AX8600R Software Manual

Configuration Command Reference Vol. 1

For Version 12.1

AX86R-S004X

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-S004X

■ Copyright

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.

  - Capacity limits
  - Basic operations (e.g. logging in)
  - Ethernet
  - Filters and QoS
  - Network management
  - 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
VRRP	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

Chapter 1. Reading the Manual

Command description format
Command mode list
Specifiable values for parameters

Command description format

Each command is described in the following format:

Function

Describes the purpose of the command.

Syntax

Defines the input format of the command. The format is governed by the following rules:

1. Parameters for setting values or character strings are enclosed in angle brackets (<>).
2. Characters that are not enclosed in angle brackets (<>) are keywords that must be typed exactly as they appear.
3. {A|B} indicates that either A or B must be selected.
4. Parameters or keywords enclosed in square brackets ([]) are optional and can be omitted.
5. For details on the parameter input format, see *Specifiable values for parameters*.

Input mode

Indicates the mode required to enter the command. The name of a sub-mode of a configuration command mode corresponds to the name displayed on the command prompt.

Parameters

Describes in detail the parameters that can be set by the command. The default value and the values that can be specified for each parameter are described.

Default behavior

If there are default values for parameters, or a default behavior when a command is not entered, related information is provided here.

Impact on communication

If a setting has an impact on communication, such as interruptions to communication, that impact is described here.

When the change is applied

Describes whether set commands reflected in the running configuration are immediately effective, or whether they take effect only after temporarily stopping operation, such as by restarting the device.

Notes

Provides cautionary information on using the command.

Related commands

Describes the commands that must be set in order to use the applicable command.

Command mode list

The following table lists the command modes.

Table 1-1: Command mode list

No.	Prompt displayed for the command mode	Description	Command for mode transition
1	(config)	Global configuration mode	# configure
2	(config-line)	Configures remote login and console.	(config)# line vty (config)# line console
3	(config-view)	Configures view.	(config)# parser view
4	(config-if)	Configures a management port.	(config)# interface mgmt
		Configures an AUX port.	(config)# interface async
		Configures an Ethernet interface.	(config)# interface gigabitethernet (config)# interface tengigabitethernet (config)# interface hundredgigabitethernet
		Configures a port channel interface.	(config)# interface port-channel
		Configures a loopback interface.	(config)# interface loopback
		Configures a null interface.	(config)# interface null
5	(config-if-range)	Configures multiple Ethernet interfaces.	(config)# interface range gigabitethernet (config)# interface range tengigabitethernet (config)# interface range hundredgigabitethernet
		Configures multiple port channel interfaces.	(config)# interface range port-channel
6	(config-subif)	Configures an Ethernet subinterface.	(config)# interface gigabitethernet (config)# interface tengigabitethernet (config)# interface hundredgigabitethernet (When specified in the subinterface index)
		Configures a port channel subinterface.	(config)# interface port-channel (When specified in the subinterface index)
7	(config-subif-range)	Configures multiple Ethernet subinterfaces.	(config)# interface range gigabitethernet (config)# interface range tengigabitethernet (config)# interface range hundredgigabitethernet (When specified in the subinterface index)
		Configures multiple port channel subinterfaces.	(config)# interface range port-channel (When specified in the subinterface index)
8	(config-adv-acl)	Configures an Advance filter.	(config)# advance access-list
9	(config-ext-nacl)	Configures an IPv4 packet filter.	(config)# ip access-list extended
10	(config-std-nacl)	Configures an IPv4 address filter.	(config)# ip access-list standard
11	(config-ipv6-acl)	Configures an IPv6 filter.	(config)# ipv6 access-list
12	(config-ext-macl)	Configures a MAC filter.	(config)# mac access-list extended

No.	Prompt displayed for the command mode	Description	Command for mode transition
13	(config-adv-qos)	Configures Advance QoS flow.	(config)# advance qos-flow-list
14	(config-ip-qos)	Configures IPv4 QoS flow.	(config)# ip qos-flow-list
15	(config-ipv6-qos)	Configures IPv6 QoS flow.	(config)# ipv6 qos-flow-list
16	(config-mac-qos)	Configures MAC QoS flow.	(config)# mac qos-flow-list
17	(config-msg-list)	Configures message type output conditions.	(config)# message-list <*group name*>
18	(config-ip-pbr)	Configures IPv4 policy-based routing.	(config)# ip policy-list
19	(config-ipv6-pbr)	Configures IPv6 policy-based routing.	(config)# ipv6 policy-list
20	(config-router)	Configures RIP.	(config)# router rip
		Configures OSPF.	(config)# router ospf
		Configures BGP4/BGP4+.	(config)# router bgp
21	(config-router-af)	Configures RIP for each VRF.	(config)# router rip (config-router)# address-family ipv4 vrf
		Configures BGP4 for each VRF. (config-router-af) (ipv4 vrf) mode	(config)# router bgp (config-router)# address-family ipv4 vrf
		Configures BGP4+ global network. (config-router-af) (ipv6) mode	(config)# router bgp (config-router)# address-family ipv6
		Configures BGP4+ for each VRF. (config-router-af) (ipv6 vrf) mode	(config)# router bgp (config-router)# address-family ipv6 vrf
22	(config-route-map)	Configures route-map.	(config)# route-map
23	(config-rtr-rip)	Configures RIPng.	(config)# ipv6 router rip
24	(config-rtr)	Configures OSPFv3.	(config)# ipv6 router ospf
25	(config-vrf)	Configures config-vrf.	(config)# vrf definition
26	(<*Command mode*>-TPL)	Configures the template. template mode <*Command mode*>: Optional command mode	(config)# template
27	(<*Command mode*>-TPL-INS)	Configures the insert position command. insert mode <*Command mode*>: Optional command mode	(<*Command mode*>-TPL)# insert
28	(<*Command mode*>-TPL-REP)	Configures the replace position command. replace mode <*Command mode*>: Optional command mode	(<*Command mode*>-TPL)# replace

Specifiable values for parameters

The following table describes the values that can be specified for parameters.

Table 1-2: Specifiable values for parameters

Parameter type	Description	Input example
Name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for the second and subsequent characters.	neighbor office1 peer-group
Host name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and periods (.) can be used for the second and subsequent characters.	ip host telnet-host 192.168.1.1
Access list name, QoS flow list name, policer entry name, Name of policy-based routing list, QoS queue list name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for the second and subsequent characters.	ip access-list standard inbound1 ip access-list standard 10
Template name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and underscores (_) can be used for the second and subsequent characters.	template tmpl-01-01
Template parameter	Alphanumeric characters, hyphens (-), and underscores (_) can be used.	template tmpl $param-01-01
IPv4 address, Subnet mask	Specify these items in decimal format, separating 1-byte decimal values by a period (.).	192.168.0.14 255.255.255.0
Wildcard mask	The same input format as IPv4 addresses. The set bits in an IPv4 address represent an arbitrary value.	255.255.0.0
IPv6 address	Specify this item in hexadecimal format, separating 2-byte hexadecimal values by colons (:).	2001:db8:1234:5678:9abc:def0:1234:5678 fe80::1
add/remove specification	Add to or delete from the information when multiple interfaces have been specified. The add specification adds information to the current information. The remove specification deletes information from the current information.	monitor session 1 source interface add gigabitethernet 1/1 monitor session 1 source interface remove gigabitethernet 1/1

Any character string

Alphanumeric characters and special characters can be specified for parameters. Some special characters, however, cannot be used. Character codes are listed in the following table. Characters other than alphanumeric characters in the following list of character codes are special characters.

Table 1-3: List of character codes

Character	Code	Character	Code	Character	Code	Character	Code	Character	Code	Character	Code
Space	0x20	0	0x30	@	0x40	P	0x50	`	0x60	p	0x70
!	0x21	1	0x31	A	0x41	Q	0x51	a	0x61	q	0x71
"	0x22	2	0x32	B	0x42	R	0x52	b	0x62	r	0x72
#	0x23	3	0x33	C	0x43	S	0x53	c	0x63	s	0x73
$	0x24	4	0x34	D	0x44	T	0x54	d	0x64	t	0x74
%	0x25	5	0x35	E	0x45	U	0x55	e	0x65	u	0x75
&	0x26	6	0x36	F	0x46	V	0x56	f	0x66	v	0x76
'	0x27	7	0x37	G	0x47	W	0x57	g	0x67	w	0x77
(	0x28	8	0x38	H	0x48	X	0x58	h	0x68	x	0x78
)	0x29	9	0x39	I	0x49	Y	0x59	i	0x69	y	0x79
*	0x2A	:	0x3A	J	0x4A	Z	0x5A	j	0x6A	z	0x7A
+	0x2B	;	0x3B	K	0x4B	[	0x5B	k	0x6B	{	0x7B
,	0x2C	<	0x3C	L	0x4C	\	0x5C	l	0x6C	|	0x7C
-	0x2D	=	0x3D	M	0x4D	]	0x5D	m	0x6D	}	0x7D
.	0x2E	>	0x3E	N	0x4E	^	0x5E	n	0x6E	~	0x7E
/	0x2F	?	0x3F	O	0x4F	_	0x5F	o	0x6F	---	---

Notes

- To enter a question mark (?, or 0x3F), press **Ctrl** + **V**, and then type a question mark. You cannot copy and paste any specification string that includes a question mark.

Special characters that cannot be specified

Table 1-4: Special characters that cannot be specified

Character name	Character	Code
Double quotation mark	"	0x22
Dollar sign	$	0x24
Single quotation mark	'	0x27

Character name	Character	Code
Semicolon	;	0x3B
Backslash	\	0x5C
Grave accent mark	`	0x60
Left curly bracket	{	0x7B
Right curly bracket	}	0x7D

Example of specification string

access-list 10 remark "mail:xx@xx %tokyo"

How to specify an interface

The following table describes how to specify the parameters <*interface type*> and <*interface number*> that correspond to the interface type group.

Table 1-5: How to specify an interface

Interface type group	Interface name specified for <*interface type*>	Interface number specified for <*interface number*>
Ethernet interface	gigabitethernet	<*nif no.*>/<*port no.*>
	tengigabitethernet	<*nif no.*>/<*port no.*>
	hundredgigabitethernet	<*nif no.*>/<*port no.*>
Ethernet subinterface	gigabitethernet	<*nif no.*>/<*port no.*>.<*subinterface index*>
	tengigabitethernet	<*nif no.*>/<*port no.*>.<*subinterface index*>
	hundredgigabitethernet	<*nif no.*>/<*port no.*>.<*subinterface index*>
Port channel interface	port-channel	<*channel group number*>
Port channel subinterface	port-channel	<*channel group number*>.<*subinterface index*>
Loopback interface	loopback	0 or <*loopback id*>
Null interface	null	0
Management port	mgmt	0
AUX port	async	1

Specification of multiple interfaces

Use this method to specify the same information for multiple interfaces at the same time. You can specify the interface names and interface numbers that correspond to the following interface type groups from among the groups shown in *Table 1-5: How to specify an interface*.

- Ethernet interface
- Ethernet subinterface
- Port channel interface
- Port channel subinterface

When specifying multiple interfaces, you can specify interfaces that belong to the same interface type group at the same time, but you cannot specify interfaces that belong to different interface groups at the same time.

Syntax

```
interface range <interface type> <interface number>
```

You can specify no more than 16 input formats, separating each by a comma (,).

Input example

```
interface range gigabitethernet 1/1-3
interface range gigabitethernet 1/1-3, tengigabitethernet 3/1
interface range port-channel 2.10-20, port-channel 3.100, port-channel 5.200
```

Range of <sfu no.> values

The following table lists the range of <*sfu no.*> values.

Table 1-6: Range of <sfu no.> values

No.	Model	Range of values
1	All models	1 to 4

Range of <pru no.> values

The following table lists the range of <*pru no.*> values.

Table 1-7: Range of <pru no.> values

No.	Model	Range of values
1	AX8616R	1 to 4
2	AX8632R	1 to 8

Range of <nif no.> and <port no.> values

The following table lists the range of <*nif no.*> values.

Table 1-8: Range of <nif no.> values

No.	Model	Range of values
1	AX8616R	1 to 16
2	AX8632R	1 to 32

The following tables list the range of <*port no.*> values for each NIF.

Table 1-9: Range of <port no.> values

No.	NIF name	Range of values
1	NL1G-12T	1 to 12
2	NL1G-12S	1 to 12
3	NLXG-6RS	1 to 6
4	NMCG-1C	1

Range of values that can be set for <channel group number>

The following table lists the range of <*channel group number*> values.

Table 1-10: Range of <channel group number> values

No.	Model	Range of values
1	AX8616R	1 to 192

No.	Model	Range of values
2	AX8632R	1 to 384

Range of <subinterface index> values

The range of <*subinterface index*> values is from 1 to 65535.

Range of values that can be set for <vlan id>

The following table lists the range of <*vlan id*> values.

Table 1-11: Range of <vlan id> values

No.	Range of values
1	1 to 4095

How to specify <interface id list> and the range of specifiable values

In <*interface id list*>, you can specify several interfaces of the following Ethernet types by using hyphens (-) and commas (,). You can also specify a single interface by omitting what is inside the brackets [ ]. The range of permitted values is the same as the range of <*nif no.*> and <*port no.*> values in the above tables.

- For gigabit Ethernet interfaces

  gigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>]
- For 10 gigabit Ethernet interfaces

  tengigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>]
- For 100 gigabit Ethernet interfaces

  hundredgigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>]

Example of a range specification that uses a hyphen (-) and comma (,):

gigabitethernet 1/1-2,gigabitethernet 1/5,tengigabitethernet 3/1

Range of values that can be set for <vrf id>

The following table lists the range of <*vrf id*> values.

Table 1-12: Range of <vrf id> values

No.	Range of values
1	1 to 1024

Specifiable values for <message type>

The following table lists the values that can be specified for <*message type*>.

Table 1-13: Range of <message type> values

No.	Specifiable values
1	BCU
2	SFU
3	PRU
4	NIF
5	PS

No.	Specifiable values
6	FAN
7	KEY
8	CONFIGERR
9	CMDRSP
10	SOFTWARE
11	CONFIG
12	ACCESS
13	NTP
14	SOP-KEY
15	SOP-RSP
16	SNMP
17	PORT
18	ChGr
19	CFM
20	IP
21	PBR
22	DHCP
23	VRRP
24	RIP
25	RIPng
26	OSPF
27	OSPFv3
28	BGP4
29	BGP4+
30	UNICAST
31	PIM-IPv4
32	IGMP
33	PIM-IPv6
34	MLD
35	MULTI-IPv4
36	MULTI-IPv6
37	MULTI-INFO

Chapter 2. Operation Terminal Connection

ftp-server
line console
line vty
speed
transport input

ftp-server

Permits access from remote operation terminals by using FTP. To permit or deny a remote operation terminal's access to the Device, enter `config-line` mode, create a common access list that is used to restrict both Telnet and FTP access, and specify the IPv4 or IPv6 address of the remote operation terminal in the access list.

Syntax

To set information:

```
ftp-server
ftp-server vrf {<vrf id> | all}
```

To delete information:

```
no ftp-server
no ftp-server vrf {<vrf id> | all}
```

Input mode

```
(config)
```

Parameters

vrf {<*vrf id*> | all}

<*vrf id*>

Accepts access from the specified VRF. The global network is excluded.

If you want to specify an individual VRF for access, you can set up to four entries per device.

all

Accepts access from all VRFs including the global network.

1. Default value when this parameter is omitted:

   Accepts access from the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

Default behavior

Does not allow remote FTP access.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `config-line` mode is used to specify an access list for the Device, the access list can be used to control (permit or deny) FTP log-in access to the Device from remote operation terminals whose IPv4 or IPv6 addresses are specified in the access list.
2. If the `vrf all` parameter is specified, an individual global network or VRF cannot be specified.
3. If you specify an individual VRF that is allowed to access the Device, a total of up to four

VRF IDs can be specified by using this command and the `transport input` command.

Related commands

`line vty`
`ip access-group`
`ipv6 access-class`
`transport input`

line console

Entering this command changes the mode to `config-line` mode, which permits settings related to the specified CONSOLE (RS232C) port.

Syntax

To set information:

```
line console 0
```

To delete information:

```
no line console
```

Input mode

`(config)`

Parameters

None

Default behavior

The console can be connected to a CONSOLE (RS232C) port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

`speed`

line vty

Permits Telnet remote access to a device. This command is also used to limit the number of remote users that can be simultaneously logged in to the device.

Configuring this command enables remote access using the telnet protocol from any remote operation terminal to be accepted. To control access, set the `ip access-group`, `ipv6 access-class`, or `transport input` command.

Syntax

To set information:

```
line vty 0 <number>
```

To delete information:

```
no line vty
```

Input mode

```
(config)
```

Parameters

<*number*>

Sets the number of users who are able to log in simultaneously.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 15 (The number of users who can log in can be set to any value from 1 to 16).

Default behavior

Does not accept remote access that uses the Telnet protocol.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you change the maximum number of concurrent users, current user sessions will not be terminated. The change does not close the sessions of users who are currently logged in.

Related commands

```
transport input
ip access-group
ipv6 access-class
```

speed

Sets the communication speed of the CONSOLE (RS232C) port. If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out. If the communication speed is changed from a remote operation terminal while user login authentication from CONSOLE (RS232C) is in progress, the authentication might fail.

Syntax

To set or change information:

```
speed <number>
```

To delete information:

```
no speed
```

Input mode

```
(config-line)
```

Parameters

<*number*>

Sets the communication speed for CONSOLE (RS232C) in bit/s.

1. Default value when this parameter is omitted:

   Sets the communication speed of CONSOLE (RS232C) to 9600 bit/s.

2. Range of values:

   1200, 2400, 4800, 9600, 19200

Default behavior

The communication speed of CONSOLE (RS232C) is 9600 bit/s.

Impact on communication

None

When the change is applied

If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out.

Notes

1. If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out. If the communication speed is changed from a remote operation terminal while user login authentication from CONSOLE (RS232C) is in progress, the authentication might fail.

Related commands

```
line console
```

transport input

Restricts access from remote operation terminals based on protocol.

Syntax

To set or change information:

```
transport input {telnet | all | none}
transport input vrf {<vrf id> | all} {telnet | all | none}
```

To delete information:

```
no transport input
no transport input vrf {<vrf id> | all}
```

Input mode

```
(config-line)
```

Parameters

vrf {<*vrf id*> | all}

<*vrf id*>

Accepts access from the specified VRF. The global network is excluded.

If you want to specify an individual VRF for access, you can set up to four entries per device.

all

Accepts access from all VRFs including the global network.

1. Default value when this parameter is omitted:

   Accepts access from the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

{telnet | all | none}

telnet

Accepts remote access that uses the Telnet protocol.

all

Accepts remote access using any protocol (currently only Telnet is supported).

Only the Telnet protocol supports access from VRFs.

none

Does not accept remote access using any protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Accepts remote access that uses the Telnet protocol from the global network.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To permit or restrict FTP connections, use the `ftp-server` command in global configuration mode.
2. If the `vrf all` parameter is specified, an individual global network or VRF cannot be specified.
3. If you specify an individual VRF that is allowed to access the Device, a total of up to four VRF IDs can be specified by using this command and the `ftp-server` command.

Related commands

```
line vty
ftp-server
ip access-group
ipv6 access-class
```

Chapter

3. Editing and Working withConfigurations

apply-template
commit
configuration commit-mode
delete
end
end-template
insert
load
quit (exit)
replace
rollback
save
show
status
template
top

apply-template

Applies configuration commands set in the template to the configuration being edited.

Syntax

To set information:

```
apply-template <template name> [$<parameter> [ ... ] ]
```

Input mode

```
(config)
```

Parameters

<template name>

Specifies the name of the template to be applied to the configuration being edited.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the template name that was already created with the `template` command.

$*<parameter>*

Specifies the value to replace the template parameter. When `$`*<parameter>*`#`*<index>* is used for the template parameter in the template, it is replaced in the same way as `$`*<parameter>*.

Omits this parameter if template parameters are not specified when creating the template.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Enclose a character string in double quotation marks. Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If an error occurs while applying the configuration commands set in the template to the configuration being edited, the state before executing this command is restored and application stops.
2. If this command is executed when the configuration commands that check whether `y` or `n` are set in the template, all are applied as `y` to the configuration being edited without checking whether they are `y` or `n`.

3. When the configuration commit mode is auto-applied commit mode, if this command is executed, the configuration set in the template is immediately applied to the running configuration. In manual commit mode, the configuration is applied to the running configuration in a batch when the `commit` command is executed.

Related commands

`template`

commit

If the configuration commit mode is manual commit mode, the content of the edited configuration is applied to the running configuration and saved in the startup configuration.

Syntax

```
commit [running]
```

Input mode

Configuration command mode

Parameters

running

The content of the edited configuration is applied only to the running configuration and is not saved in the startup configuration.

1. Default value when this parameter is omitted:

   Saves the edited configuration in the startup configuration.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `commit` command.

Table 3-1: Response messages for the commit command

Message	Description
A commit of the configuration finished successfully.	The content of the edited configuration was applied to the specified configuration.

Notes

1. If the configuration commit mode is auto-applied commit mode, you cannot execute this command.

Related commands

`rollback`

configuration commit-mode

Sets the configuration commit mode. The following are the configuration commit modes supported in the Device.

- Auto-applied commit mode

  Immediately applies content of the edited configuration to the running configuration. To save the edited content in the startup configuration, execute the `save` command.

- Manual commit mode

  Applies the content of the edited configuration in a batch to the running configuration when the `commit` command is executed, and saves it in the startup configuration.

Syntax

To set information:

```
configuration commit-mode manual
```

To delete information:

```
no configuration commit-mode
```

Input mode

```
(config)
```

Parameters

manual

Sets the configuration commit mode to manual commit mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The configuration commit mode becomes auto-applied commit mode.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. While the configuration commit mode is being changed by this command, you cannot execute configuration commands to edit configurations, or operation commands.
2. When the configuration commit mode is manual commit mode, if you exit configuration command mode by executing the `quit (exit)` command or `end` command after revising the configuration, the configuration being edited is retained. To resume editing the configuration, execute the `configure (configure terminal)` operation command.

Related commands

None

delete

Deletes a configuration command set in the template.

Syntax

To delete information:

```
delete <command> [<parameter>]
```

Input mode

template mode

Parameters

<*command*>

Specifies the configuration command syntax to be set in the template.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a command that is supported in the Device.

<*parameter*>

Specifies the configuration command parameter to be set in the template.

1. Default value when this parameter is omitted:

   Follows the command specified in the <*command*> parameter.

2. Range of values:

   Specifies the parameter of the command specified in the <*command*> parameter.

Default behavior

None

Impact on communication

None

When the change is applied

Applies the configuration commands set in the template at the time the `apply-template` command is executed.

Notes

1. The command syntax specified in the parameter of this command should completely match the command syntax of the configuration command set in the template, including the parameter value.
2. In the command syntax specified in the parameters of this command, specify the configuration command set in the current hierarchy.

Related commands

None

end

Ends configuration command mode and returns you to administrator mode.

Syntax

```
end
```

Input mode

Configuration command mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `end` command.

Table 3-2: Response messages for the end command

Message	Description
The changes to the configuration have not been saved. Do you want to exit configure mode without saving the changes? (y/n):	You are trying to exit the configuration command mode without saving the edited configuration to a startup configuration file. Enter `y` to exit the configuration command mode. Entering `n` aborts the `end` command. If necessary, use the `commit` or `save` command to save the edited configuration to a startup configuration file.

Notes

1. You can temporarily exit the configuration command mode without saving the configuration to a startup configuration file. At this time, the configuration status will be "being edited". After editing the configuration, execute the `commit` or `save` command to save the edited configuration to a startup configuration file.
2. After editing the configuration, if you execute this command without saving to a startup configuration file, the edited configuration will be different from the startup configuration file. For this reason, if you enter configuration command mode again and then enter the end command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.
3. Do not interrupt the end command by pressing **Ctrl** + **C** before the command processing finishes. If the processing is interrupted, configuration command mode does not end. Subsequent execution of a configuration command might cause the error message `A logical inconsistency occurred.` to be output. If this message is output, use the end command to end configuration command mode.

Related commands

None

end-template

Ends template mode and returns to global configuration mode.

Syntax

To set information:

```
end-template
```

Input mode

template mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

None

Related commands

```
template
```

insert

Inserts a configuration command at any position in the template. After this command is executed, the mode switches to insert mode.

Syntax

To set information:

```
insert <command> [<parameter>]
```

Input mode

template mode

Parameters

<*command*>

Specifies the configuration command to insert into the template.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a command that is supported in the Device.

<*parameter*>

Specifies the configuration command parameter to insert into the template.

1. Default value when this parameter is omitted:

   Follows the command specified in the <*command*> parameter.

2. Range of values:

   Specify the parameter of the command specified in the <*command*> parameter.

Default behavior

None

Impact on communication

None

When the change is applied

Applies the configuration commands set in the template when the `apply-template` command is executed.

Notes

1. In insert mode, specify the configuration command for the position where you want to insert a command in the template. The configuration command specified with the parameter of this command will be inserted on the line above the specified configuration command. In insert mode, specify a configuration command on the same level as the level this command is executed on in the exact same format, including command syntax and parameter values. After specification of the configuration command, it returns to template mode.
2. In insert mode, if the `top` command, `end` command or `quit (exit)` command is specified, exit insert mode without inserting the command.
3. If, in the template, a configuration command with a command string that completely matches already exists, including parameter values, you cannot insert the configuration command.

4. For configuration commands specified with this command and in insert mode, specify configuration commands that are supported by the Device, including command syntax and parameter values. Errors occur if you specify unsupported command syntax and parameter values.

Related commands

None

load

Applies the specified configuration file to the configuration being edited. Based on the context of the specified file, the currently-edited configuration can be set, changed or deleted.

Syntax

```
load [-f] merge <file name> [debug]
```

Input mode

Configuration command mode

Parameters

-f

Executes the command without displaying a confirmation message.

1. Default value when this parameter is omitted:

   A confirmation message is displayed.

2. Range of values:

   None

merge <*file name*>

Specifies the name of the configuration file to be merged into the currently-edited configuration.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   If specifying a local configuration file, specify the name of a file stored in the device. If specifying a remote configuration file, specify the name of a remote file in one of the following URL formats:

   * FTP

     ftp://[<*user name*>[:<*password*>]@]<*host*>[:<*port*>]/<*file path*>

   * TFTP

     tftp://<*host*>[:<*port*>]/<*file path*>

   * HTTP

     http://[<*user name*>[:<*password*>]@]<*host*>[:<*port*>]/[<*file path*>]

   The meaning of each variable is as follows:

   <*user name*>

   Specify a user name for the remote server.

   <*password*>

   Specify the password for the remove server.

   <*host*>

   Specify the name or IP address of the remote server

   To use an IPv6 address, it needs to be enclosed in [ ] parentheses.

(Example) [2001:db8::1]

<*port*>

Specify a port number.

<*file path*>

Specify the path to the file on the remote server.

If <*user name*> and <*password*> are omitted when FTP or HTTP is specified, anonymous login is performed. If only <*password*> is omitted, a prompt is displayed requesting the password.

debug

When specifying a remote configuration file, details about the communication status are displayed.

If the error `The file transfer failed.` occurs while attempting to access a remote configuration file, retry the command with the debug parameter specified to display detailed error messages such as server responses.

1. Default value when this parameter is omitted:

   When specifying a remote configuration file, details about the communication status are not displayed.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `load` command.

Table 3-3: Response messages for the load command

Message	Description
Do you want to apply the specified configuration file to the configuration being edited? (y/n):	Confirms whether or not to apply it in the configuration being edited. Enter `y` to apply it. Entering `n` aborts the application.

For details about the error messages for this command, see *17.1.4 Errors related to the handling of the configuration file*.

Notes

1. If a merge cannot be performed because of a reason such as there being inconsistency between the configuration file being edited and the merge-source configuration file while executing this command, the content of the first error is output. At this point, the configuration being edited is not changed. Review the merge-source configuration file or the configuration being edited and execute the command again.
2. Executed commands are recorded in the operation log. For this reason, if this command is executed with <*password*> specified when specifying the remote configuration file name, the

password might be seen by other users. To ensure security, we recommend that you omit <*password*> and use the inquiry prompt to input the password.

