



Edge Gateway Series CLI User's Manual



Licenses and Trademarks

License

- This product uses software based on open-source licenses such as GPL (GNU General Public License).
Details are described on our Web site.
[Open Source Software License Agreement \(amnimo X/G/R Series\)](#)
[Open Source Software License Agreement \(amnimo C series\)](#)
- Scope of Warranty and Responsibility
No warranty is made regarding the operation of the open-source software itself in accordance with the terms of the GPL and other applicable laws.

Trademark

- Product names, company names, and other proper nouns used herein are trademarks or registered trademarks of the respective companies.

Introduction.

Thank you for adopting our AI Edge Gateway amnimo X series** ("AI Edge Gateway"), Edge Gateway amnimo G series ("Edge Gateway"), IoT Router amnimo R series ("IoT Router"), Thank you very much for adopting the Compact Router amnimo C series ("Compact Router") (the above-mentioned products in our series are hereinafter referred to as "Products").

The Edge Gateway Series CLI User's Manual (this "Manual") describes the command line interface (CLI) control of the Edge Gateway, IoT Router, and Compact Router.

This publication is intended for system integrators and administrators who understand telecommunications terminology and concepts.

To take full advantage of the functions of this product and to use it properly and safely, please read this manual carefully before use to fully understand its functions and operations and to become familiar with its handling.

*The AI Edge Gateway will be the content of the planned release.

About this Product

Target firmware version in manual

This manual is based on the following versions of firmware.

Product	Firmware Version
AI Edge Gateway* 	2.0.0
Edge Gateway  	2.1.0
IoT Routers  	
Indoor type Compact Router 	1.13.0
Indoor type wireless LAN Compact Router 	
Outdoor Type Wireless LAN Compact Router 	

*The AI Edge Gateway will be the content of the planned release.

Precautions for this product

- This product does not guarantee backward compatibility with product versions with respect to configuration data.
- IoT Router only supports operation by amsh.
- Compact Router cannot be operated by bash.

About This Book

Notes on this document

- The contents of this document are subject to change without notice.
- Reproduction or reprinting of the contents of this document, in whole or in part, without permission is prohibited.
- While every effort has been made to ensure the accuracy of the information contained in this document, if you have any questions or find any errors, please contact our customer support.

Contact: amnimo Customer Support
E-mail: support@amnimo.com
URL: <https://support.amnimo.com>

- Please note that revisions may not be made for specification changes, structural changes, or changes in parts used that are not considered to be particularly detrimental to functionality/performance.

Manual List

■ General

- [amnimo gateway Series CLI User's Manual](#) (this manual)
- [amnimo gateway Series GUI User's Manual](#)
- [Device Management System Manual](#)

■ amnimo X/G/R Series

- [amnimo X Series Edge Gateway User's Manual](#) (Japanese Edition)
- [amnimo X Series Edge Gateway Startup Guide](#) (Japanese Edition)
- [amnimo G Series Edge Gateway User's Manual](#)
- [amnimo G Series Edge Gateway Startup Guide](#)
- [amnimo R Series IoT Router User's Manual](#) (Japanese Edition)
- [amnimo R Series IoT Router Startup Guide](#) (Japanese Edition)
- [amnimo gateway series developer's manual](#) (amnimo X/G series only)
- [Edge Gateway Series Open Source Software License Agreement](#)

■ amnimo C Series

- [amnimo C Series Compact Router User's Manual](#) (Japanese Edition)
- [amnimo C Series Compact Router Startup Guide](#) (Japanese Edition)
- [Edge Gateway C Series Open Source Software License Agreement](#) (Japanese Edition)

Icons and symbols used in this manual

Icons and symbols in this manual have the following meanings

	Information of special note regarding functions and operation.
	Supplemental information regarding functions and operation is provided.
	This section contains reference information within this document and to other documents.
	Indicates that the command can be operated in general user mode.
	Indicates that the command can be operated in administrator mode.
	Indicates that the command can be operated in setting mode.

How to see compatible models

This manual is compatible with multiple models. Icons for supported models are shown below.

- If the following icons appear at the beginning of a chapter or section, it corresponds to the model described in that chapter or section.
- If the following icons are not indicated at the beginning of a section or subsection, it corresponds to the model with the icon notation of the chapter or section to which it belongs.
- Icons with red shaded lines indicate unsupported models.

	Indicates that the AI Edge Gateway Indoor Type is supported.
	Indicates that the Edge Gateway Indoor Type is supported.
	Indicates that the Edge Gateway Outdoor Type is supported.
	Indicates that the IoT Router Indoor Type is compatible with the IoT Router Indoor Type.
	Indicates that the IoT Router Outdoor Type is supported.
	Indicates support for Compact Router Indoor Type routers.
	Indicates compatibility with Compact Router Indoor Type with wireless LAN.
	Indicates compatibility with Compact Router Outdoor Type with wireless LAN.

Command Description

The command format of this manual is written as follows

Writing on the surface	Description
VALUE	<ul style="list-style-type: none"> ● Bolded values are fixed values. ● Bold italicized text is a setting parameter or keyword. It cannot be omitted.
[A B]	Select A or B. Can be omitted.
< A B >	Select A or B. It cannot be omitted.
[0 - 9]	Select one of the values from 0 to 9. Can be omitted.
< 0 - 9 >	Select one of the values from 0 to 9. It cannot be omitted.
↵	Indicates a line break (Enter key input).

Output format description

The format of the output format in this document is described as follows

Parameters for which a setting must exist

parameter ***PARAMETER***

Option Setting Parameters

PARAMETER

The output conditions of the parameters are described in the description of the Output items of the relevant parameters.

Table of Contents

Licenses and Trademarks	2
Introduction.....	3
About this Product.....	4
About This Book.....	5
Manual List.....	5
Table of Contents.....	9
<hr/>	
Chap 1. CLI Basics.....	16
1.1 Connect to this product via CLI.....	16
1.1.1 Connecting with a terminal emulator	16
1.1.2 Log in to this product.....	19
1.1.3 Change the bootloader password for this product	21
1.2 Launch the CLI for this product.....	23
1.2.1 Running the amsh program	23
1.2.2 Run the amsh program with the option	23
1.3 Overview of the CLI for this product	24
1.3.1 About Operation Modes	24
1.3.2 About Command Prompt.....	24
1.4 Change the operation mode.....	25
1.5 Execute command.....	26
1.5.1 Use the input completion function.....	26
1.5.2 Browse command history.....	27
1.5.3 Read the error message	28
1.6 Use convenient functions.....	29
1.6.1 Refer to Help.....	29
<hr/>	
Chap 2. Basic Operation of this Product.....	30
2.1 Reboot the product.....	30
2.2 Turn off the power to the product	31
2.3 Browse for information on this product.....	31
2.4 Operate the firmware	32
2.4.1 Displays the firmware version.....	32
2.4.2 Check the firmware files	32
2.4.3 Delete the firmware	33
2.4.4 Update firmware	34
2.4.5 Synchronize redundant areas of firmware	36
2.4.6 Set the redundant area to be activated	37
2.4.7 Update firmware package information.....	38
2.4.8 Update the firmware package.....	38
2.4.9 Delete the firmware package information file.....	39

2.5	Working with package repositories	40
2.5.1	Add package repository credentials	40
2.5.2	Removing credentials from the package repository	40
2.5.3	View package repository credentials.....	41
2.6	Change a user's password	42
2.6.1	Change the password of the logged-in user himself/herself.....	42
2.6.2	Change password by specifying user	43
2.7	Set up your account.....	44
2.7.1	Display the user list	44
2.7.2	Show logged-in users of users	44
2.7.3	Display user settings	44
2.7.4	Configuring Users.....	47
2.7.5	Display group settings	49
2.7.6	Set up a group	52
2.7.7	Group Permissions For various parameters of the configuration.....	55
<hr/>		
Chap 3.	Manipulation of configuration files.....	63
3.1	Initialize settings	63
3.2	Display a list of settings	64
3.3	Display a list of configuration files	65
3.4	Writing to the configuration file	65
3.5	Read the configuration file.....	67
3.6	Rename the configuration file	68
3.7	Copy the configuration file	69
3.8	Delete configuration files	69
<hr/>		
Chap 4.	Storage Operations	70
4.1	View storage devices.....	70
4.2	Configure storage partitions	73
4.2.1	Create partitions	73
4.2.2	Delete partitions	74
4.3	Formatting Storage	75
4.4	Display storage mount status.....	76
4.5	Controlling the mount state of storage partitions	77
4.5.1	Mount partitions	77
4.5.2	Unmount partitions	78
4.6	Check storage	79
4.7	Display storage usage.....	81
4.8	View storage settings.....	82
4.9	Set up storage and save configuration information.....	85
4.9.1	Configure storage mount settings.....	85

4.9.2	Configure storage unmounting settings.....	86
4.9.3	Inspect/repair the file system.....	86
4.9.4	Disable the ability to inspect/repair the file system	87
4.9.5	Periodically check storage read/write status	87
4.9.6	Disable periodic checks of storage read/write status.....	88
4.9.7	Handle fail-safe in case of fsck/mount/read/write process failure	89
4.9.8	Disable fail-safe handling of fsck/mount/read/write process failures..	90
4.9.9	Display storage formatting information	91
4.10	File Operations	92
4.10.1	List files.....	92
4.10.2	Move a file	93
4.10.3	Copy files.....	94
4.10.4	Delete a file	94
<hr/>		
Chap 5.	Mobile Operation	95
5.1	View the mobile module	95
5.2	Controlling the mobile module	99
5.2.1	Turn on the power to the mobile module	99
5.2.2	Reset the power supply of the mobile module	99
5.2.3	Update SIM information.....	100
5.2.4	Turn off the mobile module	101
5.2.5	Check PIN setting status	102
5.2.6	Unlock the SIM card.....	103
5.2.7	Enable PIN code	104
5.2.8	Disable PIN code	105
5.2.9	Change PIN code	106
5.2.10	Unlock PIN by PUK code	107
5.3	Display the communication status of the mobile line	108
5.4	Manually connect a mobile line	112
5.5	Disconnect the mobile line.....	112
5.6	View mobile line settings.....	113
5.7	Set up a mobile line	118
5.7.1	Supplementation of each mobile setting item.....	122
5.7.2	Execution example	128
5.7.3	Automatic time correction function (supported from V1.5.0).....	133
<hr/>		
Chap 6.	Network Settings	134
6.1	Configure PPP settings.....	134
6.1.1	Display PPP status.....	134
6.1.2	Connect PPP manually	135
6.1.3	Disconnect PPP	135
6.1.4	Display PPP settings.....	136
6.1.5	Configure PPP settings.	139
6.2	Configure interface settings.	143
6.2.1	Display interface status	143

6.2.2	Display interface settings	144
6.2.3	Configure the interface and save configuration information	153
6.3	Configure routing settings	163
6.3.1	Display the routing table	163
6.3.2	Display routing settings	164
6.3.3	Configure routing table settings	165
6.4	Configure packet filtering settings	166
6.4.1	Display packet filtering settings	166
6.4.2	Set default policy for packet filtering	169
6.4.3	Configure packet filtering rules	170
6.5	Configure NAT settings	172
6.5.1	Display NAT settings	172
6.5.2	Configuring Dynamic SNAT	174
6.5.3	Setting up a static SNAT	176
6.5.4	Set DNAT	178
6.6	Configure common settings for packet filtering and NAT	180
6.6.1	Display packet matching condition settings	180
6.6.2	Set packet matching conditions	184
6.6.3	Delete packet match condition	191
6.6.4	Display log output settings	192
6.6.5	Configure log output	192
6.7	Configure IPsec settings	193
6.7.1	Display IPsec status	193
6.7.2	Connect IPsec manually	196
6.7.3	Disconnect IPsec	196
6.7.4	Display IPsec settings	197
6.7.5	Configure IPsec	206
6.8	Configure wireless LAN settings	218
6.8.1	Displays the status of the wireless LAN access point	218
6.8.2	Display a list of devices connected to the wireless LAN access point	220
6.8.3	Disconnect the device connected to the wireless LAN access point	221
6.8.4	View wireless LAN access point settings	222
6.8.5	Configure wireless LAN access point settings	227
6.8.6	Displays the status of the wireless LAN station	235
6.8.7	Switching the access point to which the wireless LAN station is connected	237
6.8.8	View wireless LAN station settings	239
6.8.9	Configure the wireless LAN station settings	244
6.8.10	Connect using the WPS function	250
6.8.11	Display WPS function settings	252
6.8.12	Configure the WPS function	254
6.8.13	Restrictions on wireless LAN functionality and interface	255
<hr/>		
Chap 7.	Server Settings	256
7.1	Set the host name	256
7.1.1	Show hostname	256
7.1.2	Display host name settings	256

7.1.3	Change the host name	257
7.2	Set the time zone	258
7.2.1	Display time zone	258
7.2.2	View time zone settings	258
7.2.3	Set the time zone.....	259
7.3	Set the time	260
7.3.1	Manually set the time	260
7.3.2	Display NTP status.....	262
7.3.3	Display NTP settings	266
7.3.4	Configure NTP settings	270
7.4	Configure SSH settings.....	274
7.4.1	Displaying SSH settings	274
7.4.2	Configure SSH	276
7.5	Configure DNS settings	278
7.5.1	Search for a name in the DNS	278
7.5.2	Display DNS status	279
7.5.3	View DNS settings.....	280
7.5.4	Configure DNS settings.....	284
7.6	Configure DHCP server settings	288
7.6.1	Display a list of DHCP leases	288
7.6.2	Display DHCP server settings.....	289
7.6.3	Configure DHCP server settings.....	293
7.7	Set up a schedule.....	297
7.7.1	Display the operating status of the schedule	297
7.7.2	View schedule settings.....	299
7.7.3	Set a schedule.....	306
7.8	Manage system logs.....	317
7.8.1	Display Syslog messages.....	317
7.8.2	Display Syslog settings.....	319
7.8.3	Configure Syslog settings.	322
7.8.4	Display amlog message.....	323
7.8.5	Clear amlog logs	326
7.9	Configure GUI settings.....	327
7.9.1	Displaying GUI settings	327
7.9.2	Configure GUI settings	329
7.10	Configure DHCP relay settings	330
7.10.1	Display DHCP relay settings.....	330
7.10.2	Configure DHCP relay settings.....	332
7.11	Setting up a proxy server.....	334
7.11.1	Display proxy server settings	334
7.11.2	Configure proxy server settings.....	339
<hr/>		
Chap 8.	Hardware Management.....	344
8.1	Control USB devices.....	344

8.1.1	Display USB devices	344
8.1.2	Control USB devices	344
8.2	Configure PoE settings.	346
8.2.1	Display PoE status	346
8.2.2	Controlling the PoE port.....	348
8.2.3	Display PoE settings	350
8.2.4	Configure PoE.....	352
8.3	Manage D IN/D OUT status	354
8.3.1	Display the status of D IN.....	354
8.3.2	Display the status of D OUT	355
8.3.3	Controls the state of D OUT.....	356
8.4	Display DIP switch status	357
<hr/>		
Chap 9.	Maintenance and Management	358
9.1	Display the status of this product.....	358
9.1.1	Display input voltage	358
9.1.2	Display the temperature inside the enclosure.....	359
9.2	Configure CPU operation settings.....	360
9.2.1	Display CPU operation	360
9.2.2	Display CPU operation settings.....	362
9.2.3	Configure CPU operation	363
9.3	Set high and low temperature protection	364
9.3.1	Display high and low temperature protection settings.....	364
9.3.2	Set high and low temperature protection	367
9.4	Check network status.....	371
9.4.1	Examine network reachability	371
9.4.2	Examine network routes.....	373
9.4.3	Find out which MAC address corresponds to an IP address	375
9.4.4	Control ARP table information	377
9.4.5	Dump packets to examine communication contents	378
9.4.6	Display the results of dumping packets.....	380
9.4.7	Delete the results of dumping packets	381
<hr/>		
Chap 10.	Applications for this product.....	382
10.1	Configure DMS settings.....	382
10.1.1	Display DMS status	382
10.1.2	Control DMS	383
10.1.3	Display DMS settings	383
10.1.4	Configure DMS settings.....	384
10.2	Configure Nx Witness settings.....	385
10.2.1	Display Nx Witness status.....	385
10.2.2	Controlling Nx Witness.....	386
10.2.3	View Nx Witness settings	387
10.2.4	Configure Nx Witness settings.	389
10.2.5	Write Nx Witness settings	390

10.2.6	Load Nx Witness settings.....	390
10.3	Configure remote.it settings	391
10.3.1	Display the status of remote.it	391
10.3.2	Controlling remote.it	392
10.3.3	View remote.it settings	393
10.3.4	Configure remote.it settings.....	395
10.4	Execute application commands	396
<hr/>		
Chap 11.	external command.....	397
11.1	Controlling configuration files	397
11.1.1	Basics of configuration file control commands.....	397
11.1.2	Initialize the configuration file	397
11.1.3	Read the configuration file	398
11.1.4	Save the configuration file.....	398
11.1.5	Rename the configuration file	399
11.1.6	Copy the configuration file	399
11.1.7	Delete configuration files	400
11.1.8	Display a list of configuration files	400
11.2	Control hardware.....	401
11.2.1	Basics of Hardware Control Commands.....	401
11.2.2	Display hardware information.....	403
11.2.3	Display DIP switch status.....	403
11.2.4	Display the status of the PUSH switch.....	404
11.2.5	Controlling the startup area	405
11.2.6	Controls the lighting of LEDs.....	406
11.2.7	Control PoE controller	408
11.2.8	Control USB port	409
11.2.9	Controls digital inputs	410
11.2.10	Control digital outputs.....	411
11.2.11	Controls the reboot process.....	413
11.2.12	Display command version	413
<hr/>		
Chap 12.	appendix.....	414
12.1	CLI functions supported in each mode.....	414
12.2	CLI functions supported by each product.....	417
12.3	fail-safe	423
	Revision History.....	425

Chap 1. CLI Basics

This chapter describes the basic operations of the Command Line Interface (CLI), a user interface provided to execute commands entered from the keyboard and output the results to a window.

1.1 Connect to this product via CLI

There are two ways to connect to this product via CLI

- Connecting using a serial console
Connecting this product to a PC with a serial cable and using a terminal emulator to connect from the PC



The method of connecting to the serial console is different for each product, Refer to the respective user's manuals.

- Connecting via SSH (Secure Shell)
Connect from a PC connected to the same network (Ethernet) as the product by specifying the IP address of the product using a terminal emulator or the ssh command.



SSH is disabled by default on this product.

➔ For information on how to enable SSH, see "7.4 Configure SSH Settings" for details on how to enable SSH.

1.1.1 Connecting with a terminal emulator

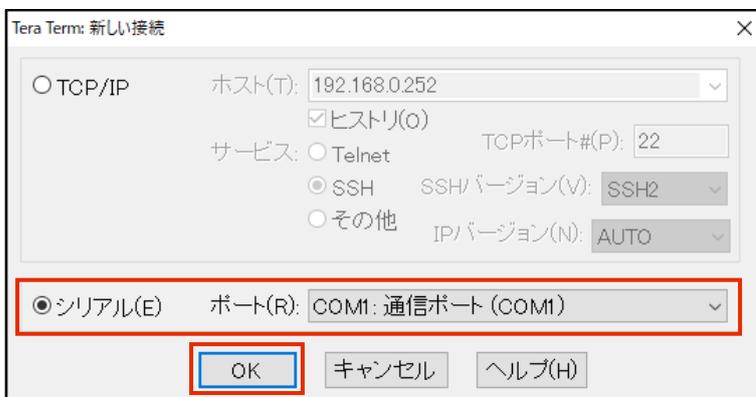


This section describes the procedure for connecting to this product using Tera Term (Ver 4.105), a Windows terminal emulator.

■ Connect via serial console

Connect from the "Tera Term new connection" screen of Tera Term.

1. Select "Serial," then select the serial port to be used from the drop-down list and click the "OK" button.



The "Serial Port Settings and Connections" screen appears.

2. Select "Serial Port" from the "Settings" menu, the "Serial Port Settings and Connections" dialog appears, set the serial port connection settings, and click the "Reconfigure Current Connection" button.



When connected to the product, the terminal emulator will display a login prompt.

■ Connect via SSH

Connect from the "Tera Term new connection" screen of Tera Term.

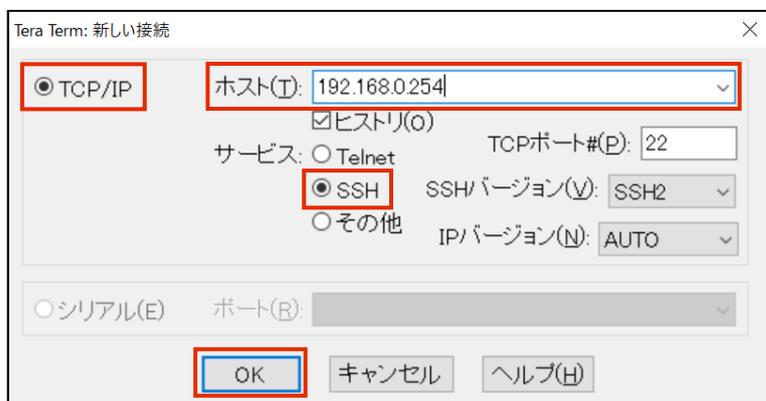
1. Make the following settings in the "Tera Term new connection" window and click the [OK] button.
 - ① Select "TCP/IP"
 - ② Enter the IP address in the "Host" field. Enter IP address in "Host"



The following figure shows an example configuration when connected to the following ports

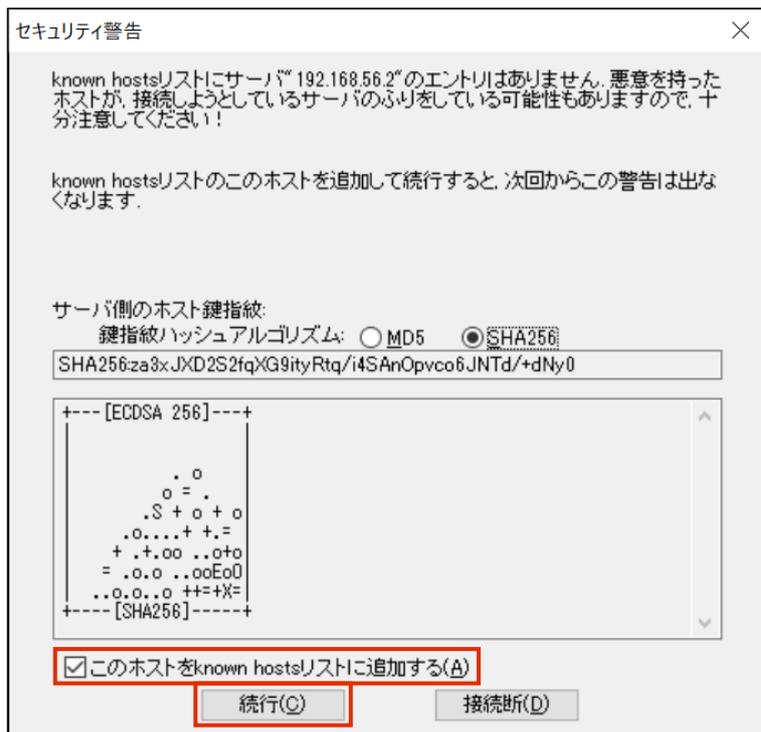
Edge Gateway: lan0-3
IoT Router: eth1

- ③ Select "SSH" under "Services"



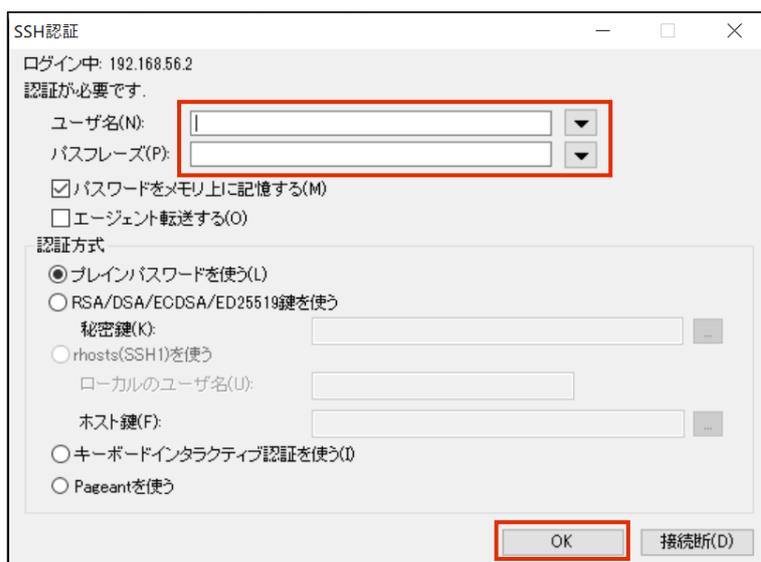
When connecting to a new host, a "Security Warning" screen will appear.

2. Check the "Add this host to the known hosts list" checkbox and click the Continue button.



The "SSH Authentication" screen appears.

3. Enter the authentication information and click the "OK" button.



When connected to the product, the terminal emulator will display a login prompt.

1.1.2 Log in to this product



The procedure for logging in to the product differs for the first time and for the second and subsequent times.

Log in for the first time

Enter "admin" as the login name and press Enter without entering a password to log in.

You will need to change your password after logging in.

```

Ubuntu 18.04.5 LTS amnimo ttyMV0

amnimo login: admin          ←Enter the login name "admin" and press Enter.
Password: ←Enter without password ←Enter without entering a password
Last login: Mon Oct 12 15:54:21 UTC 2020 on ttyMV0
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.19.93-02928-g44990b3300f7 aarch64)
(Abbreviations.)
Changing password for admin.
(current) UNIX password: ←Enter without password          ←Enter without password
Enter new UNIX password: ←Enter new UNIX password to be set ←Enter new password
and press Enter

```



The password must be a string of characters that meets the following criteria

- 8 characters or more
- Includes at least two types of uppercase and lowercase letters, numbers, and symbols

Even if a password satisfies the above conditions, it cannot be set if any of the following conditions apply

- Words in the dictionary (e.g., test)
- Words with regularity, such as number or alphabet keyboard sequences (e.g., 1234, abcde, qwert)
- Combination of the above (e.g., test1234)

■ Log in for the second time or later

To log in a second time or later, enter the password you set the first time.

amnimo G series/ amnimo R series

```

Ubuntu 18.04.5 LTS amnimo ttyMV0

amnimo login: admin ←Enter the login name "admin" and press Enter.
Password:          ←Enter the password you set and press Enter
Last login: Mon Oct 12 15:58:31 UTC 2020 on ttyMV0
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.19.145-00773-gd341a7f2d77d aarch64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

  .JggggJ..
    ?TMMMMMMMMNNggggggggg&...
  .JJ.. _TMMMMMMMMMMMMMMMMMMm...
  .MMMMMN, ?MMMMMMMM#Y "7?? 7TMMMMNg, ?
  dMMMMMN{ (MMMMMN. .... 7MMMMNe.
  MMMMMMMMr .MMMMMMMMMMm. _MMMMMm-
  _?7TY: (MMMMMMMMMMMMMMN. (MMMMN.
  .gNNngJ... .MMMMMMMMMMMMMMMP MMY
  jMMMMMM#~ dMMMMMMB "7!` MMY#.
  .HMMMMM#% (MMMMMMB! . .JJggggx MMY#~
  (MMMMMM= .dMMMMMD` (MMMMMP MMY#~
  _7"! jMMMMMMMMMMMMMMMMM$ MMY#
  .MMMMMMr .wMMMMMM9 MMYC
  .MMMMMN& ?T "Y9=` . MMYD
  _HMMMMMMmJ.. ... .JgR.. .MMY`
  7MMMMMMMMMMMMMMMMNNMMMMMM#
  .TMMMMMMMMMMMMMMMMM#"

```

■ About the login prompt

The prompts that appear when connecting to this product vary depending on the series and settings of the connected Edge Gateway.

amnimo G series/ amnimo R series

```

Ubuntu 18.04.3 LTS amnimo ttyMV0

amnimo login:.
```

amnimo C series

```

amnimo C series AC10 version 1.5.0 build 00000

amnimo login:.
```

1.1.3 Change the bootloader password for this product



The boot loader (hereafter referred to as U-Boot) can log in on the U-Boot when it is started in U-Boot command mode. Since the initial password is fixed, it is recommended to update it for security reasons.

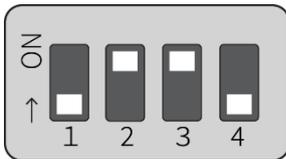


This function is not available on Compact Router.

■ Booting in U-Boot command mode

Before connecting the power supply, set the DIP switch to "U-Boot command mode" and connect the power supply.

DIP switch settings for U-Boot command mode



When the power is turned on, the following password input screen (input period: 10 seconds) will appear. Enter the password and press Enter to log in.

Execution example

```
TIM-1.0
WTMI-devel-18.12.1-118f0bd
WTMI: system early-init
SVC REV: 5, CPU VDD voltage: 1.108V
(Abbreviations.)
STATUS:SN=[300002],MAC0=[E8:1B:4B:00:30:02],BS=[a:0 b:385 h:0 s:0],DIPBM=[ubootcommand]
am_show_board_status: CNTFRQ_EL0=12500000 Hz

Please enter password - autoboot in 10 sec... ←Please enter password - autoboot in 10 seconds...
Return to boot status(0x55) for login
Amnimo>> run stopwdt ←          ← Stop automatic reset of watchdog IC
Amnimo>>
```



- Please check with our support for the initial password.
- Failure to enter the password is limited to three attempts; if more than three attempts fail, the system will boot in Linux boot mode.
- When working on the U-Boot, the run stopwdt command can be used to stop the reset by the watchdog IC to give you more time to work; note that if you do not run the run stopwdt command, it will automatically reset after a few minutes.

Change your password in U-Boot

You can use the `ampasswd` command to change your password.

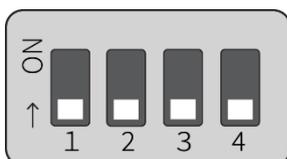
Execution example

```
Amnimo>> ampasswd ↵  
Current Password: ↵Enter after entering the current password  
New Password: ↵Enter the password you want to change, and press Enter.  
Retry Password: ↵Enter the password you want to change again.  
OK  
Amnimo>>
```

Booting in Linux boot mode

Set the DIP switch to "Linux boot mode" and reboot using the `reset` command.

Linux boot mode DIP switch settings



Execution example

```
Amnimo>> reset↵ ↵ restart
```

1.2 Launch the CLI for this product



To simplify the configuration of this product, the amsh program is available as a dedicated CLI.



The Compact Router runs the amsh program directly when you log in. Therefore, it is not possible to start it with the amsh option.



```
amnimo C series AC10 version 1.5.0 build 00000
```

```
amnimo login: admin ←Enter the login name "admin" and press Enter.
Password:      ←Enter the password you set and press Enter
Last login: Wed Jan 1 00:01:24 +0000 2020 on /dev/ttyGS0.
amnimo$.
```

1.2.1 Running the amsh program

The amsh program is invoked as follows

Execution example

```
admin@amnimo:~$ amsh ↵
```

1.2.2 Run the amsh program with the option

Describes the startup options for the amsh program.

option

option	Contents																											
-V <level>	Specify the log level to be output to the console or syslog of the CLI program. Logs with a higher priority than the specified priority (the lower the number, the higher the priority) will be output.																											
--verbose <level>																												
	<table border="1"> <thead> <tr> <th>Setting Parameter</th> <th>degree of relative priority</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>none</td> <td>0</td> <td>Do not display</td> </tr> <tr> <td>emerg</td> <td>1</td> <td>Logs requiring very urgent action</td> </tr> <tr> <td>alert</td> <td>2</td> <td>Logs requiring more urgent action</td> </tr> <tr> <td>crit</td> <td>3</td> <td>Logs requiring urgent action</td> </tr> <tr> <td>err</td> <td>4</td> <td>Log of Errors</td> </tr> <tr> <td>warning</td> <td>5</td> <td>Warning Level Log</td> </tr> <tr> <td>info</td> <td>6</td> <td>Logs for displaying various information</td> </tr> <tr> <td>debug</td> <td>7</td> <td>Debug Log</td> </tr> </tbody> </table>	Setting Parameter	degree of relative priority	Contents	none	0	Do not display	emerg	1	Logs requiring very urgent action	alert	2	Logs requiring more urgent action	crit	3	Logs requiring urgent action	err	4	Log of Errors	warning	5	Warning Level Log	info	6	Logs for displaying various information	debug	7	Debug Log
Setting Parameter	degree of relative priority	Contents																										
none	0	Do not display																										
emerg	1	Logs requiring very urgent action																										
alert	2	Logs requiring more urgent action																										
crit	3	Logs requiring urgent action																										
err	4	Log of Errors																										
warning	5	Warning Level Log																										
info	6	Logs for displaying various information																										
debug	7	Debug Log																										
-v	Displays the version of the CLI program.																											
-h	Display help for the CLI program.																											

Execution example

```
amnimo@amnimo:~$ amsh --help ↵ ← display help
Copyright (c) 2020 amnimo Inc. All Rights Reserved.
amnimo G series shell program version 1.0.0

Usage: amsh [<OPTIONS> ...].
```

OPTOINS: .

```
-V <level>, --verbose <level >: verbose output to console and syslog
-v                               : display the version number
-h, --help                       : display this help and exit
```

1.3 Overview of the CLI for this product



This section provides an overview of the CLI dedicated to the Edge Gateway series.

1.3.1 About Operation Modes

The following three types of CLI operation modes exist for this product.

The operations that can be performed differ depending on the operation mode.

➔ For information on the operations that can be performed in each operating mode, see " 12.1 CLI functions supported in each mode " for information on the operations that can be performed in each mode of operation.

- General User Mode
General user mode is a mode in which users belonging to the user group can operate. Users can perform operations necessary for operational management.
Immediately after the amsh program is executed, it is in general user mode.
- Admin Mode
Administrator mode is a mode in which users belonging to the admin group can operate the product. In addition to operations in the general user mode, the user can control the product (restart the product, control various ports, etc.).
The administrator mode is entered by executing the enable command in the general user mode.
- Configuration Mode
Setting mode is a mode that can be operated by users belonging to the admin group. Various settings can be checked and configured.
The configuration mode is entered by executing the configure command in the admin mode.

1.3.2 About Command Prompt

The command prompt will vary depending on the host name and mode of operation.

The configured host name is followed by "\$" for general user mode and "#" for administrator mode. In the configuration mode, "(mode directory name)" appears before the "#".



In this document, the host name is referred to as "amnimo".
The mode directory name is also indicated as "cfg".

ユーザーモード

```
amnimo$.
```

管理者モード

```
amnimo#
```

設定モード

```
amnimo(cfg)#.
```

1.4 Change the operation mode



This section describes how to change the mode of operation while amsh is running.

Change from general user mode to administrator mode

Shifts to administrator mode.

Only the owner of administrative privileges can enter administrator mode.

```
amnimo$ enable ↵
password:      ↵ Enter the password and press Enter
amnimo#
```

Change from administrator mode to setting mode

Shifts to setting mode.

Only the owner with administrative privileges can enter the configuration mode.

```
amnimo# configure ↵
amnimo(cfg)#.
```

Change from setting mode to administrator mode

Exit configuration mode and return to administrator mode.

```
amnimo(cfg)# exit ↵
amnimo#
```

Change from administrator mode to general user mode

Exit administrator mode and return to general user mode.

```
amnimo# exit ↵
amnimo$.
```

Exit general user mode and stop amsh

Executing exit in general user mode will terminate the amsh program and return you to the Linux CLI.

```
amnimo$ exit ↵
user1$.
```

1.5 Execute command



This section describes the functions available when entering commands in the CLI and the contents of the output when executing commands.

1.5.1 Use the input completion function

Commands and arguments can be automatically completed by typing the "Tab" key in the middle of entering a command.

If there are multiple applicable commands, a list of candidate commands is displayed.

Execution example

The following is an example of an Edge Gateway in action.

```

amnimo(cfg)# int          ← Press "Tab" key here
amnimo(cfg)# interface    ← command is completed

amnimo(cfg)# interface et  ← Press "Tab" key here
amnimo(cfg)# interface eth eth0 ← Argument is completed

amnimo(cfg)# interface lan ← Press "Tab" key here.
lan0 lan1 lan2 lan3       ← List of argument candidates is displayed.

amnimo(cfg)# s            ← Press "Tab" key here
ssh syslog show          ← List of candidate commands is displayed.

amnimo(cfg)# ex↵        ← Execute without exit
amnimo#                  ← Recognized as exit and executed
  
```



- For IoT Routers, the following information appears as a list of "eth" candidates

```
amnimo(cfg)# interface eth eth0 eth1
```



- For IoT Routers and indoor type Compact Router, the "lan" candidate list is not displayed because LAN ports are not implemented.

1.5.2 Browse command history

Commands executed in the past are stored as history data. By entering the "↑" and "↓" keys, you can view the commands that were executed in the past.

- ↑ Up key: Displays one previous command in the command history.
- ↓ key: Displays one most recent command in the command history.

If the most recent command was command-a, command-b, and command-c, the history can be traced as follows.

Execution example

```
amnimo(cfg)# command-a↵
amnimo(cfg)# command-b↵
amnimo(cfg)# command-c↵
amnimo(cfg)#
amnimo(cfg)# command-c
amnimo(cfg)# command-c
amnimo(cfg)# command-b
will be displayed.
amnimo(cfg)# command-b
amnimo(cfg)# command-a
amnimo(cfg)# command-a
amnimo(cfg)# command-b
amnimo(cfg)# command-b
amnimo(cfg)# command-a
yed.
```

← Press the "↑" key with no command input
 ← The most recently executed command is displayed.
 ← Press "↑" key again
 ← Go back one history and the command you executed
 will be displayed.
 ← Press "↑" key again
 ← One more previously executed command is displayed
 ← Followed by "↓" key
 ← One most recently executed command is displayed
 ← Followed by "↓" key
 ← One more most recently executed command is displayed.

1.5.3 Read the error message

The message displayed when the command is executed contains a great deal of information.

This section describes the messages that are sent when an error occurs.

■ In the event of an abnormality

If an error occurs when executing the command, a message will be displayed according to the verbose option of the amsh program.

➔ For more information, see " 1.2.2 Run the amsh program with the option " for more information.

Execution example

```
amnimo$ enable ↵
amnimo# configure ↵
amnimo(cfg)# hoge ↵
Messages are displayed according to the output LEVEL of the verbose option
amnimo(cfg)#.
```

■ When a required field is missing

If any of the required input items are missing when the command is executed, the missing configuration items are listed.

Below is an example of setting up an account for a particular user with the account command. You are trying to change the password in account configuration mode, but you are getting an error because you need to configure the group; if you abort the configuration with the exit command, you will be asked if you are sure you want to abort.

Execution example (V1.8.0 or later)

```
amnimo$ enable ↵
amnimo# configure ↵
amnimo(cfg)# account user username1 ↵
amnimo(cfg-account-username1)# password secret ENCRYPT-USERNAME1-PASSWORD ↵
You must fill in the following required fields: ← The group setting is missing.
group
amnimo(cfg-account-username1)# exit↵ ← Exit account setup mode
You must fill in the following required fields:
group
Cancel configuration? (y/N). ← Press y or Y to cancel configuration;
press n or N or Enter to return to configuration
```



- (y/N) represents y (yes) or N (no). The uppercase letter is set as the default. Pressing Enter without typing anything will select the uppercase one.
- If you enter a letter other than y (Y) or n (N), you will be asked again if you want to abort.

1.6 Use convenient functions



This section describes features that are useful in using the CLI.

1.6.1 Refer to Help

"?" key displays a list of command and parameter candidates and a help message. If there is no candidate list, the carriage return "<cr>" character is displayed.

Execution example

```
amnimo(cfg)#                               ← Press "?" key without typing anything
  interfaceSetup      network interface setting.
(Omitted.)
  Exit               Exit current mode and back to previous mode.

amnimo(cfg)# interface                       ← Command followed by a space followed by "?" key
  <IFNAME>           Interface's name.

amnimo(cfg)# s                               ← Press the "?" key in the middle of the input.
  ssh               Setup ssh service setting.
  syslog            Setup syslog service setting.
  show              Show configuration.

amnimo(cfg)# exit                            ← Command followed by a space followed by "?" key
  <cr>              ← <cr> is displayed because the <exit> command has no para
  meter
```

Chap 2. Basic Operation of this Product

This chapter describes basic operations of the unit, such as rebooting the product and updating firmware.

2.1 Reboot the product



To reboot the product, run the reboot command in administrator mode.

Format

```
reboot [type <soft | hard>].
```

Setting items

Item	Contents						
type	Specifies the restart type.						
	<table border="1"><thead><tr><th>Value</th><th>Contents</th></tr></thead><tbody><tr><td>soft</td><td>Perform a software reboot. Stop the system and then reboot. It is set as the default value.</td></tr><tr><td>hard</td><td>Perform a hardware reboot. Without shutting down the system, power off the hardware and reboot.  Performing a hardware reboot may cause file system corruption.</td></tr></tbody></table>	Value	Contents	soft	Perform a software reboot. Stop the system and then reboot. It is set as the default value.	hard	Perform a hardware reboot. Without shutting down the system, power off the hardware and reboot.  Performing a hardware reboot may cause file system corruption.
	Value	Contents					
soft	Perform a software reboot. Stop the system and then reboot. It is set as the default value.						
hard	Perform a hardware reboot. Without shutting down the system, power off the hardware and reboot.  Performing a hardware reboot may cause file system corruption.						

Execution example

管理者モード

```
amnim0# reboot type soft ↵  
Are you sure you want to restart? ←Enter the "y" key followed by Enter
```



To cancel execution of the command, type the "n" key followed by Enter.

2.2 Turn off the power to the product



To transition the product to the shutdown state, execute the poweroff command in administrator mode.

Execution example

管理者モード

```
amnimo# poweroff ↵
Do you want to stop the system? ←Enter the "y" key followed by Enter
```



To cancel execution of the command, type the "n" key followed by Enter.

2.3 Browse for information on this product



Displays the model's name and serial number of the product.

Execution example

Command input and output is the same in all modes. Below is an example of running the General User mode on the Edge Gateway.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device information ↵
manufacturer  amnimo
board         AG10
series       G
model        AG10-010JP-10-512G
serial       012345
revision     0
date:        2020-01-01t00:00:00z
```



If the model is different, the contents specific to the model are displayed in board, series, and model.

2.4 Operate the firmware

Firmware updates and settings.

2.4.1 Displays the firmware version



To display firmware version information, run the show firmware command.

Execution example

Command input and output are the same in general user mode and administrator mode. Below is an example of administrator mode execution on the Edge Gateway.

ユーザーモード 管理者モード

```
amnimo G series AG10 version 1.4.0 build 13992
Kernel: 4.19.195-03776-g3ad1b025c60 #1 SMP PREEMPT Wed Aug 4 05:18:02 UTC 2021
Bootloader: g88baf9249d (Jul 30 2021 - 05:24:48 +0000)
BootArea: 1
Partitions: 5
```



If the model is different, the contents specific to the model will be displayed.

2.4.2 Check the firmware files



Verify that the firmware exists. For firmware located on an external server, download the firmware.

Format

```
firmware file check URL
```

Setting items

Item	Contents
URL	<p>The URL can be HTTP or FTP.</p> <p>Below is an example configuration with the file name as firmware file ag10-v1.0.0-b1.amf for the Edge Gateway Way.</p> <ul style="list-style-type: none"> ● To use a file that exists in storage file:///media/usb/ag10-v1.0.0-b1.amf ● When using a file that resides on a TFTP server tftp://example.com/ag10-v1.0.0-b1.amf ● To use a file that resides on an FTP server that supports password authentication ftp://username:password@example.com/ag10-v1.0.0-b1.amf ● When using a file that resides on an HTTP server that supports Basic Authentication http://username:password@example.com/ag10-v1.0.0-b1.amf ● If you are using a file that resides on an HTTPS server that supports Basic Authentication https://username:password@example.com/ag10-v1.0.0-b1.amf



To obtain our public firmware, you will need the following information: "connection and firmware", "account name", and "password".

The URL for the latest firmware used in the example run of this procedure is

- Edge Gateway Indoor Type AI Edge Gateway
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ax11.amf](https://(account name):(password)@package.amnimo.com/firmware/ax11.amf)
- Indoor Type Edge Gateway
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ag10.amf](https://(account name):(password)@package.amnimo.com/firmware/ag10.amf)
- Outdoor Type Edge Gateway
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ag20.amf](https://(account name):(password)@package.amnimo.com/firmware/ag20.amf)
- IoT Router Indoor Type
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ar10.amf](https://(account name):(password)@package.amnimo.com/firmware/ar10.amf)
- IoT Router Outdoor Type
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ar20.amf](https://(account name):(password)@package.amnimo.com/firmware/ar20.amf)
- Indoor Compact Router
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ac10.amf](https://(account name):(password)@package.amnimo.com/firmware/ac10.amf)
- Compact Router Indoor Type with wireless LAN
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ac15.amf](https://(account name):(password)@package.amnimo.com/firmware/ac15.amf)
- Compact Router Outdoor Type with wireless LAN
[https://\(account name\):\(password\)@package.amnimo.com/firmware/ac25.amf](https://(account name):(password)@package.amnimo.com/firmware/ac25.amf)

Please contact our support separately for your account and password as well as the firmware URL specifying the version.

Execution example

管理者 モード

```

Downloading
amnimo# firmware file check ftp://amnimo:xxxxx@amnimo-host/firmware/staging/ag10-1.0.0
-b12345.amf ↵
Downloading...
##### 36.3%
After downloading is complete
amnimo# firmware file check ftp://amnimo:xxxxx@amnimo-host/firmware/staging/ag10-1.0.0
-b12345.amf ↵
Downloading...
##### 100.0%
version: amnimo G series AG10 version 1.0.0 build 12345
contents: rootfs bootloader

```

2.4.3 Delete the firmware



Downloaded firmware files can be deleted with the firmware file delete command.



- Downloaded firmware files are stored in RAM.
- If no files have already been downloaded, "ERROR: Firmware file does not exist." will be displayed when the command is executed.

Execution example

管理者 モード

```
amnimo# firmware file delete ↵
Deleted!
```

2.4.4 Update firmware



There are two areas of the product's firmware to be updated: the boot area and the redundant area. To update each area, execute the **firmware area update** command. After executing this command, you will be asked if you want to reboot. If you allow the reboot, the firmware will be updated. (This method of updating the firmware is referred to as a "global update.")



Before executing this command, the firmware file must be downloaded.

Format

```
firmware area update [target <back | both>] [force <true | false>] [url URL].
```

Setting items

Item	Contents						
target	<p>Set the target to be updated.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>back</td> <td>Update redundant areas that are not currently activated.</td> </tr> <tr> <td>both</td> <td>Update both redundant areas.</td> </tr> </tbody> </table> <p> The default value is "back" for V1.7.0 and below, and "both" for V1.8.0 and above.</p>	Setting	Contents	back	Update redundant areas that are not currently activated.	both	Update both redundant areas.
Setting	Contents						
back	Update redundant areas that are not currently activated.						
both	Update both redundant areas.						
force	<p>Sets whether or not the user is confirmed upon restart.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>true</td> <td>Force restart without user confirmation.</td> </tr> <tr> <td>false</td> <td>Check with the user before rebooting.</td> </tr> </tbody> </table>	Setting	Contents	true	Force restart without user confirmation.	false	Check with the user before rebooting.
Setting	Contents						
true	Force restart without user confirmation.						
false	Check with the user before rebooting.						
url	<p>The URL can be HTTP or FTP. The following is an example configuration with the file name ag10-v1.0.0-b1.amf.</p> <ul style="list-style-type: none"> ● When using a file that exists in storage e.g.) file:///media/usb/ag10-v1.0.0-b1.amf ● When using a file that exists on a TFTP server e.g.) tftp://example.com/ag10-v1.0.0-b1.amf ● When using a file that exists on an FTP server that supports password authentication e.g.) ftp://username:password@example.com/ag10-v1.0.0-b1.amf ● When using a file that exists on an HTTP server that supports Basic Authentication e.g.) http://username:password@example.com/ag10-v1.0.0-b1.amf ● When using a file that exists on an HTTPS server that supports Basic Authentication e.g.) https://username:password@example.com/ag10-v1.0.0-b1.amf <p> If the URL is omitted, a firmware check is performed and if firmware has already been downloaded, it is used; if not, an error is generated.</p>						

Execution example 1 (V1.8.0 or later)

Here is an example of performing an update in administrator mode with the farm already downloaded.

管理者 モード

```
amnimo# firmware area update ↵
Do you want to update (full update) the area with the following contents?
After updating, restart the gateway.
Update area: Both sides
reboot to update? (y/N): ↵ Enter "y" key followed by Enter
```



To cancel execution of the command, type Enter or press the "n" key followed by Enter.

Execution example 2 (V1.8.0 or later)

The following is an example of executing the firmware download and updating a redundant area that is not currently running by specifying the firmware URL (ftp://username:password@example.com/ag10-v1.0.0-b1.amf) in administrator mode.

管理者 モード

```
amnimo# firmware area update target back url ftp://username:password@example.com/ag10.
amf ↵
Do you want to update (full update) the area with the following contents?
After updating, restart the gateway.
Update area: One side
reboot to update? (y/N): ↵ Enter "y" key followed by Enter
```



To cancel execution of the command, type Enter or press the "n" key followed by Enter.

2.4.5 Synchronize redundant areas of firmware



To copy the currently activated redundant area to the other redundant area, execute the firmware area sync command.

The copy targets the rootfs and userfs areas. The contents of the destination redundant area are deleted.

After executing this command, you will be asked if you want to reboot. If you allow the reboot, the firmware will be updated.

Format

```
firmware area sync [force <true | false>].
```

Setting items

Item	Contents						
force	Sets whether or not the user is confirmed upon restart. <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>true</td> <td>Force restart without user confirmation.</td> </tr> <tr> <td>false</td> <td>Check with the user before rebooting.</td> </tr> </tbody> </table>	Setting	Contents	true	Force restart without user confirmation.	false	Check with the user before rebooting.
Setting	Contents						
true	Force restart without user confirmation.						
false	Check with the user before rebooting.						

Execution example

管理者モード

```
amnimo# firmware area sync ↵
reboot to sync? (y/N): ← "y" key followed by Enter
```



To cancel execution of the command, type Enter or press the "n" key followed by Enter.

2.4.6 Set the redundant area to be activated



Displays and configures the currently activated redundant area.

Show redundant areas

Displays the current redundancy area.

- 0: When the redundant area is 0
- 1: When the redundant area is 1

Execution example

Command input and output are the same in general user mode and administrator mode. An example of execution in general user mode is shown below.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device boot ↵
1
```

Set up a redundant area to be activated next time

To set up a redundant area to boot next time, execute the device boot command.

One of the following values is specified as a parameter to this command.

- 0: When the startup area is 0
- 1: When the startup area is 1

Execution example

管理者モード 設定モード

```
amnimo# device boot 0 ↵
```

2.4.7 Update firmware package information



To obtain package update information and view a list of packages that have updates, run the *firmware package update* command.



This function is not available on Compact Router.

Execution example

管理者 モード

```
amnimo# firmware package update ↵
package name          new version          old version
-----
amnimo-cli            1.2.0                1.1.0
libag-baes            1.1.0                1.0.0
libarchive            3.2.2-3.1ubuntu0.6  3.1.2-7ubuntu2
isc-dhcp-client       4.3.5-3ubuntu7.1    4.2.4-7ubuntu12
(Omitted.)
-----
```

2.4.8 Update the firmware package



To update the firmware package, run the firmware package upgrade command.

The packages to be updated are those that appear when the firmware package information is updated. (Hereafter, the method of updating by this function is referred to as "differential update.")

➔ " 2.4.7 Update firmware package information "



- It is not possible to specify individual firmware packages to be updated.
- This function uses the apt package management system.
 - The "--force-confold" option is applied when updating packages. This ensures that even if the configuration file for each package is changed in a package update, the configuration file before the change is used.
- After updating the package, it is recommended to reboot this device for security reasons.
- This function is not available on Compact Router.

Execution example

管理者 モード

```
amnimo# firmware package upgrade ↵
Downloading amnimo-cli...
Installing amnimo-cli ...
```

About general update and differential update

The differences between whole and differential updates are described below. According to the characteristics of each, it is possible to use them differently depending on the usage situation.

		General Update	Differential Update
Update area	Setting area	not subject (to) (The configuration file is retained.)	not subject (to) (The configuration file is retained.)
	rootfs	General Update  Since the area will be initialized, any packages that users have installed on their own will also be removed.	Differential Update  User-installed packages are retained.
	userfs	not subject (to)	not subject (to)
	shared area	not subject (to)	not subject (to)
	SSD	not subject (to)	not subject (to)
Update redundant areas		addressable	designation not possible
Communication costs for downloading		large (e.g. serving size)	small
Update time		long (time)	short  <ul style="list-style-type: none"> The startup area and redundant area cannot be updated simultaneously. When updating both sides, a separate area synchronization is required, which takes about 10 minutes. Depending on the number of packages with differences, this may take longer than an overall update.

2.4.9 Delete the firmware package information file



To remove the firmware package information file, run the firmware package clean command.



This function is not available on Compact Router.

Execution example

管理者モード

```
amnimo# firmware package clean ↵
```



If you have removed a firmware package and wish to retrieve it again, please update the package information.

➔ " 2.4.7 Update firmware package information "

2.5 Working with package repositories



Performs operations related to package repositories.



This function is not available on Compact Router.

2.5.1 Add package repository credentials

To add credentials for the package repository, run the apt auth command.

Format

```
apt auth hostname HOSTNAME username USERNAME password PASSWORD
```

Setting items

Item	Contents
HOSTNAME	Enter the hostname of the package repository.
USERNAME	Enter the username used to authenticate the package repository. <ul style="list-style-type: none"> ● The maximum length is 32 characters, excluding "%" and "?" from "user" as defined in RFC 1738. characters from "user" specified in RFC 1738. ● Only alphanumeric characters can be used for the first character and the last character.
PASSWORD	Enter the password used to authenticate the package repository. <ul style="list-style-type: none"> ● The maximum length is 32 characters, excluding "%" and "?" from "user" as defined in RFC 1738. characters from "user" specified in RFC 1738. ● Passwords are kept in plain text.

Execution example

設定 モード

```
amnimo(cfg)# apt auth hostname package.amnimo.com username testuser1 password testpass
1 ↵
```

2.5.2 Removing credentials from the package repository

To remove authentication information by hostname, run the no apt auth command.

Format

```
no apt auth HOSTNAME
```

Setting items

Item	Contents
HOSTNAME	Enter the name of the host to be deleted.

Execution example

設定 モード

```
amnimo(cfg)# no apt auth package.amnimo.com ↵
```

2.5.3 View package repository credentials

To view the authentication information for the package repository, run the *show config apt auth* command.

Format

```
show config apt auth
```

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# show config apt auth ↵  
# ---- Apt auth configure ----  
apt auth hostname package1.amnimo.com username testuser1 password testpass1
```

2.6 Change a user's password



There are two ways to change a user's password: the logged-in user can change his/her own password, or the administrator can change the password of another user.

2.6.1 Change the password of the logged-in user himself/herself

A logged-in user can change the password for his or her own account by executing the *account password* command.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ account password ↵
(current) password: ← Enter current password and press Enter
Enter new password: ← Enter new password and press Enter
Retype new password: ← Enter new password again and press Enter
passwd: password updated successfully
```



If the password could not be changed because the conditions were not met, the following error message will be displayed

If the password for the account you are logged into is incorrect

```
passwd: Authentication token manipulation error
passwd: password unchanged
```

If the new password does not match the new password you re-enter

```
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
```

If the current password and the new password are the same

```
Password unchanged.
passwd: Authentication token manipulation error.
passwd: password unchanged.
```

If the new password is too easy

```
Bad: new password is too simple
passwd: Authentication token manipulation error.
passwd: password unchanged
```



The password must be a string that meets the following conditions. The string can be "password" as defined in RFC1738.

- 8 characters or more
- Includes at least two types of uppercase and lowercase letters, numbers, and symbols

Even if a password satisfies the above conditions, it cannot be set if any of the following conditions apply

- Words in the dictionary (e.g., test)
- Words with regularity, such as number or alphabet keyboard sequences (e.g.,

1234, abcde, qwert)

- Combination of the above (e.g., test1234)



passwd: Authentication token manipulation error." and "passwd: password unchanged." are displayed when there is a problem with the password input and it exits.

2.6.2 Change password by specifying user

Changes the password for the specified user.

Format

```
account password USERNAME
```

Setting items

Item	Contents
USERNAME	Specify the username whose password you wish to change.

Execution example

設定モード

```
amnimo(cfg)# account password username1 ↵
Enter new password:           ← Enter new password and press Enter
Retype new password:         ← Enter new password again and press Enter
passwd: password updated successfully
```



If the password could not be changed because the conditions were not met, the following error message will be displayed

If the new password does not match the new password you re-enter

```
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
```

If the new password is too easy

```
Bad: new password is too simple
```



The password must be a string of characters that meets the following conditions. The string can be "password" as defined in RFC1738.

- 8 characters or more
- Includes at least two types of uppercase and lowercase letters, numbers, and symbols

Even if a password satisfies the above conditions, it cannot be set if any of the following conditions apply

- Words in the dictionary (e.g., test)
- Words with regularity, such as number or alphabet keyboard sequences (e.g., 1234, abcde, qwert)
- Combination of the above (e.g., test1234)

2.7 Set up your account



Display user list, display user/group setting information, and configure user/group settings.

2.7.1 Display the user list

To view a list of users, run the *show account* command.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

```

管理者 モード 設定 モード
amnimo# show account ↵
amnimo
username1
username2
(Omitted.)

```

2.7.2 Show logged-in users of users

To view the currently logged-in user, run the *show account now* command to view your own user.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

```

ユーザー モード 管理者 モード 設定 モード
amnimo$ show account now ↵
username1

```

2.7.3 Display user settings

To view user configuration information for the currently registered user, run the *show config account* command.

Format (V1.7.0 or earlier)

```
show config account [USERNAME].
```

Format (V1.8.0 or later)

```
show config account user [USERNAME].
```

Setting items

Item	Contents
USERNAME	Specify a username.

Output format (V1.8.0 or later)

```
# ---- account user USERNAME configure ----
account user USERNAME
```

```
password secret ENCRYPT-PASSWORD
group GROUP
LOGOUT-SEC
EXPIRES-DAY
```

Output item

Item	Contents						
ENCRYPT-PASSWORD	The encrypted password is displayed.						
GROUP	<p>The following user groups and the group names set by the group setting function described below will be displayed.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>admin</td> <td>Admin User</td> </tr> <tr> <td>user</td> <td>general user</td> </tr> </tbody> </table>	Value	Description	admin	Admin User	user	general user
Value	Description						
admin	Admin User						
user	general user						
LOGOUT-SEC	<p>The time (in seconds) until automatic logout with no operation is displayed in the range of 1 to 3600.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "auto-logout <i>logout time</i>" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no auto-logout" is displayed</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "auto-logout <i>logout time</i> " is displayed.	Disable	The message "no auto-logout" is displayed
Setting	Display						
Enable	The message "auto-logout <i>logout time</i> " is displayed.						
Disable	The message "no auto-logout" is displayed						
EXPIRES-DAY	<p>The password expiration date (in days) is displayed in the range of 1 to 9999.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "password-expires <i>setting time</i>" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no password-expires" is displayed</td> </tr> </tbody> </table> <p> Not shown on Compact Router.</p>	Setting	Display	Enable	The message "password-expires <i>setting time</i> " is displayed.	Disable	The message "no password-expires" is displayed
Setting	Display						
Enable	The message "password-expires <i>setting time</i> " is displayed.						
Disable	The message "no password-expires" is displayed						

Execution example (V1.8.0 or later)

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# show config account user↵
# ---- transition to configure mode ----
configure
# ---- account amnimo configure ----
account user amnimo
password secret nlp5T84z0jPAIbdo0sx/qw==
group admin
no auto-logout
no password-expires
exit
# ---- account username1 configure ----
account user username1
password secret Kg/9Eyd1USoHeZmB92RPVg==
group admin
auto-logout 60
password-expires 90
exit
# ---- account username2 configure ----
account user username2
```

```
password secret oksgDyd1U9TdBHAnqY1Skg==
group user
auto-logout 60
password-expires 90
exit
# ---- exit configure mode ----
exit
```

2.7.4 Configuring Users

To change the settings of an existing user or add a new user, go to the user's advanced configuration mode and execute the configuration commands. The settings made here will be written to a configuration file.

Format (V1.7.0 or earlier)

```
account USERNAME
group <admin | user>
password
password secret ENCRYPT-PASSWORD
auto-logout <1 - 3600>
no auto-logout
password-expires <1 - 9999>
no password-expires
exit
no account USERNAME
```

Format (V1.8.0 or later)

```
account user USERNAME
group <admin | user> ← Group names created with the group settings function can also be selected.
password
password secret ENCRYPT-PASSWORD
auto-logout <1 - 3600>
no auto-logout
password-expires <1 - 9999>
no password-expires
exit
no account USERNAME
```

Command

Command	Contents								
account user	<p>Execute the user configuration command, specifying the username in USERNAME.</p> <p> Executing a command in the configuration mode will enter the advanced configuration mode for the specified user.</p> <p> For the username, set a string that meets the following criteria</p> <ul style="list-style-type: none"> ● At least 1 character, up to 32 characters ● Lower case letters, numbers or '_'. ● String with only numbers is prohibited. (Version 2.0.0 or later) 								
group	<p>Specify the following user groups and the group names set by the group setting function described below.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>admin</td> <td>Admin User</td> </tr> <tr> <td>user</td> <td>general user</td> </tr> <tr> <td>Any group</td> <td>Group name added with the group settings function</td> </tr> </tbody> </table>	Setting	Contents	admin	Admin User	user	general user	Any group	Group name added with the group settings function
Setting	Contents								
admin	Admin User								
user	general user								
Any group	Group name added with the group settings function								

Command	Contents
password	<p>Set a password. If the password change is successful, the encrypted password is saved.</p> <p> The password must be a string that meets the following criteria: "password" as defined in RFC1738.</p> <ul style="list-style-type: none"> ● 8 characters or more ● Includes at least two types of uppercase and lowercase letters, numbers, and symbols <p>Even if a password satisfies the above conditions, it cannot be set if any of the following conditions apply</p> <ul style="list-style-type: none"> ● Words in the dictionary (e.g., test) ● Words with regularity, such as number or alphabet keyboard sequences (e.g., 1234, abcde, qwert) ● Combination of the above (e.g., test1234)
password secret	Specify an encrypted password string in ENCRYPT-PASSWORD to update the password.
auto-logout	Specify the time (in seconds) before automatic logout with no operation, in the range of 1 to 3600.
no auto-logout	Disable automatic logout.
password-expires	Specify the password expiration date (in days) in the range of 1 to 9999.  Compact Router cannot be configured.
no password-expires	Set an unlimited password expiration date.  Compact Router cannot be configured.
show config	Displays the user's settings. ➔ For more information, see "2.7.3 Display user settings" for more information.
exit	Exits the user's advanced setting mode and enters the setting mode.
no account	Delete a user by specifying the username in USERNAME.

Execution example (V1.8.0 or later)

設定モード

Example of adding administrator user1 (auto logout: disabled, password expiration: unlimited)

```
amnimo(cfg)# account user user1 ↵
amnimo(cfg-account-user1)# password ↵
Enter new password:                ← Enter password and press Enter
Retype new password:              ← Enter password again and press Enter
passwd: password updated successfully. ← Password changed successfully.
amnimo(cfg-account-user1)# group admin ↵
amnimo(cfg-account-user1)# exit ↵
```

Example of adding a general user guest

```
amnimo(cfg)# account user guest ↵
amnimo(cfg-account-guest)# password secret jVh/Ewuxz8cuK1f4AmKOnA==↵ ← set encrypted password
amnimo(cfg-account-guest)# group user ↵
amnimo(cfg-account-guest)# auto-logout 300↵ ← Set auto logout to 300 seconds
amnimo(cfg-account-guest)# password-expires 3↵ ← Set password expires 3 days
amnimo(cfg-account-guest)# exit ↵
```

Example of deleting the general user guest

```
amnimo(cfg)# no account user guest ↵
```

2.7.5 Display group settings

To view the group configuration information for the currently registered user, run the **show config group** command.



- This function only supports GUI permissions, not CLI (amsh) operating permissions. newly created groups on the CLI will have the same permissions as the default settings.
- The admin group, admin, is not shown.

Format

```
show config account group [GROUPNAME].
```

Setting items

Item	Contents
GROUPNAME	Specify a group name.

Output Format

```
# ---- account group GROUPNAME configure ----
account group GROUPNAME
authorization scope SCOPE_ID
```

Output item

Item	Contents								
GROUPNAME	The group name is displayed.								
SCOPE_ID	<p>The list of permissions granted to the group is displayed in the following format.</p> <pre>ACTION:SUBJECT:RESOURCE</pre> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ACTION</td> <td>Indicates operating privileges. If omitted, it indicates that all operating privileges are granted. If omitted, also omits ":".</td> </tr> <tr> <td>SUBJECT</td> <td>Indicates the functional category to which operating privileges are granted. If omitted, all functional categories are indicated. If omitted, ":" is also omitted.</td> </tr> <tr> <td>RESOURCE</td> <td>Indicates the ability to grant operating privileges.</td> </tr> </tbody> </table> <p>➔ For details on each parameter, see "2.7.7 Group Permissions" of the configuration "</p>	Parameter	Description	ACTION	Indicates operating privileges. If omitted, it indicates that all operating privileges are granted. If omitted, also omits ":".	SUBJECT	Indicates the functional category to which operating privileges are granted. If omitted, all functional categories are indicated. If omitted, ":" is also omitted.	RESOURCE	Indicates the ability to grant operating privileges.
Parameter	Description								
ACTION	Indicates operating privileges. If omitted, it indicates that all operating privileges are granted. If omitted, also omits ":".								
SUBJECT	Indicates the functional category to which operating privileges are granted. If omitted, all functional categories are indicated. If omitted, ":" is also omitted.								
RESOURCE	Indicates the ability to grant operating privileges.								

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# show config account group
# ---- transition to configure mode ----
configure
# ---- account group user configure ----
account group user
authorization scope show:device:information
authorization scope show:device:firmware
```

```

authorization scope show:device:boot
authorization scope show:device:hostname
authorization scope show:device:timezone
authorization scope show:device:account_user
authorization scope update:config:account_user_password
authorization scope show:device:mobile_module
authorization scope show:device:mobile
authorization scope show:device:ppp
authorization scope show:device:interface
authorization scope show:device:routing_static
authorization scope execute:device:nslookup
authorization scope show:device:dns
authorization scope show:device:dhcp_lease_list
authorization scope show:device:ipsec
authorization scope show:device:ntp
authorization scope show:device:storage
authorization scope show:device:schedule
authorization scope show:device:poe
authorization scope show:device:usb
authorization scope execute:device:ping
authorization scope execute:device:traceroute
authorization scope show:device:arp
authorization scope show:device:cpu
authorization scope show:device:temperature
authorization scope show:device:voltage
authorization scope show:device:datetime
authorization scope show:device:dout
authorization scope show:device:din
authorization scope show:device:dip_switch
authorization scope show:device:dms
authorization scope show:device:nxwitness
authorization scope show:device:remoteit
exit
# ---- account group group1 configure ----
account group group1
authorization scope show:device:information
authorization scope show:device:firmware
authorization scope show:device:boot
authorization scope show:device:hostname
authorization scope show:device:timezone
authorization scope show:device:account_user
authorization scope update:config:account_user_password
authorization scope show:device:mobile_module
authorization scope show:device:mobile
authorization scope show:device:ppp
authorization scope show:device:interface
authorization scope show:device:routing_static
authorization scope execute:device:nslookup
authorization scope show:device:dns
authorization scope show:device:dhcp_lease_list
authorization scope show:device:ipsec
authorization scope show:device:ntp
authorization scope show:device:storage
authorization scope show:device:schedule
authorization scope show:device:poe
authorization scope show:device:usb
authorization scope execute:device:ping
authorization scope execute:device:traceroute
authorization scope show:device:arp
authorization scope show:device:cpu

```

```
authorization scope show:device:temperature
authorization scope show:device:voltage
authorization scope show:device:datetime
authorization scope show:device:dout
authorization scope show:device:din
authorization scope show:device:dip_switch
authorization scope show:device:dms
authorization scope show:device:nxwitness
authorization scope show:device:remoteit
exit
# ---- exit configure mode ----
exit
```

2.7.6 Set up a group

To change the settings of an existing group or add a new group, go to the group's advanced configuration mode and execute the configuration commands. The settings made here will be written to a configuration file.



- This function only supports GUI permissions, not CLI (amsh) operating permissions. newly created groups on the CLI will have the same permissions as the default settings.
- It cannot be set for admin, which is the administrator group.
- This function is supported by firmware V1.8.0 or later; CLI-related operation permission settings will be supported in a future release.

Format

```
account group GROUPNAME
authorization scope SCOPE_ID
no authorization scope SCOPE_ID
exit
no account group GROUPNAME
```

Command

Command	Contents												
account group	<p>Execute the group setup command, specifying the group name in GROUPNAME.</p> Executing a command in the configuration mode will enter the detailed configuration mode for the specified group. The group name should be a string that meets the following criteria <ul style="list-style-type: none"> ● At least 1 character, up to 24 characters ● Lower case letters, numbers or '_' ● String with only numbers is prohibited. (Version 2.0.0 or later) 												
authorization scope	<p>Set the privileges to be granted to the group.</p> <table border="1"> <thead> <tr> <th>parameter</th> <th>Description.</th> </tr> </thead> <tbody> <tr> <td>SCOPE_ID</td> <td>Indicates the authorization setting to be granted.</td> </tr> </tbody> </table> <p>SCOPE_ID is set in the following format.</p> <div style="background-color: #f0f0f0; padding: 5px; text-align: center;">ACTION:SUBJECT:RESOURCE</div> <table border="1"> <thead> <tr> <th>parameter</th> <th>Description.</th> </tr> </thead> <tbody> <tr> <td>ACTION</td> <td>Indicates operating privileges. If omitted, it indicates that all operating privileges are granted. If omitted, also omits ":".</td> </tr> <tr> <td>SUBJECT</td> <td>Indicates the functional category to which operating privileges are granted. If omitted, all functional categories are indicated. If omitted, ":" is also omitted.</td> </tr> <tr> <td>RESOURCE</td> <td>Indicates the ability to grant operating privileges.</td> </tr> </tbody> </table> <p>➔ For details on each parameter, see "2.7.7 Group Permissions For various parameters of the configuration "</p>	parameter	Description.	SCOPE_ID	Indicates the authorization setting to be granted.	parameter	Description.	ACTION	Indicates operating privileges. If omitted, it indicates that all operating privileges are granted. If omitted, also omits ":".	SUBJECT	Indicates the functional category to which operating privileges are granted. If omitted, all functional categories are indicated. If omitted, ":" is also omitted.	RESOURCE	Indicates the ability to grant operating privileges.
parameter	Description.												
SCOPE_ID	Indicates the authorization setting to be granted.												
parameter	Description.												
ACTION	Indicates operating privileges. If omitted, it indicates that all operating privileges are granted. If omitted, also omits ":".												
SUBJECT	Indicates the functional category to which operating privileges are granted. If omitted, all functional categories are indicated. If omitted, ":" is also omitted.												
RESOURCE	Indicates the ability to grant operating privileges.												
no authorization scope	Deletes the privileges granted to the group.												
show config	<p>Displays group settings.</p> <p>➔ For more information, see "2.7.5 Display group settings.</p>												

Command	Contents
Exit	Exit the group detail setting mode and enter the setting mode.
no account	Delete a group by specifying a username in USERNAME.

Execution example

The following executable example adds group1, grants configuration privileges related to SSH, and removes display privileges related to the mobile module.

設定モード

```

amnimo(cfg)# account group group1 ↵
amnimo(cfg-acnt-group-group1)# show config ↵
↓ Following is the default setting
authorization scope show:device:information
authorization scope show:device:firmware
authorization scope show:device:boot
authorization scope show:device:hostname
authorization scope show:device:timezone
authorization scope show:device:account_user
authorization scope update:config:account_user_password
authorization scope show:device:mobile_module
authorization scope show:device:mobile
authorization scope show:device:ppp
authorization scope show:device:interface
authorization scope show:device:routing_static
authorization scope execute:device:nslookup
authorization scope show:device:dns
authorization scope show:device:dhcp_lease_list
authorization scope show:device:ipsec
authorization scope show:device:ntp
authorization scope show:device:storage
authorization scope show:device:schedule
authorization scope show:device:poe
authorization scope show:device:usb
authorization scope execute:device:ping
authorization scope execute:device:traceroute
authorization scope show:device:arp
authorization scope show:device:cpu
authorization scope show:device:temperature
authorization scope show:device:voltage
authorization scope show:device:datetime
authorization scope show:device:dout
authorization scope show:device:din
authorization scope show:device:dip_switch
authorization scope show:device:dms
authorization scope show:device:nxwitness
authorization scope show:device:remoteit
amnimo(cfg-acnt-group-group1)# authorization scope show:config:ssh↵← Grant SSH configuration control display authority
amnimo(cfg-acnt-group-group1)# authorization scope update:config:ssh↵← Authorization to change SSH settings
amnimo(cfg-acnt-group-group1)# authorization scope delete:config:ssh↵← Authorization to delete SSH settings
amnimo(cfg-acnt-group-group1)# no authorization scope show:device:mobile↵← Remove mobile status display authority
amnimo(cfg-acnt-group-group1)# no authorization scope show:device:mobile_module↵← Remove authorization to display mobile module information
amnimo(cfg-acnt-group-group1)# show config
authorization scope show:device:information

```

```
authorization scope show:device:firmware
authorization scope show:device:boot
authorization scope show:device:hostname
authorization scope show:device:timezone
authorization scope show:device:account_user
authorization scope update:config:account_user_password
authorization scope show:device:ppp
authorization scope show:device:interface
authorization scope show:device:routing_static
authorization scope execute:device:nslookup
authorization scope show:device:dns
authorization scope show:device:dhcp_lease_list
authorization scope show:device:ipsec
authorization scope show:device:ntp
authorization scope show:device:storage
authorization scope show:device:schedule
authorization scope show:device:poe
authorization scope show:device:usb
authorization scope execute:device:ping
authorization scope execute:device:traceroute
authorization scope show:device:arp
authorization scope show:device:cpu
authorization scope show:device:temperature
authorization scope show:device:voltage
authorization scope show:device:datetime
authorization scope show:device:dout
authorization scope show:device:din
authorization scope show:device:dip_switch
authorization scope show:device:dms
authorization scope show:device:nxwitness
authorization scope show:device:remoteit
authorization scope show:config:ssh ← setting is added.
authorization scope update:config:ssh ← setting is added.
authorization scope delete:config:ssh ← setting is added.
```

2.7.7 Group Permissions For various parameters of the configuration

This section describes each parameter of the authorization setting in authorization scope.



Functions related to authority settings vary by model. For details, see "12.2 CLI functions supported by each product" for details.

Operating authority

Authorization for the following types of operations can be granted. It depends on the function category and function to change to the operation authorization that can be specified.

Parameter	Contents
show	Authorization to display information.
append	Authorization to add settings.
update	Authorization to update settings.
delete	Authorization to delete settings.
execute	Grants authority to execute control.

Functional Category

The following functional categories can be specified. The functional categories that can be specified depend on the functionality.

Parameter	Contents
device	Indicates the function category related to the device itself.
config	Indicates the functional categories related to the configuration file.
firmware	Indicates functional categories related to firmware.

List of Group Permission Settings

The following authorization settings can be configured by combining the above operation authorization and function categories.

