Common to all NIFs	Y
	Management port	N
Link aggregation	Static	Y
	LACP	Y
	Standby link link-down mode	Y
	Standby link not-link-down mode	Y
	Mixed-speed mode	Y
Filters and QoS	Filters and QoS	Y
IP packet forwarding	IPv4 and ARP	Y
	IPv6 and NDP	Y
	Policy-based routing	Y ^{#1}
	DHCP/BOOTP relay agent	Y
	DHCPv6 relay agent	Y
	VRRP	N
Unicast routing protocol	Static routing	Y
	RIP, RIP2, and RIPng	N
	OSPF and OSPFv3	Y ^{#2}
	BGP4 and BGP4+	Y ^{#2}
IPv4 multicast routing protocols	PIM-SM	N
	PIM-SSM	N
IPv6 multicast routing protocols	PIM-SM	N
	PIM-SSM	N

Legend: Y: Supported, N: Not supported

#1

While next-hop selection is suppressed after system switchover, communication continues by forwarding packets to the next hop selected before the system switchover.

#2

When the graceful restart functionality is used.

(2) Behavior when configurations are inconsistent

When a BCU is added or replaced, differences between the active BCU configuration and the standby BCU configuration might occur. If system switchover occurs in this state, conflicts in behavior might occur because the settings of the running hardware are different from the configuration for the new active BCU.

For that reason, the Device outputs a system message when it detects an inconsistency between the active BCU configuration and the standby BCU configuration. The Device also outputs a system message if there is a difference in configurations at startup. If the inconsistency is resolved after the configurations are synchronized with one another, a system message is output, indicating that

they are consistent. During synchronization of configurations, configuration editing is temporarily suppressed.

13.1.5 Notes on using the BCU duplex configuration

(1) Notes on login

Depending on how the operation terminal is connected, the system to which you can log in differs as follows:

- Serial port
You can log in to the active BCU and the standby BCU by connecting a console to these BCUs.
- Management port
You can log in to the active BCU by using its management port. You cannot log in to the standby BCU by using its management port.
- Communication port
If you log in from a remote operation terminal via the communication port, log in to the active BCU. You cannot log in to the standby BCU.
- Dial-up IP connection to serial port (AUX)
If you log in from a remote operation terminal via a dial-up IP connection, you can log in to both the active BCU and the standby BCU.

(2) Notes on system switchover

When system switchover occurs, the condition after system switchover might not be applied to the information displayed by an operation command or in the information obtained by the MIB until either of the following messages is output:

- Message type: BCU, Message ID: 0110100d
- Message type: BCU, Message ID: 0110100e

13.2 Operation for the BCU duplex configuration

13.2.1 List of operation commands

The following table describes the operation commands for the BCU duplex configuration.

Table 13-3: List of operation commands

Command name	Description
inactivate bcu standby	Stops the standby BCU.
activate bcu standby	Starts the standby BCU.
redundancy force-switchover	Switches between the active BCU and the standby BCU.
synchronize	Synchronizes the user setting information and usage information of the standby BCU with those of the active BCU.
show system ^{#1}	Shows the operating status of the BCU.
reload ^{#1}	Restarts the BCU.
show logging ^{#2}	Shows the operation log of the active or standby BCU.

#1

See 10. *Device and Software Management* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

#2

See 16. *Log Management* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

13.2.2 Checking the status of the standby BCU

You can check the status of the standby BCU by using the `show system` command. In addition, by specifying the `standby` parameter in the `show logging` command, you can display the operation log of the standby BCU. However, if the standby BCU cannot start due to a failure, you cannot display the operation log.

13.2.3 Restarting a BCU

By specifying the `standby` parameter in the `reload` command, you can restart the standby BCU. In addition, by specifying the `active` parameter, you can restart the active BCU. In this case, the BCU that restarts is the one that becomes the new standby BCU after system switchover.

If you omit all the parameters, the Device restarts.

13.2.4 Replacing a BCU

By replacing the standby BCU during operation in a duplex configuration, you can replace BCUs without stopping the Device. Before replacement, stop the standby BCU to be replaced by using the `inactivate bcu standby` command. To replace the active BCU, before replacement, perform system switchover in advance by using the `redundancy force-switchover` command. After completing the replacement work, start the standby BCU by executing the `activate bcu standby` command.

13.2.5 Synchronizing the user setting information and usage information

If the information shown in *Table 13-1: User setting information and usage information synchronized during operation* is inconsistent between the active and standby systems during

operation, you must check the synchronization timing and make the information consistent.

13.2.6 Performing system switchover

If the Device is operating in a duplex configuration, you can switch the active BCU by executing the `redundancy force-switchover` command from the active BCU.

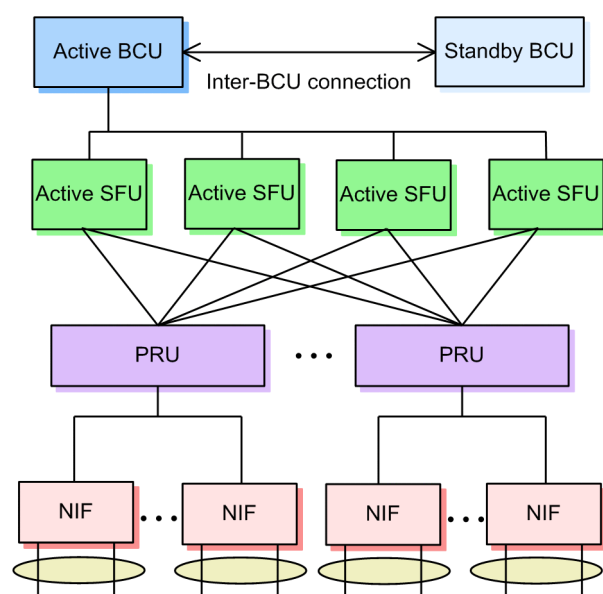
13.3 Description of SFU redundancy

13.3.1 Device configuration when there is redundancy

To create a redundant configuration for a switch fabric unit (SFU), install two or more SFUs in the Device. In a redundant SFU configuration, every SFU operates as an active system. In a redundant SFU configuration, if a failure occurs in an SFU, communication continues by using another SFU operating as an active system. Note that you can maximize the packet transfer performance by installing three or more SFUs in the Device.

The figure below shows the interfaces in a configuration that has redundant BCUs, SFUs, PRUs, and NIFs. Each active SFU connects to each PRU using an independent interface to transfer packets.

Figure 13-2: Interfaces in a configuration with redundant BCUs, SFUs, PRUs, and NIFs



13.3.2 How a redundant configuration operates

Every SFU operates as an active system. If three or more SFUs operate as active systems, the packet transfer performance is maximized. If four SFUs operate as active systems, the packet transfer performance can be maintained if a failure occurs.

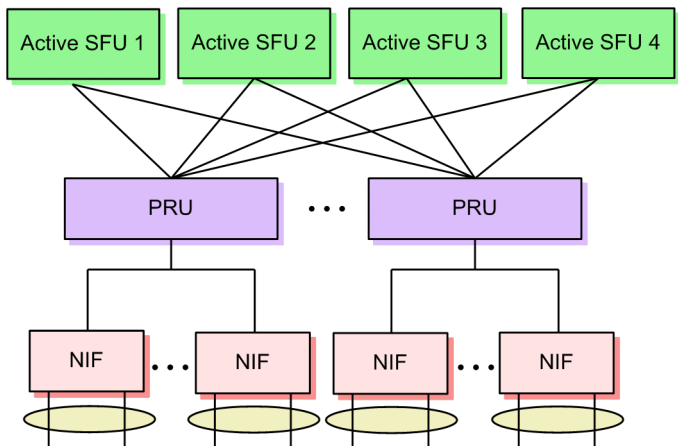
13.3.3 SFU operation when a failure occurs

In an SFU redundant configuration, if a failure occurs in an SFU, communication continues by using the other normal SFUs. The following shows an example of how SFUs operate when a failure occurs.

Before a failure occurs

Four SFUs whose operating status is running are operating. The following figure shows the operation of SFUs before a failure occurs.

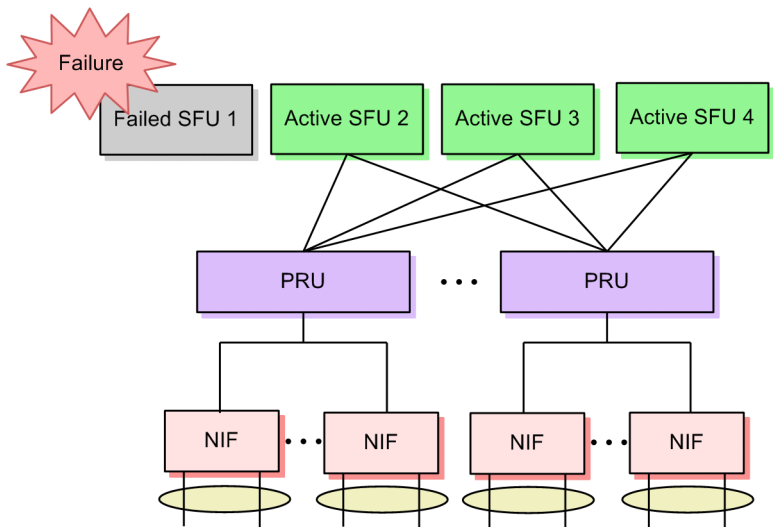
Figure 13-3: Operation before a failure occurs



After s failure occurs

If a failure occurs in SFU1, operation continues by using the other normal SFUs. The following figure shows the operation of the SFUs after a failure occurs.

Figure 13-4: Operation after a failure occurs



13.4 Operation for SFU redundancy

13.4.1 List of operation commands

The following table describes the operation commands for SFU redundancy.

Table 13-4: List of operation commands

Command name	Description
show system [#]	Shows the SFU operating status

#

See *10. Device and Software Management* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

13.4.2 Checking the SFU status

You can check the SFU operating status by using the `show system` command. An example is shown below:

Figure 13-5: Checking the SFU operating status

```
> show system
Date 20XX/12/10 15:11:20 UTC
System: AX8632R, OS-RE, Ver.12.1, [123.1]
      :
      :
SFU1 : active (restart required), fatal error restart 0 time
      Elapsed time : 2 days 2:30
      Lamp : STATUS LED = green , ACTIVE LED = light off
SFU2 : notconnect
      :
SFU4 : active, fatal error restart 0 time
      Elapsed time : 2 days 2:30
      Lamp : STATUS LED = green , ACTIVE LED = light off
      :
>
```


13.5 Description of power supply unit (PS) redundancy

13.5.1 Overview

In the Device, a redundant PS configuration can be created by installing a backup PS. If a redundant PS configuration is created, even when a PS fails and stops supplying power, the remaining PSs automatically start balancing the power load to achieve a stable power supply. In addition, the failed PS can be replaced while the device is active.

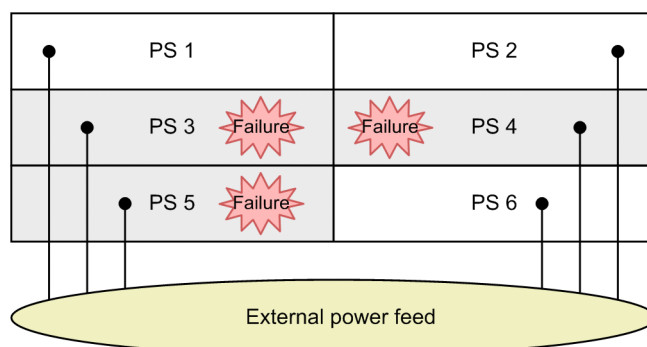
The Device supports redundancy of power supply units and power feeds as methods of creating a redundant PS configuration.

If redundancy in the PS configuration is lost due to a PS failure, the Device outputs a system message and issues an SNMP trap if the `power redundancy-mode` configuration command has been set. If you want to continue the operation in a redundant configuration, replace the failed PS or add a PS. When you replace, add, or move a PS, see the *Hardware Instruction Manual* and observe the precautions.

13.5.2 Redundant power supply units

In this method, at least one additional backup PS is installed over the number of PSs required for device operation. Even if one PS fails, power supply continues with the remaining PSs. Operations can continue if at least the required number of PSs is operating regardless of the installation position of the failed PS. The following figure shows an example of a configuration that has redundant power supply units.

Figure 13-6: Example of a configuration that has redundant power supply units



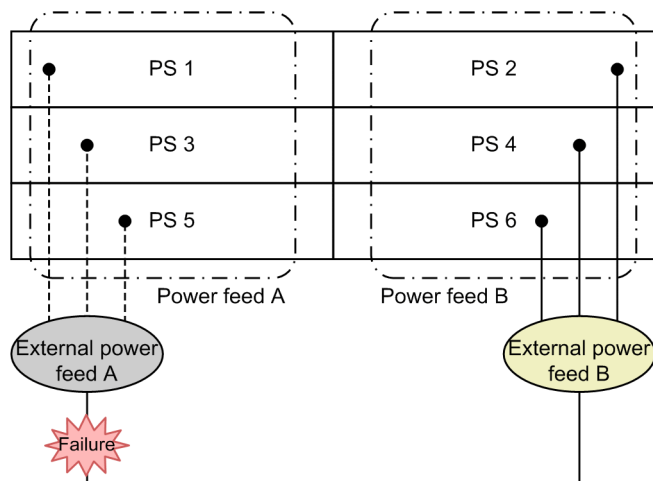
If six PSs are installed and three PSs are required for operation, the operation can continue even if three PSs fail.

If redundancy in the PS configuration is lost due to a PS failure or if redundancy is restored after recovery from failure, the Device outputs a system message and issues an SNMP trap.

13.5.3 Redundant power feeds

In this method, the number of installed backup PSs is the same as the number of PSs required for device operation, and these PSs are divided into two groups and connected directly to different external power feeds. In the same way as redundant power supply units, if the number of PSs required for device operation and the backup PSs are operating, even if one PS fails, power supply can continue with the remaining PSs. In addition, even if power supply from one external power feed becomes cut off, power supply continues from the other external power feed to the Device. The following figure shows an example of a configuration that has redundant power feeds.

Figure 13-7: Example of a configuration that has redundant power feeds



There are two external power feeds. The positions of PSs that can be connected to each feed are predetermined. The following table describes the installation positions of PSs for redundant power feeds.

Table 13-5: Installation positions of PSs for redundant power feeds

Model	Power feed A	Power feed B
AX8616R	PS1, PS3	PS2, PS4
AX8632R	PS1, PS3, PS5	PS2, PS4, PS6

If redundancy in the PS configuration is lost due to a PS failure or if redundancy is restored after recovery from failure, the Device outputs a system message and issues an SNMP trap. Also, if one of the external power feeds fails and redundancy in the power feed configuration is lost, or if redundancy is restored after recovery from a failure, the Device outputs a system message and issues an SNMP trap.

13.5.4 Supply power management

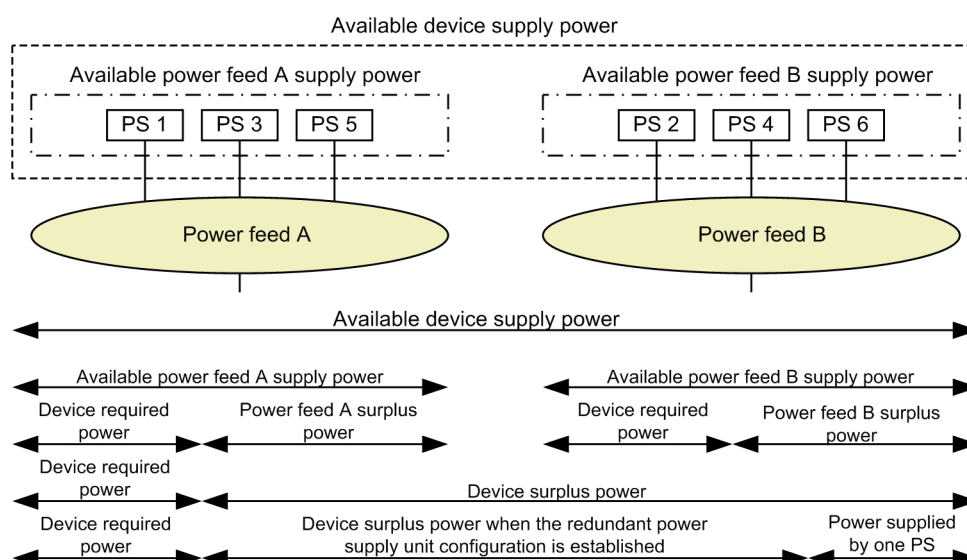
The Device manages supply power according to how the PS, PRU, and NIF are installed. The following table describes the terms related to supply power management.

Table 13-6: Terms related to supply power management

Term	Meaning
Available device supply power	Total amount of power supplied by the PSs (that are supplying power normally) installed in the Device.
Available power feed A supply power	Total amount of power supplied by PSs (that are supplying power normally) installed in power feed A.
Available power feed B supply power	Total amount of power supplied by the PSs (that are supplying power normally) installed in power feed B.
Device required power	Power needed to operate the Device. This does not include the power required for inactive PRUs and NIFs.
Device surplus power	Surplus power that can be used by the Device when no redundant power supply unit and no redundant power feed are required (power obtained by subtracting the "device required power" from the "available device supply power"). If the value is negative, the "available device supply power" is not sufficient.

Term	Meaning
Device surplus power when the redundant power supply unit configuration is established	Surplus power that can be used in the Device while securing power supply unit redundancy (power obtained by subtracting the "power supplied by one PS" from the "device surplus power"). If the value is negative, redundancy in the power supply unit configuration is not established.
Power feed A surplus power	Surplus power that can be used in power feed A (power obtained by subtracting the "device required power" from the "available power feed A supply power"). If the value is negative, redundancy in the power feed configuration is not established in power feed A.
Power feed B surplus power	Surplus power that can be used in power feed B (power obtained by subtracting the "device required power" from the "available power feed B supply power"). If the value is negative, redundancy in the power feed configuration is not established in power feed B.

Figure 13-8: Supply power management (example of installing six PSs)



The Device manages supply power by operating as follows:

(1) When the Device starts up

If the device surplus power is insufficient when PRUs or NIFs start, the Device suppresses the startup of PRUs or NIFs after outputting a system message and issuing an SNMP trap. At that time, suppression is performed per PRU slot. The board whose startup is suppressed will be stopped due to power shortage.

(2) When a PRU or NIF board is added

If the device surplus power is insufficient when PRUs or NIFs start, the Device suppresses the startup of the relevant board after outputting a system message and issuing an SNMP trap. The board whose startup is suppressed will stop because of a power shortage.

(3) When a PS failure occurs

If a PS failure occurs, the Device outputs a PS failure system message and issues an SNMP trap for each failed PS.

If the value for the device surplus power is negative due to a PS failure, the Device continues operation after outputting a system message and issuing an SNMP trap. However, if the number of

PSs is less than the number of PSs required for operation, operation might be unable to continue.

If the value for the device surplus power when a redundant power supply unit configuration is established is negative and PS redundancy is lost, the Device outputs a system message and issues an SNMP trap. Also, in a redundant power feed configuration, if the value for the power feed A surplus power or the power feed B surplus power is negative and PS redundancy is lost, the Device outputs a system message and issues an SNMP trap.

(4) When PS recovers from failure

When the PS recovers from a failure, the Device outputs a PS failure recovery system message and issues an SNMP trap for each failed PS.

Even if the value for the device surplus power reaches or exceeds 0 and the power supply shortage is resolved, PRUs and NIFs stopped due to the power shortage do not start automatically.

If the value for the device surplus power when the redundant power supply unit configuration is established reaches or exceeds 0 and PS redundancy is established, the Device outputs a system message and issues an SNMP trap. Also, in a redundant power feed configuration, if the value for the power feed A surplus power or the power feed B surplus power reaches or exceeds 0 and PS redundancy is established, the Device outputs a system message and issues an SNMP trap.

13.6 PS (power supply unit) redundancy configuration

13.6.1 List of configuration commands

The following table describes the configuration commands for PS (power supply unit) redundancy.

Table 13-7: List of configuration commands

Command name	Description
power redundancy-mode	Sets the monitoring mode for power redundancy. When the PS redundancy configuration is established or lost according to the specified monitoring mode for power redundancy, a system message is displayed.

13.6.2 Configuring the redundant power supply unit

In a redundant power supply unit configuration, a system message can be output and an SNMP trap can be issued when the redundant configuration is established or lost.

Points to note

To display a system message for redundancy of power supply units, you need to specify that the redundant power supply unit is to be monitored for power redundancy by using the `power redundancy-mode` command.

Command examples

1. **(config)# power redundancy-mode 1**

Specifies that the redundant power supply unit is to be monitored for power redundancy.

13.6.3 Configuring the redundant power feed

In the redundant power feed configuration, the Device checks the redundancy of power feeds in addition to PS redundancy established by the redundant power supply unit. When the redundant power feed configuration is established or lost, the Device can output a system message and issue an SNMP trap.

Points to note

To display a system message for a redundant power feed, you need to specify that the redundant power feed is to be monitored for power redundancy by using the `power redundancy-mode` command.

Command examples

1. **(config)# power redundancy-mode 2**

Specifies that both the redundant power supply unit and redundant power feed are to be monitored for power redundancy.

13.7 Operation for PS (power supply unit) redundancy

13.7.1 List of operation commands

The following table describes the operation commands for PS (power supply unit) redundancy.

Table 13-8: List of operation commands

Command name	Description
show system [#]	Shows the device's operating status.
show environment [#]	Shows information about the Device's environment.

#

See 10. *Device and Software Management* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

13.7.2 Checking the PS status

In the items under `Power environment` displayed by the `show environment` command, you can check the PS type, the redundancy configuration, and the status of each PS.

Figure 13-9: Checking the PS status

```
> show environment
:
Power environment
  Input voltage: AC200-240V
  Power redundancy mode: 2 (Power Supply + Input Source)
  Power supply redundancy status
    Power supply: active = 4, required = 1 (Redundant)
    Input source: active = 2(from A) 2(from B), required = 1 (Redundant)
  PS1: active
  PS2: active
  PS3: active
  PS4: active
  :
```

The details you can check are described per display item as follows:

Power redundancy mode

Shows the monitoring mode for power redundancy set in the configuration.

If no mode is displayed, no value is set in the configuration. For that reason, a system message is not output or an SNMP trap is not issued if the PS redundancy configuration is established or lost.

Power supply

Shows the status of the redundant power supply unit including the number of PSs supplying power to the Device and the number of PSs necessary for the operation of the Device.

If the number of PSs supplying power to the Device is equal to or less than the number of PSs necessary for the operation of the Device, redundancy in the power supply unit configuration is not established. If you want to operate the Device in a redundant power supply unit configuration, replace or add PSs.

Example 1:

If the number of PSs necessary for the operation of the Device is two, and the number of PSs supplying power to the Device is three (redundancy in the power supply unit configuration is established)

Power supply : active = 3 required = 2 (Redundant)

Example 2:

If the number of PSs necessary for the operation of the Device is two, and the number of PSs supplying power to the Device is two (redundancy in the power supply unit configuration is not established)

Power supply : active = 2 required = 2 (Non-Redundant)

Input source

Shows the status of redundant power feed, including the number of PSs supplying power to power feed A, the number of PSs supplying power to power feed B, and the number of PSs necessary for operation of the Device.

If the number of PSs supplying power to power feed A or power feed B is less than the number of PSs necessary for the operation of the Device, redundancy in the power feed configuration is not established. If you want to operate the Device in the redundant power feed configuration, replace or add PSs.

Example 1:

If the number of PSs in each power feed necessary for the operation of the Device is two, the number of PSs supplying power to power feed A is three, and the number of PSs supplying power to power feed B is two (redundancy in the power feed configuration is established)

Input source : active = 3 (from A), 2 (from B) required = 2 (Redundant)

Example 2:

If the number of PSs in each power feed necessary for the operation of the Device is two, the number of PSs supplying power to power feed A is three, and the number of PSs supplying power to power feed B is one (redundancy in the power feed configuration is not established)

Input source : active = 3 (from A), 1 (from B) required = 2 (Non-Redundant)

PS<*ps no.*>

Shows the status of each PS.

13.7.3 Checking the supply power

In the items under `Power usage` displayed by the `show environment` command, you can check the available supply power, required power, and surplus power of the Device.

Figure 13-10: Checking the power status

```
> show environment
:
Power usage
  Total power capacity:                10168.00 W
    Input source A:                    5084.00 W
    Input source B:                    5084.00 W
  Total power allocated:                1477.00 W
  Total power available for additional boards: 8691.00 W
  Power available (Power supply unit redundant case): 6149.00 W
  Power available (Input source redundant case)
    Input source A:                    3607.00 W
    Input source B:                    3607.00 W
.
```


Chapter

14. System Message Output and Log Management

This chapter describes system message output and log management.

- 14.1 Description
- 14.2 Configuration
- 14.3 Operation

14.1 Description

14.1.1 Outputting messages

The Device reports operating information and failure information as system messages.

System messages, operation command response messages, and configuration error messages can be output to operation terminals, but can also be sent to other devices on the network by using the syslog interface or email functionality. Also, if the trap sending functionality is used, a system message trap can be sent to the SNMP manager. This functionality means logs can be managed centrally even if multiple devices are being managed.

Items to be output to each destination and operation terminal can be specified based on conditions appropriate for each destination.

Note that the Device does not support functionality to receive syslog messages from other devices. In syslog messages generated on the Device, the HOSTNAME field of the HEADER part defined in RFC 3164 is not set.

14.1.2 Storing logs

System messages, operation command response messages, and configuration error messages are stored in the Device as entries in the operation log and statistics log. You can use this information to manage the operating statuses of the Device and the statuses of failures. In addition, you can set the number of operation log entries to be stored per message type. The following describes the features of the operation log and statistics log:

Operation log

An operation log records information about events that occur during device operation in chronological order. This information is the same as the system messages. The following information is stored as operation log entries:

- Operation command response messages
- Configuration error messages
- System messages

Statistics log

In the statistics log, system messages regarding failures and warnings occurring on the Device are grouped by message ID. In addition, the statistics log also contains information such as the date and time the event occurred for the first time, the date and time the event last occurred, and the cumulative number of times that the event occurred.

Administrators can view the information by using an operation command.

When BCU restarts or stops, the operation log and statistics log are automatically saved into the internal flash memory. However, if BCU restarts or stops due to a failure, the operation log and statistics log might not be saved. For that reason, we recommend that a syslog message be sent.

14.2 Configuration

14.2.1 List of configuration commands

The following table describes the configuration commands for system message output and log management.

Table 14-1: List of configuration commands

Command name	Description
logging email	Specifies the destination email address for email transmission.
logging email-filter	Specifies the conditions for email transmission by using the message type list and event level.
logging email-from	Specifies the source email address for email transmission.
logging email-interval	Specifies the interval for email transmission.
logging email-server	Specifies the SMTP server information.
logging save-count	Specifies the minimum number of operation log entries to be stored per message type.
logging syslog-facility	Specifies the facility to be added to the header section of the syslog send data.
logging syslog-filter	Specifies the conditions for syslog transmission by using the message type list and event level.
logging syslog-host	Specifies the destination syslog server.
logging syslog-severity	Specifies the severity to be added to the header section of the syslog send data.
message-list	Generates a message type list.
message-type	Specifies the message type to be managed as an output condition.
username ^{#1}	With the <code>logging-console</code> parameter, specifies the system message screen output conditions based on the message type list and event level.
snmp-server traps ^{#2}	With the <code>system_msg_trap_message_list</code> and <code>system_msg_trap_event_level</code> parameters, specifies the conditions for system message trap transmission based on the message type list and event level.