3. In the URL notation, a single `/` located between the <*host*> specification and the <*filepath*> specification is not included as a path component. For example, to specify `/usr/home/staff/a.cnf` on the FTP remote server, specify `ftp://`<*host*>`//usr/home/staff/a.cnf`.
4. If the `end`, `quit (exit)` or `top` commands are specified in the configuration file specified as a parameter of this command, they commands ignored without being applied in the configuration being edited. If the following commands are specified, an error occurs.
   - banner {motd | motd-ftp | login | login-ftp} plain-text
   - commit
   - enable password input
   - rollback
   - save
   - show
   - status
   - username <*user name*> [<*user id*>] [no-flash] password input
5. If a configuration command that can be set in multiple configuration command modes is specified for the configuration file specified as a parameter of this command, specify in advance a configuration command that switches to the mode that you want to set. To return to the second level after switching to the third level in sub-mode by executing the `address-family ipv4` or `address-family ipv6` command, specify the `exit-address-family` command. To return to global configuration mode from the sub-mode of a given layer, specify `!`.
6. If applying the configuration file that was saved by using the `save` command or `copy` operation command to the configuration being edited with this command, an error might occur due to duplicated configurations. In this case, review the merge-source configuration file or the configuration being edited and execute the command again.

Related commands

None

quit (exit)

Returns the mode to the level that is one level higher. If you are editing a configuration in global configuration mode, this command ends configuration mode and returns you to administrator mode. If you are editing data in sub-mode, you are returned to the level that is one level higher.

For details about operations in user mode and administrator mode, see *2. Switching the Command Input Mode* in the manual *Operation Command Reference Vol. 1 For Version 12.1*.

Syntax

```
quit
exit
```

Input mode

Configuration command mode, user mode, and administrator mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `quit` (`exit`) command.

Table 3-4: Response messages for the quit (exit) command

Message	Description
The changes to the configuration have not been saved. Do you want to exit configure mode without saving the changes? (y/n):	You are trying to exit the configuration command mode without saving the edited configuration to a startup configuration file. Enter `y` to exit the configuration command mode. Entering `n` aborts the command. If necessary, use the `commit` or `save` command to save the edited configuration to a startup configuration file.

Notes

Note the following if you use the `quit (exit)` command in configuration command mode:

1. You can use the `quit (exit)` command to temporarily exit the configuration command mode without saving the configuration to a startup configuration file. At this time, the configuration status will be "being edited". After editing the configuration, execute the `commit` or `save` command to save the edited configuration to a startup configuration file.
2. After editing the configuration, if you execute this command without saving to a startup configuration file, the edited configuration will be different from the startup configuration file. For this reason, if you enter configuration command mode again and then enter the end command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.
3. Do not interrupt the end command by pressing **Ctrl** + **C** before the command processing finishes. If the processing is interrupted, configuration command mode does not end.

Subsequent execution of a configuration command might cause the error message `A logical inconsistency occurred.` to be output. If this message is output, use the `end` command to end configuration command mode.

Related commands

None

replace

Overwrites the configuration command set in the template. After this command is executed, the mode switches to replace mode.

Syntax

To change information:

```
replace <command> [<parameter>]
```

Input mode

template mode

Parameters

<*command*>

Specifies the configuration command used after overwriting the command that will be set in the template.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a command that is supported in the Device.

<*parameter*>

Specifies the parameters of the configuration command used after overwriting the command that will be set in the template.

1. Default value when this parameter is omitted:

   Follows the command specified in the <*command*> parameter.

2. Range of values:

   Specify the parameter of the command that was specified in the <*command*> parameter.

Default behavior

None

Impact on communication

None

When the change is applied

Applies the configuration commands set in the template at the time the `apply-template` command is executed.

Notes

1. In replace mode, specify the configuration command to be overwritten that is set in the template. Specify a configuration command on the same level as the level this command is executed on in the exact same format, including command syntax and parameter values. After specification of the configuration command, it returns to template mode.
2. If a configuration command is set under the level in which the configuration command to be overwritten is located, all configuration commands under the level are deleted before overwriting the configuration command.
3. It is not possible overwrite a configuration command with another configuration command

with the exactly same parameter values and command string.

4. For configuration commands specified with this command and in replace mode, specify configuration commands that are supported by the Device, including command syntax and parameter values. Errors occur if you specify unsupported command syntax and parameter values.

Related commands

None

rollback

Changes the configuration being edited back to the specified status.

Syntax

```
rollback [running]
```

Input mode

Configuration command mode

Parameters

running

Changes the configuration being edited back to the running configuration.

1. Default value when this parameter is omitted:

   Changes the configuration being edited back to the running configuration.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the rollback command.

Table 3-5: Response messages for the rollback command

Message	Description
A rollback of the configuration finished successfully.	Indicates that the configuration being edited was changed back to the specified configuration.
The configuration being edited will be discarded. Do you want to roll back the configuration? (y/n):	You are attempting to discard the configuration being edited and change it back to the specified configuration. Enter `y` to change it back to the specified configuration. Entering `n` aborts the `rollback` command.

Notes

1. If the configuration commit mode is auto-applied commit mode, you cannot execute this command.

Related commands

```
commit
```

save

Saves the edited configuration to the startup configuration file or to a backup configuration file. If the `subset` parameter is specified, the edited configuration is partially saved.

Syntax

```
save [-f] [<file name>] [debug]
save [-f] <file name> [debug] subset [<command> [<parameter>]]
```

Input mode

Configuration command mode

Parameters

-f

Executes the command without displaying a confirmation message.

1. Default value when this parameter is omitted:

   A confirmation message is displayed.

2. Range of values:

   None

<file name>

Specifies the name of the configuration file to be saved. This file will be the backup configuration file.

1. Default value when this parameter is omitted:

   The startup configuration file (`startup-config`) is overwritten by the configuration that is being edited.

   In the following cases, this parameter cannot be omitted:

   * When the `subset` parameter is specified

   * When the configuration commit mode is the manual commit mode

2. Range of values:

   If specifying a local configuration file, specify the name of a file stored in the device.

   If specifying a remote configuration file, specify the name of a remote file in one of the following URL formats:

   * FTP

     ftp://[<*user name*>[:<*password*>]@]<*host*>[:<*port*>]/<*file path*>

   * TFTP

     tftp://<*host*>[:<*port*>]/<*file path*>

debug

When specifying a remote configuration file, details about the communication status are displayed.

If the error `The file transfer failed.` occurs while attempting to access a remote configuration file, retry the command with the debug parameter specified to display detailed error messages, such as server responses.

1. Default value when this parameter is omitted:

When specifying a remote configuration file, details about the communication status are not displayed.

2. Range of values:

None

subset [<*command*> [<*parameter*>]]

Saves the configuration being edited partially.

1. Default value when this parameter is omitted:

Saves the configuration being edited entirely.

2. Range of values:

In <*command*>, specify the configuration command to be included in the saving file. If omitted, configurations under the current configuration command mode are targeted.

In <*parameter*>, specify parameters such as <*vlan id*> or <*access list name*> to limit the items to be saved.

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `save` command.

Table 3-6: Response messages for the save command

Message	Description
Do you want to save the configuration in the file <*file name*>? (y/n):	This message confirms whether you want to execute the `save` command for the specified file. Enter `y` to execute the command. Enter `n` to cancel this operation.
The specified file already exists. Do you want to overwrite the configuration in the file <*file name*>? (y/n):	This message notifies you that the specified file already exists, and asks you to confirm whether you want to execute the `save` command and overwrite it. Enter `y` to execute the command. Enter `n` to cancel this operation.

For details about the error messages for this command, see *17.1.4 Errors related to the handling of the configuration file*.

Notes

1. If the commit mode of the configuration is the manual commit mode, because this command creates a backup configuration, use the `commit` command to save the configuration being edited to the startup configuration.
2. Saving the configuration file does not exit configuration command mode. To finish editing and exit configuration command mode, use the `quit (exit)` command or `end` command.
3. If you do not have permission to write the configuration file to the save destination, your edits are not saved to the file. To save edits to a file on a remote server, your remote server access permissions must be changed to allow you to write to the remote server.
4. You can use the `status` command to check whether the configuration has been changed but

not saved.

5. Specify configuration commands that can be specified as parameters of the `show` command in the subset parameters <*command*> and <*parameter*>. If the `subset` parameters are specified, the output to the backup configuration file is the same as the result of executing the `show` command with the same parameters as those specified in the `subset` parameters. However, the `banner` command is not output in text format even when the `plain-text` parameter is specified, and the output results are the same as the case where it is not specified.
6. If the command is executed in sub-mode (configuration command mode) by specifying the `subset` parameter, the configuration from the second level is saved to the backup configuration regardless of the executed directory and the commands and parameters specified in the `subset` parameters.

Related commands

None

show

Displays the configuration being edited.

Syntax

```
show [ <command> [ <parameter> ] ]
```

Input mode

Configuration command mode

Parameters

<*command*>

Specifies a configuration command.

1. Default value when this parameter is omitted:

   Displays all the setting information of the configuration.

<*parameter*>

Specifies parameters such as <*vlan id*> or <*access list name*> to limit the displayed items.

1. Default value when this parameter is omitted:

   Displays the entire <*command*> that was specified.

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If there are many items in the configuration, the command might take time to execute.
2. If the configuration is edited, the `copy` command is executed, or a NIF is inserted while this command is being executed, this command might be aborted.
3. If a NIF is connected or replaced, the configuration might be changed automatically. In this case, the last-modified time displayed on the first line is also updated.

Related commands

None

status

Shows the status of the configuration being edited.

Syntax

```
status
```

Input mode

Configuration command mode

Parameters

None

Displayed information

The table below describes the items displayed for the `status` command.

Table 3-7: Information displayed by the status command

Title		Displayed information
File name		The file being edited is displayed. • Running configuration: running-config
Commit mode		The commit mode of the configuration is displayed. • Auto-applied commit mode: Auto commit • Manual commit mode: Manual commit
Last modified time		The last-modified time and the person who updated the file are displayed. Depending on the edit status, the following information is displayed: • The file contains initial installation defaults, and the file has not been changed: Not modified • The file has not been edited since the device was started: <*Date*> by <*User*> (not modified) • The file was edited and changed but not saved: <*Date*> by <*User*> (not saved) • The file was edited, changed and saved: <*Date*> by <*User*> (saved)
Buffer	Total	Displays the total amount of storage that is available, including the configuration file that is currently being edited.
	Available	Displays the amount of storage remaining for use by the configuration file that is currently being edited. This unavailable capacity is also displayed as a percentage of the total amount.
	Fragments	The amount of currently-edited configuration file space that is unavailable -- for example, because it is fragmented (items have been deleted, but the area has not been reclaimed) -- is displayed. This unavailable capacity is also displayed as a percentage of the total amount.
Login user		The names of users currently logged in to the device, and their login times are displayed. `edit` is displayed next to users who are editing the configuration.

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If the remaining capacity becomes very small, it might not be sufficient to execute some configuration commands.
2. If a NIF is connected or replaced, the configuration might be changed automatically. In this case, the last-modified time is also updated.

Related commands

None

template

Creates a configuration command template. After this command is executed, the mode switches to template mode.

Syntax

To set information:

```
template <template name> [$<parameter> [ ... ] ]
```

To change information:

```
template <template name> change-parameter [$<parameter> [ ... ] ]
```

To delete information:

```
no template <template name>
```

Input mode

```
(config)
```

Parameters

<template name>

Specifies the template name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name of no more than 31 characters.

   An alphabetical character can be specified for the first character of the name, and alphanumeric characters, hyphens (-), and underscores (_) can be specified for the subsequent characters. For details, see *Specifiable values for parameters*.

$*<parameter>*

Specifies the template parameter (a string that can replace an optional parameter of the configuration command to be registered with the template). This parameter can be used as a parameter of a configuration command in the template.

To apply changes in the template, replace this parameter with the value specified in the parameter of the `apply-template` command and execute the configuration command. A maximum of 100 template parameters can be set to one template.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify a string with `$` + 31 or fewer characters.

   For details, see *Specifiable values for parameters*.

change-parameter [$*<parameter>* [...]]

When executing this command, change the template parameter specified to the template parameter that was specified with the `change-parameter` parameter.

1. Default value when this parameter is omitted:

   Do not change the template parameter.

2. Range of values:

None

Default behavior

None

Impact on communication

None

When the change is applied

Applies the configuration commands set in the template at the time the `apply-template` command is executed.

Notes

1. In template mode, configuration commands are set to the template in the order specified by the user.
2. In template mode, a template parameter specified with this command can be used for one of the optimal parameters separated with blank spaces in the syntax of the configuration command. However, if the parameter is an Ethernet subinterface or a port channel subinterface, specify <*nif no.*>/<*port no.*> and <*subinterface index*> or <*channel group number*> and <*subinterface index*> respectively to the two template parameters.
3. To insert a configuration command between configuration commands set in the template, use the `insert` command.
4. To overwrite a configuration command set in the template, use the `replace` command.
5. To delete a configuration command set in the template, use the `delete` command. If a configuration command with deletion syntax is entered, do not delete it from the template and set the deletion syntax to the template as is.
6. Multiple configuration commands that are exactly the same, including their parameter values, cannot be set in the template. To set multiple configuration commands that switch to configuration command mode, the second and subsequent settings will be executed by re-editing the first command. To set multiple configuration commands using template parameters, specify them with template parameters in the format of `$`<*parameter*>`#`<*index*>. Specify a number in range from 1 to 99 in <*index*>.
7. When using this command to edit an existing template, even if the configuration of the template parameter was changed and executed after the configuration was set when the template was made, the existing template parameter configuration will not be used for editing, and the original configuration will be edited. To edit and change the configuration of the template parameter set in the template, specify the `change-parameter` parameter.
8. In template mode, an operation command cannot be executed if `$` is placed at the beginning of the command.
9. The following configuration commands cannot be set in templates:
   - apply-template
   - commit
   - delete
   - end
   - insert
   - load
   - quit (exit)
   - replace

- rollback
- save
- show
- status
- template
- top

Related commands

```
end-template
apply-template
delete
insert
replace
```

top

Returns to global configuration mode from sub-mode.

Syntax

```
top
```

Input mode

Configuration command mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

None

Related commands

None

Chapter

4. Management Port

description
duplex
interface mgmt
shutdown
speed

description

Sets the supplementary information. Use this command to create a note about the management port. You can check the note via ifDescr (SNMP MIB) if this command is set.

Syntax

To set or change information:

```
description <string>
```

To delete information:

```
no description
```

Input mode

```
(config-if)
```

Management port

Parameters

<*string*>

Sets supplementary information for the management port.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
interface mgmt
```

duplex

Sets the half duplex or full duplex mode for a management port.

Syntax

To set or change information:

```
duplex { half | full | auto }
```

To delete information:

```
no duplex
```

Input mode

`(config-if)`

Management port

Parameters

{ half | full | auto }

Sets the half duplex or full duplex mode for a management port.

half

Sets the line to half duplex (fixed) mode.

full

Sets the line to full duplex (fixed) mode.

auto

Determines the half duplex or full duplex mode by auto-negotiation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`auto` is set for the `speed` and `duplex` commands.

Impact on communication

If any management port settings are changed by using this command while the management port is up, the port goes down and then comes up again.

Accordingly, the following might occur:

- If management port communication is in progress, it is stopped.
- Dynamic ARP entries and dynamic NDP entries generated for the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is specified for `speed` or `duplex`, auto-negotiation is performed.

2. If auto-negotiation is not used , you must set `duplex` to `full` or `half`, and set `speed` to `10` or `100`.

Related commands

```
interface mgmt
speed
```

interface mgmt

Moves to the management port level.

Syntax

To set information:

```
interface mgmt 0
```

To delete information:

```
no interface mgmt 0
```

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A management port cannot be used if an IP address is not set for the port.
2. Configuring (enabling) the management port does not count towards the capacity limit (maximum number of interfaces).

Related commands

None

shutdown

Sets the management port to the shutdown state.

Syntax

To set information:

```
shutdown
```

To delete information:

```
no shutdown
```

Input mode

```
(config-if)
```

Management port

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

```
interface mgmt
```

speed

Sets the line speed of a management port.

Syntax

To set or change information:

```
speed { 10 | 100 | auto | auto { 10 | 100 | 1000 | 10 100 1000 }}
```

To delete information:

```
no speed
```

Input mode

```
(config-if)
```

Management port

Parameters

{ 10 | 100 | auto | auto { 10 | 100 | 1000 | 10 100 1000 }}

Sets the line speed of a management port.

10

Sets the line speed to 10 Mbps.

100

Sets the line speed to 100 Mbps.

auto

Sets the line speed to auto-negotiation.

auto { 10 | 100 | 1000 | 10 100 1000 }

Auto-negotiation is performed at the specified line speed. This setting prevents the line speed from operating at an unexpected speed, and the line usage rate from increasing. If negotiation at the specified line speed does not succeed, the link does not come up.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`auto` is set for the `speed` and `duplex` commands.

Impact on communication

If any management port settings are changed by using this command while the management port is up, the port goes down and then comes up again.

Accordingly, the following might occur:

- If management port communication is in progress, it is stopped.
- Dynamic ARP entries and dynamic NDP entries generated for the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is specified for `speed` or `duplex`, auto-negotiation is performed.
2. If auto-negotiation is not used , you must set `speed` to `10` or `100`, and set `duplex` to `full` or `half`.

Related commands

```
interface mgmt
duplex
```

Chapter

5. Dial-up IP Connection

interface async
ip address (AUX)
peer default ip address

interface async

Sets items about AUX ports.

Entering this command switches to `config-if` mode where information about AUX ports can be set.

Syntax

To set information:

```
interface async 1
```

To delete information:

```
no interface async
```

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ip address (AUX)
peer default ip address
```

ip address (AUX)

Sets an IPv4 address for an AUX port.

Syntax

To set or change information:

```
ip address <ip address> <subnet mask>
```

To delete information:

```
no ip address
```

Input mode

```
(config-if)
```

Parameters

<*ip address*>

Specifies the local IPv4 address of an AUX port.

<*subnet mask*>

Specifies the subnet mask.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   128.0.0.0 to 255.255.255.255 (bits must be contiguous)

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. Note, however, that if this command is used to make changes during a dial-up IP connection, the changes will take effect from the next connection.

Notes

1. For dial-up IP connections, both peer default ip address and ip address (AUX) must be set.

Related commands

```
interface async
peer default ip address
```

peer default ip address

Specifies the destination address of an AUX port.

Syntax

To set or change information:

```
peer default ip address <ip address>
```

To delete information:

```
no peer default ip address
```

Input mode

```
(config-if)
```

Parameters

<ip address>

Specifies the destination address of an AUX port.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. Note, however, that if this command is used to make changes during a dial-up IP connection, the changes will take effect from the next connection.

Notes

1. For dial-up IP connections, both peer default ip address and ip address (AUX) must be set.

Related commands

```
interface async
ip address (AUX)
```

Chapter

6. Login Security and RADIUS or TACACS+

aaa accounting commands
aaa accounting exec
aaa authentication enable
aaa authentication enable attribute-user-per-method
aaa authentication enable end-by-reject
aaa authentication login
aaa authentication login console
aaa authentication login end-by-reject
aaa authorization commands
aaa authorization commands console
banner
commands exec
enable password
ip access-group
ipv6 access-class
parser view
radius-server host
radius-server key
radius-server retransmit
radius-server timeout
tacacs-server host
tacacs-server key
tacacs-server timeout
username

aaa accounting commands

Logs accounting information when commands are used.

Syntax

To set or change information:

```
aaa accounting commands { 15 | 0-15 } default { start-stop | stop-only } [
broadcast ] group tacacs+
```

To delete information:

```
no aaa accounting commands
```

Input mode

```
(config)
```

Parameters

{ 15 | 0-15 }

Specifies the command level for accounting.

15

Only configuration commands are subject to accounting.

0-15

Both operation commands and configuration commands are subject to accounting.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{start-stop | stop-only}

Specifies the trigger of accounting for commands.

start-stop

Sends a start instruction before a command is executed and a stop instruction after the command is executed.

stop-only

Sends a stop instruction before a command is executed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

broadcast

If this parameter is specified, accounting information is sent in turn to all servers (maximum of four) set by the `tacacs-server host` command, and continues regardless of whether the information sent succeeded or failed, or whether any acknowledgements were received from any of the servers.

1. Default value when this parameter is omitted:

   Accounting information will be repeatedly sent in turn to a maximum of four servers

until the information is successfully sent to, and acknowledgements are received from, the servers.

group tacacs+

The TACACS+ server is used as the accounting server.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

`tacacs-server host`

aaa accounting exec

Enables accounting of login and logout.

Syntax

To set or change information:

```
aaa accounting exec default { start-stop | stop-only } [ broadcast ] { group
radius | group tacacs+ }
```

To delete information:

```
no aaa accounting exec
```

Input mode

```
(config)
```

Parameters

{start-stop | stop-only}

Sets the trigger for accounting.

start-stop

Sends a start instruction at login and a stop instruction at logout.

stop-only

Sends a stop instruction at logout only.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

broadcast

If this parameter is specified, accounting information is sent in turn to all servers (maximum of four) set by the `radius-server host` command or the `tacacs-server host` command, and continues regardless of whether the information sent succeeded or failed, or whether any acknowledgements were received from any of the servers.

1. Default value when this parameter is omitted:

   Accounting information will be repeatedly sent in turn to a maximum of four servers until the information is successfully sent to, and acknowledgements are received from, the servers.

{group radius | group tacacs+}

Sets the type of an accounting server.

group radius

The RADIUS server is used as the accounting server.

group tacacs+

The TACACS+ server is used as the accounting server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
radius-server host
tacacs-server host
```

aaa authentication enable

Specifies the authentication method to be used when changing to administrator mode (by the `enable` command). If the first specified authentication method fails, the second specified method is used for authentication. You can change how authentication works when the first method fails by using the `aaa authentication enable end-by-reject` command.

Syntax

To set or change information:

```
aaa authentication enable default <method> [<method> [<method>] ]
```

To delete information:

```
no aaa authentication enable
```

Input mode

```
(config)
```

Parameters

default <*method*> [<*method*> [<*method*>]]

Specifies the authentication method to be used when changing to administrator mode (`enable` command) for <*method*>.

Specify any of the parameters below for <*method*>. You cannot set the same <*method*> more than once.

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

enable

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the `group radius` parameter or the `group tacacs+` parameter is specified, you cannot switch to administrator mode if communication with a RADIUS or TACACS+ server is impossible or if the authentication fails. Therefore, we recommend that you specify the `enable` parameter at the same time as the parameters mentioned above.

Related commands

```
aaa authentication enable attribute-user-per-method
aaa authentication enable end-by-reject
radius-server
tacacs-server
```

aaa authentication enable attribute-user-per-method

When changing to administrator mode (by the `enable` command), change the user name attribute to be used for authentication as follows for each authentication method:

- For RADIUS authentication, `$enab15$` is sent as the User-Name attribute.
- For TACACS+ authentication, the login user name is sent as the User attribute.

Syntax

To set information:

```
aaa authentication enable attribute-user-per-method
```

To delete information:

```
no aaa authentication enable attribute-user-per-method
```

Input mode

```
(config)
```

Parameters

None

Default behavior

"admin" is sent as the User-Name attribute when changing to administrator mode (by the `enable` command).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Use this command to suit your RADIUS or TACACS+ server.

Related commands

```
aaa authentication enable
```

aaa authentication enable end-by-reject

Terminates the authentication if an attempt to change to administrator mode (by the `enable` command) is denied. If the authentication fails due to an abnormality such as an inability to communicate, the next authentication method specified by the `aaa authentication enable` command is used to perform the authentication.

Syntax

To set information:

```
aaa authentication enable end-by-reject
```

To delete information:

```
no aaa authentication enable end-by-reject
```

Input mode

```
(config)
```

Parameters

None

Default behavior

If the authentication fails, regardless of the reason for failure, the next authentication method specified by the `aaa authentication enable` command is used to perform the authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is only valid for authentication methods specified by the `aaa authentication enable` command.

Related commands

```
aaa authentication enable
```

aaa authentication login

Specifies the authentication method to be used at login. If the first specified authentication method fails, the second specified method is used for authentication. You can change how authentication works when the first method fails by using the `aaa authentication login end-by-reject` command.

Syntax

To set or change information:

```
aaa authentication login default <method> [<method> [<method>] ]
```

To delete information:

```
no aaa authentication login
```

Input mode

```
(config)
```

Parameters

default <*method*> [<*method*> [<*method*>]]

Specifies the authentication method to be used at login for <*method*>.

Specify any of the parameters below for <*method*>. You cannot set the same <*method*> more than once.

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

local

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the `group radius` parameter or the `group tacacs+` parameter is specified, you cannot log in to the Device if communication with a RADIUS or TACACS+ server is impossible or if the authentication fails. Therefore, we recommend that you specify the `local` parameter at the same time as the parameters mentioned above.

Related commands

```
radius-server host
tacacs-server host
aaa authentication login console
aaa authentication login end-by-reject
```

aaa authentication login console

Applies the authentication method specified by the `aaa authentication login` command when the user logs in from the console (RS232C) or AUX port.

Syntax

To set information:

```
aaa authentication login console
```

To delete information:

```
no aaa authentication login console
```

Input mode

```
(config)
```

Parameters

None

Default behavior

Local password authentication is used when a user logs in from the console (RS232C) or AUX port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To perform RADIUS or TACACS+ authentication, you must also set the `aaa authentication login` command.
2. When the `local` parameter is not specified as the authentication method by the `aaa authentication login` command, and the `aaa authentication login console` command is set, the user cannot log in from the console (RS232C) and AUX if communication with a RADIUS or TACACS+ server is impossible, authentication fails, or the user logs in from a standby BCU.

Related commands

```
aaa authentication login
aaa authentication login end-by-reject
```

aaa authentication login end-by-reject

Terminates authentication if login authentication is denied. If the authentication fails due to an abnormality such as an inability to communicate, the next authentication method specified by the `aaa authentication login` command is used to perform the authentication.

Syntax

To set information:

```
aaa authentication login end-by-reject
```

To delete information:

```
no aaa authentication login end-by-reject
```

Input mode

```
(config)
```

Parameters

None

Default behavior

If authentication fails, regardless of the reason for failure, the next authentication method specified by the `aaa authentication login` command is used to perform the authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is only valid for authentication methods specified by the `aaa authentication login` command.

Related commands

```
aaa authentication login
```

aaa authorization commands

This command is specified to perform command authorization by using a RADIUS server, TACACS+ server, or by using local (configuration-based) authorization.

Note that, after successfully logging in, you will not be authorized to execute any commands except `logout`, `exit`, `quit`, `disable`, `end`, `set terminal`, `show whoami`, and `who am i` if any of the following apply:

- If the command class or the command list cannot be obtained as a vendor-specific attribute or an attribute value when authentication is performed on a RADIUS server or a TACACS+ server
- If the user name and the associated command class (`username view-class`) or command lists (`username view`, `parser view`, or `commands exec`) are not configured when authentication is performed by using a local password

Syntax

To set or change information:

```
aaa authorization commands default <method> [<method> [<method>] ]
```

To delete information:

```
no aaa authorization commands
```

Input mode

```
(config)
```

Parameters

default <*method*> [<*method*> [<*method*>]]

For <*method*>, specifies the method to be used for command authorization.

Specify any of the parameters below for <*method*>. You cannot set the same <*method*> more than once.

group radius

Command authorization is performed by a RADIUS server.

group tacacs+

Command authorization is performed by a TACACS+ server.

local

Local command authorization is performed.

Default behavior

Command authorization is not performed.

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. With this setting, when authentication is performed on the RADIUS server or TACACS+ server specified by the `aaa authentication login` command, or by using a local password, the use of command class or command list related commands is authorized. This command

alone is not sufficient for command authorization. You also need to have used the `aaa authentication login` command in advance.

2. Note that, after successful login, you will not be authorized to execute any commands except `logout`, `exit`, `quit`, `disable`, `end`, `set terminal`, `show whoami`, and `who am i` if any of the following applies:
   - If the command class or the command list cannot be obtained as a vendor-specific attribute or an attribute value when authentication is performed on a RADIUS server or a TACACS+ server
   - If the user name and the associated command class (`username view-class`) or command list (`username view`) are not configured when authentication is performed by using a local password

Related commands

```
radius-server host
tacacs-server host
aaa authentication login
aaa authorization commands console
parser view
commands exec
username
```

aaa authorization commands console

Authorizes the commands specified by the `aaa authorization commands` command when the user logs in from the console (RS232C) or AUX port.

Syntax

To set information:

```
aaa authorization commands console
```

To delete information:

```
no aaa authorization commands console
```

Input mode

```
(config)
```

Parameters

None

Default behavior

Commands are not authorized when a user logs in from the console (RS232C) or AUX port.

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. This command alone is not sufficient for command authorization. You also need to set the `aaa authorization commands` command.
2. With this setting, if a user logs in from the console (RS232C) or AUX port, command authorization is used to restrict the commands that can be executed.

Related commands

```
aaa authorization commands
```

banner

Sets the messages to be displayed before and after a user logs in. Depending on the specified parameters, messages can be displayed before or after a user login via Telnet, console, or FTP. A separate message can be set for FTP access.

The following table describes how the login message is displayed according to parameter settings.

Table 6-1: List of operations according to parameter settings

Description		Operation	
login(motd)	**login-ftp(motd-ftp)**	**Message displayed for Telnet or console access**	**Message displayed for FTP access**
Message A is set.	Not set	Message A is displayed.	Message A is displayed.
Message A is set.	The `disable` parameter is set.	Message A is displayed.	Not displayed
Message A is set.	Message B is set.	Message A is displayed.	Message B is displayed.
Not set	Message B is set.	Not displayed	Message B is displayed.
Not set (initial state)	Not set (initial state)	Not displayed	Not displayed

Syntax

To set or change information:

```
banner login { {encode "<encoded message>"} | plain-text }
banner login-ftp { {encode "<encoded message>"} | plain-text | disable }
banner motd { {encode "<encoded message>"} | plain-text }
banner motd-ftp { {encode "<encoded message>"} | plain-text | disable }
```

To delete information:

```
no banner {motd | motd-ftp | login | login-ftp }
```

Input mode

```
(config)
```

Parameters

login

Sets the message to be displayed before a user logs in via Telnet, console, or FTP.

plain-text

Enter the login message as a plain-text string. After the command is entered, the following message appears and you can enter a string in lines.