Parameter	Contents
execute:device:reboot	Equipment restart control
execute:device:poweroff	Equipment power-down possible state transition
show:device:information	Device Information Display  This operation authorization is required to use the GUI.
show:device:firmware	Firmware version display
execute:firmware:file_check	Firmware file confirmation
execute:firmware:file_delete	Firmware file deletion
execute:firmware:area_update	Firmware update
execute:firmware:area_sync	Redundant area synchronization
show:device:boot	Startup area display
execute:device:boot	Startup area setting
execute:firmware:package_update	apt package information update
execute:firmware:package_upgrade	apt package update
execute:firmware:package_clean	apt package information removal
show:config:apt_auth_hostname	View credentials for apt package repositories
append:config:apt_auth_hostname	Add credentials for apt package repositories
update:config:apt_auth_hostname	Updating credentials in apt package repositories

Parameter	Contents
delete:config:apt_auth_hostname	Delete credentials in apt package repositories
execute:config:initialize	initialization
show:config:file	Persistence setting list display
execute:config:file_save	persistent setup write
execute:config:file_load	Read persistence setting
execute:config:file_move	Permanent setting name change
execute:config:file_copy	Persistence setting copy
execute:config:file_delete	Delete persistence setting
show:device:file	file list view
execute:device:file_move	File Movement Control
execute:device:file_copy	file copy control
execute:device:file_delete	file deletion control
show:device:hostname	Host Name Display
show:config:hostname	Host Name Setting Display
update:config:hostname	Host name setting change
show:device:timezone	Time Zone Display
show:config:timezone	Time zone setting display
update:config:timezone	Change time zone setting
update:config:account_user_password	Change User Password
show:device:account_user	Logged-in user display
show:config:account_user	User setting display
append:config:account_user	Add user settings
update:config:account_user	Change User Preferences
delete:config:account_user	Delete user settings
show:config:account_group	group settings indication
append:config:account_group	Add group settings
update:config:account_group	Change group settings
delete:config:account_group	Delete group settings
show:device:mobile_module	Mobile Module Information Display
execute:device:mobile_module	Mobile Module Control
show:device:mobile	Mobile Status Display
execute:device:mobile_connect	Mobile connection control (manual connection mode)
execute:device:mobile_disconnect	Mobile disconnection control
show:config:mobile_module	Mobile Module Settings Display
show:config:mobile_peer	Mobile peer setting display
append:config:mobile_peer	Mobile peer settings added
update:config:mobile_peer	Mobile peer setting change
delete:config:mobile_peer	Mobile Peer Settings Deleted
show:device:ppp	PPP status display
execute:device:ppp_connect	PPP connection control (manual connection)
execute:device:ppp_disconnect	PPP Disconnection Control
show:config:ppp_peer	PPP setting display

Parameter	Contents
append:config:ppp_peer	PPP settings added
update:config:ppp_peer	PPP setting change
delete:config:ppp_peer	Delete PPP settings
show:device:interface	interface status indication
show:config:interface	Interface setting display
append:config:interface	Interface settings added
update:config:interface	Interface setting change
delete:config:interface	Delete interface settings
show:device:routing_static	routing table display
show:config:routing_static	Routing setting display
append:config:routing_static	Additional routing settings
update:config:routing_static	Change routing settings
delete:config:routing_static	Delete routing settings
show:config:filter_input	Filter setting display (input)
append:config:filter_input	Add filter setting (input)
update:config:filter_input	Filter setting change (input)
delete:config:filter_input	Delete filter setting (input)
show:config:filter_output	Filter setting display (output)
append:config:filter_output	Add filter setting (output)
update:config:filter_output	Filter setting change (output)
delete:config:filter_output	Delete filter setting (output)
show:config:filter_forward	Filter setting display (forward)
append:config:filter_forward	Add filter setting (forward)
update:config:filter_forward	Change filter settings (forward)
delete:config:filter_forward	Delete filter settings (forward)
show:config:nat_snat_dynamic	Display of NAT settings (dynamic-snat)
append:config:nat_snat_dynamic	Additional NAT settings (dynamic-snat)
update:config:nat_snat_dynamic	Change NAT settings (dynamic-snat)
delete:config:nat_snat_dynamic	Delete NAT settings (dynamic-snat)
show:config:nat_snat_static	Display of NAT settings (static-snat)
append:config:nat_snat_static	Add NAT configuration (static-snat)
update:config:nat_snat_static	Change NAT settings (static-snat)
delete:config:nat_snat_static	Delete NAT settings (static-snat)
show:config:nat_dnat	NAT setting display (dnat)
append:config:nat_dnat	Add NAT settings (dnat)
update:config:nat_dnat	Change NAT settings (dnat)
delete:config:nat_dnat	NAT setting deletion (dnat)
execute:device:nslookup	DNS (forward and reverse) lookup
show:device:dns	DNS status display
show:config:dns	DNS Settings Display
append:config:dns	DNS settings added
update:config:dns	DNS setting change
delete:config:dns	Delete DNS settings

Parameter	Contents
show:device:dhcp_lease_list	DHCP lease list display
show:config:dhcp	DHCP server setting display
append:config:dhcp	Additional DHCP server settings
update:config:dhcp	DHCP server setting change
delete:config:dhcp	Delete DHCP server settings
show:device:ipsec	IPsec status display
execute:device:ipsec_connect	IPsec connection control (manual connection)
execute:device:ipsec_disconnect	IPsec disconnection control
show:config:ipsec	IPsec setting display
append:config:ipsec	IPsec settings added
update:config:ipsec	IPsec Configuration Control
delete:config:ipsec	Deletion of IPsec settings
show:device:ntp	NTP status display
show:config:ntp	NTP setting display
update:config:ntp	NTP setting change
delete:config:ntp	NTP settings deleted (default settings)
show:config:ssh	SSH setting display
update:config:ssh	Change SSH settings
delete:config:ssh	Delete SSH settings (default settings)
show:device:storage_partition	Storage partition display
execute:device:storage_partition	Storage partition control
show:device:storage_format	Storage Format Display
execute:device:storage_format	Storage Format Control
show:device:storage_mount	Storage mount display
execute:device:storage_mount	Storage mount control
execute:device:storage_fsck	Storage Check Control
show:device:storage_usage	Storage Usage Status Display
show:config:storage	Storage Settings Display
append:config:storage	Additional storage settings
update:config:storage	Change storage settings
delete:config:storage	Storage Settings Deleted
show:device:schedule_general_control	Display of schedule operation status (general-control)
show:device:schedule_keep_alive	Scheduled operation status display (keep-alive)
show:device:schedule_user_define	Schedule operation status display (user-define)
show:config:schedule_general_control	Schedule setting display (general-control)
append:config:schedule_general_control	Add schedule setting (general-control)
update:config:schedule_general_control	Change schedule settings (general-control)
delete:config:schedule_general_control	Delete schedule setting (general-control)
show:config:schedule_keep_alive	Schedule setting display (keep-alive)
append:config:schedule_keep_alive	Add schedule setting (keep-alive)
update:config:schedule_keep_alive	Change schedule settings (keep-alive)
delete:config:schedule_keep_alive	Delete schedule settings (keep-alive)

Parameter	Contents
show:config:schedule_user_define	Schedule setting display (user-define)
append:config:schedule_user_define	Add schedule setting (user-define)
update:config:schedule_user_define	Change schedule settings (user-define)
delete:config:schedule_user_define	Delete schedule setting (user-define)
show:device:poe	PoE status display
execute:device:poe	PoE port control (power on/off, reset)
show:config:poe	PoE setting display
update:config:poe	PoE setting change
delete:config:poe	Delete PoE settings (restore default values)
show:device:usb	USB device list display
execute:device:usb	USB device control (power on/off, reset)
show:device:syslog_local	Syslog message display
show:config:syslog_local	Display of Syslog settings (local)
update:config:syslog_local	Syslog configuration change (local)
show:config:syslog_remote	Display of Syslog settings (remote)
update:config:syslog_remote	Syslog setting change (REMOTE)
execute:device:amlog	amlog control
show:device:amlog	amlog display
execute:device:ping	ping control
execute:device:traceroute	TRACEROUTE Control
show:device:arp	ARP Information Display
execute:device:arp	ARP Information Control
execute:device:packet_dump	packet dump control
show:device:packet_dump_file	Packet dump file display
execute:device:packet_dump_file	packet dump file control
show:device:cpu	CPU operation indication
show:config:cpu	CPU operation setting display
update:config:cpu	CPU operation setting control
show:config:temperature	High/low temperature protection setting display
update:config:temperature	High/low temperature protection setting control
delete:config:temperature	High/low temperature protection setting deleted (default setting)
show:device:temperature	Temperature display inside the enclosure
show:device:voltage	Voltage indication
show:device:datetime	Time display
execute:device:datetime_manual	Time setting (manual)
execute:device:datetime_ntpdate	Time setting (ntpdate)
show:device:dout	DOUT status display
execute:device:dout	DOUT Control
show:device:din	DIN status indication
show:device:din_logger	DIN Logger Display
show:config:din_logger	DIN logger setting display
update:config:din_logger	Change DIN Logger Settings

Parameter	Contents
show:device:dip_switch	DIP switch status indication
show:device:dms	DMS status display
execute:device:dms	DMS Control
show:config:dms	DMS setting display
update:config:dms	DMS setting control
execute:device:nxwitness	Nx Witness Control
show:device:nxwitness	Nx Witness Display
show:config:nxwitness	Nx Witness Settings Display
update:config:nxwitness	Nx Witness Setting Control
execute:device:nxwitness_save	Nx Witness Settings Write
execute:device:nxwitness_load	Nx Witness setting read
execute:firmware:snap_shot	FW snapshot generation
show:config:gui	GUI setting display
update:config:gui	GUI setting control
show:device:remoteit	remote.it status display
execute:device:remoteit	remote.it control
show:config:remoteit	remote.it setting display
update:config:remoteit	remote.it setting control
execute:device:application	Application Command Execution
show:config:dhcp_relay	DHCP relay setting display
append:config:dhcp_relay	Add DHCP relay settings
update:config:dhcp_relay	Change DHCP relay settings
delete:config:dhcp_relay	Delete DHCP relay setting
show:config:proxy	Proxy server setting display
update:config:proxy	Change proxy server settings
show:config:proxy_listen_port	Display of proxy server setting listening port number
update:config:proxy_listen_port	Change proxy server setting standby port number
show:device:WiFi_ap_status	Wireless LAN access point status display
show:device:WiFi_ap_connect	Wireless LAN access point connection status display
execute:device:WiFi_ap_connect	Wireless LAN access point connection control
show:device:WiFi_sta_status	Wireless LAN station status display
show:device:WiFi_sta_connect_select	Wireless LAN station switching control status display
execute:device:WiFi_sta_connect_select	Wireless LAN station switching control
execute:device:WiFi_wps	WPS Control
show:config:WiFi_ap	Wireless LAN access point setting display
append:config:WiFi_ap	Additional wireless LAN access point settings
update:config:WiFi_ap	Wireless LAN access point setting change
delete:config:WiFi_ap	Delete wireless LAN access point settings
show:config:WiFi_sta	Wireless LAN station setting display
append:config:WiFi_sta	Additional wireless LAN station configuration
update:config:WiFi_sta	Wireless LAN station configuration change
delete:config:WiFi_sta	Wireless LAN station settings deleted
show:config:WiFi_wps	WPS setting display

Parameter	Contents
update:config:WiFi_wps	Change WPS settings
show:config:simple_settings	<p>Simplified setting display</p> <p> This is the same as the following authorization.</p> <pre>show:config:mobile_peer show:config:interface show:config:apt_auth_hostname show:config:dms show:config:nxwitness show:config:remoteit</pre>
update:config:simple_settings	<p>Simple configuration update</p> <p> This is the same as the following authorization.</p> <pre>append:config:mobile_peer update:config:mobile_peer delete:config:mobile_peer append:config:interface update:config:interface delete:config:interface append:config:apt_auth_hostname update:config:apt_auth_hostname delete:config:apt_auth_hostname update:config:dms update:config:nxwitness update:config:remoteit</pre>
show:device:equipment_information	<p>Device Information Display</p> <p> This is the same as the following authorization.</p> <pre>show:device:information show:device:firmware show:device:boot show:device:mobile_module</pre>
show:device:storage	<p>Storage Information Display</p> <p> This is the same as the following authorization.</p> <pre>show:device:storage_partition show:device:storage_format show:device:storage_mount show:device:storage_usage</pre>
execute:device:storage	<p>Storage Control</p> <p> This is the same as the following authorization.</p> <pre>execute:device:storage_partition execute:device:storage_fsck execute:device:storage_format execute:device:storage_mount</pre>

Parameter	Contents
show:device:schedule	<p>Schedule display</p> <p> This is the same as the following authorization.</p> <pre>show:device:schedule_general_control show:device:schedule_keep_alive show:device:schedule_user_define</pre>
execute:firmware:package	<p>Firmware Package Differential Update</p> <p> This is the same as the following authorization.</p> <pre>execute:firmware:package_update execute:firmware:package_upgrade execute:firmware:package_clean</pre>
execute:firmware:area	<p>Whole firmware update</p> <p> This is the same as the following authorization.</p> <pre>execute:firmware:file_check execute:firmware:area_update execute:firmware:file_delete</pre>
execute:device:datetime	<p>Time setting</p> <p> This is the same as the following authorization.</p> <pre>execute:device:datetime_manual execute:device:datetime_ntpdate</pre>
execute:config:file_download	<p>Download control of the persistence configuration file</p>
execute:config:file_upload	<p>Upload control of persistence configuration files</p> <p> This is the same as the following authorization.</p> <pre>execute:config:file_save execute:device:reboot</pre>



This chapter describes the operation of the configuration file that saves the product's settings.

3.1 Initialize settings

Reset settings to factory defaults.



- The configuration file is not initialized by executing this command. Therefore, if this command is executed and then restarted without writing to the configuration file, the system will start up with the settings before the configuration was initialized.
- If you are using the normal Linux CLI, you can initialize the settings with the following command

```
sudo amcfg init
```



If you are using a Compact Router, the following restrictions apply
When initializing the settings of a device enabled in the device management system and connecting to the device management system again, please **deactivate the device from the device management system side** and re-enable it after the device is initialized.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# config initialize ↵
Do you want to initialize the settings?    ←Enter the "y" key followed by Enter
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:kCDYzetsJhvXc7L/+XPmLdQ7zsNnXCwdoBed2jMyYG0 root@amnimo (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:icLKggm53e6Dvpds61+d5n7ArOiZ12hM2nLet1/o08g root@amnimo (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:CtWGK0BNYxgYwuZsnADJ3QX50czqC3NlnBTsSypeQN4 root@amnimo (ED25519)
Would you like to save settings and reboot the system? (y/N): n ← Enter "y" and press E
nter, the device will reboot immediately after a new line.
Need to register for a new password.
Enter password for admin.
Enter new password:                ← Enter new password and press Enter
Retype new password:                ← Enter new password again and press Enter
passwd: password updated successfully.
```



To cancel execution of the command, type the "n" key followed by Enter.

3.2 Display a list of settings

Displays a list of settings in the current configuration file.

Execution example

管理者 モード

```
amnimo# show config ↵
# ---- transition to configure mode ----
configure
# ---- hostname configure ----
hostname amnimo
# ---- account amnimo configure ----
account amnimo
password secret ENCRYPT-ADMIN-PASSWORD
group admin
no auto-logout
no password-expires
exit
(Omitted.)
# ---- exit configure mode ----
exit
amnimo#
```

設定 モード

```
amnimo(cfg)# show config ↵
# ---- hostname configure ----
hostname amnimo
# ---- account amnimo configure ----
account amnimo
password secret ENCRYPT-ADMIN-PASSWORD
group admin
no auto-logout
no password-expires
exit
(Omitted.)
amnimo(cfg)#.
```

3.3 Display a list of configuration files

Displays the name of the configuration file and the last modified date of the file in RFC 3339 format.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# show config file ↵
startup-config 2020-01-02T00:00:00+09:00
backup-20200101 2020-01-01T00:00:00+09:00
backup-20200202 2020-01-02T00:00:00Z+09:00
```



The "startup-config" file is referenced at startup of the product.

3.4 Writing to the configuration file

Writes the configuration set by the command to the configuration file.

Format

```
config file save [FILENAME].
```

Setting items

Item	Contents
FILENAME	<p>Enter the name of the configuration file.</p> <ul style="list-style-type: none"> • A maximum file name of 32 characters can be set. • The characters that can be used as file names are "alphanumeric characters" (case-sensitive) and "-" (hyphen) (cannot be used at the beginning or end). <p> <ul style="list-style-type: none"> • Entering the "Tab" key completes the entry of the configuration file name "startup-config". • If you omit entering a configuration file name, "startup-config" will be set. </p>

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# config file save startup-config ↵
```



The Compact Router displays the progress of the write process.



```
amnimo# config file save startup-config ↵
rrrrrrrrrrwrrrrrrrrrrwrrrrrrrrw ←Progress indication
```



If you are using the normal Linux CLI, you can write your settings to a configuration file with the following command

```
sudo amcfg save [FILENAME].
```

3.5 Read the configuration file

Loads settings from a configuration file.

➔ For more information on the setting items, see "3.4 Writing to the configuration file" for information on setting items.

Format

```
config file load FILENAME
```

Setting items

Item	Contents
FILENAME	<p>Enter the name of the configuration file.</p> <ul style="list-style-type: none"> ● A maximum file name of 32 characters can be set. ● You can set the unreserved characters specified in RFC 1738. <div style="display: flex; align-items: flex-start;">  <ul style="list-style-type: none"> ● Entering the "Tab" key completes the entry of the configuration file name "startup-config". ● If you omit entering a configuration file name, "startup-config" will be set. </div>

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# config file load startup-config ↵
```



If you are using the normal Linux CLI, you can read the configuration file with the following command

```
sudo amcfg load [FILENAME].
```

3.6 Rename the configuration file

Rename the configuration file.

Format

```
config file move SRC-FILENAME DST-FILENAME
```

Setting items

Item	Contents
SRC-FILENAME	<p>Enter the name of the configuration file before the change.</p> <ul style="list-style-type: none"> ● The maximum number of characters is 32. ● You can set the unreserved characters specified in RFC 1738. <p> Entering the "Tab" key completes the entry of the configuration file name.</p>
DST-FILENAME	<p>Enter the name of the modified configuration file.</p> <ul style="list-style-type: none"> ● The maximum number of characters is 32. ● You can set the unreserved characters specified in RFC 1738. <p> Entering the "Tab" key completes the entry of the configuration file name.</p>

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# config file move backup-20200101 backup-20200101-2 ↵
```



- The name of the startup configuration file "startup-config" cannot be changed.
- If you are using the normal Linux CLI, you can rename the configuration file with the following command

```
sudo amcfg move SRC-FILENAME DST-FILENAME
```

3.7 Copy the configuration file

Copy the configuration file.

➔ For more information on the setting items, see " 3.6 Rename the configuration file "for more information about the setting items.

Format

```
config file copy SRC-FILENAME DST-FILENAME
```

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# config file copy startup-config startup-config_2 ↵
```



If you are using the normal Linux CLI, you can copy the configuration file with the following command

```
sudo amcfg copy SRC-FILENAME DST-FILENAME
```

3.8 Delete configuration files

Deletes a configuration file by specifying a file name.

➔ For more information on the setting items, see " 3.4 Writing to the configuration file" for information on setting items.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# no config file startup-config_2 ↵
```



If you are using the normal Linux CLI, you can delete the configuration file with the following command. However, the startup configuration file "startup-config" cannot be deleted.

```
sudo amcfg delete FILENAME
```

Chap 4. Storage Operations

This chapter describes general storage operations such as mounting, checking, and viewing usage of storage, as well as file operations.

4.1 View storage devices



To view storage device information, run the *show device storage* partition command.

Format

```
show device storage partition [PARTITION].
```

Setting items

Item	Contents
PARTITION	<p>Specify the name of the partition whose mount status you want to display.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> </div> <ul style="list-style-type: none"> Available partition names are mmcblk<1-9>p<1-9> and sd<a-z><1-9>. Only the usage of the specified PARTITION is displayed. If partitions mmcblk<1-9>p<1-9> and sd<a-z><1-9> exist under /dev, you can type "Tab" key to complete the partition name entry. If PARTITION is omitted, the status of mmcblk<1-9>p<1-9> and sd<a-z><1-9>* under /dev will be displayed. </div> <p style="margin-top: 10px;"> AI Edge Gateway will further increase the number of nvme0n1p<1-9> in the target. </p>

Output Format

```
# ---- DEVICE ----
- DISK-SIZE DISK-TYPE
NUMBER PARTITION-SIZE PARTITION-TYPE
(Omitted.)
# ---- DEVICE ----
- DISK-SIZE DISK-TYPE
NUMBER PARTITION-SIZE PARTITION-TYPE
```

Output item

Item	Contents
DEVICE	The storage device name is displayed. Storage device names are in the format mmcblk<1-9>* , sd<a-z> *
DISK-SIZE	The entire disk capacity is displayed in kilobytes.
DISK-TYPE	One of the following disk types will be displayed <ul style="list-style-type: none"> MBR GPT
NUMBER	Partition numbers from 1 to 9 are displayed.
PARTITION-SIZE	The partition capacity is displayed in kilobytes.

Item	Contents
PARTITION-TYPE	<p>The partition type is displayed. What is displayed depends on the disk type.</p> <p>For MBR</p> <ul style="list-style-type: none"> ● If the partition id is the following, "fat(partition id)" is displayed. 0x1, 0x4, 0x6, 0x7, 0xb, 0xc, 0xe, 0x11, 0x14, 0x16, 0x1b, 0x1c, 0x1e, 0x24, 0xbc, 0xc1, 0xc4, 0xc6, 0xe1, 0xe3, 0xef, 0xf2 Example: fat(0x1) ● If the partition id is the following, "linux(partition id)" will be displayed. 0x83 Example: linux(0x83) ● If other than the above partition id, "partition id" will be displayed. Example: 0x46 <p>For GPT</p> <ul style="list-style-type: none"> ● If the GUID is the following, "windows(GUID)" will be displayed. E3C9E316-0B5C-4DB8-817D-F92DF00215AE EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 5808C8AA-7E8F-42E0-85D2-E1E90434CFB3 AF9B60A0-1431-4F62-BC 68-3311714A69AD DE94BBA4-06D1-4D40-A16A-BFD50179D6AC 37AFFC90-EF7D-4E96-91C3-2D7AE055B174 E75CAF8F-F680-4CEE-AFA3-B001E56EFC2D 558D43C 5-a1ac-43c0-aac8-d1472b2923d1 Example: windows(5808C8AA-7E8F-42E0-85D2-E1E90434CFB3) ● If the partition id is the following, "linux(GUID)" will be displayed. 0FC63DAF-8483-4772-8E79-3D69D8477DE4 a19d880f-05fc-4d3b-a006-743f0f84911e 44479540-f297-41b2-9af7-d131d5f0458a 4f68bce3-e8cd-4db1-96e7-fbcaaf984b709 69dad710-2ce4-4e3c-b16c-21a1d49abed3 b921b045-1df0-41c3-af44-4c6f280d3fae bc13c2ff-59e6-4262-a352-b275fd6f7172 0657FD6D-A4AB-43C4-84E5-0933C84B4F4F e6d6d379-f507-44c2-a23c-238f2a3df928 933ac7e1-2eb4-4f13-b844-0e14e2aef915 3b8f8425-20e0-4f3b-907f-1a25a76f98e8 7ffec5c9-2d00-49b7-8941-3ea10a5586b7 ca7d7ccb-63ed-4c53-861c-1742536059cc 8da63339-0007-60c0-c436-083ac8230908 Example: linux(0FC63DAF-8483-4772-8E79-3D69D8477DE4) ● If other than the above PARTITION ID, "GUID" will be displayed. Example: 49F48D32-B10E-11DC-B99B-0019D1879648

* Only displayed if the device exists.

* AI Edge Gateway will further increase nvme0n1 to the target.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device storage partition ↵
# ---- sda ----
- 495104 MBR
1 39936 fat(0x0c)
2 39936 fat(0x0c)
3 39936 fat(0x0c)
4 39936 linux(0x83)
# ---- mmcblk1 ----
- 1955840 GPT
1 51200 linux(0FC63DAF-8483-4772-8E79-3D69D8477DE4)
2 51200 linux(0FC63DAF-8483-4772-8E79-3D69D8477DE4)
3 1852399 windows(EBD0A0A2-B9E5-44333-87C0-68B6B72699C7)
```

4.2 Configure storage partitions



Describes how to create and delete partitions on storage.

4.2.1 Create partitions

To create a partition, run the *device storage partition* command.

Format

```
device storage partition DEVICE NUMBER [type <linux | fat32>] [size SIZE]
```

Setting items

Item	Contents						
DEVICE	<p>Enter a device name.</p>  <ul style="list-style-type: none">Available device names are in the format mmcblk<1-9>, sd<a-z>.If the device exists, you can type "Tab" key to complete the device name entry.  AI Edge Gateway further increases nvme0n1 to the target.						
NUMBER	Specify a partition number in the range of 1 to 9.						
type	<p>Specify one of the following partition types</p> <table border="1"><thead><tr><th>Value</th><th>Description</th></tr></thead><tbody><tr><td>linux</td><td>This is a standard Linux partition type. (Default value)</td></tr><tr><td>fat32</td><td>FAT32 (LBA) partition type. If you are using Windows, you must select this option.</td></tr></tbody></table>	Value	Description	linux	This is a standard Linux partition type. (Default value)	fat32	FAT32 (LBA) partition type. If you are using Windows, you must select this option.
Value	Description						
linux	This is a standard Linux partition type. (Default value)						
fat32	FAT32 (LBA) partition type. If you are using Windows, you must select this option.						
size	<p>Enter the partition capacity in kilobytes in SIZE. If SIZE is omitted, the maximum value of the storage device is used.</p>  Partitioning requires at least 10 Mbytes of space.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# device storage partition mmcblk1 1 ↵  
amnimo# device storage partition mmcblk1 1 type fat32 ↵  
amnimo# device storage partition mmcblk1 1 type fat32 size 31166976 ↵  
amnimo# device storage partition mmcblk1 1 size 31166976 type fat32 ↵  
amnimo# device storage partition mmcblk1 1 size 31166976 ↵
```

4.2.2 Delete partitions

To remove a storage partition, execute the *no device storage partition* command.

Format

```
no device storage partition PARTITION
```

Setting items

Item	Contents
PARTITION	<p>Enter a partition name.</p> <ul style="list-style-type: none"> Available partition names are of the form mmcbk1-9>p<1-9>, sd<a-z><1-9>. If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p>AI Edge Gateway will further increase the number of nvme0n 1p<1-9> in the target.</p>

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# no device storage partition mmcbk1p1 ↵
```

4.3 Formatting Storage



To format a partition, run the *device storage format* command.

Format

```
device storage format PARTITION [type <ext4 | xfs | vfat>] [aes <256 | 512>]
```

Setting items

Item	Contents								
PARTITION	<p>Specify a partition name.</p> <p> Available partition names are mmcblk<1-9>p<1-9>, sd<a-z><1-9>.</p> <p> AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.</p>								
type	<p>Specifies the file system type.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ext4</td> <td>EXT4 file system (default value)</td> </tr> <tr> <td>xfs</td> <td>XFS file system</td> </tr> <tr> <td>vfat</td> <td> <p>VFAT file system</p> <p> The maximum partition size for VFAT is 2TByte. Please note that the 4 TByte SSD option is available for Edge Gateway Outdoor Type.</p> </td> </tr> </tbody> </table>	Value	Description	ext4	EXT4 file system (default value)	xfs	XFS file system	vfat	<p>VFAT file system</p> <p> The maximum partition size for VFAT is 2TByte. Please note that the 4 TByte SSD option is available for Edge Gateway Outdoor Type.</p>
Value	Description								
ext4	EXT4 file system (default value)								
xfs	XFS file system								
vfat	<p>VFAT file system</p> <p> The maximum partition size for VFAT is 2TByte. Please note that the 4 TByte SSD option is available for Edge Gateway Outdoor Type.</p>								
aes	<p>Specify if you want to encrypt partitions. Specify 256 or 512 as the key length (bit) to be used for encryption.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>256</td> <td>Use a 256-bit master key.</td> </tr> <tr> <td>512</td> <td>Use 512-bit master key.</td> </tr> </tbody> </table> <p> <ul style="list-style-type: none"> • If aes is specified, a password must be set when the command is executed. • A partition size of at least 100 MBytes is required. </p>	Value	Description	256	Use a 256-bit master key.	512	Use 512-bit master key.		
Value	Description								
256	Use a 256-bit master key.								
512	Use 512-bit master key.								

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# device storage format mmcblk1 aes 256 ↵
Enter password:                    ←Enter password and press Enter
Retype password:                  ←Enter the password again and press Enter
```

4.4 Display storage mount status



To view the storage mount status, run the *show device storage mount* command.

Format

```
show device storage mount [PARTITION].
```

Setting items

Item	Contents
PARTITION	<p>Specify the name of the partition whose mount status you want to display.</p> <ul style="list-style-type: none"> Available partition names are mmcbk<1-9>p<1-9>, sd<a-z><1-9>. Only the usage of the specified PARTITION is displayed. If partitions mmcbk<1-9>p<1-9> and sd<a-z><1-9> exist under /dev, you can type "Tab" key to complete the partition name entry. If PARTITION is omitted, the mount status of mmcbk<1-9>p<1-9> and sd<a-z><1-9> under /dev is displayed. <p>AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.</p>

Output Format

```
Partition Type MountPoint
PARTITION VFSTYPE POINT
(Omitted.)
```

Output item

Item	Contents								
PARTITION	The partition name is displayed.								
VFSTYPE	<p>The file system type is displayed.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ext4</td> <td>EXT4 file system</td> </tr> <tr> <td>xfs</td> <td>XFS file system</td> </tr> <tr> <td>vfat</td> <td>VFAT file system</td> </tr> </tbody> </table>	Value	Description	ext4	EXT4 file system	xfs	XFS file system	vfat	VFAT file system
Value	Description								
ext4	EXT4 file system								
xfs	XFS file system								
vfat	VFAT file system								
POINT	Mounting points are displayed.								

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザー モード
管理者 モード
設定 モード

```
amnimo$ show device storage mount ↵
Partition Type MountPoint
mmcbk1p1 ext4 /media/sdcard1
mmcbk1p2 vfat /media/sdcard2
mmcbk1p4 ext4 /media/sdcard4
```

4.5 Controlling the mount state of storage partitions



Describes how to mount and unmount storage partitions.



- The functions described in this section do not make the mount state permanent.
If you wish to make the mount state permanent, use the function in "4.9 Set up storage and save configuration information".

4.5.1 Mount partitions

To mount a storage partition, run the *device storage mount* command.

Format

```
device storage mount PARTITION [POINT [type <ext4 | xfs | vfat>] [options OPTIONS]]
```

Setting items

Item	Contents								
PARTITION	Specify a partition name.  <ul style="list-style-type: none">Available partition names are mmcblk<1-9>p<1-9>, sd<a-z><1-9>.If partitions mmcblk<1-9>p<1-9> and sd<a-z><1-9> exist under /dev, you can type "Tab" key to complete the partition name entry.  AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.								
POINT	Specify a mount point name with up to 32 alphanumeric characters.  <ul style="list-style-type: none">Absolute paths can be specified.For relative paths, the POINT directory is created in the current directory.								
type	Specifies the file system type. <table border="1"><thead><tr><th>Value</th><th>Description</th></tr></thead><tbody><tr><td>ext4</td><td>EXT4 file system (default value)</td></tr><tr><td>xfs</td><td>XFS file system</td></tr><tr><td>vfat</td><td>VFAT file system</td></tr></tbody></table>	Value	Description	ext4	EXT4 file system (default value)	xfs	XFS file system	vfat	VFAT file system
Value	Description								
ext4	EXT4 file system (default value)								
xfs	XFS file system								
vfat	VFAT file system								
options	Specify mount options. The default value is "defaults".								



- If POINT, type, or OPTIONS is omitted, the partition, if registered, will be mounted according to its settings. If the partition is not registered, an error will result.
- If PARTITION or POINT is already mounted, an error will result.
If PARTITION or POINT is registered in the configuration file but not mounted, it can be mounted.
- If the PARTITION is encrypted, it will be mounted after decryption.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# device storage mount mmcblk1p1 ↵  
amnimo# device storage mount mmcblk1p1 /media/sdcard1 ↵  
amnimo# device storage mount mmcblk1p1 /media/sdcard1 type ext4 ↵
```

```
amnimo# device storage mount mmcblk1p1 /media/sdcard1 type ext4 options defaults ↵
Enter password:          ↵ If the partition is encrypted, enter the password and press E
nter
```

4.5.2 Unmount partitions

To unmount a storage partition, execute the *no device storage mount* command.

Format

```
no device storage mount PARTITION
```

Setting items

Item	Contents
PARTITION	<p>Enter a partition name.</p> <ul style="list-style-type: none">Available partition names are of the form mmcblk<1-9>p<1-9>, sd<a-z><1-9>.If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p> AI Edge Gateway will further increase the number of nvme0n 1p<1-9> in the target.</p>

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# no device storage mount mmcblk1p1 ↵
```

4.6 Check storage



To check storage, run the *device storage fsck* command.

Format

```
device storage fsck PARTITION [type <ext4 | xfs | vfat>] [check | preen | customize CUS
TOMIZE]
```

Setting items

Item	Contents								
PARTITION	<p>Specify a partition name.</p> <ul style="list-style-type: none"> Available partition names are mmcblk<1-9>p<1-9>, sd<a-z><1-9>. If partitions mmcblk<1-9>p<1-9> and sd<a-z><1-9> exist under /dev, you can type "Tab" key to complete the partition name entry. <p> AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.</p>								
type	<p>Specifies the file system type.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ext4</td> <td>EXT4 file system (default value)</td> </tr> <tr> <td>xfs</td> <td>XFS file system</td> </tr> <tr> <td>vfat</td> <td>VFAT file system</td> </tr> </tbody> </table>	Value	Description	ext4	EXT4 file system (default value)	xfs	XFS file system	vfat	VFAT file system
Value	Description								
ext4	EXT4 file system (default value)								
xfs	XFS file system								
vfat	VFAT file system								
check	<p>Checks for bad sectors but does not repair errors.</p> <ul style="list-style-type: none"> The behavior is the same as when "-n" is specified as an option for the fsck or xfs_repair command. Supports input completion. 								
preen	<p>Repair minor errors. Set by default.</p> <ul style="list-style-type: none"> The behavior is the same as when "-y" is specified as an option to the fsck command. Supports input completion. 								
customize	<p>You can pass options to the fsck or xfs_repair command.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CUSTOMIZE</td> <td>Options for fsck or xfs_repair command</td> </tr> </tbody> </table> <p> Supports input completion.</p>	Value	Description	CUSTOMIZE	Options for fsck or xfs_repair command				
Value	Description								
CUSTOMIZE	Options for fsck or xfs_repair command								



- If the PARTITION is encrypted, it is decrypted using the password registered in the configuration file. If no password is registered in the settings file, the password must be entered.
- The output logs of fsck and xfs_repair are output to the CLI.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# device storage fsck mmcblk1p1 type ext4 check ↵
amnimo# device storage fsck mmcblk1p1 type ext4 preen ↵
amnimo# device storage fsck mmcblk1p1 type ext4 customize -y ↵
Enter password: Enter password          ← If the partition is encrypted and no password
is registered in the configuration file, enter the password and press Enter
```

4.7 Display storage usage



To view storage usage, run the *show device storage usage* command.

Format

```
show device storage usage [PARTITION].
```

Setting items

Item	Contents
PARTITION	<p>Specify the name of the partition whose usage you want to view.</p>  <ul style="list-style-type: none"> Available partition names are mmcbk<1-9>p<1-9>, sd<a-z><1-9>. If PARTITION is omitted, the storage usage of the mounted partition is displayed. In that case, mmcbk<1-9>p<1-9> and sd<a-z><1-9> under /dev will be displayed. If a PARTITION is specified, the usage status of only that PARTITION will be displayed. If partitions mmcbk<1-9>p<1-9> and sd<a-z><1-9> exist under /dev, you can type "Tab" key to complete the partition name entry.  AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.

Output Format

```
Partition Size Used Avail Use% MountPoint
PARTITION SIZE USED AVAIL PERCENT POINT
(Omitted.)
```

Output item

Item	Contents
PARTITION	The partition name is displayed.
SIZE	All capacities are displayed.
USED	The used capacity is displayed.
AVAIL	Free space is displayed.
PERCENT.	Usage rates are displayed.
POINT	Mounting points are displayed.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```
amnimo$ show device storage usage ↵
Partition Size Used Avail Use% MountPoint
mmcbk0p1 13g 637m 12g 6% /
mmcbk0p3 3.9G 20M 3.7G 1% /var/log
mmcbk1p2 7.0G 4.0K 7.0G 1% /media/sd2
mmcbk1p1 7.9G 36M 7.4G 1% /media/sdcard1
mmcbk1p4 4.9G 20M 4.6G 1% /media/sdcard4
```

4.8 View storage settings



To view the storage configuration, run the *show config storage* command.

Format

```
show config storage [PARTITION].
```

Setting items

Item	Contents
PARTITION	<p>Specify the name of the partition for which you want to view storage settings.</p>  <ul style="list-style-type: none"> Available partition names are mmcbk<1-9>p<1-9>, sd<a-z><1-9>. If PARTITION is omitted, the storage usage of the mounted partition is displayed. In that case, mmcbk<1-9>p<1-9> and sd<a-z><1-9> under /dev will be displayed. If a PARTITION is specified, setting information for that PARTITION only will be displayed. If partitions mmcbk<1-9>p<1-9> and sd<a-z><1-9> exist under /dev, you can type "Tab" key to complete the partition name entry.  AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.

Output Format

```
storage mount PARTITION POINT type VFSTYPE options OPTIONS CRYPT
FSCK PARTITION OPTIONS
MONITOR PARTITION INTERVAL
FAILSAFE PARTITION RETRY INTERVAL2 REBOOT
```

Output item

Item	Contents								
PARTITION	The partition name is displayed.								
POINT	Mounting points are displayed.								
VFSTYPE	<p>The file system type is displayed.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ext4</td> <td>EXT4 file system</td> </tr> <tr> <td>xfs</td> <td>XFS file system</td> </tr> <tr> <td>vfat</td> <td>VFAT file system</td> </tr> </tbody> </table>	Value	Description	ext4	EXT4 file system	xfs	XFS file system	vfat	VFAT file system
Value	Description								
ext4	EXT4 file system								
xfs	XFS file system								
vfat	VFAT file system								
CRYPT	<p>This information is displayed when storage is encrypted.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The "crypt secret {encrypted password}" will be displayed.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The "crypt secret {encrypted password}" will be displayed.	Disable	Not displayed.		
Setting	Display								
Enable	The "crypt secret {encrypted password}" will be displayed.								
Disable	Not displayed.								
FSCK	<p>Information is displayed when fsck is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "storage fsck" appears.</td> </tr> <tr> <td>Disable</td> <td>The message "no storage fsck" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "storage fsck" appears.	Disable	The message "no storage fsck" is displayed.		
Setting	Display								
Enable	The message "storage fsck" appears.								
Disable	The message "no storage fsck" is displayed.								

Item	Contents
OPTIONS	The fsck option settings are displayed.
	FCK setting Display
	Enable Option values are displayed. Disable Not displayed.
MONITOR	Information is displayed when the read/write monitor function is enabled/disabled.
	Setting Display
	Enable The message "storage monitor" appears. Disable The message "no storage monitor" appears.
INTERVAL	The interval between read/write checks is displayed.
	MONITOR settings Display
	Enable The message "interval {interval between checks}" is displayed. Disable Not displayed.
FAILSAFE	Displays information on when the fail-safe feature is enabled/disabled. If the node value does not exist, the default value "true" is used.
	Setting Display
	Enable The message "storage failsafe" is displayed. Disable The message "no storage failsafe" is displayed.
RETRY	The maximum number of retries when fsck/mount/read/write fails is displayed.
	FAILSAFE setting Display
	Enable The message "retry {max retry count}" is displayed. Disable Not displayed.
INTERVAL2	Displays the retry interval after a failed fsck/mount.
	FAILSAFE setting Display
	Enable The message "interval {retry interval}" is displayed. Disable Not displayed.
REBOOT	The maximum number of reboots when fsck/mount/read/write fails is displayed.
	FAILSAFE setting Display
	Enable The message "reboot {maximum reboot count}" is displayed. Disable Not displayed.

Execution example 1

The following is an example of execution when fsck, monitor function, and fail-safe function are enabled.

管理者 モード 設定 モード

```
amnimo(cfg)# show config storage ↵
# ---- storage mmcblk1p1 configure ----
storage mount mmcblk1p1 /media/sdcard1 type ext4 options defaults
storage fsck mmcblk1p1 preen
storage monitor mmcblk1p1 interval 10m
storage failsafe mmcblk1p1 retry 3 interval 10 reboot 3
```

Execution example 2

An example run with storage encryption, fsck, monitor and failsafe functions disabled is shown below.

管理者 モード 設定 モード

```
amnimo(cfg)# show config storage ↵
# ---- storage mmcblk1p1 configure ----
storage mount mmcblk1p1 /media/sdcard1 type ext4 options defaults
no storage fsck mmcblk1p1
no storage monitor mmcblk1p1
no storage failsafe mmcblk1p1
```

Execution example 3

An example run with storage encryption, fsck, monitor and failsafe functions enabled is shown below.

管理者 モード 設定 モード

```
amnimo(cfg)# show config storage ↵
# ---- storage mmcblk1p1 configure ----
storage mount mmcblk1p1 /media/sdcard1 type ext4 options defaults crypt secret TMrOPL0
CE+4FWZ1B1nwIoQ==
storage fsck mmcblk1p1 preen
storage monitor mmcblk1p1 interval 10m
storage failsafe mmcblk1p1 retry 3 interval 10 reboot 3
```

4.9 Set up storage and save configuration information



Configure settings for storage mount/unmount, file system inspection/repair, storage read/write check, fsck/mount, etc. The settings made here are written to a configuration file.

4.9.1 Configure storage mount settings.

To configure storage mount settings, run the storage mount command.



This setting can be registered for up to 5 cases.

Format

```
storage mount PARTITION POINT [type <ext4 | xfs | vfat>] [options OPTIONS] [crypt [secret ENCRYPT-PASSWORD]]
```

Setting items

Item	Contents
PARTITION	Specify a partition name. <ul style="list-style-type: none"> Available partition names are of the form mmcblk<1-9>p<1-9>, sd<a-z><1-9>. If a partition exists, you can type "Tab" key to complete the entry of the partition name.  AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.
POINT	Specifies a mount point.
type	Specifies the file system type. The default value is "ext4".
options	Specify mount options in OPTIONS. The default value is "defaults".
crypt	Specify if mounting on an encrypted partition.
secret	Specify an encrypted password string for ENCRYPT-PASSWORD.  If crypt is specified and secret is not specified, "Enter password:" will be displayed and you will be prompted for the password to encrypt the partition.

Execution example 1

The following is an example of execution when crypt is specified.

設定 モード

```
amnimo(cfg)# storage mount mmcblk1p1 /media/sdcard1 crypt ↵
Enter password:      ← Enter the encryption password for the partition and press Enter
```

Execution example 2

The following is an example of execution when crypt and secret are specified.

設定 モード

```
amnimo(cfg)# storage mount mmcblk1p1 /media/sdcard1 type ext4 options defaults crypt secret TMrOPL0CE+4FWZ1B1nwIoQ== ↵
```

4.9.2 Configure storage unmounting settings.

To configure the storage unmount settings, execute the *no storage mount* command.

Format

```
no storage mount PARTITION
```

Setting items

Item	Contents
PARTITION	<p>Specify a partition name.</p> <ul style="list-style-type: none"> Available partition names are of the form <code>mmcblk<1-9>p<1-9></code>, <code>sd<a-z><1-9></code>. If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p>AI Edge Gateway will further increase the number of <code>nvme0n1 p<1-9></code> in the target.</p>

Execution example

設定 モード

```
amnimo(cfg)# no storage mount mmcblk1p1 ↵
```

4.9.3 Inspect/repair the file system

To enable the file system inspection/repair function, run the *storage fsck* command.

Format

```
storage fsck PARTITION [check | preen | customize CUSTOMIZE].
```

Setting items

Item	Contents
PARTITION	<p>Specify a partition name.</p> <ul style="list-style-type: none"> Available partition names are of the form <code>mmcblk<1-9>p<1-9></code>, <code>sd<a-z><1-9></code>. If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p>AI Edge Gateway will further increase the number of <code>nvme0n1 p<1-9></code> in the target.</p>
check	Checks for bad sectors but does not repair errors.
preen	Repair minor errors. (Set by default.)
customize	Specifies options to pass to the <code>fsck</code> command (or the <code>xfs_repair</code> command if the file system is <code>xfs</code>).

Execution example

Enable the inspect/repair function for partition `/dev/mmcblk1p1` in configuration mode.

設定 モード

```
amnimo(cfg)# storage fsck mmcblk1p1 preen ↵
```

4.9.4 Disable the ability to inspect/repair the file system

To disable the ability to inspect/repair the file system, run the *no storage fsck* command.

Format

```
no storage fsck PARTITION
```

Setting items

Item	Contents
PARTITION	<p>Specify a partition name.</p> <ul style="list-style-type: none"> Available partition names are of the form <code>mmcblk<1-9>p<1-9></code>, <code>sd<a-z><1-9></code>. If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p>AI Edge Gateway will further increase the number of <code>nvme0n1 p<1-9></code> in the target.</p>

Execution example

Disable the inspect/repair function for partition `/dev/mmcblk1p1` in configuration mode.

設定モード

```
amnimo(cfg)# no storage fsck mmcblk1p1 ←
```

4.9.5 Periodically check storage read/write status

To periodically check the storage read/write status, run the *storage monitor* command.

Format

```
storage monitor PARTITION [interval TIME].
```

Setting items

Item	Contents
PARTITION	<p>Specify a partition name.</p> <ul style="list-style-type: none"> Available partition names are of the form <code>mmcblk<1-9>p<1-9></code>, <code>sd<a-z><1-9></code>. If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p>AI Edge Gateway will further increase the number of <code>nvme0n1 p<1-9></code> in the target.</p>
interval	<p>Specify in TIME the interval between retries when a read/write check fails.</p> <ul style="list-style-type: none"> The unit of measure can be specified as w (week), d (day), h (hour), or m (minute). A range from 1 minute (1m) to 2 weeks (2w) can be specified in any of the above units.

Execution example

In configuration mode, set the check interval for partition `/dev/mmcblk1p1` to 10 minutes.

設定モード

```
amnimo(cfg)# storage monitor mmcblk1p1 interval 10m ←
```

4.9.6 Disable periodic checks of storage read/write status

To disable the ability to periodically check the storage read/write status, execute the *no storage monitor* command.

Format

```
no storage monitor PARTITION
```

Setting items

Item	Contents
PARTITION	<p>Specify a partition name.</p> <ul style="list-style-type: none"> Available partition names are of the form mmcbk<1-9>p<1-9>, sd<a-z><1-9>. If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p> AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.</p>

Execution example

設定 モード

```
amnimo(cfg)# no storage monitor mmcbk1p1 ↵
```

4.9.7 Handle fail-safe in case of fsck/mount/read/write process failure

To handle fail-safe (retry and reboot) when the fsck/mount process fails, run the **storage failsafe** command.

➔ For more information on fail-safe features, see "12.3 fail-safe".

Format

```
storage failsafe PARTITION [retry COUNT] [interval TIME] [reboot COUNT]
```

Setting items

Item	Contents
PARTITION	Specify a partition name. <ul style="list-style-type: none"> Available partition names are of the form mmcblk<1-9>p<1-9>, sd<a-z><1-9>. If a partition exists, you can type "Tab" key to complete the entry of the partition name.  AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.
retry	Specify the maximum number of retries when fsck/mount/read/write process fails in COUNT. The default value is "10".
interval	Specify the retry interval (in seconds) when the fsck/mount process fails in TIME. The default value is "3".
reboot	Specify the maximum number of reboots when fsck/mount/read/write process fails in COUNT. The default value is "3".

Execution example

In configuration mode, set the failsafe function for /dev/mmcblk1p1 with 3 retries, 10 seconds between retries, and a maximum reboot count of 3 times.

設定 モード

```
amnimo(cfg)# storage failsafe mmcblk1p1 retry 3 interval 10 reboot 3 ↵
```

4.9.8 Disable fail-safe handling of fsck/mount/read/write process failures

To disable fail-safe handling when the storage fsck/mount process fails, execute the *no storage monitor* command.

Format

```
no storage failsafe PARTITION
```

Setting items

Item	Contents
PARTITION	<p>Specify a partition name.</p> <ul style="list-style-type: none"> Available partition names are of the form mmcblk<1-9>p<1-9>, sd<a-z><1-9>. If a partition exists, you can type "Tab" key to complete the entry of the partition name. <p>AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.</p>

Execution example

設定 モード

```
no storage failsafe mmcblk1p1 ↵
```

4.9.9 Display storage formatting information

To display storage format information, run the ***show device storage format*** command with the partition name as an argument. If no argument is specified, information for all partitions will be displayed.

Format

```
show device storage format PARTITION
```

Setting items

Item	Contents
PARTITION	Specify a partition name. <ul style="list-style-type: none"> Available partition names are of the form mmcblk<1-9>p<1-9>, sd<a-z><1-9>. If a partition exists, you can type "Tab" key to complete the entry of the partition name.  AI Edge Gateway will further increase the number of nvme0n1 p<1-9> in the target.

Output Format

```
Partition Type Crypt
PARTITION TYPE CRYPT
(Omitted.)
```

Output item

Item	Contents										
PARTITION	The partition name is displayed.										
TYPE	The file system type is displayed. <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>-</td> <td>Indicates either of the following states <ul style="list-style-type: none"> Encrypted and unmounted Unformatted state </td> </tr> <tr> <td>ext4</td> <td>EXT4 file system</td> </tr> <tr> <td>xfs</td> <td>XFS file system</td> </tr> <tr> <td>vfat</td> <td>VFAT file system</td> </tr> </tbody> </table>	Value	Description	-	Indicates either of the following states <ul style="list-style-type: none"> Encrypted and unmounted Unformatted state 	ext4	EXT4 file system	xfs	XFS file system	vfat	VFAT file system
Value	Description										
-	Indicates either of the following states <ul style="list-style-type: none"> Encrypted and unmounted Unformatted state 										
ext4	EXT4 file system										
xfs	XFS file system										
vfat	VFAT file system										
CRYPT	The encryption status of the partition is displayed. <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Disable</td> <td>unencrypted state</td> </tr> <tr> <td>Enable</td> <td>encrypted state</td> </tr> </tbody> </table>	Value	Description	Disable	unencrypted state	Enable	encrypted state				
Value	Description										
Disable	unencrypted state										
Enable	encrypted state										

Execution example

Displays formatting information for /dev/sda1 formatted in unencrypted ext4 in user mode.

ユーザーモード
管理者モード
設定モード

```
ag10-sy3$ show device storage format sda1 ↵
Partition Type Crypt
sda1 ext4 Disable
```

4.10 File Operations



Lists, moves, copies, and deletes files.



This function is not available on Compact Router.

4.10.1 List files

To list files, run the *show file* command.

Format

```
show file [PATH].
```

Setting items

Item	Contents
PATH	Files in the directory specified in the PATH are listed.  If PATH is omitted, files in the logged-in user's home directory are listed.

Output Format

```
PERMISSION OWNER GROUP SIZE TIMESTAMP FILENAME
```

Output item

Item	Contents
PERMISSION	File permissions are displayed.  The format is the same as when the "ls -l" command is executed.
OWNER	The name of the owner of the file is displayed.
GROUP	The group name of the file is displayed.
SIZE	The file size (in bytes) is displayed.
TIMESTAMP	The time the file was modified (local time) is displayed in RFC 3339 format.
FILENAME	The file name is displayed.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# show file /etc/amnimo/config.yaml ↵ ←If file name is specified in PATH
-rw-r--r-- root root 8325 2020-01-01T00:00:00Z config.yaml
amnimo# show file /etc/amnimo ↵ ←If you specify a directory in PATH
-rw-r--r-- root root 762 2020-01-01T00:00:00Z amenv.conf
-rw-r--r-- root root 265 2020-01-01T00:00:00Z archive.list
-rw-r--r-- root root 8325 2020-01-01T00:00:00Z config.yaml
drwxr-xr-x root root root 4096 2020-01-01T00:00:00Z default
-rwxr-xr-x root root 861 2020-01-01T00:00:00Z encrypt
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z if-configured.d
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z if-configuring.d
```

```

drwxr-xr-x root root 4096 2020-01-01T00:00:00Z if-down.d
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z if-post-down.d
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z if-post-up.d
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z if-up.d
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z service
-rwxr-xr-x root root root 243 2020-01-01T00:00:00Z uvol-detection
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z uvol-detection.d
-rwxr-xr-x root root root 242 2020-01-01T00:00:00Z uvol-recovery
drwxr-xr-x root root 4096 2020-01-01T00:00:00Z uvol-recovery.d

```

4.10.2 Move a file

To move a file, execute the *file move* command.

Format

```
file move SRC-FILENAME DST-FILENAME
```

Setting items

Item	Contents
SRC-FILENAME	Specify the name of the file to be moved from.  Entering the "Tab" key completes the entry of the configuration file name.
DST-FILENAME	Specify the name of the file to be moved.  Entering the "Tab" key completes the entry of the configuration file name.



- The same file name cannot be specified for SRC-FILENAME and DST-FILENAME.
- Directories cannot be specified for SRC-FILENAME and DST-FILENAME.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# file move /etc/amnimo/config.yaml.backup /etc/amnimo/config.yaml.backup2 ↵
```

4.10.3 Copy files

To copy a file, execute the *file copy* command.

Format

```
file copy <config | SRC-FILENAME> <config | DST-FILENAME>
```

Setting items

Item	Contents
config	The "/etc/amnimo/config.yaml" is set.
SRC-FILENAME	Specify the name of the file to be moved from.  Entering the "Tab" key completes the entry of the configuration file name.
DST-FILENAME	Specify the name of the file to be moved.  Entering the "Tab" key completes the entry of the configuration file name.



- The same file name cannot be specified for SRC-FILENAME and DST-FILENAME.
- Directories cannot be specified for SRC-FILENAME and DST-FILENAME.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# file copy config /etc/amnimo/config.yaml.backup ↵
```

4.10.4 Delete a file

To delete a file, execute the *no file* command.

Format

```
no file <PATH>.
```

Setting items

Item	Contents
PATH	Specify the file to be deleted in the PATH.



PATH cannot specify a directory.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# no file /etc/amnimo/config.yaml.backup2 ↵
```



This chapter controls the mobile module's power supply, displays communication status, manually connects and disconnects, and configures the mobile line.

5.1 View the mobile module

To view the mobile module, run the *show device mobile* command.

Format

```
show device mobile [module MODULE-NUMBER] [sim [SIM-NUMBER]]
```

Setting items

Item	Contents
module	Specify the mobile module number in <i>MODULE-NUMBER</i> .  This is valid when multiple mobile modules are installed.
simulation	Specify the SIM slot number (SIM: Subscriber identity module: contract information recording module) in <i>SIM-NUMBER</i> .

Output Format

```
# ---- module MODULE-NUMBER ----
manufacturer  MANUFACTURER
MODEL        model
fw_version    FW_VERSION
imei         IMEI
# ---- sim sim-number ----
PIN-STATUS   PIN-STATUS
iccid        ICCID
IMSI         IMSI
MSISDN
```

Output item

Item	Contents								
MODULE-NUMBER	The mobile module number is displayed.								
SIM-NUMBER	The SIM slot number is displayed.								
MANUFACTURER	The name of the mobile module manufacturer is displayed.								
model	The model name of the mobile module is displayed.								
FW_VERSION	Displays the firmware version of the mobile module.								
IMEI	The IMEI of the mobile module is displayed.								
PIN-STATUS	The SIM or eSIM PIN code status is displayed.								
	<table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>READY</td> <td> <ul style="list-style-type: none"> ● SIM-enabled state PIN lock disabled or PIN lock unlocked </td> </tr> <tr> <td>SIM PIN</td> <td> <ul style="list-style-type: none"> ● PIN code-aware state waiting state for PIN unlock </td> </tr> <tr> <td>SIM PUK</td> <td> <ul style="list-style-type: none"> ● PUK code standby state PIN code input incorrectly entered a certain number of times and locked. </td> </tr> </tbody> </table>	Display	Contents	READY	<ul style="list-style-type: none"> ● SIM-enabled state PIN lock disabled or PIN lock unlocked 	SIM PIN	<ul style="list-style-type: none"> ● PIN code-aware state waiting state for PIN unlock 	SIM PUK	<ul style="list-style-type: none"> ● PUK code standby state PIN code input incorrectly entered a certain number of times and locked.
	Display	Contents							
	READY	<ul style="list-style-type: none"> ● SIM-enabled state PIN lock disabled or PIN lock unlocked 							
SIM PIN	<ul style="list-style-type: none"> ● PIN code-aware state waiting state for PIN unlock 								
SIM PUK	<ul style="list-style-type: none"> ● PUK code standby state PIN code input incorrectly entered a certain number of times and locked. 								
ICCID	The ICCID (IC Card Identifier: Individual Identification Number) of the SIM or eSIM is displayed.								
IMSI	The IMSI (International Mobile Subscriber Identity: Subscriber Identification Number) of the SIM or eSIM is displayed.								
MSISDN	If MSISDN (Mobile Subscriber ISDNNumber: phone number) is set in the SIM or eSIM, "msisdn MSISDN" will be displayed. MSISDN may not be set depending on the contract.								



The SIM information displayed by this function may not be up to date. Please check the latest SIM information after updating the SIM information.

➔ " 5.2.3 Update SIM information "

Execution example

Execution example 1

The input and output of the commands in Execution Examples 1 through 5 are the same in all modes. The following is an example of execution in General User mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device mobile ↵
# ---- module 0 ----
manufacturer  GOSUNCN
model          ME3630-J2A
fw_version     ME3630J2AV1.0B18 [Sep 15 2018 17:04:51].
imei          123456789012345
# ---- module 0 sim 0 ----
iccid         1122334455667788990
imsi          998877665544332
msisdn        07012345678
# ---- module 0 sim 1 ----
iccid         1122334455667788990
imsi          998877665544332
msisdn        07012345678
```

Execution example 2

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device mobile module 0 ↵
# ---- module 0 ----
manufacturer  GOSUNCN
model          ME3630-J2A
fw_version     ME3630J2AV1.0B18 [Sep 15 2018 17:04:51].
imei          123456789012345
# ---- module 0 sim 0 ----
iccid         1122334455667788990
imsi          998877665544332
msisdn        07012345678
# ---- module 0 sim 1 ----
iccid         1122334455667788990
imsi          998877665544332
msisdn        07012345678
```

Execution example 3

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device mobile sim ↵
# ---- module 0 sim 0 ----
iccid         1122334455667788990
imsi          998877665544332
msisdn        07012345678
# ---- module 0 sim 1 ----
iccid         1122334455667788990
imsi          998877665544332
msisdn        07012345678
```

Execution example 4

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device mobile module 0 sim ↵
# ---- module 0 sim 0 ----
iccid          1122334455667788990
imsi           998877665544332
msisdn         07012345678
# ---- module 0 sim 1 ----
iccid          1122334455667788990
imsi           998877665544332
msisdn         07012345678
amnimo$ show device mobile sim module 0 ↵
(same output as above)
```

Execution Example 5

ユーザーモード 管理者モード 設定モード

```
amnimo$ show device mobile module 0 sim 0 ↵
# ---- module 0 sim 0 ----
iccid          1122334455667788990
imsi           998877665544332
msisdn         07012345678
amnimo$ show device mobile sim 0 module 0 ↵
(same output as above)
```

5.2 Controlling the mobile module

Turns mobile module power on/off, resets, and updates SIM information.

5.2.1 Turn on the power to the mobile module



To turn on power to the mobile module, execute the *device mobile power* command.

Format

```
device mobile power module <MODULE-NUMBER>.
```

Setting items

Item	Contents
MODULE-NUMBER	Specify the mobile module number and turn on the power.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# device mobile power module 0 ← turn on mobile module 0
```

5.2.2 Reset the power supply of the mobile module



To reset the power to the mobile module, run the *device mobile reset* command with the reset option.

Format

```
device mobile reset module <MODULE-NUMBER>.
```

Setting items

Item	Contents
MODULE-NUMBER	Reset the power supply by specifying the number of the mobile module.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# device mobile reset module 0 ← reset mobile module 0
```

5.2.3 Update SIM information

To update the SIM information, run the *device mobile information* command.

Format

```
device mobile information module <MODULE-NUMBER>
```

Setting items

Item	Contents
module	Update the SIM information by specifying the mobile module number in MODULE-NUMBER.

Execution example

Command input and output are the same in administrator mode and configuration mode. Below is an example of administrator mode execution when a SIM is inserted in both sim0 and sim1.

管理者 モード 設定 モード

```
amnimo# device mobile information module 0 → update all sim information in mobile module 0
# ---- module 0 sim 0 ----
PIN          READY
iccid        1122334455667788990
imsi         998877665544332
msisdn       07012345678
# ---- module 0 sim 1 ----
PIN          READY
iccid        2122334455667788990
imsi         898877665544332
msisdn       08098761234
```

5.2.4 Turn off the mobile module

To turn off the mobile module, execute the *no device mobile power* command.

Format

```
no device mobile power module <MODULE-NUMBER>.
```

Setting items

Item	Contents
MODULE-NUMBER	Specify the mobile module number in MODULE-NUMBER to turn off the mobile module.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# no device mobile power module 0 ← turn off mobile module 0
```

5.2.5 Check PIN setting status

To check the status of the PIN (Personal Identification Number) setting, execute the *device mobile pin status* command.



This command is not available when the mobile module interface (ecm0) is enabled.

Format

```
device mobile pin status module <MODULE-NUMBER> sim <SIM-NUMBER>
```

Setting items

Item	Contents
MODULE-NUMBER	Specify the number of the target mobile module.
SIM-NUMBER	Specify the number of the SIM connected to the target mobile module.

Output

Item	Contents
READY: MT is not pending for any password	PIN lock disabled or PIN lock unlocked
SIM PUK: MT is waiting phone-to-very first SIM/UICC card password to be given	PIN code input incorrectly entered a certain number of times and locked.
SIM PIN: MT is waiting SIM PIN to be given	waiting state for PIN unlock

Execution example

With the mobile module interface ecm0 disabled, check the PIN setting status of SIM0 and SIM1 on mobile module 0. Command input and output are the same in administrator mode and configuration mode. An example of execution in administrator mode is shown below.

管理者モード 設定モード

```
amnimo# device mobile pin status module 0 sim 0 ↵
READY: MT is not pending for any password ← PIN lock is disabled or PIN lock is unlocked
amnimo# device mobile pin status module 0 sim 1 ↵
SIM PUK: MT is waiting phone-to-very first SIM/UICC card password to be given ← PIN cod
e input wrongly entered a certain number of times, locked
```

5.2.6 Unlock the SIM card

To unlock the SIM card lock, execute the *device mobile pin unlock* command.



Please contact the carrier that issued your SIM for the PIN code.

Format

```
device mobile pin unlock <PIN-CODE> module <MODULE-NUMBER> sim <SIM-NUMBER>
```

Setting items

Item	Contents
PIN-CODE	Specify the PIN code.
MODULE-NUMBER	Specify the number of the target mobile module.
SIM-NUMBER	Specify the number of the SIM connected to the target mobile module.

Execution example

Unlock the SIM card lock on SIM0 of mobile module 0 by entering the PIN code. Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

Setting items	Configuration details
PIN code	1234

管理者 モード 設定 モード

```
amnimo# device mobile pin unlock 1234 module 0 sim 0 ↵
```

5.2.7 Enable PIN code

To enable the PIN code, execute the *device mobile pin enable* command.



Please contact the carrier that issued your SIM for the PIN code.

Format

```
device mobile pin enable <PIN-CODE> module <MODULE-NUMBER> sim <SIM-NUMBER>
```

Setting items

Item	Contents
PIN-CODE	Specify the PIN code.
MODULE-NUMBER	Specify the number of the target mobile module.
SIM-NUMBER	Specify the number of the SIM connected to the target mobile module.

Execution example

Enables the SIM0 PIN code for mobile module 0. Command input and output are the same in administrator mode and configuration mode. Below is an example of administrator mode execution.

Setting items	Configuration details
PIN code	1234

管理者 モード 設定 モード

```
amnimo# device mobile pin enable 1234 module 0 sim 0 ↵
```

5.2.8 Disable PIN code

To disable the PIN code, execute the *device mobile pin disable* command.



Please contact the carrier that issued your SIM for the PIN code.

Format

```
device mobile pin disable <PIN-CODE> module <MODULE-NUMBER> sim <SIM-NUMBER>
```

Setting items

Item	Contents
PIN-CODE	Specify the PIN code.
MODULE-NUMBER	Specify the number of the target mobile module.
SIM-NUMBER	Specify the number of the SIM connected to the target mobile module.

Execution example

Disables the SIM0 PIN code on mobile module 0. Command input and output are the same in administrator mode and configuration mode. Below is an example of administrator mode execution.

Setting items	Configuration details
PIN code	1234

管理者 モード 設定 モード

```
amnimo# device mobile pin disable 1234 module 0 sim 0 ↵
```

5.2.9 Change PIN code

To change the PIN code, execute the *device mobile pin change* command.



Please contact the carrier that issued your SIM for the PIN code.

Format

```
device mobile pin change <OLD-PIN-CODE> <NEW-PIN-CODE> module <MODULE-NUMBER> sim <SIM-NUMBER>
```

Setting items

Item	Contents
OLD-PIN-CODE	Specifies the current PIN code.
NEW-PIN-CODE	Specify a new PIN code to be set.
MODULE-NUMBER	Specify the number of the target mobile module.
SIM-NUMBER	Specify the number of the SIM connected to the target mobile module.

Execution example

Change the SIM0 PIN code of mobile module 0 from 1234 to 9876. Command input and output are the same in administrator mode and configuration mode. An example of execution in administrator mode is shown below.

Setting items	Configuration details
current PIN code	1234
new PIN code	9876

管理者 モード 設定 モード

```
amnimo# device mobile pin change 1234 9876 module 0 sim 0 ↵
```

5.2.10 Unlock PIN by PUK code

To unlock the PIN lock by PUK (Personal Unblocking Key) code, execute the *device mobile puk* command.



Please contact the carrier that issued your SIM for the PIN code/PUK code.



If you fail to enter the PUK code a certain number of times, your SIM card will become unusable and may need to be reissued. Please note that a reissue fee may be incurred.

Format

```
device mobile puk <PUK-CODE> <PIN-CODE> module <MODULE-NUMBER> sim <SIM-NUMBER>
```

Setting items

Item	Contents
PUK-CODE	Specify the PUK code.
PIN-CODE	Specify a new PIN code to be set.
MODULE-NUMBER	Specify the number of the target mobile module.
SIM-NUMBER	Specify the number of the SIM connected to the target mobile module.

Execution example

The PIN lock status is released by the PUK code of SIM0 of mobile module 0. Command input and output are the same in administrator mode and configuration mode. An example of execution in administrator mode is shown below.

Setting items	Configuration details
PUK Code	12345678
new PIN code	9876

管理者 モード 設定 モード

```
amnimo# device mobile puk 12345678 9876 module 0 sim 0 ↵
```

5.3 Display the communication status of the mobile line

To display the communication status of the mobile line, run the *show mobile* command.

Format

```
show mobile [IFNAME].
```

Setting items

Item	Contents
IFNAME	Specifies the interface name.  If IFNAME is omitted, information on all interfaces configured for mobile will be displayed.

Output Format

```
# ---- mobile IFNAME ----
number      MODULE-NUMBER
module      MODULE-NAME
peer        MOB-PEER-NAME
session     SESSION-NAME
sim         SIM-NUMBER
apn         APN
state       STATE
rat         RAT
ARFCN
UARFCN
EARFCN
band        BAND
mcc         MCC
mnc         MNC
TAC
cellid      CELLID
LAC
PCI
PSC
BSIC
rssi        RSSI
RSCP
RSRP
RSRQ
SINR
ecio        ECIO
```

Output item

Item	Contents																
IFNAME	The interface name is displayed.																
MODULE-NUMBER	The mobile module number is displayed.																
MODULE-NAME	The mobile module name is displayed.																
MOB-PEER-NAME	The name of the mobile module setting is displayed.																
SESSION-NAME	The mobile session name will be displayed.																
SIM-NUMBER	The SIM slot number is displayed.																
APN	The APN (Access Point Name) is displayed.																
STATE	The status of the mobile module is displayed. <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>dialing</td> <td>during the connection process</td> </tr> <tr> <td>connected</td> <td>state of connectivity</td> </tr> <tr> <td>disconnected</td> <td>disconnected state</td> </tr> </tbody> </table>	Value	Description	dialing	during the connection process	connected	state of connectivity	disconnected	disconnected state								
Value	Description																
dialing	during the connection process																
connected	state of connectivity																
disconnected	disconnected state																
RAT	The connection RAT (Radio Access Technology, mobile communication line) is displayed. <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>GPRS</td> <td>2G</td> </tr> <tr> <td>EDGE</td> <td>2G</td> </tr> <tr> <td>WCDMA</td> <td>3G</td> </tr> <tr> <td>HSDPA</td> <td>3G</td> </tr> <tr> <td>HSUPA</td> <td>3G</td> </tr> <tr> <td>HSDPA-HSUPA</td> <td>3G</td> </tr> <tr> <td>E-UTRAN</td> <td>4G</td> </tr> </tbody> </table>	Value	Description	GPRS	2G	EDGE	2G	WCDMA	3G	HSDPA	3G	HSUPA	3G	HSDPA-HSUPA	3G	E-UTRAN	4G
Value	Description																
GPRS	2G																
EDGE	2G																
WCDMA	3G																
HSDPA	3G																
HSUPA	3G																
HSDPA-HSUPA	3G																
E-UTRAN	4G																
ARFCN	The ARFCN (Absolute Radio Frequency Channel Number) is displayed; if the connection is 2G, "arfcn {acquired value}" is displayed.																
UARFCN	UARFCN (Universal Terrestrial Radio Access (UTRA) Absolute Radio Frequency Channel Number) will be displayed; if connected via 3G, "uarfcn {acquired value}" will be displayed.																
EARFCN	EARFCN (E-UTRA Absolute Radio Frequency Channel Number) will be displayed, or "earfcn {acquired value}" if connected via 4G.																
BAND	The frequency band to be used is displayed.																
MCC	The MCC (Mobile Country Code: the operational area code of the mobile operator) is displayed.  <ul style="list-style-type: none"> For a complete list, please refer to the following website https://mcc-mnc-list.com/list Examples are shown below. Japan: 440, 441 U.S.A.: 310-316 																
MNC	MNC (Mobile Network Code: Telecommunications Carrier Identification Code) is displayed.  <ul style="list-style-type: none"> For a complete list, please refer to the following website https://mcc-mnc-list.com/list Examples are shown below. NTT Docomo: 10 Softbank: 20 KDDI: 50, 51, 53, 54 																

Item	Contents																								
TAC	TAC (Tracking Area Code: identification code for the area where the mobile terminal is located) is displayed; if connected via 4G, "tac {acquired value}" is displayed.																								
CELLID	CELLID (Cell Identify: base station ID) is displayed.																								
LAC	The LAC (Location Area Code: area code of the base station) is displayed; if the connection is made via 3G, "lac {acquired value}" is displayed.																								
PCI	PCI (Physical Cell Id: Physical Cell ID) will be displayed; if connected via 4G, it will be displayed as "pci {acquired value}".																								
PSC	PSC (Primary Scrambling Code: W-CDMA system base station identification code) is displayed; if connected via 3G, "psc {acquired value}" is displayed.																								
BSIC	BSIC (Base Station Identity Code: GSM system base station identification code) is displayed. if the connection is made via 2G, "bsic {acquired value}" is displayed.																								
RSSI	RSSI (Received Signal Strength Indicator) is displayed. <table border="1"> <thead> <tr> <th>Antenna Level</th> <th>LED(ANT)</th> <th>RSSI level</th> </tr> </thead> <tbody> <tr> <td>unused</td> <td> switching off the light</td> <td></td> </tr> <tr> <td>normal</td> <td> Green LED lit</td> <td>-73dBm min.</td> </tr> <tr> <td>slightly normal</td> <td> Green LED blinks (500ms interval)</td> <td>-74dBm to -83dBm</td> </tr> <tr> <td>medium</td> <td> Green LED blinks (125ms interval)</td> <td>-84dBm to -93dBm</td> </tr> <tr> <td>slightly weak</td> <td> Red LED blinks (125ms interval)</td> <td>-94dBm to -109dBm</td> </tr> <tr> <td>weak</td> <td> Red LED blinks (500ms interval)</td> <td>-110dBm to -112dBm</td> </tr> <tr> <td>out of range</td> <td> Red LED lights up</td> <td>-113dBm or less</td> </tr> </tbody> </table>	Antenna Level	LED(ANT)	RSSI level	unused	 switching off the light		normal	 Green LED lit	-73dBm min.	slightly normal	 Green LED blinks (500ms interval)	-74dBm to -83dBm	medium	 Green LED blinks (125ms interval)	-84dBm to -93dBm	slightly weak	 Red LED blinks (125ms interval)	-94dBm to -109dBm	weak	 Red LED blinks (500ms interval)	-110dBm to -112dBm	out of range	 Red LED lights up	-113dBm or less
Antenna Level	LED(ANT)	RSSI level																							
unused	 switching off the light																								
normal	 Green LED lit	-73dBm min.																							
slightly normal	 Green LED blinks (500ms interval)	-74dBm to -83dBm																							
medium	 Green LED blinks (125ms interval)	-84dBm to -93dBm																							
slightly weak	 Red LED blinks (125ms interval)	-94dBm to -109dBm																							
weak	 Red LED blinks (500ms interval)	-110dBm to -112dBm																							
out of range	 Red LED lights up	-113dBm or less																							
RSCP	RSCP (Received Signal Code power in dBm: desired wave received power) is displayed; if connected via 3G, "rscp {acquired value}" is displayed. <table border="1"> <thead> <tr> <th>Antenna Level</th> <th>RSCP Level</th> </tr> </thead> <tbody> <tr> <td>normal</td> <td>-90dBm min.</td> </tr> <tr> <td>medium</td> <td>-90dBm to -100dBm</td> </tr> <tr> <td>slightly weak</td> <td>-100dBm to 113dBm</td> </tr> <tr> <td>out of range</td> <td>-113dBm or less</td> </tr> </tbody> </table>	Antenna Level	RSCP Level	normal	-90dBm min.	medium	-90dBm to -100dBm	slightly weak	-100dBm to 113dBm	out of range	-113dBm or less														
Antenna Level	RSCP Level																								
normal	-90dBm min.																								
medium	-90dBm to -100dBm																								
slightly weak	-100dBm to 113dBm																								
out of range	-113dBm or less																								
RSRP	RSRP (Reference Signal Received Power: Reference signal received power, received sensitivity) is displayed. if connected via 4G, "rsrp {acquired value}" is displayed. <table border="1"> <thead> <tr> <th>Antenna Level</th> <th>RSRP Level</th> </tr> </thead> <tbody> <tr> <td>normal</td> <td>-105dBm min.</td> </tr> <tr> <td>medium</td> <td>-105dBm to -15dBm</td> </tr> <tr> <td>slightly weak</td> <td>-115dBm to -120dBm</td> </tr> <tr> <td>out of range</td> <td>-120dBm max.</td> </tr> </tbody> </table>	Antenna Level	RSRP Level	normal	-105dBm min.	medium	-105dBm to -15dBm	slightly weak	-115dBm to -120dBm	out of range	-120dBm max.														
Antenna Level	RSRP Level																								
normal	-105dBm min.																								
medium	-105dBm to -15dBm																								
slightly weak	-115dBm to -120dBm																								
out of range	-120dBm max.																								
RSRQ	RSRQ (Reference Signal Received Quality) is displayed; if connected via 4G, "rsrq {acquired value}" is displayed.																								
SINR	SINR (Signal to Interference plus Noise Ratio: the ratio of interference power + noise power to received power) is displayed. if connected via 4G, "sinr {acquired value}" is displayed.																								
ECIO	EC/IO (Pilot Strength EC/IO=RSCP/RSSI: desired signal power to interference power ratio) is displayed.																								

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show mobile ecm0 ↵
# ---- mobile ecm0 ----
number          0
module          ME3630-J2A
peer            amnimo-mobile
session        amnimo-session
sim             0
apn             amnimo
state           connected
RAT             E-UTRAN
earfcn          1850
band            3
mcc             440
mnc             10
tac             4633
cellid          49507893
pci             404
rssi            -68.0
rsrp            -95.0
rsrq            -7.1
sinr            186.0
ecio            0.0
```

5.4 Manually connect a mobile line

To manually initiate a mobile line connection, run the *mobile connect* command.

Format

```
mobile connect IFNAME [session SESSION-NAME].
```

Setting items

Item	Contents
IFNAME	Specifies the interface name.
SESSION-NAME	Specify a session name.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# mobile connect ecm0 ↵
```

5.5 Disconnect the mobile line

To force the mobile line to disconnect, execute the *no mobile connect* command.

However, in always-on mode, the connection is automatically reconnected.

Format

```
no mobile connect IFNAME
```

Setting items

Item	Contents
IFNAME	Specifies the interface name.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# no mobile connect ecm0 ↵
```

5.6 View mobile line settings

To view the mobile configuration, run the *show config mobile peer* command.

Format

```
show config mobile peer [MOB-PEER-NAME].
```

Setting items

Item	Contents
MOB-PEER-NAME	Specify the name of the mobile line.  If MOB-PEER-NAME is omitted, all mobile settings will be displayed.

Output Format

```
# ---- transition to configure mode ----
configure
# ---- mobile peer MOB-PEER-NAME configure ----
mobile peer MOB-PEER-NAME
verbose VERBOSE
module MODULE-NAME
FAILSAFE
# ---- session SESSION-NAME configure ----
session SESSION-NAME
ENABLE
priority PRIORITY
SIM SIM
PIN
apn APN
USERNAME
password secret ENCRYPT-PASSWORD
connect CONNECT
authentication AUTHENTICATION
operator OPERATOR
attach-timeout ATTACH-TIMEOUT
call-timeout CALL-TIMEOUT
IDLE-TIMEOUT
CONNECTION-TIMEOUT
RECONNECT-TIMEOUT
DISCONNECT-DETECTION
RETRY
rat select RAT-SELECT
rat preferred RAT-PREFERRED
rat mode RAT-MODE
RAT-SERVICE-BANDS
exit
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents								
MOB-PEER-NAME	The name of the mobile line is displayed.								
VERBOSE	Message output level is displayed.								
MODULE-NAME	The module name is displayed.								
FAILSAFE	Displays information on when the failsafe setting is enabled/disabled. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "FAILSAFE RETRY FAILSAFE-RETRY reboot FAILSAFE-REBOOT" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no failsafe" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "FAILSAFE RETRY FAILSAFE-RETRY reboot FAILSAFE-REBOOT" is displayed.	Disable	The message "no failsafe" is displayed.		
Setting	Display								
Enable	The message "FAILSAFE RETRY FAILSAFE-RETRY reboot FAILSAFE-REBOOT" is displayed.								
Disable	The message "no failsafe" is displayed.								
FAILSAFE-RETRY	The number of fail-safe retries is displayed.								
FAILSAFE-REBOOT	The number of fail-safe reboots is displayed.								
SESSION-NAME	The session name is displayed.								
ENABLE	Information is displayed when the session is enabled/disabled. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.		
Setting	Display								
Enable	The message "enable" is displayed.								
Disable	The message "no enable" is displayed.								
PRIORITY	Priority is displayed. 0" is the highest priority and "9" is the lowest priority.								
SIM	The SIM slot number is displayed.								
PIN	If the SIM PIN code is set, "pin {set value}" will be displayed.								
APN	The APN will be displayed.								
USERNAME	If a username is set, "username {configuration value}" will be displayed.								
ENCRYPT-PASSWORD	If a password has been set, "password secret {encrypted setting value}" will be displayed.								
CONNECT	The connection method is displayed. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>manual</td> <td>Manual connection</td> </tr> <tr> <td>always</td> <td>always-on connection</td> </tr> </tbody> </table>	Setting	Contents	manual	Manual connection	always	always-on connection		
Setting	Contents								
manual	Manual connection								
always	always-on connection								
AUTHENTICATION	The authentication method is displayed. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>pap</td> <td>PAP (Password Authentication Protocol) is used as the authentication method for communication.</td> </tr> <tr> <td>CHAP.</td> <td>Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.</td> </tr> <tr> <td>both</td> <td>Both PAP and CHAP are used for the authentication method of communication.</td> </tr> </tbody> </table>	Setting	Contents	pap	PAP (Password Authentication Protocol) is used as the authentication method for communication.	CHAP.	Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.	both	Both PAP and CHAP are used for the authentication method of communication.
Setting	Contents								
pap	PAP (Password Authentication Protocol) is used as the authentication method for communication.								
CHAP.	Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.								
both	Both PAP and CHAP are used for the authentication method of communication.								

Item	Contents								
OPERATOR	The network operator selection method is displayed.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>automatic</td> <td>Automatically selects available communication networks.</td> </tr> <tr> <td>manual {PLMN value}</td> <td>Specifies and fixes the available PLMN (Public Land Mobile Network). The setting range is 0 to 9999999.</td> </tr> <tr> <td>manual-automatic {PLMN value}</td> <td>Specifies and fixes the available PLMN (Public Land Mobile Network). The setting range is 0 to 99999999. If the module cannot connect to the specified PLMN, it will automatically specify a PLMN to which it can connect.</td> </tr> </tbody> </table>	Setting	Contents	automatic	Automatically selects available communication networks.	manual {PLMN value}	Specifies and fixes the available PLMN (Public Land Mobile Network). The setting range is 0 to 9999999.	manual-automatic {PLMN value}	Specifies and fixes the available PLMN (Public Land Mobile Network). The setting range is 0 to 99999999. If the module cannot connect to the specified PLMN, it will automatically specify a PLMN to which it can connect.
	Setting	Contents							
	automatic	Automatically selects available communication networks.							
manual {PLMN value}	Specifies and fixes the available PLMN (Public Land Mobile Network). The setting range is 0 to 9999999.								
manual-automatic {PLMN value}	Specifies and fixes the available PLMN (Public Land Mobile Network). The setting range is 0 to 99999999. If the module cannot connect to the specified PLMN, it will automatically specify a PLMN to which it can connect.								
ATTACH-TIMEOUT	<p>The connection waiting time is displayed.</p>  The connection latency is "the time it takes to establish communication with the base station."								
CALL-TIMEOUT	<p>The call waiting time is displayed.</p>  Call waiting time is "the time from the establishment of communication with the base station until it is authenticated."								
IDLE-TIMEOUT	<p>If no-communication detection time is set, "idle-timeout {set value}" is displayed.</p>  No communication is a state in which packets received through the mobile module are monitored and no target packets are detected. However, the following packets are not monitored <ul style="list-style-type: none"> ● IGMP packet ● The following ICMP packets destination unreachable, echo request ● The following UDP packets DNS, DHCP, NTP, SSDP ● SYN packet ● Packets with Ethernet type numbers other than IPv4 								
CONNECTION-TIMEOUT	If the maximum connection time is set, "connection-timeout {configuration value}" is displayed.								
RECONNECT-TIMEOUT	If the reconnect wait time is set, "reconnect-timeout {configuration value}" is displayed.								
DISCONNECT-DETECTION	If the disconnect detection feature is set, the message "disconnect-detection time DISCONNECT-TIME rssi DISCONNECT-RSSI" is displayed.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>DISCONNECT-TIME</td> <td>The unconnected detection time (seconds) is displayed.</td> </tr> <tr> <td>DISCONNECT-RSSI</td> <td>The disconnection detection RSSI value (dBm) is displayed.</td> </tr> </tbody> </table>	Setting	Contents	DISCONNECT-TIME	The unconnected detection time (seconds) is displayed.	DISCONNECT-RSSI	The disconnection detection RSSI value (dBm) is displayed.		
	Setting	Contents							
DISCONNECT-TIME	The unconnected detection time (seconds) is displayed.								
DISCONNECT-RSSI	The disconnection detection RSSI value (dBm) is displayed.								
RETRY	<p>If the number of line connection retries is set, "retry {set value}" is displayed.</p> <p>If no retry is performed, "no retry" is displayed.</p>								
RAT-SELECT	The RAT (Radio Access Technology) service is displayed.								
RAT-PREFERRED	The RAT Preferred setting is displayed.								