#1

See 6. *Login Security and RADIUS or TACACS+* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

#2

See 13. *SNMP* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

14.2.2 Configuring the minimum number of operation log entries to be stored

Points to note

The minimum value can be set for the number of log entries to be stored into the Device per message type. By using this setting, you can protect a specified number of log entries even if the total amount of stored log entries exceeds the size of the storage area. If there is free space in the log storage area, a number of log entries greater than specified are stored.

Command examples

1. **(config)# logging save-count BCU 3000**

Stores 3000 operation log entries for the message type BCU.

14.2.3 Configuring syslog output

Points to note

Use the syslog output functionality to send user input commands and messages to the syslog server.

Command examples

1. **(config)# logging syslog-host 192.0.2.1**
Specifies the IPv4 address 192.0.2.1 for the destination syslog server.
2. **(config)# logging syslog-host 2001:db8:1:1::1**
Specifies the IPv6 address 2001:db8:1:1::1 for the destination syslog server.
3. **(config)# logging syslog-host 192.0.2.1 vrf 2**
Specifies the IPv4 address 192.0.2.1 and VRF ID 2 for the destination syslog server.

14.2.4 Configuring email output

Points to note

Use the email functionality to send log information to a remote host or a PC.

Command examples

1. **(config)# logging email system@example.com**
Specifies `system@example.com` as the destination email address.
2. **(config)# logging email-server 192.0.2.1**
Specifies `192.0.2.1` as the address of the SMTP server used for email transmission.

14.2.5 Controlling message output

The message output conditions can be set in the Device according to the output destination such as the console screen of an operation terminal and the syslog server.

(1) Example of creating a message type list

Points to note

Create a message type list in which output targets and output-suppressed targets are specified by message types.

If a message type list in which output-suppressed targets have been specified is set as an output condition, messages for any types other than the specified message types are to be output. If specifying the event level is omitted, messages for event level 6 or lower are to be output. If specifying the message type list is omitted, messages for all message types are to be output.

Command examples

1. **(config)# message-list MSG_LIST**
Creates a message type list (`MSG_LIST`).
2. **(config-msg-list)# message-type include BCU**

```
(config-msg-list)# exit
```

Sets the message type BCU as an output target.

3.

```
(config)# message-list SAMPLE_LIST
```

Creates a message type list (SAMPLE_LIST).

4.

```
(config-msg-list)# message-type exclude BCU
```



```
(config-msg-list)# exit
```

Sets the message type BCU as an output-suppression target.

(2) Example of setting conditions for outputting messages to operation terminals

Points to note

To set conditions for outputting messages to operation terminals, use the `logging-console` parameter of the `username` command.

Command examples

1.

```
(config)# username default_user logging-console message-list MSG_LIST event-level 4
```

Sets the message type list (MSG_LIST) and event level 4 or lower as a condition for outputting messages to the operation terminals of all logged-in users.

(3) Example of setting conditions for sending messages to the syslog server

Points to note

To set conditions for sending messages to the syslog server, use the `logging syslog-filter` command.

Command examples

1.

```
(config)# logging syslog-filter message-list MSG_LIST
```

Sets the message type list (MSG_LIST) as a condition for sending messages to the syslog server.

(4) Example of setting conditions for sending messages to the email server

Points to note

To set conditions for sending messages to the email server, use the `logging email-filter` command.

Command examples

1.

```
(config)# logging email-filter event-level 4
```

Sets event level 4 or lower as a condition for sending messages to the email server.

(5) Example of setting conditions for sending messages to the SNMP server

Points to note

Use the `system_msg_trap_message_list` and `system_msg_trap_event_level` parameters of the `snmp-server traps` command to set conditions for sending messages to the SNMP

server.

Command examples

1. **(config)# snmp-server traps system_msg_trap_message_list
SAMPLE_LIST system_msg_trap_event_level 4**

Sets the message type list (*SAMPLE_LIST*) and event level 4 or lower as a condition for sending messages to the SNMP server.

14.3 Operation

14.3.1 List of operation commands

The following table describes the operation commands for system message output and log management.

Table 14-2: List of operation commands

Command name	Description
show logging	Shows the log entries recorded by the Device and the minimum number of log entries to be stored.
clear logging	Clears the log entries recorded by the Device.

14.3.2 Viewing and deleting log entries

(1) Viewing log entries

You can view entries in the operation log and statistics log by using the `show logging` command. The following figure shows the result of executing the command.

Figure 14-1: Result of executing the show logging command

```
> show logging
Date 20XX/11/07 15:54:12 UTC
System information
  AX8616R, OS-RE, Ver.12.1, BCU1(active)
Logging information
20XX/11/07 15:54:12 UTC 1-1(A) S6 KEY operator(tty00): > show logging
20XX/11/07 15:53:45 UTC 1-1(A) S6 BCU 01101001 00 023902000000 Initialization is
complete.
20XX/11/07 15:49:34 UTC 1-1(A) S3 PS 01202020 00 0aec02000000 The power supply
is insufficient.
```

To filter and output operation log entries, specify the `message-type` and `event-level` parameters in the `show logging` command. The following figures show the result of executing the command.

Figure 14-2: Result of executing the show logging command (with the message-type parameter specified)

```
> show logging message-type BCU
Date 20XX/11/07 15:54:12 UTC
System information
  AX8616R, OS-RE, Ver.12.1, BCU1(active)
Logging information
20XX/11/07 15:53:45 UTC 1-1(A) S6 BCU 01101001 00 023902000000 Initialization is
complete.
```

Figure 14-3: Result of executing the show logging command (with event-level parameter specified)

```
> show logging event-level 4
Date 20XX/11/07 15:54:12 UTC
System information
  AX8616R, OS-RE, Ver.12.1, BCU1(active)
Logging information
20XX/11/07 15:49:34 UTC 1-1(A) S3 PS 01202020 00 0aec02000000 The power supply
is insufficient.
```

(2) Deleting log entries

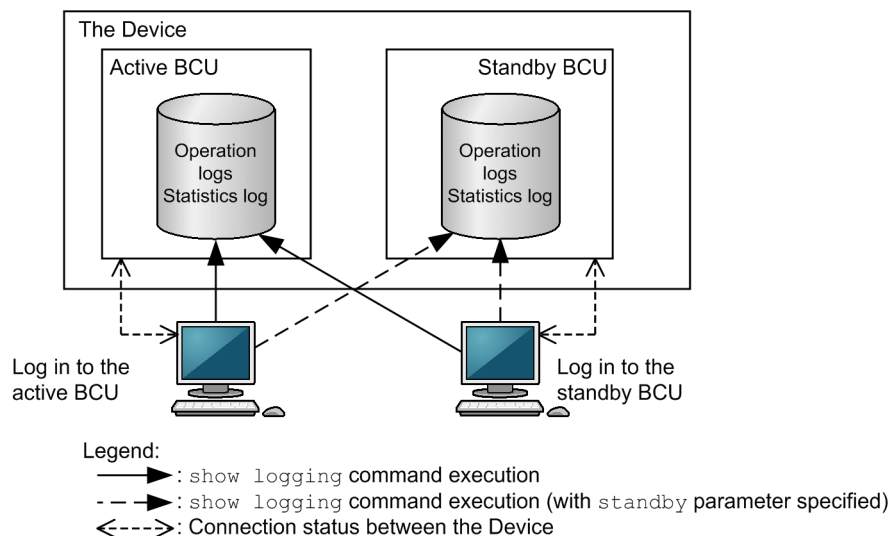
You can delete entries in the operation log and statistics log by using the `clear logging` command.

(3) Viewing and deleting log entries in the BCU duplex configuration

When you view or delete log entries in the BCU duplex configuration, the target system differs depending on the specification of the `standby` parameter.

The figure below shows the target to be viewed when the `standby` parameter is specified in the `show logging` command. Note that log entries in the active BCU cannot be deleted from the standby BCU.

Figure 14-4: Viewing log entries in the BCU duplex configuration

**(4) Checking the number of operation log entries to be stored**

You can check the set number of operation log entries to be stored by specifying the `save-count` parameter in the `show logging` command.

Chapter

15. SNMP

This chapter describes the SNMP agent functionality of the Device, with a focus on supported specifications.

- 15.1 Description
- 15.2 Configuration
- 15.3 Operation

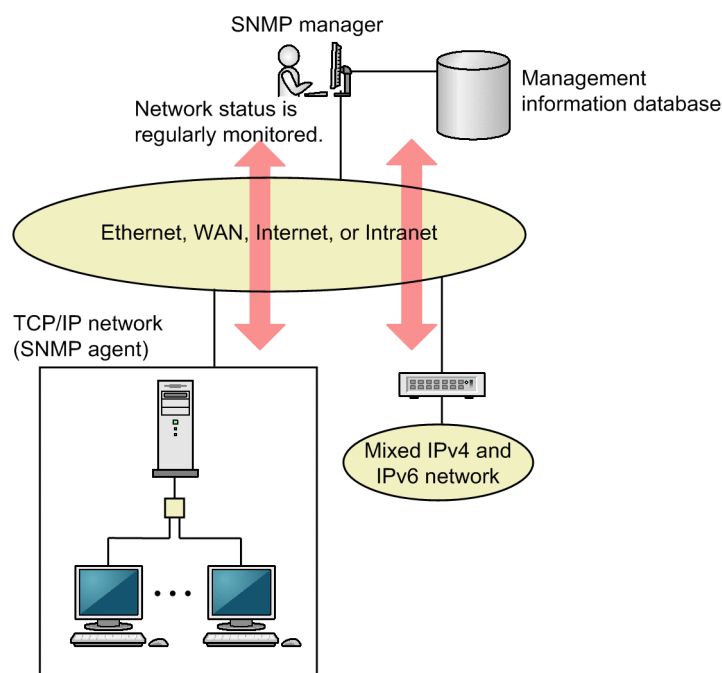
15.1 Description

15.1.1 Overview of SNMP

(1) Network management

Maintaining the operating environment and performance of a network system requires high-level network management. The Simple Network Management Protocol (SNMP) is an industry-standard network management protocol with which you can manage a multi-vendor network consisting of network devices that support SNMP. A server that manages a network by collecting management information is called an SNMP manager, and a network device that is managed is called an SNMP agent. The following figure provides an overview of network management.

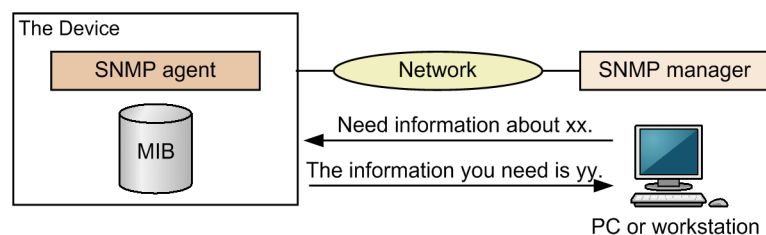
Figure 15-1: Overview of network management



(2) SNMP agent functionality

The Device SNMP agent is a program included in the devices on a network. An SNMP agent has functionality that provides the SNMP manager with information internal to device. This information is called the management information base (MIB). SNMP manager is software that retrieves the information on a device, edits and processes it, and provides it to the network administrator for management of the network. The following figure shows an example of MIB retrieval.

Figure 15-2: Example of MIB retrieval

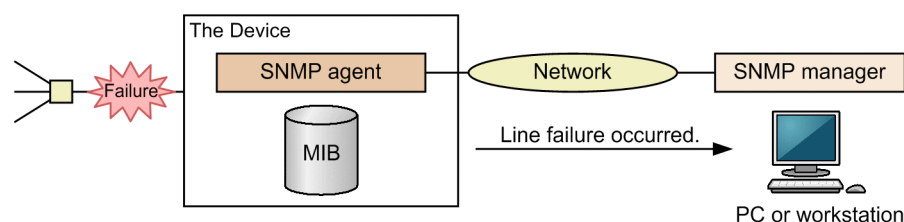


An SNMP command for displaying MIB information is included as an operation command on the Device. This command displays an SNMP agent MIB on the local device and a remote device.

The Device supports SNMPv1 (RFC 1157), SNMPv2C (RFC 1901), and SNMPv3 (RFC 3410). To manage a network using an SNMP manager, use the SNMPv1, SNMPv2C, or SNMPv3 protocol. Note that the SNMPv1, SNMPv2C, and SNMPv3 protocols can be used simultaneously.

In addition, an SNMP agent has functionality, called a trap or an inform for reporting events (mainly failure information). The SNMP manager can learn about changes by receiving traps or informs without regularly monitoring changes to the device status. Note, however, that the SNMP manager cannot verify whether a trap has arrived from a device because traps use UDP. Accordingly, some traps might not arrive at the SNMP manager due to network congestion. The following figure shows an example of a trap.

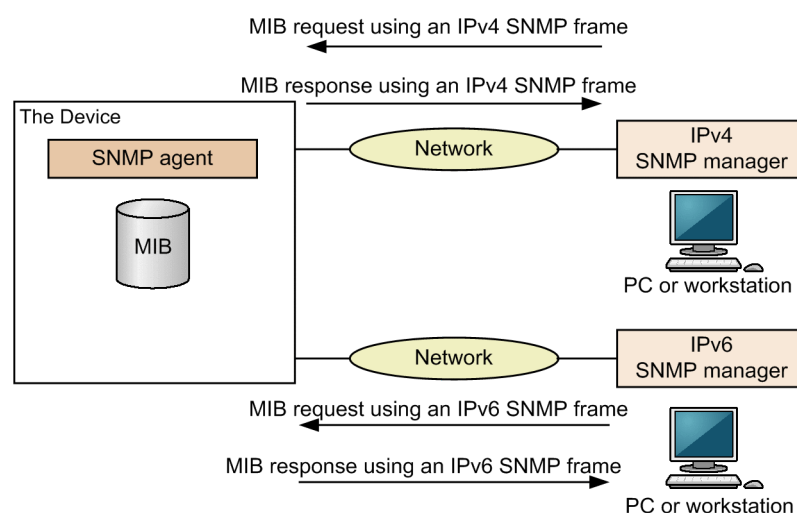
Figure 15-3: Example of a trap



Like a trap, an inform is an event notification function using UDP, but it requests a response from the SNMP manager. Therefore, you can verify whether an inform request has arrived by checking for a response. This allows you to deal with a problem such as network congestion by resending an inform.

SNMP on the Device supports IPv6. By setting IPv4 or IPv6 addresses of SNMP managers in the configuration, the Device can respond to MIB requests from the SNMP managers and can send traps or informs to the SNMP managers. The following figure shows an example of MIB requests from IPv4 and IPv6 SNMP managers and the responses.

Figure 15-4: Example for MIB requests from IPv4 and IPv6 SNMP managers and the responses



(3) SNMPv3

In addition to having all SNMPv2C functionality, SNMPv3 includes functionality for improved management security. By authenticating and encrypting SNMP packets transmitted over a network, SNMP packets are protected from network risks such as sniffing, spoofing, defacing, and resending, security functionality that was not possible in SNMPv2C, which combined a

community name and the IP address of an SNMP manager.

(a) **SNMP entity**

In SNMPv3, an SNMP manager and SNMP agent are collectively called an SNMP entity. SNMPv3 on the Device supports SNMP entities equivalent to SNMP agents.

(b) **SNMP engine**

The SNMP engine provides services for sending and receiving authenticated and encrypted messages and for controlling access to managed objects. The SNMP engine and the SNMP entity are in a one-to-one relationship. SNMP engines within the same management domain are identified by unique SNMP engine IDs.

(c) **User authentication and privacy functionality**

SNMPv1 and SNMPv2C authenticate community names, but SNMPv3 authenticates users. In addition, SNMPv3 supports privacy functionality (encryption and decryption) that was not supported in SNMPv1 and SNMPv2C. User authentication and the privacy functionality can be set for each user.

The Device supports the following two protocols for user authentication:

- HMAC-MD5-96, which uses the message digest algorithm. The first 96 bits of the 128-bit digest are used. The private key is 16 octets.
- HMAC-SHA-96, which uses the SHA message digest algorithm. The first 96 bits of the 160-bit SHA digest are used. The private key is 20 octets.

The following protocol is supported as the privacy protocol:

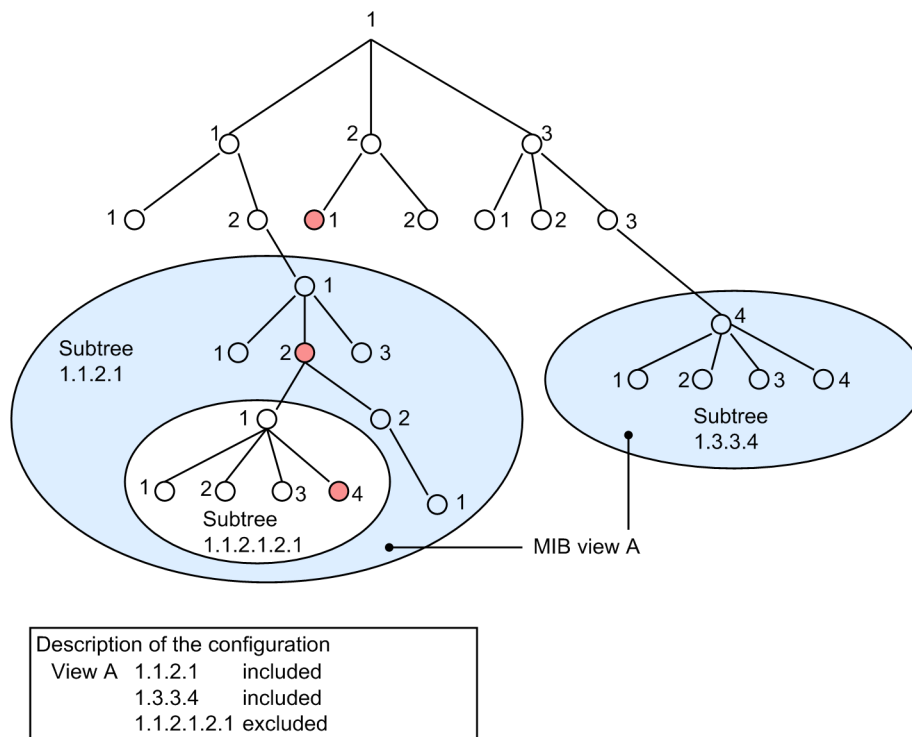
- CBC-DES (Cipher Block Chaining - Data Encryption Standard), which is an encryption protocol that enforces in CBC mode DES (56-bit key), a symmetric-key cryptography algorithm.

(d) **Access control by the MIB view**

In SNMPv3, a collection of accessible MIB objects can be set for each user. This collection is called a MIB view. A MIB view is expressed by aggregating view subtrees that indicate the trees of MIB object IDs. When aggregating view subtrees, you can choose *included* (for inclusion in the MIB view) or *excluded* (for exclusion from the MIB view) for each view subtree. A MIB view can be set as a read view, write view, or notify view for individual users.

The figure below shows an example of a MIB view. When configuring a MIB view such as the one shown in *Figure 15-5: Example of a MIB view*, group the MIB subtrees that are to be a part of a MIB tree to configure them. As shown in the figure, object ID 1.1.2.1.2 can be accessed in MIB view A because it is included in subtree 1.1.2.1. However, object ID 1.2.1 cannot be accessed because it is not included in any subtrees. Also, object ID 1.1.2.1.2.1.4 cannot be accessed because subtree 1.1.2.1.2.1 is excluded from view A.

Figure 15-5: Example of a MIB view



15.1.2 MIB overview

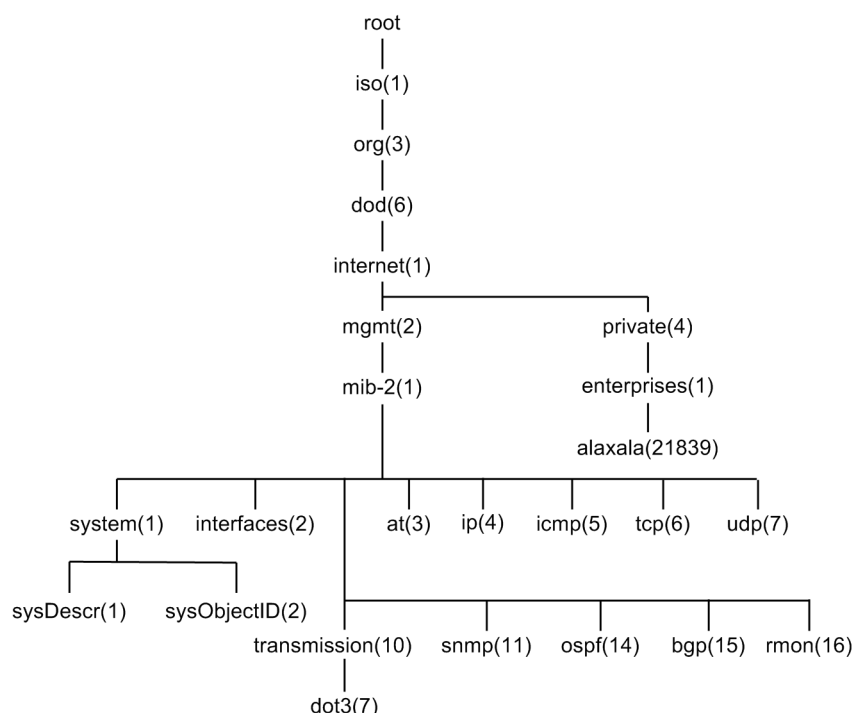
A device manages and provides SNMP managers with the following two types of MIBs: One is defined in an RFC, and the other is information prepared by the vendor who developed the device.

A MIB defined in an RFC is called a *standard MIB*. Because standard MIBs are standardized, there are no differences in the information provided. A MIB provided independently by a device manufacturer is called a *private MIB*, and its contents vary depending on the device. Note, however, that MIB operations, including the retrieval and specification of information, are common to both standard and private MIBs. An operation specifies only the device and the target MIB information. Specify the device by using an IP address and specify the MIB information by using an object ID.

(1) Structure of a MIB

Because a MIB has a tree structure, each node is identified by a number. Each item of MIB information is uniquely identified by assigning a sequential number to each node starting from the root. This sequential number is called the object ID. The object ID is assigned by adding, from the root, lower-level object group numbers by using dot notation. For example, the sysDescr MIB in the figure below is expressed by its object ID 1.3.6.1.2.1.1.1. The following figure shows an example of a MIB tree structure.

Figure 15-6: MIB tree structure



(2) Expressing MIB objects

An object ID consists of numbers in dot notation (for example, 1.3.6.1.2.1.1.1). Because a number-only ID is not easy to understand, some managers use mnemonics such as sysDescr for specification. If you specify a MIB by using a mnemonic, you must ascertain beforehand the MIB mnemonics the SNMP manager can use. To check the mnemonics that SNMP commands for the Device can use, execute the `snmp lookup` command.

(3) Index

Although you use an object ID when you specify a MIB, some MIBs have only one information item whereas other MIBs contain multiple information items. You can identify a MIB by using an index. An index is expressed by adding a number after the object ID, and is used to indicate the number of the item of information.

If a MIB contains only one information item, add `.0` after the MIB object ID. If a MIB contains multiple information items, add a number indicating the number of the information items after the MIB object ID. For example, `ifType` (1.3.6.1.2.1.2.2.1.2) indicates the interface type. The Device has multiple interfaces. To check a specific interface type, you must specify the type specifically as type of the second interface. If you specify the type by using the MIB, add the index `.2` to indicate the second item after the MIB, resulting in `ifType.2` (1.3.6.1.2.1.2.2.1.2.2).

How an index is expressed depends on the MIB. A MIB entry expressed as `INDEX {xxxxx,yyyyy,zzzzz}` in the MIB definition section of an RFC or other document has as its index `xxxxx`, `yyyyy`, and `zzzzz`. Check the index for each MIB before performing MIB operations.

(4) MIBs supported by the Device

The Device provides the MIBs necessary for managing networks, such as those for device status, interface statistics, and device information. Note that the definition file of private MIBs (ASN.1) is provided with the software.

For details about MIBs, see *MIB Reference For Version 12.1*.

15.1.3 SNMPv1 and SNMPv2C operations

For the collection or setting of management data (MIB: management information base), SNMP provides the following four operations:

- **GetRequest:** Extracts the information of the specified MIB.
- **GetNextRequest:** Extracts information of the MIB after the specified MIB.
- **GetBulkRequest:** Extended version of GetNextRequest.
- **SetRequest:** Sets a value for the specified MIB.

The above operations are performed for a device (SNMP agent) from the SNMP manager. Each operation is described below.

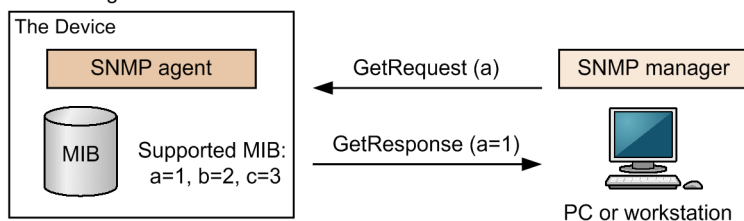
(1) GetRequest operation

The GetRequest operation is used when an SNMP manager extracts MIB information from a device (agent functionality). One or more MIBs can be specified for this operation.

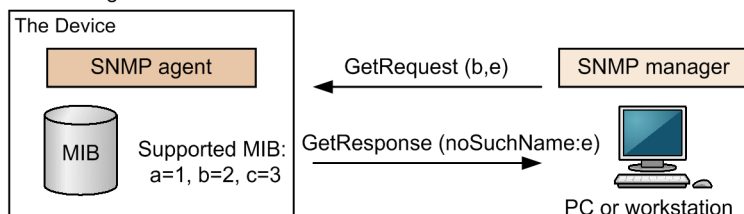
If the device holds the applicable MIB, the GetResponse operation returns the MIB information. If the device does not hold the applicable MIB, the GetResponse operation returns noSuchName. The following figure shows the GetRequest operation.

Figure 15-7: GetRequest operation

- When the target MIB exists

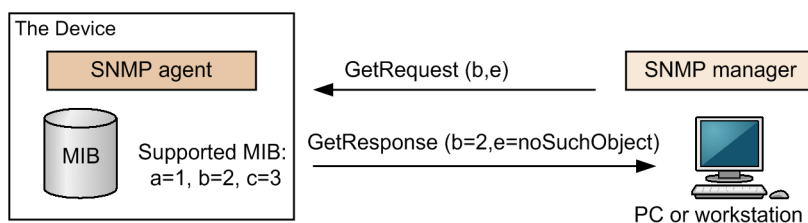


- When the target MIB does not exist



In SNMPv2C, if the device does not hold the applicable MIB, the GetResponse operation returns noSuchObject as the MIB value. The following figure shows the GetRequest operation for SNMPv2C.