```
--- Press CTRL+D or only '.' on last line ---
```

At this point, enter the string you want to display for the login message. At the end of the string, press the **Ctrl** + **D** keys or enter a period (.) to close the input page.

Entries are automatically set in the `encode` parameter configuration. Any login message that was set previously is deleted. If you want to check a text-format image of what the screen will look like, use the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command.

1. Default value when this parameter is omitted:

   No login messages are displayed.

2. Range of values:

   A string consisting of a maximum of 720 alphanumeric characters

3. Notes on using this parameter:

   When entering login messages, check the screen settings for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command is executed or a client is connected, the prompt might become difficult to read, and the screen display might freeze. If you want to cancel setting the login message while entering the login message, press the **CTRL**+**C** keys to abort it. If you enter far more characters than the maximum number of characters permitted in a line, you may find that no further keyboard input (including the **CTRL**+**D** keys or a line break) is accepted. If this happens, use the **Backspace** key to delete entered characters and then re-enter them, or use the **CTRL**+**C** keys to abort.

   While entering a message, if you find that the previous character in a single line is not deleted when you press the **Backspace** key, change the setting of the **Backspace** key of the terminal so that the BS control code (ASCII 0x08 ^H) is sent. Note that the **Backspace** key does not affect characters in other than the current line.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message. Any login message that was set previously is deleted. Normally this is used to encode a message that was entered with the `plain-text` parameter. If you want to check a text-format image of what the screen will look like, use the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command.

1. Default value when this parameter is omitted:

   No login messages are displayed.

2. Range of values:

   Enter a Base64-encoded string enclosed in double-quotation marks (") (a maximum of 960 characters).

3. Notes on using this parameter:

   When entering login messages, check the screen settings for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command is executed, or a client is connected, the prompt might become difficult to read and the screen display might freeze.

login-ftp

Individually sets or disables the message to be displayed before a user logs in through FTP access. For FTP access, this setting has priority over the login setting.

plain-text

Enter the login message as a plain-text string. For details, see the *plain-text* section under the `login` parameter above.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message. For details, see the *encode* section under the `login` parameter above.

disable

Does not display a login message for FTP access even when the `login` parameter is set.

motd

Sets the message to be displayed after a user logs in through Telnet, console, or FTP access.

plain-text

Enter the login message as a plain-text string. For details, see the *plain-text* section under the `login` parameter above.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message. For details, see the *encode* section under the `login` parameter above.

motd-ftp

Individually sets or disables a message to be displayed after a user logs in through FTP access. For FTP access, this setting has priority over the `motd` setting.

plain-text

Enter the login message as a plain-text string. For details, see the *plain-text* section under the `login` parameter above.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message.

For details, see the *encode* section under the `login` parameter above.

disable

Does not display a login message for FTP access even when the `motd` parameter is set.

Default behavior

No login messages are displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting a login message, if a client log-in prompt is unnecessary (for example: when no password is required, and the user name is automatically passed by the client), the login message and the post-authentication screen are displayed in turn.

   When entering a login message, check the screen setting for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command is executed or a client is connected, the prompt might become difficult to read and the screen display might freeze.

Related commands

None

commands exec

Adds a command string to a command list used when local command authorization is enabled.

A maximum of 40 commands, including permitted and restricted commands, can be set in a command list.

Syntax

To set information:

```
commands exec {include | exclude} all <command>
```

To delete information:

```
no commands exec {include | exclude} all <command>
```

Input mode

```
(config-view)
```

Parameters

{include | exclude}

Restricts use of the specified command string.

Command strings for which the `include` parameter is specified are configured as permitted commands. Command strings for which the `exclude` parameter is specified are configured as restricted commands.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

all <*command*>

Specifies a command string to be added to the command list.

The Device judges whether the initial character string of the command entered by the user matches any of the command strings specified in the command lists (match beginning).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 50 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

   In addition, commas (,) cannot be used in this parameter.

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. A maximum of 40 commands, including permitted and restricted commands, can be set in a command list. A string consisting of a maximum of 50 characters can be set as a command string.

Related commands

```
aaa authorization commands
parser view
username
```

enable password

Sets the password for administrator mode.

Syntax

To set or change information:

```
enable password {input | hidden <hidden password>}
```

To delete information:

```
no enable password
```

Input mode

```
(config)
```

Parameters

{input | hidden <*hidden password*>}

Sets the password for administrator mode.

input

Specifies the password from password input mode. The specified password will be automatically hashed and set to the configuration.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a string with 128 or fewer characters. Alphanumeric and special characters can be specified. For details, see *Any character string* in *Specifiable values for parameters*.

   For a security reason, the password should contain six or more characters. We recommend that you use upper-case alphabetic characters, numbers, and symbols in addition to lower-case alphabetic characters. If fewer than six characters are entered or only lower case alphabetic characters are used, an error is displayed. However, if the same string is specified again after the error is displayed, that string can be set as the password.

hidden <*hidden password*>

Specifies a hashed password that was created by using the `make hidden-password` operation command, or a hashed password that was created in the configuration of another device. If a string other than a hashed password string is specified, the system fails to perform local password authentication and the mode cannot be changed to administrator mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a hashed password string with 100 characters, including double quotation marks (").

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

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. This setting is common to all types of remote access (Telnet or FTP).

No more than 128 entries, spread over multiple lines, including access list entries set by using `ip access-group` and `ipv6 access-class`, can be set.

Syntax

To set information:

```
ip access-group <access list name> [vrf {<vrf id>| all}] in
```

To delete information:

```
no ip access-group <access list name> [vrf {<vrf id>| all}]
```

Input mode

```
(config-line)
```

Parameters

<access list name>

Specifies the access list name (the access list name of `ip access-list standard`) of the IPv4 address filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with 31 or fewer characters.

   For details, see *Specifiable values for parameters*.

vrf {<*vrf id*> | all}

Applies an access list for access from VRFs.

<*vrf id*>

Applies an access list for access from a specified VRF.

all

Applies an access list for access from all VRFs including the global network.

1. Default value when this parameter is omitted:

   Applies an access list for access from the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

Default behavior

Access using IPv4 addresses is permitted from all remote operation terminals.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet or FTP).
2. To allow FTP connections, set `ftp-server`.
3. When `ip access-group` is not set, access using IPv4 addresses is permitted from all remote operation terminals.
4. Changing the IPv4 addresses that are permitted to access the Device will not terminate current user sessions. The change does not close the sessions of users who are currently logged in.
5. The access list that is specified for `vrf all` is applied after the access lists that are set for the global network and each `vrf` <*vrf id*> is applied.

Related commands

```
line vty
ftp-server
transport input
ipv6 access-class
ip access-list standard
```

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. This setting is common to all types of remote access (Telnet or FTP).

No more than 128 entries, spread over multiple lines, including access list entries set by using `ip access-group` and `ipv6 access-class`, can be set.

Syntax

To set information:

```
ipv6 access-class <access list name> [vrf {<vrf id>| all}] in
```

To delete information:

```
no ipv6 access-class <access list name> [vrf {<vrf id>| all}]
```

Input mode

```
(config-line)
```

Parameters

<access list name>

Specifies the access list name (the access list name of `ipv6 access-list`) of the IPv6 filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with 31 or fewer characters.

   For details, see *Specifiable values for parameters*.

vrf {*<vrf id>* | all}

Applies an access list for access from VRFs.

<vrf id>

Applies an access list for access from a specified VRF.

all

Applies an access list for access from all VRFs, including the global network.

1. Default value when this parameter is omitted:

   Applies an access list for access from the global network.

2. Range of values:

   For *<vrf id>*, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

Default behavior

Access using IPv6 addresses is permitted from all remote operation terminals.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet or FTP).
2. To allow FTP connections, set `ftp-server`.
3. When `ipv6 access-class` is not set, access using IPv6 addresses is permitted from all remote operation terminals.
4. Changing the IPv6 addresses that are permitted to access the Device will not terminate current user sessions. The change does not close the sessions of users who are currently logged in.
5. The access list that is specified for `vrf all` is applied after the access lists that are set for the global network and each `vrf` <*vrf id*> are applied.

Related commands

```
line vty
ftp-server
transport input
ip access-group
ipv6 access-list
```

parser view

Generates a command list used when local command authorization is enabled. Entering this command switches to config-view mode in which information about the command list can be set.

A maximum of 20 command lists can be generated per device.

Syntax

To set information:

```
parser view <view name>
```

To delete information:

```
no parser view <view name>
```

Input mode

```
(config)
```

Parameters

<*view name*>

Specifies the name of a command list to be generated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name of no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. A maximum of 20 command lists can be generated per device.

Related commands

```
aaa authorization commands
commands exec
username
```

radius-server host

Configures the RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

```
radius-server host {<ipv4 address> | <ipv6 address> [interface <interface
type> <interface number>] |<host name>} [auth-port <port>] [acct-port <port>]
[timeout <seconds>] [retransmit <retries>] [key <string>] [{auth-only |
acct-only}]
```

To delete information:

```
no radius-server host {<ipv4 address> | <ipv6 address> [interface <interface
type> <interface number>] |<host name>}
```

Input mode

```
(config)
```

Parameters

{<*ipv4 address*> | <*ipv6 address*> [interface <*interface type*> <*interface number*>] | <*host name*>}

Specifies the IPv4 address, IPv6 address, or host name of the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*ipv4 address*>, specify an IPv4 address.

   For <*ipv6 address*>, specify an IPv6 address.

   For <*host name*>, specify a host name with 64 or fewer characters. For details, see *Specifiable values for parameters*.

   If an IPv6 link local address is specified in <*ipv6 address*>, the `interface` parameters can also be specified.

   Interface names and numbers corresponding to the following interface type groups can be specified for <*interface type*> and <*interface number*>. For details, see *How to specify an interface* in *Specifiable values for parameters*.

   * Ethernet interface

   * Ethernet subinterface

   * Port channel interface

   * Port channel subinterface

   * Management port

key <*string*>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   The RADIUS key set by using `radius-server key` is used. If this parameter is not set, the RADIUS server is disabled.

2. Range of values:

Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

auth-port <*port*>

Specifies the RADIUS server port number.

1. Default value when this parameter is omitted:

   Port number 1812 is used.

2. Range of values:

   1 to 65535

acct-port <*port*>

Specifies the port number for RADIUS server accounting.

1. Default value when this parameter is omitted:

   Port number 1813 is used.

2. Range of values:

   1 to 65535

{auth-only | acct-only}

Restricts use of the specified RADIUS server. It can be used only for the specified purpose. A RADIUS server specified with the `auth-only` option is used as a server dedicated to authentication. A RADIUS server specified with the `acct-only` option is used as a server dedicated to accounting.

1. Default value when this parameter is omitted:

   The RADIUS server can be used for all purposes (authentication and accounting).

2. Range of values:

   None

retransmit <*retries*>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   The number of times configured by using `radius-server retransmit` is used. If this parameter is not set, the initial value is 3.

2. Range of values:

   0 to 15

timeout <*seconds*>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   The period configured by using `radius-server timeout` is used. If this parameter is not set, the initial value is 5.

2. Range of values:

   1 to 30

Default behavior

Because the RADIUS server is not configured, no RADIUS communication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of four RADIUS servers can be specified per device.
2. When multiple RADIUS servers are specified, the RADIUS server that is first in the configuration file listing is the first server used for authentication.
3. If the `key` parameter is omitted and the `radius-server key` command is not set, the RADIUS server is disabled.

Related commands

```
radius-server key
radius-server retransmit
radius-server timeout
aaa authentication login
aaa authorization commands
aaa accounting exec
```

radius-server key

Sets the default RADIUS server key for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

```
radius-server key <string>
```

To delete information:

```
no radius-server key
```

Input mode

```
(config)
```

Parameters

<string>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `key` settings for the `radius-server host` command have priority over the settings for this command.

Related commands

```
radius-server host
radius-server retransmit
radius-server timeout
aaa authentication login
aaa authorization commands
aaa accounting exec
```

radius-server retransmit

Sets the default number of retransmissions to a RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

```
radius-server retransmit <retries>
```

To delete information:

```
no radius-server retransmit
```

Input mode

```
(config)
```

Parameters

<*retries*>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 15

Default behavior

The default value for the number of times an authentication request is retransmitted to a RADIUS server is 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `retransmit` settings for the `radius-server host` command have priority over the settings for this command.

Related commands

```
radius-server host
radius-server key
radius-server timeout
aaa authentication login
aaa authorization commands
aaa accounting exec
```

radius-server timeout

Sets a response timeout value for a RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

```
radius-server timeout <seconds>
```

To delete information:

```
no radius-server timeout
```

Input mode

```
(config)
```

Parameters

<*seconds*>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 30

Default behavior

The default response timeout value for the RADIUS server is 5 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `timeout` settings for the `radius-server host` command have priority over the settings for this command.

Related commands

```
radius-server host
radius-server key
radius-server retransmit
aaa authentication login
aaa authorization commands
aaa accounting exec
```

tacacs-server host

Configures the TACACS+ server used for authentication or authorization.

Syntax

To set or change information:

```
tacacs-server host {<host name> | <ip address>} [key <string>] [port <port>]
[timeout <seconds>] [{auth-only | acct-only}]
```

To delete information:

```
no tacacs-server host {<host name> | <ip address>}
```

Input mode

```
(config)
```

Parameters

{<*host name*> | <*ip address*>}

Specifies the IPv4 address or the host name of the TACACS+ server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address (in dot notation) or a host name can be specified.

   Specify the host name with 64 or fewer characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

key <*string*>

Specifies the shared private key used for encryption or authentication of communication with the TACACS+ server. The same shared private key must be set for the client and the TACACS+ server.

1. Default value when this parameter is omitted:

   The shared private key configured by using `tacacs-server key` is used. If this parameter must be set to encrypt communication with the TACACS+ server.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

port <*port*>

Specifies the TCP port number for TACACS+ server authentication.

1. Default value when this parameter is omitted:

   Port number 49 is used.

2. Range of values:

   1 to 65535

timeout <*seconds*>

Sets the timeout period (in seconds) for a response from the TACACS+ server.

1. Default value when this parameter is omitted:

   The period configured by using `tacacs-server timeout` is used. If this parameter is not set, the initial value is 5.

2. Range of values:

   1 to 30

{auth-only | acct-only}

Restricts use of the specified TACACS+ server. It can be used only for the specified purpose.

A TACACS+ server specified with the `auth-only` parameter is used as a server dedicated to authentication. A TACACS+ server specified with the `acct-only` parameter is used as a server dedicated to accounting.

1. Default value when this parameter is omitted:

   The TACACS+ server can be used for all purposes (authentication and accounting).

2. Range of values:

   None

Default behavior

Because the TACACS+ server is not configured, no TACACS+ communication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of four TACACS+ servers can be specified per device.
2. When multiple TACACS+ servers are specified, the TACACS+ server that is first in the configuration file listing is the first server used for authentication.

Related commands

```
tacacs-server key
tacacs-server timeout
aaa authentication login
aaa authorization commands
aaa accounting exec
aaa accounting commands
```

tacacs-server key

Sets the default shared private key of a TACACS+ server used for authentication or authorization purposes.

Syntax

To set or change information:

```
tacacs-server key <string>
```

To delete information:

```
no tacacs-server key
```

Input mode

```
(config)
```

Parameters

<*string*>

Specifies the shared private key used for encryption or authentication of communication with the TACACS+ server. The same shared private key must be set for the client and the TACACS+ server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `key` settings specific to the `tacacs-server host` command have priority over the settings for this command.

Related commands

```
tacacs-server host
tacacs-server timeout
aaa authentication login
aaa authorization commands
aaa accounting exec
aaa accounting commands
```

tacacs-server timeout

Sets the default response timeout value for a TACACS+ server used for authentication or authorization purposes.

Syntax

To set or change information:

```
tacacs-server timeout <seconds>
```

To delete information:

```
no tacacs-server timeout
```

Input mode

```
(config)
```

Parameters

<*seconds*>

Specifies the timeout period (in seconds) for a response from the TACACS+ server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 30

Default behavior

The default response timeout value for the TACACS+ server is 5 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `timeout settings specific to the tacacs-server host` command have priority over the settings for this command.

Related commands

```
tacacs-server host
tacacs-server key
aaa authentication login
aaa authorization commands
aaa accounting exec
aaa accounting commands
```

username

Sets the users who log in to the device. Each user's settings are activated when their user accounts are in the device.

In each device, a maximum of 100 users can be set in default_user that includes all users.

The following settings are made in the device:

- Creates a user account in the device and set the password.
- For a specified user, sets the command list or command class permitted by local command authorization.
- Also specifies the auto logout period for each user, paging, and help message display operation.
- Specifies the output conditions that determine when system messages appear on the screen by message types and event levels. The screen output conditions can be set only to default_user.

Syntax

To set information:

```
username <user name> [<user id>] [no-flash] password {input | hidden <hidden password>}
username <user name> exec-timeout <minutes>
username <user name> logging-console { message-list <group name> | event-level <event level> | message-list <group name> event-level <event level> }
username <user name> terminal-pager {enable | disable}
username <user name> terminal-help {all | no-utility}
username <user name> view <view name>
username <user name> view-class {root | allcommand | noconfig | noenable}
```

To change information:

```
username <user name> password {input | hidden <hidden password>}
username <user name> exec-timeout <minutes>
username <user name> logging-console { message-list <group name> | event-level <event level> | message-list <group name> event-level <event level> }
username <user name> terminal-pager {enable | disable}
username <user name> terminal-help {all | no-utility}
username <user name> view <view name>
username <user name> view-class {root | allcommand | noconfig | noenable}
```

To delete information:

```
no username <user name>
no username <user name> <user id>
no username <user name> exec-timeout
no username <user name> logging-console
no username <user name> terminal-pager
no username <user name> terminal-help
no username <user name> view
no username <user name> view-class
```

Input mode

```
(config)
```

Parameters

<user name>

Specifies the name of the user to be set.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a string with 16 or fewer characters. Alphabetic characters can be used for the first character, and alphanumeric characters can be used for the second and subsequent characters.

The following character strings used in the device cannot be specified:

root, toor, daemon, bin, games, postfix, named, ntpd, sshd, smmsp, uucp, nobody, admin, share, script

For `exec-timeout`, `terminal-pager`, `terminal-help`, or `logging-console`, you can specify `default_user`, and have the settings apply to all users. When `default_user` is specified, the settings apply only to users who are not specified using a specific user name.

<*user id*>

Specifies the user ID of the specified user.

Creates a user account in the device based on the specified user ID and manage the account. The user ID of the created user account cannot be changed. The same user ID cannot be assigned to multiple users.

1. Default value when this parameter is omitted:

The system automatically selects the smallest value from the unused user IDs.

2. Range of values:

Specify 100 to 199 in decimal.

no-flash

Creates the home directory of the specified user on the memory (`/home/`).

The home directory of the created user account cannot be changed.

1. Default value when this parameter is omitted:

Creates the home directory of a user account in internal flash memory (`/usr/home/`).

2. Range of values:

None

password {input | hidden <*hidden password*>}

Specifies the login password of the specified user.

input

Specifies the password in password input mode. The specified password will be automatically hashed and set to the configuration.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a string with 128 or fewer characters. Alphanumeric and special characters can be specified. For details, see *Any character string* in *Specifiable values for parameters*.

For security reasons, the password should contain 6 or more characters. We recommend that you use upper case alphabetic characters, numbers, and symbols in addition to lower case alphabetic characters. If fewer than six characters are entered

or only lower case alphabetic characters are used, an error is displayed. However, if the same string is specified again after an error is shown, that string can be set as the password.

hidden <*hidden password*>

Specifies a hashed password that was created by using the `make hidden-password` operation command, or a hashed password that was created in the configuration of another device. If a string other than a hashed password string is specified, the system fails to perform local password authentication and the user cannot log in

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a hashed password string with 100 characters, including double quotation marks (").

exec-timeout <*minutes*>

Specifies the auto-logout time (in minutes) of the specified user. If 0 is specified, auto-logout does not apply.

1. Default value when this parameter is omitted:

   60

2. Range of values:

   0 to 60

logging-console { message-list <*group name*> | event-level <*event level*> | message-list <*group name*> event-level <*event level*> }

Specifies the screen output conditions for system messages.

If `message-list` and `event-level` are specified in parallel, a system message that satisfies both condition will be displayed.

message-list <*group name*>

Specifies the system message to be displayed on the screen in the message type list. Generates the message type list by using the `message-list` command.

If a message type list that does not exist in <*group name*> or a message type list with no output conditions specified is specified, system messages of all message types are targets for being output to the screen.

If this parameter is not specified, system messages of all message types are targets for being output to the screen.

event-level <*event level*>

Specifies a value as the event level of the system message to be displayed on the screen. System messages whose event levels are the specified value or less are targets for being output to the screen.

If this parameter is not specified, system messages whose event level value is 6 or less are targets for being output to the screen.

1. Default value when this parameter is omitted:

   System messages whose event level value is 6 or less are targets for being output to the screen.

2. Range of values:

For <*group name*>, specify a name with 31 or fewer characters. For details, see *Specifiable values for parameters*.

Specify a value from 0 to 7 for <*event level*>.

terminal-pager {enable | disable}

Specifies whether to enable paging (messaging) of the specified user.

enable

Paging is performed.

disable

Paging is not performed.

1. Default value when this parameter is omitted:

   enable

2. Range of values:

   None

terminal-help {all | no-utility}

For the specified user, specifies what type of operation command help messages can be displayed.

all

Enables help messages for all permissible operation commands to be displayed.

no-utility

Enables help messages for all permissible operation commands except for utility commands and file operation commands to be displayed.

1. Default value when this parameter is omitted:

   all

2. Range of values:

   None

view <*view name*>

Specifies a command list generated by the `parser view` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name of no more than 31 characters.

   An alphabetical character can be specified for the first character of such name, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be specified for the subsequent characters.

   For details, see *Name of the Parameter type* column in the *Specifiable values for parameters* table.

view-class {root | allcommand | noconfig | noenable}

Specifies a command class to be assigned to a user.

Specifies one of the following command classes that have been defined in advance on the Device: `root`, `allcommand`, `noconfig`, and `noenable`. For details, see *Table 8-11 Command*

classes in the manual *Configuration Guide Vol. 1 For Version 12.1*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The screen output conditions for user accounts, passwords and system messages are applied immediately after the setting values are changed.

Other changed settings take effect from the next login.

Response messages

The following table describes the response messages for the `username` command.

Message	Description
Do you want to delete the user account <*user name*>? (y/n):	Deletes the specified user account. If the account of a currently logging-in user is deleted, the user is forcibly logged out and his or her home directory is deleted. Enter `y` to delete the account. Enter `n` to cancel the `username` command.

Notes

1. If a user account is created using the `no-flash` parameter, when the device is restarted, the command history of the history function and the files and directories in the home directory are cleared out.
2. The default user account ("username operator 100 password hidden """) provided during the initial installation can be deleted.
3. If the account of a currently logging-in user is deleted by using the `no username` <*user name*> command or `no user name` <*username*> <*user id*> command, the user is forcibly logged out. The deletion target user should be logged out by usng the `logout` or `exit` operation command in advance.
4. If a user account is deleted by using the `no username` <*user name*> command or `no user name` <*username*> <*user id*> command, the user's home directory is also deleted. If you want to keep the files, save them in `/usr/home/share` or back them up to an external device.
5. When `default_user` is specified, the settings apply only to users who are not specified using a specific user name. For example, when 0 is set as the `exec-timeout` value for `default_user`, if the `terminal-pager` or `terminal-help` parameter is set for the user name `staff`, the setting to be applied to user `staff` is 60, and this is set as the default value when the `exec-timeout` parameter is omitted.
6. The operations for each command can be changed temporarily for the current log-in session by using the `set exec-timeout`, `set terminal pager`, or `set terminal help` operation commands after the user has logged in.
7. The `logging-console` parameter can only be specified for `default_user`.

8. If the following message types are not included in system messages, and they are specified as the output targets, the message types in question will not be displayed on the screen.

   KEY, CONFIGERR, CMDRSP

9. If parameters following `no username` <*user name*> are not specified when deleting a configuration, all parameters specified in `username` <*user name*> are deleted.

Related commands

`aaa authorization commands`
`parser view`
`commands exec`
`message-list`
`message-type`

Chapter

7. Time Settings and NTP/SNTP

clock summer-time
clock timezone
ntp access-group
ntp authenticate
ntp authentication-key
ntp broadcast
ntp broadcast client
ntp broadcastdelay
ntp master
ntp peer
ntp server
ntp trusted-key
sntp access-group
sntp authenticate
sntp authentication-key
sntp broadcast
sntp broadcast client
sntp broadcastdelay
sntp broadcast send-interval
sntp client interval
sntp master
sntp server
sntp trusted-key

clock summer-time

Sets the summer time period.

Syntax

To set or change information:

```
clock summer-time <zone name> [recurring <month> <week> { sun | mon | tue |
wed | thu | fri | sat } <hhmm> <month> <week> { sun | mon | tue | wed | thu
| fri | sat } <hhmm>] [offset <minute>]
```

To delete information:

```
no clock summer-time
```

Input mode

```
(config)
```

Parameters

<*zone name*>

Specifies the name used to identify a time zone.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A maximum of seven alphanumeric characters

recurring <*month*> <*week*> { sun | mon | tue | wed | thu | fri | sat} <*hhmm*>

Specifies the summer time start day.

<*month*>

Specifies the summer time start month.

<*week*>

Specifies the summer time start week. The first day of the month is considered the first day of the week. Specify the week number in which it begins.

{ sun | mon | tue | wed | thu | fri | sat }

Specifies a day of the week (from sun to sat) to start summer time.

<*hhmm*>

Specifies the summer time start time. Specify the hour as *hh* and minute as *mm*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*month*>, specify a value from 1 to 12.

   For <*week*>, specify a value from 1 to 5.

   Specify a number from 00 to 23 as *hh* and 00 to 59 as *mm* in <*hhmm*>.

<*month*> <*week*> { sun | mon | tue | wed | thu | fri | sat } <*hhmm*>

Specifies the summer time end day.

<*month*>

Specifies the summer time end month.

<*week*>

Specifies the summer time end week. The first day of the month is considered as first day of the week. Specify the week number in which it ends.

{ sun | mon | tue | wed | thu | fri | sat }

Specifies a day of the week (from sun to sat) to end summer time.

<*hhmm*>

Specifies the summer time end time. Specify the hour as *hh* and minute as *mm*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*month*>, specify a value from 1 to 12.

   For <*week*>, specify a value from 1 to 5.

   Specify a number from 00 to 23 as *hh* and 00 to 59 as *mm* in <*hhmm*>.

offset <*minutes*>

Specifies the time difference from the other time period in unites of minutes. A negative value indicates that the period is earlier, and a positive value indicates that the period is later.

1. Default value when this parameter is omitted:

   Sets the offset value to 60.

2. Range of values:

   -1440 to -1, or 1 to 1440

Default behavior

No summer time is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The start date and time and end date and time must not be the same.
2. The summer time setting is immediately applied in the system if the start and end date and time are omitted.
3. If a day in the 5th week is specified as the start or end date in a month that has only 4 weeks, the first day of the 4th week is used as the start or end date.

Related commands

`clock timezone`

clock timezone

Sets the time zone.

The Device maintains the date and time internally in Coordinated Universal Time (UTC). This clock timezone setting affects only the time that is set using the `set clock` command, and the time that is displayed by using an operation command.

Syntax

To set or change information:

```
clock timezone <zone name> <hours offset> [<minutes offset>]
```

To delete information:

```
no clock timezone
```

Input mode

```
(config)
```

Parameters

<zone name>

Specifies the name used to identify a time zone.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A maximum of seven alphanumeric characters

<hours offset>

Specifies the offset from UTC in hours as a decimal integer.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   -12 to -1, 0, and 1 to 12 (hours)

<minutes offset>

Specifies the offset from UTC in minutes as a decimal integer.

1. Default value when this parameter is omitted:

   0

2. Range of values:

   0 to 59 (minutes)

Default behavior

UTC is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

`clock summer-time`

ntp access-group

Creates an access group that can be permitted or denied access to NTP services by means of an IPv4 address filter. This command allows you to set a maximum of 2048 filter criteria entries for an access list.

Syntax

To set information:

```
ntp access-group {query-only | serve-only | serve | peer} <access list name>
[vrf {<vrf id> | all}]
```

To delete information:

```
no ntp access-group {query-only | serve-only | serve | peer} [vrf {<vrf id>
| all}]
```

Input mode

```
(config)
```

Parameters

{query-only | serve-only | serve | peer}

Sets the mode in which NTP services are used.

query-only

Only NTP control queries are permitted.

serve-only

NTP control queries and NTP broadcast messages are not permitted.

serve

NTP broadcast messages are not permitted.

peer

All accesses to NTP services are permitted.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<*access list name*>

Specifies the name of an access list that specifies IPv4 addresses that are permitted or denied access to the NTP service.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with 31 or fewer characters.

   For details, see *Specifiable values for parameters*.

vrf {<*vrf id*> | all}

<*vrf id*>

Specifies the VRF to which the IPv4 address filter is applied.

all

Specifies all VRFs including the global network.

1. Default value when this parameter is omitted:

   The specified address filter is applied to the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

Default behavior

All accesses to NTP services are permitted.

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `ntp peer` command, `ntp server` command, `ntp master` command, or `ntp broadcast client` command and an IPv4 address filter are set.

Notes

1. Access lists specified by this command are not subject to implicit discard entries.
2. If at least one access group is created for either a VRF instance or the global network, any access attempts with source IP addresses that do not match the specified access list are denied.
3. When the source IP address matches access lists for multiple access types, access type keywords are applied according to the following priority:

   `peer` -> `serve` -> `serve-only` -> `query-only`
4. If an access group is set in the global network, access group settings made by specifying the `vrf all` parameter are not applied to the global network. If an access group that separately specified a VRF is set in a VRF, access group settings made by specifying the `vrf all` parameter are not applied.

Related commands

```
ntp peer
ntp server
ip access-list standard
```

ntp authenticate

Enables the NTP authentication functionality.

Syntax

To set information:

```
ntp authenticate
```

To delete information:

```
no ntp authenticate
```

Input mode

```
(config)
```

Parameters

None

Default behavior

Disables the NTP authentication functionality.

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `ntp peer` command, `ntp server` command, `ntp master` command, or `ntp broadcast client` command is set.

Notes

None

Related commands

```
ntp authentication-key
ntp trusted-key
```

ntp authentication-key

Sets an authentication key. This command can set a maximum of 10 authentication key entries.

Syntax

To set or change information:

```
ntp authentication-key <key id> md5 <value>
```

To delete information:

```
no ntp authentication-key <key id>
```

Input mode

```
(config)
```

Parameters

<*key id*>

Specifies the key number in decimal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

md5 <*value*>

Specifies a value to be assigned to an authentication key.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify by using 30 or fewer alphanumeric and special characters. For details, see *Any character string* in *Specifiable values for parameters*. However, you cannot use the following characters:

   A space character, ampersand (&), left parenthesis ((), right parenthesis ()), left chevron (<), right chevron (>), left square bracket ([), right square bracket (]), or pipe (|)

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `ntp peer` command, `ntp server` command, `ntp master` command, or `ntp broadcast client` command is set.

Notes

1. For some destination devices, the range of available authentication keys might be less than 32 bits. In this case, set the value of the key to be used to a value within the valid range of the destination device.

Related commands

```
ntp peer
```

```
ntp server
ntp master
ntp authenticate
ntp trusted-key
ntp broadcast client
```

ntp broadcast

Broadcasts NTP packets to each interface and synchronizes other devices with the Device.

This command can be used together with the `ntp peer` and `ntp server` commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

```
ntp broadcast [version <number>] [key <key id>]
```

To delete information:

```
no ntp broadcast
```

Input mode

`(config-if)`

Ethernet interface or port channel interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

version <*number*>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified.

2. Range of values:

   1, 2, 3, or 4

key <*key id*>

Specifies the authentication key for access. Specifies key as the number (in decimal) set for `authentication-key`.

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `ntp peer` command, `ntp server` command, `ntp master` command, or `ntp broadcast client` command is set.

Notes

1. This functionality can use IPv4 only.

2. If no IPv4 addresses are set for an interface, no NTP broadcast packets are sent.
3. To change the IPv4 address settings of an interface, delete the `ntp broadcast` setting first.

Related commands

```
ntp broadcast client
ntp authentication-key
```

ntp broadcast client

Specifies the settings for accepting NTP broadcast messages from devices on the connected subnet. This setting enables the Device to receive NTP broadcast messages from other devices and synchronize its time with that of other devices. When this command is omitted, no NTP broadcast messages are accepted.

Syntax

To set information:

```
ntp broadcast client
```

To delete information:

```
no ntp broadcast client
```

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ntp broadcast
```

ntp broadcastdelay

Specifies the estimated latency (time delay) between the NTP broadcast server and the Device.

Syntax

To set or change information:

```
ntp broadcastdelay <micro seconds>
```

To delete information:

```
no ntp broadcastdelay
```

Input mode

```
(config)
```

Parameters

<micro seconds>

Specifies a delay time. The time is set as a decimal integer in microseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 999999

Default behavior

4000 microseconds are set as the delay time of the NTP broadcast server.

Impact on communication

None

When the change is applied

When the `ntp broadcast client` command is set, the changes take effect immediately after the setting values are changed.

Notes

None

Related commands

```
ntp broadcast client
```

ntp master

Designates the device as a local time server. Performs this setting if a reference NTP server cannot be accessed from the network to which the Device is normally connected.

Syntax

To set or change information:

```
ntp master [<stratum>]
```

To delete information:

```
no ntp master
```

Input mode

```
(config)
```

Parameters

<*stratum*>

Specifies the stratum value in decimal.

1. Default value when this parameter is omitted:

   8

2. Range of values:

   1 to 15

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you use the Device as an NTP server, and 10 or more clients are to be synchronized, synchronization might be temporarily disabled. Although the Device functionality is not affected even if the number of clients to be synchronized exceeds 10, consider your environment when deciding the number of clients.

Related commands

```
ntp peer
ntp server
```

ntp peer

Sets NTP server symmetric active/passive mode. In symmetric active/passive mode, the time of the Device can be synchronized with that of other devices, and vice versa.

This command can be used together with the `ntp broadcast` and `ntp server` commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

```
ntp peer [vrf <vrf id>] <ip address> [version <number>] [key <key id>]
[prefer]
```

To delete information:

```
no ntp peer [vrf <vrf id>] <ip address>
```

Input mode

```
(config)
```

Parameters

vrf <*vrf id*>

Specifies the VRF of an NTP time reference source (server) or an NTP client.

1. Default value when this parameter is omitted:

   Belongs to the global network.

2. Range of values:

   Specify a VRF ID.

   For details, see *Specifiable values for parameters*.

<*ip address*>

Specifies the IPv4 address of an NTP time reference source (server) or an NTP client.

version <*number*>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified.

2. Range of values:

   1, 2, 3, or 4

key <*key id*>

Specifies the authentication key for access. Specify this key as the number (in decimal) that is set for `authentication-key`.

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

prefer

When multiple time reference source devices are specified, a device with the `prefer` parameter specified takes priority.

1. Default value when this parameter is omitted:

   No priorities are set.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there is a 1000 second (about 16 minute) or longer difference between the time of a time reference source (server) device and the time of this (client) Device, the specified device time is treated as invalid (not reconcilable) and it is not synchronized. If the time of the time-reference synchronization-source device is correct, use the `set clock` operation command to synchronize the time of this Device with the time of the time-reference synchronization-source device.
2. In a configuration where this Device references multiple time-reference synchronization-source devices, if there is a 16 second or longer time difference between the time references, synchronization of this Device (that references the other devices) will succeed, but any devices that reference this Device will not be synchronized. Make sure the time of specified time-reference synchronization-source devices is correct.
3. If the Device and other devices are configured in symmetric active/passive mode, it might take a very long time to synchronize these devices. If this happens, we recommend that you reduce the number of devices in the configuration.
4. When a device references multiple time-reference synchronization-source devices, if the time of a high-priority synchronization-source device moves outside of the synchronization range (a 1000 second or longer time difference), other synchronization-source devices will be used as the time reference. If this situation is not fixed, synchronization with the other devices might also be lost. You can change the settings to manually disable the synchronization-source designation of the device whose time has moved out of the valid range. Another solution in this case is to manually reset the time of such a device to the correct value, and synchronization will be recovered.
5. If the IP address of a device is configured as its loopback interface, use the IP address of the loopback interface as the source IP address for sending NTP packets. Therefore, if you set the Device as the synchronization source or destination, specify the IP address of the loopback interface as the IP address of the Device. When adding, changing, or deleting the IP address of the loopback interface, use the `restart ntp` operation command to re-initialize the ntp program.

Related commands

```
ntp server
ntp authentication-key
```

ntp server

Sets client/server mode and specifies client mode for an NTP server. As a result, the time of the Device is synchronized to that of a time server. The time of this Device can be synchronized to that of another device, but the time of another device cannot be synchronized to that of this Device.

This command can be used together with `ntp broadcast` and `ntp peer` commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

```
ntp server [vrf <vrf id>] <ip address> [version <number>] [key <key id>]
[prefer]
```

To delete information:

```
no ntp server [vrf <vrf id>] <ip address>
```

Input mode

```
(config)
```

Parameters

vrf <*vrf id*>

Specifies the VRF to which the Device whose time is to be synchronized belongs.

1. Default value when this parameter is omitted:

   Belongs to the global network.

2. Range of values:

   Specify a VRF ID.

   For details, see *Specifiable values for parameters*.

<*ip address*>

Specifies the IPv4 address of a Device whose time is to be synchronized.

version <*number*>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified.

2. Range of values:

   1, 2, 3, or 4

key <*key id*>

Specifies the authentication key for access. Specify this key as the number (in decimal) that is set for `authentication-key`.

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

prefer

When multiple time reference source devices are specified, devices with the `prefer`

parameter specified take priority.

1. Default value when this parameter is omitted:

   No priorities are set.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there is a 1000 second (about 16 minute) or longer difference between the time of a time reference source (server) device and the time of this (client) Device, the specified device time is treated as invalid (not reconcilable) and it is not synchronized. If the time of the time-reference synchronization-source device is correct, use the `set clock` operation command to synchronize the time of this Device to the time of the time-reference synchronization-source device.
2. In a configuration where this Device references multiple time-reference synchronization-source devices, if there is a 16 second or longer time difference between the time references, synchronization of this Device (that references the other devices) will succeed, but any devices that reference this Device will not be synchronized. Make sure the time of specified time-reference synchronization-source devices is correct.
3. If the IP address of a device is configured as its loopback interface, use the IP address of the loopback interface as the source IP address for sending NTP packets. Therefore, if you set the Device as the synchronization source or destination, specify the IP address of the loopback interface as the IP address of the Device. When adding, changing, or deleting the IP address of the loopback interface, use the `restart ntp` operation command to re-initialize the ntp program.

Related commands

```
ntp peer
ntp authentication-key
```

ntp trusted-key

Sets a key number to perform authentication for security purposes when synchronizing with other devices. By default, the key to be used for authentication is not set.

This command can be used to set a maximum of 10 key number entries.

Syntax

To set information:

```
ntp trusted-key <key id>
```

To delete information:

```
no ntp trusted-key <key id>
```

Input mode

```
(config)
```

Parameters

<key id>

Specifies the key number to be used for authentication. For this key, the number (in decimal) set by using `authentication-key` is specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `ntp peer` command, `ntp server` command, `ntp master` command, or `ntp broadcast client` command is set.

Notes

None

Related commands

```
ntp authenticate
ntp authentication-key
```

sntp access-group

Creates an access group that can be permitted or denied access to SNTP services by means of an IPv4 address filter or IPv6 address filter.

This command allows you to set a maximum of 2048 filter criteria entries for an access list.

Syntax

To set or change information:

```
sntp access-group {serve | peer} <access list name> [vrf {<vrf id> | all}]
```

To delete information:

```
no sntp access-group {serve | peer} <access list name> [vrf {<vrf id> | all}]
```

Input mode

```
(config)
```

Parameters

{serve | peer}

Sets the mode in which SNTP services are used.

serve

SNTP broadcast messages are not permitted.

peer

All accesses to SNTP services are permitted.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<access list name>

Specifies the name of an access list that specifies IPv4 addresses or IPv6 addresses which are permitted or denied access to the SNTP service.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with 31 or fewer characters.

   For details, see *Specifiable values for parameters*.

vrf {*<vrf id>* | all}

<vrf id>

Specifies the VRF to which an IPv4 address filter or IPv6 address filter is applied.

all

Specifies all VRFs including the global network.

1. Default value when this parameter is omitted:

   The specified address filter is applied to the global network.

2. Range of values:

For <*vrf id*>, specify a VRF ID.

For details, see *Specifiable values for parameters*.

Default behavior

All accesses to SNTP services are permitted.

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `sntp server` command, `sntp master` command, or `sntp broadcast client` command and an IPv4 address filter or IPv6 address filter are set.

Notes

1. When the source IPv4 or IPv6 address matches access lists for multiple access types, peer is preferentially applied as an access type keyword. If multiple access lists with the same keyword are set, it is applied in the order they were set.
2. If an access list was set to <*access list name*> with the `ip access-list standard` command, it is not applied to IPv6 addresses. If an access list was set to <*access list name*> with the `ipv6 access-list` command, it is not applied to IPv4 addresses.
3. If an access group is set in the global network, access group settings made by specifying the `vrf all` parameter are not applied to the global network. If an access group that separately specified a VRF is set in a VRF, access group settings made by specifying the `vrf all` parameter are not applied.
4. The source IPv6 address specification is enabled but the rest of access lists set with the `ipv6 access-list` command are ignored. Parameters other than the source IPv6 address are not applied.

Related commands

```
sntp server
ip access-list standard
ipv6 access-list
```

sntp authenticate

Enables the SNTP authentication functionality.

Syntax

To set information:

```
sntp authenticate
```

To delete information:

```
no sntp authenticate
```

Input mode

```
(config)
```

Parameters

None

Default behavior

The SNTP authentication functionality is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `sntp server` command, `sntp master` command, or `sntp broadcast client` command is set.

Notes

None

Related commands

```
sntp authentication-key
sntp trusted-key
```

sntp authentication-key

Sets an authentication key. This command can set a maximum of three authentication key entries.

Syntax

To set or change information:

```
sntp authentication-key <key id> md5 <value>
```

To delete information:

```
no sntp authentication-key <key id>
```

Input mode

```
(config)
```

Parameters

<key id>

Specifies the key number in decimal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

md5 *<value>*

Specifies a value to be assigned to an authentication key.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify by using 30 or fewer alphanumeric and special characters. For details, see *Any character string* in *Specifiable values for parameters*. However, you cannot use the following characters:

   A space character, ampersand (&), left parenthesis ((), right parenthesis ()), left chevron (<), right chevron (>), left square bracket ([), right square bracket (]), or pipe (|)

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `sntp server` command, `sntp master` command, or `sntp broadcast client` command is set.

Notes

1. For some destination devices, the range of available authentication keys might be less than 32 bits. In this case, set the value of a key to use to a value within the valid range of the destination device.

Related commands

```
sntp server
```

```
sntp master
sntp authenticate
sntp trusted-key
sntp broadcast client
```

sntp broadcast

Sends SNTP packets via IPv4 broadcast or IPv6 multicast for each interface so that other devices will synchronize with the Device.

This command can set a maximum of 4096 entries.

Syntax

To set or change information:

```
sntp broadcast { ip | ipv6 }[version <number>] [key <key id>]
```

To delete information:

```
no sntp broadcast { ip | ipv6 }
```

Input mode

`(config-if)`

Ethernet interface or port channel interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

{ ip | ipv6 }

Specifies the address family of the SNTP packets to be sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

version <*number*>

Specifies the SNTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified.

2. Range of values:

   1, 2, 3, or 4

key <*key id*>

Specifies the authentication key for access. Specify `key` as the number (in decimal) set for `authentication-key`.

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `sntp server` command, `sntp master` command, or `sntp broadcast client` command is set.

Notes

1. To change IPv4 address or IPv6 address settings of an interface, delete the `sntp broadcast` setting first.

Related commands

```
sntp broadcast client
sntp authentication-key
```

sntp broadcast client

Specifies the setting for accepting SNTP broadcast or multicast messages from devices on the connected subnet. This setting enables the Device to receive SNTP broadcast or SNTP multicast messages from other devices and synchronize its time with that of other devices.

Syntax

To set information:

```
sntp broadcast client
```

To delete information:

```
no sntp broadcast client
```

Input mode

```
(config)
```

Parameters

None

Default behavior

Does not accept SNTP broadcast or multicast messages from devices on the connected subnet.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If both the `sntp server` and `sntp broadcast client` commands are set, the `sntp server` command is prioritized.

Related commands

```
sntp broadcast
sntp broadcastdelay
```

sntp broadcastdelay

Specifies the estimated latency (time delay) between the SNTP broadcast server and the Device.

Syntax

To set or change information:

```
sntp broadcastdelay <micro seconds>
```

To delete information:

```
no sntp broadcastdelay
```

Input mode

```
(config)
```

Parameters

<*micro seconds*>

The latency (time delay) is set as a decimal integer in microseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 999999

Default behavior

4000 microseconds are set as the delay time of the SNTP broadcast server.

Impact on communication

None

When the change is applied

1. When the `sntp broadcast client` command is set, the change takes effect immediately after the setting values are changed.

Notes

None

Related commands

```
sntp broadcast client
```

sntp broadcast send-interval

Sets the interval for sending SNTP packets via IPv4 broadcast or IPv6 multicast.

Syntax

To set or change information:

```
sntp broadcast send-interval <seconds>
```

To delete information:

```
no sntp broadcast send-interval
```

Input mode

```
(config)
```

Parameters

<*seconds*>

Specifies the polling interval in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   16 to 604800

Default behavior

Sends SNTP packets in intervals of 600 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
sntp broadcast
```

sntp client interval

Sets the interval for periodically getting time information from an SNTP server.

Syntax

To set or change information:

```
sntp client interval <seconds>
```

To delete information:

```
no sntp client interval
```

Input mode

```
(config)
```

Parameters

<seconds>

Specifies the polling interval in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   16 to 604800

Default behavior

Obtains time information from an SNTP server in intervals of 600 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
sntp server
sntp master
```

sntp master

Designates the device as a local time server. Performs this setting if a reference SNTP server cannot be accessed from the network to which the Device is normally connected.

Syntax

To set information:

```
sntp master
```

To delete information:

```
no sntp master
```

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
sntp server
```

sntp server

Sets client/server mode and specifies client mode for an SNTP server. As a result, the time of this Device is synchronized to that of a time server. The time of this Device can be synchronized to that of another device, but the time of another device cannot be synchronized to that of this Device.

This command can set a maximum of three entries.

Syntax

To set or change information:

```
sntp server [vrf <vrf id>] {<ip address> | <ipv6 address>} [version <number>]
[key <key id>] [priority <priority>]
```

To delete information:

```
no sntp server [vrf <vrf id>] {<ip address> | <ipv6 address>}
```

Input mode

```
(config)
```

Parameters

vrf <*vrf id*>

Specifies the VRF to which the Device whose time is to be synchronized belongs.

1. Default value when this parameter is omitted:

   Belongs to the global network.

2. Range of values:

   Specify a VRF ID.

   For details, see *Specifiable values for parameters*.

{<*ip address*> | <*ipv6 address*>}

Specifies the IPv4 address or IPv6 address of a Device whose time is to be synchronized.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*ip address*>, specify an IPv4 address.

   For <*ipv6 address*>, specify an IPv6 address.

version <*number*>

Specifies the SNTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified.

2. Range of values:

   1, 2, 3, or 4

key <*key id*>

Specifies the authentication key for access. Specifies this key as the number (in decimal) set for `authentication-key`.

1. Default value when this parameter is omitted:

No authentication keys are specified.

2. Range of values:

   1 to 65535

priority <*priority*>

Specifies the priority for determining the synchronization order.

If multiple SNTP servers are set as synchronization candidates, it attempts to synchronize with them in the order of priority. If the priority is the same, it attempts to synchronize with a SNTP server that synchronized with the Device earlier.

The greater the value, the higher the priority.

1. Default value when this parameter is omitted:

   1

2. Range of values:

   1 to 100

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there is a 1000 second (about 16 minute) or longer difference between the time of a time reference source (server) device and the time of this (client) Device, the specified device time is treated as invalid (not reconcilable) and it is not synchronized. If the time of the time-reference synchronization-source device is correct, use the `set clock` operation command to synchronize the time of this Device with the time of the time-reference synchronization-source device.
2. If it synchronizes with an SNTP server, it preferentially synchronizes with the SNTP server until the connection is cut. However, if there is another SNTP server with higher priority than the SNTP sever, it first attempts to synchronize with the SNTP server with higher priority from the next time.
3. If the IP address of a device is configured as its loopback interface, use the IP address of the loopback interface as the source IP address for sending SNTP packets. Therefore, if you set the Device as the synchronization source or destination, specify the IP address of the loopback interface as the IP address of the Device. When adding, changing, or deleting the IP address of the loopback interface, use the `restart sntp` operation command to re-initialize the sntp program.
4. If both the `sntp server` and `sntp broadcast client` commands are set, the `sntp server` command is prioritized.

Related commands

`sntp authentication-key`

sntp trusted-key

Sets a key number to perform authentication for security purposes when synchronizing with other devices. By default, the key to be used for authentication is not set.

This command can be used to set a maximum of three key number entries.

Syntax

To set or change information:

```
sntp trusted-key <key id>
```

To delete information:

```
no sntp trusted-key <key id>
```

Input mode

```
(config)
```

Parameters

<key id>

Specifies the key number to be used for authentication. For this key, the number (in decimal) set by using `authentication-key` is specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting values are changed if the `sntp server` command, `sntp master` command, or `sntp broadcast client` command is set.

Notes

None

Related commands

```
sntp authenticate
sntp authentication-key
```

Chapter

8. Host Names and DNS

ip domain lookup
ip domain name
ip domain reverse-lookup
ip host
ip name-server
ipv6 host

ip domain lookup

Disables the DNS resolver functionality by using the no ip domain lookup command.

Syntax

To set information:

```
no ip domain lookup
```

To delete information:

```
ip domain lookup
```

Input mode

```
(config)
```

Parameters

None

Default behavior

The DNS resolver functionality is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
hostname
ip domain name
ip name-server
```

ip domain name

Sets the domain name to be used by the DNS resolver.

Syntax

To set or change information:

```
ip domain name <domain name>
```

To delete information:

```
no ip domain name
```

Input mode

```
(config)
```

Parameters

<domain name>

Sets the domain name for the Device.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the name with 63 or fewer characters. For details about the characters that can be specified, see *Specifiable values for parameters*. Note that underscores (_) cannot be used.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

If `no ip domain lookup` is set, the change is applied to the operation after `ip domain lookup` is entered.

Notes

1. Only one domain name can be set for the Device.

Related commands

```
hostname
ip name-server
ip domain lookup
```

ip domain reverse-lookup

Disables the reverse lookup functionality (functionality for using an IP address to search for a host name) of the DNS resolver functionality by using the `no ip domain reverse-lookup` command.

Syntax

To set information:

```
no ip domain reverse-lookup
```

To delete information:

```
ip domain reverse-lookup
```

Input mode

```
(config)
```

Parameters

None

Default behavior

When the DNS resolver functionality is enabled, the reverse lookup functionality is also enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the DNS resolver functionality is disabled, it does not operate, regardless of this setting.
2. If the reverse lookup functionality of the DNS resolver functionality is disabled by this setting, the host name might not be displayed by the `traceroute` and `show ntp associations` operation commands.

Related commands

```
ip domain lookup
ip domain name
ip name-server
```

ip host

Sets the host name information mapped to an IPv4 address. This command can configure a maximum of 20 entries.

Syntax

To set or change information:

```
ip host <name> <ip address>
```

To delete information:

```
no ip host <name>
```

Input mode

```
(config)
```

Parameters

<name>

Specifies a host name to be assigned to an IPv4 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the host name with 63 or fewer characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

<ip address>

Specifies the IPv4 address of a device for which a host name is set.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. `localhost` cannot be set as a host name.
2. `127.*.*.*` cannot be set as an IPv4 address.
3. Class D or class E IPv4 addresses cannot be set.
4. Host names are not case sensitive.
5. If the same host name is specified for the `ip host` command and the `ipv6 host` command, the `ip host` command takes priority.

Related commands

```
ipv6 host
```

ip name-server

Sets the name server referenced by the DNS resolver. A maximum of three name servers can be specified. If multiple name servers are specified, inquiries to the name servers are performed in the order in which they were set. Because the DNS resolver functionality is enabled by default, it works as soon as the name server has been set.

Syntax

To set information:

```
ip name-server {<ip address>|<ipv6 address>}
```

To delete information:

```
no ip name-server {<ip address>|<ipv6 address>}
```

Input mode

```
(config)
```

Parameters

{<*ip address*>|<*ipv6 address*>}

Specifies the IPv4 or IPv6 address of the name server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*ip address*>, specify the IPv4 address of the name server.

   For <*ipv6 address*>, specify the IPv6 address of the name server.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

If `no ip domain lookup` is set, the change is applied to the operation after `ip domain lookup` is entered.

Notes

1. Set the IP address (`ip name-server`) of the DNS server correctly. If the IP address of a DNS server is not set correctly, it might take time until a communication failure with the DNS server is detected when a host name is referenced, and the operation might be affected (Example: It takes time until the login prompt appears when a remote connection is established from another device to the Device via Telnet).
2. `127.*.*.*` cannot be specified as an IP address.
3. Class D and class E addresses cannot be set as IP addresses.
4. No internal loopback address can be set as an IPv6 address.
5. No multicast address can be set as an IPv6 address.
6. If both AAAA query and A query are referenced, AAAA query is prioritized.

Related commands

```
ip domain name
ip domain lookup
```

ipv6 host

Sets the host name information mapped to an IPv6 address. This command can configure a maximum of 20 entries.

Syntax

To set or change information:

```
ipv6 host <name> <ipv6 address>
```

To delete information:

```
no ipv6 host <name>
```

Input mode

```
(config)
```

Parameters

<name>

Specifies a host name to be assigned to an IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the host name with 63 or fewer characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

<ipv6 address>

Specifies the IPv6 address of a device for which a host name is set.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. `localhost` cannot be set as a host name.
2. Host names are not case sensitive.
3. If the same host name is specified for the `ipv6 host` command and the `ip host` command, the `ip host` command takes priority.