Item	Contents	
RAT-MODE	The RAT mode settings are displayed.	
	Setting	Contents
	auto	The mobile module automatically determines the available RATs.
	manual	Specifies the RATs that can be used. The RAT to be used is specified with the rat service command.
RAT-SERVICE-BANDS	If RAT service bands were configured, "rat service RAT-SERVICE RAT-BANDS" will be displayed.	
RAT-SERVICE	The contents of the RAT service settings are displayed.	
RAT-BANDS	The band number settings are displayed.	

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# show config mobile peer amnimo-mobile ↵
# ---- transition to configure mode. ----
configure
# ---- mobile peer amnimo-mobile configure ----
mobile peer amnimo-mobile
verbose informational
module ME3630-J2A-PORT0
failsafe retry 3 reboot 3
# ---- session amnimo-session configure ----
session amnimo-session
enable
priority 0
sim 0
apn amnimo
username user
password /ARnp8GLdLN3r5FFQ2B0yQ==
connect always
operator automatic
authentication both
attach-timeout 55
call-timeout 30
reconnect-timeout 30
disconnect-detection time 30 rssi -113
no retry
rat select 4G-3G
rat preferred 4G
rat mode auto
exit
exit
# ---- exit configure mode. ----
exit
```

5.7 Set up a mobile line

To configure the mobile, go to the mobile's advanced configuration mode and execute the configuration commands. The settings made here will be written to a configuration file.

Format

```
mobile peer MOB-PEER-NAME
verbose < emergencies | alerts | critical | errors | warnings | notifications | informa
tional | debugging >
module MODULE-NAME
failsafe [retry <1 - 10>] [reboot <1 - 10>]
no failsafe
session SESSION-NAME
enable
no enable
priority <0 - 9>
sim <0 - 3>
pin PIN
no pin
apn APN
username USERNAME
no username
password
password secret ENCRYPT-PASSWORD
no password
connect <manual | always>
authentication <pap | chap | both>
no authentication
operator <automatic | manual [0-999999] | manual-automatic [0-999999]>
attach-timeout <1 - 600>
call-timeout <1 - 600>
idle-timeout <1 - 3600>
no idle-timeout
connection-timeout <1 - 86400>
no connection-timeout
reconnect-timeout <1 - 600>.
no reconnect-timeout
disconnect-detection [time <1 - 600>] [rssi <-113 - -51>]
no disconnect-detection
retry <1 - 9>
no retry
rat select <4G-3G-2G | 4G-3G | 4G-2G | 4G | 3G-2G | 3G | 2G>
rat preferred <4G | 3G | 2G>.
rat mode <auto | manual>
rat service <4G | 3G | 2G> BANDS
no rat service <4G | 3G | 2G>
exit
no session SESSION-NAME
exit
no mobile peer MOB-PEER-NAME
```

Command

Command	Contents						
mobile peer	Specify the name of the mobile line in MOB-PEER-NAME and execute the configuration command.  Executing the command in the configuration mode will enter the detailed configuration mode for the specified mobile line name.						
verbose	Specifies the message output level.  The value can be one of the following: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.						
module	Specify the module name in MODULE-NAME.						
failsafe	Enables fail-safe. Default setting is enabled. <table border="1" data-bbox="523 568 1302 763"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>retry</td> <td>Specify the number of fail-safe retries in the range of 1 to 10. The default setting is 3.</td> </tr> <tr> <td>reboot</td> <td>Specify the number of fail-safe reboots in the range of 1 to 10. The default setting is 3.</td> </tr> </tbody> </table> <p> For more information on fail-safe features, see " 12.3 fail-safe " for more information on the fail-safe feature.</p>	Setting	Contents	retry	Specify the number of fail-safe retries in the range of 1 to 10. The default setting is 3.	reboot	Specify the number of fail-safe reboots in the range of 1 to 10. The default setting is 3.
Setting	Contents						
retry	Specify the number of fail-safe retries in the range of 1 to 10. The default setting is 3.						
reboot	Specify the number of fail-safe reboots in the range of 1 to 10. The default setting is 3.						
no failsafe	Disable fail-safe.						
session	In the advanced setting mode, execute with the session name specified in SESSION-NAME.						
enable	Enable session.						
no enable	Disables the session.						
priority	Set the priority in the range of 0 to 9.						
simulation	Set the SIM slot number in the range of 0 to 3.						
pin	Set the SIM PIN code.  If the SIM's PIN is Disable, no setting is required.						
no pin	Delete the SIM PIN code.						
apn	Set the APN.						
username	Set the username.  Please include an arbitrary string of characters even if you are using a SIM that does not require a username.						
no username	Delete the username.						
password	Set password (non-encrypted).  <ul style="list-style-type: none"> ● Must be entered twice. ● The set password is stored in encrypted form. ● Please include an arbitrary string of characters even if you are using a SIM that does not require a password. 						
password secret	Set the encryption password.						
no password	Delete password.						
connect	Specifies the connection method. The default setting is "always". <table border="1" data-bbox="523 1805 1302 1930"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>manual</td> <td>Manual connection</td> </tr> <tr> <td>always</td> <td>always-on connection</td> </tr> </tbody> </table>	Setting	Contents	manual	Manual connection	always	always-on connection
Setting	Contents						
manual	Manual connection						
always	always-on connection						

Command	Contents								
authentication	<p>Specifies the authentication method. The default setting is "both".</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>pap</td> <td>PAP (Password Authentication Protocol) is used as the authentication method for communication.</td> </tr> <tr> <td>chap</td> <td>Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.</td> </tr> <tr> <td>both</td> <td>Both PAP and CHAP are used for the authentication method of communication.</td> </tr> </tbody> </table>	Setting	Contents	pap	PAP (Password Authentication Protocol) is used as the authentication method for communication.	chap	Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.	both	Both PAP and CHAP are used for the authentication method of communication.
Setting	Contents								
pap	PAP (Password Authentication Protocol) is used as the authentication method for communication.								
chap	Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.								
both	Both PAP and CHAP are used for the authentication method of communication.								
no authentication	Delete the authentication method setting.								
operator	<p>Specifies the network operator selection method. The default setting is "automatic".</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>automatic</td> <td>Automatically selects available communication networks.</td> </tr> <tr> <td>manual</td> <td>The available PLMN (Public Land Mobile Network) is specified and fixed by argument. The setting range is 0 to 9999999.</td> </tr> <tr> <td>manual-automatic</td> <td>The available PLMN (Public Land Mobile Network) is specified and fixed by argument. The setting range is 0 to 9999999. If the specified PLMN cannot be connected, the mobile module will automatically select an available network.</td> </tr> </tbody> </table>	Setting	Contents	automatic	Automatically selects available communication networks.	manual	The available PLMN (Public Land Mobile Network) is specified and fixed by argument. The setting range is 0 to 9999999.	manual-automatic	The available PLMN (Public Land Mobile Network) is specified and fixed by argument. The setting range is 0 to 9999999. If the specified PLMN cannot be connected, the mobile module will automatically select an available network.
Setting	Contents								
automatic	Automatically selects available communication networks.								
manual	The available PLMN (Public Land Mobile Network) is specified and fixed by argument. The setting range is 0 to 9999999.								
manual-automatic	The available PLMN (Public Land Mobile Network) is specified and fixed by argument. The setting range is 0 to 9999999. If the specified PLMN cannot be connected, the mobile module will automatically select an available network.								
attach-timeout	<p>Set the connection waiting time (in seconds) in the range of 1 to 600. The default setting is "55 (seconds)."</p> <p> The connection latency is "the time it takes to establish communication with the base station."</p>								
call-timeout	<p>Set the call waiting time (in seconds) in the range of 1 to 600. The default setting is "30 (seconds)."</p> <p> Call waiting time is "the time from the establishment of communication with the base station until it is authenticated."</p>								
idle-timeout	<p>Set the no-communication detection time (seconds) in the range of 1 to 3600.</p> <p>If no communication continues for a specified period of time, the line is disconnected.</p> <p> No communication is a state in which packets received through the mobile module are monitored and no target packets are detected. However, the following packets are not monitored</p> <ul style="list-style-type: none"> ● IGMP packet ● The following ICMP packets destination unreachable, echo request ● The following UDP packets DNS, DHCP, NTP, SSDP ● SYN packet ● Packets with Ethernet type numbers other than IPv4 								
no idle-timeout	Sets the no-communication detection function to disabled.								
connection-timeout	<p>Set the maximum connection time (in seconds) in the range of 1 to 86400.</p> <p>If the connection continues for the specified period of time, the line is disconnected.</p>								
no connection-timeout	Set the maximum connection time to disabled.								

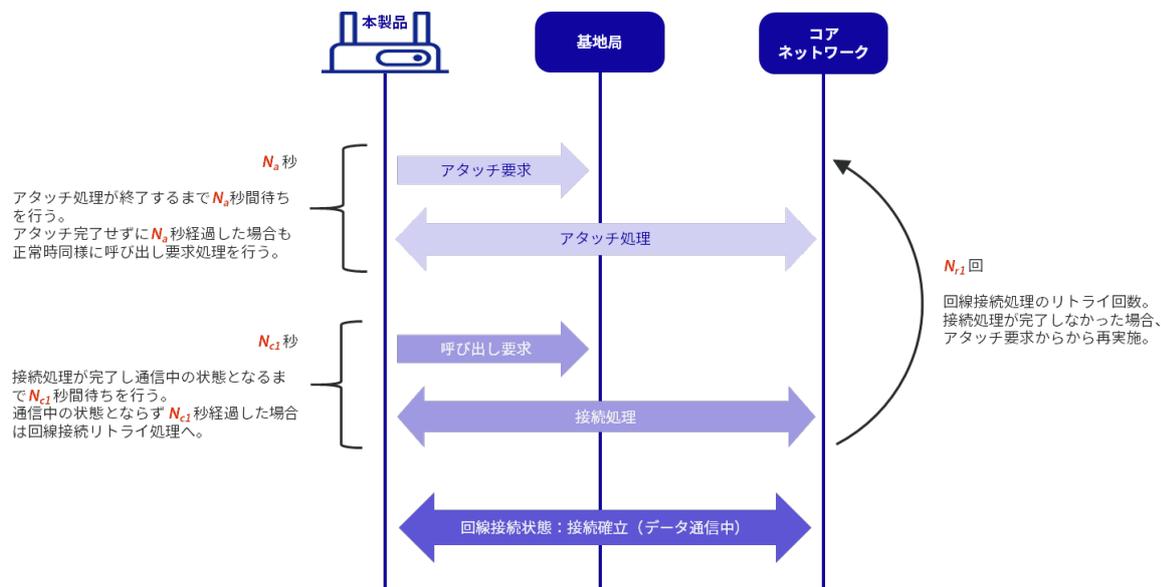
Command	Contents						
reconnect-timeout	Set the reconnection wait time (in seconds) in the range of 1 to 600. The default setting is "30 (seconds).						
no reconnect-timeout	Set the reconnect wait time to disabled.						
disconnect-detection	Enables the disconnect detection function. If the RSSI remains below the DISCONNECT-RSSI value for the DISCONNECT-TIME period, the line is disconnected. <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>time</td> <td>Specify the unconnected detection time (in seconds) in the range of 1 to 600. The default setting is "30 (seconds).</td> </tr> <tr> <td>rssi</td> <td>Specify the unconnected recognition RSSI (dBm) in the range of -113 to -51. The default setting is "-113(dB)m".</td> </tr> </tbody> </table>	Setting	Contents	time	Specify the unconnected detection time (in seconds) in the range of 1 to 600. The default setting is "30 (seconds).	rssi	Specify the unconnected recognition RSSI (dBm) in the range of -113 to -51. The default setting is "-113(dB)m".
Setting	Contents						
time	Specify the unconnected detection time (in seconds) in the range of 1 to 600. The default setting is "30 (seconds).						
rssi	Specify the unconnected recognition RSSI (dBm) in the range of -113 to -51. The default setting is "-113(dB)m".						
no disconnect-detection	Sets the disconnect detection function to disabled.						
retry	Sets the number of line connection retries in the range of 1 to 9. The default setting is disabled (no retry).						
no retry	Sets the line connection retry function to disabled.						
rat select	Specifies the RAT (Radio Access Technology) service.  The value can be 4G-3G-2G, 4G-3G, 4G-2G, 4G, 3G-2G, 3G, 2G, or AUTOMATIC. Available values vary depending on the module used. The default setting is AUTOMATIC.						
rat preferred	Specify 4G, 3G, or 2G as the RAT Preferred.  Available values vary depending on the module used.						
rat mode	Specifies the RAT mode. The default setting is "auto". <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>The mobile module automatically determines the available RATs.</td> </tr> <tr> <td>manual</td> <td>Specifies the RATs that can be used. The RAT to be used is specified with the rat service command.</td> </tr> </tbody> </table>	Setting	Contents	auto	The mobile module automatically determines the available RATs.	manual	Specifies the RATs that can be used. The RAT to be used is specified with the rat service command.
Setting	Contents						
auto	The mobile module automatically determines the available RATs.						
manual	Specifies the RATs that can be used. The RAT to be used is specified with the rat service command.						
rat service	Specify 4G, 3G, or 2G, and the band number you want to use for BANDS to set the RAT service. multiple band numbers can be set for BANDS, separated by ',' (comma).  <ul style="list-style-type: none"> ● Available values vary depending on the module used. ● Set the band number and set the RAT mode to "manual" to limit the band number. 						
no rat service	Specify 4G, 3G, or 2G and set the RAT service band to disabled.  Available values vary depending on the module used.						
exit	If in session advanced setting mode, exits session advanced setting mode and enters advanced setting mode.						
no session	Delete session settings by specifying a session name in SESSION-NAME.						
exit	If in advanced setting mode, exits advanced setting mode and transitions to setting mode.						
no mobile peer	Specify the mobile line name in MOB-PEER-NAME to delete the mobile setting.						

5.7.1 Supplementation of each mobile setting item

The following illustration supplements the items that indicate the time and number of times to be set in the advanced setting mode.

Mobile line connection control

The following figure shows when the "connection waiting time," "call waiting time," and "line connection retry count" items, which can be set from the advanced setting mode, are used when the line is connected.



Item	Supported commands	Contents	Unit	Default value
N_a	attach-timeout	connection latency	second	55
N_{c1}	call-timeout	call waiting time	second	30
N_{r1}	retry	Number of line connection retries	times	no retry

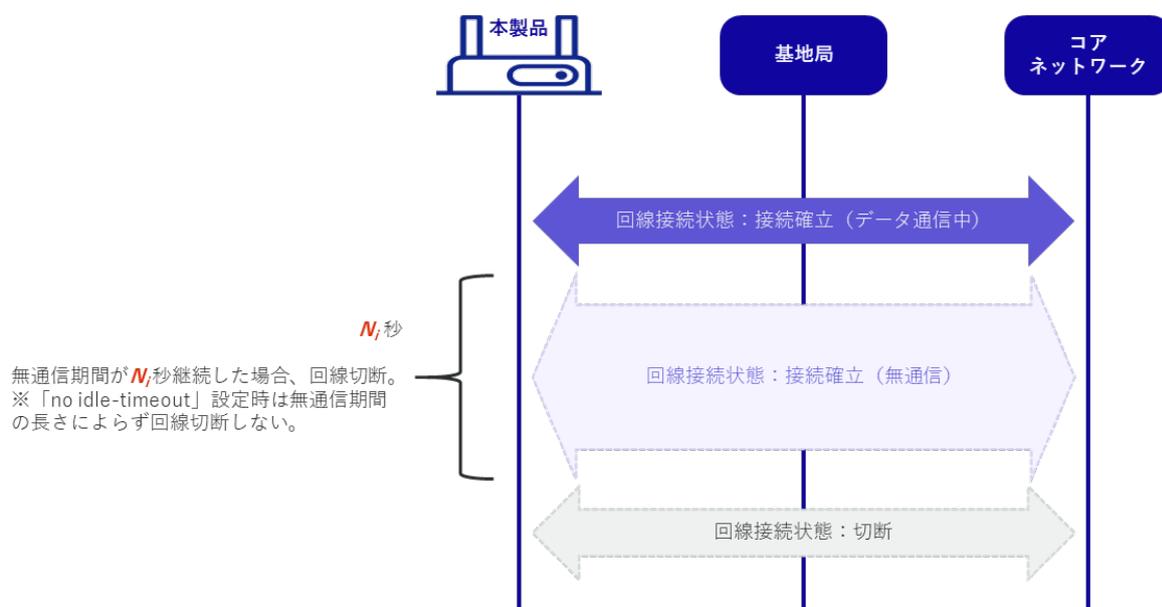
設定モード

```

amnimo(cfg)# mobile peer MOB-PEER-NAME
amnimo(cfg-mp-MOB-PEER-NAME)# session SESSION-NAME
amnimo(cfg-mps-SESSION-NAME)# attach-timeout  $N_a$  ← Specify connection wait time
amnimo(cfg-mps-SESSION-NAME)# call-timeout  $N_{c1}$  ← Call wait time
amnimo(cfg-mps-SESSION-NAME)# retry  $N_{r1}$  ← Specify the number of line connection retries
    
```

Mobile line disconnection control due to expiration of no communication detection time

By setting the "no communication detection time" from the detailed setting mode, the mobile line disconnection can be controlled when there is no communication for a specified period of time, as shown in the figure below.



This function is disabled by default, so if you wish to enable it, please configure it from the Advanced Settings mode.

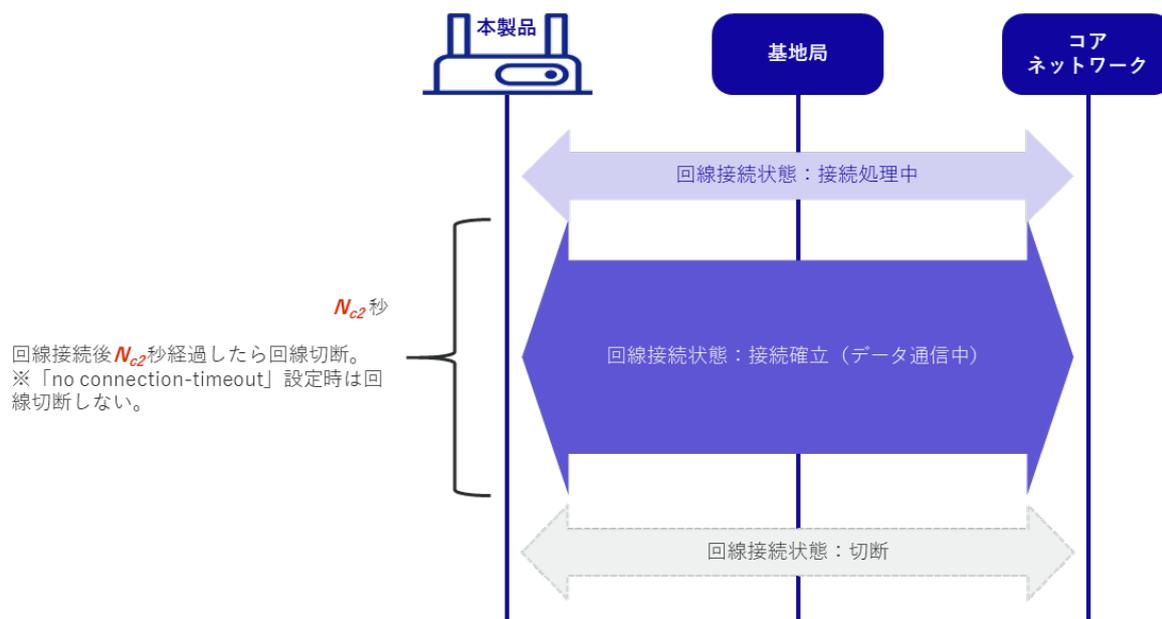
Item	Supported commands	Contents	Unit	Default value
N _i	idle-timeout	No communication detection time	second	no idle-timeout

設定モード

```
amnimo(cfg)# mobile peer MOB-PEER-NAME
amnimo(cfg-mp-MOB-PEER-NAME)# session SESSION-NAME
amnimo(cfg-mps-SESSION-NAME)# idle-timeout Ni ← Specify no communication detection time
```

Mobile line disconnection control due to expiration of maximum connection time

By setting the "Maximum Connection Time" from the Advanced Settings mode, the mobile line disconnection can be controlled when the line connection status continues for a specified period of time, as shown in the figure below.



This function is disabled by default, so if you wish to enable it, please configure it from the Advanced Settings mode.

The line connection process in the figure indicates the attachment and authentication processes.

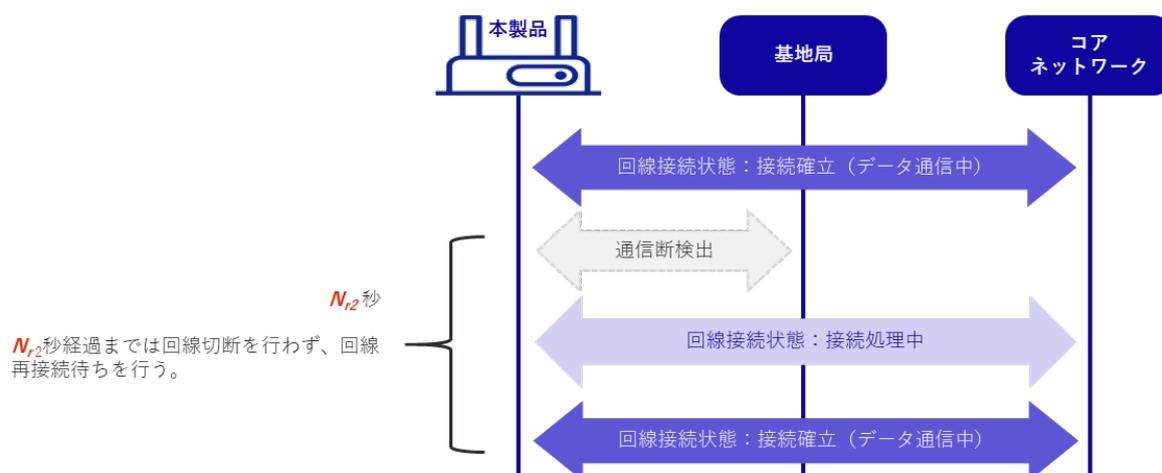
Item	Supported commands	Contents	Unit	Default value
N_{c2}	connection-timeout	Maximum connection time	second	no connection-timeout

設定モード

```
amnimo(cfg)# mobile peer MOB-PEER-NAME
amnimo(cfg-mp-MOB-PEER-NAME)# session SESSION-NAME
amnimo(cfg-mps-SESSION-NAME)# connection-timeout  $N_{c2}$  ← specify maximum connection time
```

Mobile line reconnection waiting control

By setting the "Reconnection Waiting Time" from the Advanced Settings mode, it is possible to control the connection to be maintained without disconnecting the line within the set time, as shown in the figure below, in cases where communication with the base station is temporarily unavailable.



This function keeps the line connected for a set period of time to reduce the overhead of connection processing that occurs when the line is disconnected and then reconnected, thereby improving communication stability.

If the line cannot be reconnected within the set time, the line disconnection operation is performed.

By specifying no reconnect-timeout in the advanced setting mode, it is also possible to control immediate line disconnection when a communication breakdown with the base station is detected.

Item	Supported commands	Contents	Unit	Default value
N_{r2}	reconnect-timeout	Reconnection Waiting Time	second	30

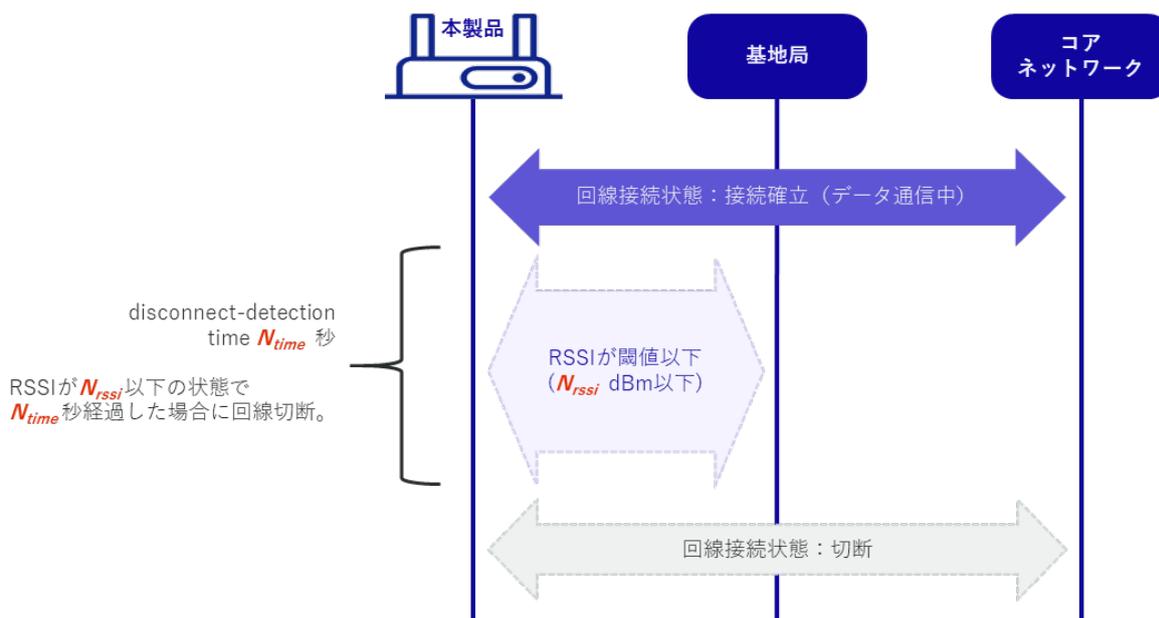
設定モード

```

amnimo(cfg)# mobile peer MOB-PEER-NAME
amnimo(cfg-mp-MOB-PEER-NAME)# session SESSION-NAME
amnimo(cfg-mps-SESSION-NAME)# reconnect-timeout  $N_{r2}$  ← Specify reconnect wait time
amnimo(cfg-mps-SESSION-NAME)# no reconnect-timeout ← to disable the function
    
```

Mobile line disconnection control with disconnection detection function

By setting the "Disconnection Detection Function" from the advanced setting mode, as shown in the figure below, it is possible to control disconnection of the line if the RSSI value falls below a specified value for a specified time or longer.



It is possible to control the line not to disconnect even when out of range by specifying no disconnect-detection in the advanced configuration mode. In this case, Execution example 2 and Example 3 in this case, line switching is not performed even if multiple sessions are configured as shown in the following example.

→ " 5.7.2 Execution example "

However, this function is not applicable when there is a disconnection from the base station or authentication server. In this case, if the line cannot be reconnected within the reconnection waiting time, the line is disconnected, and the line is switched when multiple sessions are set.

Item	Supported commands	Contents	Unit	Default value
N_{rssi} N_{time}	disconnect-detection	Disconnection detection setting - rssi: Disconnection detection RSSI value - time: Disconnection detection continuation period	rssi: dBm time: seconds	rssi: -113 time: 30

設定モード

```

amnimo(cfg)# mobile peer MOB-PEER-NAME
amnimo(cfg-mp-MOB-PEER-NAME)# session SESSION-NAME
amnimo(cfg-mps-SESSION-NAME)# disconnect-detection rssi  $N_{rssi}$  time  $N_{time}$  ← specify disconnect detection function

amnimo(cfg-mps-SESSION-NAME)# no disconnect-detection ← to disable the function
    
```

■ Disconnection events and session switching control

The session control that follows depends on each configuration item and the associated disconnect event.

No.	Disconnection event	Related commands configuration	Session control
1	line connection retry over	attach-timeout call-timeout retry	Connect to the next highest priority session
2	No communication detection time expiration	idle-timeout	Connect to the next highest priority session
3	Maximum connection time expiration	connection-timeout	Connect to the next highest priority session
4	By disconnection detection function line break detection	disconnect-detection	Connect to the next highest priority session
5	Line disconnection from base station	reconnect-timeout	Connect to the next highest priority session
6	Mobile line disconnection (Schedule setting)	schedule general-control action disconnect ecm0*	No reconnection (service interruption)
7	Mobile line disconnection (keep-alive setting)	schedule keep-alive action disconnect ecm0*	Connect to the session with the highest priority
8	Mobile line interface disable	interface ecm0 no enable	No reconnection (service interruption)
9	Disconnection by keep-alive function of DMS	-	Connect to the session with the highest priority
10	Other Errors	-	Connect to the session with the highest priority



No. 1 to 5 setting commands are commands to be executed from the mobile's advanced setting mode.

➔ Refer to " 5.7 Set up a mobile line " for details.

The setting commands No.6 to 7 are commands to be executed from the detailed setting mode of the schedule.

➔ Refer to " 7.7.3 Set a schedule" for details.

The No. 8 configuration command is a command executed from the interface's advanced configuration mode.

➔ Refer to" 6.2.3 Configure the interface and save configuration information" for details.

For details on the setting commands, please refer to the corresponding function pages.



If the connection method for session information is set to "**Manual Connection**," session switching does not occur.



*In Compact Router, the mobile line interface is rmnet_data0.



5.7.2 Execution example

Execution example 1 Setting up a single session

Setting items	Configuration details
session name	amnimo-session
SIM Slot	sim0
SIM PIN Code	1234
degree of relative priority	priority 0
APN	amnimo.net
Authentication ID (username)	user
(computer) password	pass (e.g. skipping a move, passing an examination, ticket to allow entry, etc.)

設定モード

```

amnimo(cfg)# mobile peer amnimo-mobile ←
amnimo(cfg-mp-amnimo-mobile)# session amnimo-session ←
amnimo(cfg-mps-amnimo-session)# sim 0
amnimo(cfg-mps-amnimo-session)# pin 1234
amnimo(cfg-mps-amnimo-session)# apn amnimo.net ←
amnimo(cfg-mps-amnimo-session)# username user ←
amnimo(cfg-mps-amnimo-session)# password ←
Enter new password: .          ← Enter the first password ("pass") and press Enter
Retype new password: .        ← Enter second password ("pass") and press Enter
amnimo(cfg-mps-amnimo-session)# enable ←
amnimo(cfg-mps-amnimo-session)# show config ←
enable
priority 0
sim 0
PIN 1234
apn amnimo.net
username user
password secret /ARnp8GLdLN3r5FFQ2B0yQ== ← Password entered is displayed in encrypted
form
connect always
operator automatic
authentication both
attach-timeout 300
call-timeout 300
reconnect-timeout 30
disconnect-detection time 60 rssi -113
no retry
rat select 4G-3G
rat preferred 4G
rat mode auto
amnimo(cfg-mps-amnimo-session)# exit ←
amnimo(cfg-mp-amnimo-mobile)# exit ←

```

Execution example 2 Multiple session setup (1) (When a connection fails three times in a row and the session is automatically switched)

Indicates a setting that automatically switches to low-priority session B if connection fails three times in a row in high-priority session A.

Setting items	Connection priority high session setting details	Connection priority low session setting details
session name	A	B
SIM Slot	sim0	sim1
degree of relative priority	priority 0	priority 1
APN	amnimo.net	amnimo.net
Authentication ID (username)	user	user
(computer) password	pass (e.g. skipping a move, passing an examination, ticket to allow entry, etc.)	pass (e.g. skipping a move, passing an examination, ticket to allow entry, etc.)
connection latency	attach-timeout 55 (default value)	attach-timeout 55 (default value)
call waiting time	call-timeout 30 (default value)	call-timeout 30 (default value)
Number of line connection retries	retry 3	retry 3
Reconnection Waiting Time	reconnect-timeout 30 (default value)	reconnect-timeout 30 (default value)

設定モード

```

amnimo(cfg)# mobile peer amnimo ← Go to mobile advanced settings mode
amnimo(cfg-mp-amnimo)# session A ← Go to advanced settings mode for session A
amnimo(cfg-mps-A)# priority 0 ← Specify the priority of the connection
amnimo(cfg-mps-A)# sim 0 ← Specify SIM
amnimo(cfg-mps-A)# apn amnimo.net ←
amnimo(cfg-mps-A)# username user ←
amnimo(cfg-mps-A)# password ←
Enter new password: ← Enter the first password and press Enter
Retype new password: ← Enter second password and press Enter
amnimo(cfg-mps-A)# attach-timeout 55 ← Specify 55 seconds to wait for connection (default value)
amnimo(cfg-mps-A)# call-timeout 30 ← Call wait time specified as 30 seconds (default value)
amnimo(cfg-mps-A)# retry 3 ← Specify 3 connection retries
amnimo(cfg-mps-A)# reconnect-timeout 30 ← Specify reconnect wait time as 30 seconds (default value)
amnimo(cfg-mps-A)# enable ←
amnimo(cfg-mps-A)# exit ←
amnimo(cfg-mp-amnimo)# session B ← Go to advanced settings mode for session B
amnimo(cfg-mps-B)# priority 1 ← Specify connection priority
amnimo(cfg-mps-B)# sim 1 ← Specify SIM
amnimo(cfg-mps-B)# apn amnimo.net ←
amnimo(cfg-mps-B)# username user ←
amnimo(cfg-mps-B)# password ←
Enter new password: ← Enter the first password and press Enter
Retype new password: ← Enter second password and press Enter
amnimo(cfg-mps-B)# attach-timeout 55 ← Specify 55 seconds to wait for connection (default value)
amnimo(cfg-mps-B)# call-timeout 30 ← Call wait time specified as 30 seconds (default value)
amnimo(cfg-mps-B)# retry 3 ← Specify 3 connection retries
amnimo(cfg-mps-B)# reconnect-timeout 30 ← Specify reconnect wait time as 30 seconds (default value)

```

```

amnimo(cfg-mps-B)# enable ↵
amnimo(cfg-mps-B)# exit ↵
amnimo(cfg-mp-amnimo)# exit ↵
amnimo(cfg)# interface ecm0↵      ← Go to interface advanced settings mode
amnimo(cfg-interface-ecm0)# mobile amnimo ↵
amnimo(cfg-interface-ecm0)# dhcp4 ↵
amnimo(cfg-interface-ecm0)# enable ↵
amnimo(cfg-interface-ecm0)# exit ↵
amnimo(cfg)#.

```



If a high priority line is disconnected for some reason (see Disconnection Event and Session Switching Control) and successfully connected to a low priority line, the connection will not automatically return even if the high priority line network is restored. This is because as long as the mobile module is connected to the low connection priority line, it cannot detect the restoration of the high connection priority line side.

To automatically switch back to the high priority line when the low priority line is normal, the connection-timeout setting can be configured in the low priority session settings to disconnect the line and switch to the high priority line after the line has been connected for the specified time.

As an example, an execution example of automatically switching sessions according to RSSI is shown on the next page.



For Compact Router, the mobile line interface is `rmnet_data0`.



Execution example 3 Multiple session setup (2) (when automatically switching sessions according to RSSI)

A setting that alternates between high connection priority session A and low connection priority session B according to the set value of received signal strength (RSSI) by the disconnection detection function.

Automatically switches to Session B when the received signal strength (RSSI) of Session A becomes lower than the set value, and automatically switches to Session A when the received signal strength of Session B becomes lower than the set value.

Also, if the maximum connection time is set on the Session B side and the RSSI is not lower than the set value, the connection is returned to Session A, which has a higher connection priority, after a certain period of time.

Setting items	Connection priority high session setting details	Connection priority low session setting details
session name	A	B
SIM Slot	sim0	sim1
degree of relative priority	priority 0	priority 1
APN	amnimo.net	amnimo.net
Disconnection detection function	time 30 rssi -93 The session switches when the received signal strength (rssi) becomes -93 dBm or lower continuously for 30 seconds (time) or longer.	time 30 rssi -93
Authentication ID (username)	user	user
(computer) password	pass (e.g. skipping a move, passing an examination, ticket to allow entry, etc.)	pass (e.g. skipping a move, passing an examination, ticket to allow entry, etc.)
Maximum connection time	no connection-timeout (default value)	connection-timeout 60



LED (ANT) control changes according to received signal strength.

Antenna level	LED (ANT)	RSSI level
unused	 switching off the light	
normal	 Green LED lit	-73dBm min.
slightly normal	 Green LED blinks (500ms interval)	-74dBm to -83dBm
middle	 Green LED blinks (125ms interval)	-84dBm to -93dBm
slightly weak	 Red LED blinks (125ms interval)	-94dBm to -109dBm
weak	 Red LED blinks (500ms interval)	-110dBm to -112dBm
Out of range	 Red LED lights up	-113dBm or less

```

amnimo(cfg)# mobile peer amnimo↵ ← Go to mobile advanced settings mode
amnimo(cfg-mp-amnimo)# session A ↵ ← Go to advanced settings mode for session A
amnimo(cfg-mps-A)# priority 0↵ ← Specify connection priority
amnimo(cfg-mps-A)# sim 0↵ ← Specify SIM
amnimo(cfg-mps-A)# disconnect-detection time 30 rssi -93↵ ← Set disconnect detection func
tion
amnimo(cfg-mps-A)# apn amnimo.net ↵
amnimo(cfg-mps-A)# username user ↵
amnimo(cfg-mps-A)# password ↵
Enter new password: ← Enter the first password and press Enter
Retype new password: ← Enter second password and press Enter
amnimo(cfg-mps-B)# no connection-timeout↵ ← Do not set maximum connection time (defaul
t value)
amnimo(cfg-mps-A)# enable ↵
amnimo(cfg-mps-A)# exit ↵
amnimo(cfg-mp-amnimo)# session B↵ ← Go to advanced settings mode for session B
amnimo(cfg-mps-B)# priority 1↵ ← Specify connection priority
amnimo(cfg-mps-B)# sim 1↵ ← Specify SIM
amnimo(cfg-mps-B)# disconnect-detection time 30 rssi -93↵ ← Set disconnect detection func
tion
amnimo(cfg-mps-B)# apn amnimo.net ↵
amnimo(cfg-mps-B)# username user ↵
amnimo(cfg-mps-B)# password ↵
Enter new password: ←Enter the first password and press Enter
Retype new password: ←Enter second password and press Enter
amnimo(cfg-mps-B)# connection-timeout 60↵ ← Specify maximum connection time as 60 seco
nds
amnimo(cfg-mps-B)# enable ↵
amnimo(cfg-mps-B)# exit ↵
amnimo(cfg-mp-amnimo)# exit ↵
amnimo(cfg)# interface ecm0↵ ← Go to interface advanced configuration mode
amnimo(cfg-interface-ecm0)# mobile amnimo ↵
amnimo(cfg-interface-ecm0)# dhcp4 ↵
amnimo(cfg-interface-ecm0)# enable ↵
amnimo(cfg-interface-ecm0)# exit ↵
amnimo(cfg)#.

```



For Compact Router, the mobile line interface is rmnet_data0.



5.7.3 Automatic time correction function (supported from V1.5.0)

When using a mobile line, upon successful connection, the time is obtained from the mobile network side, and if it differs from the system time by more than one day, the time is corrected to the time obtained from the mobile network side. This correction function is also enabled when the NTP function is disabled.

Chap 6. Network Settings

This chapter describes the product's network configuration, including interfaces and routing, PPP, packet filtering and NAT, and IPSec.

6.1 Configure PPP settings.



It connects and disconnects PPP, displays status, and controls settings.



This function is not available on indoor type Compact Router.

6.1.1 Display PPP status

To view the status of PPP, run the *show pppoe* command.

Format

```
show pppoe [IFNAME].
```

Setting items

Item	Contents
IFNAME	Specifies the interface name. ppp<0-9>

Output Format

```
# ---- pppoe IFNAME ----
PPP-PEER-NAME PPP-PEER-NAME
STATE STATE
```

Output item

Item	Contents								
IFNAME	The interface name is displayed. ppp<0-9>								
PPP-PEER-NAME	The PPP setting name is displayed.								
STATE	The status of the mobile module is displayed. <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>dialing</td> <td>during the connection process</td> </tr> <tr> <td>connected</td> <td>state of connectivity</td> </tr> <tr> <td>disconnected</td> <td>disconnected state</td> </tr> </tbody> </table>	Value	Description	dialing	during the connection process	connected	state of connectivity	disconnected	disconnected state
Value	Description								
dialing	during the connection process								
connected	state of connectivity								
disconnected	disconnected state								

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.



```
amnimo$ show pppoe ppp0 ↵
# ---- pppoe ppp0 ----
peer amnimo-ppp
state connected
```

6.1.2 Connect PPP manually

To make a PPP connection manually, run the *pppoe connect* command.

Format

```
pppoe connect IFNAME
```

Setting items

Item	Contents
IFNAME	Specifies the interface name. ppp<0-9>

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# pppoe connect ppp0 ↵
```

6.1.3 Disconnect PPP

To disconnect PPP, execute the *no pppoe connect* command.

Format

```
no pppoe connect IFNAME
```

Setting items

Item	Contents
IFNAME	Specifies the interface name. ppp<0-9>

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# no pppoe connect ppp0 ↵
```

6.1.4 Display PPP settings

To view the PPP configuration, run the *show config ppp peer* command.

Format

```
show config ppp peer [PPP-PEER-NAME].
```

Setting items

Item	Contents
PPP-PEER-NAME	Specify the PPP configuration name.

Output Format

```
# ---- transition to configure mode ----
configure
# ---- ppp peer PPP-PEER-NAME configure ----
ppp peer PPP-PEER-NAME
VERBOSE VERBOSE
USERNAME
password secret ENCRYPT-PASSWORD
connect CONNECT
authentication AUTHENTICATION
PASSIVE
IDLE-TIMEOUT
CONNECTION-TIMEOUT
BSDCOMP
DEFLATE
CCP
PCCOMP
VJ
VJCOMP
VJ-MAX-SLOT
PREDICTOR1
ifname IFNAME
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
PPP-PEER-NAME	The PPP setting name is displayed.						
VERBOSE	Message output level is displayed.						
USERNAME	If a username is set, "username {configuration value}" will be displayed.						
ENCRYPT-PASSWORD	If a password has been set, "password secret {encrypted setting value}" will be displayed.						
CONNECT	The connection method is displayed.						
AUTHENTICATION	The authentication method is displayed.						
PASSIVE	<p>The PASSIVE option setting is displayed.</p> <p> The passive option setting is a setting to wait for a valid LCP packet to arrive from the destination when no response is received from the destination at the start of the connection.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "PASSIVE" is displayed.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "PASSIVE" is displayed.	Disable	Not displayed.
Setting	Display						
Enable	The message "PASSIVE" is displayed.						
Disable	Not displayed.						

Item	Contents						
IDLE-TIMEOUT	If no-communication detection time is set, "idle-timeout {set value}" is displayed.						
CONNECTION-TIMEOUT	If the maximum connection time is set, "connection-timeout {configuration value}" is displayed.						
BSDCOMP	The BSD-Compress method packet compression settings are displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "bsdcomp BSDCOMP-NR BSDCOMP-NT" appears.</td> </tr> <tr> <td>Disable</td> <td>The message "no bsdcomp" appears.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "bsdcomp BSDCOMP-NR BSDCOMP-NT" appears.	Disable	The message "no bsdcomp" appears.
	Setting	Display					
Enable	The message "bsdcomp BSDCOMP-NR BSDCOMP-NT" appears.						
Disable	The message "no bsdcomp" appears.						
BSDCOMP-NR	The maximum code size (in bits) is displayed.						
BSDCOMP-NT	Displays the maximum size (in bits) of packets that the other side will send.						
DEFLATE	Deflate method packet compression settings are displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "deflate DEFLATE-NR DEFLATE-NT" appears.</td> </tr> <tr> <td>Disable</td> <td>The message "no deflate" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "deflate DEFLATE-NR DEFLATE-NT" appears.	Disable	The message "no deflate" is displayed.
	Setting	Display					
Enable	The message "deflate DEFLATE-NR DEFLATE-NT" appears.						
Disable	The message "no deflate" is displayed.						
DEFLATE-NR	The maximum window size setting is displayed. Window size is 2 ^{DEFLATE-NR} bytes.						
DEFLATE-NT	The maximum window size setting to be sent to the other party is displayed. Window size is 2 ^{DEFLATE-NT} bytes.						
CCP	CCP (Compression Control Protocol) negotiation settings are displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>Not displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no ccp" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	Not displayed.	Disable	The message "no ccp" is displayed.
	Setting	Display					
Enable	Not displayed.						
Disable	The message "no ccp" is displayed.						
PCOMP	The PCOMP (Protocol Field Compression) negotiation settings are displayed.						
VJ	The PCOMP (Protocol Field Compression) negotiation settings are displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>Not displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no vj" appears.</td> </tr> </tbody> </table>	Setting	Display	Enable	Not displayed.	Disable	The message "no vj" appears.
	Setting	Display					
Enable	Not displayed.						
Disable	The message "no vj" appears.						
VJCCOMP	Settings for the connection ID compression option in Van-Jacobson method TCP/IP header compression are displayed.						
VJ-MAX-SLOTS	Shows the setting for the number of connection slots in Van Jacobson method TCP/IP header compression/decompression.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>Not displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no vjccomp" appears.</td> </tr> </tbody> </table>	Setting	Display	Enable	Not displayed.	Disable	The message "no vjccomp" appears.
	Setting	Display					
Enable	Not displayed.						
Disable	The message "no vjccomp" appears.						
VJ-MAX-SLOTS	Shows the setting for the number of connection slots in Van Jacobson method TCP/IP header compression/decompression.						

Item	Contents						
PREDICTOR1	Predictor-1 compression usage settings are displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>Not displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no predictor1" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	Not displayed.	Disable	The message "no predictor1" is displayed.
	Setting	Display					
Enable	Not displayed.						
Disable	The message "no predictor1" is displayed.						
IFNAME	The name of the physical interface used by the PPPoE protocol is displayed.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```

amnimo# show config ppp peer amnimo-ppp ↵
# ---- transition to configure mode. ----
configure
# ---- ppp peer amnimo-ppp configure ----
ppp peer amnimo-ppp
verbose informational
username pppoeuser
password pppoePASS
connect always
no authentication
passive
bsdcomp 15,15
deflate 15,15
ccp
PCOMP
vj
vjccomp
vj-max-slots 15
predictor1
ifname eth0
exit
# ---- exit configure mode. ----
exit

```

6.1.5 Configure PPP settings.

To configure PPP, go to the PPP advanced configuration mode and execute the configuration commands. The settings made here will be written to a configuration file.

Format

```

ppp peer PPP-PEER-NAME
verbose < emergencies | alerts | critical | errors | warnings | notifications | informa
tional | debugging >
username USERNAME
no username
password
password secret ENCRYPT-PASSWORD
no password
connect <manual | always
authentication <pap | chap | both
no authentication
passive
no passive
idle-timeout <1 - 3600>
no idle-timeout
connection-timeout <1 - 86400>
no connection-timeout
bsdcomp NR,MT
no bsdcomp
deflate NR,MT
no deflate
ccp
no ccp
PCOMP
no pcomp
vj
no vj
vjccomp
no vjccomp
vj-max-slots <2 - 16>
predictor1
no predictor1
ifname IFNAME
exit
no ppp peer PPP-PEER-NAME

```

Command

Command	Contents
ppp peer	Execute by specifying the PPP configuration name in PPP-PEER-NAME.  When executed in the configuration mode with a PPP setting name, the program enters the detailed configuration mode for the specified PPP setting.
verbose	Specifies the message output level.  The value can be one of the following: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
username	Set the username.
no username	Delete the username.

Command	Contents								
password	Set password (non-encrypted).  <ul style="list-style-type: none"> • Must be entered twice. • The set password is stored in encrypted form. 								
password secret	Set the encryption password.								
no password	Delete password.								
connect	Specify the connection method. <table border="1" data-bbox="576 383 1353 510"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>manual</td> <td>Manual connection</td> </tr> <tr> <td>always</td> <td>always-on connection</td> </tr> </tbody> </table>	Setting	Contents	manual	Manual connection	always	always-on connection		
Setting	Contents								
manual	Manual connection								
always	always-on connection								
authentication	Specifies the authentication method. <table border="1" data-bbox="576 566 1353 902"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>pap</td> <td>PAP (Password Authentication Protocol) is used as the authentication method for communication.</td> </tr> <tr> <td>chap</td> <td>Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.</td> </tr> <tr> <td>both</td> <td>Uses both PAP and CHAP as authentication methods for communication.</td> </tr> </tbody> </table>	Setting	Contents	pap	PAP (Password Authentication Protocol) is used as the authentication method for communication.	chap	Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.	both	Uses both PAP and CHAP as authentication methods for communication.
Setting	Contents								
pap	PAP (Password Authentication Protocol) is used as the authentication method for communication.								
chap	Challenge Handshake Authentication Protocol (CHAP) is used as the authentication method for communication.								
both	Uses both PAP and CHAP as authentication methods for communication.								
no authentication	Delete the authentication method setting.								
passive	Set the PASSIVE option.  The passive option setting is a setting to wait for a valid LCP packet to arrive from the destination when no response is received from the destination at the start of the connection.								
no passive	Remove the PASSIVE option setting.								
idle-timeout	Set the no-communication detection time (seconds) in the range of 1 to 3600. If no communication continues for a specified period of time, the line is disconnected.								
no idle-timeout	Sets the no-communication detection function to disabled.								
connection-timeout	Set the maximum connection time (in seconds) in the range of 1 to 86400. If the connection continues for the specified period of time, the line is disconnected.								
no connection-timeout	Set the maximum connection time to disabled.								
bsdcomp	Enables the BSD-Compress method packet compression setting. <table border="1" data-bbox="576 1559 1353 1787"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>nr</td> <td>Set the maximum code size (in bits) in the range of 9 to 15.</td> </tr> <tr> <td>nt</td> <td>Sets the maximum size (in bits) of packets that the other side will send, in the range of 9 to 15.</td> </tr> </tbody> </table>	Setting	Contents	nr	Set the maximum code size (in bits) in the range of 9 to 15.	nt	Sets the maximum size (in bits) of packets that the other side will send, in the range of 9 to 15.		
Setting	Contents								
nr	Set the maximum code size (in bits) in the range of 9 to 15.								
nt	Sets the maximum size (in bits) of packets that the other side will send, in the range of 9 to 15.								
no bsdcomp	Disables the BSD-Compress method packet compression setting.								

Command	Contents						
deflate	Enables the Deflate method packet compression setting. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>nr</td> <td>Set the maximum window size setting value in the range of 8 to 15. The window size is 2^{nr} bytes.</td> </tr> <tr> <td>nt</td> <td>Set the maximum window size setting value to be sent to the other party in the range of 8 to 15. The window size is 2^{nt} bytes.</td> </tr> </tbody> </table>	Setting	Contents	nr	Set the maximum window size setting value in the range of 8 to 15. The window size is 2 ^{nr} bytes.	nt	Set the maximum window size setting value to be sent to the other party in the range of 8 to 15. The window size is 2 ^{nt} bytes.
Setting	Contents						
nr	Set the maximum window size setting value in the range of 8 to 15. The window size is 2 ^{nr} bytes.						
nt	Set the maximum window size setting value to be sent to the other party in the range of 8 to 15. The window size is 2 ^{nt} bytes.						
no deflate	Disables the Deflate method packet compression setting.						
ccp	Enables Compression Control Protocol (CCP) negotiation settings.						
no ccp	Disables the Compression Control Protocol (CCP) negotiation setting.						
PCOMP	Enables PCOMP (Protocol Field Compression) negotiation settings.						
no pcomp	Disables the PCOMP (Protocol Field Compression) negotiation setting.						
vj	Enables Van-Jacobson method TCP/IP header compression settings.						
no vj	Disables Van-Jacobson method TCP/IP header compression settings.						
vjccomp	Enables the setting of the Connection ID compression option in Van-Jacobson method TCP/IP header compression.						
no vjccomp	Disables the connection ID compression option setting for Van-Jacobson method TCP/IP header compression.						
vj-max-slots	Sets the number of connection slots in Van Jacobson method TCP/IP header compression/decompression from 2 to 16.						
predictor1	Enables the Predictor-1 compression usage setting.						
no predictor1	Disables the Predictor-1 compression usage setting.						
ifname	Sets the name of the physical interface used by the PPPoE protocol.						
exit	Exit the detailed setting mode and enter the setting mode.						
no ppp peer	Delete PPP settings by specifying PPP PEER NAME.						

Execution example

Below is an example configuration for ppp connection with chap authentication.

設定モード

```

amnimo(cfg)# ppp peer amnimo-ppp ↵
amnimo(cfg-pp-amnimo-ppp)# username pppoeuser ↵ ← Set authentication username
amnimo(cfg-pp-amnimo-ppp)# password ↵
Enter new password:. ↵ ← Enter the authentication password (1st time)
and press Enter
Retype new password:. ↵ ← Enter the authentication password (second time)
me) and press Enter
amnimo(cfg-pp-amnimo-ppp)# authentication chap ↵ ← Enable chap authentication
amnimo(cfg-pp-amnimo-ppp)# show config ↵
verbose informational
username pppoeuser
password pppoeuser
connect always
authentication chap

```

```
bsdcomp 15,15
deflate 15,15
ccp
PCOMP
vj
vjccomp
vj-max-slots 15
predictor1
ifname eth0
amnimo(cfg-pp-amnimo-ppp)# exit ↵
amnimo(cfg)#.
```

6.2 Configure interface settings.



Display and configure interface status and settings.

6.2.1 Display interface status

To view the status of an interface, run the *show interface* command.

Format

```
show interface [IFNAME].
```

Setting items

Item	Contents
IFNAME	Specifies the interface name.  If IFNAME is omitted, the status of all configured interfaces will be displayed.

Output Format

```
IFNAME: state LINK-DETECT mtu MTU
mac MAC-ADDRESS
ipv4 ipv4-address/ipv4-prefix
ipv6 ipv6-address/ipv6-prefix
```

Output item

Item	Contents
IFNAME	The interface name is displayed.
LINK-DETECT	The link status is displayed. ● Link down status: DOWN ● Link-up state: UP
MTU	The MTU (Maximum Transfer Unit) value is displayed.
MAC-ADDRESS	The MAC address is displayed in the following format <pre>xx:xx:xx:xx:xx:xx</pre> xx is a hexadecimal number.
IPv4-ADDRESS	IPv4 addresses are displayed.
IPv4-PREFIX	IPv4 prefix length is displayed.
IPv6-ADDRESS	IPv6 addresses are displayed.
IPv6-PREFIX	The IPv6 prefix length is displayed.



- ipv4 and ipv6 are shown on multiple lines.
- The output values are not the values obtained from the configuration file, but the values that are actually set.

Execution example

Command input and output is the same in all modes. Below is an example of running the General User mode on the Edge Gateway.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show interface ↵
eth0: state UP mtu 1500
  mac e8:1b:4b:00:30:01
  ipv4 192.168.0.254/24
  ipv6 fe80::ea1b:4bff:fe00:3001/64
lan0: state UP mtu 1500
  mac e8:1b:4b:00:31:01
lan1: state DOWN mtu 1500
  mac e8:1b:4b:00:31:01
lan2: state DOWN mtu 1500
  mac e8:1b:4b:00:31:01
lan3: state DOWN mtu 1500
  mac e8:1b:4b:00:31:01
br0: state UP mtu 1500
  mac e8:1b:4b:00:31:01
  ipv4 192.168.1.254/24
  ipv4 172.16.0.1/16
  ipv6 fe80::ea1b:4bff:fe00:3101/64
```

6.2.2 Display interface settings

To view the interface configuration, run the *show config interface* command.

Format

```
show config interface [IFNAME].
```

Setting items

Item	Contents
IFNAME	Specifies the interface name.  If IFNAME is omitted, all configured interface settings will be displayed.

Output format (Edge Gateway, IoT Router)

```
# ---- transition to configure mode ----
configure
# ---- interface IFNAME configure ----
interface IFNAME
ENABLE
BRIDGE
MAC-ADDRESS
PMTU
MOBILE
PPPOE4
PPPOE4-DNS
PPPOE4-ROUTE
ADDRESS
DHCP4
DHCP4-DNS
DHCP4-NTP
DHCP4-MTU
```

```

DHCP4-ROUTE
GATEWAY4
GATEWAY4-VIA
DYNAMIC-SNAT4
mtu MTU
MRU
MODE
PROXY-ARP
OPTIONAL
exit
# ---- exit configure mode ----
exit

```

Output format (Compact Router)

```

# ---- transition to configure mode ----
configure
# ---- interface IFNAME configure ----
interface IFNAME
ENABLE
BRIDGE
MAC-ADDRESS
PMTU
MOBILE
MOBILE-DNS
MOBILE-ROUTE
PPPOE4
PPPOE4-DNS
PPPOE4-ROUTE
ADDRESS
DHCP4
DHCP4-DNS
DHCP4-NTP
DHCP4-MTU
DHCP4-ROUTE
GATEWAY4
GATEWAY4-VIA
DYNAMIC-SNAT4
mtu MTU
MRU
MODE
PROXY-ARP
OPTIONAL
WIFI-AP
WIFI-STA
exit
# ---- exit configure mode ----
exit

```

Output item

Item	Contents						
IFNAME	<p>The interface name is displayed.</p>  Configurable interface names vary by product. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, br<0-9>, ecm0, ppp<0-9> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9> ● Compact Router eth0, rmnet_data0 						
ENABLE	<p>Information is displayed when the interface is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
BRIDGE	The bridge name setting is displayed.						
MAC-ADDRESS	The MAC address is displayed as "mac {set value}".						
PMTU	<p>The path MTU setting is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>The message "pmtu auto" is displayed.</td> </tr> <tr> <td>manual</td> <td>The message "pmtu manual {setting value}" is displayed.</td> </tr> </tbody> </table>	Setting	Display	auto	The message "pmtu auto" is displayed.	manual	The message "pmtu manual {setting value}" is displayed.
Setting	Display						
auto	The message "pmtu auto" is displayed.						
manual	The message "pmtu manual {setting value}" is displayed.						
MOBILE	<p>The name of the mobile peer setting used for mobile connections is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>mobile {setting value}" is displayed. The setting value contains the MOB PEER NAME (mobile peer setting name).</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	mobile {setting value}" is displayed. The setting value contains the MOB PEER NAME (mobile peer setting name).	Disable	Not displayed.
Setting	Display						
Enable	mobile {setting value}" is displayed. The setting value contains the MOB PEER NAME (mobile peer setting name).						
Disable	Not displayed.						
MOBILE-DNS	<p>The DNS settings for mobile features will be displayed.</p> <ul style="list-style-type: none"> ● When mobile peer settings are enabled <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "mobile dns {set value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).</td> </tr> <tr> <td>Disable</td> <td>The message "no mobile dns" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> ● Mobile peer settings are disabled Not displayed.  rmnet_data0 of the Compact Router. Only the interface is available.	Setting	Display	Enable	The message "mobile dns {set value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).	Disable	The message "no mobile dns" is displayed.
Setting	Display						
Enable	The message "mobile dns {set value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).						
Disable	The message "no mobile dns" is displayed.						

Item	Contents						
MOBILE-ROUTE	<p>The route settings for the mobile function will be displayed.</p> <ul style="list-style-type: none"> When mobile peer settings are enabled <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="width: 30%;">Setting</th> <th>display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "mobile route {set value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).</td> </tr> <tr> <td>Disable</td> <td>The message "no mobile route" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> If mobile peer settings are disabled Not displayed. rmnet_data0 of the Compact Router. Only the interface is available. 	Setting	display	Enable	The message "mobile route {set value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).	Disable	The message "no mobile route" is displayed.
Setting	display						
Enable	The message "mobile route {set value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).						
Disable	The message "no mobile route" is displayed.						
PPPOE4	<p>The name of the PPP peer setting used for PPPoE (IPv4) connections is displayed.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="width: 30%;">Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "pppoe4 {setting value}" is displayed. The setting value contains the PPP PEER NAME (PPP peer setting name).</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table> <p> PPPoE-related settings are not available on the rmnet_data0 interface of the Compact Router Indoor Type router.</p>	Setting	Display	Enable	The message "pppoe4 {setting value}" is displayed. The setting value contains the PPP PEER NAME (PPP peer setting name).	Disable	Not displayed.
Setting	Display						
Enable	The message "pppoe4 {setting value}" is displayed. The setting value contains the PPP PEER NAME (PPP peer setting name).						
Disable	Not displayed.						
PPPOE4-DNS	<p>PPPoE (IPv4) DNS settings are displayed.</p> <ul style="list-style-type: none"> When PPPOE4 is enabled <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="width: 30%;">Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "pppoe4 dns {configuration value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).</td> </tr> <tr> <td>Disable</td> <td>The message "no pppoe4 dns" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> If PPPOE4 is disabled Not displayed. 	Setting	Display	Enable	The message "pppoe4 dns {configuration value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).	Disable	The message "no pppoe4 dns" is displayed.
Setting	Display						
Enable	The message "pppoe4 dns {configuration value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).						
Disable	The message "no pppoe4 dns" is displayed.						
PPPOE4-ROUTE	<p>The Route setting for PPPoE (IPc4) is displayed.</p> <ul style="list-style-type: none"> When PPPOE4 is enabled <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="width: 30%;">Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "pppoe4 route {configuration value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).</td> </tr> <tr> <td>Disable</td> <td>The message "no pppoe4 route" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> If PPPOE4 is disabled Not displayed. 	Setting	Display	Enable	The message "pppoe4 route {configuration value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).	Disable	The message "no pppoe4 route" is displayed.
Setting	Display						
Enable	The message "pppoe4 route {configuration value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).						
Disable	The message "no pppoe4 route" is displayed.						
ADDRESS	<p>The IP address and prefix length are displayed as "address {configuration value}".</p>						

Item	Contents						
DHCP4	<p>DHCP (IPv4) enable setting is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "dhcp4" appears.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table> <p> Compact Router Indoor Type dhcp4 related settings are not available on the rmnet_data0 interface of the Compact Router Indoor Type.</p>	Setting	Display	Enable	The message "dhcp4" appears.	Disable	Not displayed.
Setting	Display						
Enable	The message "dhcp4" appears.						
Disable	Not displayed.						
DHCP4-DNS	<p>DHCP (IPv4) DNS settings are displayed.</p> <ul style="list-style-type: none"> When DHCP4 is enabled <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "dhcp4 dns {set value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).</td> </tr> <tr> <td>Disable</td> <td>The message "no dhcp4 dns" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> If DHCP4 is disabled Not displayed. 	Setting	Display	Enable	The message "dhcp4 dns {set value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).	Disable	The message "no dhcp4 dns" is displayed.
Setting	Display						
Enable	The message "dhcp4 dns {set value}" is displayed. The setting value contains the priority of the DNS server address that was delivered (obtained).						
Disable	The message "no dhcp4 dns" is displayed.						
DHCP4-NTP	<p>Displays the DHCP (IPv4) NTP enable/disable settings.</p> <ul style="list-style-type: none"> When DHCP4 is enabled <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "dhcp4 ntp" appears.</td> </tr> <tr> <td>Disable</td> <td>The message "no dhcp4 ntp" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> If DHCP4 is disabled Not displayed. 	Setting	Display	Enable	The message "dhcp4 ntp" appears.	Disable	The message "no dhcp4 ntp" is displayed.
Setting	Display						
Enable	The message "dhcp4 ntp" appears.						
Disable	The message "no dhcp4 ntp" is displayed.						
DHCP4-MTU	<p>Displays the DHCP (IPv4) MTU enable/disable settings.</p> <ul style="list-style-type: none"> When DHCP4 is enabled <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "dhcp4 mtu" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no dhcp4 mtu" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> If DHCP4 is disabled Not displayed. 	Setting	Display	Enable	The message "dhcp4 mtu" is displayed.	Disable	The message "no dhcp4 mtu" is displayed.
Setting	Display						
Enable	The message "dhcp4 mtu" is displayed.						
Disable	The message "no dhcp4 mtu" is displayed.						
DHCP4-ROUTE	<p>DHCP (IPv4) route settings are displayed.</p> <ul style="list-style-type: none"> When DHCP4 is enabled <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "dhcp4 route {configuration value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).</td> </tr> <tr> <td>Disable</td> <td>The message "no dhcp4 route" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> If DHCP4 is disabled Not displayed. 	Setting	Display	Enable	The message "dhcp4 route {configuration value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).	Disable	The message "no dhcp4 route" is displayed.
Setting	Display						
Enable	The message "dhcp4 route {configuration value}" is displayed. The configuration value contains the metric value of the default route that was delivered (obtained).						
Disable	The message "no dhcp4 route" is displayed.						

Item	Contents																
GATEWAY4	Gateway (IPv4) metric values are displayed.																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "gateway4 {configuration value}" is displayed.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "gateway4 {configuration value}" is displayed.	Disable	Not displayed.										
	Setting	Display															
Enable	The message "gateway4 {configuration value}" is displayed.																
Disable	Not displayed.																
<hr/>																	
GATEWAY4-VIA	The gateway (IPv4) address settings are displayed.																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "gateway4 via {configuration value}" is displayed.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "gateway4 via {configuration value}" is displayed.	Disable	Not displayed.										
	Setting	Display															
Enable	The message "gateway4 via {configuration value}" is displayed.																
Disable	Not displayed.																
<hr/>																	
DYNAMIC-SNAT4	The enable setting for dynamic SNAT (IPv4) is displayed.																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be labeled "dynamic-snat4."</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be labeled "dynamic-snat4."	Disable	Not displayed.										
	Setting	Display															
Enable	It will be labeled "dynamic-snat4."																
Disable	Not displayed.																
<hr/>																	
MTU	The MTU (Maximum Transmission Unit) value is displayed as "mtu {set value}".																
MRU	The MRU (Maximum Receive Unit) value is displayed.																
MODE	The link mode setting is displayed as "mode {set value}".																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>10BASE-T half-duplex fixed connection</td> <td>10baseT-Half</td> </tr> <tr> <td>10BASE-T full-duplex fixed connection</td> <td>10baseT-Full</td> </tr> <tr> <td>100BASE-T automatic recognition</td> <td>100baseT-Auto</td> </tr> <tr> <td>100BASE-T half-duplex fixed connection</td> <td>100baseT-Half</td> </tr> <tr> <td>100BASE-T full-duplex fixed connection</td> <td>100baseT-Full</td> </tr> <tr> <td>1000BASE-T automatic recognition</td> <td>1000baseT-Auto</td> </tr> <tr> <td>1000BASE-T full-duplex fixed connection</td> <td>1000baseT-Full</td> </tr> </tbody> </table>	Setting	Display	10BASE-T half-duplex fixed connection	10baseT-Half	10BASE-T full-duplex fixed connection	10baseT-Full	100BASE-T automatic recognition	100baseT-Auto	100BASE-T half-duplex fixed connection	100baseT-Half	100BASE-T full-duplex fixed connection	100baseT-Full	1000BASE-T automatic recognition	1000baseT-Auto	1000BASE-T full-duplex fixed connection	1000baseT-Full
	Setting	Display															
	10BASE-T half-duplex fixed connection	10baseT-Half															
	10BASE-T full-duplex fixed connection	10baseT-Full															
	100BASE-T automatic recognition	100baseT-Auto															
	100BASE-T half-duplex fixed connection	100baseT-Half															
	100BASE-T full-duplex fixed connection	100baseT-Full															
	1000BASE-T automatic recognition	1000baseT-Auto															
	1000BASE-T full-duplex fixed connection	1000baseT-Full															
	In Compact Router																
	1000baseT-Auto" and "1000baseT-Full" are Not displayed.																
<hr/>																	
PROXY-ARP	Displays the proxy ARP enable/disable settings.																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "proxy-arp" appears.</td> </tr> <tr> <td>Disable</td> <td>The message "no proxy-arp" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "proxy-arp" appears.	Disable	The message "no proxy-arp" is displayed.										
	Setting	Display															
Enable	The message "proxy-arp" appears.																
Disable	The message "no proxy-arp" is displayed.																
<hr/>																	
OPTIONAL	Displays the enable/disable setting for the interface startup wait disable function at equipment startup.																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be displayed as "optional."</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be displayed as "optional."	Disable	Not displayed.										
	Setting	Display															
	Enable	It will be displayed as "optional."															
Disable	Not displayed.																
	Not shown on Compact Router.																
<hr/>																	

Item	Contents				
WIFI-AP	<p>If an access point is configured on the interface, it will appear in the following format</p> <p style="background-color: #f0f0f0; padding: 5px;">access-point AP-NAME</p> <table border="1" data-bbox="488 300 1265 427"> <thead> <tr> <th data-bbox="488 300 703 338">Setting items</th> <th data-bbox="703 300 1265 338">Contents</th> </tr> </thead> <tbody> <tr> <td data-bbox="488 338 703 427">AP-NAME</td> <td data-bbox="703 338 1265 427">The access point identification name (SSID) is displayed.</td> </tr> </tbody> </table> <p data-bbox="488 439 1086 506">   Compact Router with wireless LAN Only wlan0 and wlan1 are displayed. </p>	Setting items	Contents	AP-NAME	The access point identification name (SSID) is displayed.
Setting items	Contents				
AP-NAME	The access point identification name (SSID) is displayed.				
WIFI-STA	<p>If the interface has a station setting, it will appear in the following format</p> <p style="background-color: #f0f0f0; padding: 5px;">access-point STA-NAME</p> <table border="1" data-bbox="488 651 1265 779"> <thead> <tr> <th data-bbox="488 651 703 689">Setting items</th> <th data-bbox="703 651 1265 689">Contents</th> </tr> </thead> <tbody> <tr> <td data-bbox="488 689 703 779">STA-NAME</td> <td data-bbox="703 689 1265 779">The station's distinguished name is displayed.</td> </tr> </tbody> </table> <p data-bbox="488 790 1086 857">   Compact Router with wireless LAN Only wlan0 and wlan1 are displayed. </p>	Setting items	Contents	STA-NAME	The station's distinguished name is displayed.
Setting items	Contents				
STA-NAME	The station's distinguished name is displayed.				

Execution example

Below is an example of running in administrator mode and advanced configuration mode on an Edge Gateway.

管理者モード

```

amnimo# show config interface ↵
# ---- transition to configure mode. ----
configure
# ---- interface eth0 configure ----
interface eth0
enable
pmtu auto
address 192.168.0.254/24
mtu 1500
mode 100baseT-Auto
proxy-arp
exit
# ---- interface lan0 configure ----
interface lan0
enable
pmtu auto
mtu 1500
mode 100baseT-Auto
proxy-arp
exit
# ---- interface lan1 configure ----
interface lan1
enable
pmtu auto
mtu 1500
mode 100baseT-Auto
proxy-arp
exit
# ---- interface lan2 configure ----
interface lan2
enable
pmtu auto
mtu 1500
mode 100baseT-Auto
proxy-arp
exit
# ---- interface lan3 configure ----
interface lan3
enable
pmtu auto
mtu 1500
mode 100baseT-Auto
proxy-arp
exit
# ---- interface br0 configure ----
interface br0
enable
bridge lan0
bridge lan1
bridge lan2
bridge lan3
mac lan0
pmtu auto
address 192.168.1.254/24

```

```
mtu 1500
proxy-arp
exit
# ---- exit configure mode. ----
exit
```

設定モード

```
amnimo(cfg)# show config ↵
amnimo(cfg-interface-eth0)# show config ↵
enable
pmtu auto
address 192.168.0.254/24
mtu 1500
mode 100baseT-Auto
proxy-arp
```



You can enter the detailed configuration mode for an interface by executing the interface command with the interface specified in the configuration mode as follows.

➔ For more information, see " 6.2.3 Configure the interface and save configuration information " for more information.

```
amnimo(cfg)# interface eth0 ↵
amnimo(cfg-interface-eth0)#.
```

6.2.3 Configure the interface and save configuration information

To configure the interface, enter the interface advanced configuration mode and execute the configuration commands. The settings made here will be written to a configuration file.

Format (Edge Gateway, IoT Router)

```

interface IFNAME
enable
no enable
bridge BRIDGE-IFNAME
no bridge BRIDGE-IFNAME
mac <auto | MAC-IFNAME | MAC-ADDRESS>.
no mac
pmtu <auto | manual [MSS]>
no pmtu
mobile MOB-PEER-NAME
no mobile
pppoe4 PPP-PEER-NAME
no pppoe4
pppoe4 dns [PRIORITY].
no pppoe4 dns
pppoe4 route [PPPOE4-ROUTE-METRIC].
no pppoe4 route
address ADDRESS/PREFIX
no address ADDRESS/PREFIX
dhcp4
no dhcp4
dhcp4 dns [PRIORITY].
no dhcp4 dns
dhcp4 ntp
no dhcp4 ntp
dhcp4 mtu
no dhcp4 mtu
dhcp4 route [DHCP4-ROUTE-METRIC].
no dhcp4 route
gateway4 via GATEWAY4-ADDRESS
gateway4 GATEWAY4-METRIC
no gateway4
dynamic-snat4
no dynamic-snat4
mtu <576 - 9676>
mru <576 - 9676>
mode <10baseT-Half | 10baseT-Full | 100baseT-Auto | 100baseT-Half | 100baseT-Full | 1000baseT-Auto | 1000baseT-Full
proxy-arp
no proxy-arp
optional
no optional
exit
no interface IFNAME

```

```

interface IFNAME
enable
no enable
bridge BRIDGE-IFNAME
no bridge BRIDGE-IFNAME
mac <auto | MAC-IFNAME | MAC-ADDRESS>.
no mac
pmtu <auto | manual [MSS]>
no pmtu
mobile MOB-PEER-NAME
no mobile
mobile dns [PRIORITY].
no mobile dns
mobile route [MOBILE-ROUTE-METRIC].
no mobile route
pppoe4 PPP-PEER-NAME
no pppoe4
pppoe4 dns [PRIORITY].
no pppoe4 dns
pppoe4 route [PPPOE4-ROUTE-METRIC].
no pppoe4 route
address ADDRESS/PREFIX
no address ADDRESS/PREFIX
dhcp4
no dhcp4
dhcp4 dns [PRIORITY].
no dhcp4 dns
dhcp4 ntp
no dhcp4 ntp
dhcp4 mtu
no dhcp4 mtu
dhcp4 route [DHCP4-ROUTE-METRIC].
no dhcp4 route
gateway4 via GATEWAY4-ADDRESS
gateway4 GATEWAY4-METRIC
no gateway4
dynamic-snat4
no dynamic-snat4
mtu <576-1500>.
mode <10baseT-Half | 10baseT-Full | 100baseT-Auto | 100baseT-Half | 100baseT-Full | 1000baseT-Auto | 1000baseT-Full
proxy-arp
no proxy-arp
optional
no optional
access-point AP-NAME
no access-point AP-NAME
station STA-NAME
no station STA-NAME
exit
no interface IFNAME

```

Command	Contents				
interface	<p>Runs by specifying the interface name.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>IFNAME</td> <td>interface.</td> </tr> </tbody> </table> <p> When an interface is specified and executed in the configuration mode, the program enters the detailed configuration mode for the specified interface.</p> <p> Configurable interface names vary by product.</p> <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, br<0-9>, ecm0, ppp<0-9> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9> ● Compact Router eth0, rmnet_data0 ● Compact Router with wireless LAN eth0, eth1, rmnet_data0, wlan0, wlan1 <p> Devices without a mobile module cannot use even if ecm0 is enabled.</p>	Setting	Contents	IFNAME	interface.
Setting	Contents				
IFNAME	interface.				
enable	Enables the interface.				
no enable	Disables the interface.				
bridge	<p>Add the interface name of the bridge.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>BRIDGE-IFNAME</td> <td>Specifies the interface of the bridge.</td> </tr> </tbody> </table> <p> Configurable interface names vary by product.</p> <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, tap<0-9>, tun<0-9> ● Edge Gateway eth0, lan<0-3>, tap<0-9>, tun<0-9> ● IoT Router eth<0-1>, tap<0-9>, tun<0-9>. ● Compact Router with wireless LAN eth0, eth1, wlan0, wlan1 <p> This command can be set only when the interface name is br<0-9>.</p> <p> Compact Router Indoor Type with wireless LAN cannot be registered as a bridge interface if wlan0 is the station setting.</p> <p> Compact Router Indoor Type routers do not have a bridge function.</p>	Setting	Contents	BRIDGE-IFNAME	Specifies the interface of the bridge.
Setting	Contents				
BRIDGE-IFNAME	Specifies the interface of the bridge.				
no bridge	<p>Deletes the bridge configuration by specifying the bridge interface name.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>BRIDGE-IFNAME</td> <td>Specifies the interface of the bridge.</td> </tr> </tbody> </table>	Setting	Contents	BRIDGE-IFNAME	Specifies the interface of the bridge.
Setting	Contents				
BRIDGE-IFNAME	Specifies the interface of the bridge.				

Command	Contents								
mac	<p>Set the MAC address of the bridge.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>MAC address is automatically assigned.</td> </tr> <tr> <td>MAC-IFNAME</td> <td>Specifies the name of the physical interface and assigns the MAC address of the concerned interface.</td> </tr> <tr> <td>MAC-ADDRESS</td> <td>Assign any MAC address.</td> </tr> </tbody> </table> <p> This can only be set if the interface name is br<0-9>. This setting is reflected after rebooting the product .</p>	Setting	Contents	auto	MAC address is automatically assigned.	MAC-IFNAME	Specifies the name of the physical interface and assigns the MAC address of the concerned interface.	MAC-ADDRESS	Assign any MAC address.
Setting	Contents								
auto	MAC address is automatically assigned.								
MAC-IFNAME	Specifies the name of the physical interface and assigns the MAC address of the concerned interface.								
MAC-ADDRESS	Assign any MAC address.								
no mac	Delete MAC address settings.								
pmtu	<p>Set the Path MTU (Path Maximum Transmission Unit).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>Path MTU is automatically set.</td> </tr> <tr> <td>manual</td> <td>Set MSS (Maximum Segment Size). Set in the range of 536 to 1460.</td> </tr> </tbody> </table>	Setting	Contents	auto	Path MTU is automatically set.	manual	Set MSS (Maximum Segment Size). Set in the range of 536 to 1460.		
Setting	Contents								
auto	Path MTU is automatically set.								
manual	Set MSS (Maximum Segment Size). Set in the range of 536 to 1460.								
no pmtu	Delete PMTU settings.								
mobile	<p>Specify the configuration name of the mobile module.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MOB-PEER-NAME</td> <td>Specify the configuration name of the mobile module. ➔ The setting name will be the name set in " 5.7 Set up a mobile line".</td> </tr> </tbody> </table> <p> It can only be set if the interface name is ecm<0-9> for Edge Gateways and IoT Routers, and rmnet_data0 for Compact Router.</p>	Setting	Contents	MOB-PEER-NAME	Specify the configuration name of the mobile module. ➔ The setting name will be the name set in " 5.7 Set up a mobile line".				
Setting	Contents								
MOB-PEER-NAME	Specify the configuration name of the mobile module. ➔ The setting name will be the name set in " 5.7 Set up a mobile line".								
no mobile	Delete mobile settings.								
mobile dns	<p>Set DNS for mobile settings.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PRIORITY</td> <td>Sets the DNS priority. Set in the range of 0 to 99. The default is "20".</td> </tr> </tbody> </table> <p>   rmnet_data0 of the Compact Router. Only the interface is available.</p>	Setting	Contents	PRIORITY	Sets the DNS priority. Set in the range of 0 to 99. The default is "20".				
Setting	Contents								
PRIORITY	Sets the DNS priority. Set in the range of 0 to 99. The default is "20".								
no mobile dns	Does not use DNS for mobile settings.								
mobile route	<p>Configures routing information for mobile settings.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MOBILE-ROUTE-METRIC</td> <td>Set the metric value. Set in the range of 0 to 255. The default is "30".</td> </tr> </tbody> </table> <p>   rmnet_data0 of the Compact Router. Only the interface is available.</p>	Setting	Contents	MOBILE-ROUTE-METRIC	Set the metric value. Set in the range of 0 to 255. The default is "30".				
Setting	Contents								
MOBILE-ROUTE-METRIC	Set the metric value. Set in the range of 0 to 255. The default is "30".								
no mobile route	Does not use routing information for mobile settings.								
pppoe4	<p>Configure PPPoE (IPv4).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PPP-PEER-NAME</td> <td>Specify the name of the PPP configuration. ➔ The setting name will be the name set in " 6.1.5 Configure PPP settings. ".</td> </tr> </tbody> </table> <p> Can only be set if the interface name is ppp<0-9>.</p>	Setting	Contents	PPP-PEER-NAME	Specify the name of the PPP configuration. ➔ The setting name will be the name set in " 6.1.5 Configure PPP settings. ".				
Setting	Contents								
PPP-PEER-NAME	Specify the name of the PPP configuration. ➔ The setting name will be the name set in " 6.1.5 Configure PPP settings. ".								