Figure 15-8: GetRequest operation for SNMPv2C



(2) GetNextRequest operation

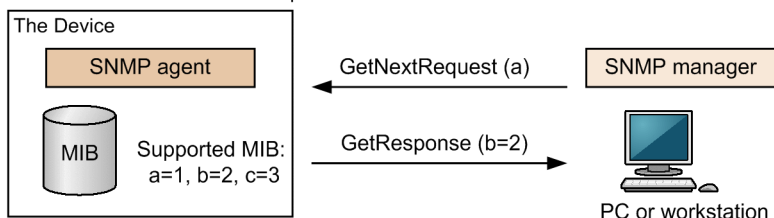
The GetNextRequest operation is similar to the GetRequest operation. Whereas the GetRequest operation is used for reading the specified MIB, the GetNextRequest operation is used to extract

the MIB after the specified MIB. One or more MIBs can be specified for this operation.

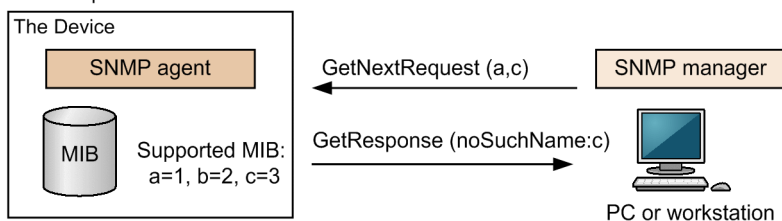
If the device holds the MIB following the specified one, the GetResponse operation returns the MIB. If the specified MIB is the last MIB, the GetResponse operation returns noSuchName. The following figure shows the GetNextRequest operation.

Figure 15-9: GetNextRequest operation

- When there is an MIB after the specified MIB

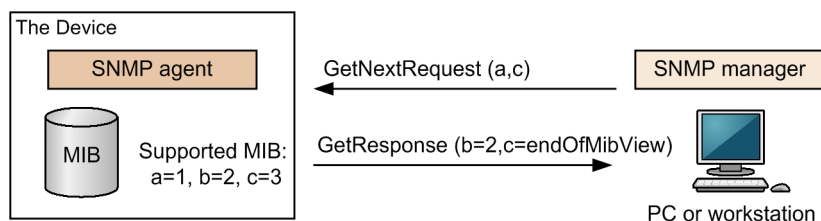


- When the specified MIB is the last MIB



In SNMPv2C, if the specified MIB is the last MIB, the GetResponse operation returns endOfMibView as the MIB value. The following figure shows the GetNextRequest operation for SNMPv2C.

Figure 15-10: GetNextRequest operation for SNMPv2C



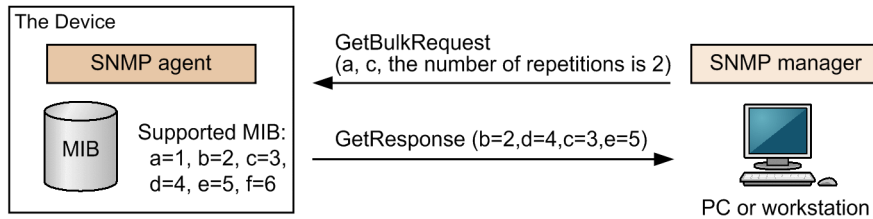
(3) GetBulkRequest operation

The GetBulkRequest operation is an extended GetNextRequest operation. By using this operation, you can set a number of repetitions. From the items after the specified MIB, you can extract as many MIBs as the specified number of repetitions. One or more MIBs can be specified for this operation.

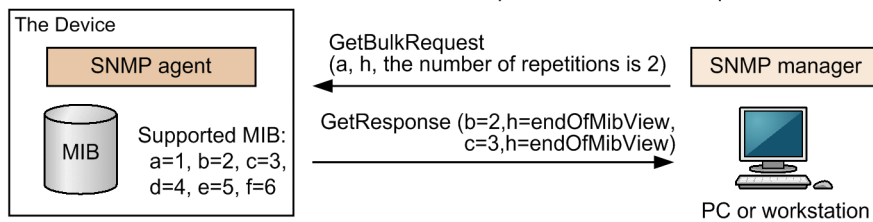
If a device has many MIBs as the specified number of repetitions from the item after the specified MIB, the GetResponse operation returns the MIB. If the specified MIB is the last MIB, or the last MIB is retrieved before the specified number of repetitions, the GetResponse operation returns endOfMibView as the MIB value. The following figure shows the GetBulkRequest operation.

Figure 15-11: GetBulkRequest operation

- When there is an MIB after the specified MIB



- When the last MIB is obtained before the number of repetitions has been completed

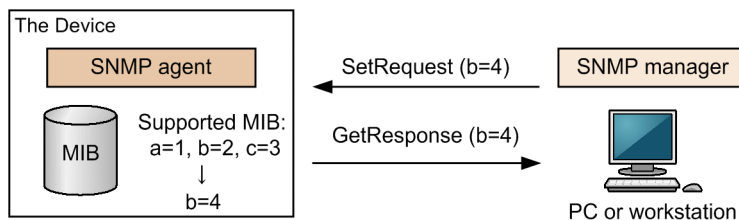


(4) SetRequest operation

The SetRequest operation is similar to the GetRequest, GetNextRequest, and GetBulkRequest operations because it is performed for a device (agent functionality) from the SNMP manager, but the method for setting a value for the SetRequest operation is different from that of the other operations.

The SetRequest operation specifies both a value to be set and a MIB. When a value is specified, the GetResponse operation returns the MIB and the setting value. The following figure shows the SetRequest operation.

Figure 15-12: SetRequest operation



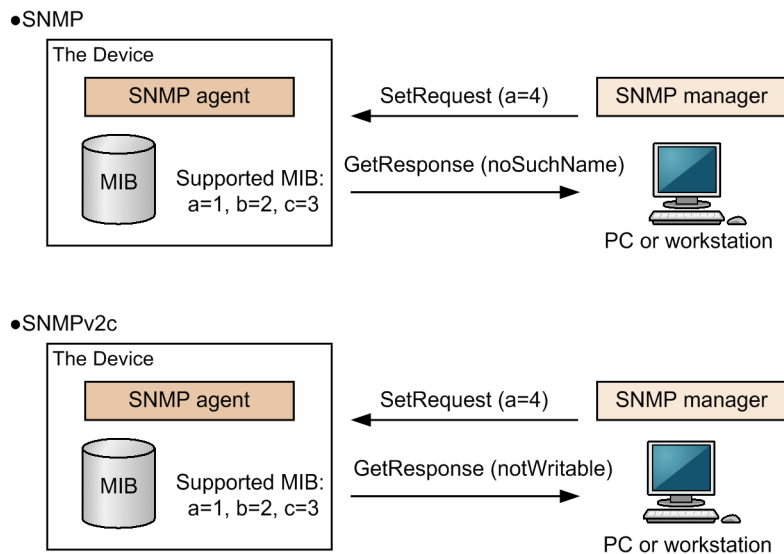
(a) Response when a MIB cannot be configured

The following are three cases when a MIB cannot be configured:

- The MIB is read-only (includes managers that belong to read-only communities).
- The setting value is not correct.
- Configuration cannot be performed because of the status of the device.

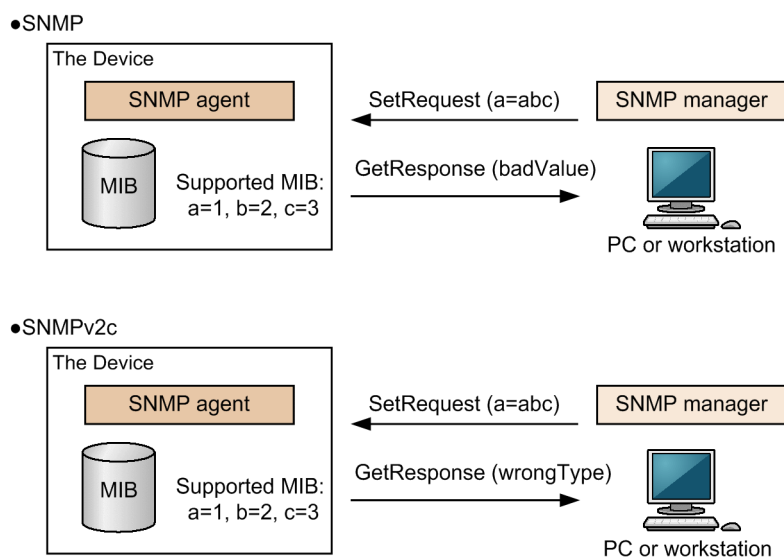
Each case returns a different response. If the MIB is read-only, GetResponse operation returns noSuchName. In SNMPv2C, if the MIB is read-only, the GetResponse operation returns notWritable. The following figure shows the SetRequest operation when the MIB is read-only.

Figure 15-13: SetRequest operation when the MIB variable is read-only



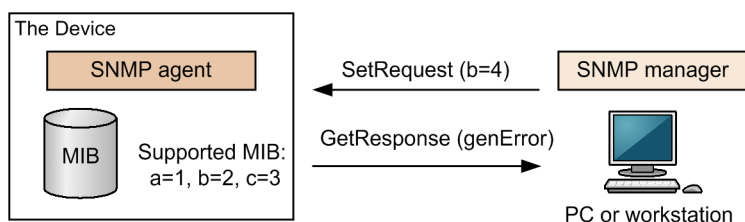
If the type of the setting value is not correct, the GetResponse operation returns `badValue`. In SNMPv2C, if the type of the setting value is not correct, the GetResponse operation returns `wrongType`. The following figure shows the SetRequest operation when the type of the setting value is not correct.

Figure 15-14: Example of the SetRequest operation when the type of the setting value is not correct



If configuration is not possible because of the status of the device, `genError` is returned. For example, when an attempt is made to set a value on a device, if a setting timeout is detected on the device, `genError` is returned. The following figure shows the SetRequest operation when configuration is not possible because of the status of the device.

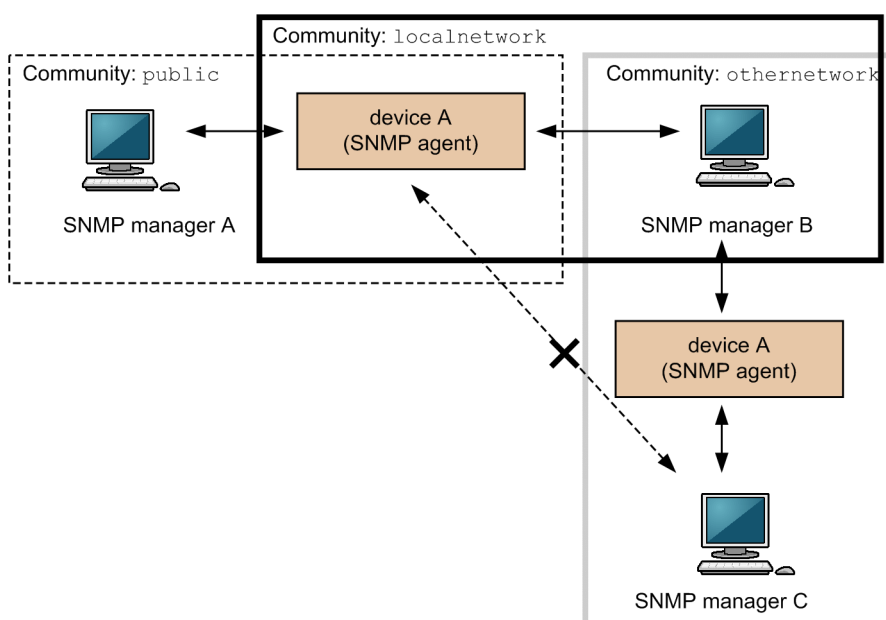
Figure 15-15: SetRequest operation when configuration is not possible because of the status of the device



(5) Operational restrictions applying to communities

In SNMPv1 and SNMPv2C, restrictions can be applied to SNMP managers that perform operations under the community concept. A community is the assignment of an SNMP manager that performs operations and an SNMP agent to a group. To perform MIB operations, the SNMP manager and the SNMP agent must belong to the same group (community). The following figure shows the operation of a community.

Figure 15-16: Operation of a community



Device A belongs to the `public` community and the `localnetwork` community, but it does not belong to the `othernetwork` community. In this case, device A accepts MIB operations requested by SNMP manager A in the `public` community and SNMP manager B in the `localnetwork` community, but it does not accept operations requested by SNMP manager C in the `othernetwork` community.

(6) Operational restrictions applying to IP addresses

In consideration of security risks, the Device can be configured so that they do not accept MIB operations if the combination of community and IP address of the SNMP manager does not match an access list. To use SNMPv1 and SNMPv2C on the Device, you must register communities by using a configuration command. A community is specified by using a character string. In addition, `public` is generally used for a community name.

(7) Error status codes for SNMP operations

If an error occurs during an operation, the SNMP agent assigns an error code for the error status and returns a response in the GetResponse operation. The response contains the number of the MIB information where the error occurred set as the error location number. If the result of the operation

is normal, a code indicating no errors is set as the error status and a response in the GetResponse operation that contains the MIB information of the operations actually performed is returned. The following table describes the error status codes.

Table 15-1: Error status codes

Error status	Code	Description
noError	0	No error occurred.
tooBig	1	The data size is too large to be set as a value in the PDU.
noSuchName	2	The specified MIB was not found or writing is not allowed.
badValue	3	The setting value is incorrect.
readOnly	4	A write attempt failed (the Device does not return this status).
genError	5	Another error occurred.
noAccess	6	A set operation was attempted for a MIB that cannot be accessed.
wrongType	7	A type different from the type required for the MIB was specified.
wrongLength	8	A length different from the length required for a MIB was specified.
wrongEncoding	9	The ASN.1 encoding was incorrect.
wrongValue	10	The MIB value was incorrect.
noCreation	11	The applicable MIB does not exist.
inconsistentValue	12	A value cannot be set due to an inconsistency.
resourceUnavailable	13	A resource required for setting a value cannot be used.
commitFailed	14	An attempt to update a value failed.
undoFailed	15	The original value could not be restored when an attempt to update a value failed.
notWritable	17	The set operation cannot be performed.
inconsistentName	18	Creation is not currently possible because the MIB does not exist.

15.1.4 SNMPv3 operation

For the collection or setting of the management data (MIB: management information base), SNMP provides the following four operations:

- GetRequest: Extracts the information of the specified MIB.
- GetNextRequest: Extracts information of the MIB after the specified MIB.
- GetBulkRequest: Extended version of GetNextRequest.
- SetRequest: Sets a value for the specified MIB.

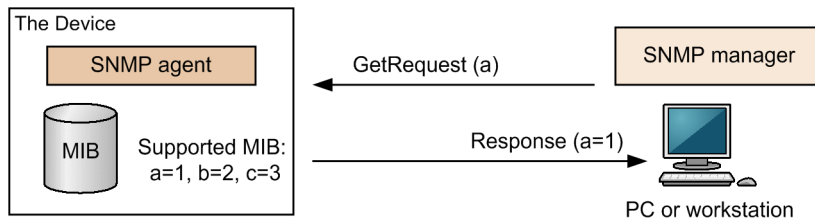
The above operations are performed for a device (SNMP agent) from the SNMP manager. Each operation is described below.

(1) GetRequest operation

The GetRequest operation is used when an SNMP manager extracts MIB information from a device (agent functionality). One or more MIBs can be specified for this operation. If a device holds the applicable MIB, the Response operation returns the MIB information.

The following figure shows the GetRequest operation.

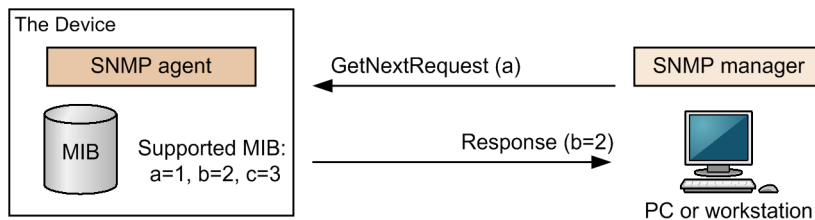
Figure 15-17: GetRequest operation

**(2) GetNextRequest operation**

The GetNextRequest operation is similar to the GetRequest operation. Whereas the GetRequest operation is used to read the specified MIB, the GetNextRequest operation is used to retrieve the MIB after the specified MIB. One or more MIBs can be specified for this operation.

The following figure shows the GetNextRequest operation.

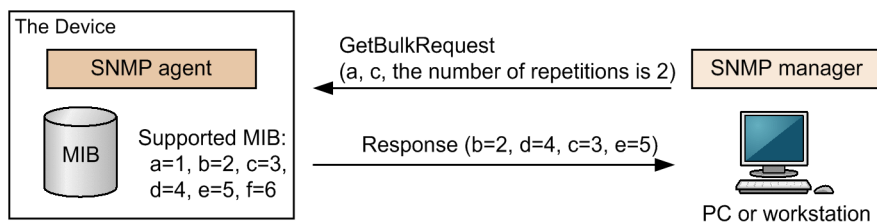
Figure 15-18: GetNextRequest operation

**(3) GetBulkRequest operation**

The GetBulkRequest operation is an extended GetNextRequest operation. By using this operation, you can set a number of repetitions. From the items after the specified MIB, you can extract as many MIBs as the specified number of repetitions. One or more MIBs can be specified for this operation.

The following figure shows the GetBulkRequest operation.

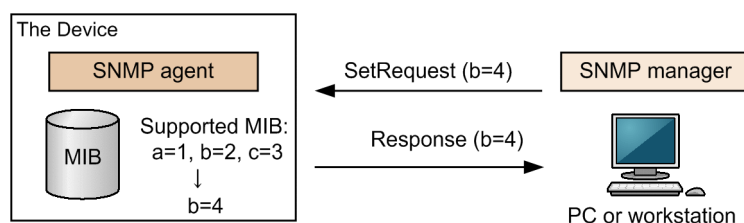
Figure 15-19: GetBulkRequest operation

**(4) SetRequest operation**

The SetRequest operation is similar to the GetRequest, GetNextRequest, and GetBulkRequest operations because it is performed for a device (agent functionality) from the SNMP manager, but the method for setting a value for the SetRequest operation is different from that of the other operations.

The SetRequest operation specifies both a value to be set and a MIB. When a value is set, the Response operation returns the MIB and the setting value.

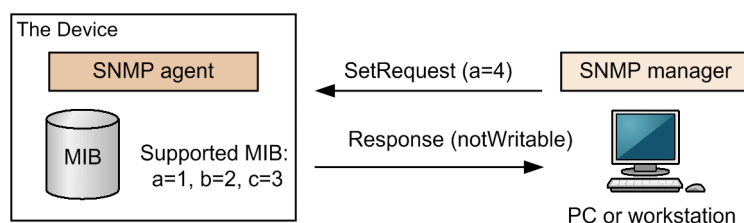
The following figure shows the SetRequest operation.

Figure 15-20: SetRequest operation**(a) Response when a MIB cannot be configured**

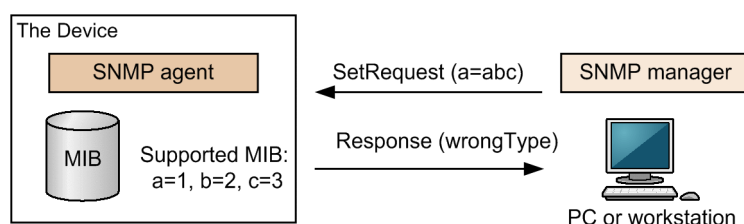
The following are three cases when a MIB cannot be configured:

- The MIB is read-only.
- The setting value is not correct.
- Configuration cannot be performed because of the status of the device.

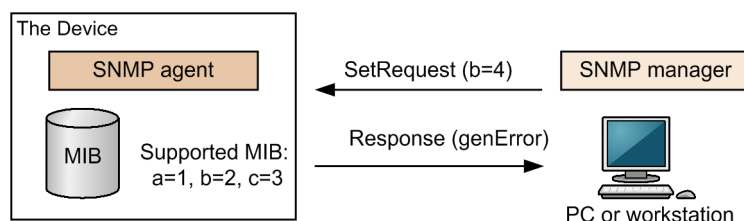
Each case returns a different response. If the MIB is read-only, the Response operation returns `notWritable`. The following figure shows the SetRequest operation when the MIB is read-only.

Figure 15-21: SetRequest operation when the MIB variable is read-only

If the type of the setting value is not correct, the Response operation returns `wrongType`. The following figure shows the SetRequest operation when the type of the setting value is not correct.

Figure 15-22: Example of the SetRequest operation when the type of the setting value is not correct

If configuration is not possible because of the status of the device, `genError` is returned. For example, when an attempt is made to set a value on a device, if a setting timeout is detected on the device, `genError` is returned. The following figure shows the SetRequest operation when configuration is not possible because of the status of the device.

Figure 15-23: SetRequest operation when configuration is not possible because of the status of the device

(5) Operational restrictions applying to SNMPv3

In SNMPv1 and SNMPv2C, verification is performed by combining a community and the IP addresses for an SNMP manager. In SNMPv3, however, MIB operations that can be performed are controlled by user authentication and the MIB view. To use SNMPv3 on the Device, you must use a configuration command to register SNMP security users, MIB views, and security groups. In addition, to send a trap, you must use a configuration command to register SNMP security users, MIB views, security groups, and trap-sending SNMP managers.

(6) Error status codes for SNMPv3 operations

If an error occurs as the result of an operation, an SNMP agent assigns an error code for the error status and returns a response in the Response operation. The response contains the number of the MIB information where the error occurred set as the error location number. If the result of the operation is normal, a code indicating no errors is set in the error status, and a response in the Response operation that contains the MIB information of the operations actually performed is returned. The following table describes the error status codes.

Table 15-2: Error status codes

Error status	Code	Description
noError	0	No error occurred.
tooBig	1	The data size is too large to be set as a value in the PDU.
noSuchName	2	The specified MIB was not found or writing is not allowed.
badValue	3	The setting value is incorrect.
readOnly	4	A write attempt failed (the Device does not return this status).
genError	5	Another error occurred.
noAccess	6	A set operation was attempted for a MIB that cannot be accessed.
wrongType	7	A type different from the type required for the MIB was specified.
wrongLength	8	A length different from the length required for a MIB was specified.
wrongEncoding	9	The ASN.1 encoding was incorrect.
wrongValue	10	The MIB value was incorrect.
noCreation	11	The applicable MIB does not exist.
inconsistentValue	12	A value cannot be set due to an inconsistency.
resourceUnavailable	13	A resource required for setting a value cannot be used.
commitFailed	14	An attempt to update a value failed.
undoFailed	15	The original value could not be restored when an attempt to update a value failed.
authorizationError	16	Authentication failed.
notWritable	17	The set operation cannot be performed.
inconsistentName	18	Creation is not currently possible because the MIB does not exist.

15.1.5 Traps

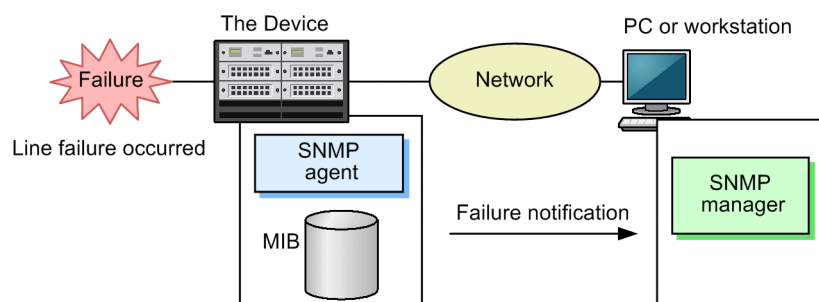
(1) Overview of traps

SNMP agents have functionality called a trap for reporting events (mainly information about failures or log information). Traps are used to report important events asynchronously to an SNMP

manager from an SNMP agent. The SNMP manager can detect changes to the device status by receiving traps. Based on such notification, the SNMP manager can extract the MIBs on devices to obtain more detailed information.

Note, however, that the SNMP manager cannot verify whether a trap has arrived from a device because traps use UDP. Accordingly, some traps might not arrive at the SNMP manager due to network congestion. The following figure shows an example of a trap.

Figure 15-24: Example of a trap



(2) Trap format (SNMPv1)

A trap frame contains the IP address of a device, and information about what has occurred in the device and when it occurred. The following figure shows the trap format (SNMPv1).

Figure 15-25: Trap format (SNMPv1)

SNMP version		Community name		Trap PDU			
TRAP	Device ID	Agent address	Trap number	Extended trap number	Time	Related MIB information	

Names in the above figure	Description
Device ID	ID for identifying the device (normally, the value for sysObjectID of MIB-II is set)
Agent address	IP address of the device on which the trap occurred
Trap number	Identification number indicating the type of the tarp
Extended trap number	Number supplementing the trap number
Time	Time that the trap occurred (expressed as the time since the device was started)
Related MIB information	MIB information related to the trap

(3) Trap format (SNMPv2C and SNMPv3)

A trap frame contains information about what has occurred in the device and when it occurred. The following figure shows the trap format (SNMPv2C and SNMPv3).

Figure 15-26: Trap format (SNMPv2C and SNMPv3)

SNMP version		Community name		Trap PDU		
TRAP	Request ID	Error status	Error index	Related MIB information		

Names in the above figure	Description
Request ID	Message ID that is different for each request
Error status	Value indicating the error that occurred
Error index	Error location for the related MIB information
Related MIB information	MIB information related to the trap

15.1.6 Informs

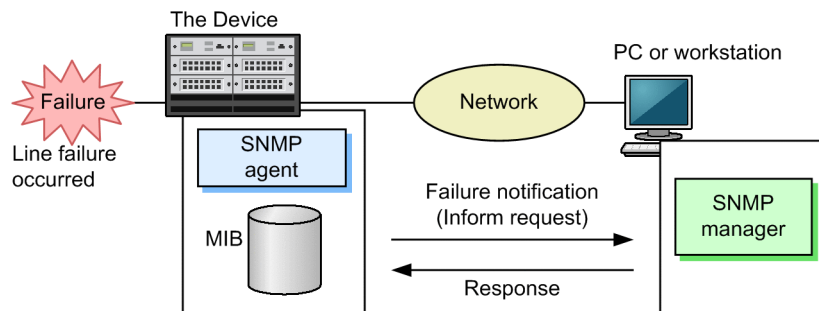
(1) Overview of informs

SNMP agents have the functionality called an inform for event notification (mainly information about failures or log information). Informs are used to report important events to an SNMP manager from an SNMP agent by issuing inform requests. The SNMP manager can detect changes to the device status by receiving inform requests. Based on such notification, the SNMP manager can extract the MIBs on devices to obtain more detailed information.

Informs are supported only for SNMPv2C. In addition, informs must be supported by the SNMP manager.

An inform is the event notification functionality using UDP like a trap, but it requests a response from the SNMP manager. Therefore, you can verify whether an inform request has arrived by checking for a response. This allows you to deal with a problem such as network congestion by resending an inform. The following figure shows an example of an inform.

Figure 15-27: Example of an inform



(2) Inform request format

An inform request frame contains information about what has occurred in the device and when it occurred. The following figure shows the inform request format.

Figure 15-28: Inform request format

SNMP version		Community name		InformRequest PDU	
INFORM	Request ID	Error status	Error index	Related MIB information	

Names in the above figure	Description
Request ID	Message ID that is different for each request
Error status	Value indicating the error that occurred
Error index	Error location for the related MIB information

Names in the above figure	Description
Related MIB information	MIB information related to this inform request

15.1.7 IP addresses used for SNMP

The IP addresses to be put in the IP header when the Device sends SNMP packets differ depending on the operation. The following table describes the IP addresses used for SNMP.