Related commands

```
ip host
```

Chapter

9. Device Management

flow detection mode
flow-table allocation
forwarding-table allocation
hardware profile
hostname
system fan mode
system high-temperature-action
system temperature-warning-level
system temperature-warning-level average

flow detection mode

Sets the flow detection mode for the filter and QoS functionality.

The maximum numbers of entries for the filter and the QoS flow functionality per PRU are determined with this command, the `flow-table allocation` command, and the `hardware profile` command.

Syntax

To set or change information:

```
flow detection mode {condition-oriented | quantity-oriented}
```

Input mode

```
(config)
```

Parameters

{condition-oriented | quantity-oriented}

Specifies the flow detection mode.

condition-oriented

Specifies condition oriented mode.

quantity-oriented

Specifies quantity oriented mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Operates in quantity oriented mode.

Impact on communication

None

When the change is applied

The change is applied by restarting PRU after the setting values are changed.

Notes

1. If quantity oriented mode is specified, delete the `advance access-group` command and `advance qos-flow-group` command settings.
2. To change flow detection mode, the number of setting entries must not exceed the capacity limit of the flow detection mode.

Related commands

```
advance access-group
advance qos-flow-group
flow-table allocation
hardware profile
```

flow-table allocation

Sets the flow allocation patterns for the filter and QoS flow functionality.

This command changes the allocation of the maximum numbers of entries for the filter and QoS flow functionality per PRU. By changing the allocation pattern according to the operating mode, you can concentrate resources on the necessary functionality.

The maximum numbers of entries for the filter and the QoS flow functionality per PRU are determined with this command, the `flow detection mode` command, and the `hardware profile` command.

Syntax

To set or change information:

```
flow-table allocation {default | filter | filter-only | qos | qos-only}
```

Input mode

```
(config)
```

Parameters

{default | filter | filter-only | qos | qos-only}

Specifies the flow allocation pattern.

default

Specifies the 50-50 allocation pattern for the filter and QoS flow.

filter

Specifies the allocation pattern that increases the maximum entries of the filter.

filter-only

Specifies the pattern that allocates all available entries to the filter.

qos

Specifies the allocation pattern that increases the maximum entries of the QoS flow.

qos-only

Specifies the pattern that allocates all available entries to the QoS flow.

For details about the flow allocation pattern, see *3.2 Capacity limits* in the manual *Configuration Guide Vol. 1 For Version 12.1*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The flow allocation pattern is activated by default.

Impact on communication

None

When the change is applied

The change is applied by restarting PRU after the setting values are changed.

Notes

1. To change the flow allocation pattern, the number of setting entries must not exceed the capacity limit of the flow allocation pattern.

Related commands

```
flow detection mode
hardware profile
```

forwarding-table allocation

Sets the allocation pattern of the maximum numbers of entries per device for the IPv4 unicast route, IPv4 multicast route, IPv6 unicast route, IPv6 multicast route, ARP entries, and NDP entries. This setting enables you to assign optimal numbers of entries to each aspect according to your operational status.

Sets this command and the `hardware profile` command to change the allocation of the maximum numbers of entries for unicast and multicast per PRU. By changing the allocation pattern according to the operating mode, you can concentrate resources on the necessary functionality.

Syntax

To set or change information:

```
forwarding-table allocation {default | ipv4-uni | ipv6-uni}
```

Input mode

```
(config)
```

Parameters

{default | ipv4-uni | ipv6-uni}

Specifies the allocation pattern for the IPv4 unicast route, IPv4 multicast route, IPv6 unicast route, IPv6 multicast route, ARP entries, and NDP entries.

default

Sets the allocation pattern that allocates entries to all routes and ARP/NDP entries.

ipv4-uni

Sets the allocation pattern that allocates entries only to the IPv4 unicast route and ARP entries.

ipv6-uni

Sets the allocation pattern that allocates entries only to the IPv6 unicast route and NDP entries.

For details about the route allocation patterns, see *3.2 Capacity limits* in the manual *Configuration Guide Vol. 1 For Version 12.1*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The route allocation pattern is activated by default.

Impact on communication

None

When the change is applied

The change is applied by restarting PRU after the setting values are changed.

Notes

1. If you use this parameter, some protocols (functions) have no entries, depending on the allocation pattern set (for example, the IPv4 multicast route for ipv6-uni and IPv6 multicast

route). In this case, communication is not possible, even if these protocols (functionalities) are configured.

2. To change the allocation pattern, the number of setting entries must not exceed the capacity limit of the route table entry allocation pattern.

Related commands

`hardware profile`

hardware profile

Sets the hardware profile.

Syntax

To set or change information:

```
hardware profile router-1
```

Input mode

```
(config)
```

Parameters

router-1

Specifies the hardware profile route-1.

This hardware profile can accommodate 2097152 (2 M) route entries and 131072 (128 K) flow entries.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the settings are set.

Notes

None

Related commands

```
forwarding-table allocation
flow-table allocation
```

hostname

Sets the identification name of a Device.

This name can be changed from the SNMP manager by using the Set operation of SNMP. If this name is changed by the `Set` operation of SNMP, the name is applied to the configuration.

Syntax

To set or change information:

```
hostname <name>
```

To delete information:

```
no hostname
```

Input mode

```
(config)
```

Parameters

<*name*>

The identification name of a Device. Set a name that is unique in the network that will be used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

No identification name is initially set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ip domain lookup
```

system fan mode

Sets the operating mode of the fan.

Syntax

To set or change information:

```
system fan mode <mode>
```

To delete information:

```
no system fan mode
```

Input mode

```
(config)
```

Parameters

<*mode*>

Sets the operating mode of the fan.

1: Normal mode

2: Low-temperature mode

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 or 2

Default behavior

1: Normal mode is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system high-temperature-action

Sets the operation mode of BCU for when the inlet air temperature of BCU exceeds the operation guarantee temperature.

Syntax

To set or change information:

```
system high-temperature-action { stop | no-stop }
```

To delete information:

```
no system high-temperature-action
```

Input mode

```
(config)
```

Parameters

{ stop | no-stop }

stop

If the inlet air temperature of BCU exceeds the operation guarantee temperature, BCU stops.

no-stop

If the inlet air temperature of BCU exceeds the operation guarantee temperature, BCU continues operation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

If the inlet air temperature of BCU exceeds the operation guarantee temperature, BCU stops.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the temperature of the BCU mounted in the device is abnormal for 10 or more minutes, the BCU is terminated regardless of the inlet air temperature of the device.
2. If operation continues under abnormal temperature when no-stop is specified as the parameter of this command, change the parameter to stop then the BCU stops immediately.

Related commands

None

system temperature-warning-level

Outputs a system message when the intake temperature of the device reaches or exceeds the specified temperature. If the inlet air temperature of the device goes down by 3 or more degrees Celsius from the specified temperature after displaying the warning message, a system message indicting the restoration of operation temperature is output.

Syntax

To set or change information:

```
system temperature-warning-level <temperature>
```

To delete information:

```
no system temperature-warning-level
```

Input mode

```
(config)
```

Parameters

<*temperature*>

Specifies the inlet air temperature (Celsius) of the device that outputs system messages. You can specify the temperature in Celsius.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   25 to 50

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the intake temperature of the device has already exceeded the specified temperature, a system message is immediately output.

Related commands

None

system temperature-warning-level average

Outputs a system message when the average intake temperature of the device reaches or exceeds the specified temperature.

Syntax

To set or change information:

```
system temperature-warning-level average [<temperature>] [period <days>]
```

To delete information:

```
no system temperature-warning-level average
```

Input mode

```
(config)
```

Parameters

<*temperature*>

Specifies the average inlet air temperature (Celsius) of the device that outputs system messages. You can specify the temperature in degrees of Celsius.

1. Default value when this parameter is omitted:

   33

2. Range of values:

   25 to 50

period <*days*>

Specifies the period (the number of days) based on which the average inlet air temperature is calculated. You can specify the value in units of days.

1. Default value when this parameter is omitted:

   30

2. Range of values:

   1 to 30

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The system message is output when starting up the device and every day at noon.

Related commands

None

Chapter

10. SFU/PRU/NIF Management

power enable
system pru priority

power enable

Use the no power enable command to disable SFU, PRU, or NIF. Also power off the SFU, PRU, and NIF.

Syntax

To set information:

```
no power enable {sfu <sfu no.> | pru <pru no.> | nif <nif no.>}
```

To delete information:

```
power enable {sfu <sfu no.> | pru <pru no.> | nif <nif no.>}
```

Input mode

```
(config)
```

Parameters

{sfu <*sfu no.*> | pru <*pru no.*> | nif <*nif no.*>}

Specifies the SFU number, PRU number, or NIF number.

sfu <*sfu no.*>

Specifies the SFU number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

pru <*pru no.*>

Specifies the PRU number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

nif <*nif no.*>

Specifies the NIF number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

SFU, PRU, and NIF run when their status is not "disable". Check the operating status of SFU and PRU with the `show system` operation command, and the status of NIF with the `show nif` operation command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system pru priority

If the power necessary to launch all installed PRUs and NIFs is insufficient when starting up the device, PRUs are started according to the priority specified with this command.

Syntax

To set information:

```
system pru <pru no.> priority <priority>
```

To delete information:

```
no system pru <pru no.> priority
```

Input mode

```
(config)
```

Parameters

<*pru no.*>

Specifies the PRU number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

<*priority*>

Specifies the priority to start the PRUs specified with the pru <*pru no.*> parameter. The lower the value, the higher the priority. If there are multiple PRUs with the same priority level, the PRUs with smaller PRU numbers are preferentially started.

This setting value is used only when the device are started.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

The device runs with the priority level 128.

Impact on communication

None

When the change is applied

The change is applied after the device is restarted.

Notes

1. No PRU starts or stops when setting or deleting this command. No PRU follows this setting to start or stop when inserting or removing a PRU. This setting is activated only at the device startup.

Related commands

None

Chapter

11. Device Redundancy

power redundancy-mode

power redundancy-mode

Sets the monitoring mode for redundant power. According to the redundant power monitoring mode, a system message appears when the power becomes redundant and stops being redundant.

Syntax

To set or change information:

```
power redundancy-mode <mode>
```

To delete information:

```
no power redundancy-mode
```

Input mode

```
(config)
```

Parameters

<*mode*>

Specifies the redundant power monitoring mode for which system messages are displayed.

1: Redundant power supply units

2: Redundant power supply units and redundant power feeds

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 or 2

Default behavior

A system message is not displayed when the power becomes redundant and stops being redundant.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

Chapter

12. System Message Output and Log Management

logging email
logging email-filter
logging email-from
logging email-interval
logging email-server
logging save-count
logging syslog-facility
logging syslog-filter
logging syslog-host
logging syslog-severity
message-list
message-type

logging email

Sets an email address for sending user input commands and messages. This command can configure a maximum of 64 entries.

Syntax

To set information:

```
logging email <e-mail address>
```

To delete information:

```
no logging email <e-mail address>
```

Input mode

```
(config)
```

Parameters

<e-mail address>

Specifies the destination email address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   You can use a maximum of 255 characters, but you can only use alphanumeric characters, hyphens (-), underscores (_), periods (.), and at marks (@).

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You must use the `logging email-server` command in advance to set the SMTP server to which an email is sent.
2. You must configure the settings related to the DNS resolver functionality in advance.
3. Make sure that the specified email address matches the address set for the destination SMTP server.
4. If an attempt to send an email fails, the email is discarded.
5. If an IP address is set for the loopback interface, the IP address is used as the source IP address during communication with the SMTP server.
6. When you use an at mark (@) in an email address, do not use it at the beginning or the end of the email address. Do not use multiple at marks (@).

Related commands

```
logging email-server
hostname
ip domain name
ip name-server
ip domain lookup
```

logging email-filter

Specifies message types and event levels as conditions for sending user input commands and messages via email. The send conditions set with this command are applied to all the output destinations set by the `logging email` command.

Syntax

To set or change information:

```
logging email-filter {message-list <group name> | event-level <event level>
| message-list <group name> event-level <event level>}
```

To delete information:

```
no logging email-filter
```

Input mode

```
(config)
```

Parameters

{message-list <*group name*> | event-level <*event level*> | message-list <*group name*> event-level <*event level*>}

Sets the conditions for sending user input commands and messages.

message-list <*group name*>

Specifies targets for being sent as email by using the message type list. Generate the message type list by using the `message-list` command.

If a message type list that does not exist in <*group name*>, or a message type list with no send conditions set is specified, all message types are targets for being sent as email.

If this parameter is not specified, system messages of all message types are targets for being sent as email.

event-level <*event level*>

Specifies the value of event level for targets for being sent as email. User input commands and messages whose event levels are the specified value or less are targets for being sent as email.

If this parameter is not specified, user input commands and messages whose event level values are 6 or less are targets for being sent as email.

If `message-list` and `event-level` are specified in parallel, user input commands and messages corresponding to both conditions are sent via email.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*group name*>, specify a name with 31 or fewer characters. For details, see *Specifiable values for parameters*.

   Specify a value from 0 to 7 for <*event level*>.

Default behavior

User input commands and messages whose event levels are 6 or less are targets for being sent as email.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
logging email
message-list
message-type
```

logging email-from

Specifies the source email address used for sending user input commands and messages.

Syntax

To set or change information:

```
logging email-from <e-mail address>
```

To delete information:

```
no logging email-from
```

Input mode

```
(config)
```

Parameters

<e-mail address>

Specifies the source email address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   You can use a maximum of 255 characters, but you can only use alphanumeric characters, hyphens (-), underscores (_), periods (.), and at marks (@).

Default behavior

The sender of the email is device-name <*nobody*>. The name specified with the `hostname` command is used as the device name. If the `hostname` command is omitted, the name of the device model is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The email address of the sender set by using this command is applied to all destination email addresses specified by using the `logging email` command.
2. When you use an at mark (@) in an email address, do not use it at the beginning or the end of the email address. Do not use multiple at marks (@).

Related commands

```
logging email
```

logging email-interval

Sets the interval for sending email containing user input commands and messages.

Syntax

To set or change information:

```
logging email-interval <seconds>
```

To delete information:

```
no logging email-interval
```

Input mode

```
(config)
```

Parameters

<*seconds*>

Specifies the interval for sending emails.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600 (seconds)

Default behavior

Sends email in intervals of one second.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The sending interval of the email set by using this command is applied to all destination email addresses specified by using the `logging email` command.
2. If the amount of unsent data stored in the device exceeds the set threshold, email is sent regardless of the setting value of this command.

Related commands

```
logging email
```

logging email-server

Sets the SMTP server information for sending emails that contain user input commands and messages. This command can configure a maximum of 16 entries.

Syntax

To set information:

```
logging email-server {<host name> | <ip address>} [port <port number>]
```

To delete information:

```
no logging email-server {<host name> | <ip address>}
```

Input mode

```
(config)
```

Parameters

{<*host name*> | <*ip address*>}

Specifies the host name or IP address of the SMTP server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*host name*>

   Specifies the host name with 64 or fewer characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

   <*ip address*>

   Specify the IPv4 address in dot notation.

port <*port number*>

Specifies the SMTP server port number.

1. Default value when this parameter is omitted:

   25

2. Range of values:

   0 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Make sure that the specified SMTP server information (the host name or IP address, and port number) matches the one set for the destination SMTP server. If the connection to the SMTP server fails while an email is being sent, the email is discarded.
2. This functionality can use IPv4 only. Therefore, if you specify as the SMTP server the name

of a host that has only an IPv6 address set by using the `ipv6 host` command, emails sent to the server will be discarded.

3. `localhost` cannot be set as a host name.
4. Host names are not case sensitive.
5. `127.*.*.*` cannot be set as an IPv4 address.
6. A class D or class E address cannot be specified as an IPv4 address.
7. If you set a host name that requires address resolution by a DNS server, it might take time to perform address resolution depending the connection conditions with the DNS server. For details about the time necessary for address resolution, see *10. Host Names and DNS* in the manual *Configuration Guide Vol. 1 For Version 12.1*.

   Email might not be sent if the address resolution takes too long.
8. If server information that cannot reach the SMTP server information from the Device, sending email to all addresses might be delayed.
9. If large amounts of messages are generated at one time, some of the information might be missing from the emails.

Related commands

```
ip host
logging email
hostname
ip domain name
ip name-server
ip domain lookup
```

logging save-count

For each message type, specifies the minimum number of saved entries for the operation log.

Syntax

To set or change information:

```
logging save-count <message type> <count>
```

To delete information:

```
no logging save-count <message type>
```

Input mode

```
(config)
```

Parameters

<*message type*>

Specifies the message type for which the minimum number of saved entries is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about the range of values, see *Specifiable values for parameters*.

<*count*>

Specifies the minimum number of saved entries in units of 100.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   100 to 10000

   However, if the total number of specified values for each message type exceeds 100000, it cannot be specified.

Default behavior

The minimum number of saved entries will be 500 regardless of the message type.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Executing this command does not delete the operation log. For saving an operation log whose entries exceeded the limit, see *Table 1-2 Features of the operation log and statistics log* in the manual *Message and Log Reference For Version 12.1*.

Related commands

None

logging syslog-facility

Sets the facility added to the header of the syslog send data when sending user input commands and messages as syslog transmissions.

Syntax

To set or change information:

```
logging syslog-facility <facility>
```

To delete information:

```
no logging syslog-facility
```

Input mode

```
(config)
```

Parameters

<*facility*>

Specifies the facility added to the header.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify local0, local1, local2, local3, local4, local5, local6, or local7.

Default behavior

Use local0 for the facility added to the header of the syslog send data.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The facility set by this command is applied to all the output destinations set by the `logging syslog-host` command.

Related commands

```
logging syslog-host
```

logging syslog-filter

Specifies the send conditions for sending the user input commands and the messages as the syslog with message type and event level. The send conditions set with this command are applied to all the output destinations set by the `logging syslog-host` command.

Syntax

To set or change information:

```
logging syslog-filter {message-list <group name> | event-level <event level>
| message-list <group name> event-level <event level>}
```

To delete information:

```
no logging syslog-filter
```

Input mode

```
(config)
```

Parameters

{message-list <*group name*> | event-level <*event level*> | message-list <*group name*> event-level <*event level*>}

Sets the conditions for sending user input commands and messages.

message-list <*group name*>

Specifies targets for being sent to syslog by using the message type list. Generate the message type list by using the `message-list` command.

If a message type list that does not exist in <*group name*>, or a message type list with no send conditions set is specified, all message types are targets for being sent to syslog.

If this parameter is not specified, system messages of all message types are targets for being sent to syslog.

event-level <*event level*>

Specifies the value of event level for targets for being sent to syslog. User input commands and messages whose event levels are the specified value or less are targets for being sent to syslog.

If this parameter is not specified, user input commands and messages whose event level values are 6 or less are targets for being sent to syslog.

If `message-list` and `event-level` are specified in parallel, user input commands and messages corresponding to both conditions are sent as syslog.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*group name*>, specify a name with 31 or fewer characters. For details, see *Specifiable values for parameters*.

   Specify a value from 0 to 7 for <*event level*>.

Default behavior

User input commands and messages whose event levels are 6 or less are targets for being sent to syslog.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
logging syslog-host
message-list
message-type
```

logging syslog-host

Sets the destination syslog server for the user input commands and the messages. This command can configure a maximum of 50 entries.

Syntax

To set information:

```
logging syslog-host <host name> [no-date-info] [version <version id>]
logging syslog-host { <ip address> | <ipv6 address> } [vrf <vrf id>]
[no-date-info] [version <version id>]
```

To delete information:

```
no logging syslog-host <host name>
no logging syslog-host { <ip address> | <ipv6 address> } [vrf <vrf id>]
```

Input mode

```
(config)
```

Parameters

<*host name*>

Specifies the destination syslog server for the user input commands and the messages.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the host name with 64 or fewer characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

{ <*ip address*> | <*ipv6 address*> }

Specifies the destination for the user input commands and the messages as an IPv4 or IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*ip address*>

   Specify the IPv4 address in dot notation.

   <*ipv6 address*>

   Specify the IPv6 address in colon notation.

vrf <*vrf id*>

Sends the user input commands and the messages to the VRF specified with the <*vrf id*> parameter of the `vrf definition` command.

1. Default value when this parameter is omitted:

   Sends the user input commands and the messages to the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

no-date-info

Sends the user input commands and the messages but excludes the generation time from the send information. The format for the send information is same as the operation log.

For details about the operation log formats, see *1.1.3 Format of operation logs* in the manual *Message and Log Reference For Version 12.1*.

1. Default value when this parameter is omitted:

   Sends all the information defined in the format for the operation log.

2. Range of values:

   None

version <*version id*>

Specifies the format version for the syslog.

If 1 is set for the <*version id*>, the syslog is sent in syslog format compliant to the RFC 5424.

1. Default value when this parameter is omitted:

   Sends the syslog in syslog format compliant to the RFC 3164.

2. Range of values:

   1

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To use the syslog functionality, a syslog daemon program must be running on the destination host and the host must be configured so that it can receive the syslog information from the Device.
2. If an IP address is set for the loopback interface, the IP address is used as the source IP address from which syslog information is sent.
3. `localhost` cannot be specified as a host name.
4. Host names are not case sensitive.
5. `127.*.*.*` cannot be set as an IPv4 address.
6. Class D or class E IPv4 addresses cannot be set.
7. IPv6 addresses can be global addresses or site-local addresses.
8. If a host name that requires address resolution by a DNS server, it might take time to perform address resolution depending the connection conditions with the DNS server. For details about the time necessary for address resolution, see *10. Host Names and DNS* in the manual *Configuration Guide Vol. 1 For Version 12.1*.

   The syslog information might not be sent if address resolution takes too long.
9. If large amounts of messages are generated at one time, some of the information might be missing from the syslog.
10. Time information will still remain in the user input command and the messages that are saved in the device even when `no-date-info` is specified.

11. The time in the user input command and the messages sent to the log destination are excluded when `no-date-info` is specified. However, the log output function itself will add the time as a header, so the send date and time of the user input command and the messages are displayed at the log destination.

Related commands

```
ip host
ipv6 host
hostname
ip domain name
ip name-server
ip domain lookup
```

logging syslog-severity

Sets the severity attached to the header section of the syslog send data when sending user input commands and messages as syslog transmissions.

Only use this command when setting the severity of all the syslog send data to the same value.

Syntax

To set or change information:

```
logging syslog-severity { <level> | <keyword> }
```

To delete information:

```
no logging syslog-severity
```

Input mode

```
(config)
```

Parameters

{ <*level*> | <*keyword*> }

Specifies the level or the keyword used to attach the severity to the header section.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The table below describes the severity levels that can be specified. Note that if a level is specified, information is displayed with the keyword.

Table 12-1: Severity levels that can be specified

Level	Keyword
0	emergencies
1	alerts
2	critical
3	errors
4	warnings
5	notifications
6	information
7	debugging

Default behavior

The event level defined by each user input command and message is used as the severity to be attached to the syslog send data.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The severity set by this command is applied to all the output destinations set by the `logging syslog-host` command.

Related commands

`logging syslog-host`

message-list

Generates the list of message types to control the output when a message is output to the screen, syslog is sent, an email is sent, and a system message trap is sent. When this command is entered, the mode can be switched to config-msg-list mode and the output conditions can be set.

You can create a maximum of 110 entries for the message type list.

Syntax

To set information:

```
message-list <group name>
```

To delete information:

```
no message-list <group name>
```

Input mode

```
(config)
```

Parameters

<group name>

Specifies the name of the message list to be applied as an output condition when the message is output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name of no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

Outputs all the message types that are targeted to be output. However, the message types that are targeted to be output target differ depending on the output destination.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
username
snmp-server traps
logging syslog-filter
logging email-filter
```

message-type

Specifies the message type to be controlled as an output condition.

Syntax

To set or change information:

```
message-type {include | exclude} <message type>
```

To delete information:

```
no message-type {include | exclude} <message type>
```

Input mode

```
(config-msg-list)
```

Parameters

{include | exclude}

Specifies the output requirements for the specified message type. Permission (`include`) and suppression (`exclude`) cannot coexist inside a single message type list.

The output of all the message types that are not specified is suppressed when permission is specified with the `include` parameter in a single message type list. Also, output of all the message types that are not specified is permitted when suppression is specified with the `exclude` parameter in a single message type list.

include

Permits the output of the specified message type.

exclude

Suppresses the output of the specified message type.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<*message type*>

Specifies the message type to control the output for each type.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about the range of values, see *Specifiable values for parameters*.

Default behavior

Output all the message types that are targeted to be output. However, the message types that are targeted to be output differ depending on the output destination.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
username
snmp-server traps
logging syslog-filter
logging email-filter
```

Chapter

13. SNMP

rmon alarm
rmon collection history
rmon event
snmp-server community
snmp-server contact
snmp-server engineID local
snmp-server group
snmp-server host
snmp-server informs
snmp-server location
snmp-server traps
snmp-server user
snmp-server view
snmp trap link-status

rmon alarm

Sets the control information of the RMON alarm group. This command can configure a maximum of 128 entries.

Syntax

To set or change information:

```
rmon alarm <number> <variable> <interval> {delta | absolute} rising-threshold
<value> rising-event-index <event no.> falling-threshold <value>
falling-event-index <event no.> [owner string] [ startup_alarm {
rising_falling | rising | falling } ]
```

To delete information:

```
no rmon alarm <number>
```

Input mode

```
(config)
```

Parameters

<*number*>

Specifies the information identification number for the RMON alarm group control information. This parameter supports the `alarmIndex` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

<*variable*>

Specifies the object identifier for the MIB used for checking the threshold. This parameter supports the `alarmVariable` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an object name in dot notation. Specify an INTEGER, Integer32, Counter32, Gauge32, or TimeTicks type object identifier (Counter64 type is not supported with the alarm function of the Device).

<*interval*>

Specifies the time interval (in seconds) for checking the threshold. This parameter supports the `alarmInterval` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   From 1 to 4294967295

{delta | absolute}

Specifies the method for checking the threshold. If `delta` is specified, the difference between the current value and the value of the last sampling is compared with the threshold. If `absolute` is specified, the current value is compared directly with the threshold. This

parameter supports the `alarmSampleType` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

rising-threshold <*value*>

Specifies the upper threshold. This parameter supports the `alarmRisingThreshold` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   From -2147483648 to 2147483647

rising-event-index <*event no.*>

Specifies the identification number of the method for generating an event if the upper threshold is exceeded. The method used to generate the event is determined by the information identification number for the control information specified by using the `event` configuration command. This parameter supports the `alarmRisigEventIndex` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An information identification number from 1 to 65535 for the control information, specified by using the `event` configuration command for <*event no.*>

falling-threshold <*value*>

Specifies the lower threshold value. This parameter supports the `alarmFallingThreshold` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   From -2147483648 to 2147483647

falling-event-index <*event no.*>

Specifies the identification number of the method for generating an event if the lower threshold is exceeded. The method used to generate the event is determined by the information identification number for the control information specified by using the `event` configuration command. This parameter supports the `alarmFallingEventIndex` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An information identification number from 1 to 65535 for the control information, specified by using the `event` configuration command for <*event no.*>

owner <*string*>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter supports the `alarmOwner` of the relevant standards.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Enclose a character string of 24 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

startup_alarm { rising_falling | rising | falling }

Specifies the timing for checking the threshold in the first sampling. If `rising` is specified, an alarm is generated when the upper threshold is exceeded in the first sampling. If `falling` is specified, an alarm is generated when a value drops below the lower threshold in the first sampling. If `rising_falling` is specified, an alarm is generated when the upper or lower threshold is crossed in the first sampling. This parameter supports the `alarmstartUpAlarm` of the relevant standards.

1. Default value when this parameter is omitted:

   rising_falling

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To access an alarm group from the SNMP manager, you must register the SNMP manager by using the `snmp-server community` command.
2. As the value for `rising-event-index` or `falling-event-index` of an alarm group, set the information identification number for an event group that has been set in the device configuration.
3. A maximum total of 128 entries can be set for the alarm groups set in the configuration and the alarm groups set by the Set operation from the SNMP manager. When the maximum number of entries have been set, even if an alarm group is set in the configuration, the added alarm group will not work. Delete unnecessary alarm settings, and then reconfigure the alarm settings.
4. If the Set operation is performed from the SNMP manager for RMON alarmTable, the result of the operation will not be applied to the configuration.
5. Some alarms might not work if they cannot collect MIB information, such as when there are too many alarm configurations or when the value set for the interval is 60 seconds or less. In such a case, the MIB value for alarmStatus is `invalid(4)`. If this happens, change the interval to a value larger than 60 seconds, or delete unnecessary alarm settings.

6. If the set interval value is too large, `valid(1)` is returned for the time being until alarmStatus changes from `valid(1)` to `invalid(4)` (as a guide, it takes time of about half of the interval value).

Related commands

```
snmp-server host
rmon event
```

rmon collection history

Sets the control information for the RMON Ethernet statistics history.

Syntax

To set or change information:

```
rmon collection history controlEntry <integer> [owner <owner name>] [buckets
<bucket number>] [interval <seconds>]
```

To delete information:

```
no rmon collection history controlEntry <integer>
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

controlEntry <*integer*>

Specifies the information identification number for the statistics history control information. This parameter supports the `historyControlIndex` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   From 1 to 65535

owner <*owner name*>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter supports the `historyControlOwner` of the relevant standards.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Enclose a character string of 24 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

buckets <*bucket number*>

Specifies the number of history entries in which statistics can be stored. This parameter supports the `historyControlBucketsRequested` of the relevant standards.