Command	Contents		
no pppoe4	Delete PPPoE (IPv4) settings.		
pppoe4 dns	Configure DNS for PPPoE (IPv4).		
	Setting	Contents	PRIORITY
Setting	Contents		
PRIORITY	Sets the DNS priority. Set in the range of 0 to 99. The default is "20".		
no pppoe4 dns	PPPoE (IPv4) DNS is not used.		
pppoe4 route	Configures PPPoE (IPv4) routing information.		
	Setting	Contents	PPPOE4-ROUTE-METRIC
Setting	Contents		
PPPOE4-ROUTE-METRIC	Set the metric value. Set in the range of 0 to 255. The default is "30".		
no pppoe4 route	PPPoE (IPv4) routing information is not used.		
address	Add a static IP address.		
	Setting	Contents	ADDRESS/PREFIX
Setting	Contents		
ADDRESS/PREFIX	Specify IP address/prefix.		
no address	Delete the static IP address.		
dhcp4	Configure DHCP (IPv4) client.		
no dhcp4	Deletes DHCP (IPv4) clients.		
dhcp4 dns	Configure DNS for DHCP (IPv4) clients.		
	Setting	Contents	PRIORITY
Setting	Contents		
PRIORITY	Sets the DNS priority. Set in the range of 0 to 99. The default is "30".		
no dhcp4 dns	DHCP (IPv4) client DNS is not used.		
dhcp4 ntp	Configure NTP for DHCP (IPv4) clients.		
no dhcp4 ntp	Does not use NTP for DHCP (IPv4) clients.		
dhcp4 mtu	Sets the MTU for the DHCP (IPv4) client.		
no dhcp4 mtu	No MTU for DHCP (IPv4) clients.		

Command	Contents		
dhcp4 route	Configures routing information for DHCP (IPv4) clients.		
	Setting	Contents	DHCP4-ROUTE-METRIC
Setting	Contents		
DHCP4-ROUTE-METRIC	Set the metric value. Set in the range of 0 to 255. The default is "30".		
no dhcp4 route	DHCP (IPv4) client routing information is not used.		
gateway4 via	Set the IP address of the gateway.		
	Setting	Contents	GATEWAY4-ADDRESS
Setting	Contents		
GATEWAY4-ADDRESS	Specify the IP address of the gateway.		
gateway4	Change the metric value of the gateway.		
	Setting	Contents	GATEWAY4-METRIC
Setting	Contents		
GATEWAY4-METRIC	Specifies the metric value of the gateway. Set in the range of 0 to 255.		
no gateway4	Delete gateway settings.		
dynamic-snat4	Set up a dynamic SNAT.  Interface lan<0-3> cannot be set.		
no dynamic-snat4	Delete dynamic SNAT settings.		

Command	Contents																
mtu	<p>Set the MTU (Maximum Transmission Unit). Set the value in the range from 576 to 9676. Default is "1500".</p> <p> The default is "1454" only if the interface name is ppp<0-9>.</p> <p> On Compact Router, eth0 can only be set to "1500" and rmnet_data0 can be set in the range of 576 to 1500.</p> <p> In AI Edge Gateway, wan0, lan<0-3> can be set from 576 to 1500.</p> <p> For version 2.1.0 or later of the Edge Gateway, the maximum value is 9668.</p>																
mru	<p>Set the MRU (Maximum Receive Unit). Set the range from 576 to 9676. The default is "1454".</p> <p> Can only be set if the interface name is ppp<0-9>.</p>																
mode	<p>Set the mode of the interface.</p> <table border="1" data-bbox="507 660 1284 996"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>10baseT-Half</td> <td>10BASE-T half-duplex fixed connection</td> </tr> <tr> <td>10baseT-Full</td> <td>10BASE-T full-duplex fixed connection</td> </tr> <tr> <td>100baseT-Auto</td> <td>100BASE-T automatic recognition</td> </tr> <tr> <td>100baseT-Half</td> <td>100BASE-T half-duplex fixed connection</td> </tr> <tr> <td>100baseT-Full</td> <td>100BASE-T full-duplex fixed connection</td> </tr> <tr> <td>1000baseT-Auto</td> <td>1000BASE-T automatic recognition</td> </tr> <tr> <td>1000baseT-Full</td> <td>1000BASE-T full-duplex fixed connection</td> </tr> </tbody> </table> <p> The interface name can only be set if it matches one of the following</p> <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3> ● Edge Gateway eth0, lan<0-3>. ● IoT Router eth<0-1> ● Indoor Compact Router eth0 ● Compact Router Indoor Type / Outdoor Type with wireless LAN lan<0-1> <p> "1000baseT-Auto" and "1000baseT-Full" cannot be set for the indoor type Compact Router.</p> <p> Compact Router Indoor Type / Outdoor Type Compact Router Indoor Type with wireless LAN is fixed to "100baseT-Auto".</p>	Setting	Contents	10baseT-Half	10BASE-T half-duplex fixed connection	10baseT-Full	10BASE-T full-duplex fixed connection	100baseT-Auto	100BASE-T automatic recognition	100baseT-Half	100BASE-T half-duplex fixed connection	100baseT-Full	100BASE-T full-duplex fixed connection	1000baseT-Auto	1000BASE-T automatic recognition	1000baseT-Full	1000BASE-T full-duplex fixed connection
Setting	Contents																
10baseT-Half	10BASE-T half-duplex fixed connection																
10baseT-Full	10BASE-T full-duplex fixed connection																
100baseT-Auto	100BASE-T automatic recognition																
100baseT-Half	100BASE-T half-duplex fixed connection																
100baseT-Full	100BASE-T full-duplex fixed connection																
1000baseT-Auto	1000BASE-T automatic recognition																
1000baseT-Full	1000BASE-T full-duplex fixed connection																
proxy-arp	Set proxy ARP.																
no proxy-arp	Delete proxy ARP.																
optional	<p>Sets the function to disable interface startup wait for equipment startup.</p> <p>   Compact Router cannot be configured.</p>																
no optional	Delete the interface startup wait disable function at equipment startup.																
access-point	<p>Sets the function to disable interface startup wait for equipment startup.</p> <p>  Only Compact Router with wireless LAN can be configured.</p>																
no access-point	Delete the interface startup wait disable function at equipment startup.																

Command	Contents
station	Sets the function to disable interface startup wait for equipment startup.  Only Compact Router with wireless LAN can be configured.
no station	Delete the interface startup wait disable function at equipment startup.
exit	Exit the detailed setting mode and enter the setting mode.
no interface	Deletes the interface specified for IFNAME.

Execution example 1

Change the IP address of eth0 from the DHCP client (default) to the fixed IP address 192.168.254.254/24.

設定 モード

```
amnimo(cfg)# interface eth0 ↵
amnimo(cfg-interface-eth0)# no dhcp4 ↵
amnimo(cfg-interface-eth0)# address 192.168.254.254/24 ↵
```

Execution example 2

Add eth0 as a bridge interface to br0 in the default configuration state.

設定 モード

```
amnimo(cfg)# interface eth0 ↵
amnimo(cfg-interface-eth0)# no dhcp4↵↵ ← Disable eth0 because its default setting is DHCP
amnimo(cfg-interface-eth0)# exit ↵
amnimo(cfg)# interface br0 ↵
amnimo(cfg-interface-br0)# bridge eth0 ↵
amnimo(cfg-interface-br0)# show config ↵
enable
bridge lan0
bridge lan1
bridge lan2
bridge lan3
bridge eth0
mac lan0
pmtu auto
address 192.168.0.254/24
mtu 1500
proxy-arp
no optional
```



- Interfaces to be added to the bridge interface must be enabled.
- If the interface to be added to the bridge interface has DHCP settings or fixed IP address settings, disable them.

Execution example 3

Set the mobile's interface to ecm0 along the

設定 モード

```
amnimo(cfg)# interface ecm0 ↵
amnimo(cfg-interface-ecm0)# mobile amnimo ↵
amnimo(cfg-interface-ecm0)# dhcp4 ↵
amnimo(cfg-interface-ecm0)# enable ↵
amnimo(cfg-interface-ecm0)# show config ↵
enable
pmtu auto
mobile amnimo
dhcp4
dhcp4 dns 30
dhcp4 ntp
dhcp4 mtu
dhcp4 route 30
mtu 1500
proxy-arp
no optional
```

Execution example 4

Configure the PPPoE interface to ppp0 according to the example in "6.1.5 Configure PPP settings."

設定 モード

```
amnimo(cfg)# interface ppp0 ↵
amnimo(cfg-interface-ppp0)# pppoe4 amnimo-ppp ↵
amnimo(cfg-interface-ppp0)# enable ↵
amnimo(cfg-interface-ppp0)# show config ↵
enable
pmtu auto
pppoe4 amnimo-ppp
pppoe4 dns 20
pppoe4 route 20
mtu 1454
mru 1454
proxy-arp
no optional
```

6.3 Configure routing settings.



Displays the routing table and routing settings and configures static routing.

6.3.1 Display the routing table

To view the routing table, run the *show routing* command.

Format

```
show routing
```

Output Format

```
TO          VIA          METRICINTERFACE    ← Header line
TO         VIA         METRIC IFNAME
(Omitted.)
```

Output item

Item	Contents
TO	The destination network is displayed.
VIA	The gateway address is displayed.
METRIC	Metric values are displayed.
IFNAME	The interface name is displayed.

Execution example (Edge Gateway, IoT Router)

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```
amnimo$ show routing ↵
TO          VIA          METRICINTERFACE
default     192.168.0.  10eth0
192.168.0.0/240  .0.0.0      0eth0
192.168.1.0/240  .0.0.0      0br0
```

Execution example (Compact Router)

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```
amnimo$ show routing ↵
Status: K - kernel route, C - connected, S - static
> - selected route, * - FIB route
STATUS TO          VIA          METRIC INTERFACE
S>*    0.0.0.0/0      172.16.0.1   10    eth0
C>*    127.0.0.0/8    0.0.0.0      10    lo      ← Not displayed if metric value is
s set automatically.
C>*    172.16.0.0/24 0.0.0.0      10    eth0    ← Not displayed if metric value is set au
tomatically.
```

6.3.2 Display routing settings

To view the routing configuration, run the *show config routing static* command.

Format

```
show config routing static [STATIC-ROUTE-NAME].
```

Setting items

Item	Contents
STATIC-ROUTE-NAME	Specify a static routing name.

Output Format

```
# ---- transition to configure mode ----
configure
# ---- routing static STATIC-ROUTE-NAME configure ----
TO-ADDRESS
VIA-ADDRESS
INTERFACE
METRIC
# ---- exit configure mode ----
exit
```

Output item

Item	Contents
STATIC-ROUTE-NAME	The static routing name is displayed.
TO-ADDRESS	The destination network address is displayed.
VIA-ADDRESS	The gateway IP address in route is displayed.
INTERFACE	The interface to which the route is assigned is displayed.
METRIC	Metric values on the route are displayed.

Execution example

管理者 モード 設定 モード

```
amnimo(cfg)# show config routing static default ↵
# ---- routing static default configure ----
routing static default
to 0.0.0.0/0
via 192.168.0.1
metric 0
exit
```

6.3.3 Configure routing table settings.

To configure routing, go to the advanced configuration mode for static routing and execute the configuration commands.

The settings made here are written to a configuration file.

Format

```
routing static STATIC-ROUTE-NAME
to TO-ADDRESS/PREFIX
via VIA-ADDRESS
interface IFNAME
metric METRIC
exit
no routing static STATIC-ROUTE-NAME
```

Command

Command	Contents
routing static STATIC-ROUTE-NAME	Execute with a static routing name in STATIC-ROUTE-NAME.  When a static routing name is specified in the configuration mode and executed, the program enters the detailed configuration mode for the specified routing name.
to	Set the destination network address.
via	Sets the gateway IP address in the route.
interface	Set the interface.
metric	Set the metric.
exit	Exit the detailed setting mode and enter the setting mode.
no routing static	Delete static routing configuration.



The gateway IP address and interface cannot be set at the same time.

Execution example

Here is an example of routing configuration in the following environment

interface	Configuration details
eth0	192.168.0.254/24 (fixed IP)

設定モード

Set default route via gateway 1 (192.168.0.1)

```
amnimo(cfg)# routing static default ↵
amnimo(cfg-rts-default)# to 0.0.0.0/0 ↵
amnimo(cfg-rts-default)# via 192.168.0.1 ↵
amnimo(cfg-rts-default)# exit ↵
```

Set route to network A (172.16.1.0/24) connected beyond gateway 2 (192.168.0.2)

```
amnimo(cfg)# routing static network_a ↵
amnimo(cfg-rts-network_a)# to 172.16.1.0/24 ↵
amnimo(cfg-rts-network_a)# via 192.168.0.2 ↵
amnimo(cfg-rts-network_a)# exit ↵
```

Delete route configuration to network A (172.16.1.0/24)

```
amnimo(cfg)# no routing static network_a ↵
```

6.4 Configure packet filtering settings.



Configures and displays packet filtering settings.

In packet filtering, packet matching conditions are set for packet input (input), output (output), and forward (forward), as well as policies for how to handle packets when they match.

A combination of matching conditions and policies is called a rule. If multiple rules are set, they are checked in order of decreasing INDEX. If a rule is applied, the rules in the subsequent INDEXes will not be checked. If none of the rules are applied, the default policy is applied.

6.4.1 Display packet filtering settings

To view packet filtering settings, run the *show config filter* command.

Format

```
show config filter < input | output | forward >
```

Setting items

Item	Contents
input	Specify to display packet filtering settings for input (input).
output	Specify to display packet filtering settings for output (output).
forward	Specify to display packet filtering settings for forwarding (forward).

Output Format

```
When displaying packet filtering settings for input (input)
# ---- transition to configure mode ----
configure
# ---- filter input configure ----
filter input default-policy DEFAULT-POLICY
# ---- rule INDEX ----
filter input INDEX
ENABLE
policy POLICY REJECT-CODE
(Logs and packet match condition settings are displayed)
exit
# ---- exit configure mode ----
exit
(Omitted below.)
```

```
When packet filtering settings for output (output) are displayed
# ---- transition to configure mode ----
configure
# ---- filter output configure ----
filter output default-policy DEFAULT-POLICY
# ---- rule INDEX ----
filter output rule INDEX
ENABLE
policy POLICY REJECT-CODE
(Logs and packet match condition settings are displayed)
exit
# ---- exit configure mode ----
exit
```

```
When packet filtering settings for forwarding (forward) are displayed
```

```
# ---- transition to configure mode ----
configure
# ---- filter forward configure ----
filter forward default-policy DEFAULT-POLICY
# ---- rule INDEX ----
filter forward rule INDEX
ENABLE
policy POLICY REJECT-CODE
(Logs and packet match condition settings are displayed)
exit
# ---- exit configure mode ----
exit
```



See the following page for information on logging and displaying packet match condition settings.

- ➔ 6.6.1 Display packet matching condition settings
- ➔ 6.6.4 Display log output settings'

Output item

Item	Contents						
DEFAULT-POLICY	The default policy is displayed.						
INDEX	The index number of the rule is displayed.						
ENABLE	Information is displayed when the filter is enabled/disabled. <table border="1" data-bbox="571 1016 1353 1146"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
POLICY	Policy settings are displayed.						
REJECT-CODE	If a reject is specified for POLICY, an error response is displayed.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo(cfg)# show config filter forward ↵
# ---- filter forward configure ----
filter forward default-policy accept
# ---- rule 100 ----
filter forward 100
enable
policy drop
match protocol udp dst-port 137:138
exit
# ---- rule 110 ----
filter forward 110
enable
policy drop
match protocol udp src-port 137:138
exit
# ---- rule 120 ----
filter forward 120
enable
policy drop
match protocol tcp dst-port 137
exit
# ---- rule 130 ----
filter forward 130
enable
policy drop
match protocol tcp src-port 137
exit
# ---- rule 140 ----
filter forward 140
enable
policy drop
match protocol tcp dst-port 139
exit
# ---- rule 150 ----
filter forward 150
enable
policy drop
match protocol tcp src-port 139
exit
# ---- rule 160 ----
filter forward 160
enable
policy drop
match protocol tcp dst-port 445
exit
# ---- rule 170 ----
filter forward 170
enable
policy drop
match protocol tcp src-port 445
exit
```

6.4.2 Set default policy for packet filtering

To set the default policy, run the filter command with either input (input), output (output), or forward (forward).

Format

```
filter < input | output | forward > default-policy < accept | drop >
```

Setting items

Item	Contents
input	Specify if you want to set the default policy for input (input).
output	Specify if you want to set the default policy for output.
forward	Specify if you want to set the default policy for forwarding.
accept	Receives packets.
drop	Discards the packet. No error response is given.

Execution example

設定モード

```
amnimo(cfg)# filter input default-policy accept ← ← Set accept as default policy f
or input
```

6.4.3 Configure packet filtering rules

To configure packet filtering rules, go to the advanced rule configuration mode and execute the configuration command. The settings made here will be written to a configuration file.

Format

```

filter <input | output | forward> INDEX
enable
no enable
policy < accept |
    drop | (in Japanese only)
    reject [icmp-net-unreachable |
        icmp-port-unreachable |
        icmp-host-unreachable |
        icmp-proto-unreachable |
        icmp-net-prohibited |
        icmp-host-prohibited |
        icmp-admin-prohibited] >
match ... (Commands defined in the packet match condition setting control can be issued here.)
log ... (Commands defined in the log output configuration can be issued here)
exit
no filter <input | output | forward> INDEX
    
```

Command

Command	Contents																						
filter input INDEX filter output INDEX filter forward INDEX	<p>Specify input, output, or forward as the destination to which the rule is to be added, specify the index number of the packet filtering rule in INDEX, and execute the command.</p> <ul style="list-style-type: none"> The index number ranges from 1 to 1000 and specifies the order in which the rules are checked. Values do not have to be sequential but will be checked in decreasing order of value. Executing a command in the configuration mode specifying the index number of a rule will enter the detailed configuration mode for the specified rule. 																						
enable	Enables the rule.																						
no enable	Disables the rule.																						
policy	<p>Set policy.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>accept</td> <td>Receives packets.</td> </tr> <tr> <td>drop</td> <td>Discards the packet. No error response is given.</td> </tr> <tr> <td>reject</td> <td>Reject packet. Error response.</td> </tr> </tbody> </table> <p>If "reject" is set, it specifies what kind of error response is made.</p> <table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>icmp-net-unreachable</td> <td>Destination network unreachable.</td> </tr> <tr> <td>icmp-port-unreachable</td> <td>Destination port unreachable.</td> </tr> <tr> <td>icmp-host-unreachable</td> <td>Destination host unreachable.</td> </tr> <tr> <td>icmp-proto-unreachable</td> <td>Protocol unreachable.</td> </tr> <tr> <td>icmp-net-prohibited</td> <td>Forwarding to the destination network is prohibited.</td> </tr> <tr> <td>icmp-host-prohibited</td> <td>Forwarding to the destination host is prohibited.</td> </tr> </tbody> </table>	Setting	Display	accept	Receives packets.	drop	Discards the packet. No error response is given.	reject	Reject packet. Error response.	Item	Contents	icmp-net-unreachable	Destination network unreachable.	icmp-port-unreachable	Destination port unreachable.	icmp-host-unreachable	Destination host unreachable.	icmp-proto-unreachable	Protocol unreachable.	icmp-net-prohibited	Forwarding to the destination network is prohibited.	icmp-host-prohibited	Forwarding to the destination host is prohibited.
Setting	Display																						
accept	Receives packets.																						
drop	Discards the packet. No error response is given.																						
reject	Reject packet. Error response.																						
Item	Contents																						
icmp-net-unreachable	Destination network unreachable.																						
icmp-port-unreachable	Destination port unreachable.																						
icmp-host-unreachable	Destination host unreachable.																						
icmp-proto-unreachable	Protocol unreachable.																						
icmp-net-prohibited	Forwarding to the destination network is prohibited.																						
icmp-host-prohibited	Forwarding to the destination host is prohibited.																						

Command	Contents	
	icmp-admin-prohibited	Forwarding is prohibited by the administrator.
match	Sets packet match conditions. → 6.6.2 Set packet matching conditions	
log	Set log output. → 6.6.5 Configure log output	
exit	Exit the detailed setting mode and enter the setting mode.	
no filter input INDEX no filter output INDEX no filter forward INDEX	Specify an index number in INDEX to delete packet filtering rules.	

Execution example

設定モード

```
amnimo(cfg)# filter input 100 ↵
amnimo(cfg-fin-100)# policy drop ↵      ← Set policy drop for packet input match condition #100
amnimo(cfg-fin-100)# exit ↵
```

6.5 Configure NAT settings.



Configures and displays settings for dynamic SNAT, static SNAT, and DNAT.

6.5.1 Display NAT settings

To view the NAT configuration, run the *show config nat* command.

Format

```
show config nat < dynamic-snat | static-snat | dnat >
```

Setting items

Item	Contents
dynamic-snat	Specify if you want to view dynamic SNAT (dynamic-snat) settings.
static-snat	Specify if you want to display static SNAT (static-snat) settings.
dnat	Specify if you want to display DNAT (dnat) settings.

Output Format

```
When dynamic SNAT (dynamic-snat) settings are displayed
# ---- transition to configure mode ----
configure
# ---- nat dynamic-snat configure ----
# ---- rule INDEX ----
nat dynamic-snat INDEX
ENABLE
OUT-INTERFACE
TO-PORT
(Logs and packet match condition settings are displayed)
exit
# ---- exit configure mode ----
exit

When static SNAT (static-snat) settings are displayed
# ---- transition to configure mode ----
configure
# ---- nat static-snat configure ----
# ---- rule INDEX ----
nat static-snat INDEX
ENABLE
out-interface OUT-INTERFACE
to-ip TO-IP
(Logs and packet match condition settings are displayed)
exit
# ---- exit configure mode ----
exit

When DNAT (dnat) settings are displayed
# ---- transition to configure mode ----
configure
# ---- nat dnat configure ----
# ---- rule INDEX ----
nat dnat INDEX
ENABLE
in-interface IN-INTERFACE
to-ip TO-IP
(Logs and packet match condition settings are displayed)
exit
```

```
# ---- exit configure mode ----
exit
```



See the following page for information on logging and displaying packet match condition settings.

- ➔ 6.6.1 Display packet matching condition settings
- ➔ 6.6.4 Display log output settings

Output item

Item	Contents						
INDEX	The index number of the NAT setting is displayed.						
ENABLE	Information is displayed when NAT rules are enabled/disabled. <table border="1" data-bbox="571 573 1353 703"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
OUT-INTERFACE	The output interface settings are displayed.						
IN-INTERFACE	The input interface settings are displayed.						
TO-PORT	If to-port is set, "to-port {destination port}" is displayed; if to-port is not set, "no to-port" is not displayed.						
TO-IP	The destination IP address is displayed.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

When dynamic SNAT (dynamic-snat) settings are displayed

```
amnimo# show config nat dynamic-snat ↵
# ---- transition to configure mode. ----
configure
# ---- nat dynamic-snat configure ----
# ---- rule 100 ----
nat dynamic-snat 100
enable
exit
# ---- exit configure mode. ----
exit
```

When static SNAT (static-snat) settings are displayed

```
amnimo# show config nat static-snat ↵
# ---- transition to configure mode. ----
configure
# ---- nat static-snat configure ----
# ---- rule 100 ----
nat static-snat 100
enable
out-interface eth0
to-ip 234.192.0.10
exit
# ---- exit configure mode. ----
exit
```

When DNAT (dnat) settings are displayed

```
amnimo# show config nat dnat ↵
```

```
# ---- transition to configure mode. ----
configure
# ---- nat dnat configure ----
# ---- rule 100 ----
nat dnat 100
enable
in-interface eth0
to-ip 234.192.0.10
exit
# ---- exit configure mode. ----
exit
```

6.5.2 Configuring Dynamic SNAT

To configure dynamic SNAT, go to advanced configuration mode and execute the configuration command.

The settings made here are written to a configuration file.

Format

```
nat dynamic-snat INDEX
enable
no enable
out-interface [not] IFNAME
to-port PORT[-PORT].
no to-port
match ...      (Commands defined in the packet match condition setting control can be issued here.)
log ...       (Commands defined in the log output configuration can be issued here)
exit
no nat dynamic-snat INDEX
```

Command

Command	Contents						
nat dynamic-snat	<p>Specify the index number of the dynamic SNAT rule in INDEX and execute the command.</p>  <ul style="list-style-type: none"> The index number ranges from 1 to 1000 and specifies the order in which the rules are checked. Values do not have to be sequential but will be checked in decreasing order of value. Executing a command in the configuration mode specifying the index number of a rule will enter the detailed configuration mode for the specified rule. 						
enable	Enables the rule.						
no enable	Disables the rule.						
out-interface	<p>Specifies the source interface to which dynamic SNAT is applied.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>IFNAME</td> <td>Specifies the source interface.</td> </tr> </tbody> </table>	Setting	Display	not	Reverses the condition specified below.	IFNAME	Specifies the source interface.
Setting	Display						
not	Reverses the condition specified below.						
IFNAME	Specifies the source interface.						
to-port	<p>Specifies the port to which the dynamic SNAT is converted (optional setting).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>PORT[-PORT].</td> <td>Specifies the port range to be converted.</td> </tr> </tbody> </table>	Setting	Display	PORT[-PORT].	Specifies the port range to be converted.		
Setting	Display						
PORT[-PORT].	Specifies the port range to be converted.						
no to-port	Deletes the setting for the port to be converted.						

Command	Contents
match	Sets packet match conditions. ➔ 6.6.2 Set packet matching conditions
log	Configure log output. ➔ 6.6.5 Configure log output
exit	Exit the detailed setting mode and enter the setting mode.
no nat dynamic-snat	Deletes the dynamic SNAT rule for the specified INDEX.

Execution example 1

The following is an example of rewriting the source address 192.168.0.x of a packet sent from a device with IP address 192.168.0.x/24 to an IP address dynamically obtained by DHCP of eth0 and sending it to the eth0 side.

interface	IP address
eth0	(DHCP client)
br0	192.168.0.1/24

設定モード

```
amnimo(cfg)# nat dynamic-snat 101 ← Specify rule number
amnimo(cfg-dsnat-101)# out-interface eth0 ← Specify outgoing interface
amnimo(cfg-dsnat-101)# match src-ip 192.168.0.0/24 ← Specify source network address
amnimo(cfg-dsnat-101)# enable ←
amnimo(cfg-dsnat-101)# exit ←
```

Execution example 2

The following is an example of setting up a dynamic-snat rule that translates packets sent from the source (network address: 192.168.0.0/24) to the destination (network address: 172.16.0.0/24) to the IP address configured on the interface (eth0) for the source IP address. Here is an example of configuring a dynamic-snat rule that translates packets sent to the source IP address to the IP address configured on the interface (eth0)

設定モード

```
amnimo(cfg)# nat dynamic-snat 102 ← Specify rule number
amnimo(cfg-dsnat-102)# out-interface eth0 ← Specify outgoing interface
amnimo(cfg-dsnat-102)# match src-ip 192.168.0.0/24 ← Specify source network address
amnimo(cfg-dsnat-102)# match dst-ip 172.16.0.0/16 ← Specify destination network address
amnimo(cfg-dsnat-102)# enable ←
amnimo(cfg-dsnat-102)# exit ←
```

About the "dynamic-snat4" setting for interface functions

Dynamic SNAT can be easily configured by enabling the dynamic-snat4 function in the settings described in "6.2.3 Configure the interface and save configuration information".

Execution example

If there is an interface with a fixed IP (Ex. br0 is set to 192.168.0.254/24) connected to other than eth0, packets coming from that network will be subject to SNAT and will be translated to the IP address of eth0 as an example of execution.

設定モード

```
amnimo(cfg)# interface eth0 ← Specify outgoing interface eth0
amnimo(cfg-interface-eth0)# dynamic-snat4 ← Specify dynamic SNAT
```

```
amnimo(cfg-interface-eth0)# exit ↵
```

6.5.3 Setting up a static SNAT

To configure a static SNAT, go to Advanced Configuration mode and execute the configuration commands.

The settings made here are written to a configuration file.

Format

```
nat static-snat INDEX
enable
no enable
out-interface [not] IFNAME
to-ip ADDRESS[-ADDRESS][:PORT[-PORT]]
match ... (Commands defined in the packet match condition setting control can be issued here.)
log ... (Commands defined in the log output configuration can be issued here)
exit
no nat static-snat INDEX
```

Command

Command	Contents						
nat static-snat INDEX	Specify the index number of the static SNAT rule in INDEX and execute the command. <ul style="list-style-type: none"> The index number ranges from 1 to 1000 and specifies the order in which the rules are checked. Values do not have to be sequential but will be checked in decreasing order of value. Executing a command in the configuration mode specifying the index number of a rule will enter the detailed configuration mode for the specified rule. 						
enable	Enables the rule.						
no enable	Disables the rule.						
out-interface	Specifies the source interface to which static SNAT is applied. <table border="1" data-bbox="571 1328 1351 1491"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>IFNAME</td> <td>Specifies the source interface.</td> </tr> </tbody> </table>	Setting	Display	not	Reverses the condition specified below.	IFNAME	Specifies the source interface.
Setting	Display						
not	Reverses the condition specified below.						
IFNAME	Specifies the source interface.						
to-ip	Specifies the static SNAT's translating IP address and port. <table border="1" data-bbox="571 1547 1351 1664"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>ADDRESS[-ADDRESS S][:PORT[-PORT]]</td> <td>Specify the range of IP addresses and port numbers to be converted.</td> </tr> </tbody> </table>	Setting	Display	ADDRESS[-ADDRESS S][:PORT[-PORT]]	Specify the range of IP addresses and port numbers to be converted.		
Setting	Display						
ADDRESS[-ADDRESS S][:PORT[-PORT]]	Specify the range of IP addresses and port numbers to be converted.						
match	Sets packet match conditions. <p>➔ 6.6.2 Set packet matching conditions</p>						
log	Set log output. <p>➔ 6.6.5 Configure log output</p>						
exit	Exit the detailed setting mode and enter the setting mode.						
no nat dynamic-snat	Deletes the static SNAT rules for the specified INDEX.						

Execution example

The following is an example of rewriting the source address 192.168.0.x of a packet sent from a device with IP address 192.168.0.x/24 to eth0 IP address 10.0.0.1 and sending it to the eth0 side.

interface	IP address
eth0	10.0.0.1/24
br0	192.168.0.1/24

設定モード

```
amnimo(cfg)# nat static-snat 100 ← Specify rule number
amnimo(cfg-ssnat-100)# out-interface eth0 ←
amnimo(cfg-ssnat-100)# to-ip 10.0.0.1 ←
amnimo(cfg-ssnat-100)# match src-ip 192.168.0.0/24 ←
amnimo(cfg-ssnat-100)# enable ←
amnimo(cfg-ssnat-100)# exit ←
```

6.5.4 Set DNAT

To configure DNAT, enter the advanced configuration mode and execute the configuration command.

The settings made here are written to a configuration file.

Format

```

nat dnat INDEX
enable
no enable
in-interface [not] IFNAME
to-ip ADDRESS[-ADDRESS][:PORT[-PORT]]
match ...      (Commands defined in the packet match condition setting control can be issued here.)
log ...      (Commands defined in the log output configuration can be issued here)
exit
no nat dnat INDEX

```

Command

Command	Contents						
nat dnat	Specify the index number of the DNAT rule in INDEX and execute the command. <ul style="list-style-type: none"> ● The index number ranges from 1 to 1000 and specifies the order in which the rules are checked. Values do not have to be sequential but will be checked in decreasing order of value. ● Executing a command in the configuration mode specifying the index number of a rule will enter the detailed configuration mode for the specified rule. 						
enable	Enables the rule.						
no enable	Disables the rule.						
in-interface	Specifies the source interface to which DNAT is applied. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>IFNAME</td> <td>Specifies the source interface.</td> </tr> </tbody> </table>	Setting	Display	not	Reverses the condition specified below.	IFNAME	Specifies the source interface.
Setting	Display						
not	Reverses the condition specified below.						
IFNAME	Specifies the source interface.						
to-ip	Specify the IP address and port for DNAT translation. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>ADDRESS[-ADDRESS S][:PORT[-PORT]]</td> <td>Specify the range of IP addresses and port numbers to be converted.</td> </tr> </tbody> </table>	Setting	Display	ADDRESS[-ADDRESS S][:PORT[-PORT]]	Specify the range of IP addresses and port numbers to be converted.		
Setting	Display						
ADDRESS[-ADDRESS S][:PORT[-PORT]]	Specify the range of IP addresses and port numbers to be converted.						
match	Sets packet match conditions. ➔ 6.6.2 Set packet matching conditions						
log	Configure log output. ➔ 6.6.5 Configure log output						
exit	Exit the detailed setting mode and enter the setting mode.						
no nat dnat	Deletes the DNAT rule for the specified INDEX.						

Execution example

The following is an example of executing a packet received on port 11080 of eth0 and forwarded to port 80 of 192.168.0.200 of the connected device on the private network under br0.

設定 モード

```
amnimo(cfg)# nat dnat 101 ← Specify rule number
amnimo(cfg-dnat-101)# in-interface eth0 ← Specify receiving interface
amnimo(cfg-dnat-101)# to-ip 192.168.0.200:80 ← Specify destination IP address and port
amnimo(cfg-dnat-101)# match protocol tcp dst-port 11080 ← Specify packet match condition
amnimo(cfg-dnat-101)# enable ←
amnimo(cfg-dnat-101)# exit ←
```

6.6 Configure common settings for packet filtering and NAT



Packet filtering and NAT share the same configuration items for logging and packet match conditions.

6.6.1 Display packet matching condition settings

The items that appear as settings for packet matching conditions are shown below.

Output Format

```

SRC-IP
DST-IP
IN-IFNAME
OUT-IFNAME
MAC-ADDRESS
PKT-TYPE
ICMP
TCP-SRC-PORT
TCP-DST-PORT
TCP-FLAG
UDP-SRC-PORT
UDP-DST-PORT
AH-SPI
ESP-SPI
PROTOCOL-NUMBER
CONNTRACK-STATE
CONNTRACK-PROTO
CONNTRACK-ORIGSRC-IP
CONNTRACK-ORIGDST-IP
CONNTRACK-ORIGDST-IP
CONNTRACK-ORIGDST-IP
CONNTRACK-ORIGSRC-PORT
CONNTRACK-ORIGDST-PORT
CONNTRACK-REPLSRC-PORT
CONNTRACK-REPLDST-PORT
CONNTRACK-STATUS
CONNTRACK-DIRECTION
HASHLIMIT-UPTO
HASHLIMIT-ABOVE
HASHLIMIT-BURST
HASHLIMIT-MODE
HASHLIMIT-SRC-MASK
HASHLIMIT-DST-MASK
LIMIT-RATE
LIMIT-BURST

```

Output item

Item	Contents
SRC-IP	The source IP address is displayed.
DST-IP	The destination IP address is displayed.
IN-IFNAME	The input interface name is displayed.
OUT-IFNAME	The output interface name is displayed.
MAC-ADDRESS	The MAC address is displayed.
PKT-TYPE	The packet type is displayed.

Item	Contents
ICMP	If "match protocol icmp" is set, "match protocol icmp {Response Error}" is displayed. When "match protocol icmp" is not set (when "no match protocol icmp" is executed), it is not displayed.
TCP-SRC-PORT	If "match protocol tcp src-ip" is set, "match protocol tcp src-ip {source IP address of TCP packets}" will be displayed. Not displayed when "match protocol tcp src-ip" is not set (when "no match protocol tcp src-ip" is executed).
TCP-DST-PORT	If "match protocol tcp dst-ip" is set, "match protocol tcp dst-ip {IP address to which TCP packets are sent}" will be displayed. Not displayed when "match protocol tcp dst-ip" is not set (when "no match protocol tcp dst-ip" is executed).
TCP-FLAG	If "match protocol tcp flags" is set, "match protocol tcp flags {flags to be checked for TCP packets} {flags set among those to be checked}" is displayed. When "match protocol tcp flags" is not set (when "no match protocol tcp flags" is executed), it is not displayed.
UDP-SRC-PORT	If "match protocol udp src-ip" is set, "match protocol udp src-ip {source IP address of UDP packets}" will be displayed. Not displayed when "match protocol udp src-ip" is not set (when "no match protocol udp src-ip" is executed).
UDP-DST-PORT	If "match protocol udp dst-ip" is set, "match protocol udp dst-ip {IP address to which UDP packets are sent}" will be displayed. When "match protocol udp dst-ip" is not set (when "no match protocol udp dst-ip" is executed), it is not displayed.
AH-SPI	If "match protocol ah" is set, "match protocol ah {value of SPI field}" will be displayed. When "match protocol ah" is not set (when "no match protocol ah" is executed), it is not displayed.
ESP-SPI	If "match protocol esp" is set, "match protocol esp {value of SPI field}" will be displayed. When "match protocol esp" is not set (when "no match protocol esp" is executed), it is not displayed.
PROTOCOL-NUMBER	If "match protocol" is set, "match protocol {protocol number}" is displayed. When "match protocol" is not set (when "no match protocol" is executed), it is not displayed.
CONNTRACK-STATE	If "match conntrack state" is set, "match conntrack state {connection state}" will be displayed. When "match conntrack state" is not set (when "no match conntrack state" is executed), it is not displayed.
CONNTRACK-PROTO	If "match conntrack proto" is set, "match conntrack proto {protocol number}" will be displayed. When "match conntrack proto" is not set (when "no match conntrack proto" is executed), it is not displayed.
CONNTRACK-ORIGSRC-IP	If "match conntrack origsrc-ip" is set, "match conntrack origsrc-ip {source IP address of outgoing packets}" will be displayed. When "match conntrack origsrc-ip" is not set (when "no match conntrack origsrc-ip" is executed), it is not displayed.
CONNTRACK-ORIGDST-IP	If "match conntrack origdst-ip" is set, "match conntrack origdst-ip {destination IP address of outgoing packets}" will be displayed. When "match conntrack origdst-ip" is not set (when "no match conntrack origdst-ip" is executed), it is not displayed.

Item	Contents
CONNTRACK-REPLSRC-IP	If "match conntrack replsrc-ip" is set, "match conntrack replsrc-ip {source IP address of response packets}" will be displayed. When "match conntrack replsrc-ip" is not set (when "no match conntrack replsrc-ip" is executed), it is not displayed.
CONNTRACK-REPLDST-IP	If "match conntrack repldst-ip" is set, "match conntrack repldst-ip {destination IP address of response packets}" will be displayed. When "match conntrack repldst-ip" is not set (when "no match conntrack repldst-ip" is executed), it is not displayed.
CONNTRACK-ORIGSRC-PORT	If "match conntrack origsrc-port" is set, "match conntrack origsrc-port {source port of outgoing packets}" will be displayed. When "match conntrack origsrc-port" is not set (when "no match conntrack origsrc-port" is executed), it is not displayed.
CONNTRACK-ORIGDST-PORT	If "match conntrack origdst-port" is set, "match conntrack origdst-port {port to which outgoing packets are sent}" will be displayed. When "match conntrack origdst-port" is not set (when "no match conntrack origdst-port" is executed), it is not displayed.
CONNTRACK-REPLSRC-PORT	If "match conntrack replsrc-port {source port of response packets}" is set. When "match conntrack replsrc-port" is not set (when "no match conntrack replsrc-port" is executed), it is not displayed.
CONNTRACK-REPLDST-PORT	If "match conntrack repldst-port" is set, "match conntrack repldst-port {port to which response packets are sent}" is displayed. When "match conntrack repldst-port" is not set (when "no match conntrack repldst-port" is executed), it is not displayed.
CONNTRACK-STATUS	If "match conntrack status" is set, "match conntrack status {connection status}" will be displayed. When "match conntrack status" is not set (when "no match conntrack status" is executed), it is not displayed.
CONNTRACK-DIRECTION	If "match conntrack direction" is set, "match conntrack direction {direction of packets in the connection}" will be displayed. When "match conntrack direction" is not set (when "no match conntrack direction" is executed), it is not displayed.
HASHLIMIT-UPTO	If "match hashlimit upto {specified time}" is set. When "match hashlimit upto" is not set (when "no match hashlimit upto" is executed), it is not displayed.
HASHLIMIT-ABOVE	If "match hashlimit above" is set, "match hashlimit above {specified time}" is displayed. If "match hashlimit above" is not set (when "no match hashlimit above" is executed), it is not displayed.
HASHLIMIT-BURST	If "match hashlimit burst" is set, "match hashlimit burst {number of packets that can be matched consecutively}" will be displayed. When "match hashlimit burst" is not set (when "no match hashlimit burst" is executed), it is not displayed.
HASHLIMIT-MODE	If "match hashlimit mode" is set, "match hashlimit mode {hashlimit mode target}" is displayed. When "match hashlimit mode" is not set (when "no match hashlimit mode" is executed), it is not displayed.
HASHLIMIT-SRC-MASK	If "match hashlimit src-mask" is set, "match hashlimit src-mask" (address prefix to group by source IP address when srcip is specified in hashlimit-mode) is displayed. When "match hashlimit src-mask" is not set (when "no match hashlimit src-mask" is executed), it is not displayed.

Item	Contents
HASHLIMIT-DST-MASK	If "match hashlimit dst-mask" is set, "match hashlimit dst-mask" (address prefix for grouping by destination IP address when dstip is specified for hashlimit-mode) is displayed. When "match hashlimit dst-mask" is not set (when "no match hashlimit dst-mask" is executed), it is not displayed.
LIMIT-RATE	If "match limit rate" is set, "match limit rate {number of packets in specified time}" is displayed. When "match limit rate" is not set (when "no match limit rate" is executed), it is not displayed.
LIMIT-BURST	If "match limit burst" is set, "match limit burst {number of packets that can be matched consecutively}" is displayed. When "match limit burst" is not set (when "no match limit burst" is executed), it is not displayed.

➔ For an example run, see " 6.4.1 Display packet filtering settings" for an example.

6.6.2 Set packet matching conditions

This section describes the commands for setting packet matching conditions.

Format

```

match src-ip [not] ADDRESS[/PREFIX].
no match src-ip
match dst-ip [not] ADDRESS[/PREFIX].
no match dst-ip
match in-interface [not] IFNAME
no match in-interface
match out-interface [not] IFNAME
no match out-interface
match mac [not] MAC-ADDRESS
no match mac
match pkt-type < unicast | broadcast | multicast >
no match pkt-type
match protocol icmp < any |
    destination-unreachable |
    network-unreachable |
    host-unreachable |
    protocol-unreachable |
    port-unreachable |
    fragmentation-needed |
    source-route-failed |
    network-unknown |
    host-unknown |
    network-prohibited |
    host-prohibited |
    TOS-network-unreachable |
    TOS-host-unreachable |
    communication-prohibited |
    host-precedence-violation |
    precedence-cutoff |
    source-quench |
    redirect |
    network-redirect |
    host-redirect |
    TOS-network-redirect |
    TOS-host-redirect |
    echo-request |
    echo-reply |
    router-advertisement |
    router-solicitation |
    time-exceeded |
    ttl-exceeded |
    ttl-zero-during-transit |
    ttl-zero-during-reassembly |
    parameter-problem |
    ip-header-bad |
    required-option-missing |
    timestamp-request |
    timestamp-reply |
    address-mask-request |
    address-mask-reply >
no match protocol icmp
match protocol tcp src-port [not] PORT
match protocol tcp dst-port [not] PORT
match protocol tcp flags [not] < syn,ack,fin,rst,urg,psh,all,none
no match protocol tcp src-port

```

```

no match protocol tcp dst-port
no match protocol tcp flags
no match protocol tcp
match protocol udp src-port [not] PORT
match protocol udp dst-port [not] PORT
no match protocol udp src-port
no match protocol udp dst-port
no match protocol udp
match protocol ah [not] [SPI[-SPI]]
no match protocol ah
match protocol esp [not] [SPI[-SPI]]
no match protocol esp
match protocol NUMBER
no match protocol NUMBER
match conntrack state [not] < Disable,new,established,related,untracked,snat,dnat >
match conntrack proto [not] NUMBER
match conntrack origsrc-ip [not] ADDRESS[/PREFIX].
match conntrack origdst-ip [not] ADDRESS[/PREFIX].
match conntrack replsrc-ip [not] ADDRESS[/PREFIX].
match conntrack repldst-ip [not] ADDRESS[/PREFIX].
match conntrack origsrc-port [not] PORT
match conntrack origdst-port [not] PORT
match conntrack replsrc-port [not] PORT
match conntrack repldst-port [not] PORT
match conntrack status [not] < none,expected,seen_reply,assured,confirmed >
match conntrack direction < original | reply >
no match conntrack state
no match conntrack proto
no match conntrack origsrc-ip
no match conntrack origdst-ip
no match conntrack replsrc-ip
no match conntrack repldst-ip
no match conntrack origsrc-port
no match conntrack origdst-port
no match conntrack replsrc-port
no match conntrack repldst-port
no match conntrack status
no match conntrack direction
no match conntrack
match hashlimit upto NUMBER< /second | /minute | /hour | /day >
match hashlimit above NUMBER< /second | /minute | /hour | /day >
match hashlimit burst NUMBER
match hashlimit mode < srcip | srcport | dstip | dstport >
match hashlimit src-mask PREFIX
match hashlimit dst-mask PREFIX
no match hashlimit upto
no match hashlimit above
no match hashlimit burst
no match hashlimit mode
no match hashlimit src-mask
no match hashlimit dst-mask
no match hashlimit
match limit rate NUMBER< /second | /minute | /hour | /day >
match limit burst NUMBER
no match limit rate
no match limit burst
no match limit
no match

```

Command

Command	Contents								
match src-ip	The source address matches the packet with ADDRESS/PREFIX.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>ADDRESS</td> <td>Specify the source IP address.</td> </tr> <tr> <td>PREFIX</td> <td>Specifies the prefix length.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	ADDRESS	Specify the source IP address.	PREFIX	Specifies the prefix length.
	Setting	Contents							
	not	Reverses the condition specified below.							
ADDRESS	Specify the source IP address.								
PREFIX	Specifies the prefix length.								
<hr/>									
match dst-ip	Match a packet whose destination address is ADDRESS/PREFIX.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>ADDRESS</td> <td>Specify the destination IP address.</td> </tr> <tr> <td>PREFIX</td> <td>Specifies the prefix length.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	ADDRESS	Specify the destination IP address.	PREFIX	Specifies the prefix length.
	Setting	Contents							
	not	Reverses the condition specified below.							
ADDRESS	Specify the destination IP address.								
PREFIX	Specifies the prefix length.								
<hr/>									
match in-interface	Matches packets whose input interface is IFNAME.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>IFNAME</td> <td>Specifies the input interface name.  Configurable interface names vary by product. <ul style="list-style-type: none"> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0 </td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	IFNAME	Specifies the input interface name.  Configurable interface names vary by product. <ul style="list-style-type: none"> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0 		
	Setting	Contents							
	not	Reverses the condition specified below.							
IFNAME	Specifies the input interface name.  Configurable interface names vary by product. <ul style="list-style-type: none"> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0 								
<hr/>									
match out-interface	Output interface matches IFNAME packet.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>IFNAME</td> <td>Specifies the input interface name.  Configurable interface names vary by product. <ul style="list-style-type: none"> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0 </td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	IFNAME	Specifies the input interface name.  Configurable interface names vary by product. <ul style="list-style-type: none"> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0 		
	Setting	Contents							
	not	Reverses the condition specified below.							
IFNAME	Specifies the input interface name.  Configurable interface names vary by product. <ul style="list-style-type: none"> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0 								
<hr/>									
match mac	The MAC address matches the MAC-ADDRESS packet.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>MAC-ADDRESS</td> <td>Specify the MAC address in the following format xx:xx:xx:xx:xx:xx</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	MAC-ADDRESS	Specify the MAC address in the following format xx:xx:xx:xx:xx:xx		
	Setting	Contents							
	not	Reverses the condition specified below.							
MAC-ADDRESS	Specify the MAC address in the following format xx:xx:xx:xx:xx:xx								
<hr/>									
<hr/>									

Command	Contents																																																																													
match pkt-type	Matches the specified packet type.																																																																													
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>unicast</td> <td>Matches unicast.</td> </tr> <tr> <td>broadcast</td> <td>Matches broadcast.</td> </tr> <tr> <td>multicast</td> <td>Matches multicast.</td> </tr> </tbody> </table>	Setting	Contents	unicast	Matches unicast.	broadcast	Matches broadcast.	multicast	Matches multicast.																																																																					
	Setting	Contents																																																																												
	unicast	Matches unicast.																																																																												
broadcast	Matches broadcast.																																																																													
multicast	Matches multicast.																																																																													
<hr/>																																																																														
match protocol icmp	Matches packets whose ICMP message type is																																																																													
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>any</td> <td>Specifies ICMP message type.</td> </tr> <tr> <td>destination-unreachable</td> <td>→ For more information on message types, see RFC 792.</td> </tr> <tr> <td>network-unreachable</td> <td></td> </tr> <tr> <td>host-unreachable</td> <td></td> </tr> <tr> <td>protocol-unreachable</td> <td></td> </tr> <tr> <td>port-unreachable</td> <td></td> </tr> <tr> <td>fragmentation-needed</td> <td></td> </tr> <tr> <td>source-route-failed</td> <td></td> </tr> <tr> <td>network-unknown</td> <td></td> </tr> <tr> <td>host-unknown</td> <td></td> </tr> <tr> <td>network-prohibited</td> <td></td> </tr> <tr> <td>host-prohibited</td> <td></td> </tr> <tr> <td>TOS-network-unreachable</td> <td></td> </tr> <tr> <td>TOS-host-unreachable</td> <td></td> </tr> <tr> <td>communication-prohibited</td> <td></td> </tr> <tr> <td>host-precedence-violation</td> <td></td> </tr> <tr> <td>precedence-cutoff</td> <td></td> </tr> <tr> <td>source-quench</td> <td></td> </tr> <tr> <td>redirect</td> <td></td> </tr> <tr> <td>network-redirect</td> <td></td> </tr> <tr> <td>host-redirect</td> <td></td> </tr> <tr> <td>TOS-network-redirect</td> <td></td> </tr> <tr> <td>TOS-host-redirect</td> <td></td> </tr> <tr> <td>echo-request</td> <td></td> </tr> <tr> <td>echo-reply</td> <td></td> </tr> <tr> <td>router-advertisement</td> <td></td> </tr> <tr> <td>router-solicitation</td> <td></td> </tr> <tr> <td>time-exceeded</td> <td></td> </tr> <tr> <td>ttl-exceeded</td> <td></td> </tr> <tr> <td>ttl-zero-during-transit</td> <td></td> </tr> <tr> <td>ttl-zero-during-reassembly</td> <td></td> </tr> <tr> <td>parameter-problem</td> <td></td> </tr> <tr> <td>ip-header-bad</td> <td></td> </tr> <tr> <td>required-option-missing</td> <td></td> </tr> <tr> <td>timestamp-request</td> <td></td> </tr> <tr> <td>timestamp-reply</td> <td></td> </tr> <tr> <td>address-mask-request</td> <td></td> </tr> <tr> <td>address-mask-reply</td> <td></td> </tr> </tbody> </table>	Setting	Contents	any	Specifies ICMP message type.	destination-unreachable	→ For more information on message types, see RFC 792.	network-unreachable		host-unreachable		protocol-unreachable		port-unreachable		fragmentation-needed		source-route-failed		network-unknown		host-unknown		network-prohibited		host-prohibited		TOS-network-unreachable		TOS-host-unreachable		communication-prohibited		host-precedence-violation		precedence-cutoff		source-quench		redirect		network-redirect		host-redirect		TOS-network-redirect		TOS-host-redirect		echo-request		echo-reply		router-advertisement		router-solicitation		time-exceeded		ttl-exceeded		ttl-zero-during-transit		ttl-zero-during-reassembly		parameter-problem		ip-header-bad		required-option-missing		timestamp-request		timestamp-reply		address-mask-request		address-mask-reply
Setting	Contents																																																																													
any	Specifies ICMP message type.																																																																													
destination-unreachable	→ For more information on message types, see RFC 792.																																																																													
network-unreachable																																																																														
host-unreachable																																																																														
protocol-unreachable																																																																														
port-unreachable																																																																														
fragmentation-needed																																																																														
source-route-failed																																																																														
network-unknown																																																																														
host-unknown																																																																														
network-prohibited																																																																														
host-prohibited																																																																														
TOS-network-unreachable																																																																														
TOS-host-unreachable																																																																														
communication-prohibited																																																																														
host-precedence-violation																																																																														
precedence-cutoff																																																																														
source-quench																																																																														
redirect																																																																														
network-redirect																																																																														
host-redirect																																																																														
TOS-network-redirect																																																																														
TOS-host-redirect																																																																														
echo-request																																																																														
echo-reply																																																																														
router-advertisement																																																																														
router-solicitation																																																																														
time-exceeded																																																																														
ttl-exceeded																																																																														
ttl-zero-during-transit																																																																														
ttl-zero-during-reassembly																																																																														
parameter-problem																																																																														
ip-header-bad																																																																														
required-option-missing																																																																														
timestamp-request																																																																														
timestamp-reply																																																																														
address-mask-request																																																																														
address-mask-reply																																																																														
match protocol tcp src-port	Matches TCP packets whose source port is PORT.																																																																													
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>PORT</td> <td>Specifies the port number.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	PORT	Specifies the port number.																																																																							
	Setting	Contents																																																																												
not	Reverses the condition specified below.																																																																													
PORT	Specifies the port number.																																																																													
<hr/>																																																																														
match protocol tcp dst-port	Matches TCP packets whose destination port is PORT.																																																																													
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>PORT</td> <td>Specifies the port number.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	PORT	Specifies the port number.																																																																							
	Setting	Contents																																																																												
not	Reverses the condition specified below.																																																																													
PORT	Specifies the port number.																																																																													
<hr/>																																																																														

Command	Contents								
match tcp protocol flags	<p>Matches TCP packets that meet the conditions of the following flags</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>MASK</td> <td>Specify the flag to be checked among sync, ack, fi, rst, urg, psh, all, and none. To specify multiple flags, separate them with a comma (,).</td> </tr> <tr> <td>COMP</td> <td>Specifies which of the flags specified in MASK should be 1. sync, ack, fi, rst, urg, psh, all, none</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	MASK	Specify the flag to be checked among sync, ack, fi, rst, urg, psh, all, and none. To specify multiple flags, separate them with a comma (,).	COMP	Specifies which of the flags specified in MASK should be 1. sync, ack, fi, rst, urg, psh, all, none
Setting	Contents								
not	Reverses the condition specified below.								
MASK	Specify the flag to be checked among sync, ack, fi, rst, urg, psh, all, and none. To specify multiple flags, separate them with a comma (,).								
COMP	Specifies which of the flags specified in MASK should be 1. sync, ack, fi, rst, urg, psh, all, none								
match protocol udp src-port	<p>Matches UDP packets whose source port is PORT.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>PORT</td> <td>Specifies the port number.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	PORT	Specifies the port number.		
Setting	Contents								
not	Reverses the condition specified below.								
PORT	Specifies the port number.								
match protocol udp dst-port	<p>Match UDP packets whose destination port is PORT.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>PORT</td> <td>Specifies the port number.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	PORT	Specifies the port number.		
Setting	Contents								
not	Reverses the condition specified below.								
PORT	Specifies the port number.								
match protocol ah	<p>Matches if the SPI field of the AH packet is SPI.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>SPI</td> <td>Specify the value of the SPI field.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	SPI	Specify the value of the SPI field.		
Setting	Contents								
not	Reverses the condition specified below.								
SPI	Specify the value of the SPI field.								
match protocol esp	<p>Matches if the SPI field of the ESP packet is SPI.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>SPI</td> <td>Specify the value of the SPI field.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	SPI	Specify the value of the SPI field.		
Setting	Contents								
not	Reverses the condition specified below.								
SPI	Specify the value of the SPI field.								
match protocol NUMBER	<p>Matches packets whose protocol number is NUMBER.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>NUMBER</td> <td> Specifies the protocol number. → For protocol numbers, see the following web page https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml </td> </tr> </tbody> </table>	Setting	Contents	NUMBER	Specifies the protocol number. → For protocol numbers, see the following web page https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml				
Setting	Contents								
NUMBER	Specifies the protocol number. → For protocol numbers, see the following web page https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml								

Command	Contents																
match conntrack state	Matches the state of the connection.																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>new</td> <td>This is the packet that initiated the new connection.</td> </tr> <tr> <td>established</td> <td>Packets on the connection that have been confirmed to be bidirectional packets.</td> </tr> <tr> <td>related</td> <td>A packet that initiates a new connection but is associated with an existing connection.</td> </tr> <tr> <td>snat</td> <td>The source address of the packet and the destination address of the response packet are different.</td> </tr> <tr> <td>dnat</td> <td>The destination address of the packet and the source address of the response packet are different.</td> </tr> <tr> <td>Disable</td> <td>The packet is not related to an existing connection.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	new	This is the packet that initiated the new connection.	established	Packets on the connection that have been confirmed to be bidirectional packets.	related	A packet that initiates a new connection but is associated with an existing connection.	snat	The source address of the packet and the destination address of the response packet are different.	dnat	The destination address of the packet and the source address of the response packet are different.	Disable	The packet is not related to an existing connection.
	Setting	Contents															
	not	Reverses the condition specified below.															
	new	This is the packet that initiated the new connection.															
	established	Packets on the connection that have been confirmed to be bidirectional packets.															
	related	A packet that initiates a new connection but is associated with an existing connection.															
	snat	The source address of the packet and the destination address of the response packet are different.															
dnat	The destination address of the packet and the source address of the response packet are different.																
Disable	The packet is not related to an existing connection.																
match conntrack proto	Match the protocol of the packet.																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>NUMBER</td> <td>Specifies the L4 protocol number.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	NUMBER	Specifies the L4 protocol number.										
	Setting	Contents															
not	Reverses the condition specified below.																
NUMBER	Specifies the L4 protocol number.																
<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>ADDRESS</td> <td>Specify the IP address.</td> </tr> <tr> <td>PREFIX</td> <td>Specifies the prefix length.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	ADDRESS	Specify the IP address.	PREFIX	Specifies the prefix length.									
Setting	Contents																
not	Reverses the condition specified below.																
ADDRESS	Specify the IP address.																
PREFIX	Specifies the prefix length.																
match conntrack origsrc-ip match conntrack origdst-ip match conntrack replsrc-ip match conntrack repldst-ip	Matches the specified source IP address of outgoing packets (origsrc-ip), destination IP address of outgoing packets (origdst-ip), source IP address of reply packets (replsrc-ip), and destination IP address of reply packets (repldst-port).																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>ADDRESS</td> <td>Specify the IP address.</td> </tr> <tr> <td>PREFIX</td> <td>Specifies the prefix length.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	ADDRESS	Specify the IP address.	PREFIX	Specifies the prefix length.								
	Setting	Contents															
	not	Reverses the condition specified below.															
ADDRESS	Specify the IP address.																
PREFIX	Specifies the prefix length.																
<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>PORT</td> <td>Specifies the port number.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	PORT	Specifies the port number.											
Setting	Contents																
not	Reverses the condition specified below.																
PORT	Specifies the port number.																
match conntrack origsrc-port match conntrack origdst-port match conntrack replsrc-port match conntrack repldst-port	Matches the specified source IP port for outgoing packets (origsrc-port), destination IP port for outgoing packets (origdst-port), source IP port for reply packets (replsrc-port), and destination IP port for reply packets (replsrc-port).																
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>PORT</td> <td>Specifies the port number.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	PORT	Specifies the port number.										
	Setting	Contents															
	not	Reverses the condition specified below.															
	PORT	Specifies the port number.															
	match conntrack status	Matches the status of the connection.															
		<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>not</td> <td>Reverses the condition specified below.</td> </tr> <tr> <td>none</td> <td>The condition does not apply to any of the following</td> </tr> <tr> <td>expected</td> <td>Anticipated connection.</td> </tr> <tr> <td>seen_reply</td> <td>Bidirectional packets are acknowledged.</td> </tr> <tr> <td>assured</td> <td>Bidirectional packets are confirmed and do not expire.</td> </tr> <tr> <td>confirmed</td> <td>The connection is confirmed.</td> </tr> </tbody> </table>	Setting	Contents	not	Reverses the condition specified below.	none	The condition does not apply to any of the following	expected	Anticipated connection.	seen_reply	Bidirectional packets are acknowledged.	assured	Bidirectional packets are confirmed and do not expire.	confirmed	The connection is confirmed.	
Setting		Contents															
not		Reverses the condition specified below.															
none		The condition does not apply to any of the following															
expected		Anticipated connection.															
seen_reply	Bidirectional packets are acknowledged.																
assured	Bidirectional packets are confirmed and do not expire.																
confirmed	The connection is confirmed.																

Command	Contents										
match conntrack direction	<p>Match the direction of the packet.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>original</td> <td>Matches outgoing packets.</td> </tr> <tr> <td>reply</td> <td>Match response packet.</td> </tr> </tbody> </table>	Setting	Contents	original	Matches outgoing packets.	reply	Match response packet.				
Setting	Contents										
original	Matches outgoing packets.										
reply	Match response packet.										
match hashlimit upto match hashlimit above	<p>Specifies the maximum number of packets in a given time period.</p> <ul style="list-style-type: none"> ● In the case of upto, packets up to that limit are matched. ● In the case of ABOVE, packets exceeding that limit are matched. <p>The maximum number of packets is determined by the number of packets specified in "match hashlimit burst".</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>NUMBER/second</td> <td rowspan="4">Specifies the maximum number of packets in a given time period.</td> </tr> <tr> <td>NUMBER/minute</td> </tr> <tr> <td>NUMBER/hour</td> </tr> <tr> <td>NUMBER/day</td> </tr> </tbody> </table>	Setting	Contents	NUMBER/second	Specifies the maximum number of packets in a given time period.	NUMBER/minute	NUMBER/hour	NUMBER/day			
Setting	Contents										
NUMBER/second	Specifies the maximum number of packets in a given time period.										
NUMBER/minute											
NUMBER/hour											
NUMBER/day											
match hashlimit burst	<p>Specify the initial number of packets that can be matched. This packet count is decremented for each packet, and when it reaches 0, subsequent packets will not be matched. The number of packets is incremented at each time interval specified in "match limit rate".</p> <p>However, the upper limit of the increment is the number of packets specified here.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>NUMBER</td> <td>Specifies the maximum number of packets that can be matched in a given time period.</td> </tr> </tbody> </table>	Setting	Contents	NUMBER	Specifies the maximum number of packets that can be matched in a given time period.						
Setting	Contents										
NUMBER	Specifies the maximum number of packets that can be matched in a given time period.										
match hashlimit mode	<p>The limits set by match hashlimit are applied in the units specified below.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>srcip</td> <td>Specify the source IP address.</td> </tr> <tr> <td>dstip.</td> <td>Specify the destination IP address.</td> </tr> <tr> <td>srcport</td> <td>Specifies the source port number.</td> </tr> <tr> <td>dstport</td> <td>Specifies the destination port number.</td> </tr> </tbody> </table>	Setting	Contents	srcip	Specify the source IP address.	dstip.	Specify the destination IP address.	srcport	Specifies the source port number.	dstport	Specifies the destination port number.
Setting	Contents										
srcip	Specify the source IP address.										
dstip.	Specify the destination IP address.										
srcport	Specifies the source port number.										
dstport	Specifies the destination port number.										
match hashlimit src-mask	When srcip is specified for HASHLIMIT-MODE, specify the address prefix to be grouped for each source IP address, in the range of 0 to 32.										
match hashlimit dst-mask	When dstip is specified for HASHLIMIT-MODE, specify the address prefix to be grouped for each destination IP address, in the range of 0 to 32.										
match limit rate	<p>Sets the average number of packets matched within a specified time period.</p> <p>Packets are matched if there is room in the number of packets specified in "match limit burst" and not matched if there is no room.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>NUMBER/second</td> <td rowspan="4">Specifies the average number of packets that can be matched in a given time period.</td> </tr> <tr> <td>NUMBER/minute</td> </tr> <tr> <td>NUMBER/hour</td> </tr> <tr> <td>NUMBER/day</td> </tr> </tbody> </table>	Setting	Contents	NUMBER/second	Specifies the average number of packets that can be matched in a given time period.	NUMBER/minute	NUMBER/hour	NUMBER/day			
Setting	Contents										
NUMBER/second	Specifies the average number of packets that can be matched in a given time period.										
NUMBER/minute											
NUMBER/hour											
NUMBER/day											

Command	Contents				
match limit burst	<p>Sets the initial value of the number of packets that can be matched. This number of packets is decremented for each packet, and when it reaches 0, subsequent packets will not be matched. The number of packets is incremented at each time interval specified in "match limit rate".</p> <p>However, the upper limit of the increment is the number of packets specified here.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>NUMBER</td> <td>Specifies the maximum number of packets that can be matched in a given time period.</td> </tr> </tbody> </table>	Setting	Contents	NUMBER	Specifies the maximum number of packets that can be matched in a given time period.
Setting	Contents				
NUMBER	Specifies the maximum number of packets that can be matched in a given time period.				

Execution example

```

amnimo(cfg-fin-100)# match src-ip 234.192.0.1/24 ←
amnimo(cfg-fin-100)# match dst-ip 234.192.0.1/24 ←
amnimo(cfg-fin-100)# match in-interface eth0 ←
amnimo(cfg-fin-100)# match mac 00:00:5E:00:53:FF ←
amnimo(cfg-fin-100)# match pkt-type multicast ←
amnimo(cfg-fin-100)# match protocol icmp destination-unreachable ←
amnimo(cfg-fin-100)# match protocol tcp dst-port 80 ←
amnimo(cfg-fin-100)# match protocol tcp flags all syn,ack ←
amnimo(cfg-fin-100)# match protocol udp src-port 5353 ←
amnimo(cfg-fin-100)# match protocol ah 500 ←
amnimo(cfg-fin-100)# match protocol esp 500 ←
amnimo(cfg-fin-100)# match protocol 51 ←

```

6.6.3 Delete packet match condition

This section describes the delete packet match condition command.

Format

```
no match
```

Execution example

```
amnimo(cfg-fin-100) # no match ←
```

6.6.4 Display log output settings

The items that appear as log output settings are listed below.

Output Format

```
LOG
```

Output item

Item	Contents
LOG	If log is set, "log {log level} {prefix}" will be displayed. If "log" is not set (when "no log" is executed), it is not displayed.

Output Example

```
log informational
```

6.6.5 Configure log output

This section describes the log output configuration commands.

Format

```
log LEVEL [PREFIX].
```

Command

Command	Contents						
log	Configure log output settings. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>LEVEL</td> <td>Specify one of the following emergencies, alerts, criticals, errors, warnings, notifications, informational, debugging</td> </tr> <tr> <td>PREFIX</td> <td>Specifies a string to be appended to the beginning of the log.</td> </tr> </tbody> </table>	Setting	Contents	LEVEL	Specify one of the following emergencies, alerts, criticals, errors, warnings, notifications, informational, debugging	PREFIX	Specifies a string to be appended to the beginning of the log.
Setting	Contents						
LEVEL	Specify one of the following emergencies, alerts, criticals, errors, warnings, notifications, informational, debugging						
PREFIX	Specifies a string to be appended to the beginning of the log.						
no log	No log is output.						

Execution example

```
log notifications prefix ↵
```

6.7 Configure IPsec settings.



View IPsec status and settings, manually connect and disconnect, and configure IPsec settings.

6.7.1 Display IPsec status

To display IPsec status, run the *show ipsec* command with the status or xfrm option.

Format

```
show ipsec status [SA-NAME].
show ipsec xfrm state
show ipsec xfrm policy
```

Setting items

Item	Contents						
status	Specify if IPsec status information is to be displayed.  If SA-NAME is omitted, all SA statuses are displayed.						
xfrm	To view xfrm state or policy, specify one of the following options <table border="1" style="width: 100%; margin-top: 5px;"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>state</td> <td>Specify if xfrm state is to be displayed.</td> </tr> <tr> <td>policy</td> <td>Specify if you want to view xfrm policies.</td> </tr> </tbody> </table>	Setting	Contents	state	Specify if xfrm state is to be displayed.	policy	Specify if you want to view xfrm policies.
Setting	Contents						
state	Specify if xfrm state is to be displayed.						
policy	Specify if you want to view xfrm policies.						

Output Format

When the *show ipsec status* command is executed
IPSEC-STATUS

If the *show ipsec xfrm state* command is executed
IPSEC-XFRM-STATE

If the *show ipsec xfrm policy* command is executed
IPSEC-XFRM-POLICY

Output item

Item	Contents
IPSEC-STATUS	IPsec status information is displayed.
IPSEC-XFRM-STATE	The xfrm state is displayed. The protocol used in communication, SPI information, etc. are displayed.
IPSEC-XFRM-POLICY	The xfrm policy is displayed. It shows which states are used in which communication.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

```
ユーザーモード 管理者モード 設定モード
amnimo$ show ipsec status ↵
Status of IKE charon daemon (weakSwan 5.6.2, Linux 4.19.93-02926-g51250a0eff3c, aarch64):.
  uptime: 14 seconds, since Feb 28 06:34:04 2020
  malloc: sbrk 2572288, mmap 0, used 639760, free 1932528
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
  loaded plugins: charon aes rc2 sha2 sha1 md4 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters
Listening IP addresses:
  172.16.1.13
  192.168.1.254
Connections:
  sa01: 192.168.1.254....192.168.1.10 IKEv1, dpddelay=5s
  sa01: local: [test2.test2.test2] uses pre-shared key authentication
  sa01: remote: [test.test.test] uses pre-shared key authentication
  sa01: child: 192.168.0.0/24 === 192.168.10.0/24 TUNNEL, dpdaction=clear
  sa02: child: 192.168.0.0/24 === 192.168.20.0/24 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):.
  sa01[1]: ESTABLISHED 10 seconds ago, 192.168.1.254[test2.test2.test2].192.168.1.10[test.test.test].
  sa01[1]: IKEv1 SPIs: dce80832e5e9fe43_i c707f12f9adcf60c_r*, pre-shared key authentication in 2 hours
  sa01[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
  sa01{1}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: cee4939e_i ca99e852_o
  sa01{1}: AES_CBC_128/HMAC_SHA2_256_128/MODP_2048, 0 bytes_i, 0 bytes_o, rekeying in 43 minutes
  sa01{1}: 192.168.0.0/24 === 192.168.10.0/24
  sa02{2}: INSTALLED, TUNNEL, reqid 2, ESP SPIs: c7a43d8d_i c9545378_o
  sa02{2}: AES_CBC_128/HMAC_SHA2_256_128/MODP_2048, 0 bytes_i, 0 bytes_o, rekeying in 45 minutes
  sa02{2}: 192.168.0.0/24 === 192.168.20.0/24
amnimo$ show ipsec xfrm state ↵
src 192.168.1.254 dst 192.168.1.10
  proto esp spi 0xc9545378 reqid 2 mode tunnel
  replay-window 0 flag af-unspec
  auth-trunc hmac(sha256) 0x27c4dbbddf858753e42d10b58501f9173fb55dd3e88a23864ee17c8fac3b62c1 128
  enc cbc(aes) 0x1523a3ad8abe4c1a743a660c7c549c1f
  anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
src 192.168.1.10 dst 192.168.1.254
  proto esp spi 0xc7a43d8d reqid 2 mode tunnel
  replay-window 32 flag af-unspec
  auth-trunc hmac(sha256) 0x8f9347e1e732351f0d26bdec4024e6b2803bf77404701e97efb708f931d14eab 128
  enc cbc(aes) 0x22eb34273c78e5b8f791200ccd6d03b8
  anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
src 192.168.1.254 dst 192.168.1.10
  proto esp spi 0xca99e852 reqid 1 mode tunnel
  replay-window 0 flag af-unspec
  auth-trunc hmac(sha256) 0xe6c59c4464bb741a58071b44329e6292dd41f9613d988ac05d303056c9e54e66 128
  enc cbc(aes) 0xdd5c0a0654002853119cd9648d876213
```

```

    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
src 192.168.1.10 dst 192.168.1.254
    proto esp spi 0xcee4939e reqid 1 mode tunnel
    replay-window 32 flag af-unspec
    auth-trunc hmac(sha256) 0x733709c60f1d312e7c5199b8057550bc5896b19ac96aeb97f7e3
c34620f96ef3 128
    enc cbc(aes) 0x5201ae28eb579c9f08b06a4f511ed97e
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
amnimo$ show ipsec xfrm policy ↵
src 192.168.0.0/24 dst 192.168.20.0/24
    dir out priority 375423 ptype main
    tmpl src 192.168.1.254 dst 192.168.1.10
        proto esp spi 0xc9545378 reqid 2 mode tunnel
src 192.168.20.0/24 dst 192.168.0.0/24
    dir fwd priority 375423 ptype main
    tmpl src 192.168.1.10 dst 192.168.1.254
        proto esp reqid 2 mode tunnel
src 192.168.20.0/24 dst 192.168.0.0/24
    dir in priority 375423 ptype main
    tmpl src 192.168.1.10 dst 192.168.1.254
        proto esp reqid 2 mode tunnel
src 192.168.0.0/24 dst 192.168.10.0/24
    dir out priority 375423 ptype main
    tmpl src 192.168.1.254 dst 192.168.1.10
        proto esp spi 0xca99e852 reqid 1 mode tunnel
src 192.168.10.0/24 dst 192.168.0.0/24
    dir fwd priority 375423 ptype main
    tmpl src 192.168.1.10 dst 192.168.1.254
        proto esp reqid 1 mode tunnel
src 192.168.10.0/24 dst 192.168.0.0/24
    dir in priority 375423 ptype main
    tmpl src 192.168.1.10 dst 192.168.1.254
        proto esp reqid 1 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main

```

6.7.2 Connect IPsec manually

To manually initiate an IPsec connection, run the *ipsec connect* command.

Format

```
ipsec connect IPSEC-SA-NAME
```

Setting items

Item	Contents
IPSEC-SA-NAME	Specify the name of the IPsec SA policy to connect to.  Entering the "Tab" key completes the entry of the IPsec SA policy name.

Execution example

Command input and output are the same in administrator mode and configuration mode. Below is an example of connecting to IPsec SA sa01 in administrator mode.

管理者モード 設定モード

```
amnimo# ipsec connect sa01 ↵
```

6.7.3 Disconnect IPsec

To disconnect IPsec, execute the *no ipsec connect* command.

Format

```
no ipsec connect IPSEC-SA-NAME
```

Setting items

Item	Contents
IPSEC-SA-NAME	Specifies the name of the IPsec SA policy to be disconnected.  Entering the "Tab" key completes the entry of the IPsec SA policy name.

Execution example

Command input and output are the same in administrator mode and configuration mode. Below is an example of running disconnect IPsec SA sa01 in administrator mode.

管理者モード 設定モード

```
amnimo# no ipsec connect sa01 ↵
```

6.7.4 Display IPsec settings

To view IPsec settings, run the **show config ipsec** command with one of the following options: log-level, ike, or sa.

Format

```
show config ipsec log-level
show config ipsec ike [IKE-NAME].
show config ipsec sa [SA-NAME].
```

Setting items

Item	Contents
log-level	Specify if you want to display the log level for each feature used in IPsec.
ike	Specify the name of the IPsec IKE setting in IKE-NAME to display the IPsec IKE configuration.  If IKE-NAME is omitted, all IPsec IKE settings are displayed.
sa	Specify the name of the IPsec SA setting in SA-NAME to display the IPsec SA settings.  If SA-NAME is omitted, all IPsec SA settings are displayed.

Output Format

```
When run with the log-level option
# ---- transition to configure mode ----
configure
# ---- ipsec log-levle configure ----
ipsec loglevel
asn LOGLEVEL
cfg LOGLEVEL
chd LOGLEVEL
dmn LOGLEVEL
enc LOGLEVEL
esp LOGLEVEL
ike LOGLEVEL
imc LOGLEVEL
imv LOGLEVEL
job LOGLEVEL
knl LOGLEVEL
lib LOGLEVEL
mgr LOGLEVEL
net LOGLEVEL
pts LOGLEVEL
tls LOGLEVEL
tnc LOGLEVEL
exit
# ---- exit configure mode ----
exit
```

```
When executed with the -ike option
# ---- transition to configure mode ----
configure
# ---- ipsec ike ike-name configure ----
ipsec ike ike-name
local address LOCAL-ADDRESS
LOCAL-IDENTIFY
```

```

remote address REMOTE-ADDRESS
REMOTE-IDENTIFY
version IKE-VERSION
MOBIKE
AUTHENTICATION
IKE-MODE
FLAGMENTATION
retry RETRY-COUNT
IKE-TRANSFORM-RESTRICTION
IKE-TRANSFORM
lifetime IKE-LIFETIME
DPD-ACTION
dpd interval DPD-INTERVAL
dpd timeout DPD-TIMEOUT
exit
# ---- exit configure mode ----
exit

```

When executed with the `-sa` option

```

# ---- transition to configure mode ----
configure
# ---- ipsec sa SA-NAME configure ----
ipsec sa SA-NAME
ENABLE
key-exchange ike USE-IKE-NAME
NEGOTIATION-MODE
REKEY
type SA-TYPE
mode SA-MODE
IPCOMP
SA-TRANSFORM-RESTRICTION
SA-TRANSFORM
lifetime SA-LIFE-TIME
LOCAL-SUBNET
REMOTE-SUBNET
exit
# ---- exit configure mode ----
exit

```

Output item

Item	Contents														
LOGLEVEL	<p>Log level settings for each function are displayed.</p> <table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>silent</td> <td>No log is output.</td> </tr> <tr> <td>audit</td> <td>A basic log is output.</td> </tr> <tr> <td>control</td> <td>The control flow log is output.</td> </tr> <tr> <td>controlmore</td> <td>Detailed control flow logs are output.</td> </tr> <tr> <td>raw</td> <td>It even outputs a log of binary information.</td> </tr> <tr> <td>private</td> <td>Even logs of keys and other sensitive information are output.</td> </tr> </tbody> </table>	Display	Contents	silent	No log is output.	audit	A basic log is output.	control	The control flow log is output.	controlmore	Detailed control flow logs are output.	raw	It even outputs a log of binary information.	private	Even logs of keys and other sensitive information are output.
Display	Contents														
silent	No log is output.														
audit	A basic log is output.														
control	The control flow log is output.														
controlmore	Detailed control flow logs are output.														
raw	It even outputs a log of binary information.														
private	Even logs of keys and other sensitive information are output.														
IKE-NAME	<p>The name of the IPsec IKE setting is displayed.</p>  <ul style="list-style-type: none"> ● If there is no setting, it will not be displayed. ● If there are multiple settings, all setting names are displayed. 														

Item	Contents												
LOCAL-ADDRESS	The address on the local side is displayed in the following format, depending on the setting value. any ipv4 X.X.X.X ipv6 X::X:X												
LOCAL-IDENTIFY	The local side ID setting is displayed in the following format, depending on the set value. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Setting</th> <th>Form</th> </tr> </thead> <tbody> <tr> <td>IPv4</td> <td>local id ipv4 ADDRESS</td> </tr> <tr> <td>IPv6</td> <td>local id ipv6 ADDRESS</td> </tr> <tr> <td>FQDN</td> <td>local id fqdn FQDN</td> </tr> <tr> <td>UserFQDN</td> <td>local id userfqdn USERFQDN</td> </tr> <tr> <td>key id</td> <td>local id key KEYID</td> </tr> </tbody> </table> <p> If there is no setting, it will not be displayed.</p>	Setting	Form	IPv4	local id ipv4 ADDRESS	IPv6	local id ipv6 ADDRESS	FQDN	local id fqdn FQDN	UserFQDN	local id userfqdn USERFQDN	key id	local id key KEYID
Setting	Form												
IPv4	local id ipv4 ADDRESS												
IPv6	local id ipv6 ADDRESS												
FQDN	local id fqdn FQDN												
UserFQDN	local id userfqdn USERFQDN												
key id	local id key KEYID												
REMOTE-ADDRESS	The address of the remote side is displayed.												
REMOTE-IDENTIFY	The remote side ID setting is displayed in the following format, depending on the set value. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Setting</th> <th>Form</th> </tr> </thead> <tbody> <tr> <td>IPv4</td> <td>remote id ipv4 ADDRESS</td> </tr> <tr> <td>IPv6</td> <td>remote id ipv6 ADDRESS</td> </tr> <tr> <td>FQDN</td> <td>remote id fqdn FQDN</td> </tr> <tr> <td>UserFQDN</td> <td>remote id userfqdn USERFQDN</td> </tr> <tr> <td>key id</td> <td>remote id key KEYID</td> </tr> </tbody> </table> <p> If there is no setting, it will not be displayed.</p>	Setting	Form	IPv4	remote id ipv4 ADDRESS	IPv6	remote id ipv6 ADDRESS	FQDN	remote id fqdn FQDN	UserFQDN	remote id userfqdn USERFQDN	key id	remote id key KEYID
Setting	Form												
IPv4	remote id ipv4 ADDRESS												
IPv6	remote id ipv6 ADDRESS												
FQDN	remote id fqdn FQDN												
UserFQDN	remote id userfqdn USERFQDN												
key id	remote id key KEYID												
IKE-VERSION	The version of IKE is displayed.												
MOBIKE	Information is displayed when Mobike protocol operation is enabled/disabled. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The name "mobike" will appear on the screen.</td> </tr> <tr> <td>Disable</td> <td>The message "no mobike" will be displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The name "mobike" will appear on the screen.	Disable	The message "no mobike" will be displayed.						
Setting	Display												
Enable	The name "mobike" will appear on the screen.												
Disable	The message "no mobike" will be displayed.												
AUTHENTICATION	The settings used for authentication are displayed.  If there is no setting, it will not be displayed.												
IKE-MODE	IKE mode is displayed. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>main</td> <td>main mode</td> </tr> <tr> <td>aggressive</td> <td>aggressive mode</td> </tr> </tbody> </table>	display	Contents	main	main mode	aggressive	aggressive mode						
display	Contents												
main	main mode												
aggressive	aggressive mode												
FLAGMENTATION	Information is displayed when fragmentation is enabled/disabled. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be labeled "flagmentation."</td> </tr> <tr> <td>Disable</td> <td>The message "no flagmentation" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be labeled "flagmentation."	Disable	The message "no flagmentation" is displayed.						
Setting	Display												
Enable	It will be labeled "flagmentation."												
Disable	The message "no flagmentation" is displayed.												
RETRY-COUNT	The retry count setting is displayed.												

Item	Contents										
IKE-TRANSFORM-RESTRICTION	<p>Displays information on when IKE's transform-limiting behavior is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "TRANSFORM RESTRICTION" appears.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "TRANSFORM RESTRICTION" appears.	Disable	Not displayed.				
Setting	Display										
Enable	The message "TRANSFORM RESTRICTION" appears.										
Disable	Not displayed.										
IKE-TRANSFORM	<p>IKE transform settings are displayed in the following format.</p> <pre>transform encryption ENCRYPTION integrity INTEGRITY prf PFS dh-group GROUP</pre> <p> <ul style="list-style-type: none"> ● If there is no setting, it will not be displayed. ● If there are multiple settings, all setting names are displayed. </p>										
IKE-LIFETIME	IKE lifetime is displayed.										
DPD-ACTION	<p>The operation when disconnected by DPD (Dead Peer Detection) is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>clear</td> <td>The message "dpd action clear" is displayed.</td> </tr> <tr> <td>hold</td> <td>The message "dpd action held" is displayed.</td> </tr> <tr> <td>restart</td> <td>The message "dpd action restart" is displayed.</td> </tr> <tr> <td>none</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Contents	clear	The message "dpd action clear" is displayed.	hold	The message "dpd action held" is displayed.	restart	The message "dpd action restart" is displayed.	none	Not displayed.
Setting	Contents										
clear	The message "dpd action clear" is displayed.										
hold	The message "dpd action held" is displayed.										
restart	The message "dpd action restart" is displayed.										
none	Not displayed.										
DPD-INTERVAL	The interval of the DPD is displayed.										
DPD-TIMEOUT	The timeout for DPD is displayed.										
SA-NAME	<p>The name of the IPsec SA setting is displayed.</p> <p> <ul style="list-style-type: none"> ● If there is no setting, it will not be displayed. ● If there are multiple settings, all setting names are displayed. </p>										
ENABLE	<p>Displays information on when IPsec SA settings are enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.				
Setting	Display										
Enable	The message "enable" is displayed.										
Disable	The message "no enable" is displayed.										
USE-IKE-NAME	The IKE name to be used is displayed.										
NEGOTIATION-MODE	<p>IPsec connection behavior is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>initiate</td> <td>The message "negotiation-mode initiate" is displayed.</td> </tr> <tr> <td>ondemand</td> <td>The message "negotiation-mode ondemand" is displayed.</td> </tr> <tr> <td>hold</td> <td>The message "negotiation-mode hold" is displayed.</td> </tr> </tbody> </table>	Setting	Contents	initiate	The message "negotiation-mode initiate" is displayed.	ondemand	The message "negotiation-mode ondemand" is displayed.	hold	The message "negotiation-mode hold" is displayed.		
Setting	Contents										
initiate	The message "negotiation-mode initiate" is displayed.										
ondemand	The message "negotiation-mode ondemand" is displayed.										
hold	The message "negotiation-mode hold" is displayed.										
REKEY	<p>Information is displayed when rekey is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The word "rekey" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no rekey" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The word "rekey" is displayed.	Disable	The message "no rekey" is displayed.				
Setting	Display										
Enable	The word "rekey" is displayed.										
Disable	The message "no rekey" is displayed.										

Item	Contents								
SA-TYPE	<p>The protocol type is displayed.</p> <table border="1"> <thead> <tr> <th>display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>esp. in film-making</td> <td>ESP Protocol</td> </tr> <tr> <td>ah</td> <td>AH Protocol</td> </tr> </tbody> </table>	display	Contents	esp. in film-making	ESP Protocol	ah	AH Protocol		
display	Contents								
esp. in film-making	ESP Protocol								
ah	AH Protocol								
SA-MODE	<p>The communication mode is displayed.</p> <table border="1"> <thead> <tr> <th>display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>tunnel</td> <td>tunnel mode</td> </tr> <tr> <td>transport</td> <td>transport mode</td> </tr> <tr> <td>passthrough</td> <td>pass-through mode</td> </tr> </tbody> </table> <p> Pass-through mode is not an IPsec pass-through function.</p>	display	Contents	tunnel	tunnel mode	transport	transport mode	passthrough	pass-through mode
display	Contents								
tunnel	tunnel mode								
transport	transport mode								
passthrough	pass-through mode								
IPCOMP	<p>Displays information when IPComp is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be labeled "ipcomp."</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be labeled "ipcomp."	Disable	Not displayed.		
Setting	Display								
Enable	It will be labeled "ipcomp."								
Disable	Not displayed.								
ANTI-REPLAY	<p>Displays information on when the replay protection setting is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be labeled "anti-replay."</td> </tr> <tr> <td>Disable</td> <td>The message "no anti-replay" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be labeled "anti-replay."	Disable	The message "no anti-replay" is displayed.		
Setting	Display								
Enable	It will be labeled "anti-replay."								
Disable	The message "no anti-replay" is displayed.								
SA-TRANSFORM-RESTRICTION	<p>Information is displayed on when the behavior that limits SA transforms is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "TRANSFORM RESTRICTION" appears.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "TRANSFORM RESTRICTION" appears.	Disable	Not displayed.		
Setting	Display								
Enable	The message "TRANSFORM RESTRICTION" appears.								
Disable	Not displayed.								
SA-TRANSFORM	<p>SA transform settings are displayed in the following format.</p> <pre>transform encryption ENCRYPTION integrity INTEGRITY pfs PFS</pre> <p> <ul style="list-style-type: none"> ● If there is no setting, it will not be displayed. ● If there are multiple settings, all settings will be displayed. </p>								
SA-LIFETIME	<p>The SA lifetime is displayed.</p>								
LOCAL-SUBNET	<p>The local side subnet is displayed in the following format</p> <pre>local subnet LOCAL-SUBNET</pre> <p> <ul style="list-style-type: none"> ● If there is no setting, it will not be displayed. ● If there are multiple settings, all settings will be displayed. </p>								
REMOTE-SUBNET	<p>The remote side subnet is displayed in the following format</p> <pre>remote subnet REMOTE-SUBNET</pre> <p> <ul style="list-style-type: none"> ● If there is no setting, it will not be displayed. ● If there are multiple settings, all settings will be displayed. </p>								

Execution example

Below is a running example of an IPsec connection in administrator and configuration modes.

管理者モード

```
amnimo# show config ipsec log-level←          ← Show log level for each function
# ---- transition to configure mode ----
configure
# ---- ipsec log-levle configure ----
ipsec loglevel
asn contro
cfg contro
chd contro
dmn contro
enc contro
esp contro
ike contro
imc contro
imv contro
JOB CONTROL
knl contro
lib contro
mgr contro
NET CONTROL
pts contro
tls contro
tnc contro
exit
# ---- exit configure mode ----
exit
amnimo# show config ipsec ike ike01←          ← Show IPsec IKE settings
# ---- transition to configure mode ----
configure
# ---- ipsec ike ike-name configure ----
ipsec ike ike01
local address 192.168.0.254
remote address 192.168.0.253
version 2
mobike
authentication pre-shared-key secret dGVzdA==
mode main
fragmentation
retry 3
transform encryption aes128 integrity sha1 prf sha1 dh-group 14
lifetime 3h
dpd interval 150s
dpd timeout 30s
exit
# ---- exit configure mode ----
exit
amnimo# show config ipsec sa sa01←           ← Show IPsec SA settings
# ---- transition to configure mode ----
configure
# ---- ipsec sa sa01 configure ----
ipsec sa sa01
enable
key-exchange ike ike01
negotiation-mode initiate
rekey
type esp
```

```
mode tunnel
transform encryption aes128 integrity sha1 pfs 14
lifetime 1h
exit
# ---- exit configure mode ----
exit
```

```

amnimo(cfg)# show config ipsec log-level ← Show log level for each function
# ---- ipsec log-levle configure ----
ipsec log-level
asn contro
cfg contro
chd contro
dmn contro
enc contro
esp contro
ike contro
imc contro
imv contro
JOB CONTROL
knl contro
lib contro
mgr contro
NET CONTROL
pts contro
tls contro
tnc contro
exit
amnimo(cfg)# show config ipsec ike ike01 ← Show IPsec IKE settings
# ---- ipsec ike ike-name configure ----
ipsec ike ike01
local address 192.168.0.254
remote address 192.168.0.253
version 2
mobike
authentication pre-shared-key secret dGVzdA==
mode main
fragmentation
retry 3
transform encryption aes128 integrity sha1 prf sha1 dh-group 14
lifetime 3h
dpd interval 150s
dpd timeout 30s
exit
amnimo(cfg)# show config ipsec sa sa sa01 ← Show IPsec SA settings
# ---- ipsec sa sa01 configure ----
ipsec sa sa01
enable
key-exchange ike ike01
negotiation-mode initiate
rekey
type esp
mode tunnel
transform encryption aes128 integrity sha1 pfs 14
lifetime 1h
exit

```



Running the show config command in IPsec advanced configuration mode will display the same information as in configuration mode.

To enter the IPsec advanced configuration mode, execute the ipsec command with one of the options "log-levle", "ike", or "sa".

Below is an example of displaying IPsec configuration information in each advanced configuration mode.