Table 15-3: IP addresses used for SNMP

Operation	Source IP address	Destination IP address
<ul style="list-style-type: none"> • GetResponse • Response 	The destination IP address when an operation that triggers GetResponse and Response (GetRequest, GetNextRequest, GetBulkRequest, or SetRequest) is received	The source IP address when an operation that triggers GetResponse and Response (GetRequest, GetNextRequest, GetBulkRequest, or SetRequest) is received
<ul style="list-style-type: none"> • Traps • Informs 	When an IP address is set for the loopback interface The loopback interface IP address When an IP address is not set for the loopback interface IP address of the sending interface	IP address of the destination SNMP manager

15.1.8 RMON MIB

RMON (Remote Network Monitoring) functionality includes the provision of Ethernet statistics, generation of an event from the checking of threshold values in the collected statistics, and the capture of packets. RMON is defined in RFC 2819.

This section provides an overview for the statistics, history, alarm, and event groups of the RMON MIBs.

(1) Statistics group

The statistics group collects basic statistics about monitored subnetworks. Examples include the total number of packets in a subnetwork, the number of packets for each packet type such as broadcast packets, and the number of errors, which includes CRC errors and collision errors. The statistics group provides statistics about subnetwork traffic conditions and line status.

(2) History group

The history group samples statistics that are almost the same as the information collected by the statistics group, and retains the sampled information as history information.

A history group has a control table named historyControlTable and a data table named etherHistoryTable. historyControlTable is a MIB used to set the sampling interval and the number of history records, among other items.

etherHistoryTable is a MIB of history information about the sampled statistics. The history group retains statistics on the device for a certain period of time. Compared to regular polling by an SNMP manager to collect statistics, network load is lower and continuous statistics for a certain period can be obtained.

(3) Alarm group

The alarm group is a MIB that configures the interval for checking monitored MIBs and the threshold values for logging when the MIB reaches the threshold value, for issuing a trap or an inform to an SNMP manager. When you use the alarm group, you must configure the event group.

Two types of methods, namely the delta method (compares the delta (fluctuating range) of a MIB value with a threshold value) and the absolute method (directly compares a MIB with a threshold

value), can be used for MIB monitoring by the alarm group.

The threshold value check by the delta method can, for example, collect logs and issue a trap or an inform to the SNMP manager when the CPU usage change is 50 percent or more. The threshold value check by the absolute method can, for example, collect logs and issue a trap or an inform to the SNMP manager when the CPU usage reaches 80 percent.

(4) Event group

The event group consists of the eventTable group MIB, which specifies the behavior when a MIB threshold value set in the alarm group is exceeded, and the logTable group MIB, which logs information when a threshold value is exceeded.

The eventTable group MIB is used to set, when a threshold value is reached, whether information is to be logged or a trap or an inform is to be issued to an SNMP manager, or whether both actions or neither action is required.

The logTable group MIB logs information on the device when logging is specified by the eventTable group MIB. Because the number of log entries on a device is fixed, if the limit is exceeded, new information replaces old information in the log. Note that if you do not save log information regularly to the SNMP manager, some logged information might be lost.

15.1.9 Notes on connecting to an SNMP manager

(1) Tuning the cycle for collecting MIB information

To detect a new device on a network or to monitor traffic conditions, an SNMP manager extracts MIBs regularly from devices supported by the SNMP agent. If the interval for extracting MIBs is too short, the load on the network devices or network itself increases. In addition, depending on the device status or the configuration, a timeout might occur on the SNMP manager when it extracts a MIB. In particular, the possibility of a response timeout is high in the following cases:

- When too many SNMP managers are connected

When many SNMP managers are connected to a Device and the operations for collecting MIB information result in congestion

- When many SNMP events occur simultaneously

In this case, because a large number of traps or informs are issued from a Device, a response might time out if MIBs are extracted or MIBs are extracted in parallel according to the trap or inform issued from a Device.

If response timeouts occur frequently, adjust the polling cycle or the value of the response monitoring timer for the SNMP manager. The three major SMNP manager tuning parameters are as follows:

- Polling interval
- Response monitoring timer
- Number of retries when a response monitoring timeout occurs

15.2 Configuration

15.2.1 List of configuration commands

The following table describes the configuration commands for SNMP and RMON.

Table 15-4: List of configuration commands

Command name	Description
rmon alarm	Sets the control information of an RMON alarm group.
rmon collection history	Sets the control information for the RMON Ethernet statistics history.
rmon event	Sets the control information for an RMON event group.
snmp-server community	Sets the access list for the SNMP community.
snmp-server contact	Sets the contact information of the Device. This setting is equivalent to sysContact defined in RFC 3418.
snmp-server engineID local	Sets SNMP engine ID information.
snmp-server group	Sets SNMP security group information.
snmp-server host	Registers the network management device (SNMP manager) to which traps or informs are sent.
snmp-server informs	Sets the conditions for resending informs.
snmp-server location	Sets the name of the location where the Device is installed. This setting is equivalent to sysLocation defined in RFC 3418.
snmp-server traps	Sets the timing for issuing a trap or an inform.
snmp-server user	Sets SNMP security user information.
snmp-server view	Sets MIB view information.
snmp trap link-status	When a link-up failure or link-down failure occurs on a line, suppresses the sending of traps or informs (SNMP link-down and link-up traps).

15.2.2 Configuring MIB access permissions in SNMPv1 and SNMPv2C

Points to note

Configure access to the MIB of the Device from the SNMP manager.

Command examples

1. **(config)# ip access-list standard LIST1**

(config-std-nacl)# permit 10.1.1.1 0.0.0.0

Configures the access list that allows access from IP address 10.1.1.1.

2. **(config)# snmp-server community "NETWORK" ro LIST1**

Configures the MIB access mode for the community of an SNMP manager and the applicable access list.

- Community name: NETWORK
- Access list: LIST1
- Access mode: read only

15.2.3 Configuring MIB accesses in SNMPv3

Points to note

To access a MIB in SNMPv3, configure a collection of MIB objects as a MIB view and set user authentication and privacy information as an SNMP security user. Also, to associate the MIB view with the SNMP security user, configure the SNMP security group.

Command examples

1. `(config)# snmp-server view "READ_VIEW" 1.3.6.1 included`
`(config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded`
`(config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included`

Configures a MIB view.

- Registers the Internet group MIB (subtree: 1.3.6.1) in the READ_VIEW view.
- Excludes the snmpModules group MIB (subtree: 1.3.6.1.6.3) as belonging to the READ_VIEW view.
- Registers the system group MIB (subtree: 1.3.6.1.2.1.1) in the WRITE_VIEW view.

2. `(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"`

Configures an SNMP security user.

- SNMP security user name: ADMIN
- SNMP security group name: ADMIN_GROUP
- Authentication protocol: HMAC-MD5
- Authentication password: ABC*_1234
- Encryption protocol: CBC-DES
- Encryption password: XYZ/+6789

3. `(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"`

Configures an SNMP security group.

- SNMP security group name: ADMIN_GROUP
- Security level: Authentication required, encryption required
- Read view name: READ_VIEW
- Write view name: WRITE_VIEW

15.2.4 Configuring the sending of traps in SNMPv1 and SNMPv2C

Points to note

Register the SNMP manager that issues a trap.

Command examples

1. `(config)# snmp-server host 10.1.1.1 traps "NETWORK" version 1 snmp`

Configures an SNMP manager to issue standard traps.

- Community name: NETWORK
- IP address of the SNMP manager: 10.1.1.1
- Traps to be issued: coldStart, warmStart, linkDown, linkUp, and authenticationFailure

15.2.5 Configuring the sending of traps in SNMPv3

Points to note

After configuring a MIB view and an SNMP security user, configure an SNMP security group, and then configure the SNMP trap mode.

Command examples

1. **(config)# snmp-server view "ALL_TRAP_VIEW" * included**

Configures a MIB view.

- Registers all subtrees in the ALL_TRAP_VIEW view.

2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**

Configures an SNMP security user.

- SNMP security user name: ADMIN
- SNMP security group name: ADMIN_GROUP
- Authentication protocol: HMAC-MD5
- Authentication password: ABC*_1234
- Encryption protocol: DES
- Encryption password: XYZ/+6789

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"**

Configures an SNMP security group.

- SNMP security group name: ADMIN_GROUP
- Security level: Authentication required, encryption required
- Notify view name: ALL_TRAP_VIEW

4. **(config)# snmp-server host 10.1.1.1 traps "ADMIN" version 3 priv snmp**

Configures an SNMP manager so that it can issue standard traps in SNMPv3.

- IP address of the SNMP manager: 10.1.1.1
- SNMP security user name: ADMIN
- Security level: Authentication required, encryption required
- Traps to be issued: coldStart, warmStart, linkDown, linkUp, and authenticationFailure

15.2.6 Configuring the sending of informs in SNMPv2C

Points to note

Register the SNMP manager that issues an inform.

Command examples

1. `(config)# snmp-server host 10.1.1.1 informs "NETWORK" version 2c snmp`

Configures an SNMP manager to issue standard informs.

- Community name: NETWORK
- IP address of the SNMP manager: 10.1.1.1
- Informs to be issued: coldStart, warmStart, linkDown, linkUp, and authenticationFailure

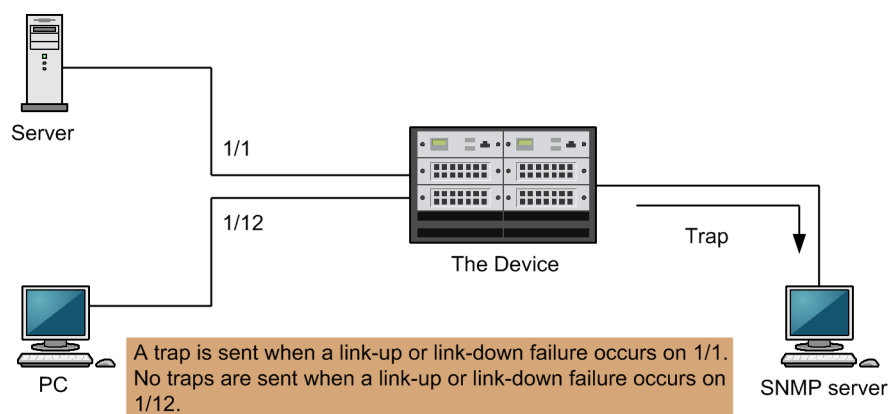
15.2.7 Suppressing link traps

The Device issues an SNMP trap or an inform by default when a link-up or a link-down failure occurs on an Ethernet interface. You can suppress the sending of link traps for each Ethernet interface by specifying suppression in the configuration file. For example, by sending traps or informs only to important lines such as a line connecting to a server, and suppressing the sending of link traps on another line, you can eliminate unnecessary processing by Devices, networks, and SNMP managers.

Points to note

Determine the link trap configuration based on the operation policies of the entire network.

Figure 15-29: Link trap configuration



In the above figure, because a trap or an inform is sent from port 1/1, you do not need to edit the configuration file. Configure port 1/12 so that it does not send traps or informs.

Command examples

1. `(config)# interface gigabitethernet 1/12`
`(config-if)# no snmp trap link-status`

Configures the port so that traps or informs are not sent when a link-up or link-down failure occurs.

2. `(config-if)# exit`

15.2.8 Configuring control information for the RMON Ethernet history group

Points to note

Configure the control information for the RMON Ethernet statistics history. The command can configure up to 32 entries. You must register an SNMP manager beforehand.

Command examples

1. **(config)# interface gigabitethernet 1/5**

Switches to the interface mode for gigabit Ethernet interface 1/5.

2. **(config-if)# rmon collection history controlEntry 33 owner "NET-MANAGER" buckets 10**

Sets the information identification number of the control information for statistics history information, the identification information of the person responsible for configuration, and the number of history entries for storing statistics.

- Information identification number: 33
- Number of entries obtained for history information: 10
- Identification information about the person responsible for configuration: NET-MANAGER

15.2.9 Threshold check for specific MIB values by RMON

Points to note

Configure a device to be used to regularly check the threshold value for a specific MIB value, and to notify the SNMP manager of an event if the threshold value is exceeded.

If you specify `trap` as an event execution method, you must configure the SNMP trap mode beforehand.

Command examples

1. **(config)# rmon event 3 log trap public**

Configures an event to be executed when an alarm is generated.

- Information identification number: 3
- Event execution method: log or trap
- Trap-sending community name: public

2. **(config)# rmon alarm 12 "ifOutDiscards.1" 256111 delta rising-threshold 400000 rising-event-index 3 falling-threshold 100 falling-event-index 3 owner "NET-MANAGER"**

Configures control information for the RMON alarm group for the following conditions:

- Control information identification number for the RMON alarm group: 12
- Object identifier for the MIB used for checking the threshold: `ifOutDiscards.1`
- Time interval for checking the threshold: 256111 seconds
- Method for checking the threshold: difference value check (delta)
- Upper threshold value: 400000
- Identification number of the method for generating an event if the upper threshold is exceeded: 3
- Lower threshold value: 100
- Identification number of the method for generating an event if the lower threshold is exceeded: 3
- Identification information for the person responsible for configuration: NET-MANAGER

15.2.10 Configuring permissions for accessing MIBs from VRF in SNMPv1 and SNMPv2C

Points to note

Configure access to the Device MIBs from the SNMP manager in VRF.

Command examples

1. **(config)# ip access-list standard LIST2**

```
(config-std-nacl)# permit 10.1.1.1 0.0.0.0
```

Configures the access list that allows access from IP address 10.1.1.1.

2. **(config)# snmp-server community "NETWORK" ro LIST2 vrf 2**

Configures the MIB access mode for the community of an SNMP manager and the applicable access list.

- Community name: NETWORK
- Access list: LIST2
- Access mode: read only
- VRF ID: 2

15.2.11 Configuring permissions for accessing MIBs from VRF in SNMPv3

Points to note

To access a MIB in SNMPv3, configure a collection of MIB objects as a MIB view and set user authentication, privacy information, and a VRF ID that grants access as an SNMP security user. Also, to associate the MIB view with the SNMP security user, configure the SNMP security group.

Command examples

1. **(config)# snmp-server view "READ_VIEW" 1.3.6.1 included**

```
(config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded
```

```
(config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included
```

Configures a MIB view.

- Registers the Internet group MIB (subtree: 1.3.6.1) in the READ_VIEW view.
- Excludes the snmpModules group MIB (subtree: 1.3.6.1.6.3) as belonging to the READ_VIEW view.
- Registers the system group MIB (subtree: 1.3.6.1.2.1.1) in the WRITE_VIEW view.

2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789" vrf 2**

Configures an SNMP security user.

- SNMP security user name: ADMIN
- SNMP security group name: ADMIN_GROUP
- Authentication protocol: HMAC-MD5
- Authentication password: ABC*_1234
- Encryption protocol: CBC-DES

- Encryption password: XYZ/+6789
- VRF ID: 2

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"**

Configures an SNMP security group.

- SNMP security group name: ADMIN_GROUP
- Security level: Authentication required, encryption required
- Read view name: READ_VIEW
- Write view name: WRITE_VIEW

15.2.12 Configuring settings for sending traps to a VRF in SNMPv1 and SNMPv2C

Points to note

Configures an SNMP manager on a VRF so that traps can be issued.

Command examples

1. **(config)# snmp-server host 10.1.1.1 vrf 2 traps "NETWORK" version 1 snmp**

Configures an SNMP manager to issue standard traps.

- Community name: NETWORK
- IP address of the SNMP manager: 10.1.1.1
- Traps to be issued: coldStart, warmStart, linkDown, linkUp, and authenticationFailure
- VRF ID: 2

15.2.13 Configuring settings for sending traps to a VRF in SNMPv3

Points to note

After configuring a MIB view and an SNMP security user, configure an SNMP security group, and then configure the SNMP trap mode. The VRF ID registered as an SNMP security user must be the same as the VRF ID set in SNMP trap mode.

Command examples

1. **(config)# snmp-server view "ALL_TRAP_VIEW" * included**

Configures a MIB view.

- Registers all subtrees in the ALL_TRAP_VIEW view.

2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789" vrf 2**

Configures an SNMP security user.

- SNMP security user name: ADMIN
- SNMP security group name: ADMIN_GROUP
- Authentication protocol: HMAC-MD5
- Authentication password: ABC*_1234

- Encryption protocol: DES
- Encryption password: XYZ/+6789
- VRF ID: 2

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"**

Configures an SNMP security group.

- SNMP security group name: ADMIN_GROUP
- Security level: Authentication required, encryption required
- Notify view name: ALL_TRAP_VIEW

4. **(config)# snmp-server host 10.1.1.1 vrf 2 traps "ADMIN" version 3 priv snmp**

Configures an SNMP manager so that it can issue standard traps in SNMPv3.

- IP address of the SNMP manager: 10.1.1.1
- SNMP security user name: ADMIN
- Security level: Authentication required, encryption required
- Traps to be issued: coldStart, warmStart, linkDown, linkUp, and authenticationFailure
- VRF ID: 2

15.2.14 Configuring settings for sending informs to a VRF in SNMPv2C

Points to note

Configures an SNMP manager on a VRF so that informs can be issued.

Command examples

1. **(config)# snmp-server host 10.1.1.1 vrf 2 informs "NETWORK" version 2c snmp**

Configures an SNMP manager to issue standard informs.

- Community name: NETWORK
- IP address of the SNMP manager: 10.1.1.1
- Informs to be issued: coldStart, warmStart, linkDown, linkUp, and authenticationFailure
- VRF ID: 2

15.3 Operation

15.3.1 List of operation commands

The following table describes the operation commands for SNMP and RMON.

Table 15-5: List of operation commands

Command name	Description
show snmp	Shows SNMP information.
show snmp pending	Shows pending inform requests to be sent.
snmp lookup	Shows supported MIB object names and object IDs.
snmp get	Shows the specified MIB value.
snmp getnext	Shows the MIB value following the specified one.
snmp walk	Shows the specified MIB tree.
snmp getif	Shows MIB information for the interface group.
snmp getroute	Shows the IP routing table (ipRouteTable).
snmp getarp	Shows the IP address translation table (ipNetToMediaTable).
snmp getforward	Shows the IP forwarding table (ipForwardTable).
snmp rget	Shows the MIB value for the specified remote device.
snmp rgetnext	Shows the MIB value following the specified remote device.
snmp rwalk	Shows information about the MIB tree for the specified remote device.
snmp rgetroute	Shows the IP routing table (ipRouteTable) of the specified remote device.
snmp rgetarp	Shows the IP address translation table (ipNetToMediaTable) of the specified remote device.

15.3.2 Checking communication with SNMP managers

When you manage networks using SNMP by configuring the SNMP agent functionality on the Device, check the following:

- MIBs on the Device can be retrieved from an SNMP manager on a network.
- An SNMP trap or an inform is sent from the Device to an SNMP manager on a network, and, for an inform, a response can be received.

You can use the `show snmp` command to check the status of communication with an SNMP manager.

Figure 15-30: Result of executing the show snmp command

```
> show snmp
Date 20XX/03/18 13:34:17 UTC
Contact: snmp@example.com
Location: Japan
SNMP packets input  : 149346      (get:186696 set:0)
  Get-request PDUs   : 1992
  Get-next PDUs      : 147354
  Get-bulk PDUs      : 0
  Set-request PDUs   : 0
  Response PDUs      : 0          (with error 0)
  Error PDUs         : 0
```

```

        Bad SNMP version errors: 0
        Unknown community name : 0
        Illegal operation       : 0
        Encoding errors         : 0

SNMP packets output : 149475
  Trap PDUs          : 125
  Inform-request PDUs : 4
  Response PDUs      : 149346 (with error 499)
    No errors         : 148847
    Too big errors    : 0
    No such name errors : 499
    Bad values errors : 0
    General errors    : 0
  Timeouts           : 1
  Drops              : 0

[TRAP]
  Host: 192.168.0.65, sent:3
  Host: 192.168.0.210, sent:61

[INFORM]
  Timeout(sec)       : 30
  Retry              : 3
  Pending informs    : 2/25 (current/max)
  Host: 192.168.0.1
    sent             :2      retries:1
    response:0        pending:2      failed:0      dropped:0
  Host: 2001:db8::10
    sent             :1      retries:0
    response:0        pending:1      failed:0      dropped:0

```

If MIBs cannot be obtained from the SNMP manager, make sure that the value for `Error PDUs` under `SNMP packets input` has not increased and PDUs have been successfully received. If the value for `Error PDUs` has increased, check the configuration settings. If PDUs have failed to be received, make sure that the network settings are correct and no error occurred on the route to the SNMP manager.

If traps or informs cannot be received by the SNMP manager, make sure that the IP address of the SNMP manager is set for `Host` under `[TRAP]` and `[INFORM]`. If the IP address of the SNMP manager has not been set, execute the `snmp-server host` configuration command to set information about the SNMP manager.

If the problem cannot be corrected after these actions, see the *Troubleshooting Guide*. For details about the MIBs that can be obtained from the Device and for details about traps and informs, see *MIB Reference For Version 12.1*.

Chapter

16. Ethernet

This chapter describes Ethernet as used with the Device.

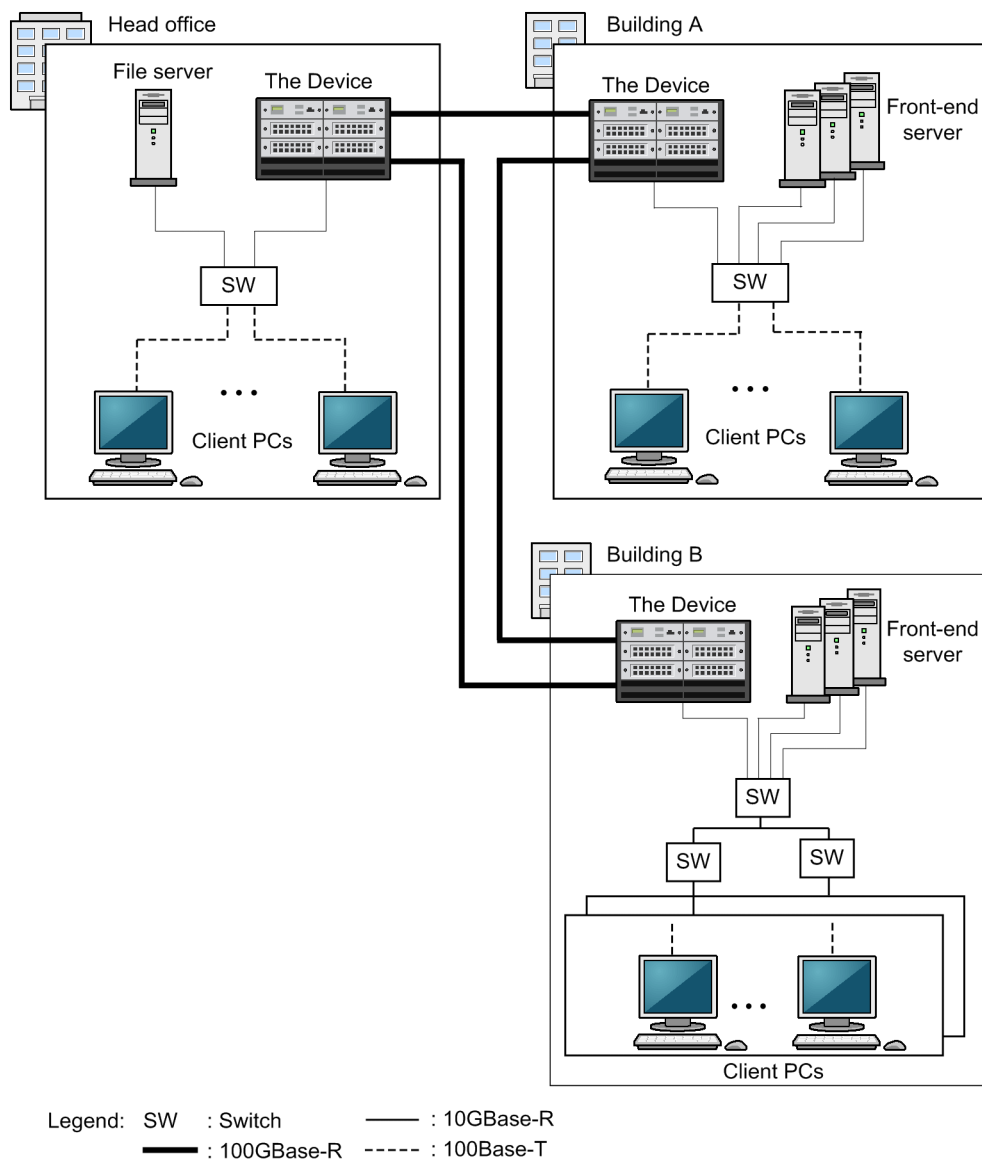
- 16.1 Description of information common to all Ethernet interfaces
- 16.2 Configuration common to all Ethernet interfaces
- 16.3 Operations common to all Ethernet interfaces
- 16.4 Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces
- 16.5 Configuration of 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces
- 16.6 Description of the 1000BASE-X interface
- 16.7 Configuration of the 1000BASE-X interface
- 16.8 Description of the 10GBASE-R interface
- 16.9 Configuration of the 10GBASE-R interface
- 16.10 Description of 100GBASE-R
- 16.11 Configuration of the 100GBASE-R interface

16.1 Description of information common to all Ethernet interfaces

16.1.1 Network configuration example

The figure below shows an example of a typical Ethernet configuration that uses the Device. In this example, the use of 10GBASE-R for connections between buildings and between servers improves communication performance between servers, as compared to the use of 10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, or 10GBASE-R.

Figure 16-1: Ethernet configuration example



16.1.2 Physical interfaces

There are four types of Ethernet interfaces:

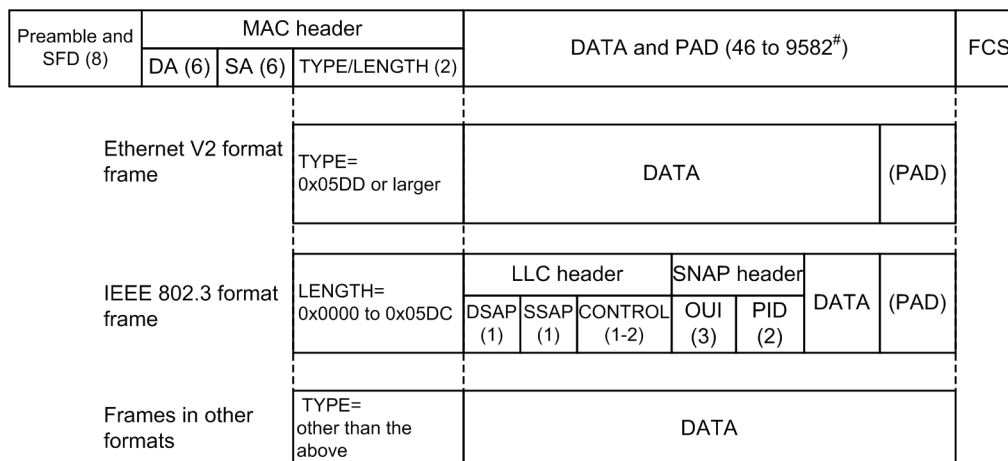
- Interface using a 10BASE-T, 100BASE-TX, or 1000BASE-T twisted pair cable (UTP)
- Interface using a 1000BASE-X optical fiber cable
- Interface using a 10GBASE-R optical fiber cable

- Interface using a 100GBASE-R optical fiber cable

16.1.3 MAC sublayer control

The following figure shows frame formats. The Device supports frames in Ethernet V2 format.