1. Default value when this parameter is omitted:

   50

2. Range of values:

   From 1 to 65535

   Note: If a value from between 51 to 65535 is specified for <*bucket number*>, operation is the same as if 50 had been specified.

interval <*seconds*>

Specifies the time interval (in seconds) for collecting statistics. This parameter supports the `historyControlInterval` of the relevant standards.

1. Default value when this parameter is omitted:

   1800

2. Range of values:

   From 1 to 3600

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To access an Ethernet history group from the SNMP manager, you must register the SNMP manager by using the `snmp-server community` command.
2. A maximum total of 32 entries can be set for the history groups set in the configuration and the history groups set by the `Set` operation from the SNMP manager. When the maximum number of entries have been set, even if a history group is set in the configuration, the added history group will not work. Delete unnecessary history settings, and then reconfigure the history settings.
3. If the `Set` operation is performed from the SNMP manager for RMON historyControlTable, the result of the operation will not be applied to the configuration.
4. If the status of the NIF that corresponds to the interface set by the history configuration of RMON becomes inactivate, etherHistory information from the time of the status change cannot be obtained. Therefore, the historyControlStatus value will reply with `invalid(4)`. However, it will take time for the historyControlStatus to change from `valid(1)` to `invalid(4)` (roughly about half the time of the interval value).

Related commands

```
interface
snmp-server community
```

rmon event

Sets the control information for an RMON event group. This command can configure a maximum of 16 entries.

Syntax

To set or change information:

```
rmon event <event no.> [log] [trap <community>] [description <string>] [owner
<string>]
```

To delete information:

```
no rmon event <event no.>
```

Input mode

```
(config)
```

Parameters

<*event no.*>

Specifies the information identification number for the control information of an RMON event group. This parameter supports the `eventIndex` of the relevant standards.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   From 1 to 65535

log

This parameter specifies the method for generating an alarm (event) and generates an alarm log. This parameter supports the `eventType` of the relevant standards.

1. Default value when this parameter is omitted:

   An alarm log is not generated.

2. Range of values:

   None

trap <*community*>

This parameter specifies the method for generating an alarm (event) and sends an SNMP trap or inform to the community specified for <*community*>. This parameter supports the `eventType` of the relevant standards.

1. Default value when this parameter is omitted:

   No traps or informs are issued.

2. Range of values:

   Enclose a character string of 60 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

description <*string*>

Uses a character string to specify the description of an event. Use this parameter as a note regarding the event. This parameter supports the `eventDescription` of the relevant

standards.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Enclose a character string of 79 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

owner <*string*>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter supports the `eventOwner` of the relevant standards.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Enclose a character string of 24 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When an event group is accessed from the SNMP manager and traps or informs are sent to the SNMP manager, you must register the SNMP manager by using the `snmp-server community` and `snmp-server host` commands.
2. To send traps or informs to the SNMP manager, specify the IP address of the destination SNMP manager and `rmon` by using the `snmp-server host` command.
3. A trap or an inform is sent only if the community name used when the SNMP manager is registered matches the community name of the event group.
4. Set the information identification number that has been set for the corresponding event group as the value for `rising-event-index` or `falling-event-index` of an alarm group. If the values are different, no event is executed when an alarm is generated.
5. A maximum total of 16 entries can be set for the event groups set in the configuration and the event groups set by the `Set` operation from the SNMP manager. When the maximum number of entries have been set, even if an event group is set in the configuration, the added event group will not work. Delete unnecessary event settings, and then reconfigure the event settings.
6. If the `Set` operation is performed from the SNMP manager for RMON eventTable, the result

of the operation will not be applied to the configuration.

Related commands

```
snmp-server host
rmon alarm
```

snmp-server community

Sets the access list for the SNMP community. A maximum of 50 addresses can be registered by this command.

Syntax

To set or change information:

```
snmp-server community <community> [{ ro | rw }] [<access list name>] [vrf
<vrf id>]
```

To delete information:

```
no snmp-server community <community> [vrf <vrf id>]
```

Input mode

```
(config)
```

Parameters

<*community*>

Sets the community name for the SNMP manager.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of 60 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

{ ro | rw }

Sets the MIB operating mode for the manager that has the specified IP address belonging to the community with the specified community name. GetRequest, GetNextRequest, and GetBulkRequest are permitted when `ro` is specified. GetRequest, GetNextRequest, GetBulkRequest, and SetRequest are permitted when `rw` is specified.

1. Default value when this parameter is omitted:

   ro

2. Range of values:

   None

<*access list name*>

Specifies the name of the access list in which the permissions for this community are set. If the specified <*access list name*> has not been set, all accesses are permitted.

One access list is permitted for one community.

1. Default value when this parameter is omitted:

   All accesses are permitted.

2. Range of values:

   Specify an access list name with 31 or fewer characters.

   For details, see *Specifiable values for parameters*.

vrf <*vrf id*>

Permits accesses from the VRF specified in <*vrf id*>.

1. Default value when this parameter is omitted:

   Permits access from the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. An access list different from the setting cannot be specified when changing the information.

Related commands

None

snmp-server contact

Sets the contact information of the Device.

Syntax

To set or change information:

```
snmp-server contact <contact>
```

To delete information:

```
no snmp-server contact
```

Input mode

```
(config)
```

Parameters

<contact>

Sets information, such as contact information, to used when a failure occurs on the Device. This information can be referenced by using the name set in `[sysContact]` of the system group for inquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the `Set` operation of SNMP. If this name is changed by the `Set` operation of SNMP, the name is applied to the configuration. This parameter is equivalent to `sysContact` of RFC 3418.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of 60 of fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about `name`, `contact`, and `location` from the SNMP manager, you must use the `snmp-server community` command to register the SNMP manager.

Related commands

None

snmp-server engineID local

Sets the SNMP engine ID information.

Syntax

To set or change information:

```
snmp-server engineID local <engineid string>
```

To delete information:

```
no snmp-server engineID local
```

Input mode

```
(config)
```

Parameters

<engineid string>

Sets an SNMP engine ID.

The SNMP engine ID values set for a device are as follows:

1st to 4th octets: A value obtained by a bit OR of an enterprise code and `0x80000000`.

5th octet: Fixed value of 4

6th to 32nd octets: The settings value for *<engineid string>*

The SNMP engine ID set on the device can be referenced by the snmp operation command. An example is as follows.

1st to 4th octets: `0x80FFFF`

5th octet: `0x04` (Fixed value)

6th to 32nd octets: `0x736E6D705F546F6B796F31`

The following value can be obtained if referenced with the snmp operation command that is set with the value above.

```
80 00 FF FF 04 73 6E 6D 70 5F 54 6F 6B 79 6F 31
```

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of 27 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The SNMP engine ID values set for a device are as follows:

1st to 4th octets: A value obtained by a bit OR of an enterprise code and `0x80000000`.

5th octet: Fixed value of `128`

6th to 9th octets: A random number

10th to 13th octets: The value of the universal timer value when the ID was automatically generated

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there are many users (a maximum of 50) set by using the `snmp-server user` command, it takes a maximum of 20 seconds to reference with the SNMP manager after setting, changing, or deleting the snmp-server engine ID local command.

Related commands

```
snmp-server view
snmp-server user
snmp-server group
snmp-server host
```

snmp-server group

Sets the SNMP security group information. The security level information and the access control information that consists of the SNMP view information set by the `snmp-server view` command are grouped. A maximum of 50 group names can be set by this command.

Syntax

To set or change information:

```
snmp-server group <group name> v3 {noauth | auth | priv} [ read <view name>]
[write <view name>] [notify <view name>]
```

To delete information:

```
no snmp-server group <group name> v3 { noauth | auth | priv }
```

Input mode

```
(config)
```

Parameters

<*group name*>

Configures an SNMP security group name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of 32 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

{ noauth | auth | priv }

Sets the security level of access control. When an SNMP packet is received, the processing checks whether the received packet matches the security level set by this parameter. When an SNMP packet is sent, the SNMP packet is generated with the security level set by this parameter.

`noauth`: Authentication and encryption are not required.

`auth`: Authentication is required, and encryption is not required.

`priv`: Authentication and encryption are both required.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

read <*view name*>

Sets the `read` view name for access control. When an SNMP packet with any of the following PDU types is received, if the read view name specified for <*view name*> exists in the SNMP MIB view information, the MIB view is checked:

* GetRequest-PDU

* GetNextRequest-PDU

* GetBulkRequest-PDU

1. Default value when this parameter is omitted:

   The read access permission is not granted.

2. Range of values:

   Enclose a character string of 32 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

write <*view name*>

Sets the `write` view name of access control. When an SNMP packet with the SetRequest-PDU PDU type is received, if the write view name specified for <*view name*> exists in the SNMP MIB view information, the MIB view is checked.

1. Default value when this parameter is omitted:

   The write access permission is not granted.

2. Range of values:

   Enclose a character string of 32 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

notify <*view name*>

Sets the notify view name of access control. When a trap (an SNMP packet with the SNMPv2-Trap-PDU PDU type) is sent, if the notify view name specified for <*view name*> exists in the SNMP MIB view information, the MIB view is checked.

1. Default value when this parameter is omitted:

   The notify access permission is not granted.

2. Range of values:

   Enclose a character string of 32 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a MIB view name that has not been set by the `snmp-server view` command is set for the read view name, write view name, or notify view name of this command, the view name information set by this command is invalid.

Related commands

```
snmp-server engineID local
snmp-server view
snmp-server user
snmp-server host
```

snmp-server host

Registers the network management device (SNMP manager) to which traps or informs are sent. This command can configure a maximum of 50 entries.

Syntax

To set or change information:

```
snmp-server host <manager address> [vrf <vrf id>] { traps | informs } <string>
[version { 1 | 2c | 3 { noauth | auth | priv } }] [snmp] [{ospf_state |
ospf_state_private }] [{ ospf_error | ospf_error_private }] [bgp] [vrrp]
[rmon] [air-fan] [power] [login] [memory] [system-msg] [standby_system]
[temperature] [frame_error_snd] [frame_error_rcv] [board]
```

To delete information:

```
no snmp-server host <manager address> [vrf <vrf id>]
```

Input mode

```
(config)
```

Parameters

<*manager address*>

Sets the IP address of the SNMP manager.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv4 address (in dot notation) or an IPv6 address (in colon notation) for <*manager address*>. The global address can be specified as an IPv6 address.

vrf <*vrf id*>

Issues a trap or an inform to the VRF specified for <*vrf id*> in the `vrf definition` command.

1. Default value when this parameter is omitted:

   A trap or an inform is issued to the global network.

2. Range of values:

   Specify a VRF ID for <*vrf id*>.

   For details, see *Specifiable values for parameters*.

{traps | informs}

Sets the type of event notification that will be sent to the SNMP manager.

- If `traps` is specified, traps will be issued. The SNMP manager does not send a response.
- If `informs` is specified, informs will be issued. Because informs request the SNMP manager to send a response, the SNMP agent monitors for a response. If no response is returned, the inform is resent. This parameter can be used only in version SNMPv2C.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<*string*>

For SNMPv1 and SNMPv2C, this parameter sets the name of the community for the SNMP manager. For SNMPv3, this parameter sets the security user name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of 60 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

version { 1 | 2c | 3 { noauth | auth | priv }}

Specifies the sending version of the manager that has the specified IP address belonging to the community with the specified community name. If `1` is specified, the SNMPv1 version traps are issued. If `2c` is specified, SNMPv2C version traps or informs are issued. If `3` is specified, SNMPv3 version traps are issued.

If `3` is specified, this parameter also sets the security level for sending the traps.

- If `noauth` is specified, traps are sent without authentication and encryption required.
- If `auth` is specified, traps are sent with authentication required and without encryption required.
- If `priv` is specified, traps are sent with both authentication and encryption required.

1. Default value when this parameter is omitted:

   1

2. Range of values:

   None

[snmp] [{ospf_state | ospf_state_private }] [{ ospf_error | ospf_error_private }] [bgp] [vrrp] [rmon] [air-fan] [power] [login] [memory] [system-msg] [standby_system] [temperature] [frame_error_snd] [frame_error_rcv] [board]

By setting each parameter, you can select the traps or informs to be sent. The following table describes the traps or informs that will be sent when parameters are set.

Table 13-1: Correspondence between parameters and traps or informs

Parameter	Traps and informs
snmp	coldStart
	warmStart
	linkUp
	linkDown
	authenticationFailure
ospf_state	ospfVirtNbrStateChange
	ospfNbrStateChange
	ospfVirtIfStateChange
	ospfIfStateChange

Parameter	Traps and informs
ospf_state_private	axOspfVirtNbrStateChange
	axOspfNbrStateChange
	axOspfVirtIfStateChange
	axOspfIfStateChange
ospf_error	ospfVirtIfConfigError
	ospfIfConfigError
	ospfVirtIfAuthFailure
	ospfIfAuthFailure
ospf_error_private	axOspfVirtIfConfigError
	axOspfIfConfigError
	axOspfVirtIfAuthFailure
	axOspfIfAuthFailure
bgp	bgpEstablished
	bgpBackwardTransition
vrrp	vrrpTrapNewMaster
	vrrpTrapAuthFailure
	vrrpTrapProtoError
rmon	risingAlarm
	fallingAlarm
air-fan	axAirFanUnitStopTrap
	axAirFanUnitRecoveryTrap
power	axPowerSupplyFailureTrap
	axPowerSupplyRecoveryTrap
	axPowerSupplyStatusChangeTrap
	axPowerRedundancyFailureTrap
	axPowerRedundancyRecoveryTrap
	axPowerSupplyInsufficientTrap
	axPowerSupplyInsufficientRecoveryTrap
login	axLoginSuccessTrap
	axLoginFailureTrap
	axLogoutTrap
memory	axBcuMemoryUsageAlarmTrap
	axBcuMemoryUsageRecoveryTrap
system-msg	axSystemMsgTrap

Parameter	Traps and informs
standby_system	axStandbyUpSimplexToDuplexTrap
	axStandbyDownDuplexToSimplexTrap
temperature	axBcuTemperatureTrap
frame_error_snd	axFrameErrorSendTrap
frame_error_rcv	axFrameErrorReceiveTrap
board	axSfuStateChangeTrap
	axPruStateChangeTrap
	axNifStateChangeTrap

snmp

`coldStart`, `warmStart`, `linkDown`, `linkUp`, and `authenticationFailure` traps or informs are sent.

{ ospf_state | ospf_state_private }

Sends a trap or an inform to notify about a change in the OSPF status. If `ospf_state` is specified, a standard trap or inform that complies with the RFC is issued. However, if the OSPF domain is being partitioned, all domains other than the domain with the smallest domain number will issue private traps or informs. If `ospf_state_private` is specified, all OSPF domains will issue private traps or informs.

The following table lists the traps or informs to be issued.

Table 13-2: Traps and informs to be issued for each parameter (Notifications about changes of the OSPF status)

Parameter	Traps and informs to be issued
ospf_state	Domain with the smallest domain number: • ospfVirtIfStateChange • ospfNbrStateChange • ospfVirtNbrStateChange • ospfIfStateChange All domains other than the domain with the smallest domain number: • axOspfVirtIfStateChange • axOspfNbrStateChange • axOspfVirtNbrStateChange • axOspfIfStateChange
ospf_state_private	All domains: • axOspfVirtIfStateChange • axOspfNbrStateChange • axOspfVirtNbrStateChange • axOspfIfStateChange

{ ospf_error | ospf_error_private }

Sends a trap or an inform to notify reception about an OSPF error packet. If `ospf_error` is specified, a standard trap or inform that complies with the RFC is issued. However, if the OSPF domain is being partitioned, all domains other than the domain with the smallest domain number will issue private traps or informs. If `ospf_error_private` is specified, all OSPF domains will issue private traps or informs.

The following table lists the traps or informs to be issued.

Table 13-3: Traps and informs to be issued for each parameter (Notifications to reception about OSPF error packets)

Parameter	Traps and informs to be issued
ospf_error	Domain with the smallest domain number: • ospfIfConfigError • ospfVirtIfConfigError • ospfIfAuthFailure • ospfVirtIfAuthFailure All domains other than the domain with the smallest domain number: • axOspfIfConfigError • axOspfVirtIfConfigError • axOspfIfAuthFailure • axOspfVirtIfAuthFailure
ospf_error_private	All domains: • axOspfIfConfigError • axOspfVirtIfConfigError • axOspfIfAuthFailure • axOspfVirtIfAuthFailure

bgp

A trap or an inform is sent when a BGP link is established or closed.

vrrp

A trap or an inform is sent when the VRRP status is changed.

rmon

A trap or an inform is sent when the value exceeds the upper threshold or drops below the lower threshold of the `rmon` alarm.

air-fan

A trap or an inform is sent if the following events occur:

- A fan failure occurrens or is restored
- A fan is removed or inserted

power

A trap or an inform is sent if the following events occur:

- A power supply unit failure occurs or is restored
- A power supply unit is removed or inserted
- A power supply unit stops or starts being fed power
- Redundancy configuration of a power supply unit is started or canceled.
- An unsupported power supply is detected
- An insufficient power feed occurs or is restored

login

A trap or an inform is sent if the following events occur:

- A login is successful or fails
- logout

memory

A trap or an inform is sent when a memory shortage occurs, or when the shortage is

restored.

system-msg

A trap or an inform is sent when a system message is output.

standby_system

A trap or an inform is sent when the operating status of the standby BCU has changed from operating to anything other than operating, or from anything other than operating to operating.

temperature

A trap is sent when the temperature changes.

frame_error_snd

A trap or an inform is sent when a frame reception error occurs.

frame_error_rcv

A trap or an inform is sent when a frame sending error occurs.

board

A trap or an inform is sent when the SFU, PRU, or NIF status is changed.

1. Default value when this parameter is omitted:

   A trap or an inform is not issued for each parameter.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the list of supported MIBs and supported traps, see the manual *MIB Reference For Version 12.1*.
2. When `3` has been set for the version, if a security user name that has not been set in the `snmp-server user` command is set by this command, the security user information set in this command becomes invalid.

Related commands

```
snmp-server engineID local
snmp-server view
snmp-server user
snmp-server group
```

snmp-server informs

Sets the conditions for sending informs. This setting is valid for SNMP managers for which the `informs` parameter of the `snmp-server host` command is set.

Syntax

To set or change information:

```
snmp-server informs [retries <retries>] [timeout <seconds>] [pending
<pending>]
```

To delete information:

```
no snmp-server informs
```

Input mode

```
(config)
```

Parameters

retries <*retries*>

Sets the maximum number of times an inform can be resent to the SNMP manager. If 0 is set, the informs are not resent.

1. Default value when this parameter is omitted:

   3

2. Range of values:

   From 0 to 100

timeout <*seconds*>

Sets the timeout time in seconds of informs for the SNMP manager.

1. Default value when this parameter is omitted:

   30

2. Range of values:

   From 1 to 21474835

pending <*pending*>

Sets the maximum number of inform events that the Device can retain at the same time. If the SNMP manager does not respond, an inform event is held. If the number of inform events retained exceeds the maximum, excess events are discarded starting from the oldest ones.

1. Default value when this parameter is omitted:

   25

2. Range of values:

   From 1 to 80000

Default behavior

The initial values for all parameters of this command are used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

`snmp-server host`

snmp-server location

Sets the name of the location where the Device is installed.

Syntax

To set or change information:

```
snmp-server location <location>
```

To delete information:

```
no snmp-server location
```

Input mode

```
(config)
```

Parameters

<*location*>

Sets the name of the location where the Device is installed. This information can be referenced by using the name set in `[sysLocation]` of the system group for inquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the `Set` operation of SNMP. If this name is changed by the `Set` operation of SNMP, the name is applied to the configuration. This parameter is equivalent to `sysLocation` defined in RFC 3418.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of 60 or fewer characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about `name`, `contact`, and `location` from the SNMP manager, you must use the `snmp-server community` command to register the SNMP manager.

Related commands

None

snmp-server traps

Sets the timing for issuing a trap or an inform.

Syntax

To set or change information:

```
snmp-server traps [{ limited_coldstart_trap | unlimited_coldstart_trap }]
[link_trap_bind_info { private | standard }] [{system_msg_trap_message_list
<group name> | system_msg_trap_event_level <event level> |
system_msg_trap_message_list <group name> system_msg_trap_event_level <event
level>}] [agent-address <agent address>]
```

To delete information:

```
no snmp-server traps
```

Input mode

```
(config)
```

Parameters

{ limited_coldstart_trap | unlimited_coldstart_trap }

Limits the times that `coldStart` is issued. The following table provides an overview of the events that cause the `coldStart` set by using this parameter to be issued.

Table 13-4: Events causing coldStart to be issued for each parameter

Parameter	Events
limited_coldstart_trap	• When a device starts • When a system switchover is performed
unlimited_coldstart_trap	• When a device starts • When an IP address is added, deleted, or changed due to a change in the configuration • When the `set clock` command is used to change the time • When a system switchover is performed

1. Default value when this parameter is omitted:

   limited_coldstart_trap

2. Range of values:

   None

link_trap_bind_info {private | standard}

Configures the MIB to be added when a `linkDown` or `linkUp` trap is issued.

The following table describes the MIBs to be added when a `linkDown` or `linkUp` trap set by using this parameter is issued.

Table 13-5: MIBs to be added when a linkDown or linkUp trap is issued for each parameter

Parameter	MIBs to be added when a linkDown or linkUp trap is issued
private	• (Common to SNMPv1 and SNMPv2C) `ifIndex`, `ifDescr`, and `ifType`
standard	• (For SNMPv1) `ifIndex` • (For SNMPv2C) `ifIndex`, `ifAdminStatus`, and `ifOperStatus`

1. Default value when this parameter is omitted:

   standard

2. Range of values:

   None

{system_msg_trap_message_list <*group name*> | system_msg_trap_event_level <*event level*> | system_msg_trap_message_list <*group name*> system_msg_trap_event_level <*event level*>}

Specify the condition for sending system message traps from among private traps or informs.

system_msg_trap_message_list <*group name*>

Specify the system message to be sent as the system message trap in the message type list. Generate the message type list by using the `message-list` command.

If a message type list that does not exist in the <*group name*>, or a message type list that is not specifying a filter condition is specified, system messages with all the message types will become the sending target for the system message trap.

If this parameter is not specified, system messages with all the message types will become the send target for the system message trap.

system_msg_trap_event_level <*event level*>

Specifies the event level of the system messages to be sent as the system message trap in numeric value. The system message with the event level equal or less than the specified numeric value will be the sending target for the system message trap.

System messages with an event level value of 6 or less will become the send target for the system message trap when this parameter is not specified.

When the `system_msg_trap_message_list` and the `system_msg_trap_event_level` are specified concurrently, the system message that matchess both conditions is sent as the system message trap.

1. Default value when this parameter is omitted:

   System messages with an event level value of 6 or less will become the send target for the system message trap.

2. Range of values:

   For <*group name*>, specify a name with 31 or fewer characters. For details, see *Specifiable values for parameters*.

   Specify a value from 0 to 7 for <*event level*>.

agent-address <*agent address*>

Specifies the IPv4 address to be used for the agent address in the trap notification frame in SNMPv1 format. Because only the SNMPv1 frame format can have the agent address field in Trap-PDUs, the address set by using this command is applied to SNMPv1 traps.

Note that this parameter is applied only to the traps to be issued to global networks.

1. Default value when this parameter is omitted:

   When this parameter has not been set, if an IPv4 address has been set for interface loopback, that address is used for the agent address. If such an address has not been set, the IPv4 address for the interface that has the lowest `ifIndex` is used as the agent address in the trap notification frame. If no IPv4 address has been set for the Device, `0.0.0.0` is used.

2. Range of values:

   Specify an IPv4 address from `0.0.0.0` to `255.255.255.255` for <*agent address*>.

Default behavior

The initial values for all parameters of this command are used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the list of supported MIBs and supported traps, see the manual *MIB Reference For Version 12.1*.
2. If the following message type that is not included in the system message is specified as a send target, the system message trap is not sent.
   - KEY
   - CONFIGERR
   - CMDRSP

Related commands

```
message-list
message-type
```

snmp-server user

Sets the SNMP security user information. The user information created by this command is to be used in the `snmp-server group` command and the `snmp-server host` command. This command can configure a maximum of 50 entries.

This command configures the authentication protocol and the encryption protocol. You can configure the encryption protocol after the authentication protocol has been configured. The following table lists the combinations of the authentication protocols and the encryption protocols.

Table 13-6: Combination of the authentication protocol and the encryption protocol

No.	Authentication protocol	Encryption protocol
1	None	None
2	MD5 or SHA	None
3	MD5 or SHA	DES

Syntax

To set or change information:

```
snmp-server user <user name> <group name> v3 [auth { md5 | sha }
<authentication password> [priv des <privacy password>]] [vrf <vrf id>]
```

To delete information:

```
no snmp-server user <user name>
```

Input mode

```
(config)
```

Parameters

<user name>

Configures an SNMP security user name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

<group name>

Sets the name of the SNMP security group to which the SNMP security user belongs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

v3 [auth { md5 | sha } <*authentication password*> [priv des <*privacy password*>]]

auth { md5 | sha } <*authentication password*>

Specifies the authentication protocol and the authentication password.

`md5`: HMAC-MD5 is used for the authentication protocol.

`sha`: HMAC-SHA1 is used for the authentication protocol.

priv des <*privacy password*>

Specifies the encryption protocol and the encryption password.

1. Default value when this parameter is omitted:

   If `auth` and subsequent parameter options are omitted, an authentication protocol will not be used.

   If `priv des` and subsequent parameter options are omitted, an encryption protocol will not be used.

2. Range of values:

   For <*authentication password*> and <*privacy password*>, set a character string consisting of 8 to 32 characters, enclosed in double quotation marks. Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

vrf <*vrf id*>

Permits accesses from the VRF specified in <*vrf id*>.

1. Default value when this parameter is omitted:

   Permits access from the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a security group name that has not been set by the `snmp-server group` command is set in this command, the security group information set in this command will be invalid.

Related commands

```
snmp-server engineID local
snmp-server view
snmp-server group
snmp-server host
```

snmp-server view

Sets the MIB view information. The MIB view information is used to check the object ID for Variable Bindings contained in SNMP PDUs. The MIB view consists of one subtree or multiple subtrees. A subtree is set by the combination of the object ID and view type. The MIB view created by this command is to be used in the `snmp-server group` command.

The following table describes the number of entries for each parameter that can be set in this command.

Table 13-7: Number of entries for each parameter

No.	Parameter	Maximum number of entries
1	MIB view	50 entries per device
2	Subtree	30 entries for a MIB view
3		500 entries per device

Syntax

To set or change information:

```
snmp-server view <view name> <oid tree> { included | excluded }
```

To delete information:

```
no snmp-server view <view name> <oid tree>
```

Input mode

```
(config)
```

Parameters

<view name>

Sets a MIB view name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters (for example, a space), you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

<oid tree>

Sets an object ID that indicates a subtree.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an object ID in dot notation. You can use 64 or fewer characters. You can also use a wildcard (*) for each sub-ID (numbers separated by a period).

{ included | excluded }

Sets the inclusion or exclusion of a subtree. Specify `included` to include the subtree in the

MIB view. Specify `excluded` to exclude the subtree from the MIB view.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When you change or delete information, if a wildcard (*) is specified for a sub-ID for <*oid tree*>, this entry is treated the same as the entry for which the sub-ID of the same position is `0`. Also, if you set `0` for a sub-ID, this entry is treated the same as the entry for which the sub-ID of the same position is a wildcard (*).