```
amnimo(cfg)# ipsec log-level ↵
amnimo(cfg-ips-log)# show config ↵
asn contro                               ← Same as setting mode
cfg contro
(Omitted.)
amnimo(cfg)# ipsec ike ike01↵
amnimo(cfg-ips-ike-ike01)# show config↵
local address 192.168.0.254              ← Same as the configuration mode
remote address 192.168.0.253
(Omitted.)
amnimo(cfg-ips-ike-ike01)# exit ↵
amnimo(cfg)# ipsec sa sa01 ↵
amnimo(cfg-ips-sa-sa01)# show config ↵
enable                                   ← Same as setting mode
key-exchange ike ike01
(Omitted.)
```

6.7.5 Configure IPsec

To configure IPsec, go to advanced configuration mode and execute the configuration commands. IPsec has advanced configuration modes for log level, IKE, and SA settings. Each of these advanced configuration modes can be entered by executing the `ipsec` command with an option. The settings made here are written to a configuration file.

■ Set the log level

To set the log level for each function, run the *`ipsec log-level`* command.

Format

```
ipsec log-level
asn LOGLEVEL
cfg LOGLEVEL
chd LOGLEVEL
dmn LOGLEVEL
enc LOGLEVEL
esp LOGLEVEL
ike LOGLEVEL
imc LOGLEVEL
imv LOGLEVEL
job LOGLEVEL
knl LOGLEVEL
lib LOGLEVEL
mgr LOGLEVEL
net LOGLEVEL
pts LOGLEVEL
tls LOGLEVEL
tnc LOGLEVEL
exit
```

Command

Command	Contents														
ipsec log-level	Execute the command to set the IPsec logging level.  Executing a command in the setting mode shifts to the detailed setting mode.														
asn	Specify the log level for low-level encoding/decoding (ASN.1, X.509, etc.) in LOGLEVEL. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>silent</td> <td>No log is output.</td> </tr> <tr> <td>audit</td> <td>Outputs basic logs.</td> </tr> <tr> <td>control</td> <td>Outputs control flow logs.</td> </tr> <tr> <td>controlmore</td> <td>Outputs detailed control flow logs.</td> </tr> <tr> <td>raw</td> <td>It even outputs a log of binary information.</td> </tr> <tr> <td>private</td> <td>It even outputs log of keys and other sensitive information.</td> </tr> </tbody> </table>	Setting	Contents	silent	No log is output.	audit	Outputs basic logs.	control	Outputs control flow logs.	controlmore	Outputs detailed control flow logs.	raw	It even outputs a log of binary information.	private	It even outputs log of keys and other sensitive information.
Setting	Contents														
silent	No log is output.														
audit	Outputs basic logs.														
control	Outputs control flow logs.														
controlmore	Outputs detailed control flow logs.														
raw	It even outputs a log of binary information.														
private	It even outputs log of keys and other sensitive information.														
cfg	Specify the log level for configuration management in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.														
chd	Specify the log level for CHILD_SA/IPsec SA in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.														

Command	Contents
dmn	Specify the logging level for main daemon setup, cleanup, signal processing, etc. in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
enc	Specify the log level for encode/decode (encrypt/decrypt operations) in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
esp. in film-making	Specify the log level of the IPsec library in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
ike	Specify the log level for IKE SA/ISAKMP SA in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
IMC	Specify the logging level of the Integrity Measurement Collector (IMC) in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
imv	Specify the logging level of the Integrity Measurement Verifier (LMV) in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
job	Specify the logging level for queuing/processing and thread pool management in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
knl	Specify the logging level for the kernel interface of the IPsec network in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
lib	Specify the log level of the strongswan library in LOGLEVEL. You can specify silent, audit, control, controlmore, raw, and private.
mgr	Specify the log level of the IKE_SA manager that handles synchronization of IKE_SA accesses in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
net	Specify the logging level for packet exchange in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
pts.	Specify the logging level of PTS (Platform Trust Service) in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
tls.	Specify the log level of the TLS library in LOGLEVEL. You can specify silent, audit, control, controlmore, raw, and private.
tnc	Specify the logging level for the TNC (Trusted Network Connect) feature in LOGLEVEL. The following can be specified: silent, audit, control, controlmore, raw, and private.
exit	Exit the detailed setting mode and enter the setting mode.

設定モード

```
amnimo(cfg)# ipsec log-level ←  
amnimo(cfg-ips-log)# asn controlmore  
amnimo(cfg-ips-log)# cfg controlmore  
amnimo(cfg-ips-log)# chd controlmore  
amnimo(cfg-ips-log)# dmn controlmore  
amnimo(cfg-ips-log)# enc controlmore  
amnimo(cfg-ips-log)# esp controlmore  
amnimo(cfg-ips-log)# ike controlmore  
amnimo(cfg-ips-log)# imc controlmore  
amnimo(cfg-ips-log)# imv controlmore  
amnimo(cfg-ips-log)# job controlmore  
amnimo(cfg-ips-log)# knl controlmore  
amnimo(cfg-ips-log)# lib controlmore  
amnimo(cfg-ips-log)# mgr controlmore  
amnimo(cfg-ips-log)# net controlmore  
amnimo(cfg-ips-log)# pts controlmore  
amnimo(cfg-ips-log)# tls controlmore  
amnimo(cfg-ips-log)# tnc controlmore  
amnimo(cfg-ips-log)# exit
```

Configure IPsec IKE

To configure IPsec IKE, run the *ipsec ike* command.

Format

```
ipsec ike ike-name
local address <any | LOCAL-ADDRESS> (in Japanese only)
local id <ipv4 ADDRESS | ipv6 ADDRESS | fqdn FQDN | userfqdn USERFQDN | key KEYID>
no local id
remote address <any | REMOTE-ADDRESS> (in Japanese)
remote id <ipv4 ADDRESS | ipv6 ADDRESS | fqdn FQDN | userfqdn USERFQDN | key KEYID>
no remote id
version <1 | 2>
mobike
no mobike
authentication pre-shared-key [secret PRE-SHARED-KEY-DATA].
mode <main | aggressive
fragmentation
no fragmentation
retry <forever | <1 - 255>>>
transform restriction
no transform restriction
transform encryption <aes128 | aes192 | aes256 | 3des> integrity <md5 | sha1 | sha256 |
  sha384 | sha512> prf <md5 | sha1 | sha256 | sha384 | sha512 sha512> dh-group <1 | 2 |
  5 | 14 | 15 | 16 | 17 | 18>
no transform encryption <aes128 | aes192 | aes256 | 3des> integrity <md5 | sha1 | sha25
  6 | sha384 | sha512> prf <md5 | sha1 | sha256 | sha384 | sha512> dh-group <1 | 2 | 5 |
  14 | 15 | 16 | 17 | 18>
lifetime <1081s - 86400s | 1m - 1440m | 1h - 24h>.
dpd action <clear | hold | restart
no dpd action
dpd interval <1s - 86400s | 1m - 1440m | 1h - 24h>.
dpd timeout <1s - 86400s | 1m - 1440m | 1h - 24h>.
exit
no ipsec ike ike-name
```

Command

Command	Contents												
ipsec ike	Execute the command to configure an IKE for IPsec, specifying the IKE name in IKE-NAME.  Executing a command in the configuration mode will enter the advanced configuration mode of the IKE.												
local address	Set LOCAL-ADDRESS to the address of the local side. To allow all addresses, specify "any".												
local id	Set the local side ID. <table border="1" data-bbox="571 1653 1353 2092"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ipv4</td> <td>Set the IPv4 format address to ADDRESS.</td> </tr> <tr> <td>ipv6</td> <td>Set the IPv6 format address to ADDRESS.</td> </tr> <tr> <td>fqdn</td> <td>Set the FQDN to an address in FQDN format.</td> </tr> <tr> <td>userfqdn</td> <td>Set USERFQDN to an address in USER FQDN format.</td> </tr> <tr> <td>key</td> <td>  ID payload type is RFC822_ADDR ID.  Set an ID in the KEY ID format to KEYID.  ID with an ID payload type of KEY_ID.</td> </tr> </tbody> </table>	Setting	Contents	ipv4	Set the IPv4 format address to ADDRESS.	ipv6	Set the IPv6 format address to ADDRESS.	fqdn	Set the FQDN to an address in FQDN format.	userfqdn	Set USERFQDN to an address in USER FQDN format.	key	 ID payload type is RFC822_ADDR ID.  Set an ID in the KEY ID format to KEYID.  ID with an ID payload type of KEY_ID.
Setting	Contents												
ipv4	Set the IPv4 format address to ADDRESS.												
ipv6	Set the IPv6 format address to ADDRESS.												
fqdn	Set the FQDN to an address in FQDN format.												
userfqdn	Set USERFQDN to an address in USER FQDN format.												
key	 ID payload type is RFC822_ADDR ID.  Set an ID in the KEY ID format to KEYID.  ID with an ID payload type of KEY_ID.												

Command	Contents													
no local id	Delete the local side ID setting.													
remote address	Set the REMOTE-ADDRESS to the address of the remote (destination) side. To allow all addresses, specify "any".													
remote id	Set the remote side ID. <table border="1" data-bbox="571 302 1353 743"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ipv4</td> <td>Set the IPv4 format address to ADDRESS.</td> </tr> <tr> <td>ipv6</td> <td>Set the IPv6 format address to ADDRESS.</td> </tr> <tr> <td>fqdn</td> <td>Set the FQDN to an address in FQDN format.</td> </tr> <tr> <td>userfqdn</td> <td>Set USERFQDN to an address in USER FQDN format.</td> </tr> <tr> <td rowspan="2">key</td> <td> ID payload type is RFC822_ADDR ID.</td> </tr> <tr> <td> ID with an ID payload type of KEY_ID.</td> </tr> </tbody> </table>	Setting	Contents	ipv4	Set the IPv4 format address to ADDRESS.	ipv6	Set the IPv6 format address to ADDRESS.	fqdn	Set the FQDN to an address in FQDN format.	userfqdn	Set USERFQDN to an address in USER FQDN format.	key	 ID payload type is RFC822_ADDR ID.	 ID with an ID payload type of KEY_ID.
Setting	Contents													
ipv4	Set the IPv4 format address to ADDRESS.													
ipv6	Set the IPv6 format address to ADDRESS.													
fqdn	Set the FQDN to an address in FQDN format.													
userfqdn	Set USERFQDN to an address in USER FQDN format.													
key	 ID payload type is RFC822_ADDR ID.													
	 ID with an ID payload type of KEY_ID.													
no remote id	Deletes the remote side ID setting.													
version	Sets the IKE version. <table border="1" data-bbox="571 840 1353 967"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Set IKE version 1.</td> </tr> <tr> <td>2</td> <td>Set IKE version 2.</td> </tr> </tbody> </table>	Setting	Contents	1	Set IKE version 1.	2	Set IKE version 2.							
Setting	Contents													
1	Set IKE version 1.													
2	Set IKE version 2.													
mobike	Enables Mobike protocol operation.  Valid only for IKEv2.													
no mobike	Disables Mobike protocol operation.  Valid only for IKEv2.													
authentication	Configure authentication settings. <table border="1" data-bbox="571 1265 1353 1460"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>pre-shared-key*</td> <td>Specify a pre-shared key (PSK) in PRE-SHARED-KEY-DATA.</td> </tr> <tr> <td>secret</td> <td>Used to specify the preshared key (PSK) as an encrypted string.</td> </tr> </tbody> </table>  Due to a typographical error, "pre-shard-key" is used in AG/AR. This will be corrected in a future release.	Setting	Contents	pre-shared-key*	Specify a pre-shared key (PSK) in PRE-SHARED-KEY-DATA.	secret	Used to specify the preshared key (PSK) as an encrypted string.							
Setting	Contents													
pre-shared-key*	Specify a pre-shared key (PSK) in PRE-SHARED-KEY-DATA.													
secret	Used to specify the preshared key (PSK) as an encrypted string.													
mode	Specifies the IKE mode.  Valid only for IKEv1. <table border="1" data-bbox="571 1668 1353 1796"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>main</td> <td>Set to main mode.</td> </tr> <tr> <td>aggressive</td> <td>Set to aggressive mode.</td> </tr> </tbody> </table>	Setting	Contents	main	Set to main mode.	aggressive	Set to aggressive mode.							
Setting	Contents													
main	Set to main mode.													
aggressive	Set to aggressive mode.													
fragmentation	Enable fragmentation.													
no fragmentation	Disable fragmentation.													
retry	Set the number of retries in the range of 1 to 255. Specify "forever" for no limit on the number of retries.													
transform restriction	Enables behavior limited to specified transforms only.													
no transform restriction	Disables the behavior of limiting to specified transforms only.													
transform	Set the transform settings. Up to four transforms can be set. The													

Command	Contents										
	<p>indexes are added in the order of setting.</p> <table border="1" data-bbox="571 181 1353 2045"> <thead> <tr> <th data-bbox="571 181 791 219">Setting</th> <th data-bbox="791 181 1353 219">Contents</th> </tr> </thead> <tbody> <tr> <td data-bbox="571 219 791 533">encryption</td> <td data-bbox="791 219 1353 533"> Specify one of the following encryption algorithms <ul style="list-style-type: none"> ● aes128 AES-CBC 128bits ● aes192 AES-CBC 192bits ● aes256 AES-CBC 256bits ● 3des 3DES </td> </tr> <tr> <td data-bbox="571 533 791 943">integrity</td> <td data-bbox="791 533 1353 943"> Specify one of the following authentication algorithms <ul style="list-style-type: none"> ● md5 MD5 HMAC ● sha1 SHA1 HMAC ● sha256 SHA2-256 HMAC ● sha384 SHA2-384 HMAC ● sha512 SHA2-512 HMAC </td> </tr> <tr> <td data-bbox="571 943 791 1440">prf</td> <td data-bbox="791 943 1353 1440"> Specify one of the following PRFs (Pseudo-Random Functions)  Valid only for IKEv2. <ul style="list-style-type: none"> ● md5 MD5 PRF ● sha1 SHA1 PRF ● sha256 SHA2_256 PRF ● sha384 SHA2_384 PRF ● sha512 SHA2_512 PRF </td> </tr> <tr> <td data-bbox="571 1440 791 2045">dh-group</td> <td data-bbox="791 1440 1353 2045"> Specify one of the following Diffie Hellman Groups <ul style="list-style-type: none"> ● 1 DH Group 1 (MODP768) ● 2 DH Group 2 (MODP1024) ● 5 DH Group 5 (MODP1536) ● 14 DH Group 14 (MODP2048) ● 15 DH Group 15 (MODP3072) ● 16 DH Group 16 (MODP4096) ● 17 DH Group 17 (MODP6144) ● 18 DH Group 18 (MODP8192) </td> </tr> </tbody> </table>	Setting	Contents	encryption	Specify one of the following encryption algorithms <ul style="list-style-type: none"> ● aes128 AES-CBC 128bits ● aes192 AES-CBC 192bits ● aes256 AES-CBC 256bits ● 3des 3DES 	integrity	Specify one of the following authentication algorithms <ul style="list-style-type: none"> ● md5 MD5 HMAC ● sha1 SHA1 HMAC ● sha256 SHA2-256 HMAC ● sha384 SHA2-384 HMAC ● sha512 SHA2-512 HMAC 	prf	Specify one of the following PRFs (Pseudo-Random Functions)  Valid only for IKEv2. <ul style="list-style-type: none"> ● md5 MD5 PRF ● sha1 SHA1 PRF ● sha256 SHA2_256 PRF ● sha384 SHA2_384 PRF ● sha512 SHA2_512 PRF 	dh-group	Specify one of the following Diffie Hellman Groups <ul style="list-style-type: none"> ● 1 DH Group 1 (MODP768) ● 2 DH Group 2 (MODP1024) ● 5 DH Group 5 (MODP1536) ● 14 DH Group 14 (MODP2048) ● 15 DH Group 15 (MODP3072) ● 16 DH Group 16 (MODP4096) ● 17 DH Group 17 (MODP6144) ● 18 DH Group 18 (MODP8192)
Setting	Contents										
encryption	Specify one of the following encryption algorithms <ul style="list-style-type: none"> ● aes128 AES-CBC 128bits ● aes192 AES-CBC 192bits ● aes256 AES-CBC 256bits ● 3des 3DES 										
integrity	Specify one of the following authentication algorithms <ul style="list-style-type: none"> ● md5 MD5 HMAC ● sha1 SHA1 HMAC ● sha256 SHA2-256 HMAC ● sha384 SHA2-384 HMAC ● sha512 SHA2-512 HMAC 										
prf	Specify one of the following PRFs (Pseudo-Random Functions)  Valid only for IKEv2. <ul style="list-style-type: none"> ● md5 MD5 PRF ● sha1 SHA1 PRF ● sha256 SHA2_256 PRF ● sha384 SHA2_384 PRF ● sha512 SHA2_512 PRF 										
dh-group	Specify one of the following Diffie Hellman Groups <ul style="list-style-type: none"> ● 1 DH Group 1 (MODP768) ● 2 DH Group 2 (MODP1024) ● 5 DH Group 5 (MODP1536) ● 14 DH Group 14 (MODP2048) ● 15 DH Group 15 (MODP3072) ● 16 DH Group 16 (MODP4096) ● 17 DH Group 17 (MODP6144) ● 18 DH Group 18 (MODP8192) 										

Command	Contents								
no transform	Delete transform settings. The options that can be set are the same as for the transform command.								
lifetime	Sets the lifetime of IKE. It can be specified in seconds, minutes, or hours. <table border="1"> <thead> <tr> <th>Unit</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>seconds</td> <td>Specify in the range of 1081s to 86400s.</td> </tr> <tr> <td>minutes</td> <td>Specify a range from 1m to 1440m.</td> </tr> <tr> <td>hours</td> <td>Specify in the range of 1h to 24h.</td> </tr> </tbody> </table>	Unit	Contents	seconds	Specify in the range of 1081s to 86400s.	minutes	Specify a range from 1m to 1440m.	hours	Specify in the range of 1h to 24h.
Unit	Contents								
seconds	Specify in the range of 1081s to 86400s.								
minutes	Specify a range from 1m to 1440m.								
hours	Specify in the range of 1h to 24h.								
dpd action	Specifies the action to be taken when disconnected by DPD (Dead Peer Detection). <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>clear</td> <td>Delete SA information. After deleting the information, it will not automatically connect.</td> </tr> <tr> <td>hold</td> <td>After deleting the SA information, if there is communication that matches the IPsec settings, IKE negotiation processing is performed.</td> </tr> <tr> <td>restart</td> <td>After deleting the SA information, IKE negotiation is initiated.</td> </tr> </tbody> </table>	Setting	Contents	clear	Delete SA information. After deleting the information, it will not automatically connect.	hold	After deleting the SA information, if there is communication that matches the IPsec settings, IKE negotiation processing is performed.	restart	After deleting the SA information, IKE negotiation is initiated.
Setting	Contents								
clear	Delete SA information. After deleting the information, it will not automatically connect.								
hold	After deleting the SA information, if there is communication that matches the IPsec settings, IKE negotiation processing is performed.								
restart	After deleting the SA information, IKE negotiation is initiated.								
no dpd action	Delete DPD settings.								
dpd interval	Sets the interval for DPD. Can be specified in seconds, minutes, or hours. <table border="1"> <thead> <tr> <th>Unit</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>seconds</td> <td>Specify in the range of 1s to 86400s.</td> </tr> <tr> <td>minutes</td> <td>Specify a range from 1m to 1440m.</td> </tr> <tr> <td>hours</td> <td>Specify in the range of 1h to 24h.</td> </tr> </tbody> </table>	Unit	Contents	seconds	Specify in the range of 1s to 86400s.	minutes	Specify a range from 1m to 1440m.	hours	Specify in the range of 1h to 24h.
Unit	Contents								
seconds	Specify in the range of 1s to 86400s.								
minutes	Specify a range from 1m to 1440m.								
hours	Specify in the range of 1h to 24h.								
dpd timeout	Sets the timeout for DPD. Can be specified in seconds, minutes, or hours. <table border="1"> <thead> <tr> <th>Unit</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>seconds</td> <td>Specify in the range of 1s to 86400s.</td> </tr> <tr> <td>minutes</td> <td>Specify a range from 1m to 1440m.</td> </tr> <tr> <td>hours</td> <td>Specify in the range of 1h to 24h.</td> </tr> </tbody> </table>	Unit	Contents	seconds	Specify in the range of 1s to 86400s.	minutes	Specify a range from 1m to 1440m.	hours	Specify in the range of 1h to 24h.
Unit	Contents								
seconds	Specify in the range of 1s to 86400s.								
minutes	Specify a range from 1m to 1440m.								
hours	Specify in the range of 1h to 24h.								
no ipsec ike	Specify the IKE name in IKE-NAME to delete the setting.								
exit	Exit the detailed setting mode and enter the setting mode.								

Execution example

The following is an example of running the IKE-side configuration for IPsec connection.

設定モード

```
amnimo(cfg)# ipsec ike ike01 ↵
amnimo(cfg-ips-ike-ike01)# local address 192.168.0.254 ↵
amnimo(cfg-ips-ike-ike01)# remote address 192.168.0.253 ↵
amnimo(cfg-ips-ike-ike01)# version 2 ↵
amnimo(cfg-ips-ike-ike01)# mobike ↵
amnimo(cfg-ips-ike-ike01)# authentication pre-shared-key secret dGVzdA== ↵
amnimo(cfg-ips-ike-ike01)# mode main ↵
amnimo(cfg-ips-ike-ike01)# fragmentation ↵
amnimo(cfg-ips-ike-ike01)# retry 3 ↵
amnimo(cfg-ips-ike-ike01)# transform encryption aes128 integrity sha1 prf sha1 dh-grou
```

```
p 14 ↵  
amnimo(cfg-ips-ike-ike01)# lifetime 3h ↵  
amnimo(cfg-ips-ike-ike01)# dpd action restart ↵  
amnimo(cfg-ips-ike-ike01)# dpd interval 150s ↵  
amnimo(cfg-ips-ike-ike01)# dpd timeout 30s ↵  
amnimo(cfg-ips-ike-ike01)# exit ↵
```

Configure IPsec SA

To configure IPsec SA, run the *ipsec sa* command.

Format

```
ipsec sa SA-NAME
enable
no enable
key-exchange ike IKE-NAME
negotiation-mode <initiate | ondemand | hold
rekey
no rekey
type <esp | ah>
mode <tunnel | transport
ipcomp
no ipcomp
anti-replay
no anti-replay
transform restriction
no transform restriction
transform encryption <aes128 | aes192 | aes256 | 3des> integrity <md5 | sha1 | sha256 |
sha384 | sha512> [pfs <1 | 2 | 5 | 14 | 15 | 16 | 17 | 18 | none>]
no transform encryption <aes128 | aes192 | aes256 | 3des> integrity <md5 | sha1 | sha25
6 | sha384 | sha512> [pfs <1 | 2 | 5 | 14 | 15 | 16 | 17 | 18 | none>]
lifetime <1081s - 86400s | 1m - 1440m | 1h - 24h>.
local subnet <X.X.X.X/XX | X:X::X:X/XX>
no local subnet [<X.X.X.X/XX | X:X::X:X/XX>]
remote subnet <X.X.X.X/XX | X:X::X:X/XX>
no remote subnet [<X.X.X.X/XX | X:X::X:X/XX>]
exit
no ipsec sa SA-NAME
```

Command

Command	Contents								
ipsec sa	Execute the command to configure the SA for IPsec, specifying the SA name in SA-NAME.  Executing a command in the setting mode will shift the SA into the detailed setting mode.								
enable	Enable IPsec SA settings.								
no enable	Disable IPsec SA settings.								
key-exchange ike	Specify the IKE name to be used in the key exchange in IKE-NAME.								
negotiation-mode	Configure IPsec connection behavior.  IPsec connections work in the following order <ul style="list-style-type: none"> ● Perform the INITIATE operation ● Add a route (initiate operation by communication) ● Only SA setting is performed (initiate operation is not performed) <p>Note that in all settings, when Initiate communication is received from the other party, it will operate as the Responder side if possible.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>initiate</td> <td>Specifies the operation to Initiate.</td> </tr> <tr> <td>ondemand</td> <td>Specifies the action to add a route (initiate action by communication).</td> </tr> <tr> <td>hold</td> <td>Specifies an action that only sets SA.</td> </tr> </tbody> </table>	Setting	Contents	initiate	Specifies the operation to Initiate.	ondemand	Specifies the action to add a route (initiate action by communication).	hold	Specifies an action that only sets SA.
Setting	Contents								
initiate	Specifies the operation to Initiate.								
ondemand	Specifies the action to add a route (initiate action by communication).								
hold	Specifies an action that only sets SA.								

Command	Contents								
rekey	Enable rekey.								
no rekey	Disable rekey.								
type	Specifies the protocol type.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>esp</td> <td>Specifies the ESP protocol.</td> </tr> <tr> <td>ah</td> <td>Specifies the AH protocol.</td> </tr> </tbody> </table>	Setting	Contents	esp	Specifies the ESP protocol.	ah	Specifies the AH protocol.		
	Setting	Contents							
esp	Specifies the ESP protocol.								
ah	Specifies the AH protocol.								
mode	<p>Specifies the communication mode.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>tunnel</td> <td>Specifies tunnel mode. IPsec communication between host-host, host-subnet, and subnet-subnet.</td> </tr> <tr> <td>transport</td> <td>Specifies the transport mode. IPsec communication between host and host.</td> </tr> <tr> <td>passthrough</td> <td>Specifies the pass-through mode. IPsec communication is not performed for the specified subnet.</td> </tr> </tbody> </table> <p> Pass-through mode is not an IPsec pass-through function.</p>	Setting	Contents	tunnel	Specifies tunnel mode. IPsec communication between host-host, host-subnet, and subnet-subnet.	transport	Specifies the transport mode. IPsec communication between host and host.	passthrough	Specifies the pass-through mode. IPsec communication is not performed for the specified subnet.
Setting	Contents								
tunnel	Specifies tunnel mode. IPsec communication between host-host, host-subnet, and subnet-subnet.								
transport	Specifies the transport mode. IPsec communication between host and host.								
passthrough	Specifies the pass-through mode. IPsec communication is not performed for the specified subnet.								
ipcomp	Enables IPComp (IP Payload Compression Protocol).								
no ipcomp	Disables IPComp.								
anti-replay	Enables the replay protection setting.								
no anti-replay	Disables the replay protection setting.								
transform restriction	Enables behavior limited to specified transforms only.								
no transform restriction	Disables the behavior of limiting to specified transforms only.								
transform	Set the transform settings. Up to four transforms can be set. The indexes are added in the order of setting.								
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>encryption</td> <td>Specify one of the following encryption algorithms <ul style="list-style-type: none"> ● aes128 AES-CBC 128bits ● aes192 AES-CBC 192bits ● aes256 AES-CBC 256bits ● 3des 3DES </td> </tr> <tr> <td>integrity</td> <td>Specify one of the following authentication algorithms <ul style="list-style-type: none"> ● md5 MD5 HMAC ● sha1 SHA1 HMAC ● sha256 SHA2-256 HMAC ● sha384 SHA2-384 HMAC ● sha512 SHA2-512 HMAC </td> </tr> </tbody> </table>	Setting	Contents	encryption	Specify one of the following encryption algorithms <ul style="list-style-type: none"> ● aes128 AES-CBC 128bits ● aes192 AES-CBC 192bits ● aes256 AES-CBC 256bits ● 3des 3DES 	integrity	Specify one of the following authentication algorithms <ul style="list-style-type: none"> ● md5 MD5 HMAC ● sha1 SHA1 HMAC ● sha256 SHA2-256 HMAC ● sha384 SHA2-384 HMAC ● sha512 SHA2-512 HMAC 		
	Setting	Contents							
encryption	Specify one of the following encryption algorithms <ul style="list-style-type: none"> ● aes128 AES-CBC 128bits ● aes192 AES-CBC 192bits ● aes256 AES-CBC 256bits ● 3des 3DES 								
integrity	Specify one of the following authentication algorithms <ul style="list-style-type: none"> ● md5 MD5 HMAC ● sha1 SHA1 HMAC ● sha256 SHA2-256 HMAC ● sha384 SHA2-384 HMAC ● sha512 SHA2-512 HMAC 								

Command	Contents								
	<table border="1"> <tr> <td>pfs</td> <td> Specify one of the following PFS (Perfect Forward Secrecy) <ul style="list-style-type: none"> ● 1 DH Group 1 (MODP768) ● 2 DH Group 2 (MODP1024) ● 5 DH Group 5 (MODP1536) ● 14 DH Group 14 (MODP2048) ● 15 DH Group 15 (MODP3072) ● 16 DH Group 16 (MODP4096) ● 17 DH Group 17 (MODP6144) ● 18 DH Group 18 (MODP8192) ● Not specified PFS is not used. </td> </tr> </table>	pfs	Specify one of the following PFS (Perfect Forward Secrecy) <ul style="list-style-type: none"> ● 1 DH Group 1 (MODP768) ● 2 DH Group 2 (MODP1024) ● 5 DH Group 5 (MODP1536) ● 14 DH Group 14 (MODP2048) ● 15 DH Group 15 (MODP3072) ● 16 DH Group 16 (MODP4096) ● 17 DH Group 17 (MODP6144) ● 18 DH Group 18 (MODP8192) ● Not specified PFS is not used. 						
pfs	Specify one of the following PFS (Perfect Forward Secrecy) <ul style="list-style-type: none"> ● 1 DH Group 1 (MODP768) ● 2 DH Group 2 (MODP1024) ● 5 DH Group 5 (MODP1536) ● 14 DH Group 14 (MODP2048) ● 15 DH Group 15 (MODP3072) ● 16 DH Group 16 (MODP4096) ● 17 DH Group 17 (MODP6144) ● 18 DH Group 18 (MODP8192) ● Not specified PFS is not used. 								
no transform	Delete transform settings. The options that can be set are the same as for the transform command.								
lifetime	Sets the SA lifetime. It can be specified in seconds, minutes, or hours. <table border="1"> <thead> <tr> <th>Unit</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>seconds</td> <td>Specify in the range of 1081s to 86400s.</td> </tr> <tr> <td>minutes</td> <td>Specify a range from 1m to 1440m.</td> </tr> <tr> <td>hours</td> <td>Specify in the range of 1h to 24h.</td> </tr> </tbody> </table>	Unit	Contents	seconds	Specify in the range of 1081s to 86400s.	minutes	Specify a range from 1m to 1440m.	hours	Specify in the range of 1h to 24h.
Unit	Contents								
seconds	Specify in the range of 1081s to 86400s.								
minutes	Specify a range from 1m to 1440m.								
hours	Specify in the range of 1h to 24h.								
local subnet	Set the local-side subnet in the following format X.X.X.X/XX X:X::X:X/XX  A maximum of four can be set. However, only IKEv2 allows multiple settings.								
no local subnet	Deletes the specified local-side subnet.								
remote subnet	Set the remote side subnet in the following format X.X.X.X/XX X:X::X:X/XX  A maximum of four can be set. However, only IKEv2 allows multiple settings.								
no remote subnet	Deletes the specified remote-side subnet.								
exit	Exit the detailed setting mode and enter the setting mode.								
no ipsec sa	Specify the SA name in SA-NAME to delete the setting.								

Execution example

Below is an example of running the ISA-side configuration for an IPsec connection.

設定 モード

```
amnimo(cfg)# ipsec sa sa01 ↵
amnimo(cfg-ips-sa-sa01)# enable ↵
amnimo(cfg-ips-sa-sa01)# key-exchange ike ike01 ↵
amnimo(cfg-ips-sa-sa01)# negotiation-mode initiate ↵
amnimo(cfg-ips-sa-sa01)# rekey ↵
amnimo(cfg-ips-sa-sa01)# type esp ↵
amnimo(cfg-ips-sa-sa01)# mode tunnel ↵
amnimo(cfg-ips-sa-sa01)# anti-replay ↵
amnimo(cfg-ips-sa-sa01)# transform encryption aes128 integrity sha1 pfs 14 ↵
amnimo(cfg-ips-sa-sa01)# lifetime 1h ↵
amnimo(cfg-ips-sa-sa01)# local subnet 192.168.10.0/24 ↵
amnimo(cfg-ips-sa-sa01)# remote subnet 192.168.20.0/24 ↵
amnimo(cfg-ips-sa-sa01)# exit ↵
```

6.8 Configure wireless LAN settings



Configures, displays status of, and controls wireless LAN functions.

6.8.1 Displays the status of the wireless LAN access point

To display the status of a wireless LAN access point, run the ***show wifi access-point*** command. You can also specify the interface by adding it as an argument.

Format

```
show wifi access-point [WIFI-IFNAME].
```

Setting items

Item	Contents
WIFI-IFNAME	Used to specify and display the wireless LAN interface. <ul style="list-style-type: none"> ● Compact Router Indoor Type / Outdoor Type with wireless LAN wlan0, wlan1  If WIFI-IFNAME is omitted, information on all wireless LAN access point interfaces will be displayed.

Output Format

```

WIFI-IFNAME
state           STATE
ssid           SSID
bssid          BSSID
channel        CHANNEL
rx bytes       RX-BYTES
rx packets     RX-PACKETS
tx bytes       TX-BYTES
tx packets     TX-PACKETS
tx errors      TX-ERRS
tx dropped     TX-DROP
connected stations STATION

```

Output item

Item	Contents										
STATE	Displays the status of the specified wireless LAN interface. <table border="1" data-bbox="446 1500 1348 1915"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>COUNTRY_UPDATE</td> <td>The state of updating the network's national information (regulatory information on frequency bands and channel settings).</td> </tr> <tr> <td>HT_SCAN</td> <td>The state of scanning station devices and collecting corresponding radio standards, channel information, etc.</td> </tr> <tr> <td>ENABLE</td> <td>Access point is activated. Station equipment is ready to access the access point network.</td> </tr> <tr> <td>STOP</td> <td>The state in which the function of the access point is deactivated.</td> </tr> </tbody> </table>	Display	Contents	COUNTRY_UPDATE	The state of updating the network's national information (regulatory information on frequency bands and channel settings).	HT_SCAN	The state of scanning station devices and collecting corresponding radio standards, channel information, etc.	ENABLE	Access point is activated. Station equipment is ready to access the access point network.	STOP	The state in which the function of the access point is deactivated.
Display	Contents										
COUNTRY_UPDATE	The state of updating the network's national information (regulatory information on frequency bands and channel settings).										
HT_SCAN	The state of scanning station devices and collecting corresponding radio standards, channel information, etc.										
ENABLE	Access point is activated. Station equipment is ready to access the access point network.										
STOP	The state in which the function of the access point is deactivated.										
SSID	Displays the SSID (ServiceSet Identifier) of the specified wireless LAN interface.										
BSSID	Displays the BSSID (Basic ServiceSet Identifier) of the specified wireless LAN interface.										
CHANNEL	Displays the channel number of the specified wireless LAN interface.										

Item	Contents
RX-BYTES	Displays the number of bytes received for the specified wireless LAN interface.
RX-PACKETS	Displays the number of packets received on the specified wireless LAN interface.
TX-BYTES	Displays the number of bytes transmitted for the specified wireless LAN interface.
TX-PACKETS	Displays the number of packets sent on the specified wireless LAN interface.
TX-ERRS	Displays the number of outgoing packets that could not be processed due to CRC errors detected on the specified wireless LAN interface.
TX-DROP	Displays the number of outgoing packets of unsupported protocols intentionally discarded for the specified wireless LAN interface.
STATION	Displays the number of devices connected to the specified wireless LAN interface.

Execution example

The input and output of the command is the same in all modes. Below is an example of running the command to display the status of the access point in wlan0 in administrator mode.

ユーザーモード
管理者モード
設定モード

```
amnimo# show wifi access-point wlan0
wlan0
state ENABLED
ssid amnimo-2G-123456
bssid 34:69:87:12:34:56
channel 12
rx bytes 24792964
rx packets 198437
tx bytes 68585289
tx packets 89658
tx errs 0
tx drop 0
connected stations 1
```

6.8.2 Display a list of devices connected to the wireless LAN access point

To view a list of devices (stations) connected to the wireless LAN access point, run the ***show wifi connect*** command. You must add the interface as an argument.

Format

```
show wifi connect WIFI-IFNAME access-point
```

Setting items

Item	Contents
WIFI-IFNAME	Used to specify the wireless LAN interface. <ul style="list-style-type: none"> ● Compact Router Indoor Type with wireless LAN wlan0, wlan1

Output Format

```
MAC-ADDRESS  
...  
MAC-ADDRESS
```

Output item

Item	Contents
MAC-ADDRESS	The MAC address of the connected station is displayed in the following format <pre>xx:xx:xx:xx:xx:xx</pre> xx is a hexadecimal number.

Execution example

The input and output of the command is the same in all modes. Below is an example of running the command to display the status of the access point in wlan0 in administrator mode.

ユーザーモード
管理者モード
設定モード

```
amnimo# show wifi connect wlan0 access-point
e8:1b:4b:00:45:ea
00:00:5e:00:53:5a
00:00:5e:00:53:60
```

6.8.3 Disconnect the device connected to the wireless LAN access point

To disconnect a device (station) connected to a wireless LAN access point, execute the *no wifi connect* command. The target interface and the MAC address of the target device must be added as arguments.

Format

```
no wifi connect WIFI-IFNAME access-point MAC-ADDRESS
```

Setting items

Item	Contents
WIFI-IFNAME	Used to specify the wireless LAN interface. <ul style="list-style-type: none"> ● Compact Router Indoor Type / Outdoor Type with wireless LAN wlan0, wlan1
MAC-ADDRESS	The MAC address of the connected station is specified in the following format <div style="text-align: center; background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <code>xx:xx:xx:xx:xx:xx</code> </div> xx is a hexadecimal number.

Execution example

The input and output of the command is the same in administrator mode and configuration mode. Below is an example execution that displays disconnecting station 00:00:5e:00:53:4c, which is connected to the wlan0 access point in administrator mode.

管理者 モード 設定 モード

```
amnimo# no wifi connect wlan0 access-point 00:00:5e:00:53:4c
```

6.8.4 View wireless LAN access point settings

To display the wireless LAN access point configuration, run the *show config wifi access-point* command. You can also specify the access point by adding it as an argument.

Format

```
show config wifi access-point [AP-NAME].
```

Setting items

Item	Contents
AP-NAME	Specify the name of the wireless LAN access point whose settings are to be displayed.

Output Format

```
# ---- Transition to configure mode ----
configure
# ---- access-point AP-NAME configure ----
wifi access-point AP-NAME
ENABLED
band BAND
SSID
channel mode MODE
NUMBER
channel width WIDTH
SHORT-GUARD-INTERVAL
transmit-power TRANSMIT-POWER
max-station MAX-STATION
STEALTH
PRIVACY-SEPARATOR
dtim-period DTIM-PERIOD
beacon-interval BEACON-INTERVAL
RTS-THRESHOLD
security type TYPE
SECURITY-KEY
REKEY
MAC-ADDRESS-FILTERING
MAC-ADDRESS
exit
# ---- Exit configure mode ----
exit
```

Output item

Item	Contents						
AP-NAME	Displays the name of the wireless LAN access point whose settings are to be displayed.						
ENABLED.	Displays the enable/disable setting of the access point function. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
BAND	The frequency band setting used is displayed. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>2.4GHz</td> <td>2.4GHz" is displayed.</td> </tr> <tr> <td>5GHz</td> <td>5GHz" is displayed.</td> </tr> </tbody> </table>	Setting	Display	2.4GHz	2.4GHz" is displayed.	5GHz	5GHz" is displayed.
Setting	Display						
2.4GHz	2.4GHz" is displayed.						
5GHz	5GHz" is displayed.						
SSID	SSID will be displayed.						

Item	Contents												
MODE	Auto channel select mode setting is displayed.												
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>auto mode</td> <td>"auto" is displayed.</td> </tr> <tr> <td>manual mode</td> <td>The message "MANUAL" will appear.</td> </tr> </tbody> </table>	Setting	Display	auto mode	"auto" is displayed.	manual mode	The message "MANUAL" will appear.						
	Setting	Display											
	auto mode	"auto" is displayed.											
	manual mode	The message "MANUAL" will appear.											
	W52 mode	It will be labeled "w52."  Only if the frequency band is 5GHz.											
W53 mode	It will be labeled "w53."  Only if the frequency band is 5GHz.												
W56 mode	It will display "w56."  Only if the frequency band is 5GHz.												
NUMBER	<p>The connection channel number list setting is displayed. It is displayed in the following format</p> <p style="background-color: #e0e0e0; padding: 5px;">channel number CHANNEL_NUM</p> <table border="1"> <thead> <tr> <th>parameter</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>CHANNEL_NUM</td> <td>Channel numbers are displayed. If there are multiple channels, they are separated by ",".</td> </tr> </tbody> </table> <p> Not displayed when auto channel select mode setting is other than "manual mode"</p>	parameter	Display	CHANNEL_NUM	Channel numbers are displayed. If there are multiple channels, they are separated by ",".								
parameter	Display												
CHANNEL_NUM	Channel numbers are displayed. If there are multiple channels, they are separated by ",".												
WIDTH	The bandwidth settings are displayed.												
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>20 MHz bandwidth system</td> <td>"20 MHz" is displayed.</td> </tr> <tr> <td>40 MHz bandwidth system (HT40+, lower end of primary channel)</td> <td>"40 MHz+" is displayed.</td> </tr> <tr> <td>40 MHz bandwidth system (HT40-, upper end of primary channel)</td> <td>"40MHz-" is displayed.</td> </tr> <tr> <td>80 MHz bandwidth system (VHT80)</td> <td>"80 MHz" is displayed.</td> </tr> </tbody> </table>	Setting	Display	20 MHz bandwidth system	"20 MHz" is displayed.	40 MHz bandwidth system (HT40+, lower end of primary channel)	"40 MHz+" is displayed.	40 MHz bandwidth system (HT40-, upper end of primary channel)	"40MHz-" is displayed.	80 MHz bandwidth system (VHT80)	"80 MHz" is displayed.		
	Setting	Display											
	20 MHz bandwidth system	"20 MHz" is displayed.											
	40 MHz bandwidth system (HT40+, lower end of primary channel)	"40 MHz+" is displayed.											
40 MHz bandwidth system (HT40-, upper end of primary channel)	"40MHz-" is displayed.												
80 MHz bandwidth system (VHT80)	"80 MHz" is displayed.												
SHORT-GUARD-INTERVAL	<p>The short guard interval setting is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "channel short-guard-interval" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no channel short-guard-interval" is displayed.</td> </tr> </tbody> </table> <p> Always enabled when the bandwidth setting is "80 MHz Bandwidth System".</p>	Setting	Display	Enable	The message "channel short-guard-interval" is displayed.	Disable	The message "no channel short-guard-interval" is displayed.						
Setting	Display												
Enable	The message "channel short-guard-interval" is displayed.												
Disable	The message "no channel short-guard-interval" is displayed.												
TRANSMIT-POWER	The transmit output setting is displayed.												
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Transmitting output 10%.</td> <td>"10" is displayed.</td> </tr> <tr> <td>Transmission output 25</td> <td>"25" is displayed.</td> </tr> <tr> <td>Transmission output 50%.</td> <td>"50" is displayed.</td> </tr> <tr> <td>Transmission output 75</td> <td>"75" is displayed.</td> </tr> <tr> <td>Transmission output 100%.</td> <td>"100" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Transmitting output 10%.	"10" is displayed.	Transmission output 25	"25" is displayed.	Transmission output 50%.	"50" is displayed.	Transmission output 75	"75" is displayed.	Transmission output 100%.	"100" is displayed.
	Setting	Display											
	Transmitting output 10%.	"10" is displayed.											
	Transmission output 25	"25" is displayed.											
Transmission output 50%.	"50" is displayed.												
Transmission output 75	"75" is displayed.												
Transmission output 100%.	"100" is displayed.												
MAX-STATION	The maximum number of station connections setting is displayed. The range is "1 to 10".												

Item	Contents																																				
STEALTH	SSID stealth setting will be displayed.																																				
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be labeled "stealth".</td> </tr> <tr> <td>Disable</td> <td>The message "no stealth" appears.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be labeled "stealth".	Disable	The message "no stealth" appears.																														
	Setting	Display																																			
Enable	It will be labeled "stealth".																																				
Disable	The message "no stealth" appears.																																				
PRIVACY-SEPARATOR	The privacy separator setting appears.																																				
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be labeled "privacy-separator."</td> </tr> <tr> <td>Disable</td> <td>The message "no privacy-separator" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be labeled "privacy-separator."	Disable	The message "no privacy-separator" is displayed.																														
	Setting	Display																																			
Enable	It will be labeled "privacy-separator."																																				
Disable	The message "no privacy-separator" is displayed.																																				
DTIM-PERIOD	The cycle of DTIM (Delivery Traffic Information Message) included in the beacon is displayed. The range is from 1 to 255. When "1" is selected, DTIM is included in the beacon sent each time.																																				
BEACON-INTERVAL	The beacon interval (kus unit = 1.024 ms) setting is displayed. The range is "20 to 1024".																																				
RTS-THRESHOLD	The RTS threshold setting is displayed. The range is "1 to 2347".																																				
TYPE	The security type setting is displayed.																																				
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Open System Certification (without encryption)</td> <td>It will be labeled "open."</td> </tr> <tr> <td>Open system authentication 128bit WEP</td> <td>The message "open-wep128" is displayed.</td> </tr> <tr> <td>Open System Authentication 64bit WEP</td> <td>open-wep64" is displayed.</td> </tr> <tr> <td>Shared key authentication 128bit WEP</td> <td>It will be labeled "shared-wep128."</td> </tr> <tr> <td>Shared key authentication 64bit WEP</td> <td>It will be labeled "shared-wep64."</td> </tr> <tr> <td>WPA-PSK (Encryption: AES-CCMP)</td> <td>It will be labeled "wpa-psk-aes."</td> </tr> <tr> <td>WPA-PSK (encryption: mixed mode)</td> <td>The message "wpa-psk-mixed" is displayed.</td> </tr> <tr> <td>WPA-PSK (encryption: TKIP)</td> <td>wpa-psk-tkip" is displayed.</td> </tr> <tr> <td>WPA-PSK/WPA2-PSK authentication mixed mode (encryption: AES-CCMP)</td> <td>It will be displayed as "wpa-wpa2-mixed-psk-aes".</td> </tr> <tr> <td>WPA-PSK/WPA2-PSK authentication mixed mode (encryption: mixed mode)</td> <td>It will be displayed as "wpa-wpa2-mixed-psk-mixed".</td> </tr> <tr> <td>WPA-PSK/WPA2-PSK authentication mixed mode (encryption: TKIP)</td> <td>wpa-wpa2-mixed-psk-tkip".</td> </tr> <tr> <td>WPA2-PSK (Encryption: AES-CCMP)</td> <td>It will be labeled "wpa2-psk-aes."</td> </tr> <tr> <td>WPA2-PSK (encryption: mixed mode)</td> <td>It will be displayed as "wpa2-psk-mixed</td> </tr> <tr> <td>WPA2-PSK (encryption: TKIP)</td> <td>wpa2-psk-tkip."</td> </tr> <tr> <td>WPA2-PSK/WPA3-SAE certification mixed mode (encryption: AES-CCMP)</td> <td>wpa2-psk-wpa3-sae-mixed-aes".</td> </tr> <tr> <td>WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)</td> <td>wpa2-psk-wpa3-sae-mixed-mixed".</td> </tr> <tr> <td>WPA3-SAE authentication (encryption: AES-CCMP)</td> <td>It will be labeled "wpa3-sae-aes."</td> </tr> </tbody> </table>	Setting	Display	Open System Certification (without encryption)	It will be labeled "open."	Open system authentication 128bit WEP	The message "open-wep128" is displayed.	Open System Authentication 64bit WEP	open-wep64" is displayed.	Shared key authentication 128bit WEP	It will be labeled "shared-wep128."	Shared key authentication 64bit WEP	It will be labeled "shared-wep64."	WPA-PSK (Encryption: AES-CCMP)	It will be labeled "wpa-psk-aes."	WPA-PSK (encryption: mixed mode)	The message "wpa-psk-mixed" is displayed.	WPA-PSK (encryption: TKIP)	wpa-psk-tkip" is displayed.	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: AES-CCMP)	It will be displayed as "wpa-wpa2-mixed-psk-aes".	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: mixed mode)	It will be displayed as "wpa-wpa2-mixed-psk-mixed".	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: TKIP)	wpa-wpa2-mixed-psk-tkip".	WPA2-PSK (Encryption: AES-CCMP)	It will be labeled "wpa2-psk-aes."	WPA2-PSK (encryption: mixed mode)	It will be displayed as "wpa2-psk-mixed	WPA2-PSK (encryption: TKIP)	wpa2-psk-tkip."	WPA2-PSK/WPA3-SAE certification mixed mode (encryption: AES-CCMP)	wpa2-psk-wpa3-sae-mixed-aes".	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)	wpa2-psk-wpa3-sae-mixed-mixed".	WPA3-SAE authentication (encryption: AES-CCMP)	It will be labeled "wpa3-sae-aes."
	Setting	Display																																			
	Open System Certification (without encryption)	It will be labeled "open."																																			
	Open system authentication 128bit WEP	The message "open-wep128" is displayed.																																			
	Open System Authentication 64bit WEP	open-wep64" is displayed.																																			
	Shared key authentication 128bit WEP	It will be labeled "shared-wep128."																																			
	Shared key authentication 64bit WEP	It will be labeled "shared-wep64."																																			
	WPA-PSK (Encryption: AES-CCMP)	It will be labeled "wpa-psk-aes."																																			
	WPA-PSK (encryption: mixed mode)	The message "wpa-psk-mixed" is displayed.																																			
	WPA-PSK (encryption: TKIP)	wpa-psk-tkip" is displayed.																																			
	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: AES-CCMP)	It will be displayed as "wpa-wpa2-mixed-psk-aes".																																			
	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: mixed mode)	It will be displayed as "wpa-wpa2-mixed-psk-mixed".																																			
	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: TKIP)	wpa-wpa2-mixed-psk-tkip".																																			
	WPA2-PSK (Encryption: AES-CCMP)	It will be labeled "wpa2-psk-aes."																																			
	WPA2-PSK (encryption: mixed mode)	It will be displayed as "wpa2-psk-mixed																																			
WPA2-PSK (encryption: TKIP)	wpa2-psk-tkip."																																				
WPA2-PSK/WPA3-SAE certification mixed mode (encryption: AES-CCMP)	wpa2-psk-wpa3-sae-mixed-aes".																																				
WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)	wpa2-psk-wpa3-sae-mixed-mixed".																																				
WPA3-SAE authentication (encryption: AES-CCMP)	It will be labeled "wpa3-sae-aes."																																				

Item	Contents						
SECURITY-KEY	<p>WEP/PSK/SAE password settings will be displayed. It is displayed in the following format</p> <pre>#security key raw RAW_KEY security key secret ENCRYPTED-KEY</pre> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>RAW_KEY</td> <td>Password settings will be displayed.</td> </tr> <tr> <td>ENCRYPTED-KEY</td> <td>Encrypted password settings are displayed.</td> </tr> </tbody> </table>	Parameter	Display	RAW_KEY	Password settings will be displayed.	ENCRYPTED-KEY	Encrypted password settings are displayed.
Parameter	Display						
RAW_KEY	Password settings will be displayed.						
ENCRYPTED-KEY	Encrypted password settings are displayed.						
REKEY	<p>The KEY update interval (seconds) setting is displayed. It is displayed in the following format</p> <pre>channel rekey REKEY-PERIOD</pre> <table border="1"> <thead> <tr> <th>parameter</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>REKEY-PERIOD</td> <td>KEY update interval (sec)</td> </tr> </tbody> </table> <p> It may not be displayed depending on the security type setting.</p>	parameter	Display	REKEY-PERIOD	KEY update interval (sec)		
parameter	Display						
REKEY-PERIOD	KEY update interval (sec)						
MAC-ADDRESS-FILTERING	<p>The MAC address filtering settings are displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will say "mac-address-filtering."</td> </tr> <tr> <td>Disable</td> <td>The message "no mac-address-filtering" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will say "mac-address-filtering."	Disable	The message "no mac-address-filtering" is displayed.
Setting	Display						
Enable	It will say "mac-address-filtering."						
Disable	The message "no mac-address-filtering" is displayed.						
MAC-ADDRESS	<p>The connection permission MAC address setting is displayed. It is displayed in the following format</p> <pre>mac-address ACCEPT-MAC-ADDR</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ACCEPT-MAC-ADDR</td> <td>MAC address allowed to connect</td> </tr> </tbody> </table>	Setting items	Contents	ACCEPT-MAC-ADDR	MAC address allowed to connect		
Setting items	Contents						
ACCEPT-MAC-ADDR	MAC address allowed to connect						

Execution example

Command input and output are the same in administrator mode and configuration mode. Below is an example of running the command in administrator mode to display the wlan0 access point configuration.

Setting items	Configuration details
frequency band	5GHz
SSID Name	amnimo-5G-000000
auto channel select mode	manual mode
connection channel number list	36,52,100,116
bandwidth	80MHz
Short Guard Interval Setting	Enable
Transmission output setting	Transmission output 100%.
Maximum number of station devices connected	8 units
SSID stealth function	Disable
Privacy separator function	Enable
Beacon Interval	50kus
DTIM cycle	2
RTS Threshold	2347
Security Type	WPA2-PSK/WPA3-SAE certification Mixed mode (Encryption: mixed mode)
security key	amnimoAC15
MAC address filtering	Enable
connection allowed MAC address	00:00:5e:00:53:01 00:00:5e:00:53:02

管理者 モード 設定 モード

```
amnimo# show config wifi access-point amnimo-5G
# ---- access-point amnimo-5G configure ----
wifi access-point amnimo-5G
enable
band 5GHz
ssid amnimo-5g-000000
channel mode manual
channel number 36,52,100,116
channel width 80MHz
channel short-guard-interval
transmit-power 100
max-station 8
no stealth
privacy-separator
beacon-interval 50
dtim-period 2
rts-threshold 2347
security type wpa2-psk-wpa3-sae-mixed-mixed
#security key raw amnimoAC15
security key secret jjaAf/TE9Dd3NbApwgvDXg==
mac-address-filtering
mac-address 00:00:5e:00:53:01
mac-address 00:00:5e:00:53:02
exit
```

6.8.5 Configure wireless LAN access point settings

To configure the wireless LAN access point, go from the configuration mode to the advanced configuration mode and execute the configuration command. The settings made here will be written to a configuration file.

Format

```
wifi access-point AP-NAME
enable
no enable
band BAND
ssid SSID
channel mode MODE
channel number NUMBER
channel width WIDTH
channel short-guard-interval
no channel short-guard-interval
transmit-power TRANSMIT-POWER
max-station MAX-STATION
stealth
no stealth
privacy-separator
no privacy-separator
dtim-period DTIM-PERIOD
beacon-interval BEACON-INTERVAL
rts-threshold rts-threshold
no rts-threshold
security type TYPE
security key
security key secret ENCRYPT-KEY
no security key
security rekey REKEY-PERIOD
no security rekey
mac-address-filtering
no mac-address-filtering
mac-address ACCEPT-MAC-ADDR
no mac-address ACCEPT-MAC-ADDR
exit
no wifi access-point AP-NAME
```

Command

Command	Contents				
wifi access-point AP-NAME	Specify the name of the wireless LAN access point in AP-NAME and enter the advanced setting mode. <table border="1" data-bbox="507 1599 1347 1682"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>AP-NAME</td> <td>Set the access point name.</td> </tr> </tbody> </table>  Multiple access point settings can be created, but only one interface each for "wlan0" and "wlan1" can be registered.	Setting	Contents	AP-NAME	Set the access point name.
Setting	Contents				
AP-NAME	Set the access point name.				
enable	Enable the wireless LAN access point.				
no enable	Disable the wireless LAN access point.				

Command	Contents												
band BAND	<p>Sets the frequency band used for BAND.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>2.4GHz</td> <td> 2.4GHz band <ul style="list-style-type: none"> Channels 1-13  The only configurable wireless LAN interface is "wlan0". </td> </tr> <tr> <td>5GHz</td> <td> 5GHz band <ul style="list-style-type: none"> W52(36/40/44/48ch) W53(52/56/60/64ch) W56(100/104/108/112/116/120/124/128/132/136/140ch)  The only configurable wireless LAN interface is "wlan1". </td> </tr> </tbody> </table>	Setting	Contents	2.4GHz	2.4GHz band <ul style="list-style-type: none"> Channels 1-13  The only configurable wireless LAN interface is "wlan0".	5GHz	5GHz band <ul style="list-style-type: none"> W52(36/40/44/48ch) W53(52/56/60/64ch) W56(100/104/108/112/116/120/124/128/132/136/140ch)  The only configurable wireless LAN interface is "wlan1".						
Setting	Contents												
2.4GHz	2.4GHz band <ul style="list-style-type: none"> Channels 1-13  The only configurable wireless LAN interface is "wlan0".												
5GHz	5GHz band <ul style="list-style-type: none"> W52(36/40/44/48ch) W53(52/56/60/64ch) W56(100/104/108/112/116/120/124/128/132/136/140ch)  The only configurable wireless LAN interface is "wlan1".												
ssid SSID	<p>Set the network name (SSID) of the access point.</p>  For the SSID, set a string that meets the following conditions. <ul style="list-style-type: none"> The "xchar" specified in RFC1738 can be set. <div style="background-color: #e0e0e0; padding: 5px; margin: 5px 0;"> abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ 123456789!"#\$%&'()*+,-./:;<=>?@[¥]^_`{ }~ </div> <ul style="list-style-type: none"> At least 1 and no more than 32 characters. 												
channel mode MODE	<p>Set the auto channel select mode to MODE.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>Automatic selection mode (default value)</td> </tr> <tr> <td>manual</td> <td> Channel manual selection mode  </td> </tr> <tr> <td>W52</td> <td> Auto selection mode within the range of W52 (5.18GHz: 36ch to 5.24MHz: 48ch)  <ul style="list-style-type: none"> The frequency band can only be selected for the 5 GHz band. </td> </tr> <tr> <td>W53</td> <td> Automatic selection mode within the range of W53 (5.26GHz: 52ch to 5.32MHz: 64ch)  <ul style="list-style-type: none"> The frequency band can only be selected for the 5 GHz band. If there is a setting for this access point in the settings on the interface side or if this access point setting is enabled, it cannot be selected. </td> </tr> <tr> <td>W56</td> <td> Automatic selection mode within the range of W56 (5.50GHz:100ch to 5.70MHz:140ch)  <ul style="list-style-type: none"> The frequency band can be selected only for the 5 GHz band . If there is a setting for this access point in the settings on the interface side or if this access point setting is enabled, it cannot be selected. </td> </tr> </tbody> </table>	Setting	Contents	auto	Automatic selection mode (default value)	manual	Channel manual selection mode 	W52	Auto selection mode within the range of W52 (5.18GHz: 36ch to 5.24MHz: 48ch)  <ul style="list-style-type: none"> The frequency band can only be selected for the 5 GHz band. 	W53	Automatic selection mode within the range of W53 (5.26GHz: 52ch to 5.32MHz: 64ch)  <ul style="list-style-type: none"> The frequency band can only be selected for the 5 GHz band. If there is a setting for this access point in the settings on the interface side or if this access point setting is enabled, it cannot be selected. 	W56	Automatic selection mode within the range of W56 (5.50GHz:100ch to 5.70MHz:140ch)  <ul style="list-style-type: none"> The frequency band can be selected only for the 5 GHz band . If there is a setting for this access point in the settings on the interface side or if this access point setting is enabled, it cannot be selected.
Setting	Contents												
auto	Automatic selection mode (default value)												
manual	Channel manual selection mode 												
W52	Auto selection mode within the range of W52 (5.18GHz: 36ch to 5.24MHz: 48ch)  <ul style="list-style-type: none"> The frequency band can only be selected for the 5 GHz band. 												
W53	Automatic selection mode within the range of W53 (5.26GHz: 52ch to 5.32MHz: 64ch)  <ul style="list-style-type: none"> The frequency band can only be selected for the 5 GHz band. If there is a setting for this access point in the settings on the interface side or if this access point setting is enabled, it cannot be selected. 												
W56	Automatic selection mode within the range of W56 (5.50GHz:100ch to 5.70MHz:140ch)  <ul style="list-style-type: none"> The frequency band can be selected only for the 5 GHz band . If there is a setting for this access point in the settings on the interface side or if this access point setting is enabled, it cannot be selected. 												

Command	Contents																					
channel number NUMBER	<p>Set the list of connection channel numbers to NUMBER.</p>  <ul style="list-style-type: none"> ● The setting is possible when the auto channel select mode is set to "manual". ● Multiple specifications can be separated by ",". ● The available channels differ depending on the frequency band (band) and bandwidth setting (channel width). <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #444; color: white;">Frequency band</th> <th style="background-color: #444; color: white;">Bandwidth</th> <th style="background-color: #444; color: white;">Configurable channel number</th> </tr> </thead> <tbody> <tr> <td rowspan="4">2.4GHz</td> <td>20MHz</td> <td>1,2,3,4,5,6,7,8,9,10,11,12,13</td> </tr> <tr> <td>40MHz+</td> <td>1,2,3,4,5,6,7,8,9</td> </tr> <tr> <td>40MHz-</td> <td>5,6,7,8,9,10,11,12,13</td> </tr> <tr> <td>80MHz</td> <td>(Cannot be set)</td> </tr> <tr> <td rowspan="4">5GHz</td> <td>20MHz</td> <td>36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140</td> </tr> <tr> <td>40MHz+</td> <td>36,44,52,60,100,108,116,124,132</td> </tr> <tr> <td>40MHz-</td> <td>40,48,56,64,104,112,120,128,136</td> </tr> <tr> <td>80MHz</td> <td>36,52,100,116</td> </tr> </tbody> </table>	Frequency band	Bandwidth	Configurable channel number	2.4GHz	20MHz	1,2,3,4,5,6,7,8,9,10,11,12,13	40MHz+	1,2,3,4,5,6,7,8,9	40MHz-	5,6,7,8,9,10,11,12,13	80MHz	(Cannot be set)	5GHz	20MHz	36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140	40MHz+	36,44,52,60,100,108,116,124,132	40MHz-	40,48,56,64,104,112,120,128,136	80MHz	36,52,100,116
Frequency band	Bandwidth	Configurable channel number																				
2.4GHz	20MHz	1,2,3,4,5,6,7,8,9,10,11,12,13																				
	40MHz+	1,2,3,4,5,6,7,8,9																				
	40MHz-	5,6,7,8,9,10,11,12,13																				
	80MHz	(Cannot be set)																				
5GHz	20MHz	36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140																				
	40MHz+	36,44,52,60,100,108,116,124,132																				
	40MHz-	40,48,56,64,104,112,120,128,136																				
	80MHz	36,52,100,116																				
channel width WIDTH	<p>Set the bandwidth to WIDTH.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #444; color: white;">Setting</th> <th style="background-color: #444; color: white;">Contents</th> </tr> </thead> <tbody> <tr> <td>20MHz</td> <td>Use 20 MHz bandwidth system.</td> </tr> <tr> <td>40MHz+</td> <td>Use 20 MHz and 40 MHz bandwidth systems. The secondary channel has priority over the primary channel. Ex. 36ch (secondary channel) ⇒ 40ch (primary channel)</td> </tr> <tr> <td>40MHz-</td> <td>Use 20 MHz and 40 MHz bandwidth systems. The secondary channel has priority over the primary channel. Ex. 40ch (primary channel) ⇒ 36ch (secondary channel)</td> </tr> <tr> <td>80MHz</td> <td>Use 20MHz, 40MHz, and 80MHz bandwidth systems. (default value)  <ul style="list-style-type: none"> ● The short guard interval setting is also enabled at the same time. ● If the frequency band is "2.4 GHz", it operates at the 40 MHz setting. </td> </tr> </tbody> </table>	Setting	Contents	20MHz	Use 20 MHz bandwidth system.	40MHz+	Use 20 MHz and 40 MHz bandwidth systems. The secondary channel has priority over the primary channel. Ex. 36ch (secondary channel) ⇒ 40ch (primary channel)	40MHz-	Use 20 MHz and 40 MHz bandwidth systems. The secondary channel has priority over the primary channel. Ex. 40ch (primary channel) ⇒ 36ch (secondary channel)	80MHz	Use 20MHz, 40MHz, and 80MHz bandwidth systems. (default value)  <ul style="list-style-type: none"> ● The short guard interval setting is also enabled at the same time. ● If the frequency band is "2.4 GHz", it operates at the 40 MHz setting. 											
Setting	Contents																					
20MHz	Use 20 MHz bandwidth system.																					
40MHz+	Use 20 MHz and 40 MHz bandwidth systems. The secondary channel has priority over the primary channel. Ex. 36ch (secondary channel) ⇒ 40ch (primary channel)																					
40MHz-	Use 20 MHz and 40 MHz bandwidth systems. The secondary channel has priority over the primary channel. Ex. 40ch (primary channel) ⇒ 36ch (secondary channel)																					
80MHz	Use 20MHz, 40MHz, and 80MHz bandwidth systems. (default value)  <ul style="list-style-type: none"> ● The short guard interval setting is also enabled at the same time. ● If the frequency band is "2.4 GHz", it operates at the 40 MHz setting. 																					
channel short-guard-interval	<p>Enables the short guard interval setting. Default is enabled.</p>  Please note that enabling this setting shortens the guard-interval time between data and reduces the data transmission time but makes it more vulnerable to radio interference.																					
no channel short-guard-interval	<p>Disables the short guard interval setting.</p>  Cannot be disabled if the bandwidth is set to "80 MHz".																					
transmit-power TRANSMIT-POWER	<p>Set the transmit output to TRANSMIT-POWER.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #444; color: white;">Setting</th> <th style="background-color: #444; color: white;">Contents</th> </tr> </thead> <tbody> <tr> <td>10</td> <td>Transmitting output 10%.</td> </tr> <tr> <td>25</td> <td>Transmission output 25</td> </tr> <tr> <td>50</td> <td>Transmission output 50%.</td> </tr> <tr> <td>75</td> <td>Transmission output 75</td> </tr> <tr> <td>100</td> <td>Transmission output 100% (default value)</td> </tr> </tbody> </table>	Setting	Contents	10	Transmitting output 10%.	25	Transmission output 25	50	Transmission output 50%.	75	Transmission output 75	100	Transmission output 100% (default value)									
Setting	Contents																					
10	Transmitting output 10%.																					
25	Transmission output 25																					
50	Transmission output 50%.																					
75	Transmission output 75																					
100	Transmission output 100% (default value)																					

Command	Contents
max-station MAX-STATION	<p>Sets the maximum number of station devices connected to MAX-STATION. The range is "1-10". The default value is "10".</p> <p> The total number of wlan0 and wlan1 connections in the specifications that can be connected is "10", and the recommended value is "8" when actual operation is considered.</p>
stealth	Enables SSID stealth feature. Default is disabled.
no stealth	Disables the SSID stealth feature.
privacy-separator	Enables the privacy separator feature. Default is enabled.
no privacy-separator	Disables the privacy separator function.
dtim-period DTIM-PERIOD	Set the DTIM (Delivery Traffic Information Message) period included in the beacon to DTIM-PERIOD. The range is from 1 to 255. The default value is "2". When set to "1", the DTIM is included in every beacon sent.
beacon-interval BEACON-INTERVAL	Set the beacon interval (kus unit = 1.024 ms) in BEACON-INTERVAL. The range is "20 to 1024". The default value is "100".
rts-threshold RTS-THRESHOLD	<p>RTS-THRESHOLD sets the RTS threshold. The range is "1 to 2347". The default value is "2347".</p> <p> When making changes, do so in stages and check network performance.</p>
no rts-threshold	Disables the RTS threshold setting.

Command	Contents																																				
security type TYPE	<p>Set the security type to TYPE. The default value* is "wpa2-psk-wpa3-sae-mixed-aes".</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>open</td> <td>Open System Certification (without encryption)</td> </tr> <tr> <td>open-wep128</td> <td>Open system authentication 128bit WEP</td> </tr> <tr> <td>open-wep64</td> <td>Open System Authentication 64bit WEP</td> </tr> <tr> <td>shared-wep128</td> <td>Shared key authentication 128bit WEP</td> </tr> <tr> <td>shared-wep64</td> <td>Shared key authentication 64bit WEP</td> </tr> <tr> <td>wpa-psk-aes</td> <td>WPA-PSK (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa-psk-mixed</td> <td>WPA-PSK (Encryption: mixed mode)</td> </tr> <tr> <td>wpa-psk-tkip</td> <td>WPA-PSK (Encryption: TKIP)</td> </tr> <tr> <td>wpa-wpa2-mixed-psk-aes</td> <td>WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa-wpa2-mixed-psk- mixed</td> <td>WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: mixed mode)</td> </tr> <tr> <td>wpa-wpa2-mixed-psk-tkip</td> <td>WPA-PSK/WPA2-PSK authenticati on mixed mode (Encryption: TKIP)</td> </tr> <tr> <td>wpa2-psk-aes</td> <td>WPA2-PSK (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa2-psk-mixed</td> <td>WPA2-PSK (Encryption: mixed mode)</td> </tr> <tr> <td>wpa2-psk-tkip</td> <td>WPA2-PSK (Encryption: TKIP)</td> </tr> <tr> <td>wpa2-psk-wpa3-sae- mixed-aes</td> <td>WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa2-psk-wpa3-sae- mixed-mixed*</td> <td>WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)</td> </tr> <tr> <td>wpa3-sae-aes</td> <td>WPA3-SAE Certification (Encryption: AES-CCMP)</td> </tr> </tbody> </table> <p> * The default value before version 1.12.0 is "wpa2-psk-wpa3-sae-mixed-mixed". It will be removed in a future update.</p>	Setting	Display	open	Open System Certification (without encryption)	open-wep128	Open system authentication 128bit WEP	open-wep64	Open System Authentication 64bit WEP	shared-wep128	Shared key authentication 128bit WEP	shared-wep64	Shared key authentication 64bit WEP	wpa-psk-aes	WPA-PSK (Encryption: AES-CCMP)	wpa-psk-mixed	WPA-PSK (Encryption: mixed mode)	wpa-psk-tkip	WPA-PSK (Encryption: TKIP)	wpa-wpa2-mixed-psk-aes	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: AES-CCMP)	wpa-wpa2-mixed-psk- mixed	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: mixed mode)	wpa-wpa2-mixed-psk-tkip	WPA-PSK/WPA2-PSK authenticati on mixed mode (Encryption: TKIP)	wpa2-psk-aes	WPA2-PSK (Encryption: AES-CCMP)	wpa2-psk-mixed	WPA2-PSK (Encryption: mixed mode)	wpa2-psk-tkip	WPA2-PSK (Encryption: TKIP)	wpa2-psk-wpa3-sae- mixed-aes	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: AES-CCMP)	wpa2-psk-wpa3-sae- mixed-mixed*	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)	wpa3-sae-aes	WPA3-SAE Certification (Encryption: AES-CCMP)
Setting	Display																																				
open	Open System Certification (without encryption)																																				
open-wep128	Open system authentication 128bit WEP																																				
open-wep64	Open System Authentication 64bit WEP																																				
shared-wep128	Shared key authentication 128bit WEP																																				
shared-wep64	Shared key authentication 64bit WEP																																				
wpa-psk-aes	WPA-PSK (Encryption: AES-CCMP)																																				
wpa-psk-mixed	WPA-PSK (Encryption: mixed mode)																																				
wpa-psk-tkip	WPA-PSK (Encryption: TKIP)																																				
wpa-wpa2-mixed-psk-aes	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: AES-CCMP)																																				
wpa-wpa2-mixed-psk- mixed	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: mixed mode)																																				
wpa-wpa2-mixed-psk-tkip	WPA-PSK/WPA2-PSK authenticati on mixed mode (Encryption: TKIP)																																				
wpa2-psk-aes	WPA2-PSK (Encryption: AES-CCMP)																																				
wpa2-psk-mixed	WPA2-PSK (Encryption: mixed mode)																																				
wpa2-psk-tkip	WPA2-PSK (Encryption: TKIP)																																				
wpa2-psk-wpa3-sae- mixed-aes	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: AES-CCMP)																																				
wpa2-psk-wpa3-sae- mixed-mixed*	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)																																				
wpa3-sae-aes	WPA3-SAE Certification (Encryption: AES-CCMP)																																				

Command	Contents												
security key	<p>Set password (non-encrypted).</p>  <ul style="list-style-type: none"> ● Must be entered twice. ● The set password is stored in encrypted form. ● The available input methods, character types, and number of digits differ depending on the security type. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #444; color: white;">Security type</th> <th style="background-color: #444; color: white;">Available input methods, character types, and number of digits</th> </tr> </thead> <tbody> <tr> <td>open</td> <td>(Cannot be set)</td> </tr> <tr> <td>open-wep64/ shared-wep64</td> <td> <ul style="list-style-type: none"> ● Character input: 5 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 10 digits Character types include. <code>abcdefABCDEF0123456789</code> </td> </tr> <tr> <td>open-wep128/ shared-wep128</td> <td> <ul style="list-style-type: none"> ● Character input: 13 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 26 digits Character types include. <code>abcdefABCDEF0123456789</code> </td> </tr> <tr> <td>wpa-psk-aes/ wpa-psk-mixed/ wpa-psk-tkip/ wpa-wpa2-mixed- psk-aes/ wpa-wpa2-mixed- psk-mixed/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-aes/ wpa2-psk-mixed/ wpa2-psk-tkip/ wpa2-psk-wpa3- sae-mixed-aes wpa2-psk-wpa3- sae-mixed-mixed</td> <td> <ul style="list-style-type: none"> ● Character input: 8 to 64 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-./:;<=>?@[¥]^_`{ }~</code> ● Hexadecimal input: 64 digits Character types include. <code>abcdefABCDEF0123456789</code> </td> </tr> <tr> <td>wpa3-sae-aes</td> <td> <ul style="list-style-type: none"> ● Character input: 8 to 128 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-./:;<=>?@[¥]^_`{ }~</code> </td> </tr> </tbody> </table>	Security type	Available input methods, character types, and number of digits	open	(Cannot be set)	open-wep64/ shared-wep64	<ul style="list-style-type: none"> ● Character input: 5 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 10 digits Character types include. <code>abcdefABCDEF0123456789</code> 	open-wep128/ shared-wep128	<ul style="list-style-type: none"> ● Character input: 13 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 26 digits Character types include. <code>abcdefABCDEF0123456789</code> 	wpa-psk-aes/ wpa-psk-mixed/ wpa-psk-tkip/ wpa-wpa2-mixed- psk-aes/ wpa-wpa2-mixed- psk-mixed/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-aes/ wpa2-psk-mixed/ wpa2-psk-tkip/ wpa2-psk-wpa3- sae-mixed-aes wpa2-psk-wpa3- sae-mixed-mixed	<ul style="list-style-type: none"> ● Character input: 8 to 64 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-./:;<=>?@[¥]^_`{ }~</code> ● Hexadecimal input: 64 digits Character types include. <code>abcdefABCDEF0123456789</code> 	wpa3-sae-aes	<ul style="list-style-type: none"> ● Character input: 8 to 128 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-./:;<=>?@[¥]^_`{ }~</code>
Security type	Available input methods, character types, and number of digits												
open	(Cannot be set)												
open-wep64/ shared-wep64	<ul style="list-style-type: none"> ● Character input: 5 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 10 digits Character types include. <code>abcdefABCDEF0123456789</code> 												
open-wep128/ shared-wep128	<ul style="list-style-type: none"> ● Character input: 13 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 26 digits Character types include. <code>abcdefABCDEF0123456789</code> 												
wpa-psk-aes/ wpa-psk-mixed/ wpa-psk-tkip/ wpa-wpa2-mixed- psk-aes/ wpa-wpa2-mixed- psk-mixed/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-aes/ wpa2-psk-mixed/ wpa2-psk-tkip/ wpa2-psk-wpa3- sae-mixed-aes wpa2-psk-wpa3- sae-mixed-mixed	<ul style="list-style-type: none"> ● Character input: 8 to 64 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-./:;<=>?@[¥]^_`{ }~</code> ● Hexadecimal input: 64 digits Character types include. <code>abcdefABCDEF0123456789</code> 												
wpa3-sae-aes	<ul style="list-style-type: none"> ● Character input: 8 to 128 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-./:;<=>?@[¥]^_`{ }~</code> 												
security key secret ENCRYPT-KEY	Specify an encrypted password string in ENCRYPT-KEY to update the password.												
no security key	Delete the password you have set.												

Command	Contents												
security rekey REKEY-PREIOD	<p>Set the KEY update interval (in seconds) in REKEY-PREIOD. The range is "0-86400".</p> <p> The settings will vary depending on the security type setting.</p> <table border="1" data-bbox="550 313 1332 1131"> <thead> <tr> <th>Security type</th> <th>Configuration details</th> </tr> </thead> <tbody> <tr> <td>open</td> <td>(Cannot be set)</td> </tr> <tr> <td>open-wep64/ shared-wep64/ open-wep128/ shared-wep128</td> <td>Default value: 300  Setting " 0" will disable it.</td> </tr> <tr> <td>Wpa-psk-tkip/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-tkip/</td> <td>Default value: 600  0" cannot be set.</td> </tr> <tr> <td>Wpa-psk-aes/ wpa2-psk-aes/ wpa-wpa2-mixed- psk-aes/ wpa2-psk-wpa3- sae-mixed-aes/ wpa3-sae-aes</td> <td>Default value: 86400  0" cannot be set.</td> </tr> <tr> <td>Wpa-psk-mixed/ wpa-wpa2-mixed- psk-mixed/ wpa2-psk-mixed/ wpa2-psk-wpa3- sae-mixed-mixed</td> <td>(Cannot be set)</td> </tr> </tbody> </table>	Security type	Configuration details	open	(Cannot be set)	open-wep64/ shared-wep64/ open-wep128/ shared-wep128	Default value: 300  Setting " 0" will disable it.	Wpa-psk-tkip/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-tkip/	Default value: 600  0" cannot be set.	Wpa-psk-aes/ wpa2-psk-aes/ wpa-wpa2-mixed- psk-aes/ wpa2-psk-wpa3- sae-mixed-aes/ wpa3-sae-aes	Default value: 86400  0" cannot be set.	Wpa-psk-mixed/ wpa-wpa2-mixed- psk-mixed/ wpa2-psk-mixed/ wpa2-psk-wpa3- sae-mixed-mixed	(Cannot be set)
Security type	Configuration details												
open	(Cannot be set)												
open-wep64/ shared-wep64/ open-wep128/ shared-wep128	Default value: 300  Setting " 0" will disable it.												
Wpa-psk-tkip/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-tkip/	Default value: 600  0" cannot be set.												
Wpa-psk-aes/ wpa2-psk-aes/ wpa-wpa2-mixed- psk-aes/ wpa2-psk-wpa3- sae-mixed-aes/ wpa3-sae-aes	Default value: 86400  0" cannot be set.												
Wpa-psk-mixed/ wpa-wpa2-mixed- psk-mixed/ wpa2-psk-mixed/ wpa2-psk-wpa3- sae-mixed-mixed	(Cannot be set)												
no security rekey	Disables the KEY update interval (seconds) setting.												
mac-address-filtering	Enables the MAC address filtering setting. Default is disabled.												
no mac-address-filtering	Disable MAC address filtering settings.												
mac-address ACCEPT-MAC-ADDR	Set the MAC address to be allowed to connect to ACCEPT-MAC-ADDR.												
no mac-address ACCEPT-MAC-ADDR	Set ACCEPT-MAC-ADDR to the MAC address of the allowed connection you wish to delete.												
exit	Moves from the advanced setting mode of the wireless LAN access point to the setting mode.												
no wifi access-point AP-NAME	Specify the name of the wireless LAN access point to be deleted in AP-NAME and delete all settings for the specified wireless LAN access point name.												

Execution example

Enable the wireless LAN access point settings according to the settings in the table below.

Setting items	Configuration details
frequency band	5GHz
SSID Name	amnimo-5G-000000
auto channel select mode	auto mode
bandwidth	80MHz
Short Guard Interval Setting	Enable
Maximum number of station devices connected	10 units
privacy separator	Enable
Beacon Interval	100kus
DTIM cycle	2
RTS Threshold	2347
Security Type	WPA2-PSK/WPA3-SAE certification Mixed mode (Encryption: mixed mode)
security key	amnimoAC15 *Enter in encrypted mode
MAC address filtering	Disable

The interface side is as follows

Setting items	Configuration details
interface	wlan1  5GHz setting is possible only for wlan1.
access point name	amnimo-5G
IP address	192.168.0.254

設定モード