Figure 16-2: Frame formats



(n): Field length (units: octets)

#

The maximum length of the DATA and PAD field of a frame in Ethernet V2 format is 9582.

(1) MAC sublayer frame format

(a) Preamble and SFD field

The Preamble and SFD field contains a 64-bit binary number. The first 62 bits are repetitions of 10, and the last two bits are 11 (1010...1011). This field is added to the beginning of the frame when the frame is sent. Frames without this 64-bit pattern cannot be received.

(b) DA and SA fields

The DA and SA fields support a 48-bit format. They do not support 16-bit or local address formats.

(c) TYPE/LENGTH

The following table describes the meanings of the TYPE/LENGTH field.

Table 16-1: Meanings of the TYPE/LENGTH field

TYPE/LENGTH value	Meaning of the field
0x0000 to 0x05DC	IEEE 802.3 CSMA/CD frame length
0x05DD or larger	Ethernet V2.0 frame type

(d) FCS

The FCS field uses a 32-bit CRC.

(2) Conditions for discarding received frames

Frames satisfying any of the following conditions are discarded:

- The frame length is not a multiple of an octet.
- The length of the received frame (from DA to FCS) is either less than 64 octets, or 1522 octets or more.

If the use of jumbo frames is selected, the length of the received frame exceeds the specified

size.

- An FCS error has occurred.
- A collision occurred during reception of the frame on a half-duplex connection interface.

(3) Handling of padding

If the length of a sent frame is less than 64 octets, padding is added immediately before the FCS field. The values to be padded are undefined.

16.1.4 VLAN Tag

(1) Overview

VLAN tagging based on the IEEE 802.1Q standard, in which IDs called tags are inserted into Ethernet frames, can be used to identify the VLAN ID and QoS priorities.

In VLAN tagging, VLAN IDs of VLAN tags are assigned to Ethernet interfaces or port channel interfaces, so that these interfaces can be used as different interfaces on a VLAN ID basis.

(2) Protocol specification

VLAN tags can embed an ID called a tag into an Ethernet frame. These tags are used to report VLAN information (a VLAN ID) to separate segments.

The figure below shows the tagged-frame format. There are two formats for Ethernet frames into which VLAN tag are inserted: Ethernet V2 and 802.3. The Device supports frames in Ethernet V2 format.

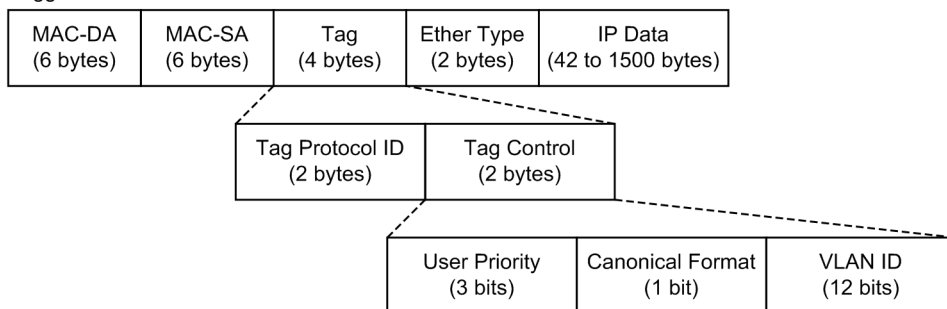
Figure 16-3: Tagged-frame format

• Ethernet V2 frame

Normal frame

MAC-DA (6 bytes)	MAC-SA (6 bytes)	Ether Type (2 bytes)	IP data (46 to 1500 bytes)
---------------------	---------------------	-------------------------	-------------------------------

Tagged frame



• IEEE 802.3LLC/SNAP frame

Normal frame

MAC-DA (6 bytes)	MAC-SA (6 bytes)	Length (2 bytes)	LLC (3 bytes)	SNAP (5 bytes)	IP Data (38 to 1492 bytes)
---------------------	---------------------	---------------------	------------------	-------------------	-------------------------------

Tagged frame

MAC-DA (6 bytes)	MAC-SA (6 bytes)	Tag (4 bytes)	Length (2 bytes)	LLC (3 bytes)	SNAP (5 bytes)	IP Data (34 to 1492 bytes)
---------------------	---------------------	------------------	---------------------	------------------	-------------------	-------------------------------

The following table describes the fields for VLAN tags.

Table 16-2: VLAN tag fields

Field	Description	How the Device handles the value
TPID (Tag Protocol ID)	Indicates an Ether Type value indicating that the IEEE 802.1Q VLAN tag continues.	Any value can be set for each device.
User Priority	Indicates the IEEE 802.1D priority.	Eight priority levels can be selected for configuration. When VLAN ID = 0 is received, User Priority is identified.
CF (Canonical Format)	Indicates whether the MAC address in the MAC header follows a standard format.	The Device supports only standard (0) formats.
VLAN ID	Indicates the VLAN ID.	VLAN IDs from 1 to 4095 can be used. When VLAN ID = 0 is received, it is handled the same way as an untagged frame. VLAN ID = 0 cannot be sent.

16.1.5 MAC address of the Device

(1) Device MAC addresses

The Device has one MAC address as a device identifier. This MAC address is called the device MAC address. A device MAC address is used as the MAC address of an IP interface or as a device identifier for functionality in Layer 2.

(2) Functionality that uses a device MAC address

The following table describes the types of functionality that use the device MAC address.

Table 16-3: Functionality that uses a device MAC address

Functionality	Purpose
IP interface	MAC address of any of the following IP interfaces: <ul style="list-style-type: none"> Ethernet interface Ethernet subinterface Port channel interface Port channel subinterface
LACP for link aggregation	Device identifier
CFM	Device identifier
LLDP	Device identifier

16.2 Configuration common to all Ethernet interfaces

16.2.1 List of configuration commands

The following table describes the configuration commands common to all Ethernet interfaces.

Table 16-4: List of configuration commands

Command name	Description
bandwidth	Sets the bandwidth.
description	Sets supplementary information.
duplex	Sets full duplex or half duplex.
flowcontrol	Sets flow control.
frame-error-notice	Sets the condition for sending a notification when a frame reception error or a frame sending error occurs.
interface gigabitethernet	Specifies a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X configuration.
interface hundredgigabitethernet	Specifies a 100GBASE-R configuration.
interface tengigabitethernet	Specifies a 10GBASE-R configuration.
link debounce	Sets the time required before a link-down is detected.
link up-debounce	Sets the time required before a link-up is detected.
mdix auto	Sets AUTO-MDI/MDI-X.
mtu	Sets the maximum Ethernet frame length.
shutdown	Shuts down Ethernet.
speed	Sets the speed.
system mtu	Sets a value as the device of the maximum Ethernet frame length.

16.2.2 Configuring multiple interfaces by a single command

Points to note

When Ethernet is configured, the same information sometimes needs to be set for multiple interfaces. In such cases, the same information can be set for the interfaces at the same time by using a range specification.

Command examples

1. **(config)# interface range gigabitethernet 1/1-4, gigabitethernet 1/7-12, tengigabitethernet 3/1**

Specifies gigabit Ethernet interfaces from 1/1 to 1/4 and from 1/7 to 1/12, and 10 gigabit Ethernet interface 3/1.

2. **(config-if-range)# *******

Performs the same configuration for all the interfaces.

16.2.3 Shutting down an Ethernet interface

Points to note

Configuring an Ethernet interface might require the execution of multiple commands. If an Ethernet interface is placed in the link-up status before all required commands are executed, communication will not be as expected. For this reason, we recommend that you first shut down the Ethernet interface, and then release the interface from the shutdown status after configuration has been completed. Always make sure that Ethernet interfaces that will not be used are shut down. Note that this setting turns the power of the ports off.

Command examples

1. **(config)# interface gigabitethernet 1/10**

Specifies that Ethernet interface 1/10 is to be configured.

2. **(config-if)# shutdown**

Shuts down the Ethernet interface.

3. **(config-if)# *******

Configures the Ethernet interfaces.

4. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

Related information

You can also use the `inactivate` operation command to stop the operation of an Ethernet interface. Note that if a device is deactivated by using this command is restarted, the status of the Ethernet interface reverts to active. However, if a device that has been shut down is restarted, its status remains disabled. To change the status from disabled to active, you must release the Ethernet interface from the shutdown status by using `no shutdown` to configure the interface.

16.2.4 Configuring jumbo frames

The maximum frame length for an Ethernet interface (from DA in the MAC header to DATA) is 1518 octets according to the standard. On the Device, the MTU can be extended by using jumbo frames to increase the amount of data that is transmitted at one time, which improves throughput.

For a port to send or receive jumbo frames, set the maximum frame length. For the maximum frame length for the port, determine the set value appropriate for the network and remote device.

(1) *Setting the maximum frame length for a specific port*

Points to note

The example below shows how to set 8192 octets as the maximum frame length for port 1/10. This setting enables the port to send and receive jumbo frames up to 8192 octets.

Command examples

1. **(config)# interface gigabitethernet 1/10**

(config-if)# shutdown

(config-if)# mtu 8192

Shuts down the Ethernet interface and sets 8192 octets as the maximum frame length for the port.

2. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

Notes

- Even if the maximum frame length for a port is set in the configuration, the maximum frame length is fixed at 1518 octets when a 10BASE-T, 100BASE-TX, or 100BASE-FX half-duplex connection is used. This note also applies when auto-negotiation results in a 10BASE-T or 100BASE-TX half-duplex connection.
- For the maximum frame length, specify a value obtained by adding 18 or more octets to the IP MTU value (the set value in the `ip mtu` configuration command). If you specify a value obtained by adding less than 18 octets to the IP MTU value, the interface operates while the IP MTU value is reduced to a value obtained by subtracting 18 octets from the specified value.

(2) Setting the maximum frame length for all ports

Points to note

The example below shows how to set 4096 octets as the maximum frame length for the ports of all Ethernet interfaces on the Device. This setting enables the ports to send and receive jumbo frames up to 4096 octets.

Command examples

1. **(config)# system mtu 4096**

Sets the maximum frame length of all ports on a device to 4096 octets.

Notes

- Even if the maximum frame length for all ports is set in the configuration, the maximum frame length is fixed at 1518 octets when a 10BASE-T, 100BASE-TX, or 100BASE-FX half-duplex connection is used. This note also applies when auto-negotiation results in a 10BASE-T or 100BASE-TX half-duplex connection.
- For the maximum frame length, specify a value obtained by adding 18 or more octets to the IP MTU value (the set value in the `ip mtu` configuration command). If you specify a value obtained by adding less than 18 octets to the IP MTU value, the interface operates while the IP MTU value is reduced to a value obtained by subtracting 18 octets from the specified value.

16.2.5 Configuring the link-down detection timer

If the wait time before a link-down is detected after the detection of a link fault is too short, depending on the remote device, the link might be unstable. You can avoid this problem by setting a link-down detection timer.

Points to note

Make sure that you set as small a link-down detection timer value as possible without risking the link becoming unstable. If the link is stable even when a link-down detection timer is not set, you do not need to set one.

Command examples

1. **(config)# interface gigabitethernet 1/10**

Specifies that Ethernet interface 1/10 is to be configured.

2. **(config-if)# link debounce time 5000**

Sets the link-down detection timer value to 5000 (milliseconds).

Notes

Using a link-down detection timer can prevent a link from becoming unstable. However, if a fault occurs, the time required for the interface to settle in the link-down status is longer. If you want this time to be short, do not set a link-down detection timer.

16.2.6 Configuring the link-up detection timer

If the wait time before a link-up is detected after the detection of a link fault is short, depending on the remote device, the network might be unstable. You can avoid this problem by setting a link-up detection timer.

Points to note

Make sure that you set as small a link-up detection timer value as possible without risking the network becoming unstable. If the network is stable even when a link-up detection timer is not set, you do not need to set one.

Command examples

1. **(config)# interface gigabitethernet 1/10**

Specifies that Ethernet interface 1/10 is to be configured.

2. **(config-if)# link up-debounce time 5000**

Sets the link-up detection timer value to 5000 (milliseconds).

Notes

The larger the value you set for the link-up detection timer, the more time it takes until communication is restored after a link fault has been corrected. If you want this time to be short, do not set a link-up detection timer.

16.2.7 Configuring the notification of a frame sending or reception error

If sending or receiving frames fails because of a minor error, the Device collects statistics about why the frames were discarded. If the number of error occurrences or the error occurrence rate over 30 seconds exceeds the threshold, the error occurrences are logged and reported by private traps.

The Device can be configured for these thresholds and for notification. If no settings are specified, the log is displayed for only the first error when 15 errors have occurred in 30 seconds.

(1) Using the number of error frames as the threshold for notification

Points to note

To set the threshold for error occurrences (the number of error frames) as the condition for error notification on the Device, execute the `frame-error-notice` command with the `error-frames` parameter specified.

Command examples

1. **(config)# frame-error-notice error-frames 50**

Sets the threshold for error occurrences (the number of error frames) to 50 (times).

(2) Using the error occurrence rate as the threshold for notification

Points to note

To set the threshold for the error occurrence rate (the error rate) as an error notification condition on the Device, execute the `frame-error-notice` command with the `error-rate` parameter specified.

Command examples

1. **(config)# frame-error-notice error-rate 20**

Sets the threshold for the error occurrence rate to 20 (%).

(3) Displaying the log when an error is reported

Points to note

To have the log displayed in the event of an error as the condition for error notification, execute the `frame-error-notice` command with either the `onetime-display` parameter or the `everytime-display` parameter specified. If you do not want the log to be displayed, specify `off` in the command. Settings configured by using this command do not affect private traps.

Command examples

1. **(config)# frame-error-notice everytime-display**

Displays the log every time an error occurs.

(4) Combining multiple conditions

The following shows an example of setting the threshold for the error occurrences (the number of error frames) in addition to setting that the log is displayed every time an error occurs.

Points to note

To set a combination of error notification conditions, specify the corresponding arguments in the `frame-error-notice` command. Note that executing the `frame-error-notice` command overrides the notification condition settings previously configured by the `frame-error-notice` command. If you want to use the previous settings, specify them again in the `frame-error-notice` command.

Command examples

1. **(config)# frame-error-notice error-frames 50 everytime-display**

Sets the threshold for error occurrences (the number of error frames) to 50 (times), and sets the log to be displayed every time an error occurs.

Notes

If you want to use private traps, use the `snmp-server host` command to configure that a trap is sent whenever a frame reception error or a frame sending error occurs.

16.3 Operations common to all Ethernet interfaces

16.3.1 List of operation commands

The following table describes the operation commands common to all Ethernet interfaces.

Table 16-5: List of operation commands

Command name	Description
show interfaces	Shows Ethernet information.
clear counters	Clears the Ethernet statistics counters.
show port	Shows Ethernet information in list format.
activate	Changes the status of an Ethernet port from inactive to active.
inactivate	Changes the status of an Ethernet port from active to inactive.

16.3.2 Checking the Ethernet operating status

You can use the `show port` command to check the status of all Ethernet ports on the Device. If you want to use an Ethernet port, confirm that `up` is displayed for `Status` of the port in the execution results. The following figure shows the result of executing the command.

Figure 16-4: Result of executing the show port command

```
> show port
Date 20XX/04/01 12:00:00 UTC
Port Counts: 12
Port  Name          Status  Speed          Duplex    FCtl  FrLen  ChGr/Status
1/1   geth1/1           up      1000BASE-SX    full(auto) off   1518   -/-
1/2   geth1/2           up      1000BASE-SX    full      on    1518   -/-
1/3   geth1/3           dis     1000BASE-SX    full(auto) -     -     -/-
1/4   geth1/4           inact   1000BASE-SX    full(auto) -     -     -/-
:
:
```

16.4 Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces

This section describes an Ethernet interface that uses a 10BASE-T, 100BASE-TX, or 1000BASE-T twisted pair cable (UTP).

16.4.1 Functionality

(1) *Connection interface*

(a) **Automatic recognition (auto-negotiation) of 10BASE-T, 100BASE-TX, and 1000BASE-T**

10BASE-T, 100BASE-TX, and 1000BASE-T support connection methods that use automatic recognition (auto-negotiation) and fixed settings.

- Connection by automatic recognition: 10BASE-T, 100BASE-TX, and 1000BASE-T (full duplex)
- Connection using fixed settings: 10BASE-T and 100BASE-TX

You can configure either of the modes shown below. Select the appropriate mode for the network to be connected. The default for the Device is auto-negotiation.

- Auto-negotiation
- 100BASE-TX full duplex
- 100BASE-TX half duplex
- 10BASE-T full duplex
- 10BASE-T half duplex

(b) **10BASE-T, 100BASE-TX, and 1000BASE-T connection specifications**

The table below describes the connection specifications for transmission speed and duplex mode (full or half) for a connection between the Device and a remote device.

Note that, depending on the remote device, auto-negotiation is sometimes unavailable for a 10BASE-T or 100BASE-TX connection. For this reason, if at all possible, use the fixed settings appropriate for the interface on the remote device.

Also note that a 1000BASE-T connection supports only full-duplex in auto-negotiation mode.

Table 16-6: Connection specifications for transmission speed and duplex mode (full or half)

Settings on the remote device		Settings on the Device				
Method	Interface	Fixed settings				Auto-negotiation
		10BASE-T half duplex	10BASE-T full duplex	100BASE-TX half duplex	100BASE-TX full duplex	
Fixed settings	10BASE-T half duplex	10BASE-T half duplex	N	N	N	10BASE-T half duplex
	10BASE-T full duplex	N	10BASE-T full duplex	N	N	N
	100BASE-TX half duplex	N	N	100BASE-TX half duplex	N	100BASE-TX half duplex
	100BASE-TX full duplex	N	N	N	100BASE-TX full duplex	N
	1000BASE-T half duplex	N	N	N	N	N
	1000BASE-T full duplex	N	N	N	N	N

Settings on the remote device		Settings on the Device				
Method	Interface	Fixed settings				Auto-negotiation
		10BASE-T half duplex	10BASE-T full duplex	100BASE-TX half duplex	100BASE-TX full duplex	
Auto-negotiation	10BASE-T half duplex	10BASE-T half duplex	N	N	N	10BASE-T half duplex
	10BASE-T full duplex	N	N	N	N	10BASE-T full duplex
	10BASE-T full duplex and half duplex	10BASE-T half duplex	N	N	N	10BASE-T full duplex
	100BASE-TX half duplex	N	N	100BASE-TX half duplex	N	100BASE-TX half duplex
	100BASE-TX full duplex	N	N	N	N	100BASE-TX full duplex
	100BASE-TX full duplex and half duplex	N	N	100BASE-TX half duplex	N	100BASE-TX full duplex
	10BASE-T/100BASE-TX full duplex and half duplex	10BASE-T half duplex	N	100BASE-TX half duplex	N	100BASE-TX full duplex
	1000BASE-T half duplex	N	N	N	N	N
	1000BASE-T full duplex	N	N	N	N	1000BASE-T full duplex
	1000BASE-T full duplex and half duplex	N	N	N	N	1000BASE-T full duplex
	10BASE-T/100BASE-TX/1000BASE-T full duplex and half duplex	10BASE-T half duplex	N	100BASE-TX half duplex	N	1000BASE-T full duplex

Legend: N: A connection is not possible

(2) Auto-negotiation

Auto-negotiation is functionality by which two devices negotiate to determine the connection conditions (transmission speed, duplex mode (full or half), and whether to use flow control).

For details on the connection specifications for the Device, see *Table 16-6: Connection specifications for transmission speed and duplex mode (full or half)*. Note that if the connection conditions are not determined by auto-negotiation, the Device attempts to establish a connection until a link is established.

(3) Flow control

The flow control functionality sends a pause packet to a remote device to instruct it to temporarily stop sending frames so that received frames are not discarded when the reception buffer on the device is full. Conversely, when the device receives a pause packet, it regulates sending to the remote device. Note that flow control is available only in full-duplex mode.

The Device monitors the usage of the reception buffer, and sends a pause packet to the remote device when sending on the remote device must be regulated. When the Device receives a pause packet, it regulates sending to the remote device. Whether to enable or disable flow control is set separately for sending and reception. The flow control settings for sending and reception are configured separately. Whether to enable or disable flow control depends on these settings and the auto-negotiation result. When specifying the flow control settings, make sure that the sending and receiving settings on the Device and the remote device do not conflict. For example, if you set `on` for the pause-packet send setting on the Device, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Device and a remote device, see *Table 16-7: Flow control for sending on the device*, *Table 16-8: Flow control for receiving on the device*, and *Table 16-9: Flow control operation determined by the auto-negotiation result*.

Table 16-7: Flow control for sending on the device

Pause-packet send setting on the Device	Pause-packet receive setting on the remote device	Flow control operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend

`on`: Enabled.

`off`: Disabled. If `off` is set when `desired` is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 16-9: Flow control operation determined by the auto-negotiation result*.

`desired`: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 16-9: Flow control operation determined by the auto-negotiation result*.

Table 16-8: Flow control for receiving on the device

Pause-packet receive setting on the Device	Pause-packet send setting on the remote device	Flow control operation
on	Enabled	Sending on the Device is regulated.
off	Disabled	Sending on the Device is not regulated.
desired	desired	Sending on the Device is regulated.

Legend

on: Enabled.

off: Disabled. If off is set when desired is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 16-9: Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined by the negotiation result. For details, see *Table 16-9: Flow control operation determined by the auto-negotiation result*.

Table 16-9: Flow control operation determined by the auto-negotiation result

Device		Remote device		Result of auto-negotiation on the Device		Flow control operation	
Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Is sending regulated on the Device ?	Is sending regulated on the remote device?
on	desired	Enabled	Enabled	on	on	Yes	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
off		Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes

Device		Remote device		Result of auto-negotiation on the Device		Flow control operation	
Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Is sending regulated on the Device ?	Is sending regulated on the remote device?
desired	on	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	on	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	on	No	No
			desired	on	on	Yes	Yes
	off	Enabled	Enabled	off	off	No	No
			Disabled	off	off	No	No
			desired	off	off	No	No
		Disabled	Enabled	on	off	No	Yes
			Disabled	off	off	No	No
			desired	on	off	No	Yes
		desired	Enabled	off	off	No	No
			Disabled	off	off	No	No
			desired	off	off	No	No
	desired	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes

(4) AUTO-MDI/MDI-X

AUTO-MDI/MDI-X automatically switches between MDI and MDI-X. The functionality enables communication via either a crossover cable or a straight cable, and is available only when auto-negotiation is used. This functionality supported only during auto-negotiation. If the connection mode (full duplex or half duplex) is fixed, MDI-X is always selected. The following table describes the MDI and MDI-X pin mappings.

Table 16-10: MDI and MDI-X pin mappings

RJ45 Pin No.	MDI			MDI-X		
	1000BASE-T	100BASE-TX	10BASE-T	1000BASE-T	100BASE-TX	10BASE-T
1	BI_DA+	TD+	TD+	BI_DB+	RD+	RD+
2	BI_DA-	TD-	TD-	BI_DB-	RD-	RD-
3	BI_DB+	RD+	RD+	BI_DA+	TD+	TD+
4	BI_DC+	Unused	Unused	BI_DD+	Unused	Unused
5	BI_DC-	Unused	Unused	BI_DD-	Unused	Unused
6	BI_DB-	RD-	RD-	BI_DA-	TD-	TD-
7	BI_DD+	Unused	Unused	BI_DC+	Unused	Unused
8	BI_DD-	Unused	Unused	BI_DC-	Unused	Unused

Note 1

For the 10BASE-T and 100BASE-TX cables, separate signal lines are used for sending (TD) and reception (RD).

Note 2

For the 1000BASE-T cable, because all eight pins are used for both sending and reception (simultaneous bi-directional communication), the signal names are different from other cables. BI_Dx indicates a bi-directional data signal.

(5) Jumbo frame

Jumbo frame support allows a device to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU length.

The Device supports only frames in Ethernet V2 format. The Device does not support frames in IEEE 802.3 format. For details about frame formats, see *16.1.3 MAC sublayer control*. For details about tagged frame formats, see *16.1.4 VLAN Tag*. Note that the device supports only 100BASE-TX (full duplex) and 1000BASE-T (full duplex) as the physical interface. The following table describes the jumbo frame support status.

Table 16-11: Jumbo frame support status

Item	Specifications
Frame format	Ethernet V2 ^{#1}
Frame length (octets) ^{#2}	1519 to 9596

#1

For details about the frame formats, see *16.1.3 MAC sublayer control*.

#2

(FCS excluded).

(6) Notes on a 10BASE-T, 100BASE-TX, or 1000BASE-T connection

- Make sure that the transmission speed and the duplex mode (full or half) settings on the local and remote devices are the same.

If these settings on the devices are different, communication might stop. If communication stops, execute the `inactivate` command, and then execute the `activate` command for the relevant ports.

- For details on the cables that can be used, see the *Hardware Instruction Manual*.
- A full-duplex interface is implemented by not using the collision detection functionality and the loopback functionality. Therefore, to use a 10BASE-T or 100BASE-TX connection for a full-duplex interface, always make sure that the remote port is set as a full-duplex interface.
- If 1000BASE-T is used, only full-duplex auto-negotiation mode is supported.

16.4.2 SFP for 10BASE-T/100BASE-TX/1000BASE-T

For the Device, you can establish a 10BASE-T, 100BASE-TX, or 1000BASE-T connection with a 1000BASE-X (SFP) port by using a special SFP. The communication functionality available for an SFP connection is the same as that available for a 10BASE-T, 100BASE-TX, or 1000BASE-T connection.

16.5 Configuration of 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces

16.5.1 Configuring ports

(1) *Setting the speed and duplex mode (full or half)*

You can set the transmission speed and duplex mode (full duplex or half duplex) used for communication between the Device and a remote device. By default, the transmission speed and duplex mode (full duplex or half duplex) are determined automatically by auto-negotiation.

(a) **Connecting to a remote device that does not support auto-negotiation**

Points to note

Depending on the remote device, 10BASE-T or 100BASE-TX connection sometimes cannot be established by auto-negotiation. If the connection cannot be established, you need to specify the transmission speed and duplex mode (full duplex or half duplex) according to the remote device, and establish a connection with fixed settings.

Command examples

1. **(config)# interface gigabitethernet 1/10**
(config-if)# shutdown
(config-if)# speed 10
(config-if)# duplex half

Shuts down the Ethernet interface and configures fixed settings for a 10BASE-T half-duplex connection with the remote device.

2. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

(b) **Using a specific communication speed even when auto-negotiation is used**

Points to note

For the Device, you can set a specific transmission speed even when auto-negotiation is used for a connection. Note that if auto-negotiation is used and a specific transmission speed is also specified, even if a connection with auto-negotiation is successful, the status of the line is not link-up unless the set transmission speed is assured. This eliminates the risk of the line being connected at an unexpected transmission speed.

Command examples

1. **(config)# interface gigabitethernet 1/10**
(config-if)# shutdown
(config-if)# speed auto 1000

Shuts down the Ethernet interface and configures settings for establishing only a 1000BASE-T connection even if the Device connects to the remote device via auto-negotiation.

2. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

Notes

If the combination of the transmission speed and duplex mode (full duplex or half duplex) is invalid, a connection with the remote device is established via auto-negotiation.