   Therefore, if you change information for one entry, the information of another entry is also overwritten. If you delete information for one entry, the information of another entry is also deleted.

   Example:

```
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.0.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# snmp-server view "READ_VIEW" 1.*.1.1 included
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.*.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# no snmp-server view "READ_VIEW" 1.0.1.1
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.1.1.1 excluded
```

Related commands

```
snmp-server engineID local
snmp-server user
snmp-server group
snmp-server host
```

snmp trap link-status

Prevents a trap or an inform (`linkDown` and `linkUp` traps) from being sent when a `link-up` failure or a `link-down` failure occurs on a line by using the `no snmp trap link-status` command.

Syntax

To set information:

```
no snmp trap link-status
```

To delete information:

```
snmp trap link-status
```

Input mode

`(config-if)`

Ethernet interface or management port

Parameters

None

Default behavior

The sending of traps or informs (`linkDown` and `linkUp` traps) is not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

Chapter 14. Ethernet

bandwidth
description
duplex
flowcontrol
frame-error-notice
interface gigabitethernet
interface hundredgigabitethernet
interface tengigabitethernet
link debounce
link up-debounce
mdix auto
mtu
shutdown
speed
system mtu

bandwidth

Assigns the bandwidth of a line. This setting is used for calculating the line usage rate on a network monitoring device.

Syntax

To set or change information:

```
bandwidth <kbit/s>
```

To delete information:

```
no bandwidth
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<*kbit/s*>

Assigns the line bandwidth in kbit/s.

This setting is used for the `ifSpeed/ifHighSpeed` (SNMP MIB) value of the applicable port, and has no impact on communication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 100000000

   Do not specify a value that exceeds the line speed of the applicable port.

Default behavior

The line speed of the applicable port becomes the bandwidth.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

description

Sets supplementary information. This command can be used as a comment about the port. Note that when this command is set, information can be checked by using the `show interfaces` or `ifDescr` (SNMP MIB) operation commands.

Syntax

To set or change information:

```
description <string>
```

To delete information:

```
no description
```

Input mode

`(config-if)`

Ethernet interface

Parameters

<string>

Sets supplementary information for an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

duplex

Sets the half duplex or full duplex mode for the port.

Syntax

To set or change information:

```
duplex {half | full |auto}
```

To delete information:

```
no duplex
```

Input mode

`(config-if)`

Ethernet interface

Parameters

{half | full |auto}

Sets the connection mode of a port to half duplex (fixed), full-duplex (fixed), or auto-negotiation.

The table below shows the combinations of line types and specifiable parameters. `auto` is set if a non-specifiable parameter for 100BASE-FX is specified.

Table 14-1: Specifiable parameters

Line type	Specifiable parameters
10BASE-T/ 100BASE-TX/ 1000BASE-T	`auto` (when `speed auto`, `auto 10`, `auto 100`, `auto 1000`, `auto 10 100`, or `auto 10 100 1000` is specified) `half` (when `speed 10` or `speed 100` is specified) `full` (when `speed 10` or `speed 100` is specified)
1000BASE-X	`auto` (when `speed auto` or `auto 1000` is specified) `full` (when `speed 1000` is specified)

half

Sets the port to half duplex (fixed) mode.

full

Sets the port to full duplex (fixed) mode.

auto

Determines the half duplex or full duplex mode by auto-negotiation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`auto` is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops

temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is specified for `speed` or `duplex`, auto-negotiation is performed.
2. If auto-negotiation is not used for 10BASE-T, 100BASE-TX, or 1000BASE-T, you must set `speed` to `10` or `100`, and set `duplex` to `full` or `half`.
3. If auto-negotiation is not used for 1000BASE-X, you must set `speed` to `1000`, and set `duplex` to `full`.
4. For 10GBASE-R or 100GBASE-R, `duplex` and `speed` cannot be specified.

Related commands

`speed`

flowcontrol

Sets flow control.

Syntax

To set or change information:

```
flowcontrol send {desired | on | off}
flowcontrol receive {desired | on | off}
```

To delete information:

```
no flowcontrol send
no flowcontrol receive
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

send {desired | on | off}

Specifies the operation for sending flow-control pause packets. Specify the same settings as those for the operation for receiving flow-control pause packets at the destination.

desired

If fixed mode is specified, pause packets are sent. If the auto-negotiation functionality is specified, whether pause packets are sent is determined through communication with the connected device.

on

Pause packets are sent.

off

Pause packets are not sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

receive {desired | on | off}

Sets the operation for receiving flow-control pause packets. Specify the same settings as those for the operation for receiving flow-control pause packets at the destination.

desired

If fixed mode is set, pause packets are received. If the auto-negotiation functionality is specified, whether pause packets are received is determined through communication with the connected device.

on

Pause packets are received.

off

Pause packets are not received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Behavior varies depending on the line type.

- For 10BASE-T, 100BASE-TX, or 1000BASE-T:

  Receive operation is `off` but send operation is `desired`.

- For 1000BASE-X:

  Receive operation is `off` but send operation is `desired`.

- For 10GBASE-R:

  Receive operation is `on` but send operation is `off`.

- For 100GBASE-R:

  Receive operation is `on` but send operation is `off`.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

frame-error-notice

Sets the condition for sending a notification when a frame reception error or a frame sending error occurs. A frame reception error or a frame sending error indicates that a frame is discarded due to a failure in receiving or sending a frame, which is caused by a minor error. The cause of the failure is collected as statistics. If in a 30-second interval, the number of error occurrences or the error occurrence rate exceeds the value that was set by this command, the errors are reported. The settings of this command are applied to all ports of the Device, and the sending side and the receiving side have the same settings.

If this configuration is not set, the errors are reported when 15 or more errors occur in a 30-second interval.

The following table shows the list of statistical items that correspond to frame reception and frame sending errors.

Table 14-2: List of statistical items

Statistical item	
Receiving	**Sending**
• CRC errors • Fragments • Jabber • Overrun • Underrun/Overrun • Symbol errors • Short frames • Long frames	• Late collision • Excessive collisions • Carrier sense lost • Excessive deferral • Underrun • Underrun/Overrun

If an error is reported, a log entry is displayed and a private trap is issued. For details about the log, see the manual *Message and Log Reference For Version 12.1*. For details about private traps, see the manual *MIB Reference For Version 12.1*.

Syntax

To set or change information:

```
frame-error-notice [error-frames <frames>] [error-rate <rate>] [{
one-time-display | everytime-display | off }]
```

Note: At least one parameter must be specified.

To delete information:

```
no frame-error-notice
```

Input mode

```
(config)
```

Parameters

error-frames <*frames*>

Sets, as the error notification condition, the threshold for the number of error occurrences (number of error frames).

1. Default value when this parameter is omitted:

   15

2. Range of values:

   1 to 4464000000

error-rate <*rate*>

Specifies, as the error notification condition, the threshold for the error occurrence rate as a percentage (%). The error occurrence rate is calculated as the rate of the number of error frames compared to the total number of frames. The fractional portion of the rate is truncated, and then it is compared with the set value. Note that if this parameter is omitted, the error occurrence rate is not regarded as a notification condition.

1. Default value when this parameter is omitted:

   The error occurrence rate is not regarded as a notification condition.

2. Range of values:

   1 to 100

The notification condition varies depending on whether the `error-frames` parameter and/or the `error-rate` parameter are set. The following table shows the error notification conditions depending on whether each parameter is set.

Table 14-3: List of error notification conditions

No.	Parameter		Receiving/sending	Error notification condition
	error-frames	error-rate		
1	Omitted	Omitted	Receiving	The number of reception error frames is 15 or more
2			Sending	The number of sending error frames is 15 or more
3		Yes	Receiving	The rate of reception error frames compared to the total number of reception frames is equal to or greater than the value that was set for <*rate*>. This setting does not regard the number of error occurrences as a notification condition.
4			Sending	The rate of sending error frames compared to the total number of sending frames is equal to or greater than the value that was set for <*rate*>. This setting does not regard the number of error occurrences as a notification condition.

No.	Parameter		Receiving/sending	Error notification condition
	error-frames	error-rate		
5	Yes	Omitted	Receiving	The number of reception error frames is equal to or greater than the value that was set for <*frames*>. This setting does not regard the error occurrence rate as a notification condition.
6			Sending	The number of sending error frames is equal to or greater than the value that was set for <*frames*>. This setting does not regard the error occurrence rate as a notification condition.
7		Yes	Receiving	The number of reception error frames is equal to or greater than the value that was set for <*frames*>, and the rate of reception error frames compared to the total number of reception frames is equal to or greater than the value that was set for <*rate*>.
8			Sending	The number of sending error frames is equal to or greater than the value that was set for <*frames*>, and the rate of sending error frames compared to the total number of sending frames is equal to or greater than the value that was set for <*rate*>.

{one-time-display | everytime-display | off }

Specifies whether to display a log entry when an error is reported. If a large number of errors occur continuously, this setting can prevent the log file from being filled with this log entry. Note that this parameter has no impact on private traps. Use the `snmp-server host` command to specify whether to issue a private trap.

one-time-display

Displays a log entry only when an error is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error occurrence after the restart is reported.

everytime-display

Displays a log entry every time an error is reported.

off

No log entries are displayed.

1. Default value when this parameter is omitted:

   one-time-display

2. Range of values:

   None

Default behavior

When 15 or more errors occur in a 30-second time interval, the errors are reported. Displays a log entry only when an error is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error after the restart is reported.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you use this command to set the configuration, you must specify at least one parameter.
2. Entering this command disables the settings specified until then. If you want to inherit the old settings, use this command to specify the applicable parameter again.

Related commands

`snmp-server host`

interface gigabitethernet

Sets the related items for 10BASE-T, 100BASE-TX, 1000BASE-T, and 1000BASE-X. Entering this command switches to config-if mode, in which information about the relevant port can be set.

Various information for the Ethernet subinterface can be set by specifying the subinterface of this command and switching to the config-subif mode.

Syntax

To set information:

```
interface gigabitethernet <nif no.>/<port no.>
interface gigabitethernet <nif no.>/<port no.>.<subinterface index>
```

To delete information:

```
no interface gigabitethernet <nif no.>/<port no.>
no interface gigabitethernet <nif no.>/<port no.>.<subinterface index>
```

Input mode

```
(config)
```

Parameters

<nif no.>/<port no.>

Specifies the NIF number and the port number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

<nif no.>/<port no.>.<subinterface index>

Specifies the NIF number, port number, and subinterface index.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

interface hundredgigabitethernet

Sets items related to 100GBASE-R. Entering this command switches to config-if mode, in which information about the relevant port can be set.

Various information for the Ethernet subinterface can be set by specifying the subinterface of this command and switching to the config-subif mode.

Syntax

To set information:

```
interface hundredgigabitethernet <nif no.>/<port no.>
interface hundredgigabitethernet <nif no.>/<port no.>.<subinterface index>
```

To delete information:

```
no interface hundredgigabitethernet <nif no.>/<port no.>
no interface hundredgigabitethernet <nif no.>/<port no.>.<subinterface
index>
```

Input mode

```
(config)
```

Parameters

<nif no.>/<port no.>

Specifies the NIF number and the port number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

<nif no.>/<port no.>.<subinterface index>

Specifies the NIF number, port number, and subinterface index.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

interface tengigabitethernet

Sets the items related to 10GBASE-R. Entering this command switches to config-if mode, in which information about the relevant port can be set.

Various information for the Ethernet subinterface can be set by specifying the subinterface of this command and switching to the config-subif mode.

Syntax

To set information:

```
interface tengigabitethernet <nif no.>/<port no.>
interface tengigabitethernet <nif no.>/<port no.>.<subinterface index>
```

To delete information:

```
no interface tengigabitethernet <nif no.>/<port no.>
no interface tengigabitethernet <nif no.>/<port no.>.<subinterface index>
```

Input mode

```
(config)
```

Parameters

<nif no.>/<port no.>

Specifies the NIF number and the port number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

<nif no.>/<port no.>.<subinterface index>

Specifies the NIF number, port number, and subinterface index.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

link debounce

Sets the link-down detection time after a link failure is detected until the actual link-down occurs. When a large value is set, temporary link-downs will not be detected, thereby preventing instability of the link.

Syntax

To set or change information:

```
link debounce [time <milli seconds>]
```

To delete information:

```
no link debounce
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

time <*milli seconds*>

Sets the debounce timer value in milliseconds.

1. Default value when this parameter is omitted:

   3000 milliseconds

2. Range of values:

   Multiples of 100, from 0 to 10000

Default behavior

For 10BASE-T, 100BASE-TX, and 1000BASE-T: Operates at 2000 milliseconds.

For 1000BASE-X, 10GBASE-R, and 100GBASE-R: Operates at 0 milliseconds.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the link is stable even when a link-down detection timer is not set, you do not need to set one.
2. If a value smaller than the default value (2000 milliseconds) is set for 10BASE-T, 100BASE-TX, or 1000BASE-T, the link might become unstable.

Related commands

None

link up-debounce

Sets the link-up detection time after a link failure is detected until the actual link-up occurs. When a large value is set, a temporary link-up will not be detected, thereby preventing instability of the network status.

Syntax

To set or change information:

```
link up-debounce time <milli seconds>
```

To delete information:

```
no link up-debounce
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

time <*milli seconds*>

Sets the debounce timer value when a link-up state occurs, in milliseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Multiples of 100, from 0 to 10000

Default behavior

When the line speed is fixed, the operating value is 1000 milliseconds. When the line speed is set to auto-negotiation, the operating value is 0 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. 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.
2. If you set a value smaller than the default value, the link might become unstable.

Related commands

```
duplex
link debounce
speed
```

mdix auto

The automatic MDI/MDIX function is disabled and fixed to the MDI by the `no mdix auto` command.

Syntax

To set information:

```
no mdix auto
```

To delete information:

```
mdix auto
```

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

During auto-negotiation, MDI and MDI-X are switched automatically.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is enabled during auto-negotiation.
2. For 1000BASE-X, this command is disabled.
3. For 10GBASE-R, this command cannot be specified.
4. For 40GBASE-R, this command cannot be specified.

Related commands

`speed`

mtu

Sets the maximum frame length of a port. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

```
mtu <length>
```

To delete information:

```
no mtu
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<*length*>

Sets the maximum frame length of a port in octets. The maximum frame length is the length from the DA of the Ethernet V2 format frame MAC header to the data.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1518 to 9596

Default behavior

The following initial values are set.

Table 14-4: Initial values of the port maximum frame length

Presence of the system mtu command	Initial value
Set	The setting value for `system mtu`
Not set	1518

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the length of the frames that can be sent or received for the target port.

   Table 14-5: Length of the frames that can be sent or received

Line type	mtu setting	system mtu setting	Length of a frame that can be sent or received (in octets)
10BASE-T (full and half-duplex), 100BASE-TX (half-duplex)	Not related	Not related	1518

Line type	mtu setting	system mtu setting	Length of a frame that can be sent or received (in octets)
Other	Set	Not related	M1#1
	Not set	Set	M2#2
		Not set	1518

#1: The value that was set by using the `mtu` command of `interface`.

#2: The value that was set by using the `system mtu` command.

2. The table below describes the length of frames that can be sent or received, depending on the settings of the `mtu` command for the interface and the settings of the MTU for the IP.

   Table 14-6: Length of frames that can be sent or received by the setting of the mtu command and ip mtu command (octet)

mtu settings	IP MTU settings	Length of a frame that can be sent or received (in octets)
Omitted	Omitted	1518
	Set	min (1518, L2#1 +18)
Set	Omitted	L1#2
	Set	min (L1#2, L2#1 +18)

#1: The value that was set by using the `ip mtu` command.

#2: The value that was set by using the `mtu` command of `interface`.

3. Specify the value by adding 18 octets or more to the specified value of the `ip mtu` command. If it is less than 18 octets, the `ip mtu` command will operate at a value equal to this setting with 18 octets subtracted.
4. In case the NIF is NMCG-1C, the frame via target port might be temporarily discarded when the maximum frame length is changed for the port that is currently communicating.

Related commands

None

shutdown

Places the port in the shutdown state. The command also turns off the port's power.

Syntax

To set information:

```
shutdown
```

To delete information:

```
no shutdown
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

None

speed

Sets the port speed.

Syntax

To set or change information:

```
speed { 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }
```

To delete information:

```
no speed
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

{ 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

Sets the line speed.

The table below shows the combinations of line types and specifiable parameters. `auto` is set if a non-specifiable parameter for 100BASE-FX is specified.

Table 14-7: Specifiable parameters

Line type	Specifiable parameters
10BASE-T/ 100BASE-TX/ 1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
1000BASE-X	1000 auto auto 1000

10

Sets the line speed to 10 Mbit/s.

100

Sets the line speed to 100 Mbit/s.

1000

Sets the line speed to 1000 Mbit/s.

auto

Sets the line speed to auto-negotiation.

auto {10 | 100 | 1000 | 10 100 | 10 100 1000}

Auto-negotiation is performed at the specified line speed. This setting prevents the line speed from operating at an unexpected speed, so the line usage rate is prevented from increasing. If negotiation at the specified line speed does not succeed, the link status does not transition to link-up status.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`auto` is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is specified for `speed` or `duplex`, auto-negotiation is performed.
2. If auto-negotiation is not used for 10BASE-T, 100BASE-TX, or 1000BASE-T, you must set `speed` to `10` or `100`, and set `duplex` to `full` or `half`.
3. If auto-negotiation is not used for 1000BASE-X, you must set `speed` to `1000`, and set `duplex` to `full`.
4. For 10GBASE-R or 100GBASE-R, `duplex` and `speed` cannot be specified.

Related commands

`duplex`

system mtu

Sets the maximum frame length of all ports. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

```
system mtu <length>
```

To delete information:

```
no system mtu
```

Input mode

```
(config)
```

Parameters

<*length*>

Sets the maximum frame length of all ports in octets. The maximum frame length is the length from the DA of the Ethernet V2 format frame MAC header to the data.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1518 to 9596

Default behavior

The maximum frame length of all ports is set to 1518.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the length of frames that can be sent or received for the port.

   Table 14-8: Length of frames that can be sent or received

Line type	mtu setting	system mtu setting	Length of a frame that can be sent or received (in octets)
10BASE-T (full and half-duplex), 100BASE-TX (half-duplex)	Not related	Not related	1518
Other	Set	Not related	M1#1
	Not set	Set	M2#2
		Not set	1518

#1: The value that was set by using the `mtu` command of `interface`.

#2: The value that was set by using the `system mtu` command.

2. Specifies the value by adding 18 or more octets to the specified value of the `ip mtu` command. If it is less than 18 octets, the `ip mtu` command will operate at a value equal to this setting with 18 octets subtracted.
3. In case the NIF is NMCG-1C, the frame via target port might be temporarily discarded when the maximum frame length is changed for the port that is currently communicating.

Related commands

None

Chapter

15. Link Aggregation

channel-group lacp system-priority
channel-group load-balance
channel-group max-active-port
channel-group max-detach-port
channel-group mode
channel-group multi-speed
channel-group non-revertive
channel-group periodic-timer
description
interface port-channel
lacp port-priority
lacp system-priority
shutdown

channel-group lacp system-priority

Sets the LACP system priority of the applicable channel group for link aggregation.

Syntax

To set or change information:

```
channel-group lacp system-priority <priority>
```

To delete information:

```
no channel-group lacp system-priority
```

Input mode

```
(config-if)
```

Port channel interface

Parameters

<*priority*>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

The settings of the `lacp system-priority` command are used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down temporarily and then goes up.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you set a restriction on the number of detached ports (`max-detach-port`) to connect the Device to a device from other manufacturers, set a higher LACP system priority level for the Device.
3. If the LACP system priority is changed, the status of all ports registered for the channel group temporarily changes to `Blocking` (communication interrupted).

Related commands

None

channel-group load-balance

Sets the allocation method for link aggregation.

Syntax

To set or change information:

```
channel-group load-balance {frame | vlan}
```

To delete information:

```
no channel-group load-balance
```

Input mode

```
(config-if)
```

Port channel interface

Parameters

{frame | vlan}

frame

Allocates in accordance with the information within the receive frame.

vlan

Allocates for each VLAN Tag of the frame to be sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The information within the receive (frame).

Impact on communication

If specified for an active port, the allocation-source might be changed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

channel-group max-active-port

Sets the maximum number of active ports that will be used for link aggregation in the applicable channel group.

Syntax

To set information:

```
channel-group max-active-port <number> [no-link-down]
```

To change information:

```
channel-group max-active-port <number>
channel-group max-active-port <number> no-link-down
```

To delete information:

```
no channel-group max-active-port
```

Input mode

`(config-if)`

Port channel interface

Parameters

<*number*>

Specifies the maximum number of ports that will be used for link aggregation in a channel group. If the number of ports that are actually used in a channel group exceeds the value specified by this command, only the specified maximum number of ports are used, and the standby link functionality is applied to the rest of the ports.

If `no-link-down` is specified, `no-link-down` cannot be omitted when changing the value.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 16

no-link-down

To use the standby link functionality in a link-not-down mode, specify this parameter. Otherwise, standby links device to the link-down status. The criteria for selecting which links are standby links are as follows:

- Select ports that have been assigned lower priority by using the `lacp port-priority` command.
- If the priority is the same, select the port with the larger NIF number and larger port number.

1. Default value when this parameter is omitted:

   Standby links device to link-down status.

2. Range of values:

   None

Default behavior

The maximum number is 16.

Impact on communication

The ports that are in use might be changed by the standby link functionality, and communication might stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when static link aggregation is used.
2. If you specify `max-active-port` command in the link-down status, match its settings to the settings of the `max-active-port` and `lacp port-priority` commands on the destination device.
3. Ports in standby link mode cannot be changed directly between the link-down and no-link-down statuses. To change the status, delete this parameter, and then set this parameter again. To change the number of ports in a link-not-down mode, you must specify the `no-link-down` parameter.
4. If this command is set and a port in link-down status is selected as a standby link, only the log entries that indicate detachment are displayed. Log entries indicating aggregation for the ports are not displayed.

Related commands

```
channel-group mode
lacp port-priority
```

channel-group max-detach-port

Limits the maximum number of detached ports in the applicable link aggregation channel group.

Syntax

To set or change information:

```
channel-group max-detach-port <number>
```

To delete information:

```
no channel-group max-detach-port
```

Input mode

```
(config-if)
```

Port channel interface

Parameters

<*number*>

Specifies the maximum number of ports that can be detached from a channel group used for link aggregation for reasons such as a link down. The applicable channel group will go down when the number of ports with link-down has exceeded the specified value.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 15

Default behavior

15 is set as the limit on the maximum number of detached ports.

Impact on communication

Channel groups might go down due to a limit on the number of detached ports.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you specify the `max-detach-port` command, match its settings to the settings of the destination device.
3. This function operates when the LACP system priority of the Device that is set with number of port detachment restriction functionality (`max-detach-port`) is higher than the destination device.

Related commands

```
channel-group lacp system-priority
channel-group mode
lacp system-priority
```

channel-group mode

Creates a channel group for link aggregation.

Syntax

To set information:

```
channel-group <channel group number> mode {on | active | passive}
```

To change information:

```
channel-group <channel group number> mode {active | passive}
```

To delete information:

```
no channel-group
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<*channel group number*>

Specifies the channel group number for link aggregation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

{on | active | passive}

Specifies the mode for link aggregation.

on

Static link aggregation is performed.

active

LACP-based link aggregation is performed, and LACPDUs are always sent, regardless of their relationship with the remote device.

passive

LACP-based link aggregation is performed, but LACPDUs are sent only when an LACPDU from the remote device is received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

If this setting is specified for an active port, communication temporarily stops.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To change static link aggregation to LACP-based link aggregation, or vice versa, delete this command, change the mode, and then set the command again.
2. When `channel-group mode` is set, the `port-channel` setting of the specified channel group is automatically generated. If `port-channel` has already been set, no specific operation is required.
3. If the `port-channel` setting of the specified channel group number already exists when you set this command, you must either specify the same setting for the applicable interface and the port channel interface with the specified channel group number, or else not set a common configuration command for the applicable interface. For details, see *17.2.4 Configuring a port channel interface* in the manual *Configuration Guide Vol. 1 For Version 12.1*.
4. To delete this command, set the `shutdown` command with configuration command mode for the Ethernet interface, and then delete it.
5. Deleting this command does not delete the `port-channel` configuration (deleting all ports in a channel group does not delete the `port-channel` configuration). When deleting a channel group, you must manually delete the `port-channel` configuration.

Related commands

None

channel-group multi-speed

Sets mixed-speed mode. If this command is set, ports with different transmission speeds can be used simultaneously in a channel group for link aggregation.

Syntax

To set information:

```
channel-group multi-speed
```

To delete information:

```
no channel-group multi-speed
```

Input mode

```
(config-if)
```

Port channel interface

Parameters

None

Default behavior

Disables mixed-speed mode.

Impact on communication

The ports that are in use might be changed by the standby link functionality, and communication might stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When frames are sent, ports are allocated irrespective of the port transmission speed.
2. Set this function on the destination device, too.

Related commands

None

channel-group non-revertive

Sets the switch back suppression to the channel group. If this command is set, consolidation of the ports detached from the channel group is suppressed, and automatic switch back of the frame send port is suppressed.

Switch back suppression operates when the channel group is in the up status. The time for switch back suppression to start operating after the channel group goes up can be specified by the `seconds` parameter.

Syntax

To set or change information:

```
channel-group non-revertive [<seconds>]
```

To delete information:

```
no channel-group non-revertive
```

Input mode

`(config-if)`

Port channel interface

Parameters

<*seconds*>

Specifies the operation delay time (seconds) for switch back suppression.

1. Default value when this parameter is omitted:

   600

2. Range of values:

   0 to 86400

Default behavior

Switch back suppression is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. In the channel group, when all the ports other than the ports where switch back is suppressed go down, the ports that switch back is suppressed are consolidated to continue the up status of the channel group.
3. Execute the `clear channel-group non-revertive` operation command to consolidate the ports in the channel group where switch back is suppressed.
4. This function operates when the LACP system priority of the Device is higher than the destination device.

Related commands

None

channel-group periodic-timer

Specifies the interval for sending LACPDUs.

Syntax

To set or change information:

```
channel-group periodic-timer { long | short }
```

To delete information:

```
no channel-group periodic-timer
```

Input mode

```
(config-if)
```

Port channel interface

Parameters

{ long | short }

Specifies the interval at which the partner device sends LACPDUs to the Device.

long

30 seconds

short

1 second

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`long` (30 seconds) is set as the sending interval.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.

Related commands

```
channel-group mode
```

description

Sets supplementary information. This command can be used as a comment about the channel group. Note that when this command is set, information can be checked by using the `show channel-group` or `ifDescr` (SNMP MIB) operation command.

Syntax

To set or change information:

```
description <string>
```

To delete information:

```
no description
```

Input mode

`(config-if)`

Port channel interface

Parameters

<*string*>

Sets supplementary information for the applicable channel group used for link aggregation. Use this command to create and attach a note to the interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

interface port-channel

Sets an item related to a port channel interface. Entering this command switches to `config-if` mode, which allows you to use configuration commands to specify the channel group number. Switches to the config-subif (port channel subinterface) mode when the subinterface is specified with this command, allowing the configuration command for the port channel subinterface to be set. A port channel interface is automatically generated when the `channel-group mode` command is set.

Syntax

To set information:

```
interface port-channel <channel group number>
interface port-channel <channel group number>.<subinterface index>
```

To delete information:

```
no interface port-channel <channel group number>
no interface port-channel <channel group number>.<subinterface index>
```

Input mode

```
(config)
```

Parameters

<channel group number>

Specifies the channel group number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

<channel group number>.<subinterface index>

Specifies the channel group number and subinterface index.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you want to delete the port channel interface by using this command, do so after executing the `shutdown` command for all ports in the applicable channel group. The `shutdown` command is not required when deleting the port channel subinterface.

Related commands

None

lacp port-priority

Sets the port priority.