```

amnimo(cfg)# wifi access-point amnimo-5G ←
amnimo(cfg-wifi-ap-amnimo-5G)# band 5GHz ←
amnimo(cfg-wifi-ap-amnimo-5G)# ssid amnimo-5G-000000 ←
amnimo(cfg-wifi-ap-amnimo-5G)# channel mode auto ←
amnimo(cfg-wifi-ap-amnimo-5G)# channel width 80MHz ←
amnimo(cfg-wifi-ap-amnimo-5G)# channel short-guard-interval ←
amnimo(cfg-wifi-ap-amnimo-5G)# transmit-power 100 ←
amnimo(cfg-wifi-ap-amnimo-5G)# max-station 10 ←
amnimo(cfg-wifi-ap-amnimo-5G)# no stealth ←
amnimo(cfg-wifi-ap-amnimo-5G)# privacy-separator ←
amnimo(cfg-wifi-ap-amnimo-5G)# beacon-interval 100 ←
amnimo(cfg-wifi-ap-amnimo-5G)# dtim-period 2 ←
amnimo(cfg-wifi-ap-amnimo-5G)# rts-threshold 2347 ←
amnimo(cfg-wifi-ap-amnimo-5G)# security type wpa2-psk-wpa3-sae-mixed-mixed ←
amnimo(cfg-wifi-ap-amnimo-5G)# security key secret jjaAf/TE9Dd3NbApwgvDXg== ←
amnimo(cfg-wifi-ap-amnimo-5G)# no mac-address-filtering ←
amnimo(cfg-wifi-ap-amnimo-5G)# enable ←
amnimo(cfg-wifi-ap-amnimo-5G)# exit ←
amnimo(cfg)# interface wlan1←           ← Make interface wlan1 a wireless LAN access point. (Because 5GHz setting is only for wlan1)
amnimo(cfg-interface-wlan1)# access-point amnimo-5G← ← Enter the preconfigured wireless LAN access point name.
amnimo(cfg-interface-wlan1)# address 192.168.0.254/24← ← Set IP address of wireless LAN access point.
amnimo(cfg-interface-wlan1)# enable←           ← Enable interface.

```

```
amnimo(cfg-interface-wlan1)# exit ↵
amnimo(cfg)#.
```

6.8.6 Displays the status of the wireless LAN station

To display the status of a wireless LAN station, run the show wifi station command. You can also specify the interface by adding it as an argument.

Format

```
show wifi station [WIFI-IFNAME].
```

Setting items

Item	Contents
WIFI-IFNAME	Used to specify and display the wireless LAN interface. <ul style="list-style-type: none"> ● Compact Router Indoor Type / Outdoor Type with wireless LAN wlan0  If WIFI-IFNAME is omitted, information on all wireless LAN interfaces will be displayed.

Output Format

```
WIFI-IFNAME
state          STATE
ssid           SSID
bssid          BSSID
channel        CHANNEL
security       SECURITY
pairwise cipher PAIRWISE
group cipher   GROUP
rx bytes       RX-BYTES
rx packets     RX-PACKETS
tx bytes       TX-BYTES
tx packets     TX-PACKETS
tx retries     TX-RETRIES
tx failed      TX-FAILED
signal         SIGNAL dBm
tx bitrate     TX-BITRATE
```

Output item

Item	Contents						
STATE	Displays the status of the specified wireless LAN interface. <table border="1" data-bbox="448 1554 1227 1682"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SCANNING</td> <td>Searching for access points</td> </tr> <tr> <td>COMPLETED</td> <td>Access point connection complete</td> </tr> </tbody> </table>	Display	Contents	SCANNING	Searching for access points	COMPLETED	Access point connection complete
Display	Contents						
SCANNING	Searching for access points						
COMPLETED	Access point connection complete						
SSID	Displays the SSID (ServiceSet Identifier) of the specified wireless LAN interface.						
BSSID	Displays the BSSID (Basic ServiceSet Identifier) of the specified wireless LAN interface.						
CHANNEL	Displays the channel number of the specified wireless LAN interface.						
SECURITY	Displays the encryption standard for the specified wireless LAN interface.						
PAIRWISE	Displays the type of encryption scheme for unicast communication for the specified wireless LAN interface.						
GROUP	Displays the type of encryption scheme for broadcast or multicast communications for the specified wireless LAN interface.						

Item	Contents
RX-BYTES	Displays the number of bytes received for the specified wireless LAN interface.
RX-PACKETS	Displays the number of packets received on the specified wireless LAN interface.
TX-BYTES	Displays the number of bytes sent for the specified wireless LAN interface.
TX-PACKETS	Displays the number of packets sent on the specified wireless LAN interface.
TX-RETRIES	Displays the number of transmission retries for the specified wireless LAN interface.
TX-FAILED	Displays the number of transmission failures for the specified wireless LAN interface.
SIGNAL	Displays the received signal strength (dBm) for the specified wireless LAN interface.
TX-BITRATE	Displays the transmission speed (theoretical) for the specified wireless LAN interface.

Execution example

The input and output of the command is the same in all modes. The following is a sample execution that displays the status of station wlan0 connected to the access point in administrator mode.

- Access point side setting

Item	Contents
SSID	amnimo-5G
Encryption Mode	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: AES-CCMP)
frequency band	W52

ユーザーモード
管理者モード
設定モード

```

amnimo# show wifi station wlan0
wlan0
state          COMPLETED
ssid          amnimo-5G
bssid         1c:b1:7f:a6:68:2f
channel       44
security      WPA2-PSK
pairwise cipher CCMP
group cipher   CCMP
rx bytes      7838829
rx packets    23595
tx bytes      4730
tx packets    0
tx retries    0
tx failed     0
signal        -21 dBm
tx bitrate    54.0 Mbit/s

```

6.8.7 Switching the access point to which the wireless LAN station is connected

To switch between connected access points as a wireless LAN station, run the *wifi connect* command. The target interface must be added as an argument.

Format

```
wifi connect WIFI-IFNAME station select
```

Setting items

Item	Contents
WIFI-IFNAME	Used to specify the wireless LAN interface. <ul style="list-style-type: none"> ● Compact Router Indoor Type with wireless LAN wlan0

Output Format

```
network-id  ssid  bssid  flags
NW-ID      SSID  BSSID
NW-ID      SSID  BSSID  FLAGS
...
select network-id: INPUT-NW-ID ← entry field
RESULT
```

input-Output item

Item	Contents										
NW-ID	Displays the management number of the configured wireless LAN access point (hereafter referred to as "network block").  Depending on the network block settings, you may see more than one as a list.										
SSID	Displays the SSID (ServiceSet Identifier) of the network block.										
BSSID	Displays the BSSID (Basic ServiceSet Identifier) of the network block.										
FLAGS	Displays the status of network blocks. <table border="1" data-bbox="411 1249 1329 1496"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>(blank)</td> <td>Valid network block (not selected)</td> </tr> <tr> <td>CURRENT</td> <td>in the process of being selected</td> </tr> <tr> <td>DISABLE</td> <td>Disable network block</td> </tr> <tr> <td>TEMP-DISABLED</td> <td>Connection failed due to password mismatch, etc. and is temporarily disabled.</td> </tr> </tbody> </table>	Display	Contents	(blank)	Valid network block (not selected)	CURRENT	in the process of being selected	DISABLE	Disable network block	TEMP-DISABLED	Connection failed due to password mismatch, etc. and is temporarily disabled.
Display	Contents										
(blank)	Valid network block (not selected)										
CURRENT	in the process of being selected										
DISABLE	Disable network block										
TEMP-DISABLED	Connection failed due to password mismatch, etc. and is temporarily disabled.										
INPUT-NW-ID	Sets the management number of the network block to be selected. (Input item)										
RESULT	Displays switching results. <table border="1" data-bbox="411 1585 1329 1783"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>OK</td> <td>success</td> </tr> <tr> <td>Failed to select WiFi connection destination.</td> <td>Connection failure due to timeout (max. 3 min.)</td> </tr> <tr> <td>Disable number selected.</td> <td>Disable network block control number entry</td> </tr> </tbody> </table>	Display	Contents	OK	success	Failed to select WiFi connection destination.	Connection failure due to timeout (max. 3 min.)	Disable number selected.	Disable network block control number entry		
Display	Contents										
OK	success										
Failed to select WiFi connection destination.	Connection failure due to timeout (max. 3 min.)										
Disable number selected.	Disable network block control number entry										

Execution example

The input and output of commands are the same in administrator mode and configuration mode. Below is an example of executing a connection from a wireless LAN access point (amnimo-5G-1) to another wireless LAN access point (amnimo-5G-0) connectable by the wlan0 wireless LAN station in administrator mode.

管理者 モード 設定 モード

```
amnimo# show wifi station ← show status of connection to amnimo-5G-1
wlan0
  state          COMPLETED
  ssid           amnimo-5g-1
  bssid          1c:b1:7f:a6:68:2f
  channel        44
  security        WPA2-PSK
  pairwise cipher CCMP
  group cipher    CCMP
  rx bytes        391647
  rx packets      1181
  tx bytes        5864
  tx packets      0
  tx retries      0
  tx failed       0
  signal          -27 dBm
  tx bitrate      54.0 Mbit/s
amnimo# wifi connect wlan0 station select ← switch wifi access point
network-id  ssid  bssid  flags
0           amnimo-5G-0  any           ← amnimo-5G-0 (switch to, not selected)
1           amnimo-5G-1  any  CURRENT    ← amnimo-5G-1 (currently connected)

Select network-id: 0          ← Set network ID to 0 (amnimo-5G-0)
OK
...
amnimo# show wifi station ← Show status of connection to amnimo-5G-0

wlan0
  state          COMPLETED
  ssid           amnimo-5g-0
  bssid          1e:b1:7f:a6:68:2f
  channel        44
  security        NONE
  pairwise cipher WEP-104
  group cipher    WEP-104
  rx bytes        393483
  rx packets      1186
  tx bytes        6590
  tx packets      0
  tx retries      0
  tx failed       0
  signal          -30 dBm
  tx bitrate      54.0 Mbit/s
```

6.8.8 View wireless LAN station settings

To display the wireless LAN access point configuration, run the *show config wifi access-point* command. You can also specify the access point by adding it as an argument.

Format

```
show config wifi station [STA-NAME].
```

Setting items

Item	Contents
STA-NAME	Specify the name of the wireless LAN station whose settings you wish to view.

Output Format

```
configure
# ---- station STA-NAME configure ----
wifi station STA-NAME
ENABLED
band BAND
SSID
BSSID
priority PRIORITY
max-inactivity-limit MAX-INACTIVITY-LIMIT
dtim-period DTIM-PERIOD
beacon-interval BEACON-INTERVAL
SHORT-GUARD-INTERVAL
security type TYPE
SECURITY-KEY
scan-channel mode MODE
NUMBER
exit
# ---- Exit configure mode ----
exit
```

Output item

Item	Contents								
STA-NAME	Displays the name of the wireless LAN station whose settings are to be displayed.								
ENABLED.	Displays the enable/disable setting of the station function. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.		
Setting	Display								
Enable	The message "enable" is displayed.								
Disable	The message "no enable" is displayed.								
BAND	The frequency band setting used is displayed. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>2.4GHz</td> <td>2.4GHz" is displayed.</td> </tr> <tr> <td>5GHz</td> <td>5GHz" is displayed.</td> </tr> <tr> <td>2.4GHz/5GHz simultaneous use</td> <td>The word "BOTH" is displayed.</td> </tr> </tbody> </table>	Setting	Display	2.4GHz	2.4GHz" is displayed.	5GHz	5GHz" is displayed.	2.4GHz/5GHz simultaneous use	The word "BOTH" is displayed.
Setting	Display								
2.4GHz	2.4GHz" is displayed.								
5GHz	5GHz" is displayed.								
2.4GHz/5GHz simultaneous use	The word "BOTH" is displayed.								
SSID	The SSID of the wireless LAN access point to which you are connecting is displayed.								
BSSID	The BSSID of the wireless LAN access point to which you are connecting is displayed.								
PRIORITY	The priority group setting for the station is displayed. The range is "0-9", with the smaller number having priority.								

Item	Contents						
MAX-INACTIVITY-LIMIT	<p>The inactivity time limit (in seconds) of the station is displayed. The range is "1 to 2347".</p> <p> If the station does not send anything within the inactivity time limit, an empty data frame is sent to the station to see if it is still in range. If this frame is not ACKed, the station is de-associated and de-authenticated. This feature is used to clear the station table of old entries when the STA moves out of range.</p>						
DTIM-PERIOD	<p>The cycle of DTIM (Delivery Traffic Information Message) included in the beacon is displayed. The range is "1 to 10".</p> <p>[2] the DTIM is included in the beacon sent each time.</p> <p> Used if not overridden by network block.</p>						
BEACON-INTERVAL	<p>The beacon interval (kus unit = 1.024 ms) setting is displayed. The range is "20 to 1024".</p> <p> Used if not overridden by network block.</p>						
SHORT-GUARD-INTERVAL	<p>The short guard interval setting is displayed.</p> <table border="1" data-bbox="400 759 1278 954"> <thead> <tr> <th data-bbox="400 759 576 797">Setting</th> <th data-bbox="576 759 1278 797">Display</th> </tr> </thead> <tbody> <tr> <td data-bbox="400 797 576 875">Enable</td> <td data-bbox="576 797 1278 875">The message "channel short-guard-interval" is displayed.</td> </tr> <tr> <td data-bbox="400 875 576 954">Disable</td> <td data-bbox="576 875 1278 954">The message "no channel short-guard-interval" is displayed.</td> </tr> </tbody> </table> <p> Always enabled when the bandwidth setting is "80 MHz Bandwidth System".</p>	Setting	Display	Enable	The message "channel short-guard-interval" is displayed.	Disable	The message "no channel short-guard-interval" is displayed.
Setting	Display						
Enable	The message "channel short-guard-interval" is displayed.						
Disable	The message "no channel short-guard-interval" is displayed.						

Item	Contents																																				
TYPE	The security type setting is displayed.																																				
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Open System Certification (without encryption)</td> <td>It will be labeled "open."</td> </tr> <tr> <td>Open system authentication 128bit WEP</td> <td>The message "open-wep128" is displayed.</td> </tr> <tr> <td>Open System Authentication 64bit WEP</td> <td>open-wep64" is displayed.</td> </tr> <tr> <td>Shared key authentication 128bit WEP</td> <td>It will be labeled "shared-wep128."</td> </tr> <tr> <td>Shared key authentication 64bit WEP</td> <td>It will be labeled "shared-wep64."</td> </tr> <tr> <td>WPA-PSK (Encryption: AES-CCMP)</td> <td>It will be labeled "wpa-psk-aes."</td> </tr> <tr> <td>WPA-PSK (encryption: mixed mode)</td> <td>The message "wpa-psk-mixed" is displayed.</td> </tr> <tr> <td>WPA-PSK (encryption: TKIP)</td> <td>wpa-psk-tkip" is displayed.</td> </tr> <tr> <td>WPA-PSK/WPA2-PSK authentication mixed mode (encryption: AES-CCMP)</td> <td>It will be displayed as "wpa-wpa2-mixed-psk-aes".</td> </tr> <tr> <td>WPA-PSK/WPA2-PSK authentication mixed mode (encryption: mixed mode)</td> <td>It is displayed as "wpa-wpa2-mixed-psk-mixed".</td> </tr> <tr> <td>WPA-PSK/WPA2-PSK authentication mixed mode (encryption: TKIP)</td> <td>wpa-wpa2-mixed-psk-tkip".</td> </tr> <tr> <td>WPA2-PSK (Encryption: AES-CCMP)</td> <td>It will be labeled "wpa2-psk-aes."</td> </tr> <tr> <td>WPA2-PSK (Encryption: mixed mode)</td> <td>It will be displayed as "wpa2-psk-mixed".</td> </tr> <tr> <td>WPA2-PSK (encryption: TKIP)</td> <td>wpa2-psk-tkip."</td> </tr> <tr> <td>WPA2-PSK/WPA3-SAE certification mixed mode (encryption: AES-CCMP)</td> <td>wpa2-psk-wpa3-sae-mixed-aes".</td> </tr> <tr> <td>WPA2-PSK/WPA3-SAE certification Mixed mode (Encryption: mixed mode)</td> <td>wpa2-psk-wpa3-sae-mixed-mixed".</td> </tr> <tr> <td>WPA3-SAE authentication (encryption: AES-CCMP)</td> <td>It will be labeled "wpa3-sae-aes."</td> </tr> </tbody> </table>	Setting	Display	Open System Certification (without encryption)	It will be labeled "open."	Open system authentication 128bit WEP	The message "open-wep128" is displayed.	Open System Authentication 64bit WEP	open-wep64" is displayed.	Shared key authentication 128bit WEP	It will be labeled "shared-wep128."	Shared key authentication 64bit WEP	It will be labeled "shared-wep64."	WPA-PSK (Encryption: AES-CCMP)	It will be labeled "wpa-psk-aes."	WPA-PSK (encryption: mixed mode)	The message "wpa-psk-mixed" is displayed.	WPA-PSK (encryption: TKIP)	wpa-psk-tkip" is displayed.	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: AES-CCMP)	It will be displayed as "wpa-wpa2-mixed-psk-aes".	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: mixed mode)	It is displayed as "wpa-wpa2-mixed-psk-mixed".	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: TKIP)	wpa-wpa2-mixed-psk-tkip".	WPA2-PSK (Encryption: AES-CCMP)	It will be labeled "wpa2-psk-aes."	WPA2-PSK (Encryption: mixed mode)	It will be displayed as "wpa2-psk-mixed".	WPA2-PSK (encryption: TKIP)	wpa2-psk-tkip."	WPA2-PSK/WPA3-SAE certification mixed mode (encryption: AES-CCMP)	wpa2-psk-wpa3-sae-mixed-aes".	WPA2-PSK/WPA3-SAE certification Mixed mode (Encryption: mixed mode)	wpa2-psk-wpa3-sae-mixed-mixed".	WPA3-SAE authentication (encryption: AES-CCMP)	It will be labeled "wpa3-sae-aes."
	Setting	Display																																			
	Open System Certification (without encryption)	It will be labeled "open."																																			
	Open system authentication 128bit WEP	The message "open-wep128" is displayed.																																			
	Open System Authentication 64bit WEP	open-wep64" is displayed.																																			
	Shared key authentication 128bit WEP	It will be labeled "shared-wep128."																																			
	Shared key authentication 64bit WEP	It will be labeled "shared-wep64."																																			
	WPA-PSK (Encryption: AES-CCMP)	It will be labeled "wpa-psk-aes."																																			
	WPA-PSK (encryption: mixed mode)	The message "wpa-psk-mixed" is displayed.																																			
	WPA-PSK (encryption: TKIP)	wpa-psk-tkip" is displayed.																																			
	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: AES-CCMP)	It will be displayed as "wpa-wpa2-mixed-psk-aes".																																			
	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: mixed mode)	It is displayed as "wpa-wpa2-mixed-psk-mixed".																																			
	WPA-PSK/WPA2-PSK authentication mixed mode (encryption: TKIP)	wpa-wpa2-mixed-psk-tkip".																																			
	WPA2-PSK (Encryption: AES-CCMP)	It will be labeled "wpa2-psk-aes."																																			
	WPA2-PSK (Encryption: mixed mode)	It will be displayed as "wpa2-psk-mixed".																																			
WPA2-PSK (encryption: TKIP)	wpa2-psk-tkip."																																				
WPA2-PSK/WPA3-SAE certification mixed mode (encryption: AES-CCMP)	wpa2-psk-wpa3-sae-mixed-aes".																																				
WPA2-PSK/WPA3-SAE certification Mixed mode (Encryption: mixed mode)	wpa2-psk-wpa3-sae-mixed-mixed".																																				
WPA3-SAE authentication (encryption: AES-CCMP)	It will be labeled "wpa3-sae-aes."																																				
SECURITY-KEY	WEP/PSK/SAE password settings will be displayed. It is displayed in the following format																																				
	<pre>#security key raw RAW_KEY security key secret ENCRYPTED-KEY</pre>																																				
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>RAW_KEY</td> <td>Password settings will be displayed.</td> </tr> <tr> <td>ENCRYPTED-KEY</td> <td>Encrypted password settings are displayed.</td> </tr> </tbody> </table>	Setting	Display	RAW_KEY	Password settings will be displayed.	ENCRYPTED-KEY	Encrypted password settings are displayed.																														
	Setting	Display																																			
RAW_KEY	Password settings will be displayed.																																				
ENCRYPTED-KEY	Encrypted password settings are displayed.																																				

Item	Contents						
MODE	The channel operation settings are displayed.						
	<table border="1" style="width: 100%;"> <thead> <tr> <th data-bbox="392 174 683 212">Setting</th> <th data-bbox="683 174 1356 212">Display</th> </tr> </thead> <tbody> <tr> <td data-bbox="392 212 683 250">All available channels</td> <td data-bbox="683 212 1356 250">The word "all" is displayed.</td> </tr> <tr> <td data-bbox="392 250 683 291">Manual setting</td> <td data-bbox="683 250 1356 291">The message "MANUAL" will appear.</td> </tr> </tbody> </table>	Setting	Display	All available channels	The word "all" is displayed.	Manual setting	The message "MANUAL" will appear.
	Setting	Display					
	All available channels	The word "all" is displayed.					
	Manual setting	The message "MANUAL" will appear.					
 In manual mode, the channel number setting in the next section is displayed.							
<hr/>							
NUMBER	The channel number setting list appears. It is displayed in the following format						
	channel number CHANNEL_NUM						
	<table border="1" style="width: 100%;"> <thead> <tr> <th data-bbox="392 577 683 616">parameter</th> <th data-bbox="683 577 1356 616">Display</th> </tr> </thead> <tbody> <tr> <td data-bbox="392 616 683 694">CHANNEL_NUM</td> <td data-bbox="683 616 1356 694">Channel numbers are displayed. If there are multiple channels, they are separated by ",".</td> </tr> </tbody> </table>	parameter	Display	CHANNEL_NUM	Channel numbers are displayed. If there are multiple channels, they are separated by ",".		
	parameter	Display					
	CHANNEL_NUM	Channel numbers are displayed. If there are multiple channels, they are separated by ",".					
 Not displayed when auto channel select mode setting is other than "manual mode"							
<hr/>							

Execution example

Command input and output are the same in administrator mode and configuration mode. Below is an example of running the command in administrator mode to display the wlan0 station configuration.

Setting items	Configuration details
frequency band	5GHz
SSID Name	amnimo-5G
BSSID Name	(No setting)
Priority group settings for stations	0
Inactivity time limit	300 sec.
DTIM cycle	2
Beacon Interval	100kus
Security Type	WPA2-PSK authentication Encryption: AES-CCMP
security key	amnimoAC15
channel operation setting	Manual setting
connection channel number list	1,2,3,4,5,6,7,8,9,10,11,12,13,. 36,40,44,48,. 52,56,60,64,. 100,104,108,112,116,120,124,128,132,136,140

管理者 モード 設定 モード

```
amnimo# show config wifi access-point amnimo-5G
enable
band 5GHz
ssid amnimo-5G
priority 0
max-inactivity-limit 300
dtim-period 2
beacon-interval 100
security type wpa2-psk-aes
#security key raw amnimoAC15
security key secret jjaAf/TE9Dd3NbApwgvDXg==
scan-channel mode manual
scan-channel number 1,2,3,4,5,6,7,8,9,10,11,12,13,36,40,44,48,52,56,60,64,100,104,108,
112,116,120,124,128,132,136,140
exit
```

6.8.9 Configure the wireless LAN station settings.

To configure the wireless LAN station, go from the configuration mode to the advanced configuration mode and execute the configuration commands. The settings made here will be written to a configuration file.

Format

```
wifi station STA-NAME
enable
no enable
band BAND
ssid SSID
bssid BSSID
no bssid BSSID
priority PRIORITY
max-inactivity-limit MAX-INACTIVITY-LIMIT
dtim-period DTIM-PERIOD
beacon-interval BEACON-INTERVAL
short-guard-interval
no short-guard-interval
security type TYPE
security key
security key secret ENCRYPT-KEY
no security key
scan-channel mode MODE
scan-channel number CHANNEL-NUM
exit
no wifi station STA-NAME
```

Command

Command	Contents						
wifi station STA-NAME	Specify the name of the wireless LAN station in STA-NAME to enter the advanced setting mode. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>STA-NAME</td> <td>Set the name of the wireless LAN station.</td> </tr> </tbody> </table>	Setting	Contents	STA-NAME	Set the name of the wireless LAN station.		
Setting	Contents						
STA-NAME	Set the name of the wireless LAN station.						
enable	Enable the wireless LAN station.						
no enable	Disable the wireless LAN station.						
band BAND	Sets the frequency band used for BAND. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>2.4GHz</td> <td>2.4GHz band <ul style="list-style-type: none"> ● Channels 1-13 </td> </tr> <tr> <td>5GHz</td> <td>5GHz band <ul style="list-style-type: none"> ● W52(36/40/44/48ch) ● W53(52/56/60/64ch) ● W56(100/104/108/112/116/120/124/128/132/136/140ch) </td> </tr> </tbody> </table>	Setting	Contents	2.4GHz	2.4GHz band <ul style="list-style-type: none"> ● Channels 1-13 	5GHz	5GHz band <ul style="list-style-type: none"> ● W52(36/40/44/48ch) ● W53(52/56/60/64ch) ● W56(100/104/108/112/116/120/124/128/132/136/140ch)
Setting	Contents						
2.4GHz	2.4GHz band <ul style="list-style-type: none"> ● Channels 1-13 						
5GHz	5GHz band <ul style="list-style-type: none"> ● W52(36/40/44/48ch) ● W53(52/56/60/64ch) ● W56(100/104/108/112/116/120/124/128/132/136/140ch) 						
ssid SSID	Set the network name (SSID) of the wireless LAN access point to connect to. <div style="display: flex; align-items: flex-start;">  <p>For the SSID, please set a string that meets the following conditions.</p> <ul style="list-style-type: none"> ● The "xchar" specified in RFC1738 can be set. <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!#\$%&'()*+,-. /:;<=>? @[¥]^_`{ }~ </div> <ul style="list-style-type: none"> ● At least 1 and no more than 32 characters. </div>						

Command	Contents
bssid BSSID	<p>Set the BSSID of the wireless LAN access point to connect to in the following format.</p> <p style="text-align: center;"><code>xx:xx:xx:xx:xx:xx</code></p> <p>xx is a hexadecimal number.</p>
no bssid	Delete the BSSID of the wireless LAN access point to which you have set up a connection.
priority PRIORITY	<p>Set the station's priority group setting to PRIORITY.</p> <p>The range is "0-9", with the smaller number taking precedence.</p> <p>The default value is "0".</p>
max-inactivity-limit MAX-INACTIVITY-LIMIT	<p>Set the station inactivity time limit (in seconds) to MAX-INACTIVITY-LIMIT. The range is "1 to 2347".</p> <p>The default value is "300".</p> <p> If the station does not send anything within the inactivity time limit, an empty data frame is sent to the station to see if it is still in range. If this frame is not ACKed, the station is de-associated and de-authenticated. This feature is used to clear the station table of old entries when the STA moves out of range.</p>
dtim-period DTIM-PERIOD	<p>Set the DTIM (Delivery Traffic Information Message) period included in the beacon to DTIM-PERIOD. The range is from 1 to 255.</p> <p>When "1" is selected, DTIM is included in the beacon sent each time.</p> <p>The default value is "2".</p>
beacon-interval BEACON-INTERVAL	<p>Set the beacon interval (kus unit = 1.024 ms) in BEACON-INTERVAL.</p> <p>The range is "20 to 1024".</p> <p>The default value is "100".</p>
channel short-guard-interval	<p>Enables the short guard interval setting.</p> <p>Default is enabled.</p> <p> Please note that enabling this setting shortens the guard-interval time between data and reduces the data transmission time, but makes it more vulnerable to radio interference.</p>
no channel short-guard-interval	<p>Disables the short guard interval setting.</p> <p> Cannot be disabled if the bandwidth is set to "80 MHz".</p>

Command	Contents																																				
security type TYPE	<p>Set the security type to TYPE. The default value* is "wpa2-psk-wpa3-sae-mixed-aes".</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>open</td> <td>Open System Certification (without encryption)</td> </tr> <tr> <td>open-wep128</td> <td>Open System Certification 128-bit WEP</td> </tr> <tr> <td>open-wep64</td> <td>Open System Certification 64-bit WEP</td> </tr> <tr> <td>shared-wep128</td> <td>Shared Key Authentication 128-bit WEP</td> </tr> <tr> <td>shared-wep64</td> <td>Shared Key Authentication 64-bit WEP</td> </tr> <tr> <td>wpa-psk-aes</td> <td>WPA-PSK (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa-psk-mixed</td> <td>WPA-PSK (Encryption: mixed mode)</td> </tr> <tr> <td>wpa-psk-tkip</td> <td>WPA-PSK (Encryption: TKIP)</td> </tr> <tr> <td>wpa-wpa2-mixed-psk-aes</td> <td>WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa-wpa2-mixed-psk-mixed</td> <td>WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: mixed mode)</td> </tr> <tr> <td>wpa-wpa2-mixed-psk-tkip</td> <td>WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: TKIP)</td> </tr> <tr> <td>wpa2-psk-aes</td> <td>WPA2-PSK (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa2-psk-mixed</td> <td>WPA2-PSK (Encryption: mixed mode)</td> </tr> <tr> <td>wpa2-psk-tkip</td> <td>WPA2-PSK (Encryption: TKIP)</td> </tr> <tr> <td>wpa2-psk-wpa3-sae-mixed-aes</td> <td>WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: AES-CCMP)</td> </tr> <tr> <td>wpa2-psk-wpa3-sae-mixed-mixed*</td> <td>WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)</td> </tr> <tr> <td>wpa3-sae-aes</td> <td>WPA3-SAE Certification (Encryption: AES-CCMP)</td> </tr> </tbody> </table> <p> * The default value before version 1.12.0 is "wpa2-psk-wpa3-sae-mixed-mixed". It will be removed in a future update.</p>	Setting	Contents	open	Open System Certification (without encryption)	open-wep128	Open System Certification 128-bit WEP	open-wep64	Open System Certification 64-bit WEP	shared-wep128	Shared Key Authentication 128-bit WEP	shared-wep64	Shared Key Authentication 64-bit WEP	wpa-psk-aes	WPA-PSK (Encryption: AES-CCMP)	wpa-psk-mixed	WPA-PSK (Encryption: mixed mode)	wpa-psk-tkip	WPA-PSK (Encryption: TKIP)	wpa-wpa2-mixed-psk-aes	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: AES-CCMP)	wpa-wpa2-mixed-psk-mixed	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: mixed mode)	wpa-wpa2-mixed-psk-tkip	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: TKIP)	wpa2-psk-aes	WPA2-PSK (Encryption: AES-CCMP)	wpa2-psk-mixed	WPA2-PSK (Encryption: mixed mode)	wpa2-psk-tkip	WPA2-PSK (Encryption: TKIP)	wpa2-psk-wpa3-sae-mixed-aes	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: AES-CCMP)	wpa2-psk-wpa3-sae-mixed-mixed*	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)	wpa3-sae-aes	WPA3-SAE Certification (Encryption: AES-CCMP)
Setting	Contents																																				
open	Open System Certification (without encryption)																																				
open-wep128	Open System Certification 128-bit WEP																																				
open-wep64	Open System Certification 64-bit WEP																																				
shared-wep128	Shared Key Authentication 128-bit WEP																																				
shared-wep64	Shared Key Authentication 64-bit WEP																																				
wpa-psk-aes	WPA-PSK (Encryption: AES-CCMP)																																				
wpa-psk-mixed	WPA-PSK (Encryption: mixed mode)																																				
wpa-psk-tkip	WPA-PSK (Encryption: TKIP)																																				
wpa-wpa2-mixed-psk-aes	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: AES-CCMP)																																				
wpa-wpa2-mixed-psk-mixed	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: mixed mode)																																				
wpa-wpa2-mixed-psk-tkip	WPA-PSK/WPA2-PSK authentication mixed mode (Encryption: TKIP)																																				
wpa2-psk-aes	WPA2-PSK (Encryption: AES-CCMP)																																				
wpa2-psk-mixed	WPA2-PSK (Encryption: mixed mode)																																				
wpa2-psk-tkip	WPA2-PSK (Encryption: TKIP)																																				
wpa2-psk-wpa3-sae-mixed-aes	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: AES-CCMP)																																				
wpa2-psk-wpa3-sae-mixed-mixed*	WPA2-PSK/WPA3-SAE certification mixed mode (Encryption: mixed mode)																																				
wpa3-sae-aes	WPA3-SAE Certification (Encryption: AES-CCMP)																																				

Command	Contents												
security key	<p>Set password (non-encrypted).</p>  <ul style="list-style-type: none"> ● Must be entered twice. ● The set password is stored in encrypted form. ● The available input methods, character types, and number of digits differ depending on the security type. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #444; color: white;">Security type</th> <th style="background-color: #444; color: white;">Available input methods, character types, and number of digits</th> </tr> </thead> <tbody> <tr> <td>open</td> <td>(Cannot be set)</td> </tr> <tr> <td>open-wep64/ shared-wep64</td> <td> <ul style="list-style-type: none"> ● Character input: 5 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 10 digits Character types include. <code>abcdefABCDEF0123456789</code> </td> </tr> <tr> <td>open-wep128/ shared-wep128</td> <td> <ul style="list-style-type: none"> ● Character input: 13 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 26 digits Character types include. <code>abcdefABCDEF0123456789</code> </td> </tr> <tr> <td>wpa-psk-aes/ wpa-psk-mixed/ wpa-psk-tkip/ wpa-wpa2-mixed- psk-aes/ wpa-wpa2-mixed- psk-mixed/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-aes/ wpa2-psk-mixed/ wpa2-psk-tkip/ wpa2-psk-wpa3- sae-mixed-aes wpa2-psk-wpa3- sae-mixed-mixed</td> <td> <ul style="list-style-type: none"> ● Character input: 8 to 64 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-. /:;<=>? @[¥]^_`{ }~</code> ● Hexadecimal input: 64 digits Character types include. <code>abcdefABCDEF0123456789</code> </td> </tr> <tr> <td>wpa3-sae-aes</td> <td> <ul style="list-style-type: none"> ● Character input: 8 to 128 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-. /:;<=>? @[¥]^_`{ }~</code> </td> </tr> </tbody> </table>	Security type	Available input methods, character types, and number of digits	open	(Cannot be set)	open-wep64/ shared-wep64	<ul style="list-style-type: none"> ● Character input: 5 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 10 digits Character types include. <code>abcdefABCDEF0123456789</code> 	open-wep128/ shared-wep128	<ul style="list-style-type: none"> ● Character input: 13 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 26 digits Character types include. <code>abcdefABCDEF0123456789</code> 	wpa-psk-aes/ wpa-psk-mixed/ wpa-psk-tkip/ wpa-wpa2-mixed- psk-aes/ wpa-wpa2-mixed- psk-mixed/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-aes/ wpa2-psk-mixed/ wpa2-psk-tkip/ wpa2-psk-wpa3- sae-mixed-aes wpa2-psk-wpa3- sae-mixed-mixed	<ul style="list-style-type: none"> ● Character input: 8 to 64 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-. /:;<=>? @[¥]^_`{ }~</code> ● Hexadecimal input: 64 digits Character types include. <code>abcdefABCDEF0123456789</code> 	wpa3-sae-aes	<ul style="list-style-type: none"> ● Character input: 8 to 128 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-. /:;<=>? @[¥]^_`{ }~</code>
Security type	Available input methods, character types, and number of digits												
open	(Cannot be set)												
open-wep64/ shared-wep64	<ul style="list-style-type: none"> ● Character input: 5 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 10 digits Character types include. <code>abcdefABCDEF0123456789</code> 												
open-wep128/ shared-wep128	<ul style="list-style-type: none"> ● Character input: 13 characters Character types include. <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789_</code> ● Hexadecimal input: 26 digits Character types include. <code>abcdefABCDEF0123456789</code> 												
wpa-psk-aes/ wpa-psk-mixed/ wpa-psk-tkip/ wpa-wpa2-mixed- psk-aes/ wpa-wpa2-mixed- psk-mixed/ wpa-wpa2-mixed- psk-tkip/ wpa2-psk-aes/ wpa2-psk-mixed/ wpa2-psk-tkip/ wpa2-psk-wpa3- sae-mixed-aes wpa2-psk-wpa3- sae-mixed-mixed	<ul style="list-style-type: none"> ● Character input: 8 to 64 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-. /:;<=>? @[¥]^_`{ }~</code> ● Hexadecimal input: 64 digits Character types include. <code>abcdefABCDEF0123456789</code> 												
wpa3-sae-aes	<ul style="list-style-type: none"> ● Character input: 8 to 128 characters <code>abcdefghijklmnopqrstuvwxyzABCDEF GHIJKLMNOPQRSTUVWXYZ0123456789!" #\$%&'()*+,-. /:;<=>? @[¥]^_`{ }~</code> 												

Command	Contents						
security key secret ENCRYPT-KEY	Specify an encrypted password string in ENCRYPT-KEY to update the password.						
no security key	Delete the password you have set.						
scan-channel mode M ODE	<p>Sets the channel operation settings.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>all</td> <td>All available channels</td> </tr> <tr> <td>manual</td> <td>Manual setting</td> </tr> </tbody> </table> <p> In manual mode, Enables the channel number settings described in the next section.</p>	Setting	Contents	all	All available channels	manual	Manual setting
Setting	Contents						
all	All available channels						
manual	Manual setting						
scan-channel number CHANNEL-NUM	<p>Sets the channel number setting list to be used. Set in the following format</p> <pre>scan-channel number CHANNEL-NUM</pre> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>CHANNEL-NUM</td> <td>Channel numbers are displayed. If there are multiple channels, they are separated by ",".</td> </tr> </tbody> </table> <p> Not displayed when the channel operation setting is other than "manual setting".</p>	Setting	Contents	CHANNEL-NUM	Channel numbers are displayed. If there are multiple channels, they are separated by ",".		
Setting	Contents						
CHANNEL-NUM	Channel numbers are displayed. If there are multiple channels, they are separated by ",".						
exit	Moves the wireless LAN station from the advanced configuration mode to the configuration mode.						
no wifi access-point STA-NAME	Specify the name of the wireless LAN station to be deleted in STA-NAME and delete all settings for the specified wireless LAN station name.						

Execution example

Enable the wireless LAN station settings according to the settings in the table below.

Setting items	Configuration details
frequency band	2.4GHz
SSID Name	amnimo-2G
BSSID Name	(No setting)
Priority group settings for stations	1
Inactivity time limit	300 sec.
DTIM cycle	10
Beacon Interval	1024kus
Security Type	WPA2-PSK authentication Encryption: AES-CCMP
security key	amnimoAC15
channel operation setting	All available channels

設定モード

```
amnimo(cfg)# wifi station amnimo-2G ↵
amnimo(cfg-wifi-sta-amnimo-2G)# band 2.4GHz ↵
amnimo(cfg-wifi-sta-amnimo-2G)# ssid amnimo-2G ↵
You must fill in the following required fields:
security key
amnimo(cfg-wifi-sta-amnimo-2G)# security type wpa2-psk-aes ↵
Wifi security type values changed,
So deleted Wifi key related settings.
You must fill in the following required fields:
security key
amnimo(cfg-wifi-sta-amnimo-2G)# security key
Enter new key:                ← Enter password "amnimoAC15"
Retype new key:               ← Retype password "amnimoAC15"
key: key updated successfully.
amnimo(cfg-wifi-sta-amnimo-2G)# priority 1 ↵
amnimo(cfg-wifi-sta-amnimo-2G)# beacon-interval 1024 ↵
amnimo(cfg-wifi-sta-amnimo-2G)# dtim-period 10 ↵
amnimo(cfg-wifi-sta-amnimo-2G)# enable ↵
amnimo(cfg-wifi-sta-amnimo-2G)# exit
amnimo(cfg)#.
```

6.8.10 Connect using the WPS function

The *wifi connect wps* command is used to connect to other wireless LAN access points or stations using the WPS function. This device supports both push-button and PIN methods. The target interface must be added as an argument.

Format

```
wifi connect wps <pbw | pin-get | pin-set> [wait WAIT].
```

Setting items

Item	Contents
PDC	<p>Wireless LAN connection settings (WPS-PBC) can be set up on the wireless LAN station using the push-button system with this device as the wireless LAN access point.</p>  <ul style="list-style-type: none"> This device will not work if it is configured as a wireless LAN station. The effect is the same as pressing the WPS button for more than 5 seconds. (This is useful when you want to disable the physical button for improved security and perform the same operation from the CLI.)
pin-get	<p>Used to generate PIN code for WPS. (To be supported in the next version)</p> <p>➔ To use this device as a wireless LAN station, generate a PIN code, and connect to a wireless LAN access point, see “6.8.12 Configure the WPS function”.</p>
pin-set	<p>This device can be used as a wireless LAN access point to set the PIN code generated by the wireless LAN station using the PIN method and set the wireless LAN connection settings (WPS-PIN) to the wireless LAN station.</p>  <ul style="list-style-type: none"> This device will not work if it is configured as a wireless LAN station.
WAIT	<p>Sets the time to wait for the wireless LAN connection to complete. The range is "10-3600(sec)". The default value is 60 seconds.</p>

Output format (push-button WPS)

```
.....
```

Output format (PIN method WPS)

```
Input pin: PIN-CODE
RESULT
```

input-Output item

Item	Contents						
PIN-CODE	Set the PIN code (fixed 8 digits) of the device to be connected.						
RESULT	Displays connection results.						
	<table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>OK</td> <td>success</td> </tr> <tr> <td>Disable Pin-Code.</td> <td>PIN code mistake</td> </tr> </tbody> </table>	Display	Contents	OK	success	Disable Pin-Code.	PIN code mistake
	Display	Contents					
OK	success						
Disable Pin-Code.	PIN code mistake						

Execution example 1 (push-button WPS)

The following is an example of connecting a wireless LAN station of another device to a wireless LAN access point (amnimo-2G) of wlan0 by push button WPS in the setting mode.

設定 モード

```
amnimo(cfg)# show wifi access-point wlan0 ← show amnimo-2G connected
wlan0
state          ENABLED
ssid           amnimo-2G-004600
bssid          e8:1b:4b:00:46:00
channel        12
rx bytes       0
rx packets     0
tx bytes       0
tx packets     0
tx errs        0
tx drop        0
connected stations 0          ← 0 wireless LAN stations connected to amnimo-2G
amnimo(cfg)# wifi connect wps pbc ← execute push button method WPS
..... ← Default setting lasts for 6
0 seconds, during which time the connection is made with the wireless LAN station.
amnimo(cfg)# show wifi access-point wlan0 ← show amnimo-2G connected
wlan0
state          ENABLED
ssid           amnimo-2G-004600
bssid          e8:1b:4b:00:46:00
channel        12
rx bytes       48527
rx packets     519
tx bytes       20741
tx packets     143
tx errs        0
tx drop        0
connected stations 1          ← 1 more wireless LAN station connected to amnimo-2G
```

6.8.11 Display WPS function settings

To view the WPS feature settings, run the *show config wifi wps* command. Used for wireless LAN access points.

Format

```
show config wifi wps
```

Output Format

```
configure
# ---- wps configure ----
wifi wps
ENABLED
PUSH-SWITCH
EXTERNAL-REGISTRAR
PIN
exit
# ---- Exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLED.	Displays the enable/disable setting of the WPS function.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
	Setting	Display					
	Enable	The message "enable" is displayed.					
Disable	The message "no enable" is displayed.						
<hr/>							
PUSH-SWITCH	Displays the setting for enabling/disabling physical button operation for WPS.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>push-switch" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no push-switch" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	push-switch" is displayed.	Disable	The message "no push-switch" is displayed.
	Setting	Display					
	Enable	push-switch" is displayed.					
Disable	The message "no push-switch" is displayed.						
<hr/>							
EXTERNL-REGISTRAR	Displays the setting for enabling/disabling the external registrar function. When this setting is enabled, the wireless LAN station will be able to connect using a PIN code instead of a security key.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be labeled "external-registrar."</td> </tr> <tr> <td>Disable</td> <td>The message "no external-registrar" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be labeled "external-registrar."	Disable	The message "no external-registrar" is displayed.
	Setting	Display					
	Enable	It will be labeled "external-registrar."					
Disable	The message "no external-registrar" is displayed.						
<hr/>							
PIN	Displays the PIN code used for the WPS function.						
	<pre># pin set XXXXXXXXXX</pre>  x is a number. 8 digits are displayed.						

Execution example

Command input and output are the same in administrator mode and configuration mode. Below is an example of running the command to display the WPS function settings in configuration mode.

Setting items	Configuration details
WPS function	Enable
Push-switch function for WPS	Enable
External Registrar Function	Enable
PIN code	12345678

管理者 モード 設定 モード

```
amnimo(cfg)# show config wifi wps
# ---- wps configure ----
wifi wps
enable
push-switch
external-registrar
#pin set 12345678
exit
```

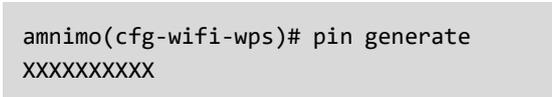
6.8.12 Configure the WPS function

To configure the WPS function, go from configuration mode to advanced configuration mode and execute the *wifi wps* command. The settings made here will be written to a configuration file.

Format

```
wifi wps
enable
no enable
push-switch
no push-switch
external-registrar
no external-registrar
pin generate
exit
```

Command

Command	Contents
wifi wps	Shifts to WPS function advanced setting mode.
enable	Enable WPS function.
no enable	Disables the WPS function.
push-switch	Enables physical WPS button operation.
no push-switch	Disables physical WPS button operation.
external-registrar	Enable the external registrar function.  When this setting is enabled, the wireless LAN station can connect using a PIN code instead of a security key.
no external-registrar	Disable the external registrar function.
pin generate	Generate PIN code.  <pre>amnimo(cfg-wifi-wps)# pin generate XXXXXXXXXX</pre>  x is a number. 8 digits are displayed.
exit	Moves from the advanced setting mode of the WPS function to the setting mode.

Execution example

Enable the wireless LAN station settings according to the settings in the table below.

Setting items	Configuration details
WPS function	Enable
Push-switch function for WPS	Disable
External Registrar Function	Enable
PIN code	98765432 (auto-generated result)

設定モード

```
amnimo(cfg)# wifi wps ←
amnimo(cfg-wifi-wps)# enable ←
amnimo(cfg-wifi-wps)# no push-switch ←
amnimo(cfg-wifi-wps)# external-registrar ←
amnimo(cfg-wifi-wps)# pin generate ←
98765432
amnimo(cfg-wifi-wps)# exit ←
amnimo(cfg)#.
```

6.8.13 Restrictions on wireless LAN functionality and interface

Compact Router Indoor Type with wireless LAN has two dedicated interfaces (wlan0, wlan1), but please note that there are some limitations as shown in the table below.

function item		wlan0	wlan1
Wireless LAN access point function ^{*1}		available	available
Supported frequency bands		2.4GHz	5GHz ^{*2}
Addition to bridge interface (brX)		additionally acceptable	
WPS function	When wlan0 and wlan1 are used	Object of control	-
	When only wlan0 is used	Object of control	-
	When using wlan1 only	-	Object of control
Wireless LAN station function ^{*1}		available	not available
Supported frequency bands		2.4GHz/5GHz	-
Addition to bridge interface (brX)		Cannot be added	-
WPS function		incompatible ^{*3}	-

1 Access point function and station function cannot be used together.

2 When using 2.4GHz and 5GHz at the same time, 5GHz band is limited to W52. 2.4GHz is not available when using W53 or W56 at 5GHz.

3 Will be supported in the future.

Chap 7. Server Settings

This chapter describes server settings that are important for using the product, including hostname, time zone and time, SSH, DNS, DHCP, scheduling, and system logs.

7.1 Set the host name



Displays and configures host names.

7.1.1 Show hostname

To display the hostname, run the *show hostname* command.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```

amnimo$ show hostname ←
amnimo      ← Host name is displayed
amnimo$.

```

7.1.2 Display host name settings

To view hostname settings, run the *show config hostname* command.

Format

```
show config hostname
```

Output Format

```

# ---- transition to configure mode ----
configure
# ---- hostname configure ----
hostname HOSTNAME
# ---- exit configure mode ----
exit

```

Output item

Item	Contents
HOSTNAME	The host name is displayed.

Execution example

管理者モード

```

amnimo# show config hostname ←
# ---- transition to configure mode ----
configure
# ---- hostname configure ----
hostname amnimo
# ---- exit configure mode ----
exit

```

```
amnimo(cfg)# show config hostname ←  
# ---- hostname configure ----  
hostname amnimo
```

7.1.3 Change the host name

To change the hostname, run the *hostname* command.

Format

```
hostname HOSTNAME
```

Setting items

Item	Contents
HOSTNAME	Specifies the host name.

Execution example

```
amnimo(cfg)# hostname amnimo2← ← Change hostname  
amnimo(cfg)# show hostname← ← Confirm hostname  
amnimo2
```

7.2 Set the time zone



Displays and sets the time zone.

7.2.1 Display time zone

To view the time zone, run the *show timezone* command.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

```

ユーザーモード 管理者モード 設定モード
amnimo$ show timezone ←
UTC                ← If time zone is set to UTC
amnimo$ show timezone ←
Asia/Tokyo        ← If time zone is set to Asia/Tokyo

```

7.2.2 View time zone settings

To view time zone settings, run the *show config timezone* command.

Format

```
show config timezone
```

Output Format

```

# ---- transition to configure mode ----
configure
# ---- timezone configure ----
timezone TZ-AREA TZ-LOCATION
# ---- exit configure mode ----
exit

```

Output item

Item	Contents
TZ-AREA	<p>The time zone region is displayed.</p> <ul style="list-style-type: none"> The region is the part of the time zone value before the "/". Example: Asia
TZ-LOCATION	<p>The name of the place in the time zone is displayed.</p> <ul style="list-style-type: none"> The place name is the portion after the "/" in the time zone value. If UTC is set for the time zone region, the place name will be left blank.

Execution example

管理者 モード

```
amnimo# show config timezone ↵
# ---- transition to configure mode ----
configure
# ---- timezone configure ----
timezone Asia Tokyo
# ---- exit configure mode ----
exit
```

設定 モード

```
amnimo(cfg)# show config timezone ↵
# ---- timezone configure ----
timezone Asia Tokyo
```

7.2.3 Set the time zone

To change the time zone, run the `timezone` command.

Format

```
timezone TIMEZONE
```

Setting items

Item	Contents
TIMEZONE	Specify the time zone.

Execution example

設定 モード

```
amnimo(cfg)# timezone UTC↵          ← Change timezone to UTC
amnimo(cfg)# timezone Asia Tokyo↵    ← Change timezone to Asia/Tokyo
```

7.3 Set the time



This section explains how to set the time manually and how to adjust the time using an NTP server.

7.3.1 Manually set the time

There are several ways to set the time manually by command operation.

■ Display the time

To display the currently set time, run the *show date* command.



Time is displayed in RFC 3339 format. However, the date and time are separated by a single space, not a T. The time zone is displayed following the time. For example, in the following case, +09:00 represents Japan Standard Time, which is 9 hours ahead.

```
2020-05-20 17:30:53+09:00
```

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show date ↵
2020-05-20 17:30:53+09:00
```

■ Set the time

To set the time manually by entering the time, run the *date manual* command.

As with the time display, the time is specified in RFC 3339 format. It is not necessary to specify a time zone.

➔ For more information on setting the time zone, see " 7.2 Set the time zone " for information on time zone settings.

Execution example

The time setting cannot be set in general user mode because it is related to the startup control of the device.

An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# date manual 2020-05-20 17:40:00 ↵
amnimo# show date                ↵ Check time
2020-05-20 17:40:10+09:00
```

■ Query an external NTP server to set the time

The ntp protocol can be used to synchronize the time.

Format

```
date ntp NTP-SERVER
```

Setting items

Item	Contents
NTP-SERVER	Specify the IP address or FQDN of the NTP server.

Execution example

The time setting cannot be set in general user mode because it is related to the startup control of the device.

An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# date ntp ntp.nict.jp ←
amnimo# show date←          ← Check time
2020-05-20 17:40:10+09:00
```

7.3.2 Display NTP status

Displays NTP status, including NTP source, NTP client, and NTP synchronization performance.

■ Display NTP source

To view NTP status, run the ***show ntp sources*** command.

➔ For information on displaying NTP clients when they exist, see the following "Display NTP Client " for information on displaying NTP clients when they are present.

Format

```
show ntp sources
```

Output Format

```
MS Name/IP address   Stratum Poll  Reach  LastRx Last sample
-----
MS NAME-IP          STM    PL    RCH   LRX   LAST-SAMPLE
```

Output item

Item	Contents														
Mega	<p>The mode of the NTP source is displayed.</p> <table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>^</td> <td>Server (Upper-level device to be synchronized)</td> </tr> <tr> <td>=</td> <td>Peers (Devices that synchronize with each other)</td> </tr> <tr> <td>#</td> <td>Locally connected reference clock (e.g., GPS module)</td> </tr> </tbody> </table>	Display	Contents	^	Server (Upper-level device to be synchronized)	=	Peers (Devices that synchronize with each other)	#	Locally connected reference clock (e.g., GPS module)						
Display	Contents														
^	Server (Upper-level device to be synchronized)														
=	Peers (Devices that synchronize with each other)														
#	Locally connected reference clock (e.g., GPS module)														
sadist	<p>The NTP source is displayed.</p> <table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>*</td> <td>synchronization</td> </tr> <tr> <td>+</td> <td>Acceptable Sources</td> </tr> <tr> <td>-</td> <td>Excluded from acceptable sources</td> </tr> <tr> <td>?</td> <td>Sources of packets not received</td> </tr> <tr> <td>an unknown</td> <td>Temporal errors occur.</td> </tr> <tr> <td>~</td> <td>Excessive amount of time variability Source.</td> </tr> </tbody> </table>	Display	Contents	*	synchronization	+	Acceptable Sources	-	Excluded from acceptable sources	?	Sources of packets not received	an unknown	Temporal errors occur.	~	Excessive amount of time variability Source.
Display	Contents														
*	synchronization														
+	Acceptable Sources														
-	Excluded from acceptable sources														
?	Sources of packets not received														
an unknown	Temporal errors occur.														
~	Excessive amount of time variability Source.														
NAME-IP	The name or IP address of the NTP source and locally connected reference clock (e.g., GPS module) are displayed.														
STM	Stratum values are displayed.														
PL	The polling interval is displayed.														
RCH	The reachability of the source is displayed in octal. A "377" indicates that a valid reply was received for the entire 8 most recent communications.														
LRX	The elapsed time since the last packet was received from the source is displayed.														
LAST-SAMPLE	<p>The offset time between the local clock and the last source is displayed in the following format xxxx [yyyy] +/- zzzz</p> <ul style="list-style-type: none"> ● xxxx: Adjustment offset value ● yyyy: Offset value at measurement ● zzzz: Estimation error 														

Execution example

Command input and output is the same in all modes. Below is an example of running the General User mode on the Edge Gateway.

```

ユーザーモード 管理者モード 設定モード
When connected to a regular NTP server
amnimo$ show ntp source ↵
MS Name/IP address  Stratum      Poll   Reach  LastRx Last sample
=====
^* 192.168.0.203    1          6     377   38     -1397us[-2217us] +/- 201ms

GPS module present (for Stratum1 NTP server)
amnimo$ show ntp source ↵
MS Name/IP address  Stratum      Poll   Reach  LastRx Last sample
=====
#* GPS1             0          4     77    25     -1130us[+3785us] +/- 200ms

```



- IoT Router Indoor Type and Compact Router Indoor Type do not support GPS, so the "When GPS module is present" execution example is not shown.
- Priority of time acquisition when using GPS
Since the Stratum of GPS is 0, the acquisition of time by GPS is given the highest priority.
It is not possible to change the priority order of time acquisition by GPS and time acquisition by an NTP server via the Internet.
 - GPS: Stratum0
 - NTP server: Stratum 1-16

■ Display NTP Client

If NTP clients exist, the *show ntp clients* command will output a list.

Format

```
show ntp clients
```

Output Format

```

Hostname      NTP    Drop  Int   Int   Last  Cmd   Drop  Int   Last
=====
HOSTNAME    NTP  DP1 I1  IL  LST1 CMD DP2 I2  LST2

```

Output item

Item	Contents
HOSTNAME	The host name of the NTP client is displayed.
NTP	The number of NTP packets received from the NTP client is displayed.
DP1	The number of NTP packets that could not be received due to response timeout from the NTP client is displayed.
I1	The average interval of NTP packets is displayed.
IL	The average interval of NTP packets after a response timeout is displayed.
LST1	The elapsed time since the last NTP packet was received is displayed.
CMD	The number of command packets received from the NTP client is displayed.
DP2	The number of command packets that could not be received due to response timeout from the NTP client is displayed.
I2	The command packet average interval is displayed.
LST2	The elapsed time since the last command packet was received is displayed.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```

amnimo$ show ntp clients ↵
Hostname      NTP    Drop  Int   Int   Last  Cmd   Drop  Int   Last
=====
192.168.0.106 79     0     6     -     14    0     0     -     -
172.16.0.2    0     0     -     -     -     1     0     -     2

```

■ Display NTP synchronization performance

To view NTP synchronization performance, run the *show ntp tracking* command.

If an NTP client exists, information is listed.

Format

```
show ntp tracking
```

Output item

Item	Contents										
Reference ID	The refid and name (or IP address) of the server the computer is currently synchronized with are displayed.										
Stratum	The number of hops from the computer to which the reference clock is connected is displayed.										
Ref time	The time (UTC) when the last measurement from the reference source was processed is displayed.										
System time	The system time is displayed.										
Last offset	The estimated local offset of the time the clock was last updated is displayed.										
RMS offset	The long-term average of the offset values is displayed.										
Frequency	The incorrect system clock rate is displayed when the system's clock fails to correct itself.										
Residual freq.	The difference between the frequency indicated by the measurement from the reference source and the currently used frequency is displayed.										
Skew.	The estimated error range of the frequency is displayed.										
Root delay	Displays the total network path delay to the stratum-1 computer with which the computer will eventually be synchronized.										
Root dispersion	The total variance accumulated through all computers back to the stratum-1 computer with which the computer will eventually be synchronized is displayed.										
Update interval	The interval between the last two clock updates is displayed.										
Leap status	The leap second synchronization status is displayed. <table border="1" data-bbox="571 1339 1353 1552"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>Normal</td> <td>Normal state</td> </tr> <tr> <td>Insert Second</td> <td>Leap second insertion state</td> </tr> <tr> <td>Delete Second</td> <td>Leap second deletion status</td> </tr> <tr> <td>Not synchronised</td> <td>Unsynchronized leap state</td> </tr> </tbody> </table>	Display	Contents	Normal	Normal state	Insert Second	Leap second insertion state	Delete Second	Leap second deletion status	Not synchronised	Unsynchronized leap state
Display	Contents										
Normal	Normal state										
Insert Second	Leap second insertion state										
Delete Second	Leap second deletion status										
Not synchronised	Unsynchronized leap state										

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

```

ユーザーモード 管理者モード 設定モード
amnimo$ show ntp tracking ↵
Reference ID   : C0A800CB (192.168.0.203)
Stratum       : 2
Ref time (UTC) : Tue Mar 18 11:14:35 2020
System time   : 0.002314539 seconds fast of NTP time
Last offset   : +0.004517063 seconds
RMS offset    : 0.004669765 seconds
Frequency     : 34.202 ppm fast
Residual freq : +3.553 ppm
Skew          : 20.510 ppm
Root delay    : 0.200332880 seconds
Root dispersion : 0.103083454 seconds
Update interval : 64.4 seconds
Leap status   : Normal

```

7.3.3 Display NTP settings

To view the NTP configuration, run the *show config ntp* command.

Format

```
show config ntp
```

Output Format

```

# ---- transition to configure mode ----
configure
#
ntp
# ---- NTP configure ----
ENABLE
max-update-skew SKEW_VALUE
make-steps THRESHOLD_VALUE LIMIT_VALUE
PRIORITY
SYNC_INTERFACE
POOL_INFO
POOL_INFO
POOL_INFO
(Omitted.)
SERVER_INFO
(Omitted.)
GPS_ENABLE
exit

```

Output item

Item	Contents						
ENABLE	Displays information if NTP server is enabled/disabled.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
	Setting	Display					
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
SKEW_VALUE	The range setting value of the error expectation error is displayed.						
THRESHOLD_VALUE	The threshold for step expression synchronization is displayed.						
LIMIT_VALUE	The number of times the step expression synchronization limit is displayed.						
PRIORITY	If the NTP server's process priority setting is configured, it will be displayed in the following format (optional setting)						
	<code>priority PRIORITY_VALUE</code>						
	<table border="1"> <thead> <tr> <th>Setting items</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>PRIORITY_VALUE</td> <td>The process priority setting of the NTP server is displayed. The setting range is 0 to 99.</td> </tr> </tbody> </table>	Setting items	Display	PRIORITY_VALUE	The process priority setting of the NTP server is displayed. The setting range is 0 to 99.		
Setting items	Display						
PRIORITY_VALUE	The process priority setting of the NTP server is displayed. The setting range is 0 to 99.						
SYNC_INTERFACE	If the NTP server synchronization settings are configured, the following format is displayed (optional setting).						
	<code>sync-interface SYNC_IFNAME</code>						
	<table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SYNC_IFNAME</td> <td>Synchronizes when the specified interface is connected/disconnected. Specify an interface in the following format. Multiple interfaces cannot be specified. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0, rmnet_data0 ● Compact Router Indoor Type with wireless LAN, Compact Router Outdoor Type with wireless LAN lan<0,1>, wlan<0,1>, br<0-9>, rmnet_data0 </td> </tr> </tbody> </table>	Setting items	Contents	SYNC_IFNAME	Synchronizes when the specified interface is connected/disconnected. Specify an interface in the following format. Multiple interfaces cannot be specified. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0, rmnet_data0 ● Compact Router Indoor Type with wireless LAN, Compact Router Outdoor Type with wireless LAN lan<0,1>, wlan<0,1>, br<0-9>, rmnet_data0 		
Setting items	Contents						
SYNC_IFNAME	Synchronizes when the specified interface is connected/disconnected. Specify an interface in the following format. Multiple interfaces cannot be specified. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0, rmnet_data0 ● Compact Router Indoor Type with wireless LAN, Compact Router Outdoor Type with wireless LAN lan<0,1>, wlan<0,1>, br<0-9>, rmnet_data0 						
POOL_INFO	If an NTP server pool is configured, it will appear in the following format						
	<code>pool POOL_ADDRESS MAX-SOURCES</code> More than one may be displayed.						
POOL_ADDRESS	The IP address and server name of the NTP server pool are displayed.						
MAX-SOURCES.	The maximum value of the source of the NTP server pool is displayed.						

Item	Contents						
GPS_ENABLE	<p>Information is displayed on when the activation of the GPS function that works with the NTP server is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>gps GPS_INTERVAL" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no gps" is displayed.</td> </tr> </tbody> </table> <p> GPS_ENABLE is not displayed for IoT Router Indoor Type, Compact Router Indoor Type with wireless LAN, and Compact Router Outdoor Type with wireless LAN because they do not support GPS.</p> <p> </p>	Setting	Display	Enable	gps GPS_INTERVAL" is displayed.	Disable	The message "no gps" is displayed.
Setting	Display						
Enable	gps GPS_INTERVAL" is displayed.						
Disable	The message "no gps" is displayed.						
GPS_INTERVAL	<p>The time interval (in milliseconds) to access the GPS module is displayed.</p> <p> GPS_INTERVAL is not displayed for IoT Router Indoor Type, Compact Router Indoor Type, and Compact Router Outdoor Type with wireless LAN, as they do not support GPS.</p> <p> </p>						
SERVER_INFO	<p>If an NTP server is configured, it will be displayed in the following format</p> <pre>server SERVER_ADDRESS [min POLLING_MIN] [max POLLING_MAX] [polltarget POLLING_TARGET] [port PORT_NO]</pre> <p>More than one may be displayed.</p>						
SERVER_ADDRESS	The IP address and server name of the NTP server are displayed. More than one may be displayed.						
POLLING_MIN	The minimum polling interval (a power of 2) is displayed.						
POLLING_MAX	The maximum polling interval (a power of 2) is displayed.						
POLLING_TAGET	The number of polling targets used by the regression algorithm within the polling interval range is displayed.						
PORT_NO	The number of the UDP port used for NTP is displayed.						

Execution example

Because NTP settings are involved in controlling device startup, the settings cannot be displayed in general user mode.

Below is an example of running the administrator and configuration modes on the Edge Gateway.

管理者 モード

```
amnimo# show config ntp ↵
# ---- transition to configure mode ----
configure
# ---- NTP configure ----
ntp
enable
max-update-skew 100.0
make-steps 1 3
sync-interface eth0
server ntp.nict.jp min 6 max 10 polltarget 6 port 123
no gps
exit
# ---- exit configure mode. ----
exit
```

設定 モード

```
amnimo(cfg)# show config ntp ↵
# ---- NTP configure ----
ntp
enable
max-update-skew 100.0
make-steps 1 3
sync-interface eth0
server ntp.nict.jp min 6 max 10 polltarget 6 port 123
no gps
exit
```



Running the show config command in NTP advanced configuration mode will display the same information as in configuration mode.