16.5.2 Configuring flow control

To prevent the Device from discarding received frames when the reception buffer has become full, the Device needs to send a pause packet to the remote device to request regulated sending. The remote device must be able to receive pause packets and regulate sending in response to a received pause packet.

Whether the Device regulates sending when it receives a pause packet from the remote device depends on the settings. The Device can negotiate whether to send pause packets to, or receive them from, the remote device during auto-negotiation.

Points to note

Determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1. **(config)# interface gigabitethernet 1/10**
(config-if)# shutdown
(config-if)# flowcontrol send on
(config-if)# flowcontrol receive on

Shuts down the Ethernet interface and enables the sending and receiving of pause packets with the remote device.

2. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

16.5.3 Configuring AUTO-MDI/MDI-X

The 10BASE-T, 100BASE-TX, or 1000BASE-T port on a Device support AUTO-MDI/MDI-X, which automatically selects MDI or MDI-X according to the cable type (straight or crossover) during auto-negotiation. If AUTO-MDI/MDI-X is disabled, MDI (for hub use) is always selected.

Points to note

To fix the MDI setting as MDI, disable AUTO-MDI/MDI-X on the interface whose MDI setting you want to fix.

Command examples

1. **(config)# interface gigabitethernet 1/24**
 Specifies that Ethernet interface 1/24 is to be configured.
2. **(config-if)# no mdix auto**
(config-if)# exit

Disables AUTO-MDI/MDI-X and fixes the MDI setting as MDI.

16.6 Description of the 1000BASE-X interface

16.6.1 Functionality

This section describes an Ethernet interface that uses a 1000BASE-X optical fiber cable.

(1) *Connection interface*

(a) **1000BASE-X**

The 1000BASE-SX, 1000BASE-SX2, 1000BASE-LX, 1000BASE-LH, and 1000BASE-BX interfaces are supported. The transmission speed and duplex mode settings are fixed at 1000 Mbit/s and full duplex.

1000BASE-SX:

Used for short-distance connections.

(550 m max. in multi-mode)

1000BASE-SX2:

Uses a two-kilometer multi-mode optical fiber cable that ensures a connection over that distance.

(2 km max. in multi-mode)

1000BASE-LX:

Used for medium-distance connections

(5 km max. in single-mode, 550 m max. in multi-mode).

1000BASE-LH:

Used for long-distance connections

(70 km max. in single-mode).

1000BASE-BX:

Because the upstream and downstream wavelengths are different, a pair of transceivers must be provided for each upstream and downstream.

The Device supports the 1000BASE-BX10-D and 1000BASE-BX10-U interfaces, prescribed in IEEE 802.3ah, and the 1000BASE-BX40-D and 1000BASE-BX40-U interfaces, which are vendor-specific interfaces.

1000BASE-BX10-D and 1000BASE-BX10-U:

Used for medium-distance connections

(10 km max. in single-mode).

1000BASE-BX40-D and 1000BASE-BX40-U:

Used for long-distance connections

(40 km max. in single-mode).

You can configure either of the modes shown below. Select the appropriate mode for the network to be connected. The default for the Device is auto-negotiation.

- Auto-negotiation
- 1000BASE-X full duplex (fixed)

(b) 1000BASE-X connection specifications

The table below describes the connection specifications for transmission speed and duplex mode (full or half) for a connection between the Device and a remote device. For details about the physical specifications for the 1000BASE-X interface, see the *Hardware Instruction Manual*.

Table 16-12: Connection specifications for transmission speed and duplex mode (full or half)

Settings on the remote device		Settings on the Device	
Method	Interface	Fixed settings	Auto-negotiation
		1000BASE full duplex	1000BASE full duplex
Fixed settings	1000BASE half duplex	N	N
	1000BASE full duplex	1000BASE full duplex	N
Auto-negotiation	1000BASE half duplex	N	N
	1000BASE full duplex	N	1000BASE full duplex

Legend: N: A connection is not possible

(2) Auto-negotiation

Auto-negotiation is the functionality by which two devices negotiate to determine which duplex mode is used and whether to use flow control.

For details on the connection specifications for the Device, see *Table 16-12: Connection specifications for transmission speed and duplex mode (full or half)*. Note that if the connection conditions are not determined by auto-negotiation, the Device attempts to establish a connection until a link is established.

(3) Flow control

The flow control operations for 1000BASE-X are the same as the flow control operations for 10BASE-T, 100BASE-TX, and 1000BASE-T. For details, see (3) *Flow control* in 16.4.1 *Functionality*.

(4) Jumbo frame

Jumbo frame support allows a device to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU length.

The Device supports only frames in Ethernet V2 format. The Device does not support frames in IEEE 802.3 format. For details about frame formats, see 16.1.3 *MAC sublayer control*. For details about tagged frame formats, see 16.1.4 *VLAN Tag*. The following table describes the jumbo frame support status.

Table 16-13: Jumbo frame support status

Item	Specifications
Frame format	Ethernet V2 ^{#1}
Frame length (octets) ^{#2}	1519 to 9596

#1

For details about the frame formats, see *16.1.3 MAC sublayer control*.

#2

(FCS excluded).

(5) Notes on a 1000BASE-X connection

- Only a connection by using auto-negotiation or a fixed connection in full-duplex mode is supported.
- Make sure that the remote device uses auto-negotiation or the fixed full-duplex mode setting.
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

16.7 Configuration of the 1000BASE-X interface

16.7.1 Configuring ports

(1) *Setting the speed and duplex mode (full or half)*

You can set the transmission speed and duplex mode (full duplex or half duplex) used for communication between the Device and a remote device. By default, the transmission speed and duplex mode (full duplex or half duplex) are determined automatically by auto-negotiation.

Points to note

The Devices connect to remote devices by auto-negotiation. If auto-negotiation is not used, set the transmission speed to 1000 Mbit/s, specify the duplex mode (full or duplex) as full duplex, and establish a connection with the fixed setting.

Command examples

1.

```
(config)# interface gigabitethernet 1/1
(config-if)# shutdown
(config-if)# speed 1000
(config-if)# duplex full
```

Shuts down the Ethernet interface and configures fixed settings for a 1000-Mbit/s full-duplex connection with the remote device.

2.

```
(config-if)# no shutdown
```

Releases the Ethernet interface from the shutdown status.

Notes

If the combination of the transmission speed and duplex mode (full duplex or half duplex) is invalid, a connection with the remote device is established via auto-negotiation.

16.7.2 Configuring flow control

To prevent the Device from discarding received frames when the reception buffer has become full, the Device needs to send a pause packet to the remote device to request regulated sending. The remote device must be able to receive pause packets and regulate sending in response to a received pause packet.

Whether the Device regulates sending when it receives a pause packet from the remote device depends on the settings. The Device can negotiate whether to send pause packets to, or receive them from, the remote device during auto-negotiation.

Points to note

Determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1.

```
(config)# interface gigabitethernet 1/1
(config-if)# shutdown
(config-if)# flowcontrol send on
(config-if)# flowcontrol receive on
```

Shuts down the Ethernet interface and enables the sending and receiving of pause packets with

the remote device.

2. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

16.8 Description of the 10GBASE-R interface

16.8.1 Functionality

This section describes an Ethernet interface that uses a 10GBASE-R optical fiber cable.

(1) Connection interface

(a) 10GBASE-R

The 10GBASE-SR, 10GBASE-LR, and 10GBASE-ER interfaces are supported. The transmission speed and duplex mode settings are fixed at 10 Gbit/s and full duplex.

10GBASE-SR:

Used for short-distance connections (300 m max.[#] in multi-mode).

#

The maximum distance depends on the cable used. For details about the distance for each cable, see the *Hardware Instruction Manual*.

10GBASE-LR:

Used for medium-distance connections (10 km max. in single-mode).

10GBASE-ER:

Used for long-distance connections (40 km max. in single-mode).

(b) 10GBASE-R connection specifications

For details about the physical specifications for the 10GBASE-R interface, see the *Hardware Instruction Manual*.

(2) Flow control

The flow control functionality sends a pause packet to a remote device to instruct it to temporarily stop sending frames so that received frames are not discarded when the reception buffer on the device is full. Conversely, when the device receives a pause packet, it regulates sending to the remote device.

The Device monitors the usage of the reception buffer, and sends a pause packet to the remote device when sending on the remote device must be regulated. When the Device receives a pause packet, it regulates sending to the remote device. Whether to enable or disable flow control is set separately for sending and reception. When specifying the flow control settings, make sure that the sending and receiving settings on the Device and the remote device do not conflict. For example, if you set on for the pause-packet send setting on the Device, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Device and remote device, see *Table 16-14: Flow control for sending on the device* and *Table 16-15: Flow control for receiving on the device*.

Table 16-14: Flow control for sending on the device

Pause-packet send setting on the Device	Receive pause packet on the remote device	Flow control Operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend: on: Enabled, off: Disabled, desired: Enabled

Table 16-15: Flow control for receiving on the device

Pause-packet receive setting on the Device	Send pause packet on the remote device	Flow control Operation
on	Enabled	Sending on the Device is regulated.
off	Disabled	Sending on the Device is not regulated.
desired	desired	Sending on the Device is regulated.

Legend: on: Enabled, off: Disabled, desired: Enabled

(3) Jumbo frame

Jumbo frame support allows a device to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU length.

The Device supports only frames in Ethernet V2 format. The Device does not support frames in IEEE 802.3 format. For details about frame formats, see *16.1.3 MAC sublayer control*. For details about tagged frame formats, see *16.1.4 VLAN Tag*. The following table describes the jumbo frame support status.

Table 16-16: Jumbo frame support status

Item	Specifications
Frame format	Ethernet V2 ^{#1}
Frame length (octets) ^{#2}	1519 to 9596

#1

For details about the frame formats, see *16.1.3 MAC sublayer control*.

#2

(FCS excluded).

(4) Notes on a 10GBASE-R connection

- In the IEEE 802.3ae standard, half-duplex mode and auto-negotiation are not prescribed for the 10GBASE-R interface. Therefore, only fixed full-duplex mode is supported for connection with the remote device.
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

16.9 Configuration of the 10GBASE-R interface

16.9.1 Configuring flow control

To prevent the Device from discarding received frames when the reception buffer has become full, the Device needs to send a pause packet to the remote device to request regulated sending. The remote device must be able to receive pause packets and regulate sending in response to a received pause packet.

Whether the Device regulates sending when it receives a pause packet from the remote device depends on the settings.

Points to note

Determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1. **(config)# interface tengigabitethernet 1/1**
(config-if)# shutdown
(config-if)# flowcontrol send on
(config-if)# flowcontrol receive on

Shuts down the Ethernet interface and enables the transmission and reception of pause packets with the remote device.

2. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

16.10 Description of 100GBASE-R

16.10.1 Functionality

This section describes an Ethernet interface that uses a 100GBASE-R optical fiber cable.0

(1) Connection interface

(a) 100GBASE-R

The 100GBASE-LR4 interface is supported. The transmission speed and duplex mode settings are fixed at 100 Gbit/s and full duplex.

100GBASE-LR4:

Used for medium-distance connections (10 km max. in single-mode).

(b) 100GBASE-R connection specifications

For details about the physical specifications for the 10GBASE-R interface, see the *Hardware Instruction Manual*.

(2) Flow control

The flow control operations for 100GBASE-R are the same as the flow control operations for 10GBASE-R. For details, see (2) *Flow control* in 16.8.1 *Functionality*.

(3) Jumbo frame

The operation of jumbo frames for 100GBASE-R is the same as the one for 10GBASE-R. For details, see (3) *Jumbo frame* in 16.8.1 *Functionality*.

(4) Notes on a 100GBASE-R connection

- In the IEEE 802.3ba standard, half-duplex mode and auto-negotiation are not prescribed for the 100GBASE-R interface. Therefore, only fixed full-duplex mode is supported for connection with the remote device.
- If you change the maximum frame length for a communicating port by using the configuration, frames sent or received via that port might be discarded temporarily.
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

16.11 Configuration of the 100GBASE-R interface

16.11.1 Configuring flow control

To prevent the Device from discarding received frames when the reception buffer has become full, the Device needs to send a pause packet to the remote device to request regulated sending. The remote device must be able to receive pause packets and regulate sending in response to a received pause packet.

Whether the Device regulates sending when it receives a pause packet from the remote device depends on the settings.

Points to note

Determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1. **(config)# interface hundredgigabitethernet 1/1**
(config-if)# shutdown
(config-if)# flowcontrol send on
(config-if)# flowcontrol receive on

Shuts down the Ethernet interface and enables the sending and receiving of pause packets with the remote device.

2. **(config-if)# no shutdown**

Releases the Ethernet interface from the shutdown status.

Chapter

17. Link Aggregation

This chapter describes link aggregation and how to use it.

- 17.1 Description of the link aggregation basic functionality
- 17.2 Configuration of the link aggregation basic functionality
- 17.3 Description of the link aggregation extended functionality
- 17.4 Configuration of the link aggregation extended functionality
- 17.5 Operation for link aggregation

17.1 Description of the link aggregation basic functionality

17.1.1 Overview

Link aggregation is functionality that connects devices by establishing multiple links between the Ethernet ports of each device, and that treats these links as one port. This port is called a channel group. Link aggregation can expand bandwidth and ensure redundancy between connected devices.

17.1.2 Link aggregation configuration

(1) Adding and removing a port

A configuration is used to set ports that make up a channel group. Setting a port by using a configuration is referred to as "add", and deleting a port by using a configuration is referred to as "remove".

- Add: Adds a port in a channel group.
- Remove: Removes a port in a channel group.

(2) Attaching and detaching a port

Causing a port to operate in a channel group is referred to as "attach", and excluding a port from a channel group for operation is referred to as "detach".

- Attach: Enables a port in a channel group to communicate.
- Detach: Disables a port in a channel group from communicating.

(3) Up and down states of a channel group

If even one of the ports in a channel group is attached, that channel group comes in the up state. If a channel group comes up, communication using it is possible.

If all the ports in a channel group are detached, that channel group goes in the down state. If a channel group goes down, communication using it stops.

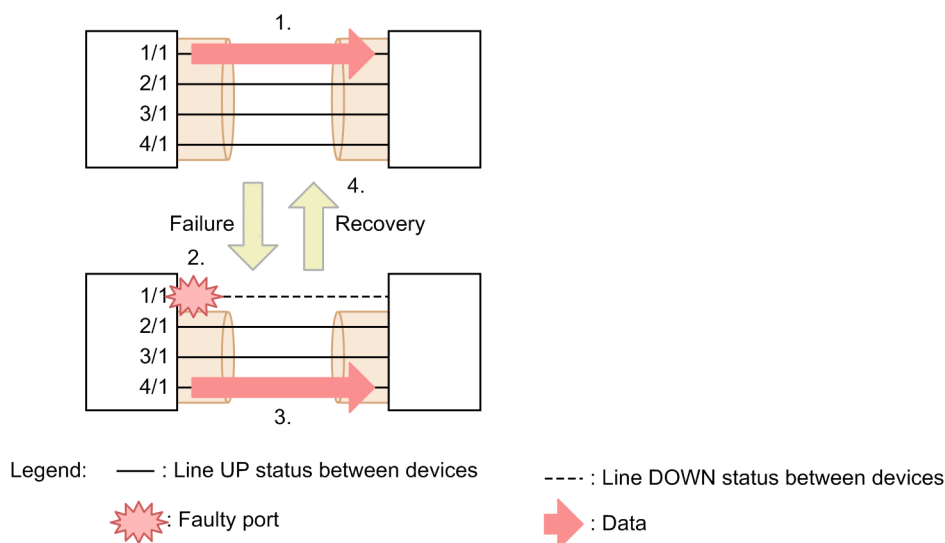
(4) Switchover and switch back

A frame sending port is selected from the attached ports. The operation when the frame sending port changes due to failure is called a switchover, and the operation when the original frame sending port is restored after recovery from failure is called a switch back.

(5) Configuration example

The figure below shows an example of a link aggregation configuration. In this example, four ports are aggregated. If a fault occurs on one of these ports, the faulty port is detached from the channel group, and communication continues by using the rest of the ports as the channel group.

Figure 17-1: Example of a link aggregation configuration



1. Four ports are attached. Frames are sent from port 1/1.
2. Port 1/1 is detached from the channel group because a failure occurs on the port. Also, the frame sending port is switched over to another port.
3. Three ports other than port 1/1, which was detached, are attached. Frames are sent from port 4/1.
4. Port 1/1 is attached to the channel group because the port recovered from the failure. Also, the frame sending port is switched back to port 1/1.

17.1.3 Supported specifications

(1) Link aggregation modes

The link aggregation of the Device supports LACP and static modes.

- LACP link aggregation

Link aggregation using the LACP (Link Aggregation Control Protocol) compliant with IEEE. LACP link aggregation starts operation of a channel group when LACP negotiation is successful. LACP is used to verify consistency and link normality between devices.

- Static link aggregation

Static link aggregation is link aggregation manually set by using configuration commands. LACP is not used. Operation of a channel group starts when the ports added to the channel group are placed in the link-up status.

(2) Supported specifications for link aggregation

The following table describes the supported specifications for link aggregation.

Table 17-1: Supported specifications for link aggregation

Item	Supported specifications
Link aggregation modes	<ul style="list-style-type: none"> • LACP • Static

Item	Supported specifications
Line speed	<ul style="list-style-type: none"> Default (when mixed-speed mode is not set): Ports with the same highest transmission speed among the ports that make up the channel group are attached. Mixed-speed mode: All the ports that make up the channel group are attached simultaneously.
Duplex mode	<ul style="list-style-type: none"> LACP link aggregation Ports operating in full duplex mode are attached. Static link aggregation Ports operating in full duplex or half duplex mode are attached. Two types of duplex mode are allowed to exist together in a channel group.

17.1.4 MAC address of the channel group

The Device uses a unique MAC address for each channel group.

17.1.5 Port allocation for sending frames

When sending frames, the Device allocates a port to each frame to distribute the traffic to ports for efficient port use. Two types of port allocation are available as shown below. You can specify one of them for each channel group by using a configuration.

- Port allocation according to information in frames
- Port allocation per VLAN tag

(1) Port allocation according to information in frames

Frames are sent from the ports allocated according to information in each frame. The following table describes reference information during IP layer forwarding operation.

Table 17-2: Reference information during IP layer forwarding operation.

Category	Forward	Sending frames originated by the device
IP frames	<ul style="list-style-type: none"> • Destination MAC address • Source MAC address • Destination IP address • Source IP address 	<ul style="list-style-type: none"> • Destination MAC address • Source MAC address • Destination IP address • Source IP address
Other frames	--	<ul style="list-style-type: none"> • Destination MAC address • Source MAC address

Legend: --: Not applicable

(2) Port allocation per VLAN tag

Frames are sent from the ports allocated per VLAN tag of the frames. The following table describes port allocation operation per VLAN tag.

Table 17-3: Port allocation operation per VLAN tag

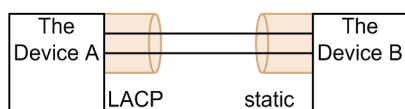
Operation category	Information source
IP layer forwarding	VLAN tags of forwarding frames
Sending frames originated by the device	VLAN tags of frames originated by the device

17.1.6 Notes on using link aggregation

(1) Configurations in which link aggregation is not possible

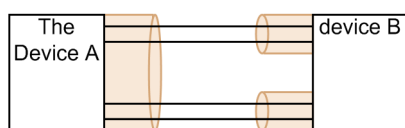
To use link aggregation, the settings of the connected devices must match. The following figure shows configurations in which link aggregation is not possible.

Figure 17-2: Configuration when connected devices are in different mode



If a configuration is created in such a way that two devices operate in different modes as shown in the above figure, LACP negotiation is not established and communication is cut off.

Figure 17-3: Configuration when channel groups of connected devices are in a point-to-multipoint relationship



If a point-to-multipoint configuration is created in such a way that Device A has one channel group while device B has multiple channel groups as shown in the above figure, a communication problem occurs between these devices such as a loop configuration in which frames sent from Device A come back via device B.

(2) Setting link aggregation

When you configure link aggregation, first, change the status of the ports to link-down, and then make sure that the connections between devices are not in a configuration such as those in (1) Configurations in which link aggregation is not possible. Next, return the ports to the link-up status.

17.2 Configuration of the link aggregation basic functionality

17.2.1 List of configuration commands

The following table describes the configuration commands for the link aggregation basic functionality.

Table 17-4: List of configuration commands

Command name	Description
channel-group lacp system-priority	Sets the LACP system priority for each channel group.
channel-group load-balance	Specifies the port allocation method when frames are sent.
channel-group mode	Adds a port to a channel group. Also sets a mode for a channel group.
channel-group periodic-timer	Sets the interval for LACPDUs to be sent by the partner device.
description	Sets supplementary information about a channel group.
interface port-channel	Sets a port channel interface or a port channel subinterface.
lacp port-priority	Sets the LACP port priority.
lacp system-priority	Sets the default for the LACP system priority.
shutdown	Stops communication for a channel group.

17.2.2 Configuring static link aggregation

Points to note

For static link aggregation, use the `channel-group mode` command to set the channel group number and `on` mode from configuration mode. Static link aggregation starts when these settings are set by the `channel-group mode` command.

Command examples

1. **(config)# interface range gigabitethernet 1/1-2**
Places the Device in configuration mode for configuring ports 1/1 and 1/2.
2. **(config-if-range)# channel-group 10 mode on**
Adds ports 1/1 and 1/2 to channel group 10 in static mode.

17.2.3 Configuring LACP link aggregation

(1) Setting the channel group

Points to note

For LACP link aggregation, use the `channel-group mode` command to specify the channel group number, and either `active` or `passive` mode in configuration mode.

Command examples

1. **(config)# interface range gigabitethernet 1/1-2**
Places the Device in configuration mode for configuring ports 1/1 and 1/2.
2. **(config-if-range)# channel-group 10 mode active**

Adds ports 1/1 and 1/2 to channel group 10 in LACP mode. If `active` mode is specified, the LACP starts sending LACPDU in active mode, independently of the partner device. If `passive` mode is specified, the LACP starts sending LACPDU only when LACPDU are received from the partner device.

(2) Setting the LACPDU sending interval

Points to note

The example below shows how to set the interval at which the partner device sends LACPDU to the Device. The Device receives LACPDU at the set interval.

For the LACPDU sending interval, set `long` (30 seconds) or `short` (1 second). The default is `long` (30 seconds). Setting `short` (1 second) makes it possible to detect a failure that does not cause link-down status, shortening the length of the communication stoppage in the event of failure.

Command examples

1. **(config)# interface port-channel 10**
(config-if)# channel-group periodic-timer short

Sets the LACPDU sending interval of channel group 10 to `short` (1 second).

Notes

Fault detection is earlier with the `short` setting (1 second), but the burden of the link aggregation program is increased due to an increase in the LACPDU traffic. If a timeout message is output or if communication often stops temporarily by setting `short` (1 second), use either the default value of `long` (30 seconds) or static mode.

17.2.4 Configuring a port channel interface

A port channel interface is used to set the functionality that operate on a channel group.

A port channel interface is set up manually by using configuration commands or generated automatically when the `channel-group` mode command is executed in configuration mode.

(1) Setting the functionality that operates on a channel group

Points to note

A port channel interface is used to set the functions that operate on a channel group, such as IP addresses. The following describes an example of setting a port channel interface.

Command examples

1. **(config)# interface range gigabitethernet 1/1-2**
(config-if-range)# channel-group 10 mode on
(config-if-range)# exit

Adds ports 1/1 and 1/2 to channel group 10 in static mode. The port channel interface for channel group 10 is automatically generated.

2. **(config)# interface port-channel 10**

Switches channel group 10 to configuration mode.

3. **(config-if)# ip address 192.0.2.1 255.255.255.0**

Sets an IP address for a port channel.

(2) Shutdown of a port channel interface

Points to note

When shutdown is set for a port channel, communication passing over its channel group stops. Ports in the link-up status keep that status.

Command examples

1. `(config)# interface range gigabitethernet 1/1-2`
`(config-if-range)# channel-group 10 mode on`
`(config-if-range)# exit`

Adds ports 1/1 and 1/2 to channel group 10 in static mode.

2. `(config)# interface port-channel 10`
`(config-if)# shutdown`

Changes the mode to configuration mode, and sets `shutdown`. Channel group 10 is shut down, so communication over ports 1/1 and 1/2 stops.

17.2.5 Configuring the allocation method

Set the port allocation method when frames are sent.

(1) Port allocation according to information in frames

Points to note

Set port allocation according to information in each frame for a channel group.

Command examples

1. `(config)# interface port-channel 10`
`(config-if)# channel-group load-balance frame`

Sets the allocation method for channel group 10 to port allocation according to information in each frame.

(2) Port allocation per VLAN tag

Points to note

Set port allocation per VLAN tag for a channel group.

Command examples

1. `(config)# interface port-channel 10`
`(config-if)# channel-group load-balance vlan`

Sets the allocation method for channel group 10 to port allocation per VLAN tag.

17.2.6 Deleting a channel group

Before you remove ports from a channel group or delete an entire channel group, you must set `shutdown` in Ethernet interface configuration mode for the ports that will be removed.

(1) Removing ports from a channel group

Points to note

The example below shows how to remove a port from a channel group. The removed port can operate independently of the channel group.

The `interface port-channel` command settings are not deleted even if all of the ports in the channel group are deleted. For details about deleting an entire channel group, see *(2) Deleting an entire channel group*.

Command examples

1. **(config)# interface gigabitethernet 1/1**

(config-if)# shutdown

Sets `shutdown` for port 1/1 to place the port in the link-down status so that the port can be removed safely from the channel group.

2. **(config-if)# no channel-group**

Removes port 1/1 from the channel group.

(2) Deleting an entire channel group

Points to note

The example below shows how to delete an entire channel group. The ports added to a deleted channel group can operate independently.

An entire channel group is deleted by deleting the `interface port-channel` setting. After this is deleted, the `channel-group` mode command settings are automatically deleted from each port added to the channel group.

Command examples

1. **(config)# interface range gigabitethernet 1/1-2**

(config-if-range)# shutdown

(config-if-range)# exit

Sets `shutdown` for all ports added to the channel group to place these ports in the link-down status so that the entire channel group can be deleted safely.

2. **(config)# no interface port-channel 10**

Deletes channel group 10. The `channel-group` mode command settings configured for ports 1/1 and 1/2 are also deleted automatically.

17.3 Description of the link aggregation extended functionality

17.3.1 Standby link functionality

(1) Description

The standby link functionality replaces a faulty port with a standby port in the same channel group to maintain the number of active ports in the channel group. This functionality can prevent a reduction of available bandwidth if a fault occurs.

The standby link functionality is available only when static link aggregation is used.

(2) How a standby link is selected

The maximum number of active ports in a channel group is set in the configuration. The rest of the ports in the channel group are standby ports.

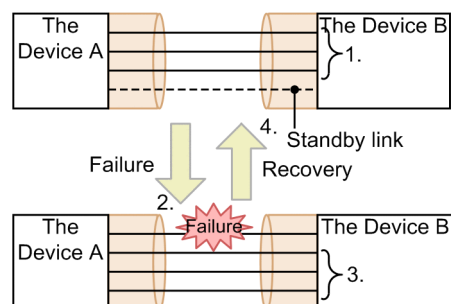
Standby ports are determined based on the port priority, NIF number, and port number set in the configuration. The following table describes the selection principle.