Syntax

To set or change information:

```
lacp port-priority <priority>
```

To delete information:

```
no lacp port-priority
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<*priority*>

Specifies the port priority. The lower the value, the higher the priority.

When on is specified for the `channel-group mode` command:

This parameter is used with the `max-active-port` command to select the standby links.

When `active` or `passive` is specified for the `channel-group mode` command:

This parameter applies to port priority for the LACP protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

128 is set as the port priority.

Impact on communication

If you specify the port priority for an active port by setting `channel-group mode` to `active` or `passive`, communication is temporarily interrupted. If you specify port priority for active ports by setting `channel-group mode` to `on`, ports that use the standby link functionality might be changed, and communication might temporarily stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you specify the `max-active-port` command, match its settings to the settings of `max-active-port` for the destination device.
2. If you change <*priority*>, the status of the applicable port temporarily changes to `Blocking` (communication interrupted).

Related commands

```
channel-group max-active-port
channel-group mode
```

lacp system-priority

Sets the effective LACP system priority for the Device.

Syntax

To set or change information:

```
lacp system-priority <priority>
```

To delete information:

```
no lacp system-priority
```

Input mode

```
(config)
```

Parameters

<priority>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

If the `channel-group lacp system-priority` command has been set, that setting is used. If the `channel-group lacp system-priority` command has not been set, 128 is used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down temporarily and then goes up.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you set a restriction on the number of detached ports (`channel-group max-detach-port`) to connect the Device to a device from other manufacturers, set a higher LACP system priority level for the Device.
3. If the LACP system priority is changed, the status of all ports registered for the channel group temporarily changes to `Blocking` (communication interrupted).

Related commands

```
channel-group max-detach-port
```

shutdown

Always disables the applicable channel group for link aggregation, and stops communication.

Syntax

To set information:

```
shutdown
```

To delete information:

```
no shutdown
```

Input mode

```
(config-if)
```

Port channel interface

Parameters

None

Default behavior

Allows the operation of the applicable channel group.

Impact on communication

If a priority is specified for an active channel group, the channel group goes down.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

Chapter

16. IP Interface

description
dot1q ethertype
encapsulation dot1q
shutdown
snmp trap link-status

description

Sets the supplemental explanation of the Ethernet subinterface or the port channel subinterface. This can be used as a note for the Ethernet subinterface or the port channel subinterface.

Syntax

To set or change information:

```
description <string>
```

To delete information:

```
no description
```

Input mode

```
(config-subif)
```

Ethernet subinterface or port channel subinterface

Parameters

<*string*>

Sets the supplemental explanation of the Ethernet subinterface or the port channel subinterface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Alphanumeric and special characters can be specified. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

dot1q ethertype

Sets the TPID (Tag Protocol IDentifier) value of a VLAN tag that is assigned by a Device. This command is set when you connect to a network in which a non-standard TPID value is used.

Syntax

To set or change information:

```
dot1q ethertype <hex>
```

To delete information:

```
no dot1q ethertype
```

Input mode

```
(config)
```

Parameters

<*hex*>

Sets the TPID value of a VLAN tag that is assigned by a Device. This command sets the default value of the entire Device.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Four-digit hexadecimal

Default behavior

`0x8100` is used as the TPID value.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

encapsulation dot1q

Sets the VLAN ID to logically multiplex the Ethernet subinterface or the port channel subinterface with the VLAN Tag.

Syntax

To set or change information:

```
encapsulation dot1q {<vlan id> | untagged}
```

To delete information:

```
no encapsulation dot1q
```

Input mode

```
(config-subif)
```

Ethernet subinterface or port channel subinterface

Parameters

{<*vlan id*> | untagged}

Specifies the VLAN ID used for Tag-VLAN linkage or untagged.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about the range of values, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

shutdown

Sets the Ethernet subinterface or the port channel subinterface to the shutdown status.

Syntax

To set information:

```
shutdown
```

To delete information:

```
no shutdown
```

Input mode

```
(config-subif)
```

Ethernet subinterface or port channel subinterface

Parameters

None

Default behavior

None

Impact on communication

Stops the communication in the specified Ethernet subinterface or the port channel subinterface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

None

snmp trap link-status

Controls the sending of the trap or the inform (`linkDown` trap and `linkUp` trap) when the Ethernet subinterface or the port channel subinterface has gone up or down.

Syntax

To set information:

```
snmp trap link-status
```

To delete information:

```
no snmp trap link-status
```

Input mode

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

None

Default behavior

Traps or informs (`linkDown` and `linkUp` traps) are not sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, the trap or inform is sent when the interface goes up or down after the sending is set with this command.

Notes

None

Related commands

None

Chapter 17. Error Messages Displayed When Editing the Configuration

17.1 Common errors

17.1.1 Syntax errors

Table 17-1: Error messages related to syntax errors

Message	Description
The '$<*parameter*>' is duplicated.	The $<*parameter*> specified in the template is duplicated.
The '$<*parameter*>' is invalid.	While handling $<*parameter*>, the problems below occurred. Review the $<*parameter*> settings. • A parameter $<*parameter*> that was not set by the template command was input to the configuration command. Use the parameter $<*parameter*> that was set by the template command. • The settings of the parameter $<*parameter*> used in the template cannot be deleted. Remove the parameter $<*parameter*> that was used in the template from the list of items for deletion. • The number of $<*parameter*> parameters specified with the parameter of the `apply-template` command exceeds the number of $<*parameter*> parameters set with the parameter of the `template` command. The number of $<*parameter*> parameters specified with the parameter of the `apply-template command should be less than the number of` $<*parameter*> parameters set with the parameter of the `template` command. • The value is not set to the parameter $<*parameter*> that is used in the template. For the parameter $<*parameter*> specified in the parameters of the `apply-template` command, include all the $<*parameter*> parameters that are used in the template.
The configuration command cannot be inserted because the hierarchy does not match.	A configuration command cannot be inserted because the hierarchy is different.
The configuration command cannot be replaced because the hierarchy does not match.	A configuration command cannot be replaced because the hierarchy is different.
The configuration command syntax is incorrect. (line = <*line number*>, message = <*error message*>)	The command syntax in the configuration file is invalid. Review the configuration file or the configuration being edited.
	<*line number*>: Number of lines in a merge file <*error message*>: Error message content
The configuration command syntax is incorrect. (line = <*line number*>, syntax = <*error syntax*>)	The configuration command syntax is invalid. Set the configuration again with the correct syntax.
	<*line number*>: Line number where the error occurred <*error syntax*>: Error syntax
The IPv4 address is invalid. (address = <*value1*>)	<*value1*> is outside the valid IPv4 address range. Set a value within the range.
	<*value1*>: Invalid value
The IPv6 address is invalid. (address = <*value1*>)	<*value1*> is outside the valid IPv6 address range. Set a value within the range.
	<*value1*>: Invalid value
The MAC address is invalid. (address = <*value1*>)	<*value1*> is outside the valid MAC address range. Set a value within the range.
	<*value1*>: Invalid value

Message	Description
The mask is invalid. (mask = <*value1*>)	<*value1*> is outside the valid subnet mask range. Set a value within the range.
	<*value1*>: Invalid value
The parameter is outside the range. (parameter = <*value1*>, minimum value = <*value2*>, maximum value = <*value3*>)	The value of the <*value1*> parameter is outside the valid range. Set a value within the range.
	<*value1*>: Parameter name <*value2*>: Minimum value <*value3*>: Maximum value
The specified 'file name', 'command', or 'parameter' is too long.	The specified file name, command or parameter is too long.
The syntax is incorrect. (syntax = <*value1*>)	The configuration command syntax or the value is invalid. Set the configuration again with the correct syntax or value.
	<*value1*>: Invalid value
The value is too long or is invalid. (maximum = <*value1*> characters)	The number of characters exceeds the maximum value (<*value1*>), or an invalid character is contained. Use the determined format.
	<*value1*>: Number of characters that can be entered
The value is too long or is invalid. (maximum = <*value1*> digits)	The number of characters you entered exceeds the maximum number of digits (<*value1*>), or an invalid character exists. Use the determined format.
	<*value1*>: Number of digits that can be entered
There are not enough parameters.	No parameters are specified. Specify the necessary parameters.

17.1.2 Errors related to exceeding the maximum

Table 17-2: Error messages related to exceeding the maximum

Message	Description
The maximum number of entries are already configured. (failed entry = <*value1*>)	An attempt is being made to set a configuration that is larger than the capacity limit or to change a configuration in an environment that is already at the maximum capacity limit. Delete configurations that are no longer used, and then set the configuration again.
	<*value1*>: Entry name for the maximum capacity limit
The number of elements in the list is too many. (The maximum number of elements = <*value1*>)	The maximum number of specifiable elements is <*value1*>. Check if the number does not exceed the capacity limit.
	<*value1*>: The maximum number of elements that can be specified for a list
The sequence number exceeds the maximum value. Try the 'resequence' command.	The sequence number exceeds the maximum value. To specify an entry, execute the `resequence` command, and then specify this entry again.
The specified number of interfaces exceeds the maximum.	The interface cannot be set because the number of interfaces exceeds the maximum value.

17.1.3 Errors when editing the configuration

Table 17-3: Error messages displayed when editing the configuration

Message	Description
A different name is already configured.	A different name is already set.
A required parameter has no value. (parameter = <*value1*>)	Because the <*value1*> information that is a prerequisite condition for a setting does not exist, the setting cannot be specified. Set the <*value1*> information.
	<*value1*>: Configuration
An error occurred when the 'apply-template' command is under execution. (line = <*line number*>, syntax = <*error syntax*>, message = <*error message*>)	An error occurred while the `apply-template` command was being executed.
	<*line number*>: Number of lines in template <*error syntax*>: Error syntax <*error message*>: Error message content
No change is possible because there is no such data.	Cannot be changed because there is no matching data. Check if information to be changed exists.
No deletion is possible because there is no such data.	It cannot be deleted because there is no matching data. Check if the information to be deleted exists.
The command cannot be executed in the current configuration commit mode.	This command cannot be executed in the current configuration commit mode.
The configuration file cannot be saved because the specified command or parameter is incorrect.	The configuration file cannot be saved because the specified command or parameter is invalid.
The specified interface was not found.	The specified interface was not found. Check the interface setting.
The specified value was not found. (value = <*value1*>)	The specified <*value1*> information was not found. Check if the <*vlaue1*> information has been set.
	<*value1*>: Configuration
This configuration cannot be deleted because it is referenced by another configuration.	This configuration cannot be changed because it is specified by another configuration. Delete the configuration that refers to this configuration, and then retry the deletion.
This configuration cannot be set because the following item has already been set. (item = <*value1*>)	<*value1*> information has already been set. Delete <*value1*> information or check that the required information is set.
	<*value1*>: The configuration set
This configuration cannot be set because the following item has already been set. (item = <*value1*>, configuration = <*value2*>)	<*value1*> information has already been set. <*value2*> could not be set. Delete <*value1*> information or check that the required information is set.
	<*value1*>: The configuration set <*value2*>: The configuration specified
This configuration has already been set.	This configuration has been set.
Use the 'commit' command to save the configuration to the startup configuration.	Use the commit command to save the configuration to the startup configuration in manual commit mode.

17.1.4 Errors related to the handling of the configuration file

Table 17-4: Error messages related to the handling of the configuration file

Message	Description
A file name or directory path is too long.	The path to the target is too long. Shorten the path length.
Access permission is required.	The access permission for the target does not exist. Remove the access restrictions for the file or directory using the `chmod` operation command.
Specify a file name that is not a directory name.	The directory cannot be specified. Specify a file name.
The configuration file is empty.	There are no contents in the configuration.
The file format is incorrect.	The file format is invalid. Make sure the name of the specified file is correct.
The file name is too long.	The specified file name is too long. Shorten the file name.
The file transfer failed. (reason = <*reason*>)	A file transfer with the remote server failed. Retry the command with the `debug` parameter specified to check.
	<*reason*>: Additional information
There is no such file or directory.	The specified file or directory is not found. Specify the correct file name or directory name.

17.1.5 Errors related to conflicts between the hardware and the configurations

Table 17-5: Error messages related to conflict between the hardware and the configurations

Message	Description
A port is not mounted. (NIF/port = <*value1*>)	The number of the port which is not mounted is specified. Set the number of the port that is mounted, or check the status of the applicable NIF and port in the Device.
	<*value1*>: NIF number/port number
The line type is invalid.	The line type is invalid.
The NIF number is invalid. (NIF = <*value1*>)	<*value1*> is outside the valid NIF number range. Set a value within the range.
	<*value1*>: Invalid value
The port number is invalid. (port = <*value1*>)	<*value1*> is outside the valid port number range. Set a value within the range.
	<*value1*>: Invalid value
This configuration is active.	This configuration cannot be modified because it is in compliance with the implementation.

17.1.6 Errors related to the device and software status

Table 17-6: Error messages related to the device and software status

Message	Description
A logical inconsistency occurred.	An internal program problem occurred.
A process is starting. Wait a while, and then try again. (process = <*process*>)	A program is being started. Wait a while, and then try again.
	<*process*>: Program name
A resource is temporarily unavailable. Wait a while, and then try again.	Resource is temporarily insufficient. Wait a while, and then try again.
Command execution failed because a NIF board was being changed.	The command cannot be executed because the NIF is being changed.
Command execution failed because a switchover was in progress.	The command cannot be executed because a system switchover is in progress.
Command execution failed because another command was executing.	The command cannot be executed because it conflicts with a command which is being executed.
Command execution failed because multiple commands cannot be executed at the same time.	Multiple commands cannot be executed concurrently.
Command execution failed because the active and standby configurations do not match.	The configuration of the active BCU and the standby BCU devices does not match. When the software versions of the active BCU and the standby BCU match, restart the standby BCU, and match the running configuration and editing configuration of the standby BCU to the active BCU. When the software versions of the active BCU and the standby BCU do not match, after matching the software versions of the active BCU and standby BCU, restart both BCUs.
Command execution failed because the configuration file was being edited.	This command cannot be executed because another user is editing the configuration.
Command execution failed because the configuration file was being saved.	No edit command can be executed while saving the configuration.
Command execution failed because the software versions do not match.	The command cannot be executed because the software versions of the active BCU and the standby BCU do not match.
Command execution failed because the system was synchronizing the active and standby configurations.	The command cannot be executed because the standby BCU configuration is synchronizing with the active BCU configuration.
Communication failed between the active and standby systems.	Communication failed between the active BCU and standby BCU devices. The configuration might not be applied to the standby BCU. Use the `synchronize diff` command to check the synchronization state of the configuration. When the standby BCU is not synchronized with the active BCU, if the software versions of the active BCU and the standby BCU match, restart the standby BCU, and match the running configuration and editing configuration of the standby BCU to the active BCU. When the software versions of the active BCU and the standby BCU do not match, after matching the software versions of the active BCU and standby BCU, restart both BCUs.
Configuration data could not be deleted temporarily. Wait a while, and then try again.	Deletion is not permitted temporarily because the configuration you entered is not completed. Wait a while, and then try again.

Message	Description
The 'save' command is executing. Wait a while, and then try again.	The operation is not permitted because the `save` command is being executed. Wait a while, and then try again.
The command cannot be executed because of a change in the configuration commit mode.	The command cannot be executed because commit mode of the configuration is being changed.
The command is temporarily unexecutable because the standby system is not operating.	The command cannot be executed temporarily because the standby BCU is not operating.
The configuration data is being changed. Wait a while, and then try again.	The configuration you entered cannot be edited because it is not completed. Wait a while, and then try again.
The configuration file was successfully changed on the active system, but not on the standby system because copying of the configuration file failed.	The configuration of the active BCU device was saved successfully, but application of the configuration to the standby BCU device failed.
The configuration was successfully changed on the active system, but not on the standby system. (reason = <*reason*>)	The configuration of the standby BCU cannot be changed because a problem occurred in an internal program. When the software versions of the active BCU and the standby BCU match, restart the standby BCU, and match the running configuration and editing configuration of the standby BCU to the active BCU. When the software versions of the active BCU and the standby BCU do not match, after matching the software versions of the active BCU and standby BCU, restart both BCUs.
	<*reason*>: Additional information
The maximum number of entries are already configured. Configuration memory is insufficient. (entry = <*value1*>)	Memory for the configuration is full. Delete entries that are no longer needed, execute the `save` or `commit` command, and then add an entry.
	<*value1*>: Entry name
The standby configuration cannot be changed because shared memory of the standby system is insufficient. (reason = <*reason*>)	The configuration of the standby BCU cannot be changed because of a shortage of shared memory on the standby BCU. When the software versions of the active BCU and the standby BCU match, restart the standby BCU, and match the running configuration and editing configuration of the standby BCU to the active BCU. When the software versions of the active BCU and the standby BCU do not match, after matching the software versions of the active BCU and standby BCU, restart both BCUs.
	<*reason*>: Additional information
The standby configuration cannot be changed because the boards of the active and standby systems do not match.	The configuration of the standby BCU cannot be changed because different board types are installed on the active BCU and the standby BCU.
There is not enough free space on the device.	Capacity at the write destination is insufficient. Delete files that are no longer needed.
There is not enough memory, or the configuration file is too large.	There is not enough memory to save the configuration because it is too large.

17.2 Errors when specifying login security and RADIUS or TACACS+ settings

Table 17-7: Error messages when specifying login security and RADIUS or TACACS+ settings

Message	Description
Enter a longer password.	We recommend using a minimum of six characters for passwords.
Enter a shorter password.	A maximum of 128 characters can be used for passwords.
For a strong password, avoid using only lowercase English letters. We recommend using a combination of uppercase and lowercase English letters, symbols, and numbers.	Not only lower case alphabetic characters, but also combinations of upper case alphabetic characters, symbols and numbers are recommended.
The list name has already been used by another access list.	This access list name was used for another access list. Specify an access list name that is not being used for another access list or specify the name of an applicable access list.
The number of entries exceeds the maximum. (failed entry = <*value1*>)	You are trying to add more than the allowable maximum number of entries. Delete entries that are no longer needed, and then add the entries.
	<*value1*>: Entry name
The passwords are not the same. Please enter them again.	The new password and the re-entered password are not the same. Re-enter the password.
The port number in auth-port and acct-port is duplicated.	The port numbers for `auth-port` and `acct-port` are the same.
The string is too long or contains an invalid character. (maximum length = <*value1*>)	The number of characters exceeds the maximum value (<*value1*>), or an invalid character is contained. Use the determined format.
	<*value1*>: Number of characters that can be entered
The user account cannot be deleted because there must always be at least one user account.	Because at least one user account must exist, that user account cannot be deleted. Check the `username` setting.
This <*user id*> is already being used by another user.	This user ID is already being used by another user.
This command cannot be used to delete your own account.	The account of the user executing this command cannot be deleted. Delete it after logging in under a different user name.
This parameter cannot be changed to <*value1*>.	Changing to <*value1*> is not allowed. Delete it, and then add it again.
	<*value1*>: User ID, no-flash

17.3 Errors when specifying time and NTP/SNTP settings

Table 17-8: Error messages when specifying time and NTP/SNTP settings

Message	Description
NTP and SNTP cannot be set together.	NTP and SNTP are mutually exclusive, and only one can be set at a time. Check the settings of NTP or SNTP.
The IP configuration cannot be deleted because an SNTP broadcast configuration has been set.	`sntp broadcast` command information exists. Delete the `ip address` command after deleting the `sntp broadcast` command information.
The IP subnetmask cannot be changed because an SNTP broadcast configuration has been set.	`sntp broadcast` command information exists. Change the subnet mask of the `ip address` command after deleting the `sntp broadcast` command information.
The IPv6 configuration cannot be deleted because an SNTP broadcast configuration has been set.	`sntp broadcast` command information exists. Delete the `ipv6 address` command after deleting the `sntp broadcast` command information.
The start time is same as the end time.	The start date and end date cannot be set to the same value. Set the start date and end date to different values.

17.4 Errors when specifying host names and DNS settings

Table 17-9: Error messages when specifying host names and DNS settings

Message	Description
The same host name has already been set.(host name = <*value*>)	The same host name has already been set.
	<*value*>: Host name

17.5 Errors when specifying device resources settings

Table 17-10: Errors messages when specifying the device resources settings

Message	Description
The flow detection mode cannot be changed because the 'advance access-group' command or the 'advance qos-flow-group' command is set.	The flow detection mode cannot be changed because an advance access list or advance QoS flow list is applied to the device. Delete the `advance access-group` command, or `advance qos-flow-group` command before changing the flow detection mode to `quantity-oriented`.
The flow detection mode cannot be changed because the number of flow entries exceeds the maximum.	The flow detection mode cannot be changed because the number of filter entries or the number of QoS flow entries exceeds the capacity limit. Before changing the flow detection mode, specify the number of entries that are set so that they are within the capacity limit of the changed flow detection mode.
The flow distribution pattern ('flow-table allocation') cannot be changed because the number of flow entries exceeds the maximum.	The flow distribution pattern cannot be changed because the number of filter entries or the number of QoS flow entries exceeds the capacity limit. Before changing the flow distribution pattern, specify the number of entries that are set so that they are within the capacity limit of the changed flow detection mode.

17.6 Errors when specifying the output of system messages settings

Table 17-11: Error messages when specifying the output of system messages settings

Message	Description
The 'include' and 'exclude' parameters cannot be mixed.	The permit parameters (`include`) and suppress parameters (`exclude`) cannot be mixed within a single message type list.
The range of possible values that can be set by using the 'save-count' command was exceeded.	The total of the setting values for operation log entries has exceeded the range that can be set by a user. Review the operation log entries that have been set, and set a value so that the sum does not exceed 100000 entries.

17.7 Errors when specifying SNMP settings

Table 17-12: Error messages when specifying SNMP settings

Message	Description
The access list has already been set.(access list name = <*access list name*>)	The access list information was already set. Delete the access list information or check that the information is set correctly.
	<*access list name*>: Access list name
The inform functionality is supported by SNMPv2C.	The inform function is supported by SNMPv2C. Select SNMPv2C to use the inform function.
The number of group information entries exceeds 50. (group name = <*group name*>)	The number of entries specified as group information exceeded 50. Delete unnecessary entries, and then add the new one.
	<*group name*>: Group name
The number of MIB view entries exceeds 50. (MIB view = <*view name*>)	The number of MIB view entries exceeded 50. Delete unnecessary MIB view entries, and then add the new one.
	<*view name*>: MIB view name
The number of subtrees in the MIB view exceeds 30. (MIB view = <*view name*>, subtree = <*oid tree*>)	The number of subtrees in one MIB view exceeded 30. Delete unnecessary subtrees, and then add the new one.
	<*view name*>: MIB view name <*oid tree*>: Indicates subtree information.
The oid-tree value is invalid.(oid-tree = <*oid tree*>)	The value of an object ID that indicates a subtree is invalid. Specify an object ID in dot notation.
	<*oid tree*>: Indicates subtree information.
The RMON alarm rising threshold must be greater than the falling threshold.	The upper threshold value is less than the lower threshold value. The upper threshold value must be equal to or larger than the lower threshold value.

17.8 Errors when specifying Ethernet settings

Table 17-13: Error messages when specifying the Ethernet settings

Message	Description
A subinterface cannot be set because a channel-group is already set for the port.	The applicable port cannot be set to the subinterface because it is set to a channel group. If specifying the subinterface, specify a port that is not set to a channel group.
A subinterface cannot be set because an IP address is already set for the port.	The subinterface cannot be set because the IP address is set to the Ethernet port. Delete the IP address of the Ethernet port, or set the subinterface to another Ethernet port.
The following items conflict: 'the IP interface' and 'the mirror port' cannot be set together.	The IP address cannot be set for an interface that is set to a mirror port.
The interface cannot be deleted because the following items conflict: the interface and the IPv4 policy-based routing list configuration.	The specified interface cannot be deleted because it is used in an IPv4 policy base routing list. Delete the applicable sending interface from the IPv4 policy base routing list before deleting the specified interface.
The interface cannot be deleted because the following items conflict: the interface and the IPv6 policy-based routing list configuration.	The specified interface cannot be deleted because it is used in an IPv6 policy base routing list. Delete the applicable sending interface from the IPv6 policy base routing list before deleting the specified interface.
The number of interfaces exceeds the maximum number for this device.	The number of interfaces exceeds the maximum capacity of the Device. Check the setting details inside the device, and delete subinterfaces and port channels that are not being used.
this command is different from this one in channel-group port.	The configured command and the port channel configuration do not match. Make the configuration of the port channel and the configuration of the command consistent.

17.9 Errors when specifying link aggregation settings

Table 17-14: Error messages when specifying link aggregation settings

Message	Description
A channel group cannot be set because a MEP is already set for the port.	The channel group cannot be set because the MEP is set for the Ethernet port. Delete the MEP of the Ethernet port, or set the channel group to another Ethernet port.
A channel group cannot be set because a subinterface is already set for the port.	The channel group cannot be set because the subinterface is set for the Ethernet port. Delete the subinterface, or set the channel group to another Ethernet port.
A channel group cannot be set because an IP address is already set for the port.	The channel group cannot be set because the IP address is set for the Ethernet port. Delete the IP address of the Ethernet port, or set the channel group to another Ethernet port.
A channel group cannot be set because CFM configuration is already set for the port.	The channel group cannot be set because CFM is set for the Ethernet port. Delete the CFM setting of the Ethernet port, or set the channel group to another Ethernet port.
A subinterface cannot be set because an IP address is already set for the channel group.	The subinterface cannot be set because the IP address is set for the channel group. Delete the IP address of the channel group, or set the subinterface to another channel group.
The 'channel group number' cannot be changed because a different channel group number is already set. (attempted channel group number = <*value1*>)	The number of the channel group that is currently set cannot be changed. To change it, you must delete channel group mode, and then set it again.
	<*value1*>: Channel group you attempted to set
The 'channel-group mode' cannot be changed because a different mode is already set. (attempted mode = <*mode*>)	The mode of the channel group that is currently set cannot be changed. To change it, you must delete channel group mode, and then set it again.
	<*mode*>: Mode you attempted to set
The channel group cannot be deleted because the following items conflict: the channel group and the IPv4 policy-based routing list configuration.	The specified channel group cannot be deleted because it is used in an IPv4 policy base routing list. Delete the applicable sending interface from the IPv4 policy base routing list before deleting the specified channel group.
The channel group cannot be deleted because the following items conflict: the channel group and the IPv6 policy-based routing list configuration.	The specified channel group cannot be deleted because it is used in an IPv6 policy base routing list. Delete the applicable sending interface from the IPv6 policy base routing list before deleting the specified channel group.
The channel group cannot be set because the number of flow entries exceeds the maximum.	Channel group commands cannot be set because the number of filter entries or the number of QoS entries exceeds the capacity limit. The number of entries exceeds the capacity limit in settings of the channel group commands because an access list or QoS flow list has been applied to the specified port channel subinterface. Set the commands of the channel group as follows: • Set the commands after deleting the access list and QoS flow list from the applicable interface. • Set the commands in a range that does not exceed the capacity limit.
The following items conflict: 'the channel group port' and 'the mirror port' cannot be set together.	The channel group cannot be set for an interface set to a mirror port.
The number of interfaces exceeds the maximum number for this device.	The number of interfaces exceeds the maximum capacity of the Device. Check the setting details inside the device, and delete the subinterfaces and port channels that are not being used.

Message	Description
The number of ports for the channel group exceeds the maximum.	No more channel groups can be set to the port. Check the number of ports for each channel group again.
The ports cannot be detached from the channel group because 'shutdown' is not configured on some of the ports.	The ports cannot be deleted from the channel group because there is a port that is not set to `shutdown`. Use the configuration to shut down the applicable port.
There is a configuration inconsistency in terms of 'dot1q ethertype' or 'mtu' between some ports in the channel group.	Different `tpid` or `mtu` settings were found on ports specified for the same channel group. Make the configuration of the ports specified for the same channel group consistent.
There is a link-aggregation mode inconsistency between some ports in the channel group.	Different link aggregation modes are set on ports specified for the same channel group. Make the link aggregation mode for the ports specified to the same channel group consistent.

17.10 Errors when specifying IP interface settings

Table 17-15: Error messages when specifying the IP interface settings

Message	Description
The following items conflict: 'the subinterface' and 'the mirror port' cannot be set together.	The subinterface cannot be set for an interface that is set to a mirror port.
The specified VLAN ID is already used on the same port or channel group.	The same VLAN ID is already set to the same port or the same channel group. Check the setting details, and specify a different VLAN ID.
The VLAN ID cannot be changed because an IP address is already set.	The VLAN ID cannot be changed because an IP address is already set. If you change the VLAN ID, delete the IP address.
The VLAN ID cannot be deleted because an IP address is already set.	The VLAN ID cannot be deleted because an IP address is already set. If you delete the VLAN ID, delete the IP address.

Index