```
amnimo(cfg)# ntp↵          ← Go to NTP advanced configuration mode
amnimo(cfg-ntp)# show config ↵
enable                    ← Same as setting mode
(Omitted.)
```

7.3.4 Configure NTP settings

To configure NTP, go to the advanced configuration mode and execute the configuration command.

The settings made here are written to a configuration file.

Format

```
ntp
max-update-skew SKEW_VALUE
make-steps THRESHOLD_VALUE LIMIT_VALUE
priority PRIORITY_VALUE
sync-interface SYNC_IFNAME
pool POOL_ADDRESS MAX-SOURCES
gps [GPS_INTERVAL].
server SERVER_ADDRESS [min POLLING_MIN] [max POLLING_MAX] [polltarget POLLING_TARGET]
[port PORT_NO] ← Server configuration items in no particular order
no server SERVER_ADDRESS
no pool POOL_ADDRESS
no gps
no make-steps
no max-update-skew
no priority
no sync-interface
no enable
exit
no ntp
```

Command

Command	Contents						
ntp	Execute the NTP configuration command.  Executing a command in the setting mode shifts to the detailed setting mode.						
max-update-skew	Error expectation error range from 0.1 to 214748364 range from 0.1 to 214748364. The default is "100.0".						
make-steps	Sets the threshold and limit number of times for step expression synchronization. <table border="1" data-bbox="411 1384 1327 1778"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>THRESHOLD_VALUE</td> <td>Sets the threshold for step expression synchronization in the range of 0.1 to 214748364. The default is "1". Synchronization is initiated when the threshold set here is exceeded.</td> </tr> <tr> <td>LIMIT_VALUE</td> <td>The number of times the step expression synchronization limit is displayed in the range of 1 to 214748364. The default is "3". If the number of times the limit set here is exceeded, STEP-style synchronization will stop.</td> </tr> </tbody> </table>	Setting	Contents	THRESHOLD_VALUE	Sets the threshold for step expression synchronization in the range of 0.1 to 214748364. The default is "1". Synchronization is initiated when the threshold set here is exceeded.	LIMIT_VALUE	The number of times the step expression synchronization limit is displayed in the range of 1 to 214748364. The default is "3". If the number of times the limit set here is exceeded, STEP-style synchronization will stop.
Setting	Contents						
THRESHOLD_VALUE	Sets the threshold for step expression synchronization in the range of 0.1 to 214748364. The default is "1". Synchronization is initiated when the threshold set here is exceeded.						
LIMIT_VALUE	The number of times the step expression synchronization limit is displayed in the range of 1 to 214748364. The default is "3". If the number of times the limit set here is exceeded, STEP-style synchronization will stop.						
priority	Set the process priority of the NTP server (optional setting). <table border="1" data-bbox="411 1832 1327 1946"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PRIORITY_VALUE</td> <td>Sets the process priority of the NTP server in the range of 0 to 99.</td> </tr> </tbody> </table>	Setting	Contents	PRIORITY_VALUE	Sets the process priority of the NTP server in the range of 0 to 99.		
Setting	Contents						
PRIORITY_VALUE	Sets the process priority of the NTP server in the range of 0 to 99.						

Command	Contents					
sync-interface	Configure NTP server synchronization settings (optional setting).					
	Setting	Contents	SYNC_IFNAME	<p>Specify the interface to be synchronized at the time of connection/disconnection in the following format. Multiple interfaces cannot be specified.</p> <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0, rmnet_data0 ● Compact Router Indoor Type with wireless LAN, Compact Router Outdoor Type with wireless LAN lan<0,1>, wlan<0,1>, br<0-9>, rmnet_data0 		
Setting	Contents					
SYNC_IFNAME	<p>Specify the interface to be synchronized at the time of connection/disconnection in the following format. Multiple interfaces cannot be specified.</p> <ul style="list-style-type: none"> ● AI Edge Gateway wan0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, lan<0-3>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, ecm<0-9>, ppp<0-9>, tun<0-9>, tap<0-9> ● Indoor Compact Router eth0, rmnet_data0 ● Compact Router Indoor Type with wireless LAN, Compact Router Outdoor Type with wireless LAN lan<0,1>, wlan<0,1>, br<0-9>, rmnet_data0 					
pool	Set the NTP server pool mode by specifying the IP address and server name of the NTP server pool. Multiple settings can be configured.					
	Setting	Contents	POOL_ADDRESS	Set the IP address and server name of the NTP server pool.	MAX-SOURCES.	Sets the maximum number of sources for the NTP server pool in the range of 1 to 16. The default is "4".
	Setting	Contents				
POOL_ADDRESS	Set the IP address and server name of the NTP server pool.					
MAX-SOURCES.	Sets the maximum number of sources for the NTP server pool in the range of 1 to 16. The default is "4".					
gps	Enable the startup of the GPS daemon gpsd, which works with the NTP server.					
	Setting	Contents	GPS_INTERVAL	<p>You can set the time interval (in milliseconds) to access the GPS module from 100.0 to 1000.0. The default is "100.0".</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">   </div> <ul style="list-style-type: none"> ● The NTP server obtains GPS information from the gpsd daemon. ● If GPS_INTERVAL is omitted, the default value of "100.0" is used. ● Compact Router Indoor Type with wireless LAN will be fixed at "1000.0". </div>		
	Setting	Contents				
GPS_INTERVAL	<p>You can set the time interval (in milliseconds) to access the GPS module from 100.0 to 1000.0. The default is "100.0".</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">   </div> <ul style="list-style-type: none"> ● The NTP server obtains GPS information from the gpsd daemon. ● If GPS_INTERVAL is omitted, the default value of "100.0" is used. ● Compact Router Indoor Type with wireless LAN will be fixed at "1000.0". </div>					
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">    </div> <p>IoT Router Indoor Type, Compact Router Indoor Type, and Compact Router Outdoor Type with wireless LAN do not support GPS, so gps commands cannot be executed.</p> <p>By enabling this setting, it is possible to synchronize the time from "stratum-0" with GPS. In this case, the product will operate as "stratum-1".</p> </div>						

Command	Contents										
server	<p>Specify the IP address and server name of the NTP server in SERVER_ADDRESS and set to NTP server mode.</p> <p>If the following are not specified, default values are set. The following may also be specified in any order.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>min</td> <td>Sets the minimum polling interval (a power of 2) to the NTP server in the range of -4 to 24. The default is "6" (64 seconds).</td> </tr> <tr> <td>max</td> <td>Sets the maximum polling interval (a power of 2) to the NTP server, from 0 to 24. The default is "10" (1024 seconds).</td> </tr> <tr> <td>polltarget</td> <td>Sets the number of polling targets to be used by the regression algorithm within the polling interval range, from 6 to 60. The default is "6".</td> </tr> <tr> <td>port</td> <td>Set the number of the UDP port to be used for NTP in the range of 1 to 65535. The default is "123".</td> </tr> </tbody> </table>	Setting	Contents	min	Sets the minimum polling interval (a power of 2) to the NTP server in the range of -4 to 24. The default is "6" (64 seconds).	max	Sets the maximum polling interval (a power of 2) to the NTP server, from 0 to 24. The default is "10" (1024 seconds).	polltarget	Sets the number of polling targets to be used by the regression algorithm within the polling interval range, from 6 to 60. The default is "6".	port	Set the number of the UDP port to be used for NTP in the range of 1 to 65535. The default is "123".
Setting	Contents										
min	Sets the minimum polling interval (a power of 2) to the NTP server in the range of -4 to 24. The default is "6" (64 seconds).										
max	Sets the maximum polling interval (a power of 2) to the NTP server, from 0 to 24. The default is "10" (1024 seconds).										
polltarget	Sets the number of polling targets to be used by the regression algorithm within the polling interval range, from 6 to 60. The default is "6".										
port	Set the number of the UDP port to be used for NTP in the range of 1 to 65535. The default is "123".										
enable	<p>Enable NTP server startup and start the service; if the GPS daemon is disabled, enable the GPS daemon as well.</p> <p> IoT Router Indoor Type Compact Router Indoor Type and Compact Router Outdoor Type with wireless LAN do not support GPS, so the GPS daemon cannot be enabled.</p> <p> </p>										
show	<p>Displays NTP server settings.</p> <p>➔ For more information, see "7.3.3 Display NTP settings" for more information.</p>										
no server	Delete NTP server settings.										
no pool	Delete NTP server pool settings.										
no gps	<p>Delete GPS daemon configuration and stop GPS daemon.</p> <p> IoT Router Indoor Type Compact Router Indoor Type with wireless LAN and Compact Router Outdoor Type with wireless LAN do not support GPS, so the no gps command cannot be executed.</p> <p> </p>										
no make-steps	Remove step expression synchronization thresholds.										
no max-update-skew	Delete the Error Prediction Error Range setting.										
no priority	Delete the process priority setting for the NTP server.										
no sync-interface	Delete NTP server synchronization settings.										
no enable	<p>Disables the NTP server startup and stops the service; if the GPS daemon is enabled, it also disables the GPS daemon.</p> <p> IoT Router Indoor Type Compact Router Indoor Type with wireless LAN and Compact Router Outdoor Type with wireless LAN do not support GPS.</p> <p> </p>										
exit	Exit NTP advanced configuration mode and enter configuration mode.										
no ntp	Delete NTP settings.										

Execution example 1

Below is an example of how to set the Edge Gateway to Japanese Standard Time as published by NICT, with a minimum polling interval to the NTP server of 64 seconds (6th power of 2), a maximum polling interval of 1024 seconds (10th power of 2), a polling target count of 6, and an NTP port number of 123. The NTP port number is set to 123.

設定モード

```
amnimo(cfg)# ntp ←
amnimo(cfg-ntp)# server ntp.nict.jp min 6 max10 polltarget 6 port 123 ←
amnimo(cfg-ntp)# enable ←
amnimo(cfg-ntp)# exit ←
```

Execution example 2

The following is an example of how to configure an Edge Gateway to synchronize its time with GPS.

設定モード

```
amnimo(cfg)# ntp ←
amnimo(cfg-ntp)# gps 1000.0 ← ← Synchronize time by GPS at 1000ms intervals
amnimo(cfg-ntp)# enable ←
amnimo(cfg-ntp)# exit ←
```

Timing of Time Acquisition

The timing of time acquisition differs when using GPS and when using an NTP server via the Internet.

Synchronization destination	Time acquisition timing
GPS	<p>Time synchronization will be performed at the time (in milliseconds) set in GPS_INTERVAL.</p> <p> IoT Router Indoor Type Compact Router Indoor Type with wireless LAN and Compact Router Outdoor Type with wireless LAN do not support GPS.</p> <p></p> <p></p>
NTP Server	<p>Time synchronization will be performed at the time (in unit seconds) set in POLLING_MIN and POLLING_MAX.</p> <p>In addition, if it is configured with sync-interface SYNC_IFNAME, time acquisition is performed at the timing when the relevant interface is connected.</p>

7.4 Configure SSH settings



Display SSH (Secure Shell) settings and configure SSH settings.

7.4.1 Displaying SSH settings

To view SSH settings, run the *show config ssh* command.

Format

```
show config ssh
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- ssh configure ----
ssh
ENABLE
port PORT_NO
keepalive
ciphers CIPHER_TYPE
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLE	Displays information about when the SSH server is enabled/disabled. <table border="1" style="width: 100%; margin-top: 5px;"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
PORT_NO	The port number of the SSH server is displayed.						
CIPHER_TYPE	The available encryption methods for the SSH server are listed. By default, "default" is displayed.						

Execution example

Since SSH settings are involved in the startup control of the device, the settings cannot be displayed in general user mode. Below is an example of running in administrator mode and configuration mode.

管理者モード

```
amnimo# show config ssh ↵
# ---- transition to configure mode. ----
configure
# ---- ssh configure ----
ssh
enable
port 22
keepalive
ciphers default
exit
# ---- exit configure mode. ----
exit
```

設定モード

```
amnimo(cfg)# show config ssh ↵
# ---- ssh configure ----
ssh
enable
port 22
keepalive
ciphers default
exit
```



Running the *show config* command in SSH advanced configuration mode will display the same information as in configuration mode.

```
amnimo(cfg)# ssh      ← Go to SSH advanced configuration mode
amnimo(cfg-ssh)# show config ↵
enable               ← Same as setting mode
(Omitted.)
```

7.4.2 Configure SSH

To configure SSH, enter the advanced configuration mode and execute the configuration commands.

The settings made here are written to a configuration file.

Format

```
ssh
port PORT_NO
keepalive
ciphers CIPHER_TYPE
show config
no keepalive
enable
no enable
exit
no ssh
```

Command

Command	Contents																		
ssh	Execute SSH configuration commands.  Executing a command in the setting mode shifts to the detailed setting mode.																		
port	Specify the SSH port number in the range of 1 to 65535 for PORT_NO.																		
keepalive	Enable TCP keep-alive.																		
ciphers	Set CIPHER_TYPE to the encryption methods available on the SSH server. Multiple ciphers can be specified, separated by commas. <table border="1" data-bbox="467 1122 1246 1671"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>default</td> <td> <ul style="list-style-type: none"> ● chacha20-poly1305@openssh.com ● aes128-ctr ● aes192-ctr ● aes256-ctr ● aes128-gcm@openssh.com ● aes256-gcm@openssh.com </td> </tr> <tr> <td>aes128-ctr</td> <td>AES128bit CTR (Counter)</td> </tr> <tr> <td>aes192-ctr</td> <td>AES192bit CTR (Counter)</td> </tr> <tr> <td>aes256-ctr</td> <td>AES256bit CTR (Counter)</td> </tr> <tr> <td>aes128-cbc</td> <td>AES128-bit CBC (Cihper Block Chaining)</td> </tr> <tr> <td>aes192-cbc</td> <td>AES192-bit CBC (Cihper Block Chaining)</td> </tr> <tr> <td>aes256-cbc</td> <td>AES256-bit CBC (Cihper Block Chaining)</td> </tr> <tr> <td>3des-cbc</td> <td>Triple-DES CBC (Cihper Block Chaining)</td> </tr> </tbody> </table>	Setting	Contents	default	<ul style="list-style-type: none"> ● chacha20-poly1305@openssh.com ● aes128-ctr ● aes192-ctr ● aes256-ctr ● aes128-gcm@openssh.com ● aes256-gcm@openssh.com 	aes128-ctr	AES128bit CTR (Counter)	aes192-ctr	AES192bit CTR (Counter)	aes256-ctr	AES256bit CTR (Counter)	aes128-cbc	AES128-bit CBC (Cihper Block Chaining)	aes192-cbc	AES192-bit CBC (Cihper Block Chaining)	aes256-cbc	AES256-bit CBC (Cihper Block Chaining)	3des-cbc	Triple-DES CBC (Cihper Block Chaining)
Setting	Contents																		
default	<ul style="list-style-type: none"> ● chacha20-poly1305@openssh.com ● aes128-ctr ● aes192-ctr ● aes256-ctr ● aes128-gcm@openssh.com ● aes256-gcm@openssh.com 																		
aes128-ctr	AES128bit CTR (Counter)																		
aes192-ctr	AES192bit CTR (Counter)																		
aes256-ctr	AES256bit CTR (Counter)																		
aes128-cbc	AES128-bit CBC (Cihper Block Chaining)																		
aes192-cbc	AES192-bit CBC (Cihper Block Chaining)																		
aes256-cbc	AES256-bit CBC (Cihper Block Chaining)																		
3des-cbc	Triple-DES CBC (Cihper Block Chaining)																		
show config	Displays SSH server settings.  For more information, see " 7.4.1 Displaying SSH settings " for more information.																		
no keepalive	Disables TCP keep-alive.																		
enable	Start the service.																		
no enable	Stop the service.																		
exit	Exit SSH advanced setting mode and enter setting mode.																		
no ssh	Delete SSH settings.																		

Execution example

Below is an example of running without the Cipher Block Chaining (CBC) mode and running on a port number other than 22/TCP.

設定 モード

```
amnimo(cfg)# ssh ↵
amnimo(cfg-ssh)# ciphers aes128-ctr,aes192-ctr,aes256-ctr ↵
amnimo(cfg-ssh)# port 222 ↵
amnimo(cfg-ssh)# enable ↵
amnimo(cfg-ssh)# exit ↵
```

7.5 Configure DNS settings



Search for DNS names, view status and settings, and configure DNS settings.

7.5.1 Search for a name in the DNS

To look up a name in the DNS, run the *nslookup* command.

Format

```
nslookup <DOMAIN | ADDRESS> [query-type QUERY-TYPE [server SERVER-ADDRESS]]
```

Setting items

Item	Contents
DOMAIN	Specify the domain name to be queried.
ADDRESS	Specify the address to query. When an address is specified, it is searched in reverse order.
QUERY-TYPE	Specify one of the following query types: a, aaaa, ptr, mx, ns, soa, txt, or any. If omitted, a (IPv4) and aaaa (IPv6) are set for forward lookup and ptr for reverse lookup.
SERVER-ADDRESS	Specify the DNS server address to query. If omitted, its own default name server is set.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ nslookup google.co.jp query-type a server 8.8.8.8 ↵
; <<> DiG 9.11.3-1ubuntu1.11-Ubuntu <<> google.co.jp @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26406
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.co.jp.                IN      A

;; ANSWER SECTION:
google.co.jp.                299    IN      A      172.217.161.227

;; Query time: 67 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Feb 18 14:18:17 JST 2020
;; MSG SIZE rcvd: 57
```

7.5.2 Display DNS status

To view DNS status, run the *show dns* command. To view the DNS cache, run the *show dns cache* command.

Format

```
show dns
show dns cache
```

Output Format

```
Output of show dns
server-address ADDRESS
```

```
Output of show dns cache
START_RRSET_CACHE
-rrset-cache-data-
END_RRSET_CACHE
START_MSG_CACHE
-MSG-CACHE-DATA-
END_MSG_CACHE
EOF
```

Output item

Item	Contents
ADDRESS	The address of the currently used DNS server to query is displayed. If there are multiple DNS servers to query, multiple addresses will be displayed.
RRSET-CACHE-DATA	Resource Record Set (RRset) cache data is displayed.
MSG-CACHE-DATA	msg cache data will be displayed.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```
amnimo$ show dns ↵
server-address 8.8.8.8 8.8.4.4
amnimo$.
amnimo$ show dns cache ↵
START_RRSET_CACHE
;rrset 3093 1 1 8 0
x.arin.net. 42693 IN A 199.71.0.63
x.arin.net. 42693 IN RRSIG A 5 3 43200 20200302130008 20200217120008 646
08 arin.net. BpaLgmjMKKIhZ20088fNBU21VGxmvcmwUMtusWRBhIEhm2b1tv9ijX0 geDZ1ESfrguA9KxzJ
gQSbw3xL6+gykMHLp33ynfAS7BiopVY0QgNIXE9wGvV0nwkMMC1Tjdekt4J3sQbJNhPFRWxZDi5a5jea9RrK
3o5p+bVeV0jaXU= ;{id = 64608}
;rrset 3093 1 0 8 0
pdns196.ultradns.info. 3093 IN A 156.154.68.196
(Omitted.)
END_RRSET_CACHE
START_MSG_CACHE
msgid google.co.jp. in AAAA 32896 1 393 0 1 0 0
google.co.jp. in AAAA 0
msg pdns196.ultradns.info. IN AAAA 32896 1 393 0 1 1 0
pdns196.ultradns.info. in AAAA 0
(Omitted.)
```

```
END_MSG_CACHE
EOF
```

7.5.3 View DNS settings

To view the DNS configuration, run the *show config dns* command.

Format

```
show config dns
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- dns configure ----
dns
ENABLE
port port-number
QUERY-PORT-RANGE
log-level NUNBER
DNSSEC-SERVICE
DNSSEC-PERMISSIVE
cache-ttl min CACHE-MIN-TTL max CACHE-MAX-TTL
cache-ttl negative-max cache-negative-max-ttl
ROOT-SERVER
SERVER-ADDRESS
FORWARD
LOCAL-ZONE
LOCAL-ADDRESS
LOCAL-CNAME ← Alias definition (CNAME) is supported since V1.8.0.
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLE	Information is displayed when DNS servers are enabled/disabled. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
PORT-NUMBER	The DNS port number setting is displayed.						
QUERY-PORT-RANGE	The DNS port range settings are displayed in the following format <pre>min <i>MIN-PORT</i> max <i>MAX-PORT</i></pre> <table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MIN-PORT</td> <td>The port range (start value) of the query is displayed in the range 1024 to 65534.</td> </tr> <tr> <td>MAX-PORT</td> <td>The port range (end value) of the query is displayed in the range of 1025 to 65535.</td> </tr> </tbody> </table>	Item	Contents	MIN-PORT	The port range (start value) of the query is displayed in the range 1024 to 65534.	MAX-PORT	The port range (end value) of the query is displayed in the range of 1025 to 65535.
Item	Contents						
MIN-PORT	The port range (start value) of the query is displayed in the range 1024 to 65534.						
MAX-PORT	The port range (end value) of the query is displayed in the range of 1025 to 65535.						

Item	Contents												
LOG-LEVEL	The log output level is displayed.												
	<table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>operational</td> <td>Outputs operation information.</td> </tr> <tr> <td>detail-operational</td> <td>Outputs detailed operation information.</td> </tr> <tr> <td>query</td> <td>Outputs query-level information.</td> </tr> <tr> <td>algorithm</td> <td>Outputs algorithm-level information.</td> </tr> <tr> <td>client-cache-miss</td> <td>Outputs cache miss level information.</td> </tr> </tbody> </table>	Display	Contents	operational	Outputs operation information.	detail-operational	Outputs detailed operation information.	query	Outputs query-level information.	algorithm	Outputs algorithm-level information.	client-cache-miss	Outputs cache miss level information.
	Display	Contents											
	operational	Outputs operation information.											
	detail-operational	Outputs detailed operation information.											
	query	Outputs query-level information.											
algorithm	Outputs algorithm-level information.												
client-cache-miss	Outputs cache miss level information.												
DNSSEC-SERVICE	Information is displayed when DNSSEC is enabled.												
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "dnssec service" appears.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "dnssec service" appears.	Disable	Not displayed.						
	Setting	Display											
Enable	The message "dnssec service" appears.												
Disable	Not displayed.												
DNSSEC-PERMISSIVE	Information on valid responses to DNSSEC validation errors is displayed.												
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "dnssec permissive" is displayed.</td> </tr> <tr> <td>Disable</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "dnssec permissive" is displayed.	Disable	Not displayed.						
	Setting	Display											
Enable	The message "dnssec permissive" is displayed.												
Disable	Not displayed.												
CACHE-MIN-TTL	The minimum TTL (time to live) value (in seconds) when caching is displayed.												
CACHE-MAX-TTL	The maximum TTL value (in seconds) when caching is displayed.												
CACHE-NEGATIVE-MAX-TTL	The maximum TTL value (in seconds) of the negative cache is displayed.												
ROOT-SERVER	Displays information about when the DNS root server setting is enabled/disabled.												
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>It will be displayed as "root-server."</td> </tr> <tr> <td>Disable</td> <td>The message "no root-server" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	It will be displayed as "root-server."	Disable	The message "no root-server" is displayed.						
	Setting	Display											
Enable	It will be displayed as "root-server."												
Disable	The message "no root-server" is displayed.												
SERVER-ADDRESS	The server address is displayed in the following format												
	<code>server-address ADDRESS priority PRIORITY</code>												
	<table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ADDRESS</td> <td>The server address is displayed.</td> </tr> <tr> <td>PRIORITY</td> <td>Priority is displayed.</td> </tr> </tbody> </table>	Item	Contents	ADDRESS	The server address is displayed.	PRIORITY	Priority is displayed.						
Item	Contents												
ADDRESS	The server address is displayed.												
PRIORITY	Priority is displayed.												
FORWARD	The domain to forward and the IP address to query are displayed in the following format												
	<code>forward DOMAIN address ADDRESS</code>												
	<table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>DOMAIN</td> <td>The domain is displayed.</td> </tr> <tr> <td>ADDRESS</td> <td>The address is displayed.</td> </tr> </tbody> </table>	Item	Contents	DOMAIN	The domain is displayed.	ADDRESS	The address is displayed.						
	Item	Contents											
DOMAIN	The domain is displayed.												
ADDRESS	The address is displayed.												
 Forwarding is a function that queries a specified domain to a specified address.													
LOCAL-ZONE	Local zone settings are displayed in the following format												
	<code>local zone ZONE type TYPE</code>												
	<table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ZONE</td> <td>Zone settings are displayed.</td> </tr> <tr> <td>TYPE</td> <td>Type settings are displayed.</td> </tr> </tbody> </table>	Item	Contents	ZONE	Zone settings are displayed.	TYPE	Type settings are displayed.						
Item	Contents												
ZONE	Zone settings are displayed.												
TYPE	Type settings are displayed.												

Item	Contents								
LOCAL-ADDRESS	<p>The local address settings are displayed in the following format</p> <pre>local address ADDRESS name HOSTNAME ttl TTL</pre> <table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ADDRESS</td> <td>The address is displayed.</td> </tr> <tr> <td>HOSTNAME</td> <td>The host name is displayed.</td> </tr> <tr> <td>TTL</td> <td>TTL value is displayed.</td> </tr> </tbody> </table>	Item	Contents	ADDRESS	The address is displayed.	HOSTNAME	The host name is displayed.	TTL	TTL value is displayed.
Item	Contents								
ADDRESS	The address is displayed.								
HOSTNAME	The host name is displayed.								
TTL	TTL value is displayed.								
LOCAL-CNAME	<p>Local host name alias definitions are displayed in the following format</p> <pre>local cname CNAME name HOSTNAME ttl TTL</pre> <table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>CNAME</td> <td>The hostname alias definition is displayed.</td> </tr> <tr> <td>HOSTNAME</td> <td>The hostname is displayed.</td> </tr> <tr> <td>TTL</td> <td>TTL value is displayed.</td> </tr> </tbody> </table> <p> This function is supported since V1.8.0.</p>	Item	Contents	CNAME	The hostname alias definition is displayed.	HOSTNAME	The hostname is displayed.	TTL	TTL value is displayed.
Item	Contents								
CNAME	The hostname alias definition is displayed.								
HOSTNAME	The hostname is displayed.								
TTL	TTL value is displayed.								

Execution example

Below is an example run showing the configuration in administrator and configuration mode with the DNS server settings enabled and the query address set to 8.8.8.8.

管理者モード

```
amnimo# show config dns ↵
# ---- transition to configure mode. ----
configure
# ---- dns configure ----
dns
enable
port 53
query-port-range min 1024 max 65535
log-level operational
cache-ttl min 900 max 3600
cache-ttl negative-max 900
root-server
server-address 8.8.8.8 priority 10
exit
# ---- exit configure mode. ----
exit
```

設定モード

```
amnimo(cfg)# show config dns ↵
# ---- dns configure ----
dns
enable
port 53
query-port-range min 1024 max 65535
log-level operational
cache-ttl min 900 max 3600
cache-ttl negative-max 900
root-server
server-address 8.8.8.8 priority 10
```

exit



Running the show config dns command in advanced configuration mode will display the same information.

```
amnimo(cfg-dns)# show config dns ↵  
enable           ← Same as setting mode  
port 53  
(Omitted.)
```

7.5.4 Configure DNS settings

To configure DNS, go to advanced configuration mode and execute the configuration commands. The settings made here are written to a configuration file.

Format

```

dns
enable
no enable
port PORT-NUMBER
query-port-range min <1024 - 65534> max <1025 - 65535>
log-level <operational | detail-operational | query | algorithm | client-cache-miss
dnssec service
no dnssec service
dnssec permissive
no dnssec permissive
cache-ttl min <10 - 2419200> max <10 - 2419200>
cache-ttl negative-max <10 - 2419200>
root-server
server-address ADDRESS [priority <0 - 99>]]
no server-address ADDRESS
forward DOMAIN address ADDRESS
no forward DOMAIN
local zone ZONE_STRING type < deny | refuse | static | transparent | typetransparent |
redirect | nodefault >
no local zone ZONE_STRING
local address ADDRESS name HOSTNAME [ttl <10 - 2419200>]]
no local address ADDRESS
local cname CHOSTNAME name HOSTNAME [ttl <10 - 2419200>] ← Alias definition (CNAME) is su
pported since V1.8.0.
no local cname CHOSTNAME ← Alias definition (CNAME) is supported since V1.8.0.
exit

```

Command

Command	Contents						
dns	Execute DNS configuration commands.  Executing a command in the setting mode shifts to the detailed setting mode.						
enable	Start the service.						
no enable	Stop the service.						
port	Specify the port number in PORT-NUMBER.						
query-port-range	Specify a range of ports to issue queries. <pre>query-port-range min <i>MIN_PORT</i> max <i>MAX_PORT</i></pre>  Be sure to set the value so that max is the larger value. <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MIN_PORT</td> <td>Specify the minimum value of the query issue port range, in the range 1024-65534. The default value is "1024".</td> </tr> <tr> <td>MAX_PORT</td> <td>Specify the maximum value of the query's issue port range, in the range 1025-65535. The default value is "65535".</td> </tr> </tbody> </table>	Setting	Contents	MIN_PORT	Specify the minimum value of the query issue port range, in the range 1024-65534. The default value is "1024".	MAX_PORT	Specify the maximum value of the query's issue port range, in the range 1025-65535. The default value is "65535".
Setting	Contents						
MIN_PORT	Specify the minimum value of the query issue port range, in the range 1024-65534. The default value is "1024".						
MAX_PORT	Specify the maximum value of the query's issue port range, in the range 1025-65535. The default value is "65535".						

Command	Contents												
log-level	<p>Set the level of log output to LOGLEVEL.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>operational</td> <td>Outputs operation information.</td> </tr> <tr> <td>detail-operational</td> <td>Outputs detailed operation information.</td> </tr> <tr> <td>query</td> <td>Outputs query-level information for each query.</td> </tr> <tr> <td>algorithm</td> <td>Outputs algorithm-level information.</td> </tr> <tr> <td>client-cache-miss</td> <td>Outputs cache miss client identification information.</td> </tr> </tbody> </table>	Setting	Contents	operational	Outputs operation information.	detail-operational	Outputs detailed operation information.	query	Outputs query-level information for each query.	algorithm	Outputs algorithm-level information.	client-cache-miss	Outputs cache miss client identification information.
Setting	Contents												
operational	Outputs operation information.												
detail-operational	Outputs detailed operation information.												
query	Outputs query-level information for each query.												
algorithm	Outputs algorithm-level information.												
client-cache-miss	Outputs cache miss client identification information.												
dnssec service	Enable DNSSEC (DNS Security Extensions).												
no dnssec service	Disable DNSSEC.												
dnssec permissive	Enable response to errors in DNSSEC validation.												
no dnssec permissive	Disables the response to errors in DNSSEC validation.												
cache-ttl	<p>Sets the cache retention period (in seconds).</p> <pre>cache-ttl min <i>MIN_TTL</i> max <i>MAX_TTL</i></pre> <p> Be sure to set the value so that max is the larger value.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MIN_TTL</td> <td>Specify the minimum TTL value for the cache retention period in the range of 10 to 2419200. The default value is "900".</td> </tr> <tr> <td>MAX_TTL</td> <td>Specify the maximum TTL value for the cache retention period in the range of 10 to 2419200. The default value is "3600".</td> </tr> </tbody> </table>	Setting	Contents	MIN_TTL	Specify the minimum TTL value for the cache retention period in the range of 10 to 2419200. The default value is "900".	MAX_TTL	Specify the maximum TTL value for the cache retention period in the range of 10 to 2419200. The default value is "3600".						
Setting	Contents												
MIN_TTL	Specify the minimum TTL value for the cache retention period in the range of 10 to 2419200. The default value is "900".												
MAX_TTL	Specify the maximum TTL value for the cache retention period in the range of 10 to 2419200. The default value is "3600".												
cache-ttl negative-max	<p>Sets the maximum retention period (in seconds) for negative cache.</p> <pre>cache-ttl negative-max <i>NEG_MAX_TTL</i></pre> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>NEG_MAX_TTL</td> <td>Specify the minimum TTL value for the negative cache retention period in the range of 10 to 2419200. The default value is "900".</td> </tr> </tbody> </table>	Setting	Contents	NEG_MAX_TTL	Specify the minimum TTL value for the negative cache retention period in the range of 10 to 2419200. The default value is "900".								
Setting	Contents												
NEG_MAX_TTL	Specify the minimum TTL value for the negative cache retention period in the range of 10 to 2419200. The default value is "900".												
root-server	Enables querying the DNS root server.												
no root-server	Disables queries to the DNS root server.												
server-address	<p>Set the upper-level DNS servers to query (up to two).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ADDRESS</td> <td>Specify the address of the upper-level DNS server to query.</td> </tr> <tr> <td>priority PRIORITY</td> <td>Specify the priority in PRIORITY as a number from 0 to 99. The default value is 0.</td> </tr> </tbody> </table>	Setting	Contents	ADDRESS	Specify the address of the upper-level DNS server to query.	priority PRIORITY	Specify the priority in PRIORITY as a number from 0 to 99. The default value is 0.						
Setting	Contents												
ADDRESS	Specify the address of the upper-level DNS server to query.												
priority PRIORITY	Specify the priority in PRIORITY as a number from 0 to 99. The default value is 0.												
no server-address	Deletes the upper-level DNS server to be queried by specifying its address in ADDRESS.												
forward	<p>Forward queries for specified domains to a higher-level DNS server (up to 8 configured).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>DOMAIN</td> <td>Specify the domain.</td> </tr> <tr> <td>address ADDRESS</td> <td>Specify the address of the upper-level DNS server to be queried in ADDRESS.</td> </tr> </tbody> </table>	Setting	Contents	DOMAIN	Specify the domain.	address ADDRESS	Specify the address of the upper-level DNS server to be queried in ADDRESS.						
Setting	Contents												
DOMAIN	Specify the domain.												
address ADDRESS	Specify the address of the upper-level DNS server to be queried in ADDRESS.												

Command	Contents																								
no forward	Specify the domain in DOMAIN and remove the top DNS servers to query.																								
local zone	<p>Specify the local zone and set the operation (up to 16 settings). If the specified local zone does not exist, it will be added.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ZONE_STRING</td> <td>Specifies the local zone.</td> </tr> <tr> <td>type ZONE_TYPE</td> <td>Specify for ZONE_TYPE the local zone setting operation types shown in the following table, "Specifiable Operation Types".</td> </tr> <tr> <td></td> <td>Specifies the action to be taken when the zone specified by corresponds to the zone and the setting by the local address command does not exist.</td> </tr> </tbody> </table> <p>Possible operation types</p> <table border="1"> <thead> <tr> <th>Operation type</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>deny</td> <td>No response is returned.</td> </tr> <tr> <td>refuse</td> <td>REFUSED to rcode and returns an error message.</td> </tr> <tr> <td>static</td> <td>Returns nodata or nxdomain.</td> </tr> <tr> <td>transparent</td> <td>Recursive query processing.</td> </tr> <tr> <td>typetransparent</td> <td>Recursive query processing. However, even if the type (e.g., AAAA) is different, it is treated as a match.</td> </tr> <tr> <td>redirect</td> <td>Responds to queries on its own. Used to redirect domains along with configuration by the local address command.</td> </tr> <tr> <td>nodefault</td> <td>Turn off the default setting for the AS112 zone (reverse lookup of private addresses).</td> </tr> </tbody> </table>	Setting	Contents	ZONE_STRING	Specifies the local zone.	type ZONE_TYPE	Specify for ZONE_TYPE the local zone setting operation types shown in the following table, "Specifiable Operation Types".		Specifies the action to be taken when the zone specified by corresponds to the zone and the setting by the local address command does not exist.	Operation type	Contents	deny	No response is returned.	refuse	REFUSED to rcode and returns an error message.	static	Returns nodata or nxdomain.	transparent	Recursive query processing.	typetransparent	Recursive query processing. However, even if the type (e.g., AAAA) is different, it is treated as a match.	redirect	Responds to queries on its own. Used to redirect domains along with configuration by the local address command.	nodefault	Turn off the default setting for the AS112 zone (reverse lookup of private addresses).
Setting	Contents																								
ZONE_STRING	Specifies the local zone.																								
type ZONE_TYPE	Specify for ZONE_TYPE the local zone setting operation types shown in the following table, "Specifiable Operation Types".																								
	Specifies the action to be taken when the zone specified by corresponds to the zone and the setting by the local address command does not exist.																								
Operation type	Contents																								
deny	No response is returned.																								
refuse	REFUSED to rcode and returns an error message.																								
static	Returns nodata or nxdomain.																								
transparent	Recursive query processing.																								
typetransparent	Recursive query processing. However, even if the type (e.g., AAAA) is different, it is treated as a match.																								
redirect	Responds to queries on its own. Used to redirect domains along with configuration by the local address command.																								
nodefault	Turn off the default setting for the AS112 zone (reverse lookup of private addresses).																								
no local zone	Remove the <i>local zone</i> command setting by specifying the local zone in ZONE-STRING.																								
local address	<p>Responds to queries for specified address and host name (set up to 64).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ADDRESS</td> <td>Specifies the address to respond to.</td> </tr> <tr> <td>name HOSTNAME</td> <td>Specify the host name to respond to HOSTNAME.</td> </tr> <tr> <td>ttl TTL</td> <td>Set TTL to the TTL value to be returned on response, a number between 10 and 2419200. The default value is "3600".</td> </tr> </tbody> </table>	Setting	Contents	ADDRESS	Specifies the address to respond to.	name HOSTNAME	Specify the host name to respond to HOSTNAME.	ttl TTL	Set TTL to the TTL value to be returned on response, a number between 10 and 2419200. The default value is "3600".																
Setting	Contents																								
ADDRESS	Specifies the address to respond to.																								
name HOSTNAME	Specify the host name to respond to HOSTNAME.																								
ttl TTL	Set TTL to the TTL value to be returned on response, a number between 10 and 2419200. The default value is "3600".																								
no local address	Delete the <i>local address</i> command setting by specifying an address in ADDRESS.																								
local cname	<p>Responds to queries for alias definitions and hostnames (set to a maximum of 64).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>CHOSTNAME</td> <td>Specifies an alias definition.</td> </tr> <tr> <td>name HOSTNAME</td> <td>Specify the host name to respond to HOSTNAME.</td> </tr> <tr> <td>ttl TTL</td> <td>Set TTL to the TTL value to be returned upon response, as a number from 10 to 2419200 (seconds). The default value is "3600".</td> </tr> </tbody> </table> <p> This function is supported since V1.8.0.</p>	Setting	Contents	CHOSTNAME	Specifies an alias definition.	name HOSTNAME	Specify the host name to respond to HOSTNAME.	ttl TTL	Set TTL to the TTL value to be returned upon response, as a number from 10 to 2419200 (seconds). The default value is "3600".																
Setting	Contents																								
CHOSTNAME	Specifies an alias definition.																								
name HOSTNAME	Specify the host name to respond to HOSTNAME.																								
ttl TTL	Set TTL to the TTL value to be returned upon response, as a number from 10 to 2419200 (seconds). The default value is "3600".																								

Command	Contents
no local cname	Remove the <i>local address</i> command setting by specifying an alias definition for CHOSTNAME.  This function is supported since V1.8.0.
exit	Exit the detailed setting mode and enter the setting mode.

Execution example

Below is an example of enabling DNS server configuration and setting the query address to 8.8.8.8 in configuration mode.

設定モード

```
amnimo(cfg)# dns ←
amnimo(cfg-dns)# enable
amnimo(cfg-dns)# port 53
amnimo(cfg-dns)# query-port-range min 1024 max 65535
amnimo(cfg-dns)# log-level operational
amnimo(cfg-dns)# cache-ttl min 900 max 3600
amnimo(cfg-dns)# cache-ttl negative-max 900
amnimo(cfg-dns)# root-server
amnimo(cfg-dns)# server-address 8.8.8.8 priority 10
amnimo(cfg-dns)# exit
amnimo(cfg)#.
```

7.6 Configure DHCP server settings



Displays the DHCP lease list and DHCP server settings and configures DHCP server settings.



DHCP Relay (" 7.10 Configure DHCP relay settings ") is enabled, this DHCP server setting cannot be enabled.

7.6.1 Display a list of DHCP leases

To view a list of DHCP leases, run the *show dhcp lease* command.

Format

```
show dhcp lease IFNAME
```

Setting items

Item	Contents
IFNAME	Specifies the IPv4 interface name.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.



```
amnimo$ show dhcp lease eth0 ↵
MAC                IP                hostname          valid until      manufacturer
=====
=====
11:22:33:01:d3:23   192.168.0.100    test-client1     2020-03-03 02:38:47 -NA-
e8:1b:4b:5e:4c:94   192.168.0.102    test-client3     2020-03-03 02:39:26 amnimo Inc.
```



Compact Router do not have a notation in the **manufacturer** column.

7.6.2 Display DHCP server settings

To view the DHCP server configuration, run the *show config dhcp* command.

Format

```
show config dhcp [IFNAME].
```

Setting items

Item	Contents
IFNAME	Specifies the IPv4 interface name.  If IFNAME is omitted, the DHCP server settings for all configured interfaces will be displayed.

Output Format

```
# ---- transition to configure mode ----
configure
#
dhcp IFNAME
# ---- dhcp IFNAME configure ----
ENABLE
dynamic-ipv4-address-range
netmask IPV4-ADDRESS
leasetime MIN-TIME MAX-TIME
router IPV4-ADDRESS
DNS-SERVER-NAME
domain DOMAIN-NAME
NTP-SERVER
static MAC-ADDRESS IPV4-ADDRESS
STATIC-IPV4-ADDRESS
(If there is more than one, multiple lines will be displayed)
FAILSAFE
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLE	Displays information if the DHCP server for the specified IFNAME is enabled/disabled. <table border="1" data-bbox="488 1503 1264 1630"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
IFNAME	The network interface of the DHCP server is displayed.  The interface name displayed will vary by product. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, br<0-9> ● Edge Gateway eth0, br<0-9>. ● IoT Router eth<0-1>, br<0-9>. ● Indoor Compact Router eth0 ● Compact Router Indoor Type / Outdoor Type with wireless LAN lan<0-1>, wlan<0-1>, br<0-9> 						

Item	Contents						
dynamic-ipv4-address-range	If a range of dynamically leased addresses is set, the following is displayed dynamic <i>IPV4-ADDRESS-START IPV4-ADDRESS-END</i>						
	<table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>IPV4-ADDRESS-START</td> <td>Starting IP address of lease address</td> </tr> <tr> <td>IPV4-ADDRESS-END</td> <td>End of lease address IP address</td> </tr> </tbody> </table>	Item	Contents	IPV4-ADDRESS-START	Starting IP address of lease address	IPV4-ADDRESS-END	End of lease address IP address
	Item	Contents					
	IPV4-ADDRESS-START	Starting IP address of lease address					
IPV4-ADDRESS-END	End of lease address IP address						
MIN-TIME	Minimum lease term is displayed.						
MAX-TIME	The maximum lease term is displayed.						
DNS-SERVER-NAME	If a DNS server configuration exists, the following will be displayed dns <i>SERVER-NAME, SERVER-NAME,...</i>						
	<table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SERVER-NAME</td> <td>Server IP address or server name</td> </tr> </tbody> </table>	Item	Contents	SERVER-NAME	Server IP address or server name		
	Item	Contents					
SERVER-NAME	Server IP address or server name						
DOMAIN-NAME	The DNS domain name is displayed.						
STATIC-IPV4-ADDRESS	If there is a static IP address and MAC address combination setting, the following will be displayed static <i>MAC-ADDRESS STATIC-IPV4-ADDRESS</i>						
	<table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MAC-ADDRESS</td> <td>MAC address to which the IP address is set</td> </tr> <tr> <td>STATIC-IPV4-ADDRESS</td> <td>static IPv4 address</td> </tr> </tbody> </table>	Item	Contents	MAC-ADDRESS	MAC address to which the IP address is set	STATIC-IPV4-ADDRESS	static IPv4 address
	Item	Contents					
	MAC-ADDRESS	MAC address to which the IP address is set					
STATIC-IPV4-ADDRESS	static IPv4 address						
NTP-SERVER	If the IP address of the NTP server is set, the following is displayed ntp <i>SERVER-NAME, SERVER-NAME, . . .</i>						
	<table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SERVER-NAME</td> <td>Server IP address or server name</td> </tr> </tbody> </table>	Item	Contents	SERVER-NAME	Server IP address or server name		
Item	Contents						
SERVER-NAME	Server IP address or server name						

Item	Contents										
FALESAFE	<p>If a failsafe is configured to restart the DHCP service, you will see the following</p> <p>failsafe period <i>PERIOD</i> count <i>COUNT</i> retry <i>RETRY</i> reboot <i>REBOOT</i></p> <p>If DHCP DISCOVER is received from the same client (MAC address) more than the specified number of times ("count") in a specified period ("period"), the DHCP service is restarted.</p> <table border="1"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PERIOD</td> <td>The period over which DHCPDISCOVER is sampled, in the range of 60 to 3600 (seconds). The default setting is 600 (seconds).</td> </tr> <tr> <td>COUNT</td> <td>The number of times received that are determined to be fail-safe during the DHCPDISCOVER sampling period, in the range of 2 to 255. The default setting is 3.</td> </tr> <tr> <td>RETRY</td> <td>Displays the number of fail-safe retries in the range of 1 to 10. The default setting is 3.</td> </tr> <tr> <td>REBOOT</td> <td>The number of fail-safe reboots, ranging from 1 to 10. The default setting is 3.</td> </tr> </tbody> </table> <p> The fail-safe function can be configured for each interface, but not for multiple interfaces at the same time.</p> <p> It is implemented only on Compact Router after V1.9.0. For Edge Gateway and IoT Router, implementation is planned in the future.</p> <p> For more information on fail-safe features, see " 12.3 fail-safe " for more information on the fail-safe feature.</p>	Item	Contents	PERIOD	The period over which DHCPDISCOVER is sampled, in the range of 60 to 3600 (seconds). The default setting is 600 (seconds).	COUNT	The number of times received that are determined to be fail-safe during the DHCPDISCOVER sampling period, in the range of 2 to 255. The default setting is 3.	RETRY	Displays the number of fail-safe retries in the range of 1 to 10. The default setting is 3.	REBOOT	The number of fail-safe reboots, ranging from 1 to 10. The default setting is 3.
Item	Contents										
PERIOD	The period over which DHCPDISCOVER is sampled, in the range of 60 to 3600 (seconds). The default setting is 600 (seconds).										
COUNT	The number of times received that are determined to be fail-safe during the DHCPDISCOVER sampling period, in the range of 2 to 255. The default setting is 3.										
RETRY	Displays the number of fail-safe retries in the range of 1 to 10. The default setting is 3.										
REBOOT	The number of fail-safe reboots, ranging from 1 to 10. The default setting is 3.										

Execution example

The DHCP server settings cannot be displayed in general user mode because they are related to the startup control of the device.

Below is an example of running in administrator mode and configuration mode.

管理者モード

```
amnimo# show config dhcp eth0 ↵
# ---- transition to configure mode. ----
configure
dhcp eth0
# ---- dhcp eth0 configure ----
no enable
dynamic 192.168.3.20 192.168.3.40
netmask 255.255.255.0
leasetime 600 3600
router 10.5.5.1
dns ns2.example.org
domain example.org
ntp ntp2.org
static 12:34:56:78:90:60 192.168.3.10
static 12:34:56:78:91:60 192.168.3.11
exit
# ---- exit configure mode. ----
exit
```

設定モード

```
amnimo(cfg)# show config dhcp eth0 ↵
enable
dynamic 192.168.3.20 192.168.3.40
netmask 255.255.255.0
leasetime 600 3600
router 10.5.5.1
dns ns2.example.org
domain example.org
ntp ntp2.org
static 12:34:56:78:90:60 192.168.3.10
static 12:34:56:78:91:60 192.168.3.11
```



Running the **show config** command in the advanced configuration mode of the DHCP server displays the same information as in the configuration mode.

```
amnimo(cfg)# dhcp eth0↵ ← Go to DHCP advanced configuration mode
amnimo(cfg-dhcp-eth0)# show config ↵
dhcp eth0 ← Same as configuration mode below
(Omitted.)
```

7.6.3 Configure DHCP server settings

To configure an IPv4 DHCP server, go to advanced configuration mode and execute the configuration command.

The settings made here are written to a configuration file.

Format

```
dhcp [IFNAME].
dynamic IPV4-ADDRESS IPV4-ADDRESS
netmask IPV4-ADDRESS
leasetime MIN-TIME MAX-TIME
router IPV4-ADDRESS
dns SERVER-NAME,SERVER-NAME,...
domain DOMAIN-NAME
ntp SERVER-NAME,SERVER-NAME,...
static MAC-ADDRESS IPV4-ADDRESS
show config
failsafe [period <60 - 3600>] [count <2 - 255>] [retry <1 - 10>] [reboot <1 - 10>]
no static MAC-ADDRESS
no domain
no router
no dns
no ntp
enable
no enable
exit
no dhcp IFNAME
```

Command

Command	Contents
dhcp	<p>Execute the command by specifying the interface name in IFNAME.</p> <p> Configurable interface names vary by product.</p> <ul style="list-style-type: none"> ● AI Edge Gateway wan0, br<0-9> ● Edge Gateway eth0, br<0-9>. ● IoT Router eth<0-1>, br<0-9>. ● Indoor Compact Router eth0 ● Compact Router Indoor Type with wireless LAN eth0 <p> When an interface is specified in the configuration mode and executed, the program enters the advanced configuration mode for the DHCP server (IPv4) for the specified interface.</p>
dynamic	<p>Sets the range within which dynamic IP addresses are automatically assigned to clients. Specify the IP address (IPv4) for the upper and lower limits of the range in IPV4-ADDRESS.</p> <p> <ul style="list-style-type: none"> ● Settings beyond the netmask range are not allowed. ● Even within the netmask range, no more than 256 cases can be set. </p>
netmask	<p>Specify a subnet mask for IPV4-ADDRESS. The default value is 255.255.255.0.</p>

Command	Contents						
leasetime	<p>Sets the effective time to lease an IP address.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MIN-TIME</td> <td> <p>Specify the minimum lease term.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 86400 (seconds). ● The default value is 60 seconds. </td> </tr> <tr> <td>MAX-TIME</td> <td> <p>Specify the maximum lease term.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 86400 (seconds). ● The default value is 86400 seconds. </td> </tr> </tbody> </table>	Setting	Contents	MIN-TIME	<p>Specify the minimum lease term.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 86400 (seconds). ● The default value is 60 seconds. 	MAX-TIME	<p>Specify the maximum lease term.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 86400 (seconds). ● The default value is 86400 seconds.
Setting	Contents						
MIN-TIME	<p>Specify the minimum lease term.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 86400 (seconds). ● The default value is 60 seconds. 						
MAX-TIME	<p>Specify the maximum lease term.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 86400 (seconds). ● The default value is 86400 seconds. 						
router	<p>Specify the gateway address to be notified to the DHCP client side in IPV4-ADDRESS.</p> <p> If auto is specified, the IP address of IFNAME is used. The IP address should be set within the dynamic range.</p>						
dns	<p>Specify the IP address (IPv4) or server name of the DNS server to be notified to the DHCP client in SERVER-NAME. Multiple specifications can be specified, separated by commas.</p> <p> If auto is specified, the IP address of IFNAME is used. However, you cannot specify more than one IP address. The IP address must be set within the dynamic range.</p>						
domain	<p>Specify the DNS domain name to be notified to the DHCP client in DOMAIN-NAME.</p> <ul style="list-style-type: none"> ● Must be no more than 253 characters. ● Domain names must begin and end with single-byte alphanumeric characters, and the rest of the name must consist of single-byte alphanumeric characters or "-" (hyphen) and "." (period). 						
ntp	<p>Specify the IP address (IPv4) of the NTP server to be notified to the DHCP client in SERVER-NAME. Multiple specifications can be specified, separated by commas.</p> <p> If auto is specified, the IP address of IFNAME is used. However, you cannot specify more than one IP address. The IP address must be set within the dynamic range.</p>						
static	<p>Assigns a static IP address to the client holding the specified MAC address. Up to 16 can be set.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MAC-ADDRESS</td> <td> <p>Specify the MAC address in the following format XX:XX:XX:XX:XX:XX:XX:XX</p> </td> </tr> <tr> <td>IPV4-ADDRESS</td> <td> <p>Specifies an IP address (IPv4).</p> </td> </tr> </tbody> </table>	Setting	Contents	MAC-ADDRESS	<p>Specify the MAC address in the following format XX:XX:XX:XX:XX:XX:XX:XX</p>	IPV4-ADDRESS	<p>Specifies an IP address (IPv4).</p>
Setting	Contents						
MAC-ADDRESS	<p>Specify the MAC address in the following format XX:XX:XX:XX:XX:XX:XX:XX</p>						
IPV4-ADDRESS	<p>Specifies an IP address (IPv4).</p>						
show config	<p>Displays the DHCP server settings.</p> <p>➔ For more information, see "7.6.2 Display DHCP server settings" for more information.</p>						

Command	Contents										
failsafe	<p>Enable fail-safe to restart the DHCP service.</p> <p>This failsafe function restarts the DHCP service if the DHCP DISCOVER message is received from the same client (MAC address) more than the specified number of times (specified by "count") in a specified period of time (specified by "period"). DHCP DISCOVER is received from the same client (MAC address) for a specified period of time (specified by "period").</p> <p>The default setting is disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>period</td> <td>Specify the period of time to sample DHCPDISCOVER in the range of 60 to 3600 (seconds). The default setting is 600 (seconds).</td> </tr> <tr> <td>count</td> <td>Specify the number of times to receive the DHCPDISCOVER to be judged as fail-safe during the sampling period, in the range of 2 to 255. The default setting is 3.</td> </tr> <tr> <td>retry</td> <td>Specify the number of fail-safe retries in the range of 1 to 10. The default setting is 3.</td> </tr> <tr> <td>reboot</td> <td>Specify the number of fail-safe reboots in the range of 1 to 10. The default setting is 3.</td> </tr> </tbody> </table> <p> • The fail-safe function can be configured for each interface, but not for multiple interfaces at the same time.</p> <p>• Implemented in firmware V1.9.0 or later.</p> <p>➔ For more information on fail-safe features, see "12.3 fail-safe" for more information on the fail-safe feature.</p>	Setting	Contents	period	Specify the period of time to sample DHCPDISCOVER in the range of 60 to 3600 (seconds). The default setting is 600 (seconds).	count	Specify the number of times to receive the DHCPDISCOVER to be judged as fail-safe during the sampling period, in the range of 2 to 255. The default setting is 3.	retry	Specify the number of fail-safe retries in the range of 1 to 10. The default setting is 3.	reboot	Specify the number of fail-safe reboots in the range of 1 to 10. The default setting is 3.
Setting	Contents										
period	Specify the period of time to sample DHCPDISCOVER in the range of 60 to 3600 (seconds). The default setting is 600 (seconds).										
count	Specify the number of times to receive the DHCPDISCOVER to be judged as fail-safe during the sampling period, in the range of 2 to 255. The default setting is 3.										
retry	Specify the number of fail-safe retries in the range of 1 to 10. The default setting is 3.										
reboot	Specify the number of fail-safe reboots in the range of 1 to 10. The default setting is 3.										
no failsafe	Disable fail-safe.										
no static	Deletes the assignment of a static IP address to the client that holds the MAC address specified in MAC-ADDRESS.										
no domain	Delete DNS domain name settings.										
no router	Delete the IP address setting of the gateway.										
no dns	Delete the IP address setting of the DNS server.										
no ntp	Delete the NTP server IP address setting.										
enable	Enables the DHCP server for the specified IFNAME and starts the service.										
no enable	Disables the DHCP server of the specified IFNAME and stops the service.										
exit	Exit the detailed setting mode and enter the setting mode.										
no dhcp	Stops and disables the DHCP server service for the specified IFNAME.										

Execution example

設定モード

```
amnimo(cfg)# dhcp eth0 ↵
amnimo(cfg-dhcp-eth0)# dynamic 192.168.3.20 192.168.3.40 ↵
amnimo(cfg-dhcp-eth0)# netmask 255.255.255.0 ↵
amnimo(cfg-dhcp-eth0)# leasetime 600 3600 ↵
amnimo(cfg-dhcp-eth0)# router 10.5.5.1 ↵
amnimo(cfg-dhcp-eth0)# dns ns2.example.org ↵
amnimo(cfg-dhcp-eth0)# domain example.org ↵
amnimo(cfg-dhcp-eth0)# ntp ntp2.org ↵
amnimo(cfg-dhcp-eth0)# static 12:34:56:78:90:60 192.168.3.10 ↵
amnimo(cfg-dhcp-eth0)# static 12:34:56:78:99:61 192.168.3.11 ↵
amnimo(cfg-dhcp-eth0)# enable ↵
amnimo(cfg-dhcp-eth0)# exit ↵
amnimo(cfg)# no dhcp eth0 ↵
```

7.7 Set up a schedule



Displays the operating status of the schedule, displays schedule settings, and configures schedule settings.

7.7.1 Display the operating status of the schedule

To view the operating status of the schedule, run the *show schedule* command.

This command allows the user to check the operation status of the last task executed or the task currently being executed.



- The operating status of each task is maintained in a separate file.
- When a task is executed, the operation status of the corresponding task is updated.
- If a task is deleted, the operation status of the corresponding task will not be displayed.

Format

```
show schedule
```

Output Format

NAME	TYPE	START	CMD/STATUS
TASKNAME	SCHEDULE-TYPE	START-TIME	CMD-STATUS
(Omitted.)			

Output item

Item	Contents								
TASKNAME	The task name is displayed.								
SCHEDULE-TYPE	<p>One of the following schedule types will be displayed</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>keep-alive</td> <td>The dead/alive monitoring function by ping operates at the scheduled time and executes each control process (action) regarding this device that has been set if ping fails.</td> </tr> <tr> <td>general-control</td> <td>Execute actions at the scheduled time.</td> </tr> <tr> <td>user-define</td> <td>Execute user-defined commands at scheduled times.</td> </tr> </tbody> </table> <p>    In Compact Router Not displayed. </p>	Setting	Contents	keep-alive	The dead/alive monitoring function by ping operates at the scheduled time and executes each control process (action) regarding this device that has been set if ping fails.	general-control	Execute actions at the scheduled time.	user-define	Execute user-defined commands at scheduled times.
Setting	Contents								
keep-alive	The dead/alive monitoring function by ping operates at the scheduled time and executes each control process (action) regarding this device that has been set if ping fails.								
general-control	Execute actions at the scheduled time.								
user-define	Execute user-defined commands at scheduled times.								
START-TIME	The time at which the task will start executing is displayed.								

Item	Contents										
CMD-STATUS	The action name or execution status of the task is displayed. The contents of the display will vary depending on the SCHEDULE-TYPE.										
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>keep-alive</td> <td> <ul style="list-style-type: none"> ● If a ping is being sent, "ping(running)" is displayed. ● If the ping is successful, "ping(OK)" is displayed. ● If the ping fails, the name of the action to be performed is displayed. Example: soft-reboot </td> </tr> <tr> <td>general-control</td> <td>The name of the action to be performed is displayed.</td> </tr> <tr> <td>user-define</td> <td> <ul style="list-style-type: none"> ● If the command is executed successfully, "finished" is displayed. ● If the result of executing the command is failure, "failed" is displayed. <div style="display: flex; align-items: center;">  Not shown on Compact Router. </div> </td> </tr> <tr> <td>be common</td> <td>If the task is not yet executed, "waiting" will be displayed.</td> </tr> </tbody> </table>	Setting	Contents	keep-alive	<ul style="list-style-type: none"> ● If a ping is being sent, "ping(running)" is displayed. ● If the ping is successful, "ping(OK)" is displayed. ● If the ping fails, the name of the action to be performed is displayed. Example: soft-reboot 	general-control	The name of the action to be performed is displayed.	user-define	<ul style="list-style-type: none"> ● If the command is executed successfully, "finished" is displayed. ● If the result of executing the command is failure, "failed" is displayed. <div style="display: flex; align-items: center;">  Not shown on Compact Router. </div>	be common	If the task is not yet executed, "waiting" will be displayed.
	Setting	Contents									
	keep-alive	<ul style="list-style-type: none"> ● If a ping is being sent, "ping(running)" is displayed. ● If the ping is successful, "ping(OK)" is displayed. ● If the ping fails, the name of the action to be performed is displayed. Example: soft-reboot 									
general-control	The name of the action to be performed is displayed.										
user-define	<ul style="list-style-type: none"> ● If the command is executed successfully, "finished" is displayed. ● If the result of executing the command is failure, "failed" is displayed. <div style="display: flex; align-items: center;">  Not shown on Compact Router. </div>										
be common	If the task is not yet executed, "waiting" will be displayed.										

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```

amnimo$ show schedule ↵
NAME  TYPE          START          CMD/STATUS
task1 keep-alive    2020-02-11 23:02:00 ping(running)
amnimo$ show schedule ↵
NAME  TYPE          START          CMD/STATUS
task1 keep-alive    2020-02-11 23:05:00 soft-reboot
task2 general-control 2020-02-12 01:10:00 poe-reset-supply
task3 user-define    2020-02-13 10:00:00 finished
    
```



Compact Router cannot configure user-define, so it is not shown.

7.7.2 View schedule settings

To view the schedule settings, run the *show config schedule* command.



user-define cannot be configured on Compact Router.

Format

```
show config schedule keep-alive [TASKNAME].
show config schedule general-control [TASKNAME].
show config schedule user-define [TASKNAME].
```

Output Format

```
←Tasks whose schedule type is keep-alive
# --- transition to configure mode ---
configure
# --- schedule keep-alive TASKNAME configure ---
schedule keep-alive TASKNAME
ENABLE
datetime DATETIME
action ACTION
ping dest DESTINATION
SOURCE.
ping interval INTERVAL
ping count COUNT
DEADLINE
ping timeout TIMEOUT
ping delay MAX-DELAY
ping wait MAX-WAIT
exit
# --- exit configure mode ---
exit

Tasks with schedule type general-control
# --- transition to configure mode ---
configure
# --- schedule general-control TASKNAME configure ---
schedule general-control TASKNAME
ENABLE
datetime DATETIME
action ACTION
FAILSAFE
exit
# --- exit configure mode ---
exit

Tasks with schedule type user-define
# --- transition to configure mode ---
configure
# --- schedule user-define TASKNAME configure ---
schedule user-define TASKNAME
ENABLE
datetime DATETIME
command COMMAND
exit
# --- exit configure mode ---
exit
```

Output item

Item	Contents						
TASKNAME	<p>The task name is displayed.</p>  <ul style="list-style-type: none"> ● If TASKNAME is omitted, the settings for all tasks in the corresponding schedule will be displayed. ● Entering the "Tab" key completes the task name entry. 						
ENABLE	<p>Information is displayed when the task is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
DATETIME	The date and time of the task execution will be displayed.						
DESTINATION	The destination host for ping requests is displayed.						
SOURCE.	<p>Depending on whether or not the source of the ping request is configured, it will be displayed in the following format (optional setting)</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Setting</td> <td>The message "ping source {IP-ADDRESS}" is displayed.</td> </tr> <tr> <td>No setting</td> <td>The message "no ping source" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Setting	The message "ping source {IP-ADDRESS}" is displayed.	No setting	The message "no ping source" is displayed.
Setting	Display						
Setting	The message "ping source {IP-ADDRESS}" is displayed.						
No setting	The message "no ping source" is displayed.						
INTERVAL	The interval (in seconds) at which ping requests are sent is displayed.						
COUNT	The maximum number of ping requests to be sent is displayed.						
DEADLINE	<p>Depending on whether or not the maximum ping execution time (in seconds) is set, it is displayed in the following format (optional setting)</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Setting</td> <td>The message "ping deadline {maximum execution time}" is displayed.</td> </tr> <tr> <td>No setting</td> <td>The message "no ping deadline" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Setting	The message "ping deadline {maximum execution time}" is displayed.	No setting	The message "no ping deadline" is displayed.
Setting	Display						
Setting	The message "ping deadline {maximum execution time}" is displayed.						
No setting	The message "no ping deadline" is displayed.						
TIMEOUT	The set time (in seconds) for ping request timeout is displayed.						
MAX-DELAY	The upper limit of the random waiting time (in seconds) before ping is executed is displayed.						
MAXWAIT	When switching ping destinations, the maximum random waiting time (in seconds) is displayed.						
COMMAND	The command for the task specified by the user is displayed.						
FAILSAFE	<p>The maximum number of soft-reboot or hard-reboot reboots to be performed when the number of retries (3) is exceeded in the failsafe function is displayed.</p> <ul style="list-style-type: none"> ● If the schedule type is general-control and the action is soft-reboot or hard-reboot ● If the schedule type is keep-alive and the action is soft-reboot or hard-reboot or disconnect COMM <p>Depending on whether it is enabled or disabled, it will appear in the following format</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "failsafe reboot {max reboot count}" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no failsafe" is displayed.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> ● If the action is other than the above, nothing is displayed. 	Setting	Display	Enable	The message "failsafe reboot {max reboot count}" is displayed.	Disable	The message "no failsafe" is displayed.
Setting	Display						
Enable	The message "failsafe reboot {max reboot count}" is displayed.						
Disable	The message "no failsafe" is displayed.						

ACTION	The task action is displayed.	
	Setting	Contents
	soft-reboot	<p>If a software reboot is configured, the following is displayed</p> <pre>action soft-reboot</pre> <p>If the schedule type is general-control, the following may be displayed</p> <ul style="list-style-type: none"> Scheduled reboot configuration with random execution time <pre>action soft-reboot random RANDOM-TIME</pre> <ul style="list-style-type: none"> Reboot settings based on elapsed startup time <pre>action soft-reboot uptime UPTIME</pre> <p> The random and uptime options are supported by firmware V1.11.0 or later.</p>
	hard-reboot	<p>If a hardware reboot is configured, the following is displayed</p> <pre>action hard-reboot</pre> <p>If the schedule type is general-control, the following may be displayed</p> <ul style="list-style-type: none"> Scheduled reboot configuration with random execution time <pre>action hard-reboot random RANDOM-TIME</pre> <ul style="list-style-type: none"> Reboot settings based on elapsed startup time <pre>action hard-reboot uptime UPTIME</pre> <p> The random and uptime options are supported by firmware V1.11.0 or later.</p>
	poe-reset-supply	<p>If the poe feed is set to reset, the following is displayed</p> <pre>action poe-reset-supply POE-IFNAME down-time TIME</pre> <p> Indoor Type IoT Router Indoor Type and Compact Router Indoor Type do not support PoE, so poe-reset-supply is not shown.</p>
	connect COMM	<p>Connect each communication.*1,2 The COMM will be set to ppp or ecm.*3</p> <ul style="list-style-type: none"> ppp When connecting ppp communication, the following is displayed <pre>action connect ppp PPP-IFNAME</pre> <ul style="list-style-type: none"> ecm When connecting a mobile module, the following is displayed <pre>action connect ecm ECM-IFNAME</pre>
	disconnect COMM	<p>Disconnects each communication. COMM is set to either ppp, ecm, or ipsec.</p> <ul style="list-style-type: none"> ppp When disconnecting ppp communication, the following is displayed <pre>action disconnect ppp</pre>

	<ul style="list-style-type: none"> ● ecm Disconnect the communication of the mobile module.^{※4} If the setting is to disconnect the mobile module communication, reset the mobile module, and then reconnect, the following message is displayed. <pre>action disconnect ecm ECM-IFNAME reset enable</pre> If you disconnect the ecm communication, do not reset the mobile module, and do not reconnect the configuration, you will see the following <pre>action disconnect ecm ECM-IFNAME reset disable</pre>  Compact Router are not configured to reset the mobile module. <ul style="list-style-type: none"> ● ipsec^{※5} When disconnecting IPsec communication, the following is displayed. <pre>action disconnect ipsec IPSEC-NAME</pre>
wifi TYPE WIFI-IFNAME	<p>Reset control of the wireless LAN chip; TYPE displays the wireless LAN access point or station.</p> <ul style="list-style-type: none"> ● ap For wireless LAN access points, when reconnecting after resetting the wireless LAN chip, the following message is displayed <pre>action wifi ap WIFI-IFNAME reset enable</pre> If the wireless LAN chip is not reset and is set to not reconnect, the following will be displayed <pre>action wifi ap WIFI-IFNAME reset disable</pre> ● sta Regarding the wireless LAN station, when reconnecting after resetting the wireless LAN chip, the following message appears <pre>action wifi sta WIFI-IFNAME reset enable</pre> If the wireless LAN chip is not reset and is set to not reconnect, the following will be displayed <pre>action wifi sta WIFI-IFNAME reset disable</pre>  <ul style="list-style-type: none"> ● Resetting the wireless LAN chip will also temporarily stop communication with any wireless LAN interfaces that are not specified . ● Only Compact Router with wireless LAN are supported.

- 1 Actions used in tasks with a schedule type of general-control.
- 2 Indoor type Compact Router do not support ppp.
- 3 For Compact Router, the interface of the mobile module is rmnet_data.
- 4 If the schedule type is keep-alive, reconnect.
- 5 Actions used in tasks with a keep-alive schedule type.

See the table below for the interfaces specified in each setting.

Setting	Contents
ECM-IFNAME	<ul style="list-style-type: none"> ● AI Edge Gateway, Edge Gateway, IoT Router ecm0 ● Compact Router rmnet_data0

Item	Contents
POE-IFNAME	<ul style="list-style-type: none"> ● AI Edge Gateway, Edge Gateway lan<0-3> ● IoT Router Outdoor Type eth<0-1> ● Outdoor Type Wireless LAN Compact Router lan1  Indoor Type IoT Router Indoor Type, Compact Router Indoor Type with wireless LAN, and Compact Router Indoor Type with wireless LAN do not support PoE, so POE-IFNAME cannot be specified.
IPSEC-NAME	<p>Specify the IPsec SA configuration name.</p> <p>➔ The SA setting name is the SA setting name configured in "Configuring IPsec SA" in " 6.7.5 Configure IPsec".</p> <pre style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">ipsec sa SA-NAME</pre>
PPP-IFNAME	<p>ppp<0-9></p>  Indoor type Compact Router do not support PPP, so PPP-IFNAME cannot be specified.
WIFI-IFNAME	<ul style="list-style-type: none"> ● Compact Router Indoor Type with wireless LAN wlan<0-1>

Execution example

Below is an example of running the administrator and configuration modes on the Edge Gateway.

管理者モード

```
amnimo# show config schedule keep-alive camera1 ← Schedule with schedule type
keep-alive
# ---- transition to configure mode. ----
configure
# ---- keep-alive configure ----
schedule keep-alive camera1
enable
datetime * * * * *
action poe-reset-supply lan1 down-time 60
ping dest 192.168.1.100
no ping source
ping interval 3
ping count 3
no ping deadline
ping timeout 10
ping delay 0
ping wait 3
exit
# ---- exit configure mode. ----
exit
amnimo# show config schedule general-control reboot ← Schedule with schedule type g
eneral-control
# ---- transition to configure mode. ----
configure
# ---- general-control configure ----
schedule general-control reboot
enable
datetime 0 4 31 12 *
action hard-reboot
failsafe reboot 3
exit
# ---- exit configure mode. ----
exit
amnimo# show config schedule user-define userping ← Schedule with schedule type u
ser-define
# ---- transition to configure mode. ----
configure
# ---- user-define configure ----
schedule user-define userping
enable
datetime 0 * * * * *
command ping 192.168.2.110
exit
# ---- exit configure mode. ----
exit
```

```

amnimo(cfg)# show config schedule keep-alive camera1 ← Show schedule with s
chedule type keep-alive
# ---- keep-alive configure ----
schedule keep-alive camera1
enable
datetime * * * * *
action poe-reset-supply lan1 down-time 60
ping dest 192.168.1.100
no ping source
ping interval 3
ping count 3
no ping deadline
ping timeout 10
ping delay 0
ping wait 3
exit
amnimo(cfg)# show config schedule general-control reboot ← Schedule with schedu
le type general-control
# ---- general-control configure ----
schedule general-control reboot
enable
datetime 0 4 31 12 *
action hard-reboot
failsafe reboot 3
exit
amnimo(cfg)# show config schedule user-define userping ← Show schedule with s
chedule type user-define
# ---- user-define configure ----
schedule user-define userping
enable
datetime 0 * * * * *
command ping 192.168.2.110
exit

```



Running the show config command in advanced schedule configuration mode will display the same information as in configuration mode.

Execute the schedule command with one of the following schedule types: "keep-alive", "general-control", or "user-define".