Table 17-5: Standby port selection principle

Priority	Parameter	Description
High ↑ ↓ Low	Port priority	Ports in the channel group are selected as standby ports in descending order of port priority level.
	NIF number	Ports in the channel group are selected as standby ports in descending order of NIF number.
	Port number	Ports in the channel group are selected as standby ports in descending order of port number (the port with the largest port number is selected first).

The figure below shows an example configuration for the standby link functionality. In this example, four ports belong to a channel group, and the maximum number of active ports is three.

Figure 17-4: Example of standby link functionality operation



1. The maximum number of active ports is set to 3 in a channel group with four ports.
2. A link failure occurs.
3. The standby link allows the Devices to retain the link aggregation configuration without bandwidth reduction.
4. The link recovers from the failure.

(3) Standby link modes

The standby link functionality has the following two modes:

- Link-down mode

In link-down mode, the status of the standby links changes to link-down. Set this mode for the Device only. Ports on the partner device that do not support the standby link functionality can also be used as standby ports.

- Link-not-down mode

In link-not-down mode, sending from standby links stops, but the status of the standby links does not change to link-down. Because the standby links are in the link-up status, monitoring of faults can also be performed for these standby ports. Note that in this mode, standby ports do not send data, but can receive data. Ports on a partner device that does not support the standby link functionality can also be connected.

(4) Channel group status in each standby link mode

In link-down mode, if there is only one attached port in a channel group and a failure occurs on that port, the channel group temporarily goes down when the faulty port is replaced with a standby port. In link-not-down mode, the standby port replaces the faulty port while the channel group remains in an up state.

The state in which there is only one attached port in a channel group arises in either of the following cases:

- The maximum number of active ports is set to 1 by using the `max-active-port` configuration command.
- There are one or more ports, only one of which provides the highest transmission speed, and mixed-speed mode is not set.

17.3.2 Port detachment restriction functionality

(1) Description

If the number of detached ports exceeds the limit set by a configuration, the port detachment restriction functionality makes the relevant channel group go down considering that the said channel group failed entirely. To use this functionality on the Device, set a higher LACP system priority than the one set for the partner device. When this functionality is set for the partner device, the limit on the number of detached ports must be the same value as the one set in the Device.

The port detachment restriction functionality is available only when LACP link aggregation is used.

(2) LACP system priority in the port detachment restriction functionality

The priority is determined based on the LACP system priority set in the configuration and the MAC address of the LACP system ID. The table below describes the principle for this determination. As described in the table, if both devices have the same LACP system priority, then the MAC address of the LACP system ID is used as the condition for determination. In the Device, note that the device MAC address is used as the MAC address of the LACP system ID.

Table 17-6: Principle for determining the device that judges whether all the ports in channel groups are usable for aggregation

Priority	Parameter	Remarks
High ↑	LACP system priority	The device with the smaller LACP system priority value performs judgment.
↓ Low	The MAC address of the LACP system ID	The device with the smaller MAC address value performs judgment.

17.3.3 Mixed-speed mode

(1) Description

Normally, a channel group consists of ports whose transmission speed is the same. In mixed-speed

mode, however, ports with different transmission speeds can be used concurrently in one channel group. This mode allows you to more flexibly change the configuration of a channel group.

Note that the transmission speed is not applied to port allocation when frames are sent. For example, when a 1 Gbit/s port and a 10 Gbit/s port are used in mixed-speed mode, the difference of transmission speed is not applied to the allocation of frames to ports. Normally, we recommend that you use ports whose transmission speed is the same.

(2) Example of changing the configuration of a channel group

You can change the transmission speeds used in a channel group (network reconfiguration) while the channel group remains in an up state.

To do so, use the procedure below to change the transmission speeds of ports in a channel group by using mixed-speed mode. Set the configuration shown in this procedure for the Device and for the partner device each.

1. Operate link aggregation with a channel group that consists of ports whose transmission speed is the same (two 1 Gbit/s ports).
2. Set mixed-speed mode.
3. Add two 10 Gbit/s ports to the channel group.
4. Place the two 10 Gbit/s ports you added in step 3 in the link-up status.
5. Set the `shutdown` configuration command for the two 1 Gbit/s ports.
6. Remove the two 1 Gbit/s ports from the channel group.
7. Delete mixed-speed mode.
8. The channel group now consists of two 10 Gbit/s ports.

17.3.4 Switch back suppression

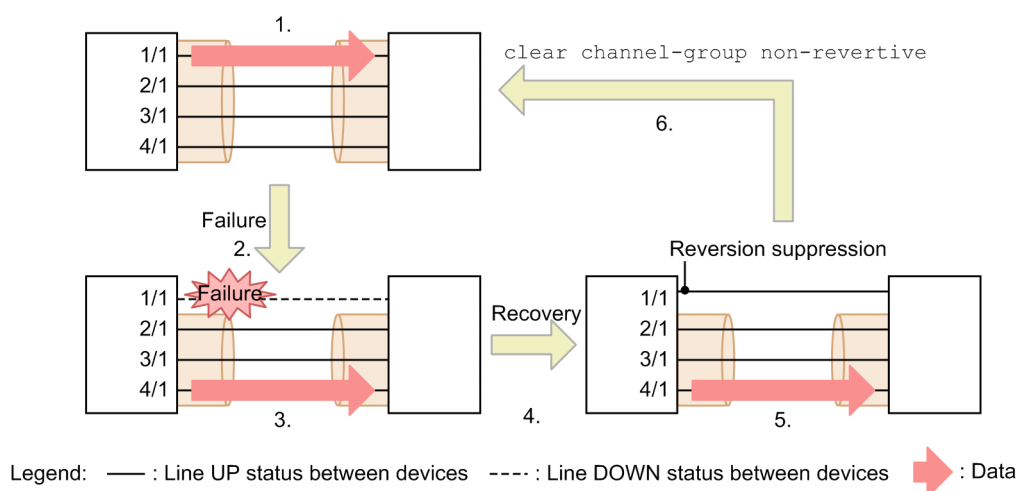
(1) Description

When a port attached to a channel group recovers from a failure after being detached, switch back suppression suppresses switch back of the port.

Switch back suppression is available only when LACP link aggregation is used.

To attach a port that is in the switch back suppression state, execute the `clear channel-group non-revertive` operation command. Because this operation command is required to attach a port that is in the switch back suppression state, the operator can intentionally switch such a port back at a time when the operation is less affected by switch back. The following figure provides an overview of switch back suppression.

Figure 17-5: Overview of switch back suppression



1. Four ports are attached. Frames are sent from port 1/1.
2. Port 1/1 is detached from the channel group because a failure occurs on the port. Also, the frame sending port is switched over to another port.
3. Three ports except port 1/1, which was detached, are attached. Frames are sent from port 4/1.
4. Port 1/1 recovers from the failure.
5. Port 1/1 is in the switch back suppression state. Frames are sent from port 4/1 (not changed).
6. Execute the `clear channel-group non-revertive` operation command to attach port 1/1 to the channel group. Also, the frame sending port is switched back to port 1/1.

(2) Switch back suppression delay time

Switch back suppression does not operate when a channel group changes from the down state to the up state because the ports added to that channel port are all attached. You can set the delay time from when a channel group comes up until when switch back suppression starts operating by using the `non-revertive` configuration command. Switch back suppression is disabled until the delay time expires.

(3) In the case of a failure during switch back suppression operation

If a port in the switch back suppression state exists when there is no more attached port, the port in the switch back suppression state is automatically attached.

(4) Switch back suppression settings

Switch back suppression operates when the LACP system priority of the Device is higher than that of the partner device. There is no need to set switch back suppression for the partner device.

(5) Operation in the case of link aggregation consisting of ports with different transmission speeds

When you add a port with higher transmission speed than any of the currently attached ports, the currently attached ports are detached. In addition, the newly added port is not attached because of switch back suppression. Thus, there is no attached port and the relevant channel group goes down. After that, when the newly added port is automatically attached as described in (3) *In the case of a failure during switch back suppression operation*, the channel group comes up.

To give priority to switch back suppression, use mixed-speed mode.

17.4 Configuration of the link aggregation extended functionality

17.4.1 List of configuration commands

The following table describes the configuration commands for the link aggregation extended functionality.

Table 17-7: List of configuration commands

Command name	Description
channel-group lacp system-priority	Sets the system priority for a channel group. The system priority is used to determine which device evaluates the aggregation condition for the port detachment restriction functionality.
channel-group max-active-port	Enables the standby link functionality, and sets the maximum number of active ports.
channel-group max-detach-port	Enables the port detachment restriction functionality.
channel-group multi-speed	Sets mixed-speed mode.
channel-group non-revertive	Enables switch back suppression for the channel group.
lacp port-priority	Sets the port priority. The port priority is used to select standby links.
lacp system-priority	Sets the default value for the system priority. The system priority is used to determine which device evaluates the aggregation condition for the port detachment restriction functionality.

17.4.2 Configuring the standby link functionality

Points to note

The standby link functionality is used to enable a channel group, and to set the maximum number of active ports in the channel group. In addition, either link-down mode or link-not-down mode can be set.

Standby ports are set on a port priority basis, whereby a port with a lower priority level is selected for a standby link earlier. Note that the smaller the port priority value, the higher its priority.

The standby link functionality is available only when static link aggregation is used.

Command examples

1. **(config)# interface port-channel 10**
Switches channel group 10 to configuration mode.
2. **(config-if)# channel-group max-active-port 3**
Enables the standby link functionality for channel group 10, and sets the maximum number of active ports in the channel group to 3. Channel group 10 operates in link-down mode.
3. **(config-if)# exit**
Returns to global configuration mode.
4. **(config)# interface port-channel 20**

```
(config-if)# channel-group max-active-port 1 no-link-down
(config-if)# exit
```

Changes the mode to configuration mode for channel group 20, enables the standby link functionality for the channel group, sets the maximum number of active ports to 1, and sets link-not-down mode.

5.

```
(config)# interface gigabitethernet 1/1
(config-if)# channel-group 20 mode on
(config-if)# lacp port-priority 300
```

Adds port 1/1 to channel group 20, and sets the port priority value to 300. Note that a smaller port priority value indicates a higher priority. Therefore, a port with the port priority value of 300, which is larger than the default value of 128, is selected for a standby link earlier than a port with the default priority.

17.4.3 Configuring the port detachment restriction functionality

Points to note

The port detachment restriction functionality is used to enable a channel group. For the command that enables this functionality, set the maximum number of ports that can be detached from a channel group. Specifying 15 is equivalent to disabling the functionality.

If the Device is to be connected to a device that supports the port detachment restriction functionality, make sure that the settings of the functionality on both devices match. If a Device is to be connected to a device that does not support this functionality, set a higher LACP system priority level on the Device. A smaller LACP system priority value indicates a higher priority.

The port detachment restriction functionality is available only when LACP link aggregation is used.

Command examples

1.

```
(config)# interface port-channel 10
```


Switches channel group 10 to configuration mode.
2.

```
(config-if)# channel-group max-detach-port 0
```


Enables the port detachment restriction functionality for channel group 10, and set the maximum number of ports that can be detached from the channel group to 0. If at least one port in the channel group becomes faulty, the entire channel group is assumed to be faulty.
3.

```
(config-if)# channel-group lacp system-priority 100
```


Sets 100 as the system priority for channel group 10.

17.4.4 Configuring mixed-speed mode

Points to note

The example below shows how to set mixed-speed mode for a channel group. In mixed-speed mode, the transmission speed is excluded from detachment conditions.

Command examples

1.

```
(config)# interface port-channel 10
```

Switches channel group 10 to configuration mode.

2. **(config-if)# channel-group multi-speed**

Sets mixed-speed mode for channel group 10.

17.4.5 Configuring the switch back suppression

Points to note

Enables switch back suppression for the channel group. If this functionality is set, when a port attached to a channel group recovers from a failure after being detached, automatic attachment of the port is suppressed.

Switch back suppression is available only when LACP link aggregation is used.

Command examples

1. **(config)# interface port-channel 10**

Switches channel group 10 to configuration mode.

2. **(config-if)# channel-group non-revertive**

Enables switch back suppression for channel group 10.

17.5 Operation for link aggregation

17.5.1 List of operation commands

The following table describes the operation commands for link aggregation.

Table 17-8: List of operation commands

Command name	Description
show channel-group	Shows link aggregation information.
show channel-group statistics	Shows link aggregation statistics.
clear channel-group statistics lacp	Clears the statistics for sent and received LACPDUs.
clear channel-group non-revertive	Clears the switch back suppression state for link aggregation.
restart lacp	Restarts the link aggregation program.
dump protocols lacp	Outputs to a file detailed event trace information and control table information collected for the link aggregation program.

17.5.2 Checking the link aggregation status

(1) Checking the connection status for link aggregation

When the `show channel-group` command is executed, information about link aggregation for a channel group is displayed. In the command execution result, `CH Status` indicates the connection status of the channel group. You can use the execution result to check whether the settings are correct.

The following figure shows the result of executing the `show channel-group` command.

Figure 17-6: Result of executing the `show channel-group` command

```
> show channel-group
Date 20XX/04/01 12:00:00 UTC
ChGr:1      Mode:LACP
  CH Status:Up      Elapsed Time:10:10:39      Bandwidth:3000000kbps
  Multi Speed:Off   Load Balance:frame
  Non Revertive:On
  Max Active Port:16
  Max Detach Port:15
  Description:4 ports aggregated.
  MAC address:0012.e2ac.8301
  Periodic Timer:Short
  Actor information
    System Priority:1      MAC:0012.e212.ff02      KEY:1
  Partner information
    System Priority:10000  MAC:0012.e2f0.69be      KEY:10
  Port(4)           :1/1-4
  Up Port(3)         :1/1-3
  Down Port(1)       :1/4
>
```

(2) Checking the operating status of each port

When the `show channel-group detail` command is executed, detailed status information of each port is displayed. In the command execution result, `Status` indicates the communication status of a port. For a port whose `Status` is `Down`, the reason is also indicated in `Reason`.

The following figure shows the result of executing the `show channel-group detail` command.

Figure 17-7: Result of executing the `show channel-group detail` command

```
> show channel-group detail
```

```

Date 20XX/04/01 12:00:00 UTC
ChGr:1      Mode:LACP
  CH Status:Up      Elapsed Time:10:10:39      Bandwidth:3000000kbps
  Multi Speed:Off   Load Balance:frame
  Non Revertive:On
  Max Active Port:16
  Max Detach Port:15
  Description:4 ports aggregated.
  MAC address:0012.e2ac.8301
  Periodic Timer:Short
  Actor information
    System Priority:1      MAC:0012.e212.ff02      KEY:1
  Partner information
    System Priority:10000  MAC:0012.e2f0.69be      KEY:10
  Port:1/1      Status:Up      Reason:-
    Speed:1G      Duplex:Full      LACP Activity:Active
    Actor Priority:128      Partner Priority:100
  Port:1/2      Status:Up      Reason:-
    Speed:1G      Duplex:Full      LACP Activity:Active
    Actor Priority:128      Partner Priority:100
  Port:1/3      Status:Up      Reason:-
    Speed:1G      Duplex:Full      LACP Activity:Active
    Actor Priority:128      Partner Priority:100
  Port:1/4      Status:Down      Reason:Non Revertive
    Speed:1G      Duplex:Full      LACP Activity:Active
    Actor Priority:128      Partner Priority:100
>

```

(3) Checking and clearing the switch back suppression state

Use the `clear channel-group non-revertive` command to clear the switch back suppression state. The following example shows how to check and clear the switch back suppression state.

1. By using the `show channel-group detail` command, confirm that port 1/4 is in the switch back suppression state.

```

> show channel-group detail
:
:
Port:1/4      Status:Down      Reason:Non Revertive
              Speed:1G      Duplex:Full      LACP Activity:Active
              Actor Priority:128      Partner Priority:100
:
:
>

```

2. By using the `clear channel-group non-revertive` command, clear the switch back suppression state of port 1/4.

```

> clear channel-group non-revertive port 1/4
Are you sure you want to make the channel-group revertive? (y/n) :y
>

```

3. By using the `show channel-group detail` command, confirm that port 1/4 is attached.

```

> show channel-group detail
:
:
Port:1/4      Status:Up      Reason:-
              Speed:1G      Duplex:Full      LACP Activity:Active
              Actor Priority:128      Partner Priority:100
:
:
>

```


Chapter

18. IP Interfaces

This chapter describes how to perform communication by setting an IP address to an interface.

- 18.1 Description
- 18.2 Configuration
- 18.3 Operation

18.1 Description

18.1.1 Overview

An interface to which an IPv4 or IPv6 address is set is called an IP interface. You can set either or both of these addresses to an interface.

The following table describes the types of interface to which an IP address can be set.

Table 18-1: Types of interface to which an IP address can be set

Interface type	Description
Ethernet interface	An IP address is directly set to an Ethernet interface. One port can be used as one interface.
Ethernet subinterface	The VLAN ID of a VLAN tag is set by assigning an index to an Ethernet interface. This setting enables that interface to be used as a different interface for each VLAN tag. An IP address is set to a subinterface.
Port channel interface	An IP address is directly set to a port channel interface. One channel group can be used as one interface.
Port channel subinterface	The VLAN ID of a VLAN tag is set by assigning an index to a port channel interface. This setting enables that interface to be used as a different interface for each VLAN tag. An IP address is set to a subinterface.
Management port	An interface that uses a twisted pair cable (UTP) for remote operation terminal connection. An IP address is set directly to this interface.
Serial connection port (AUX)	An interface that uses a serial port (AUX) for remote operation terminal connection. An IP address is set directly to this interface.
Loopback interface	A special interface that indicates the device itself. Set an IP address.
Null interface	A virtual interface for packet discarding that does not depend on any physical line. An IP address cannot be specified to this interface.

Note that an IP interface might be referred to simply as an interface in this manual.

18.1.2 Subinterface

A subinterface is a generic term for an Ethernet subinterface and port channel subinterface. A subinterface is expressed as the port number of the source Ethernet interface or the channel group number of the source port channel concatenated with a subinterface index (subinterface identification number) with a period (.) in between.

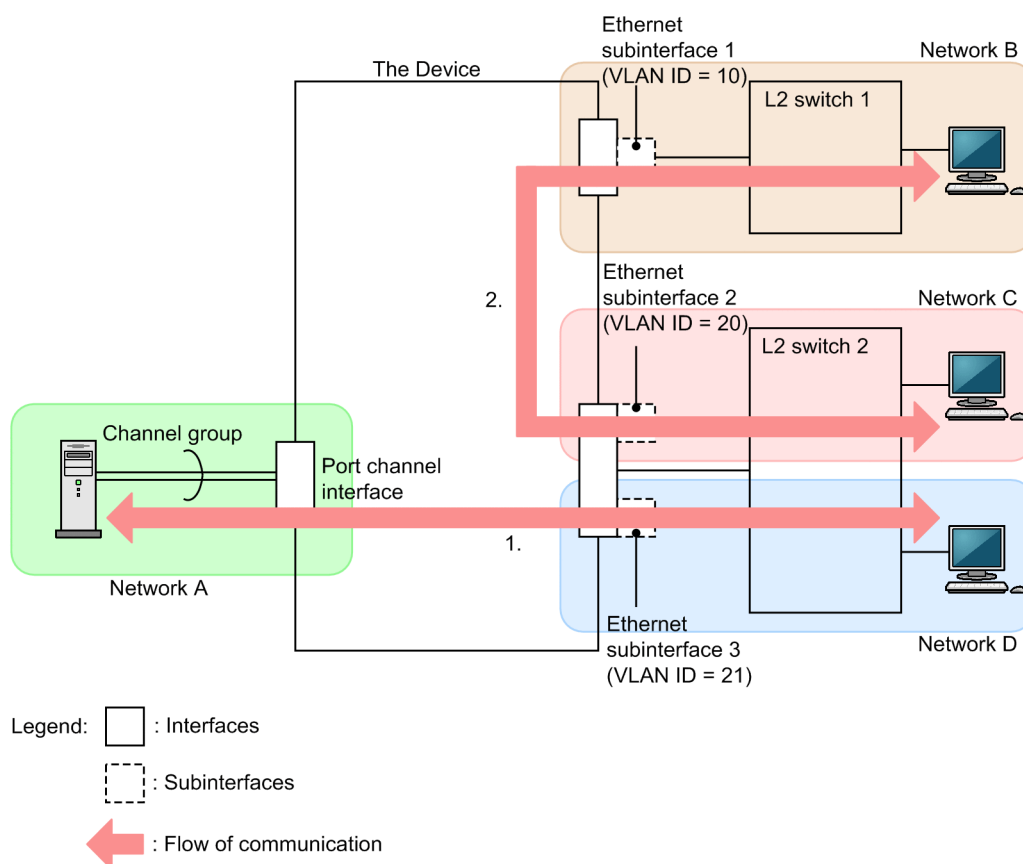
Example: 1/1.5

As a subinterface, you can set an interface using or not using a VLAN tag.

18.1.3 Example of a network configuration

The following figure shows an example of a network configuration that uses IP interfaces.

Figure 18-1: Example of a network configuration that uses IP interfaces



Settings on the Device:

- Connection to the server for network A
Sets up a port channel interface.
- Connection to L2 switch 1 for network B
Set up one subinterface for an Ethernet port and assign VLAN ID 10 to the subinterface.
- Connection to L2 switch 2 for network C and network D
Set up two subinterfaces for an Ethernet port and assign VLAN IDs 20 and 21 respectively to the subinterfaces.

Set up each of the above interfaces as an IP interface by assigning an IP address to it.

Communication details (The item numbers in the following list correspond to the numbers in the communication flow shown in the figure.)

1. Layer 3 forwarding between network A and network D (forwarding between different subnets)
The Device sends untagged frames to and receives them from the server for network A.
The Device sends tagged frames (VLAN ID=21) to and receives them from L2 switch 2 for network D.
2. Layer 3 forwarding between network B and network C (forwarding between different subnets)
The Device sends tagged frames (VLAN ID=10) to and receives them from L2 switch 1 for network B.

The Device sends tagged frames (VLAN ID=20) to and receives them from L2 switch 2 for network C.

18.1.4 Specifications for IP interface operation

(1) Supported specifications for IP interface

For an IP interface, the configuration commands that can be set and the values that can be applied by configurations are different depending on the interface type. The following table describes the correspondences between configurations and interface types.

Table 18-2: Correspondences between configurations and interface types

Command name	Interface type (for individual settings)			Description
	Ethernet interface	Port channel interface	Subinterface	
description	Y	Y	Y	You can set this command for each interface.
mtu (port)	Y	--	--	The maximum frame length for the port also applies to the port channel interface and subinterface each.
ip mtu	Y	Y	Y	If the <code>ip mtu</code> command is set, the maximum frame length set for individual ports is compared to the length parameter value in this command. The smaller of these values is applied as the IP MTU length for the relevant interface.
shutdown	Y	Y	Y	You can set this command for each interface.
snmp trap link-status	Y	--	Y	The default setting of a subinterface is not to send any trap or any inform.

Legend: Y: Supported, N: Not supported

Setting unit:

Ethernet interface: for individual ports

Port channel interface: for individual channel groups

Subinterface: for individual subinterfaces

(2) MAC address used for an IP interface

A device MAC address or management port MAC address is used for an IP interface. Which MAC address is used depends on the interface type. The following table describes the correspondence between IP interface types and MAC addresses.

Table 18-3: Correspondence between IP interface types and MAC addresses

IP interface type	MAC address to be used
Ethernet interface	Device MAC address
Ethernet subinterface	Device MAC address
Port channel interface	Device MAC address
Port channel subinterface	Device MAC address
Management port	Management port MAC address
Serial connection port (AUX)	--

IP interface type	MAC address to be used
Loopback interface	--
Null interface	--

Legend: --: No MAC address is used.

For details about a device MAC address, see *16.1.5 MAC address of the Device*.

(3) MTU used for an IP interface

For an IP interface, among the following items of information, the smallest value is used as the IP MTU value for an interface:

- *maximum-frame-length-common-to-all-ports-that-is-set-for-individual-devices* - 18
- *maximum-frame-length-set-for-individual-ports* - 18
- *IP-MTU-information-set-for-individual-interfaces*

The following table describes how the IP MTU value for an interface is determined.

Table 18-4: Determining the IP MTU value for an interface

Maximum frame length common to all ports	Maximum frame length for a port	IP MTU information	IP MTU value
Set	Set	Set	The smaller value obtained by comparing the following values: <ul style="list-style-type: none"> • <i>smallest-value-of-the-maximum-frame-length-for-a-port-among-the-ports-for-which-it-is-specified</i> - 18 • <i>set-value-of-the-IP-MTU-information</i>
Set	Not set	Set	The smaller value obtained by comparing the following values: <ul style="list-style-type: none"> • <i>maximum-frame-length-common-to-all-ports</i> - 18 • <i>set-value-of-the-IP-MTU-information</i>
Set	Set	Not set	The smaller value obtained by comparing the following values: <ul style="list-style-type: none"> • <i>smallest-value-of-the-maximum-frame-length-for-a-port-among-the-ports-for-which-it-is-specified</i> - 18 • 9216
Set	Not set	Not set	The smaller value obtained by comparing the following values: <ul style="list-style-type: none"> • <i>maximum-frame-length-common-to-all-ports</i> - 18 • 9216
Not set	Set	Set	The smaller value obtained by comparing the following values: <ul style="list-style-type: none"> • <i>smallest-value-of-the-maximum-frame-length-for-a-port-among-the-ports-for-which-it-is-specified</i> - 18 • <i>set-value-of-the-IP-MTU-information</i>
Not set	Not set	Set	The smaller value obtained by comparing the following values: <ul style="list-style-type: none"> • <i>set-value-of-the-IP-MTU-information</i> • 1500

Maximum frame length common to all ports	Maximum frame length for a port	IP MTU information	IP MTU value
Not set	Set	Not set	The smaller value obtained by comparing the following values: <ul style="list-style-type: none"> <i>smallest-value-of-the-maximum-frame-length-for-a-port-among-the-ports-for-which-it-is-specified</i> - 18 9216
Not set	Not set	Not set	1500

Note 1:

If the line type is 10BASE-T (full or half duplex) or 100BASE-TX (half duplex), the maximum IP MTU value is 1500 regardless of the settings.

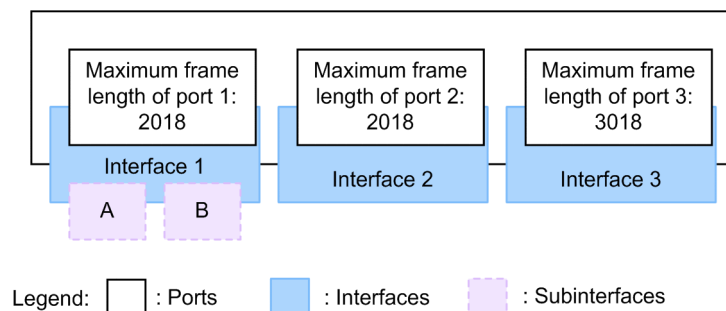
Note 2:

The maximum frame length is the maximum length of a frame in Ethernet V2 format excluding the FCS.

(a) IP MTU values for one-to-one correspondence between an interface and port

For an interface created by setting an IP address to an Ethernet interface or Ethernet subinterface, IP MTU values are determined as follows.

Figure 18-2: Example of IP MTU values for one-to-one correspondence between an interface and an port



■ IP MTU value for each interface when the IP MTU information is not set

Determined IP MTU values

Subinterface A: 2000

Subinterface B: 2000

Interface 2: 2000

Interface 3: 3000

■ IP MTU value for each interface when the IP MTU information is set

IP MTU length to be set

Subinterface A: 1000

Subinterface B: 3000

Interface 2: 2500

Interface 3: 2500

Determined IP MTU values

Subinterface A: 1000

Subinterface B: 2000

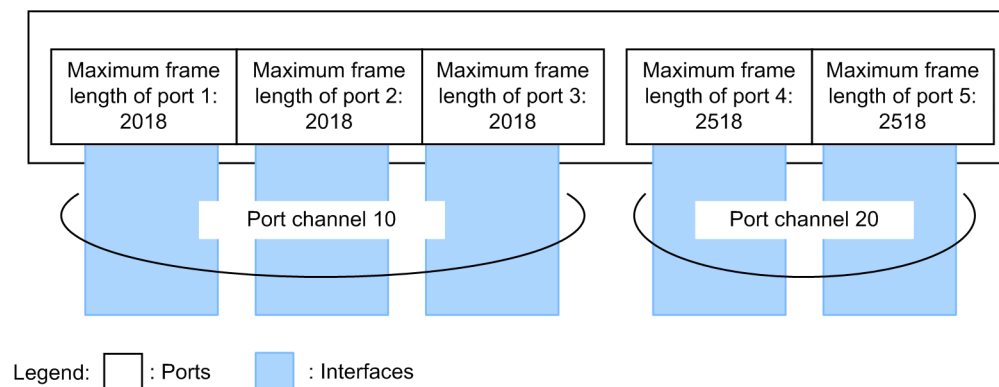
Interface 2: 2000

Interface 3: 2500

(b) IP MTU values for one-to-n correspondence between an interface and ports

The IP MTU values for an interface that multiple ports correspond to, like a port channel interface, are determined as follows.

Figure 18-3: Example of IP MTU values for port channel interfaces



■ IP MTU value for each interface when the IP MTU information is not set

Determined IP MTU values

Port channel 10: 2000

Port channel 20: 2500

■ IP MTU value for each interface when the IP MTU information is set

IP MTU length to be set

Port channel 10: 1000

Port channel 20: 3000

Determined IP MTU values

Port channel 10: 1000

Port channel 20: 2500

18.1.5 TPID value of VLAN tag

By using a configuration command, you can set any value for the TPID (Tag Protocol Identifier) of a VLAN tag used for subinterface communication. For the default value for the device, 0x8100 is used.

When a TPID value is set by a configuration command, during frame transmission or reception, a frame with any of the following TPID values is recognized as a frame with a VLAN tag.

During frame reception

Both the default TPID value and the TPID value set by a configuration command

User priority for frames to be sent

The TPID value set by a configuration command

18.2 Configuration

18.2.1 List of configuration commands

The following table describes the configuration commands for IP interfaces.

Table 18-5: List of configuration commands

Command name	Description
description	Sets supplementary information for a subinterface.
dot1q ethertype	Sets the TPID value of a VLAN tag which is assigned by a Device.
encapsulation dot1q	Sets the VLAN ID of a VLAN tag to a subinterface.
shutdown	Sets a subinterface as shut down.
snmp trap link-status	Controls transmission of a trap or an inform (linkDown and linkUp traps) when a subinterface comes up or goes down.
interface gigabitethernet ^{#1}	Sets a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X Ethernet interface or Ethernet subinterface.
interface hundredgigabitethernet ^{#1}	Sets a 100GBASE-R Ethernet interface or Ethernet subinterface.
interface tengigabitethernet ^{#1}	Sets a 10GBASE-R Ethernet interface or Ethernet subinterface.
interface port-channel ^{#2}	Sets a port channel interface or a port channel subinterface.
ip address ^{#3}	Sets an IPv4 address for an interface.

#1

See 14. *Ethernet* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

#2

See 15. *Link Aggregation* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

#3

See 2. *IPv4, ARP, and ICMP* in the manual *Configuration Command Reference Vol. 3 For Version 12.1*.

18.2.2 Configuring an IP interface

(1) Setting an Ethernet interface

Points to note

Set an IP address in configuration command mode for an Ethernet interface.

Command examples

1. **(config)# interface gigabitethernet 1/10**

Switches to configuration command mode for Ethernet interface 1/10.

2. **(config-if)# ip address 192.0.2.1 255.255.255.0**

Sets an IP address for Ethernet interface 1/10.

(2) Setting an Ethernet subinterface

Points to note

Set the VLAN ID and IP address of a VLAN tag in configuration command mode for an Ethernet subinterface.

Command examples

1. **(config-if)# interface gigabitethernet 1/10.5**

Switches to configuration command mode for Ethernet subinterface 1/10.5.

2. **(config-subif)# encapsulation dot1q 100**

Sets 100 for Ethernet subinterface 1/10.5 as the VLAN ID of the VLAN tag.

3. **(config-subif)# ip address 192.0.2.1 255.255.255.0**

Sets an IP address for Ethernet subinterface 1/10.5.

(3) Setting a port channel interface

Points to note

Set an IP address in configuration command mode for a port channel interface.

Command examples

1. **(config)# interface port-channel 10**

Switches to configuration command mode for port channel interface 10.

2. **(config-if)# ip address 192.0.2.1 255.255.255.0**

Sets an IP address for the port channel interface.

(4) Setting a port channel subinterface

Points to note

Set the VLAN ID and IP address of a VLAN tag in configuration command mode for a port channel subinterface.

Command examples

1. **(config)# interface port-channel 10.110**

Switches to configuration command mode for port channel subinterface 10.110.

2. **(config-subif)# encapsulation dot1q 100**

Sets 100 for port channel subinterface 10.110 as the VLAN ID of the VLAN tag.

3. **(config-subif)# ip address 192.0.2.1 255.255.255.0**

Sets an IP address for port channel subinterface 10.110.

18.2.3 Deleting an IP interface

(1) *Deleting an Ethernet interface*

Points to note

Delete the IP address from an Ethernet interface.

Command examples

1. **(config)# interface gigabitethernet 1/1**
Switches to configuration command mode for Ethernet interface 1/1.
2. **(config-if)# no ip address 192.0.2.1**
Deletes the IP address setting from Ethernet interface 1/1.

(2) *Deleting an Ethernet subinterface*

Points to note

To delete an Ethernet subinterface, delete the IP address and VLAN tag settings first, and then delete the Ethernet subinterface.

Command examples

1. **(config)# interface gigabitethernet 1/1.5**
Switches to configuration command mode for Ethernet subinterface 1/1.5.
2. **(config-subif)# no ip address 192.0.2.1**
Deletes the IP address setting from Ethernet subinterface 1/1.5.
3. **(config-subif)# no encapsulation dot1q**
(config-subif)# exit
Deletes the VLAN tag setting from Ethernet subinterface 1/1.5 and returns to global configuration mode.
4. **(config)# no interface gigabitethernet 1/1.5**
Deletes Ethernet subinterface 1/1.5.

(3) *Deleting a port channel interface*

Points to note

Delete the IP address from a port channel interface.

Command examples

1. **(config)# interface port-channel 10**
Switches to configuration command mode for port channel interface 10.
2. **(config-if)# no ip address 192.0.2.1**

Deletes the IP address setting from port channel interface 10.

(4) Deleting a port channel subinterface

Points to note

To delete a port channel subinterface, delete the IP address and VLAN tag settings first, and then delete the port channel subinterface.

Command examples

1. **(config)# interface port-channel 3.5**

Switches to configuration command mode for port channel subinterface 3.5.

2. **(config-subif)# no ip address 192.0.2.1**

Deletes the IP address setting from port channel subinterface 3.5.

3. **(config-subif)# no encapsulation dot1q**
(config-subif)# exit

Deletes the VLAN tag setting from port channel subinterface 3.5 and returns to global configuration mode.

4. **(config)# no interface port-channel 3.5**

Deletes port channel subinterface 3.5.

18.2.4 Shutting down a subinterface

Points to note

Like an Ethernet interface and port channel interface, a subinterface can be set as shut down. Shutdown is set for individual subinterfaces.

Command examples

1. **(config)# interface gigabitethernet 1/10.5**

Switches to configuration command mode for Ethernet subinterface 1/10.5.

2. **(config-subif)# shutdown**

Shuts down Ethernet subinterface 1/10.5.

3. **(config-subif)# *******

Sets a configuration for Ethernet interface 1/10.5.

4. **(config-subif)# no shutdown**

Releases Ethernet subinterface 1/10.5 from the shutdown status.

18.2.5 Configuring the TPID value of a VLAN tag

You can set any value for the TPID value of a VLAN tag to be used for a subinterface. Use the `dot1q ethertype` command to set the TPID value for the Device.

TPID values use the same position in a frame as an untagged frame EtherType. Because of this, it might not be possible to configure a network properly when a value used as an EtherType, for example 0x0800 (IPv4), is set. For the TPID value, set a value not used as an EtherType value.

Points to note

Set the TPID value for the Device as 0x9100. All ports operate with a VLAN tag of 0x9100.

Command examples

1. **(config)# dot1q ethertype 9100**

Sets the TPID value for the Device as 0x9100 in global configuration mode.

18.3 Operation

18.3.1 List of operation commands

The following table describes the operation commands for IP interfaces.

Table 18-6: List of operation commands

Command name	Description
show ip-dual interface ^{#1}	Shows the status and statistics of the IP interface to which IPv4 and IPv6 addresses are set.
show ip interface ^{#1}	Shows the status and statistics of the IP interface to which an IPv4 address is set.
clear ip interface statistics ^{#1}	Clears the statistics of the IP interface to which an IPv4 address is set.
show ipv6 interface ^{#2}	Shows the status and statistics of the IP interface to which an IPv6 address is set.
clear ipv6 interface statistics ^{#2}	Clears the statistics of the IP interface to which an IPv6 address is set.

#1

See 2. *IPv4, ARP, and ICMP* in the manual *Operation Command Reference Vol. 3 For Version 12.1*.

#2

See 3. *IPv6, NDP, and ICMPv6* in the manual *Operation Command Reference Vol. 3 For Version 12.1*.

18.3.2 Checking the status and statistics of the IP interface

You can check the status and statistics of the IP interface by using the `show ip-dual interface` command. The following figure shows the result of executing the `show ip-dual interface` command with an Ethernet subinterface specified.

Figure 18-4: Result of executing the show ip-dual interface command

```
>show ip-dual interface gigabitethernet 1/2.5 detail
Date 20XX/01/01 12:00:00 UTC
Eth1/2.5    VRF: 10
Status: UP,MULTICAST,BROADCAST
mtu: 1500    MAC address: 0012.e286.5300
IPv4: 192.0.2.1/24 broadcast 192.0.2.255  PRIMARY,SUBNETBROD
IPv4: 192.0.2.10/24 broadcast 192.0.2.255  VRRP
IPv6: 2001:db8:100::1/64
IPv6: fe80::212:e2ff:fe86:5300%Eth1/2.5/64
IPv4 uRPF: Strict Mode  VRRP: Enable    Multicast Routing: Disable
IPv6 uRPF: Strict Mode  VRRP: Disable    Multicast Routing: Disable
Time-since-last-status-change: 30,00:10:00
Last down at: 20XX/01/01 11:00:00 UTC
VLAN ID: 100
Description: subnetwork100
Detail status: Disable
[Out octets/packets counter]
  IPv4 Out All octets           :                20000
  IPv6 Out All octets           :                60000
  IPv4 Out All packets          :                 250
  IPv6 Out All packets          :                 750
  IPv4 Out Discards packets     :                 130
  IPv6 Out Discards packets     :                 290
  IPv4 Out Discards(BCU-CPU) packets:                 4
```

```

IPv6 Out Discards(BCU-CPU) packets:                6
[In octets/packets counter]
IPv4 In All octets                                   : 28000
IPv6 In All octets                                   : 36000
IPv4 In All packets                                  : 350
IPv6 In All packets                                  : 450
IPv4 In Error packets                                : 50
IPv6 In Error packets                                : 75
IPv4 In Discards packets                             : 15
IPv6 In Discards packets                             : 20
IPv4 In NoRoutes packets                             : 30
IPv6 In NoRoutes packets                             : 40
IPv4 In Error(BCU-CPU) packets                       : 25
IPv6 In Error(BCU-CPU) packets                       : 35
IPv4 In Discards(BCU-CPU) packets                   : 2
IPv6 In Discards(BCU-CPU) packets                   : 3

```

Appendix

- A. Relevant standards
- B. Acknowledgments

A. Relevant standards

A.1 TELNET/FTP

Table A-1: Relevant standards and recommendations for TELNET/FTP

Name (month and year issued)	Title
RFC 854 (May 1983)	TELNET PROTOCOL SPECIFICATION
RFC 855 (May 1983)	TELNET OPTION SPECIFICATIONS
RFC 959 (October 1985)	FILE TRANSFER PROTOCOL (FTP)

A.2 RADIUS or TACACS+

Table A-2: Relevant standards and recommendations for RADIUS and TACACS+

Name (month and year issued)	Title
RFC 2865 (June 2000)	Remote Authentication Dial In User Service(RADIUS)
RFC 2866 (June 2000)	RADIUS Accounting
RFC 3162 (August 2001)	RADIUS and IPv6
draft-grant-tacacs-02 (January 1997)	The TACACS+ Protocol Version 1.78

A.3 NTP

Table A-3: Relevant standard and recommendation for NTP

Name (month and year issued)	Title
RFC 1305 (March 1992)	Network Time Protocol (Version 3) Specification, Implementation and Analysis

A.4 SNTP

Table A-4: Relevant standard and recommendation for SNTP

Name (month and year issued)	Title
RFC 5905 (June 2010)	Network Time Protocol Version 4: Protocol and Algorithms Specification

A.5 DNS

Table A-5: Relevant standards and recommendations for DNS resolver

Name (month and year issued)	Title
RFC 1034 (March 1987)	Domain names - concepts and facilities
RFC 1035 (March 1987)	Domain names - implementation and specification

A.6 SYSLOG

Table A-6: Relevant standards and recommendations for SYSLOG

Name (month and year issued)	Title
RFC 3164 (August 2001)	The BSD syslog Protocol
RFC 5424 (March 2009)	The Syslog Protocol

A.7 SNMP

Table A-7: Relevant standards and recommendations for SNMP

Name (month and year issued)	Title
RFC 1155 (May 1990)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157 (May 1990)	A Simple Network Management Protocol (SNMP)
RFC 1901 (January 1996)	Introduction to Community-based SNMPv2
RFC 1902 (January 1996)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1903 (January 1996)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904 (January 1996)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905 (January 1996)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906 (January 1996)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1907 (January 1996)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908 (January 1996)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 2578 (April 1999)	Structure of Management Information Version 2 (SMIv2)
RFC 2579 (April 1999)	Textual Conventions for SMIv2
RFC 2580 (April 1999)	Conformance Statements for SMIv2
RFC 3410 (December 2002)	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411 (December 2002)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 (December 2002)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 (December 2002)	Simple Network Management Protocol (SNMP) Applications
RFC 3414 (December 2002)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415 (December 2002)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3416 (December 2002)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

Name (month and year issued)	Title
RFC 3417 (December 2002)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3584 (August 2003)	Coexistence between Version 1, Version 2, and Version 3 of the Internet- standard Network Management Framework

Table A-8: Relevant standards and recommendations for MIBs

Name (month and year issued)	Title
IEEE 8023-LAG-MIB (March 2000)	Aggregation of Multiple Link Segments
RFC 1158 (May 1990)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1213 (March 1991)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1215 (March 1991)	A Convention for Defining Traps for use with the SNMP
RFC 1354 (July 1992)	IP Forwarding Table MIB
RFC 1643 (July 1994)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 1657 (July 1994)	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
RFC 2452 (December 1998)	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC 2454 (December 1998)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC 2465 (December 1998)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466 (December 1998)	Management Information Base for IP Version 6: ICMPv6 Group
RFC 2787 (March 2000)	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 2819 (May 2000)	Remote Network Monitoring Management Information Base
RFC 2863 (June 2000)	The Interfaces Group MIB
RFC 2934 (October 2000)	Protocol Independent Multicast MIB for IPv4
RFC 3411 (December 2002)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 (December 2002)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 (December 2002)	Simple Network Management Protocol (SNMP) Applications
RFC 3414 (December 2002)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415 (December 2002)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418 (December 2002)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

Name (month and year issued)	Title
RFC 3635 (September 2003)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 4022 (March 2005)	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113 (June 2005)	Management Information Base for the User Datagram Protocol (UDP)
RFC 4293 (April 2006)	Management Information Base for the Internet Protocol (IP)
RFC 4750 (December 2006)	OSPF Version 2 Management Information Base
RFC 5643 (August 2009)	Management Information Base for OSPFv3
draft-ietf-vrrp-unified-mib-04 (September 2005)	Definitions of Managed Objects for the VRRP over IPv4 and IPv6

A.8 Ethernet

Table A-9: Relevant standards for Ethernet interfaces

Type	Standards	Model name
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, 10GBASE-R, 100GBASE-R	IEEE Std 802.3x-1997	Specification for 802.3x Full Duplex Operation
	IEEE Std 802.3 2008 Edition	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications
100GBASE-R	IEEE Std 802.3ba 2010	Media Access Control (MAC) Parameters, Physical Layer, and Management Parameters for 40Gb/s and 100Gb/s Operation

A.9 Link aggregation

Table A-10: Relevant standard for link aggregation

Standards	Model name
IEEE 802.1AX (IEEE Std 802.1AX-2008)	Aggregation of Multiple Link Segments

A.10 VLAN

Table A-11: Relevant standard and recommendation for VLANs

Standards	Model name
IEEE 802.1Q (IEEE Std 802.1Q-2003)	Virtual Bridged Local Area Networks [#]

[#]: GVRP/GMRP is not supported.

B. Acknowledgments

This product includes software developed at the Information Technology Division, US Naval Research Laboratory.

This product includes software developed by Adam Glass and Charles M. Hannum.

This product includes software developed by Adam Glass.

This product includes software developed by Berkeley Software Design, Inc.

This product includes software developed by Brini.

This product includes software developed by Bruce M. Simpson.

This product includes software developed by Charles D. Cranor and Washington University.

This product includes software developed by Charles D. Cranor, Washington University, the University of California, Berkeley and its contributors.

This product includes software developed by Charles M. Hannum.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Christopher G. Demetriou.

This product includes software developed by Christos Zoulas.

This product includes software developed by Chuck Silvers.

This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>).

This product includes software developed by Darrin B. Jewell

This product includes software developed by Eduardo Horvath.

This product includes software developed by Emmanuel Dreyfus

This product includes software developed by Frank van der Linden for the NetBSD Project.

This product includes software developed by Gordon W. Ross

This product includes software developed by Gordon W. Ross and Leo Weppelman.

This product includes software developed by Internet Initiative Japan Inc.

This product includes software developed by Jason L. Wright

This product includes software developed by Jason R. Thope for And Communications, <http://www.and.com/>

This product includes software developed by John Polstra.

This product includes software developed by Jonathan Stone and Jason R. Thorpe for the NetBSD Project.

This product includes software developed by Jonathan Stone for the NetBSD Project.

This product includes software developed by Kenneth Stailey.

This product includes software developed by Leo Weppelman.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Mats O Jansson.

This product includes software developed by Michael Graff.

This product includes software developed by Michael Shalayeff.

This product includes software developed by Niels Provos.

This product includes software developed by Paul Mackerras <paulus@samba.org>.

This product includes software developed by Pedro Roque Marques <pedro_m@yahoo.com>

This product includes software developed by Rolf Grossmann.

This product includes software developed by Ross Harvey for the NetBSD Project.

This product includes software developed by Softweyr LLC, the University of California, Berkeley, and its contributors.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by TooLs GmbH.

This product includes software developed by WIDE Project and its contributors.

This product includes software developed by Winning Strategies, Inc.

This product includes software developed by Yen Yen Lim and North Dakota State University

This product includes software developed by Zembu Labs, Inc.

This product includes software developed by the Alice Group.

This product includes software developed by the Charles D. Cranor, Washington University, University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the SMCC Technology Development Group at Sun Microsystems, Inc.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratories.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed for the NetBSD Project by Perry E. Metzger.

This product includes software developed for the NetBSD Project by Frank van der Linden

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed for the NetBSD Project by Wasabi Systems, Inc.

This product includes software developed for the NetBSD Project. See <http://www.NetBSD.org/> for information about NetBSD.

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Index

Numerics

1000BASE-X [connection interface] 284
1000BASE-X connection specifications 285
100GBASE-R [connection interface] 292
100GBASE-R connection specifications 292
10BASE-T, 100BASE-TX, and 1000BASE-T connection specifications 274
10GBASE-R [connection interface] 289
10GBASE-R connection specifications 289

A

absolute method [MIB monitoring] 250
alarm group 250
assigning an IP address to the Device [the Device] 96
AUTO-MDI/MDI-X 280
auto-negotiation [1000BASE-X] 285
auto-negotiation [10BASE-T, 100BASE-TX, and 1000BASE-T] 277
automatic recognition (auto-negotiation) of 10BASE-T, 100BASE-TX, and 1000BASE-T 274

C

capacity limit 13
checking communication between a remote operation terminal and the Device 100
CLI environment information 51
command operations 45
conditions for discarding received frames 265
configuration 55
configuration commands common to all Ethernet interfaces 268
configuration commands for checking the device 180
configuration commands for configuration setting, editing, and operation 60
configuration commands for host names and the DNS 159
configuration commands for IP interfaces 320
configuration commands for login security 102
configuration commands for managing SFUs, PRUs, and NIFs 190
configuration commands for NTP 150
configuration commands for PS (power supply unit) redundancy 221
configuration commands for RADIUS, TACACS+, and accounting 137
configuration commands for SNMP and RMON 252
configuration commands for SNTTP 153
configuration commands for system message output and log management 227
configuration commands for the device resource setting 179

configuration commands for the link aggregation basic functionality 300
configuration commands for the link aggregation extended functionality 308
configuration commands for the management port 94
configuration commands for time settings 147
configuration commands relating to connection and remote operation for an operation terminal 94
configuring and changing a login user's password 104
configuring and changing a password for switching to administrator mode 105
configuring MIB accesses in SNMPv3 253
configuring the IP addresses of remote operation terminals permitted to log in 107
configuring the maximum number of concurrent users 106
connection interface [1000BASE-X] 284
connection interface [100GBASE-R] 292
connection interface [10BASE-T, 100BASE-TX, and 1000BASE-T] 274
connection interface [10GBASE-R] 289
connection specifications for transmission speed and duplex mode (full or half) [1000BASE-X] 285
connection specifications for transmission speed and duplex mode (full or half) [10BASE-T, 100BASE-TX, and 1000BASE-T] 275
console connections 38
creating and deleting a login user 103
customizing CLI settings 51

D

delta method [MIB monitoring] 250
description of RADIUS and TACACS+ 113
device configuration 7
device management 161
device redundancy 207

E

error status codes 244
error status codes for SNMP operations 243
Ethernet 263
event group 251
example for MIB requests from IPv4 and IPv6 SNMP managers and the responses 235
example of a trap 235
example of MIB retrieval 234
expressing MIB objects 238

F

flow control [1000BASE-X] 285
flow control [100GBASE-R] 292

flow control [10BASE-T, 100BASE-TX, and 1000BASE-T] 277
 flow control [10GBASE-R] 289
 flow control for receiving on the device [10BASE-T, 100BASE-TX, and 1000BASE-T] 277
 flow control for receiving on the device [10GBASE-R] 290
 flow control for sending on the device [10BASE-T, 100BASE-TX, and 1000BASE-T] 277
 flow control for sending on the device [10GBASE-R] 289
 frame formats [MAC sublayer control] 265

G

GetBulkRequest operation 240
 GetNextRequest operation 239
 GetRequest operation 239

H

handling of padding 266
 history group 250
 host names and DNS 157

I

index 238
 inform 249
 inform request format 249
 informs 249
 IP addresses used for SNMP 250
 IP interfaces 313

J

jumbo frame [1000BASE-X] 285
 jumbo frame [100GBASE-R] 292
 jumbo frame [10BASE-T, 100BASE-TX, and 1000BASE-T] 280
 jumbo frame [10GBASE-R] 290
 jumbo frame support status [1000BASE-X] 285
 jumbo frame support status [10BASE-T, 100BASE-TX, and 1000BASE-T] 280
 jumbo frame support status [10GBASE-R] 290

L

link aggregation 295
 login security and RADIUS or TACACS+ 101

M

MAC sublayer frame format 265
 managing SFU, PRU, and NIF 190
 MDI and MDI-X pin mappings 280
 meanings of the TYPE/LENGTH field 265
 MIB overview 237
 MIBs supported by the Device 238

N

Network management 234

notes on a 1000BASE-X connection 286
 notes on a 100GBASE-R connection 292
 notes on a 10BASE-T, 100BASE-TX, or 1000BASE-T connection 281
 notes on a 10GBASE-R connection 290
 notes on connecting to an SNMP manager 251

O

operation commands common to all Ethernet interfaces 273
 operation commands for backup and restore operations 194
 operation commands for checking the device 180
 operation commands for input mode transitions and utilities 46
 operation commands for IP interfaces 325
 operation commands for link aggregation 311
 operation commands for login security 102
 operation commands for managing SFUs, PRUs, and NIFs 190
 operation commands for PS (power supply unit) redundancy 222
 operation commands for SFU redundancy 216
 operation commands for SNMP and RMON 260
 operation commands for software management 203
 operation commands for system message output and log management 231
 operation commands for the BCU duplex configuration 212
 operation commands for the device resource setting 179
 operation commands for the management port 99
 operation commands for time settings 147
 operation commands for time settings, NTP, and SNTP 155
 operation commands relating to configuration editing and operation 61
 operation commands relating to connection and remote operation for an operation terminal 99
 operation log 226
 operation of a community 243
 operational restrictions applying to communities 243
 operational restrictions applying to IP addresses 243
 operational restrictions applying to SNMPv3 247
 outputting messages 226
 overview of informs 249
 overview of login control 103
 overview of RADIUS and TACACS+ 113
 overview of SNMP 234
 overview of the Device 1
 overview of traps 247

P

private MIB 237

R

RADIUS 113
 remote login 89
 remote operation terminal 40
 remote operation terminal connections 38

response when a MIB cannot be configured 241
RMON MIB 250

S

scope of RADIUS or TACACS+ implementation 113
scope of RADIUS support 114
sequence of authentication (with end-by-reject specified)
120
sequence of authentication (without end-by-reject specified)
120
SetRequest operation 241
SNMP 233
SNMP agent 234
SNMP engine 236
SNMP entity 236
SNMPv1 and SNMPv2C operations 239
SNMPv3 operation 244
software management 199
standard MIB 237
starting the Device and logging in 37
startup messages 162
statistics group 250
statistics log 226
storing logs 226
structure of a MIB 237
system message output and log management 225
system operation panel 162

T

TACACS+ 113
template 73
template mode 74
template parameters 73
time settings, NTP, and SNTP 145
trap 247
Trap format (SNMPv1) 248
Trap format (SNMPv2C and SNMPv3) 248
traps 247

U

user authentication and privacy functionality 236