```

amnimo(cfg)# schedule keep-alive camera1 ← Go to advanced setting mode of s
chedule
amnimo(cfg-sch-ka-camera1)# show config ←
enable ← Same as setting mode
datetime * * * * *
(Omitted.)

```

7.7.3 Set a schedule

To set the schedule, go to the advanced configuration mode and execute the configuration command.

Execute the schedule command with one of the following schedule types: "keep-alive", "general-control", or "user-define" to enter the respective advanced configuration mode.

The settings made here are written to a configuration file.



user-define cannot be configured on Compact Router.

Format (for setting a task of schedule type "keep-alive")

```

schedule keep-alive TASKNAME
enable
no enable
datetime DATETIME
action soft-reboot
action hard-reboot
action poe-reset-supply POE-IFNAME [down-time TIME].
action disconnect ppp PPP-IFNAME
action disconnect ECM ECM-IFNAME [reset <enable | disable>].
action disconnect ipsec IPSEC-NAME
action wifi ap AP-IFNAME [reset <enable | disable>].
action wifi sta STA-IFNAME [reset <enable | disable>].
ping dest DESTINATION
no ping dest DESTINATION
ping source SOURCE
no ping source
ping interval INTERVAL
ping count COUNT
ping deadline DEADLINE
no ping deadline
ping timeout TIMEOUT
ping delay MAX-DELAY
ping wait MAX-WAIT
failsafe reboot COUNT
no failsafe
exit

```

Format (for setting a task of schedule type "general-control")

```

schedule general-control TASKNAME
enable
no enable
datetime DATETIME
action soft-reboot [random RANDOM-TIME | uptime UPTIME].
action hard-reboot [random RANDOM-TIME | uptime UPTIME].
action poe-reset-supply POE-IFNAME [down-time TIME].
action disconnect ppp PPP-IFNAME
action disconnect ECM ECM-IFNAME [reset <enable | disable>].
action connect ppp PPP-IFNAME
action connect ECM ECM-IFNAME
failsafe reboot COUNT
no failsafe
exit

```

Format (for setting a task of schedule type "user-define")

```

schedule user-define TASKNAME
enable
no enable
datetime DATETIME
command COMMAND
no schedule keep-alive TASKNAME
no schedule general-control TASKNAME
no schedule user-define TASKNAME
    
```

Command

Command	Contents																						
schedule keep-alive schedule general-control schedule user-define	Execute the command to set the schedule, specifying the task name in TASKNAME.  <ul style="list-style-type: none"> Task names can be up to 32 alphanumeric characters. Executing a command in the setting mode shifts to the detailed setting mode. 																						
enable	Enable task.																						
no enable	Disables the task.																						
datetime	Specify the date and time of task execution in DATETIME in the following format min hour dom month dow <ul style="list-style-type: none"> Format <table border="1" data-bbox="571 1070 1353 1361"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>min</td> <td>Minutes (0-59)</td> </tr> <tr> <td>hour</td> <td>Hour (0-23)</td> </tr> <tr> <td>dom</td> <td>Sun (1-31)</td> </tr> <tr> <td>month</td> <td>Month (1-12)</td> </tr> <tr> <td>dow</td> <td>Day of the week (0-6) The "0" represents Sunday.</td> </tr> </tbody> </table> Designation Method <table border="1" data-bbox="571 1424 1353 2033"> <thead> <tr> <th>Designation Method</th> <th>Setting Example</th> </tr> </thead> <tbody> <tr> <td>list</td> <td>Setting example: 0,10,20,30 If specified as min, it will be executed at 0, 10, 20, or 30 minutes.</td> </tr> <tr> <td>Scope.</td> <td>Setting example: 1-5 If you specify MONTH, the process will be executed in January, February, March, April, and May.</td> </tr> <tr> <td>List + Range</td> <td>Setting example: 1,6,9-11 If you specify "hour," processing will be executed at 1:00, 6:00, 9:00, 10:00, and 11:00.</td> </tr> <tr> <td>interval</td> <td>Setting example: */10 If "min" is specified, processing is executed at 10-minute intervals. If you specify "/" followed by a value, processing will be executed at intervals of the specified value.</td> </tr> </tbody> </table> 	Setting	Contents	min	Minutes (0-59)	hour	Hour (0-23)	dom	Sun (1-31)	month	Month (1-12)	dow	Day of the week (0-6) The "0" represents Sunday.	Designation Method	Setting Example	list	Setting example: 0,10,20,30 If specified as min, it will be executed at 0, 10, 20, or 30 minutes.	Scope.	Setting example: 1-5 If you specify MONTH, the process will be executed in January, February, March, April, and May.	List + Range	Setting example: 1,6,9-11 If you specify "hour," processing will be executed at 1:00, 6:00, 9:00, 10:00, and 11:00.	interval	Setting example: */10 If "min" is specified, processing is executed at 10-minute intervals. If you specify "/" followed by a value, processing will be executed at intervals of the specified value.
Setting	Contents																						
min	Minutes (0-59)																						
hour	Hour (0-23)																						
dom	Sun (1-31)																						
month	Month (1-12)																						
dow	Day of the week (0-6) The "0" represents Sunday.																						
Designation Method	Setting Example																						
list	Setting example: 0,10,20,30 If specified as min, it will be executed at 0, 10, 20, or 30 minutes.																						
Scope.	Setting example: 1-5 If you specify MONTH, the process will be executed in January, February, March, April, and May.																						
List + Range	Setting example: 1,6,9-11 If you specify "hour," processing will be executed at 1:00, 6:00, 9:00, 10:00, and 11:00.																						
interval	Setting example: */10 If "min" is specified, processing is executed at 10-minute intervals. If you specify "/" followed by a value, processing will be executed at intervals of the specified value.																						

Command	Contents								
action soft-reboot	<p>Set the action to software reboot.</p> <p>If the schedule type is general-control, the following settings are available</p> <ul style="list-style-type: none"> Scheduled reboot configuration with random execution time <pre>action soft-reboot random RANDOM-TIME</pre> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>RANDOM-TIME</td> <td> <p>Sets the random execution wait time from the task execution time until the action is executed.</p> <p>For example, if 60 seconds is set, the action will be executed after a random time in the range of 0-59 seconds.</p> <ul style="list-style-type: none"> The setting range is 60 to 86400 (seconds). Required setting. </td> </tr> </tbody> </table> <ul style="list-style-type: none"> Reboot settings based on elapsed startup time <pre>action soft-reboot uptime UPTIME</pre> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>UPTIME</td> <td> <p>Sets the startup elapsed time to determine the execution of an action when a task is executed.</p> <ul style="list-style-type: none"> The setting range is 3600 to 604800 (seconds). Required setting. </td> </tr> </tbody> </table> <p> The random and uptime options are supported by firmware V1.11.0 or later.</p>	Setting	Contents	RANDOM-TIME	<p>Sets the random execution wait time from the task execution time until the action is executed.</p> <p>For example, if 60 seconds is set, the action will be executed after a random time in the range of 0-59 seconds.</p> <ul style="list-style-type: none"> The setting range is 60 to 86400 (seconds). Required setting. 	Setting	Contents	UPTIME	<p>Sets the startup elapsed time to determine the execution of an action when a task is executed.</p> <ul style="list-style-type: none"> The setting range is 3600 to 604800 (seconds). Required setting.
Setting	Contents								
RANDOM-TIME	<p>Sets the random execution wait time from the task execution time until the action is executed.</p> <p>For example, if 60 seconds is set, the action will be executed after a random time in the range of 0-59 seconds.</p> <ul style="list-style-type: none"> The setting range is 60 to 86400 (seconds). Required setting. 								
Setting	Contents								
UPTIME	<p>Sets the startup elapsed time to determine the execution of an action when a task is executed.</p> <ul style="list-style-type: none"> The setting range is 3600 to 604800 (seconds). Required setting. 								

Command	Contents										
action hard-reboot	<p>Set action to hardware reboot.</p> <p>If the schedule type is general-control, the following settings are available</p> <ul style="list-style-type: none"> Scheduled reboot configuration with random execution time <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> action hard-reboot random <i>RANDOM-TIME</i> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>RANDOM-TIME</td> <td> <p>Sets the random execution wait time from the task execution time until the action is executed.</p> <p>For example, if 60 seconds is set, the action will be executed after a random time in the range of 0-59 seconds.</p> <ul style="list-style-type: none"> The setting range is 60 to 86400 (seconds). Required setting. </td> </tr> </tbody> </table> <ul style="list-style-type: none"> Reboot settings based on elapsed startup time <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> action hard-reboot uptime <i>UPTIME</i> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>UPTIME</td> <td> <p>Sets the startup elapsed time to determine the execution of an action when a task is executed.</p> <ul style="list-style-type: none"> The setting range is 3600 to 604800 (seconds). Required setting. </td> </tr> </tbody> </table> <div style="margin-top: 10px;"> The random and uptime options are supported by firmware V1.11.0 or later. </div>	Setting	Contents	RANDOM-TIME	<p>Sets the random execution wait time from the task execution time until the action is executed.</p> <p>For example, if 60 seconds is set, the action will be executed after a random time in the range of 0-59 seconds.</p> <ul style="list-style-type: none"> The setting range is 60 to 86400 (seconds). Required setting. 	Setting	Contents	UPTIME	<p>Sets the startup elapsed time to determine the execution of an action when a task is executed.</p> <ul style="list-style-type: none"> The setting range is 3600 to 604800 (seconds). Required setting. 		
Setting	Contents										
RANDOM-TIME	<p>Sets the random execution wait time from the task execution time until the action is executed.</p> <p>For example, if 60 seconds is set, the action will be executed after a random time in the range of 0-59 seconds.</p> <ul style="list-style-type: none"> The setting range is 60 to 86400 (seconds). Required setting. 										
Setting	Contents										
UPTIME	<p>Sets the startup elapsed time to determine the execution of an action when a task is executed.</p> <ul style="list-style-type: none"> The setting range is 3600 to 604800 (seconds). Required setting. 										
action poe-reset-supply	<p>Set action to poe feed reset.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>POE-IFNAME</td> <td>Specifies the name of the poe interface.</td> </tr> <tr> <td>down-time TIME</td> <td>Specify the time to stop poe power supply in TIME.</td> </tr> </tbody> </table>	Setting	Contents	POE-IFNAME	Specifies the name of the poe interface.	down-time TIME	Specify the time to stop poe power supply in TIME.				
Setting	Contents										
POE-IFNAME	Specifies the name of the poe interface.										
down-time TIME	Specify the time to stop poe power supply in TIME.										
action disconnect ppp	Set action to ppp communication disconnection.										
action disconnect ECM	<p>Set action to disconnect mobile module communication.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ECM</td> <td>Specify the mobile module name. Compact Router is "rmnet_data", Other devices will be "ecm".</td> </tr> <tr> <td>ECM-IFNAME</td> <td>Specify the mobile interface name.</td> </tr> <tr> <td>reset enable</td> <td>Reconnects the mobile module when it is disconnected.</td> </tr> <tr> <td>reset disable</td> <td>When the mobile module disconnects, it does not reconnect.</td> </tr> </tbody> </table> <div style="margin-top: 10px;"> Do not set up on devices that do not have a mobile module. </div> <div style="margin-top: 5px;"> The Compact Router has no settings for resetting the mobile module: for keep-alive, it reconnects after disconnection (fixed reset enable); for general-control, it does not reconnect after disconnection (fixed reset disable). </div>	Setting	Contents	ECM	Specify the mobile module name. Compact Router is "rmnet_data", Other devices will be "ecm".	ECM-IFNAME	Specify the mobile interface name.	reset enable	Reconnects the mobile module when it is disconnected.	reset disable	When the mobile module disconnects, it does not reconnect.
Setting	Contents										
ECM	Specify the mobile module name. Compact Router is "rmnet_data", Other devices will be "ecm".										
ECM-IFNAME	Specify the mobile interface name.										
reset enable	Reconnects the mobile module when it is disconnected.										
reset disable	When the mobile module disconnects, it does not reconnect.										

Command	Contents								
action disconnect ipsec	Specify the IPsec connection name in IPSEC-NAME and set the action to IPsec communication disconnection.								
action wifi ap	<p>Set Action to Reset Wireless LAN Access Point Function.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>AP-IFNAME</td> <td>Specifies the interface name of the wireless LAN access point.</td> </tr> <tr> <td>reset enable</td> <td>Reset the wireless LAN chip.</td> </tr> <tr> <td>reset disable</td> <td>Does not reset the wireless LAN chip.</td> </tr> </tbody> </table> <ul style="list-style-type: none">  This feature is only available on Compact Router with wireless LAN.  When resetting the wireless LAN chip, communication will be temporarily unavailable for the non-target wireless LAN interface as well. 	Setting	Contents	AP-IFNAME	Specifies the interface name of the wireless LAN access point.	reset enable	Reset the wireless LAN chip.	reset disable	Does not reset the wireless LAN chip.
Setting	Contents								
AP-IFNAME	Specifies the interface name of the wireless LAN access point.								
reset enable	Reset the wireless LAN chip.								
reset disable	Does not reset the wireless LAN chip.								
action wifi sta	<p>Set Action to Reset Wireless LAN Station Function.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>STA-IFNAME</td> <td>Specify the interface name of the wireless LAN station.</td> </tr> <tr> <td>reset enable</td> <td>Reset the wireless LAN chip.</td> </tr> <tr> <td>reset disable</td> <td>Does not reset the wireless LAN chip.</td> </tr> </tbody> </table> <ul style="list-style-type: none">  This feature is only available on Compact Router with wireless LAN.  When resetting the wireless LAN chip, communication will be temporarily unavailable for the non-target wireless LAN interface as well. 	Setting	Contents	STA-IFNAME	Specify the interface name of the wireless LAN station.	reset enable	Reset the wireless LAN chip.	reset disable	Does not reset the wireless LAN chip.
Setting	Contents								
STA-IFNAME	Specify the interface name of the wireless LAN station.								
reset enable	Reset the wireless LAN chip.								
reset disable	Does not reset the wireless LAN chip.								
ping dest	<p>Specifies the IP address of the host to which ping requests are sent.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>DESTINATION</td> <td> <p>Specifies the IP address of the host to which ping requests are sent.</p> <ul style="list-style-type: none"> Up to 8 destination hosts can be registered. </td> </tr> </tbody> </table>	Setting	Contents	DESTINATION	<p>Specifies the IP address of the host to which ping requests are sent.</p> <ul style="list-style-type: none"> Up to 8 destination hosts can be registered. 				
Setting	Contents								
DESTINATION	<p>Specifies the IP address of the host to which ping requests are sent.</p> <ul style="list-style-type: none"> Up to 8 destination hosts can be registered. 								
no ping dest	Deletes the IP address of the destination of the ping request.								
ping source	<p>Specifies the IP address from which ping requests are sent.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SOURCE.</td> <td>Specifies the IP address of the source host of the ping request.</td> </tr> </tbody> </table>	Setting	Contents	SOURCE.	Specifies the IP address of the source host of the ping request.				
Setting	Contents								
SOURCE.	Specifies the IP address of the source host of the ping request.								
no ping source	Deletes the IP address from which ping requests are sent.								
ping interval	<p>Specifies the interval at which ping requests are sent.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>INTERVAL</td> <td> <p>Specifies the interval (in seconds) between ping requests.</p> <ul style="list-style-type: none"> The setting range is 1 to 60 (seconds). The default value is 3 seconds. </td> </tr> </tbody> </table>	Setting	Contents	INTERVAL	<p>Specifies the interval (in seconds) between ping requests.</p> <ul style="list-style-type: none"> The setting range is 1 to 60 (seconds). The default value is 3 seconds. 				
Setting	Contents								
INTERVAL	<p>Specifies the interval (in seconds) between ping requests.</p> <ul style="list-style-type: none"> The setting range is 1 to 60 (seconds). The default value is 3 seconds. 								
ping count	<p>Specifies the maximum number of ping requests to be sent.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>COUNT</td> <td> <p>Specifies the maximum number of ping requests to be sent.</p> <ul style="list-style-type: none"> The setting range is 1 to 255. The default value is 3. </td> </tr> </tbody> </table>	Setting	Contents	COUNT	<p>Specifies the maximum number of ping requests to be sent.</p> <ul style="list-style-type: none"> The setting range is 1 to 255. The default value is 3. 				
Setting	Contents								
COUNT	<p>Specifies the maximum number of ping requests to be sent.</p> <ul style="list-style-type: none"> The setting range is 1 to 255. The default value is 3. 								

Command	Contents				
ping deadline	<p>Specify the maximum execution time per schedule for the ping request function. (Optional setting).</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>DEADLINE</td> <td> <p>Specifies the maximum execution time (in seconds) for a ping request.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 3600 (seconds). </td> </tr> </tbody> </table> <p> When either the maximum execution time or the maximum number of ping requests (ping count) for the ping request function in this setting is achieved, the action of the task set in action is executed.</p>	Setting	Contents	DEADLINE	<p>Specifies the maximum execution time (in seconds) for a ping request.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 3600 (seconds).
Setting	Contents				
DEADLINE	<p>Specifies the maximum execution time (in seconds) for a ping request.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 3600 (seconds). 				
no ping deadline	Deletes the ping maximum execution time. Deleting will not limit the maximum execution time.				
ping timeout	<p>Sets the timeout duration for ping requests.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>TIMEOUT</td> <td> <p>Sets the timeout period (in seconds) for ping requests.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 600 (seconds). ● The default value is 10 seconds. </td> </tr> </tbody> </table>	Setting	Contents	TIMEOUT	<p>Sets the timeout period (in seconds) for ping requests.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 600 (seconds). ● The default value is 10 seconds.
Setting	Contents				
TIMEOUT	<p>Sets the timeout period (in seconds) for ping requests.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 600 (seconds). ● The default value is 10 seconds. 				
ping delay	<p>Sets the maximum time to wait for a random time before executing ping transmission.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MAX-DELAY</td> <td> <p>Sets the maximum time to wait for a random time before executing ping transmission.</p> <ul style="list-style-type: none"> ● The setting range is 0 to 3600 (seconds). ● The default value is 0 seconds. </td> </tr> </tbody> </table>	Setting	Contents	MAX-DELAY	<p>Sets the maximum time to wait for a random time before executing ping transmission.</p> <ul style="list-style-type: none"> ● The setting range is 0 to 3600 (seconds). ● The default value is 0 seconds.
Setting	Contents				
MAX-DELAY	<p>Sets the maximum time to wait for a random time before executing ping transmission.</p> <ul style="list-style-type: none"> ● The setting range is 0 to 3600 (seconds). ● The default value is 0 seconds. 				
ping wait	<p>Sets the random wait time when switching ping destinations.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MAX-WAIT</td> <td> <p>Sets the random wait time when switching ping destinations.</p> <ul style="list-style-type: none"> ● The setting range is 0 to 60 (seconds). ● The default value is 3 seconds. </td> </tr> </tbody> </table>	Setting	Contents	MAX-WAIT	<p>Sets the random wait time when switching ping destinations.</p> <ul style="list-style-type: none"> ● The setting range is 0 to 60 (seconds). ● The default value is 3 seconds.
Setting	Contents				
MAX-WAIT	<p>Sets the random wait time when switching ping destinations.</p> <ul style="list-style-type: none"> ● The setting range is 0 to 60 (seconds). ● The default value is 3 seconds. 				
failsafe reboot	<p>Sets the maximum number of soft-reboot or hard-reboot reboots to execute when the number of retries (3) is exceeded in the fail-safe function.</p> <ul style="list-style-type: none"> ● If the schedule type is general-control and the action is soft-reboot or hard-reboot ● If the schedule type is keep-alive and the action is soft-reboot or hard-reboot or disconnect ecm <p>Depending on whether it is enabled or disabled, set it in the following format.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>COUNT</td> <td> <p>Set the maximum number of reboots.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 10. ● The default value is 3. </td> </tr> </tbody> </table> <p>➔ For more information on fail-safe features, see " 12.3 fail-safe " for more information on the fail-safe feature.</p>	Setting	Contents	COUNT	<p>Set the maximum number of reboots.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 10. ● The default value is 3.
Setting	Contents				
COUNT	<p>Set the maximum number of reboots.</p> <ul style="list-style-type: none"> ● The setting range is 1 to 10. ● The default value is 3. 				
no failsafe	If the action is soft-reboot or hard-reboot, the failsafe function is deactivated.				
command	Specify the command to be executed in COMMAND.				
exit	Exit the schedule detail setting mode and enter the setting mode.				
no schedule keep-alive no schedule general-control no schedule user-define	Delete the schedule by specifying the task name in TASKNAME.				

Limitations on the number of registrations for certain action settings

For the following actions related to the [fail-safe](#) function, the maximum number of registrations is

32. Please note the number of registrations.

Action	Contents	Schedule Type
soft-reboot	software reboot	<ul style="list-style-type: none"> ● keep-alive ● general-control
hard-reboot	hardware reboot	<ul style="list-style-type: none"> ● keep-alive ● general-control
disconnect ecm	Ecm communication disconnection	<ul style="list-style-type: none"> ● keep-alive
disconnect ppp*	PPP Disconnection	<ul style="list-style-type: none"> ● keep-alive
disconnect ipsec*	IPsec communication disconnection	<ul style="list-style-type: none"> ● keep-alive
poe-reset-supply**	PoE power supply reset	<ul style="list-style-type: none"> ● keep-alive
wifi ap wifi sta	Wireless LAN chip reset	<ul style="list-style-type: none"> ● keep-alive

*The number of registrations has been limited since V1.8.0.

Execution example 1 General setup example

Execute the **schedule** command with one of the following schedule types: keep-alive, general-control, or user-define.

The settings made here are written to a configuration file.

設定モード

① When the schedule type is keep-alive

Example of restarting the ecm mobile module when disconnection is detected by checking ecm communication every 10 minutes

```
amnimo(cfg)# schedule keep-alive mobile ← Set task with schedule type keep-alive
amnimo(cfg-sch-ka-mobile)# datetime */10 * * * * ←
amnimo(cfg-sch-ka-mobile)# action disconnect ecm ecm0 reset enable ←
amnimo(cfg-sch-ka-mobile)# ping dest example.com ←
amnimo(cfg-sch-ka-mobile)# enable ←
amnimo(cfg-sch-ka-mobile)# exit ←
```

② When the schedule type is "general-control

Example of a cold reboot of an Edge Gateway at 4:00 AM on December 31

```
amnimo(cfg)# schedule general-control reboot ← Set task with schedule type general-control
amnimo(cfg-sch-gc-reboot)# datetime 0 4 31 12 * ←
amnimo(cfg-sch-gc-reboot)# action hard-reboot ←
amnimo(cfg-sch-gc-reboot)# enable ←
amnimo(cfg-sch-gc-reboot)# exit ←
```

③ When the schedule type is "user-define

Example of issuing a ping command to an arbitrary IP address every hour at 0:00

```
amnimo(cfg)# schedule user-define userping ← Set task with schedule type user-define
amnimo(cfg-sch-ud-userping)# datetime 0 * * * * ←
amnimo(cfg-sch-ud-userping)# command ping 192.168.2.110 ←
amnimo(cfg-sch-ud-userping)# enable ←
amnimo(cfg-sch-ud-userping)# exit ←
```

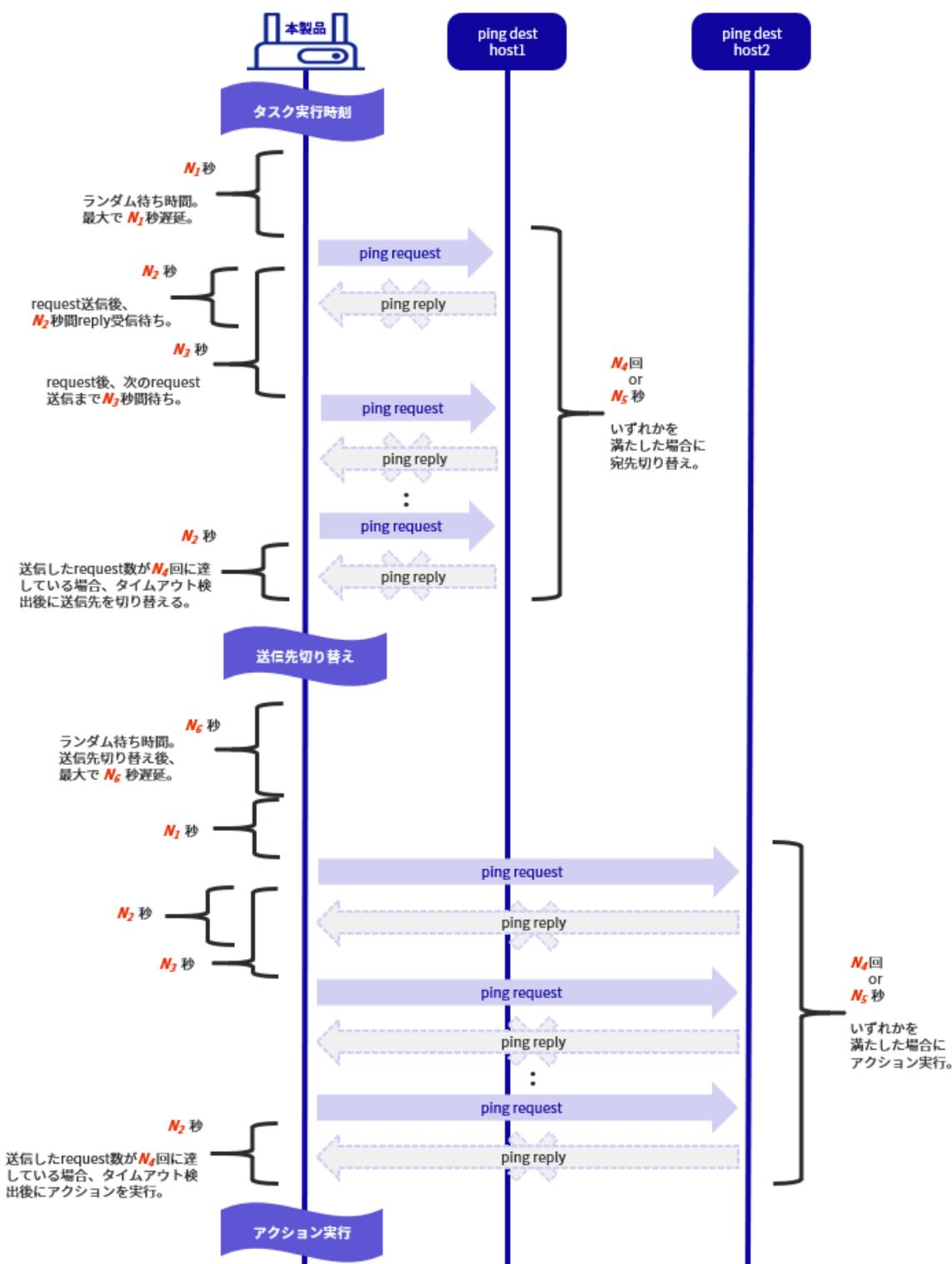


Do not use a public IP address as the destination host for pings to monitor the network connection status, as this can lead to network problems on the destination server side. It is recommended that you prepare your own connection destination separately.

Execution example 2 Specifying multiple destination hosts for ping requests

When "keep-alive" is selected as the schedule type, multiple destination hosts for ping requests can be specified.

The figure below shows an example of operation up to the execution of an action when two destination hosts (host1, host2) are set and the relationship between each setting item.



Item	Supported commands	Contents	Unit	Default value
N ₁	ping delay	Maximum time of random waiting time before ping transmission is executed	seconds	0

Item	Supported commands	Contents	Unit	Default value
N ₂	ping timeout	Timeout duration of ping request	seconds	10
N ₃	ping interval	Interval for sending ping requests	seconds	3
N ₄	ping count	Maximum number of ping requests to send	times	3
N ₅	ping deadline	Maximum execution time per schedule for the ping request function	seconds	no designation
N ₆	ping wait	Random waiting time when switching ping destinations	seconds	3

設定モード

```

amnimo(cfg)# schedule keep-alive TASKNAME ← Specify any task name
amnimo(cfg-sch-ka-TASKNAME)# datetime DATETIME ← Specify any task execution time
amnimo(cfg-sch-ka-TASKNAME)# action ACTION ← Specify any action
amnimo(cfg-sch-ka-TASKNAME)# ping dest host1 ← Specify host1 as the destination host*
amnimo(cfg-sch-ka-TASKNAME)# ping dest host2 ← Specify host2 as the destination host*
amnimo(cfg-sch-ka-TASKNAME)# ping delay N 1 ←
amnimo(cfg-sch-ka-TASKNAME)# ping timeout N 2 ←
amnimo(cfg-sch-ka-TASKNAME)# ping interval N 3 ←
amnimo(cfg-sch-ka-TASKNAME)# ping count N 4 ←
amnimo(cfg-sch-ka-TASKNAME)# ping deadline N 5 ←
amnimo(cfg-sch-ka-TASKNAME)# ping wait N 6 ←
amnimo(cfg-sch-ka-TASKNAME)# enable ←
amnimo(cfg-sch-ka-TASKNAME)# exit ←

```

※ If multiple destination hosts are registered, the order in which pings are sent to each destination host is randomized.

設定モード

- ① Example of hardware reboot of the Edge Gateway at 3:00 AM daily with a maximum random runtime of 1 hour

```
amnimo(cfg)# schedule general-control randreboot↵ ← Set task with schedule type g
eneral-control
amnimo(cfg-sch-gc-randreboot)# datetime 0 3 * * * ↵ ← Set 3:00 AM daily
amnimo(cfg-sch-gc-randreboot)# action hard-reboot random 3600↵ ← Set hardware reboot, r
andom execution time 3600 seconds (0-3599 seconds execution wait time)
amnimo(cfg-sch-gc-randreboot)# no failsafe↵ ← Disable failsafe and reboot per
manently if it fails.
amnimo(cfg-sch-gc-randreboot)# enable↵ ← Enable this schedule setting.
amnimo(cfg-sch-gc-randreboot)# exit ↵
```

- ② Example of software reboot of an Edge Gateway if 24 hours have passed since startup

```
amnimo(cfg)# schedule general-control uptimereboot↵ ← Set task with schedule type g
eneral-control
amnimo(cfg-sch-gc-uptimereboot)# datetime */5 * * * *↵ ← Set to check boot time elapse
d every 5 minutes
amnimo(cfg-sch-gc-uptimereboot)# action soft-reboot uptime 86400↵ ← Set software r
eboot at 86400 seconds (24 hours) after boot
amnimo(cfg-sch-gc-uptimereboot)# no failsafe↵ ← Disable failsafe and reboot per
manently if it fails.
amnimo(cfg-sch-gc-uptimereboot)# enable↵ ← Enable this schedule setting.
amnimo(cfg-sch-gc-uptimereboot)# exit ↵
```



The random and uptime options are supported by firmware V1.11.0 or later.

7.8 Manage system logs.

Displays Syslog messages, displays Syslog settings, and configures Syslog settings. It also displays amlog messages, which are logs of this product.

7.8.1 Display Syslog messages



To view Syslog messages, run the *show syslog message* command.

Format

```
show syslog message [follow] [lines NUMBER].
```

Setting items

Item	Contents
follow	If follow is specified, Syslog output is monitored and logged continuously. To stop logging, enter "CTRL" + "C" keys.
lines	Specify the number of log lines to be output in NUMBER. If omitted, the latest log is issued for 10 lines.

Output Format

```
SYSLOG  
(Omitted.)
```

Output item

Item	Contents
SYSLOG	The log is displayed.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード
設定 モード

```

amnimo# show syslog message↵
2020-08-07T08:02:01.253126+00:00 test 1
2020-08-07T08:02:01.255466+00:00 test 2
2020-08-07T08:02:01.295917+00:00 test 3
2020-08-07T08:02:32.883885+00:00 test 4
2020-08-07T08:02:32.886249+00:00 test 2
2020-08-07T08:02:32.918905+00:00 test 5
2020-08-07T08:02:32.928120+00:00 test 3
2020-08-07T08:02:32.964404+00:00 test 6
2020-08-07T08:02:32.971292+00:00 test 7
2020-08-07T08:02:32.971713+00:00 test 8
amnimo# show syslog message lines 15 ↵
2020-08-07T08:01:47.799239+00:00 test 2
2020-08-07T08:01:47.836894+00:00 test 3
2020-08-07T08:01:59.699354+00:00 test 1
2020-08-07T08:01:59.701602+00:00 test 2
2020-08-07T08:01:59.742651+00:00 test 3
2020-08-07T08:02:01.253126+00:00 test 1
2020-08-07T08:02:01.255466+00:00 test 2
2020-08-07T08:02:01.295917+00:00 test 3
2020-08-07T08:02:32.883885+00:00 test 4

```

← If lines and follow are not specified
← A message of ←10 lines are displayed

← When specified with ←lines 15
← A message of ←15 lines are displayed

```
2020-08-07T08:02:32.886249+00:00 test 2
2020-08-07T08:02:32.918905+00:00 test 5
2020-08-07T08:02:32.928120+00:00 test 3
2020-08-07T08:02:32.964404+00:00 test 6
2020-08-07T08:02:32.971292+00:00 test 7
2020-08-07T08:02:32.971713+00:00 test 8
amnimo# show syslog message follow ↵
2020-08-07T08:02:01.253126+00:00 test 1
2020-08-07T08:02:01.255466+00:00 test 2
2020-08-07T08:02:01.295917+00:00 test 3
2020-08-07T08:02:32.883885+00:00 test 4
2020-08-07T08:02:32.886249+00:00 test 2
2020-08-07T08:02:32.918905+00:00 test 5
2020-08-07T08:02:32.928120+00:00 test 3
2020-08-07T08:02:32.964404+00:00 test 6
2020-08-07T08:02:32.971292+00:00 test 7
2020-08-07T08:02:32.971713+00:00 test 8
Enter "Ctrl" + "C" key to exit
```

← If follow is specified

7.8.2 Display Syslog settings



To view the Syslog configuration, run the *show config syslog* command.

Format

```
show config syslog [local | remote].
```

Setting items

Item	Contents
local remote	<p>Running with "local" or "remote" allows you to view the settings for local log output or remote log forwarding separately. If omitted, both settings will be displayed.</p> <p> The "Tab" key can be used to complete the input of "local" or "remote".</p>

Output Format

```
# --- transition to configure mode ---
configure
# --- syslog local configure ---
syslog local
ENABLE
rotate-size ROTATE-SIZE
rotate-count ROTATE-COUNT
level LEVEL
exit
# --- syslog remote configure ---
syslog remote
ENABLE
SERVER-ADDRESS
server-port SERVER-PORT
level LEVEL
exit
# --- exit configure mode ---
exit
```

Output item

Item	Contents						
ENABLE	<p>Displays information on when local log output or remote log forwarding is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
ROTATE-SIZE	The threshold size for log rotation is displayed.						
ROTATE-COUNT	The number of generations of log rotation is displayed.						
LEVEL	The log output level is displayed.						
SERVER-ADDRESS	The IP address of the remote log forwarding destination is displayed in the format "server-address { IP address}". If the IP address of the remote log forwarding destination is not set, it will not be displayed.						
SERVER-PORT	Displays the port number to which remote logs are forwarded.						

Execution example

Below is an example of running in administrator mode and configuration mode.

管理者モード

```
amnimo# show config syslog ↵
# ---- transition to configure mode. ----
configure
# ---- syslog local configure. ----
syslog local
enable
rotate-size 10240
rotate-count 8
level informational
exit
# ---- syslog remote configure. ----
syslog remote
enable
server-address 192.168.0.11
server-port 514
level informational
exit
# ---- exit configure mode. ----
exit
amnimo# show config syslog local ↵
# ---- transition to configure mode. ----
configure
# ---- syslog local configure. ----
syslog local
enable
rotate-size 10240
rotate-count 8
level informational
exit
# ---- exit configure mode. ----
exit
amnimo# show config syslog remote ↵
# ---- transition to configure mode. ----
configure
# ---- syslog remote configure. ----
syslog remote
enable
server-address 192.168.0.11
server-port 514
level informational
exit
# ---- exit configure mode. ----
exit
```

設定モード

```
amnimo(cfg)# show config syslog ↵
# ---- syslog local configure. ----
syslog local
enable
rotate-size 10240
rotate-count 8
level informational
exit
```

```

# ---- syslog remote configure. ----
syslog remote
enable
server-address 192.168.0.11
server-port 514
level informational
exit
amnimo(cfg)# show config syslog local ↵
# ---- syslog local configure. ----
syslog local
enable
rotate-size 10240
rotate-count 8
level informational
exit
amnimo(cfg)# show config syslog remote ↵
# ---- syslog remote configure. ----
syslog remote
enable
server-address 192.168.0.11
server-port 514
level informational
exit

```



Running the *show config* command in the advanced configuration mode of Syslog will display the same information as in the configuration mode.

```

amnimo(cfg)# syslog local ↵           ← Go to Syslog advanced configuration mode
amnimo(cfg-syslog-local)# show config ↵
enable                               ← Same as setting mode
(Omitted.)

```

7.8.3 Configure Syslog settings.



To configure Syslog, go to advanced configuration mode and execute the configuration command. Execute the **syslog** command with "local" or "remote" to enter the respective advanced configuration mode.

The settings made here are written to a configuration file.

Format

```
To configure local log output
syslog local
enable
no enable
rotate-size SIZE
rotate-count COUNT
level <emergencies | alerts | critical | errors | warnings | notifications | informational | debugging>.
exit

To set up remote log forwarding
syslog remote
enable
no enable
server-address IPADDRESS
server-port PORT
level <emergencies | alerts | critical | errors | warnings | notifications | informational | debugging>.
exit
```

Command

Command	Contents
syslog local	Execute the local log output configuration command.  Executing the command in the configuration mode will enter the local log detail configuration mode.
syslog remote	Execute the remote log forwarding configuration command.  Executing the command in the configuration mode will enter the remote log detail configuration mode.
enable	Start the service. In the local advanced setting mode, local log output is enabled. Remote log forwarding is enabled in the REMOTE advanced setting mode.
no enable	Stop the service. In the local advanced setting mode, local log output is disabled. Remote log forwarding is disabled in the remote advanced setting mode.
rotate-size	Specifies the threshold size for local log rotation. <ul style="list-style-type: none"> ● Edge Gateways, IoT Routers Range: 512 to 10240 (default: 10240) ● Compact Router Range: 512 to 2048 (default: 2048)
rotate-count	Specifies the number of generations for local log rotation in the range of 1-8. The default setting is "8".
level	localln advanced configuration mode, specifies the output level of the local log. In remote advanced setting mode, specify the remote log output level.
server-address	Specifies the IP address of the remote log forwarding destination.

Command	Contents
server-port	Specifies the port number of the remote log forwarding destination in the range of 1 to 65535. The default setting is "514".
exit	Exit the detailed setting mode and enter the setting mode.

Execution example

Execute the **syslog** command with "local" or "remote". The settings made here will be written to the configuration file.

設定モード

```

amnimo(cfg)# syslog local ← Set local log output
amnimo(cfg-syslog-local)# rotate-size 10240 ←
amnimo(cfg-syslog-local)# rotate-count 8 ←
amnimo(cfg-syslog-local)# level informational ←
amnimo(cfg-syslog-local)# enable ←
amnimo(cfg-syslog-local)# exit ←
amnimo(cfg)# syslog remote ← Set remote log forwarding
amnimo(cfg-syslog-remote)# server-address 192.168.0.11 ←
amnimo(cfg-syslog-remote)# server-port 514 ←
amnimo(cfg-syslog-remote)# level informational ←
amnimo(cfg-syslog-remote)# enable ←
amnimo(cfg-syslog-remote)# exit ←
amnimo(cfg)# exit

```

7.8.4 Display amlog message



The **amlog** command allows you to specify the log level and extract and display a specified number of lines from the most recent log.



This function is not available on Compact Router.

Format

```

show amlog [level <emergencies | alerts | critical | errors | warnings | notifications
| informational | debugging>] [tail [TAIL_LINENUM]]

```

Setting items

Item	Contents																		
level	<p>Specify the log level as a number in LOG_LEVEL. Logs below the log level specified here will be displayed. By default, "informational" is set.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>emergencies</td> <td>LOG_EMERG. log indicating system instability.</td> </tr> <tr> <td>alerts</td> <td>LOG_ALERT, a level of logging that requires immediate action.</td> </tr> <tr> <td>critical</td> <td>LOG_CRIT. log indicating a fatal error.</td> </tr> <tr> <td>errors</td> <td>LOG_ERR. error log.</td> </tr> <tr> <td>warnings</td> <td>LOG_WARNING. warning log.</td> </tr> <tr> <td>notifications</td> <td>LOG_NOTICE, a log that normally occurs but has important information.</td> </tr> <tr> <td>informational</td> <td>LOG_INFO. information log.</td> </tr> <tr> <td>debugging</td> <td>LOG_DEBUG. debug level log.</td> </tr> </tbody> </table>	Setting	Contents	emergencies	LOG_EMERG. log indicating system instability.	alerts	LOG_ALERT, a level of logging that requires immediate action.	critical	LOG_CRIT. log indicating a fatal error.	errors	LOG_ERR. error log.	warnings	LOG_WARNING. warning log.	notifications	LOG_NOTICE, a log that normally occurs but has important information.	informational	LOG_INFO. information log.	debugging	LOG_DEBUG. debug level log.
Setting	Contents																		
emergencies	LOG_EMERG. log indicating system instability.																		
alerts	LOG_ALERT, a level of logging that requires immediate action.																		
critical	LOG_CRIT. log indicating a fatal error.																		
errors	LOG_ERR. error log.																		
warnings	LOG_WARNING. warning log.																		
notifications	LOG_NOTICE, a log that normally occurs but has important information.																		
informational	LOG_INFO. information log.																		
debugging	LOG_DEBUG. debug level log.																		
tail	<p>Specify in TAIL_LINENUM the number of lines of the latest log you wish to display.</p>  <ul style="list-style-type: none"> ● If tail is omitted, all lines are output. ● If TAIL is specified and TAIL_LINENUM is not specified, 10 lines of the latest log are displayed. 																		

Output Format

```
YYYYY-mm-ddTHH:MM:ssZ LOG_LEVEL LOG_MESSAGE
YYYYY-mm-ddTHH:MM:ssZ LOG_LEVEL LOG_MESSAGE
YYYYY-mm-ddTHH:MM:ssZ LOG_LEVEL LOG_MESSAGE
```

Output item

Item	Contents																		
YYYYY-mm-ddTHH:MM:ssZ	The date and time the log was generated are displayed.																		
LOG_LEVEL	<p>Log level values are displayed.</p> <table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>emergencies</td> <td>LOG_EMERG. log indicating system instability.</td> </tr> <tr> <td>alerts</td> <td>LOG_ALERT, a level of logging that requires immediate action.</td> </tr> <tr> <td>critical</td> <td>LOG_CRIT. log indicating a fatal error.</td> </tr> <tr> <td>errors</td> <td>LOG_ERR. error log.</td> </tr> <tr> <td>warnings</td> <td>LOG_WARNING. warning log.</td> </tr> <tr> <td>notifications</td> <td>LOG_NOTICE, a log that normally occurs but has important information.</td> </tr> <tr> <td>informational</td> <td>LOG_INFO. information log.</td> </tr> <tr> <td>debugging</td> <td>LOG_DEBUG. debug level log.</td> </tr> </tbody> </table>	Display	Contents	emergencies	LOG_EMERG. log indicating system instability.	alerts	LOG_ALERT, a level of logging that requires immediate action.	critical	LOG_CRIT. log indicating a fatal error.	errors	LOG_ERR. error log.	warnings	LOG_WARNING. warning log.	notifications	LOG_NOTICE, a log that normally occurs but has important information.	informational	LOG_INFO. information log.	debugging	LOG_DEBUG. debug level log.
Display	Contents																		
emergencies	LOG_EMERG. log indicating system instability.																		
alerts	LOG_ALERT, a level of logging that requires immediate action.																		
critical	LOG_CRIT. log indicating a fatal error.																		
errors	LOG_ERR. error log.																		
warnings	LOG_WARNING. warning log.																		
notifications	LOG_NOTICE, a log that normally occurs but has important information.																		
informational	LOG_INFO. information log.																		
debugging	LOG_DEBUG. debug level log.																		
LOG_MESSAGE	The contents of the log message are displayed. The maximum size is 246 bytes and can be stored in minutes.																		

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

管理者 モード 設定 モード

```
amnimo$ show amlog level informational tail 5 ↵
2020-07-20T10:21:48+0900 LOG_INFO U-Boot 2018.03-devel-18.12.3--g5007f1d952 (Jul 02 20
20 - 22:39:06 +0900)
2020-07-20T10:21:48+0900 LOG_INFO STATUS:SN=[300002],MAC0=[E8:1B:4B:00:30:02],BS=[a:1
b:308 h:0 s:0],DIPBM=[ubootcommand]
2020-07-20T10:22:08+0900 LOG_INFO Start mounting to /dev/mmcblk0p4
2020-07-20T10:22:08+0900 LOG_INFO Start mounting to /dev/mmcblk0p5
2020-07-20T10:22:09+0900 LOG_INFO Update bootarea to 1
```

7.8.5 Clear amlog logs



Clear all logs.

It takes several tens of seconds for the command execution to complete.



This function is not available on Compact Router.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# amlog initialize ↵
```

7.9 Configure GUI settings



Display and configure settings to configure this product via GUI (Graphical User Interface).



For models with group setting functionality, the following group permission settings are required to use the GUI functions. (The default setting is enabled.)

```
show:device:information
```

➔ For details, see " 2.7.7 Group Permissions For various parameters of the configuration " for details.

7.9.1 Displaying GUI settings

To view the GUI configuration, run the *show config gui* command.

Format

```
show config gui
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- gui configure ----
gui
ENABLED
Protocol PROTOCOL_TYPE
port PORT_NUM
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLE	Information is displayed when GUI service activation is enabled/disabled. <table border="1"><thead><tr><th>Setting</th><th>Display</th></tr></thead><tbody><tr><td>Enable</td><td>The message "enable" is displayed.</td></tr><tr><td>Disable</td><td>The message "no enable" is displayed.</td></tr></tbody></table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
PROTOCOL_TYPE	The protocol used by the GUI service is displayed. <table border="1"><thead><tr><th>Setting</th><th>Display</th></tr></thead><tbody><tr><td>HTTP</td><td>http" is displayed.</td></tr><tr><td>HTTPS</td><td>https" will be displayed.</td></tr></tbody></table>	Setting	Display	HTTP	http" is displayed.	HTTPS	https" will be displayed.
Setting	Display						
HTTP	http" is displayed.						
HTTPS	https" will be displayed.						
PORT_NUM	Displays the port number of the protocol used by the GUI service.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード

```
amnimo# show config gui ↵
# ---- transition to configure mode ----
configure
```

```
# ---- gui configure ----  
gui  
enable  
Protocol http  
port 80  
exit  
# ---- exit configure mode ----  
exit
```

7.9.2 Configure GUI settings

To configure the GUI, enter the advanced configuration mode and execute the configuration commands.

The settings made here are written to a configuration file.

Format

```
gui
enable
no enable
protocol < http | https >
port PORT_NUM
exit
```

Command

Command	Contents						
gui	Execute GUI configuration commands.  Executing a command in the setting mode shifts to the detailed setting mode.						
enable	Start the service.						
protocol	Set the protocol to be used in the GUI. <table border="1" data-bbox="576 884 1353 1169"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>http</td> <td>Specifies the HTTP protocol.  The port number is set to 80.</td> </tr> <tr> <td>https</td> <td>Specifies the HTTPS protocol.  The port number is set to 443.</td> </tr> </tbody> </table>	Setting	Contents	http	Specifies the HTTP protocol.  The port number is set to 80.	https	Specifies the HTTPS protocol.  The port number is set to 443.
Setting	Contents						
http	Specifies the HTTP protocol.  The port number is set to 80.						
https	Specifies the HTTPS protocol.  The port number is set to 443.						
port	Specify the port number of the GUI in the range of 1 to 65535 for PORT_NO.						
no enable	Stop the service.						
exit	Exit the GUI's advanced setting mode and enter the setting mode.						

Execution example

設定モード

```
amnimo(cfg)# gui ↵
amnimo(cfg-gui)# enable ↵
amnimo(cfg-gui)# protocol http ↵
amnimo(cfg-gui)# port 80 ↵
amnimo(cfg-gui)# exit ↵
```

7.10 Configure DHCP relay settings



Display and configure settings for using DHCP Relay service with this product.



DHCP Server (7.6 Configure DHCP server settings) is enabled, this DHCP Relay setting cannot be enabled.

7.10.1 Display DHCP relay settings

To view the DHCP relay configuration, run the *show config dhcp-relay* command.

Format

```
show config dhcp-relay [GROUP].
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- dhcp-relay GROUP configure ----
dhcp-relay GROUP
ENABLE
LISTEN
SERVER
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
GROUP	<p>The DHCP relay group name is displayed.</p>  <ul style="list-style-type: none"> If you omit the group name, the settings for all applicable DHCP relay groups will be displayed. Entering the "Tab" key completes the group name entry. 						
ENABLE	<p>Information is displayed when DHCP Relay service activation is enabled/disabled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
LISTEN	<p>The interface on which the DHCP Relay service listens for DHCP requests is displayed in the following format.</p> <pre>listen LISTEN_IFNAME</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>LISTEN_IFNAME</td> <td> <p>The interface listening for DHCP requests is displayed.</p> <ul style="list-style-type: none"> Edge Gateway eth0, br<0-9>, tun<0-9>, tap<0-9> IoT Router eth<0-1>, br<0-9>, tun<0-9>, tap<0-9> Compact Router eth0 </td> </tr> </tbody> </table>  <p>More than one may be displayed.</p>	Setting items	Contents	LISTEN_IFNAME	<p>The interface listening for DHCP requests is displayed.</p> <ul style="list-style-type: none"> Edge Gateway eth0, br<0-9>, tun<0-9>, tap<0-9> IoT Router eth<0-1>, br<0-9>, tun<0-9>, tap<0-9> Compact Router eth0 		
Setting items	Contents						
LISTEN_IFNAME	<p>The interface listening for DHCP requests is displayed.</p> <ul style="list-style-type: none"> Edge Gateway eth0, br<0-9>, tun<0-9>, tap<0-9> IoT Router eth<0-1>, br<0-9>, tun<0-9>, tap<0-9> Compact Router eth0 						

Item	Contents				
SERVER	The IP address of the relay destination DHCP server is displayed in the following format. <div style="background-color: #e0e0e0; padding: 5px; margin: 5px 0;">server ADDRESS</div> <table border="1" style="width: 100%; margin: 5px 0;"> <thead> <tr> <th>Item</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ADDRESS</td> <td>The DHCP server address is displayed.</td> </tr> </tbody> </table> <div style="display: flex; align-items: center; margin-top: 5px;"> More than one may be displayed. </div>	Item	Contents	ADDRESS	The DHCP server address is displayed.
Item	Contents				
ADDRESS	The DHCP server address is displayed.				

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# show config dhcp-relay ↵
# ---- dhcp-relay networkA configure ----
dhcp-relay networkA
enable
listen eth0
listen tun0
server 10.0.0.1
server 10.0.0.2
server 10.0.0.3
server 10.0.0.4
exit
# ---- Exit configure mode ----
# ---- dhcp-relay networkB configure ----
dhcp-relay networkB
no enable
listen tun1
server 172.16.0.1
exit
# ---- Exit configure mode ----
```

7.10.2 Configure DHCP relay settings

To configure the DHCP relay, enter the advanced configuration mode and execute the configuration commands.

The settings made here are written to a configuration file.

Format

```
dhcp-relay GROUP
enable
no enable
listen LISTEN_IFNAME
no listen LISTEN_IFNAME
server ADDRESS
no server ADDRESS
exit
no dhcp-relay GROUP
```

Command

Command	Contents				
dhcp-relay	Execute the command to configure DHCP relay, specifying the group name in GROUP.  Executing a command in the setting mode shifts to the detailed setting mode.				
enable	Enable DHCP Relay service.				
no enable	Disables the DHCP relay service.				
listen	The interface on which the DHCP Relay service listens for DHCP requests is configured in the following format. <pre>listen LISTEN_IFNAME</pre> <table border="1" data-bbox="411 1205 1353 1563"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>LISTEN_IFNAME</td> <td>Set the interface to listen for DHCP requests. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, br<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, br<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, tun<0-9>, tap<0-9> ● Compact Router eth0 </td> </tr> </tbody> </table>  <ul style="list-style-type: none"> ● Multiple interfaces can be configured. ● If not set, all configurable interfaces are covered. 	Setting items	Contents	LISTEN_IFNAME	Set the interface to listen for DHCP requests. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, br<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, br<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, tun<0-9>, tap<0-9> ● Compact Router eth0
Setting items	Contents				
LISTEN_IFNAME	Set the interface to listen for DHCP requests. <ul style="list-style-type: none"> ● AI Edge Gateway wan0, br<0-9>, tun<0-9>, tap<0-9> ● Edge Gateway eth0, br<0-9>, tun<0-9>, tap<0-9> ● IoT Router eth<0-1>, br<0-9>, tun<0-9>, tap<0-9> ● Compact Router eth0 				
no listen	Deletes the configuration of the interface on which the DHCP Relay service listens for DHCP requests.				
server	Set the IP address of the relay destination DHCP server. <pre>server ADDRESS</pre> <table border="1" data-bbox="411 1845 1353 1935"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ADDRESS</td> <td>IP address of the DHCP server to relay to</td> </tr> </tbody> </table>  <ul style="list-style-type: none"> ● At least one DHCP server IP address is required. ● Multiple DHCP server IP addresses can be configured. ● Up to four settings can be made. 	Setting items	Contents	ADDRESS	IP address of the DHCP server to relay to
Setting items	Contents				
ADDRESS	IP address of the DHCP server to relay to				
no server	Delete the IP address setting of the relay destination DHCP server.				

Command	Contents
exit	Exit DHCP relay advanced setting mode and enter setting mode.
no dhcp-relay	Specify the DHCP relay group name in GROUP and delete the setting.

Execution example

The following example shows the case where eth0 is set as the interface to listen for DHCP requests and the relay destination DHCP server is 10.10.10.1.

The settings made here are written to a configuration file.

設定モード

```

amnimo(cfg)# dhcp-relay networkC ← Set the DHCP relay group as "netowrkC
amnimo(cfg-dhcp-relay-networkC)# listen eth0 ← Set listen interface to eth0
amnimo(cfg-dhcp-relay-networkC)# server 10.10.10.1 ← Set the relay destination DHCP
P server as 10.10.10.1
amnimo(cfg-dhcp-relay-networkC)# enable ← Enable DHCP relay setting.
amnimo(cfg-dhcp-relay-networkC)# exit ←
amnimo(cfg)#.

```

7.11 Setting up a proxy server



Display and configure settings for using proxy server services with this product.

7.11.1 Display proxy server settings

Format

```
show config proxy
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- proxy configure ----
proxy
ENABLED.
port PROXY_PORT
SOURCE_ADDRESS_ENABLED
SOURCE_ADDRESS_VALUE
ACL_PORT_NUMBER
ACL_SSL_NUMBER
WHITELIST_FQDN_ENABLED
WHITELIST_FQDN_VALUE
BLACKLIST_FQDN_ENABLED
BLACKLIST_FQDN_VALUE
WHITELIST_URL_ENABLED
WHITELIST_URL_VALUE
BLACKLIST_URL_ENABLED
BLACKLIST_URL_VALUE
http-access HTTP_ACCESS
AUTHENTICATION_ENABLED
authentication scheme SCHEME
authentication ttl TIMETOLIVE
authentication account USERNAME secret ENCRYPT-PASSWORD
authentication process maximum MAXIMUM
authentication process startup STARTUP
authentication process idle IDLE
CASESENSITIVE
ACCESS_LOG_ENABLED
access log facility FACILITY
access log priority PRIORITY
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLE	Displays information on when the proxy server is enabled/disabled. <table border="1" data-bbox="598 1854 1353 1984"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
PROXY_PORT	The proxy server's listening port number is displayed. The default setting is "8080".						

Item	Contents						
SOURCE_ADDRESS_ENABLED	<p>Displays the Enable/Disable setting for the connection source network control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "source address enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no source address enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "source address enable" is displayed.	Disable	The message "no source address enable" is displayed.
Setting	Display						
Enable	The message "source address enable" is displayed.						
Disable	The message "no source address enable" is displayed.						
SOURCE_ADDRESS_VALUE	<p>The connection source network address setting is displayed. It is displayed in the following format</p> <p style="background-color: #f0f0f0; padding: 5px;"><code>source address IP_ADDRESS/PREFIX</code></p> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>IP_ADDRESS/PREFIX</td> <td>Network address/prefix of connection sender</td> </tr> </tbody> </table> <p> More than one may be displayed.</p>	Setting items	Contents	IP_ADDRESS/PREFIX	Network address/prefix of connection sender		
Setting items	Contents						
IP_ADDRESS/PREFIX	Network address/prefix of connection sender						
ACL_PORT_NUMBER	<p>The destination port number settings that are allowed to be accessed via the proxy server are displayed in the following format.</p> <p style="background-color: #f0f0f0; padding: 5px;"><code>acl port port_number</code></p> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PORT_NUMBER</td> <td>connection allowed destination port number</td> </tr> </tbody> </table> <p> More than one may be displayed.</p>	Setting items	Contents	PORT_NUMBER	connection allowed destination port number		
Setting items	Contents						
PORT_NUMBER	connection allowed destination port number						
ACL_SSL_NUMBER	<p>The https destination port number settings that are allowed to access via the proxy server in the following format.</p> <p style="background-color: #f0f0f0; padding: 5px;"><code>acl ssl SSL_NUMBER</code></p> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SSL_NUMBER</td> <td>https connection allowed destination port number</td> </tr> </tbody> </table> <p> More than one may be displayed.</p>	Setting items	Contents	SSL_NUMBER	https connection allowed destination port number		
Setting items	Contents						
SSL_NUMBER	https connection allowed destination port number						
WHITELIST_FQDN_ENABLED	<p>The FQDN whitelist control enable/disable setting is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "http whitelist fqdn enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no http whitelist fqdn enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "http whitelist fqdn enable" is displayed.	Disable	The message "no http whitelist fqdn enable" is displayed.
Setting	Display						
Enable	The message "http whitelist fqdn enable" is displayed.						
Disable	The message "no http whitelist fqdn enable" is displayed.						
WHITELIST_FQDN_VALUE	<p>The FQDN settings for the FQDN whitelist control are displayed in the following format</p> <p style="background-color: #f0f0f0; padding: 5px;"><code>http whitelist fqdn WHITE_FQDN</code></p> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>WHITE_FQDN</td> <td>FQDN to whitelist</td> </tr> </tbody> </table> <p> More than one may be displayed.</p>	Setting items	Contents	WHITE_FQDN	FQDN to whitelist		
Setting items	Contents						
WHITE_FQDN	FQDN to whitelist						

Item	Contents						
BLACKLIST_FQDN_ENABLED	<p>The Enable/Disable setting for FQDN blacklist control is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "http blacklist fqdn enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no http blacklist fqdn enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "http blacklist fqdn enable" is displayed.	Disable	The message "no http blacklist fqdn enable" is displayed.
Setting	Display						
Enable	The message "http blacklist fqdn enable" is displayed.						
Disable	The message "no http blacklist fqdn enable" is displayed.						
BLACKLIST_FQDN_VALUE	<p>The FQDN settings for FQDN blacklist control are displayed in the following format</p> <pre>http blacklist fqdn BLACK_FQDN</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>BLACK_FQDN</td> <td>FQDN to be blacklisted</td> </tr> </tbody> </table> <p> More than one may be displayed.</p>	Setting items	Contents	BLACK_FQDN	FQDN to be blacklisted		
Setting items	Contents						
BLACK_FQDN	FQDN to be blacklisted						
WHITELIST_URL_ENABLED	<p>The URL whitelist control enable/disable setting is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "http whitelist url enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no http whitelist url enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "http whitelist url enable" is displayed.	Disable	The message "no http whitelist url enable" is displayed.
Setting	Display						
Enable	The message "http whitelist url enable" is displayed.						
Disable	The message "no http whitelist url enable" is displayed.						
WHITELIST_URL_VALUE	<p>The FQDN setting for URL whitelist control appears in the following format</p> <pre>http whitelist url WHITE_URL</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>WHITE_URL</td> <td>URL to whitelist</td> </tr> </tbody> </table> <p> More than one may be displayed.</p>	Setting items	Contents	WHITE_URL	URL to whitelist		
Setting items	Contents						
WHITE_URL	URL to whitelist						
BLACKLIST_URL_ENABLED	<p>The URL blacklist control enable/disable setting is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "http blacklist url enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no http blacklist url enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "http blacklist url enable" is displayed.	Disable	The message "no http blacklist url enable" is displayed.
Setting	Display						
Enable	The message "http blacklist url enable" is displayed.						
Disable	The message "no http blacklist url enable" is displayed.						
BLACKLIST_URL_VALUE	<p>The FQDN settings for URL blacklist control are displayed in the following format</p> <pre>http blacklist url BLACK_URL</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>BLACK_URL</td> <td>URL to be blacklisted</td> </tr> </tbody> </table> <p> More than one may be displayed.</p>	Setting items	Contents	BLACK_URL	URL to be blacklisted		
Setting items	Contents						
BLACK_URL	URL to be blacklisted						
HTTP_ACCESS	<p>HTTP access control settings are displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>permit</td> <td>The message "http-access allowed" is displayed.</td> </tr> <tr> <td>refusal</td> <td>The message "http-access deny" is displayed.</td> </tr> </tbody> </table>	Setting	Display	permit	The message "http-access allowed" is displayed.	refusal	The message "http-access deny" is displayed.
Setting	Display						
permit	The message "http-access allowed" is displayed.						
refusal	The message "http-access deny" is displayed.						

Item	Contents						
AUTHENTICATION_ENABLED	<p>The Enable/Disable User Authentication Control setting is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "authentication enable" appears.</td> </tr> <tr> <td>Disable</td> <td>The message "no authentication enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "authentication enable" appears.	Disable	The message "no authentication enable" is displayed.
Setting	Display						
Enable	The message "authentication enable" appears.						
Disable	The message "no authentication enable" is displayed.						
SCHEME	<p>The authentication method setting for user authentication is displayed in the following format.</p> <pre>authentication scheme SCHEME_VALUE</pre> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Basic authentication</td> <td>The message "authentication scheme basic" is displayed.</td> </tr> <tr> <td>Digest Authentication</td> <td>The message "authentication scheme digest" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Basic authentication	The message "authentication scheme basic" is displayed.	Digest Authentication	The message "authentication scheme digest" is displayed.
Setting	Display						
Basic authentication	The message "authentication scheme basic" is displayed.						
Digest Authentication	The message "authentication scheme digest" is displayed.						
TIMETOLIVE	<p>The Enable period setting for user authentication is displayed in the following format</p> <pre>authentication ttl TIMETOLIVE_VALUE</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>TIMETOLIVE_VALUE</td> <td> <p>The Enable period of the user authentication is displayed.</p> <p>The range is "1m to 60m" and "1h to 168h".</p> <p>m represents minutes and h represents hours.</p> </td> </tr> </tbody> </table>	Setting items	Contents	TIMETOLIVE_VALUE	<p>The Enable period of the user authentication is displayed.</p> <p>The range is "1m to 60m" and "1h to 168h".</p> <p>m represents minutes and h represents hours.</p>		
Setting items	Contents						
TIMETOLIVE_VALUE	<p>The Enable period of the user authentication is displayed.</p> <p>The range is "1m to 60m" and "1h to 168h".</p> <p>m represents minutes and h represents hours.</p>						
USERNAME	<p>The username setting for user authentication is displayed.</p>  More than one authentication account may be displayed.						
ENCRYPT-PASSWORD	<p>The password setting for encrypted user authentication is displayed.</p>						
MAXIMUM	<p>The maximum number of processes setting for user authentication is displayed in the following format</p> <pre>authentication process maximum MAX_NUM</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MAX_NUM</td> <td> <p>The maximum number of processes is displayed.</p> <p>The range is "1 to 5". The default setting is "5".</p> </td> </tr> </tbody> </table>	Setting items	Contents	MAX_NUM	<p>The maximum number of processes is displayed.</p> <p>The range is "1 to 5". The default setting is "5".</p>		
Setting items	Contents						
MAX_NUM	<p>The maximum number of processes is displayed.</p> <p>The range is "1 to 5". The default setting is "5".</p>						
STARTUP	<p>The number of startup processes setting for user authentication is displayed in the following format</p> <pre>authentication process startup STARTUP_NUM</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>STARTUP_NUM</td> <td> <p>The number of processes setting at startup is displayed.</p> <p>The range is "1 to 5". The default setting is "5".</p> </td> </tr> </tbody> </table>	Setting items	Contents	STARTUP_NUM	<p>The number of processes setting at startup is displayed.</p> <p>The range is "1 to 5". The default setting is "5".</p>		
Setting items	Contents						
STARTUP_NUM	<p>The number of processes setting at startup is displayed.</p> <p>The range is "1 to 5". The default setting is "5".</p>						

Item	Contents						
IDLE	<p>The number of operational processes setting for user authentication is displayed in the following format</p> <pre>authentication process startup IDLE_NUM</pre> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>IDLE_NUM</td> <td>The number of processes setting during operation is displayed. The range is "1 to 5". The default setting is "1".</td> </tr> </tbody> </table>	Setting items	Contents	IDLE_NUM	The number of processes setting during operation is displayed. The range is "1 to 5". The default setting is "1".		
Setting items	Contents						
IDLE_NUM	The number of processes setting during operation is displayed. The range is "1 to 5". The default setting is "1".						
CASESENSITIVE	<p>Displays the username case identification setting for the BASIC method of user authentication. The default setting is "Enabled".</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "authentication basic casesensitive" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no authentication basic casesensitive" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "authentication basic casesensitive" is displayed.	Disable	The message "no authentication basic casesensitive" is displayed.
Setting	Display						
Enable	The message "authentication basic casesensitive" is displayed.						
Disable	The message "no authentication basic casesensitive" is displayed.						
ACCESS_LOG_ENABLED	<p>The Enable/Disable Access Log Control setting is displayed. The default setting is "Disabled".</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "access log enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no access log enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "access log enable" is displayed.	Disable	The message "no access log enable" is displayed.
Setting	Display						
Enable	The message "access log enable" is displayed.						
Disable	The message "no access log enable" is displayed.						
FACILITY	<p>Facility settings for access log output are displayed in the following format.</p> <pre>access log facility FACILITY_VALUE</pre> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>FACILITY_VALUE</td> <td> <p>One of the following facility settings will be displayed. The default setting is "daemon".</p> <ul style="list-style-type: none"> ● daemon ● local0 ● local1 ● local2 ● local3 ● local4 ● local5 ● local6 ● local7 ● user </td> </tr> </tbody> </table>	Setting	Contents	FACILITY_VALUE	<p>One of the following facility settings will be displayed. The default setting is "daemon".</p> <ul style="list-style-type: none"> ● daemon ● local0 ● local1 ● local2 ● local3 ● local4 ● local5 ● local6 ● local7 ● user 		
Setting	Contents						
FACILITY_VALUE	<p>One of the following facility settings will be displayed. The default setting is "daemon".</p> <ul style="list-style-type: none"> ● daemon ● local0 ● local1 ● local2 ● local3 ● local4 ● local5 ● local6 ● local7 ● user 						
PRIORITY	<p>Priority settings for access log output are displayed in the following format.</p> <pre>access log priority PRIORITY_VALUE</pre> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PRIORITY_VALUE</td> <td> <p>One of the following priority settings will be displayed. The default setting is "informational".</p> <ul style="list-style-type: none"> ● debugging ● informational </td> </tr> </tbody> </table>	Setting	Contents	PRIORITY_VALUE	<p>One of the following priority settings will be displayed. The default setting is "informational".</p> <ul style="list-style-type: none"> ● debugging ● informational 		
Setting	Contents						
PRIORITY_VALUE	<p>One of the following priority settings will be displayed. The default setting is "informational".</p> <ul style="list-style-type: none"> ● debugging ● informational 						

7.11.2 Configure proxy server settings.

To configure the proxy server, go to advanced configuration mode and execute the configuration commands.

The settings made here are written to a configuration file.

Format

```

proxy
port PROXY_PORT
source address enable
no source address enable
source address ADDRESS[-ADDRESS]/PREFIX
no source address ADDRESS[-ADDRESS]/PREFIX
acl port SAFE_PORT[-SAFE_PORT].
no acl port SAFE_PORT[-SAFE_PORT].
acl ssl SSL_PORT[-SSL_PORT].
no acl ssl SSL_PORT[-SSL_PORT].
http whitelist fqdn enable
no http whitelist fqdn enable
http whitelist fqdn WHITELIST_FQDN
no http whitelist fqdn WHITELIST_FQDN
http blacklist fqdn enable
no http blacklist fqdn enable
http blacklist fqdn BLACKLIST_FQDN
no http blacklist fqdn BLACKLIST_FQDN
http whitelist url enable
no http whitelist url enable
http whitelist url WHITELIST_URL
no http whitelist url WHITELIST_URL
http blacklist url enable
no http blacklist url enable
http blacklist url BLACKLIST_URL
no http blacklist url BLACKLIST_URL
http-access ACCESS
authentication enable
no authentication enable
authentication scheme SCHEME
authentication ttl TIMETOLIVE
authentication account USERNAME
authentication account USERNAME secret ENCRYPT-PASSWORD
no authentication account USERNAME
authentication process maximum MAXIMUM
authentication process startup STARTUP
authentication process idle IDLE
authentication basic casesensitive
no authentication basic casesensitive
access log enable
no access log enable
access log facility FACILITY
access log priority PRIORITY
enable
no enable
exit

```

Command

Command	Contents				
proxy	<p>Execute the proxy server configuration command.</p>  Executing a command in the setting mode shifts to the detailed setting mode.				
port	<p>Set the proxy server's listening port number.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PROXY_PORT</td> <td> <p>Specifies the port to listen on for the proxy server.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • The default value is "8080". </td> </tr> </tbody> </table>	Setting	Contents	PROXY_PORT	<p>Specifies the port to listen on for the proxy server.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • The default value is "8080".
Setting	Contents				
PROXY_PORT	<p>Specifies the port to listen on for the proxy server.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • The default value is "8080". 				
source address enable	Enables connection source network control.				
no source address enable	Disables connection source network control.				
source address	<p>Set the connection source network address.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ADDRESS[-ADDRESS]/PREFIX</td> <td> <p>Specifies the network address/prefix of the connection sender.</p>  Hyphen ('-') can be used to set address ranges. </td> </tr> </tbody> </table> <p> A maximum of 64 settings is possible.</p>	Setting	Contents	ADDRESS[-ADDRESS]/PREFIX	<p>Specifies the network address/prefix of the connection sender.</p>  Hyphen ('-') can be used to set address ranges.
Setting	Contents				
ADDRESS[-ADDRESS]/PREFIX	<p>Specifies the network address/prefix of the connection sender.</p>  Hyphen ('-') can be used to set address ranges.				
no source address	Deletes the connection source network address setting.				
acl port	<p>Set the destination port number to allow access through the proxy server.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SAFE_PORT[-SAFE_PORT].</td> <td> <p>Specifies the permitted connection destination port number.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • It is possible to use hyphen ('-') to set the port range. </td> </tr> </tbody> </table> <p> A maximum of 64 settings is possible.</p>	Setting	Contents	SAFE_PORT[-SAFE_PORT].	<p>Specifies the permitted connection destination port number.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • It is possible to use hyphen ('-') to set the port range.
Setting	Contents				
SAFE_PORT[-SAFE_PORT].	<p>Specifies the permitted connection destination port number.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • It is possible to use hyphen ('-') to set the port range. 				
no acl port	Delete the destination port number setting that allows access via a proxy server.				
acl ssl	<p>Set the https destination port number to allow access through the proxy server.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>SSL_PORT[-SSL_PORT].</td> <td> <p>Specify the https connection allowed destination port number.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • It is possible to set the port range using hyphen ('-') </td> </tr> </tbody> </table> <p> A maximum of 64 settings is possible.</p>	Setting	Contents	SSL_PORT[-SSL_PORT].	<p>Specify the https connection allowed destination port number.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • It is possible to set the port range using hyphen ('-')
Setting	Contents				
SSL_PORT[-SSL_PORT].	<p>Specify the https connection allowed destination port number.</p> <ul style="list-style-type: none"> • The setting range is 1 to 65535. • It is possible to set the port range using hyphen ('-') 				
no acl ssl	Delete the https destination port number setting that allows access via a proxy server.				
http whitelist fqdn enable	Enable FQDN whitelist control.				
no http whitelist fqdn enable	Disables FQDN whitelist control.				

Command	Contents				
http whitelist fqdn	<p>Configure FQDN settings for FQDN whitelist control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>WHITELIST_FQDN</td> <td>Specify the FQDN to be registered in the whitelist.</td> </tr> </tbody> </table> <p> A maximum of 64 settings is possible.</p>	Setting	Contents	WHITELIST_FQDN	Specify the FQDN to be registered in the whitelist.
Setting	Contents				
WHITELIST_FQDN	Specify the FQDN to be registered in the whitelist.				
no http whitelist fqdn	Delete the FQDN setting in the FQDN whitelist control.				
http blacklist fqdn enable	Enable FQDN blacklist control.				
no http blacklist fqdn enable	Disables FQDN blacklist control.				
http blacklist fqdn	<p>Configure FQDN settings for FQDN blacklist control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>BLACKLIST_FQDN</td> <td>Specify the FQDN to be registered in the blacklist.</td> </tr> </tbody> </table> <p> A maximum of 64 settings is possible.</p>	Setting	Contents	BLACKLIST_FQDN	Specify the FQDN to be registered in the blacklist.
Setting	Contents				
BLACKLIST_FQDN	Specify the FQDN to be registered in the blacklist.				
no http blacklist fqdn	Delete the FQDN setting for FQDN blacklist control.				
http whitelist url enable	Enable URL whitelist control.				
no http whitelist url enable	Disables URL whitelist control.				
http whitelist url	<p>Configure URL settings for URL whitelist control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>WHITELIST_URL</td> <td>Specify the URLs to be registered in the whitelist.</td> </tr> </tbody> </table> <p> A maximum of 64 settings is possible.</p>	Setting	Contents	WHITELIST_URL	Specify the URLs to be registered in the whitelist.
Setting	Contents				
WHITELIST_URL	Specify the URLs to be registered in the whitelist.				
no http whitelist url	Deletes URL whitelist control URL settings.				
http blacklist url enable	Enable URL blacklist control.				
no http blacklist url enable	Disables URL blacklist control.				
http blacklist url	<p>Configure URLs for URL blacklist control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>BLACKLIST_URL</td> <td>Specify URLs to be registered in the blacklist.</td> </tr> </tbody> </table> <p> A maximum of 64 settings is possible.</p>	Setting	Contents	BLACKLIST_URL	Specify URLs to be registered in the blacklist.
Setting	Contents				
BLACKLIST_URL	Specify URLs to be registered in the blacklist.				
no http blacklist url	Remove URL blacklist control URL settings.				
http-access	<p>Configure HTTP access control settings.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ACCESS</td> <td> <p>Specify whether to allow or deny HTTP access control.</p> <ul style="list-style-type: none"> ● allow Allow HTTP access control. ● deny Deny HTTP access control. </td> </tr> </tbody> </table> <p> Basically, when using allow, the HTTP/URL blacklist is used in conjunction with the HTTP/URL whitelist, and when using deny, the HTTP/URL whitelist is used in conjunction with the HTTP/URL blacklist.</p>	Setting	Contents	ACCESS	<p>Specify whether to allow or deny HTTP access control.</p> <ul style="list-style-type: none"> ● allow Allow HTTP access control. ● deny Deny HTTP access control.
Setting	Contents				
ACCESS	<p>Specify whether to allow or deny HTTP access control.</p> <ul style="list-style-type: none"> ● allow Allow HTTP access control. ● deny Deny HTTP access control. 				
authentication enable	Enable user authentication control settings.				
no authentication enable	Disable user authentication control settings.				

Command	Contents				
authentication scheme	<p>Sets the authentication method for user authentication.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>display</th> </tr> </thead> <tbody> <tr> <td>SCHEME</td> <td> <p>Specifies the authentication method for user authentication.</p> <ul style="list-style-type: none"> ● basic basic authentication ● digest Digest Authentication </td> </tr> </tbody> </table>	Setting	display	SCHEME	<p>Specifies the authentication method for user authentication.</p> <ul style="list-style-type: none"> ● basic basic authentication ● digest Digest Authentication
Setting	display				
SCHEME	<p>Specifies the authentication method for user authentication.</p> <ul style="list-style-type: none"> ● basic basic authentication ● digest Digest Authentication 				
authentication ttl	<p>Sets the Enable period of user authentication.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>TIMETOLIVE</td> <td> <p>The Enable period of user authentication is set. The range is "1m to 60m" and "1h to 168h". m represents minutes and h represents hours.</p> </td> </tr> </tbody> </table>	Setting	Contents	TIMETOLIVE	<p>The Enable period of user authentication is set. The range is "1m to 60m" and "1h to 168h". m represents minutes and h represents hours.</p>
Setting	Contents				
TIMETOLIVE	<p>The Enable period of user authentication is set. The range is "1m to 60m" and "1h to 168h". m represents minutes and h represents hours.</p>				
authentication account	<p>Set a username and password for user authentication. Passwords are set interactively. If the password is successfully changed, the encrypted password is saved.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>USERNAME</td> <td>Specify a username for user authentication.</td> </tr> </tbody> </table>	Setting	Contents	USERNAME	Specify a username for user authentication.
Setting	Contents				
USERNAME	Specify a username for user authentication.				
authentication account secret	<p>Set a username and password (after encryption) for user authentication.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ENCRYPT-PASSWORD</td> <td>Updates the password with an encrypted string.</td> </tr> </tbody> </table>	Setting	Contents	ENCRYPT-PASSWORD	Updates the password with an encrypted string.
Setting	Contents				
ENCRYPT-PASSWORD	Updates the password with an encrypted string.				
no authentication account	Delete username and password for user authentication.				
authentication process maximum	<p>Sets the maximum number of processes for user authentication.</p> <table border="1"> <thead> <tr> <th>Setting items</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>MAXINUM</td> <td> <p>Specifies the maximum number of processes.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "5". </td> </tr> </tbody> </table>	Setting items	Contents	MAXINUM	<p>Specifies the maximum number of processes.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "5".
Setting items	Contents				
MAXINUM	<p>Specifies the maximum number of processes.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "5". 				
authentication process startup	<p>Sets the number of startup processes for user authentication.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>STARTUP</td> <td> <p>Specifies the number of processes set at startup.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "5". </td> </tr> </tbody> </table>	Setting	Contents	STARTUP	<p>Specifies the number of processes set at startup.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "5".
Setting	Contents				
STARTUP	<p>Specifies the number of processes set at startup.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "5". 				
authentication process idle	<p>Sets the number of operational processes for user authentication.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>IDLE</td> <td> <p>The number of processes setting during operation is displayed.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "1". </td> </tr> </tbody> </table>	Setting	Contents	IDLE	<p>The number of processes setting during operation is displayed.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "1".
Setting	Contents				
IDLE	<p>The number of processes setting during operation is displayed.</p> <ul style="list-style-type: none"> ● The range is "1-5". ● The default setting is "1". 				
authentication basic casesensitive	Enable the username case identification setting for the BASIC method of user authentication.				
no authentication basic casesensitive	Disable the username case identification setting for the BASIC method of user authentication.				
access log enable	Enable access log control settings.				
no access log enable	Disable access log control settings.				

Command	Contents				
access log facility	<p>Set the facility for access log output.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>FACILITY</td> <td> <p>One of the following facilities is specified. By default, "daemon" is set.</p> <ul style="list-style-type: none"> ● daemon ● local0 ● local1 ● local2 ● local3 ● local4 ● local5 ● local6 ● local7 ● user </td> </tr> </tbody> </table>	Setting	Contents	FACILITY	<p>One of the following facilities is specified. By default, "daemon" is set.</p> <ul style="list-style-type: none"> ● daemon ● local0 ● local1 ● local2 ● local3 ● local4 ● local5 ● local6 ● local7 ● user
Setting	Contents				
FACILITY	<p>One of the following facilities is specified. By default, "daemon" is set.</p> <ul style="list-style-type: none"> ● daemon ● local0 ● local1 ● local2 ● local3 ● local4 ● local5 ● local6 ● local7 ● user 				
access log priority	<p>Sets the priority for access log output.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>PRIORITY</td> <td> <p>Specify one of the following priorities. By default, "informational" is set.</p> <ul style="list-style-type: none"> ● debugging ● informational </td> </tr> </tbody> </table>	Setting	Contents	PRIORITY	<p>Specify one of the following priorities. By default, "informational" is set.</p> <ul style="list-style-type: none"> ● debugging ● informational
Setting	Contents				
PRIORITY	<p>Specify one of the following priorities. By default, "informational" is set.</p> <ul style="list-style-type: none"> ● debugging ● informational 				
enable	Enable the proxy server and start the service.				
no enable	Disable the proxy server and stop the service.				
exit	Exit the detailed setting mode and enter the setting mode.				

Chap 8. Hardware Management

This chapter describes the management of hardware added to the product.

8.1 Control USB devices



Displays USB devices connected to USB bus 1 and turns devices on and off.

8.1.1 Display USB devices

To view USB devices, run the *show device usb* command.



Only devices connected to USB bus 1 are displayed.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# show device usb ↵  
Bus 001 Device 003: ID ****:**** amnimo Corp./ amnimo Corp.
```

8.1.2 Control USB devices

Set the USB port VBUS to ON or OFF.

Turn on/reset VBUS

To turn on or reset VBUS for a USB port, execute the *device usb* command.



- Only devices connected to USB bus 1 are displayed.
- If a HUB is connected to the USB bus, the HUB port is not covered.

Format

```
device usb [reset [TIME[s|m]]]
```

Setting items

Item	Contents				
reset	Turns off VBUS at the USB port for the period (seconds or minutes) specified by TIME. <table border="1"><thead><tr><th>Setting</th><th>Contents</th></tr></thead><tbody><tr><td>TIME</td><td>USB port reset time.<ul style="list-style-type: none">● Seconds designation: Range 1-3600, unit: s● Minute designation: Range 1 to 60, unit: mIf no unit is specified, seconds are specified.</td></tr></tbody></table>	Setting	Contents	TIME	USB port reset time. <ul style="list-style-type: none">● Seconds designation: Range 1-3600, unit: s● Minute designation: Range 1 to 60, unit: m If no unit is specified, seconds are specified.
Setting	Contents				
TIME	USB port reset time. <ul style="list-style-type: none">● Seconds designation: Range 1-3600, unit: s● Minute designation: Range 1 to 60, unit: m If no unit is specified, seconds are specified.				

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# device usb reset 60s ↵
```

Turn off VBUS

To turn off VBUS on the USB port, execute the *no device usb* command.



- Only devices connected to USB bus 1 are displayed.
- If a HUB is connected to the USB bus, the HUB port is not covered.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# no device usb ↵
```

8.2 Configure PoE settings.



Displays PoE status and settings, controls ports, and configures PoE settings.

8.2.1 Display PoE status

To display the status of the PoE, run the *show poe* command.

Format

```
show poe [IFNAME].
```

Setting items

Item	Contents								
IFNAME	<p>Specify the interface name of the PoE.</p> <p>The interface to be specified for IFNAME varies depending on the model.</p> <table border="1"> <thead> <tr> <th>model</th> <th>Specifiable Interfaces</th> </tr> </thead> <tbody> <tr> <td> </td> <td>lan0, lan1, lan2, lan3</td> </tr> <tr> <td></td> <td>eth0, eth1</td> </tr> <tr> <td></td> <td>lan1</td> </tr> </tbody> </table> <p> If IFNAME is omitted, the PoE status of all configured interfaces will be displayed.</p>	model	Specifiable Interfaces		lan0, lan1, lan2, lan3		eth0, eth1		lan1
model	Specifiable Interfaces								
	lan0, lan1, lan2, lan3								
	eth0, eth1								
	lan1								

Output Format

```
# ---- poe IFNAME ----
state      STATE
class      CLASS
POEPLUS    POEPLUS
limit-current ICUT
Voltage    POE-VOLTAGE
Current    POE-CURRENT
Watt       POE-WATT
```

Output item

Item	Contents						
IFNAME	The interface name is displayed.						
STATE	<p>The status of the connection to the port is displayed.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>connected</td> <td>state of connectivity</td> </tr> <tr> <td>disconnected</td> <td>disconnected state</td> </tr> </tbody> </table>	Value	Description	connected	state of connectivity	disconnected	disconnected state
Value	Description						
connected	state of connectivity						
disconnected	disconnected state						

Item	Contents																																				
CLASS	Displays the recognition results of the PoE power class classification process (classification).																																				
	<table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Class0</td> <td>Class 0 (IEE802.3af, PSE output power 15.4W)</td> </tr> <tr> <td>Class1</td> <td>Class 1 (IEE802.3af, PSE output power 4.0W)</td> </tr> <tr> <td>Class2</td> <td>Class2 (IEE802.3af, PSE output power 7.0W)</td> </tr> <tr> <td>Class 3</td> <td>Class 3 (IEE802.3af, PSE output power 15.4W)</td> </tr> <tr> <td>Class 4</td> <td>Class 4 (IEE802.3at, PSE output power 30W)</td> </tr> <tr> <td>Unknown</td> <td>unrecognized state</td> </tr> <tr> <td>Overcurrent</td> <td>Over current condition</td> </tr> <tr> <td>Class-mismatch</td> <td>Classification Mismatch</td> </tr> </tbody> </table>	Value	Description	Class0	Class 0 (IEE802.3af, PSE output power 15.4W)	Class1	Class 1 (IEE802.3af, PSE output power 4.0W)	Class2	Class2 (IEE802.3af, PSE output power 7.0W)	Class 3	Class 3 (IEE802.3af, PSE output power 15.4W)	Class 4	Class 4 (IEE802.3at, PSE output power 30W)	Unknown	unrecognized state	Overcurrent	Over current condition	Class-mismatch	Classification Mismatch																		
	Value	Description																																			
	Class0	Class 0 (IEE802.3af, PSE output power 15.4W)																																			
	Class1	Class 1 (IEE802.3af, PSE output power 4.0W)																																			
	Class2	Class2 (IEE802.3af, PSE output power 7.0W)																																			
	Class 3	Class 3 (IEE802.3af, PSE output power 15.4W)																																			
	Class 4	Class 4 (IEE802.3at, PSE output power 30W)																																			
	Unknown	unrecognized state																																			
Overcurrent	Over current condition																																				
Class-mismatch	Classification Mismatch																																				
POEPLUS	Information is displayed when PoE-Plus (IEEE802.3at) is enabled/disabled.																																				
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "on" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "off" will be displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "on" is displayed.	Disable	The message "off" will be displayed.																														
	Setting	Display																																			
Enable	The message "on" is displayed.																																				
Disable	The message "off" will be displayed.																																				
ICUT	Displays the setting status of the PoE current limit.																																				
	<table border="1"> <thead> <tr> <th>Model</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td rowspan="2"></td> <td>110mA</td> <td>Current limit 110mA (PoEPlus disabled)</td> </tr> <tr> <td>204mA</td> <td>Current limit 204mA (PoEPlus disabled)</td> </tr> <tr> <td rowspan="2"></td> <td>374mA</td> <td>Current limit 374mA (PoEPlus disabled)</td> </tr> <tr> <td>592mA</td> <td>Current limit 592mA (PoEPlus enabled)</td> </tr> <tr> <td rowspan="2"></td> <td>645mA</td> <td>Current limit 645mA (PoEPlus enabled)</td> </tr> <tr> <td>754mA</td> <td>Current limit 754mA (PoEPlus enabled)</td> </tr> <tr> <td rowspan="2"></td> <td>920mA</td> <td>Current limit 920mA (PoEPlus enabled)</td> </tr> <tr> <td rowspan="7"></td> <td>375mA</td> <td>Current limit 375mA (PoEPlus disabled)</td> </tr> <tr> <td>110mA</td> <td>Current limit 110mA (PoEPlus disabled)</td> </tr> <tr> <td>188mA</td> <td>Current limit 188mA (PoEPlus disabled)</td> </tr> <tr> <td>650mA</td> <td>Current limit 650mA (PoEPlus enabled)</td> </tr> <tr> <td>500mA</td> <td>Current limit 500mA (PoEPlus enabled)</td> </tr> <tr> <td>625mA</td> <td>Current limit 625mA (PoEPlus enabled)</td> </tr> <tr> <td>920mA</td> <td>Current limit 920mA (PoEPlus enabled)</td> </tr> </tbody> </table>	Model	Value	Description		110mA	Current limit 110mA (PoEPlus disabled)	204mA	Current limit 204mA (PoEPlus disabled)		374mA	Current limit 374mA (PoEPlus disabled)	592mA	Current limit 592mA (PoEPlus enabled)		645mA	Current limit 645mA (PoEPlus enabled)	754mA	Current limit 754mA (PoEPlus enabled)		920mA	Current limit 920mA (PoEPlus enabled)		375mA	Current limit 375mA (PoEPlus disabled)	110mA	Current limit 110mA (PoEPlus disabled)	188mA	Current limit 188mA (PoEPlus disabled)	650mA	Current limit 650mA (PoEPlus enabled)	500mA	Current limit 500mA (PoEPlus enabled)	625mA	Current limit 625mA (PoEPlus enabled)	920mA	Current limit 920mA (PoEPlus enabled)
	Model	Value	Description																																		
		110mA	Current limit 110mA (PoEPlus disabled)																																		
		204mA	Current limit 204mA (PoEPlus disabled)																																		
		374mA	Current limit 374mA (PoEPlus disabled)																																		
		592mA	Current limit 592mA (PoEPlus enabled)																																		
		645mA	Current limit 645mA (PoEPlus enabled)																																		
		754mA	Current limit 754mA (PoEPlus enabled)																																		
		920mA	Current limit 920mA (PoEPlus enabled)																																		
			375mA	Current limit 375mA (PoEPlus disabled)																																	
	110mA		Current limit 110mA (PoEPlus disabled)																																		
	188mA		Current limit 188mA (PoEPlus disabled)																																		
	650mA		Current limit 650mA (PoEPlus enabled)																																		
	500mA		Current limit 500mA (PoEPlus enabled)																																		
625mA	Current limit 625mA (PoEPlus enabled)																																				
920mA	Current limit 920mA (PoEPlus enabled)																																				
POE-VOLTAGE	The current voltage value is displayed (unit: V).																																				
POE-CURRENT	The current current value is displayed (unit: mA).																																				
POE-WATT	The current power value is displayed (unit: W).																																				

Execution example

Command input and output is the same in all modes. Below is an example of running the Edge Gateway in General User mode.

ユーザーモード
管理者モード
設定モード

```

amnimo$ show poe lan0 ←
# ---- Poe lan0 ----
state connected
class Class0
poepplus off
limit-current 374mA
Voltage 53.894V
Current 50.235mA

```

8.2.2 Controlling the PoE port

To control a PoE port, execute the *device poe* command.

Format (AI Edge Gateway, Edge Gateway Outdoor Type IoT Router)

```
device poe reset <IFNAME> [0-3600].
no device poe power <IFNAME>
device poe power <IFNAME>
device poe icut <IFNAME> <110|204|374|592|645|754|920|auto>
device poe
no device poe
```

Format (Compact Router Outdoor Type with wireless LAN)

```
device poe reset <IFNAME> [0-3600].
no device poe power <IFNAME>
device poe power <IFNAME>
device poe icut <IFNAME> auto
device poe
no device poe
```

Command

Command	Contents								
device poe reset	<p>Reset the PoE port. Specify the interface name of the PoE in IFNAME and the OFF period (in seconds) at reset in the number from 0 to 3600. The interface to be specified for IFNAME varies depending on the model. (The same applies to subsequent functions.)</p> <table border="1"> <thead> <tr> <th>model</th> <th>Specifiable Interfaces</th> </tr> </thead> <tbody> <tr> <td>  </td> <td>lan0, lan1, lan2, lan3</td> </tr> <tr> <td></td> <td>eth0, eth1</td> </tr> <tr> <td></td> <td>lan1</td> </tr> </tbody> </table> <p> If the number is omitted, it will be reset to the default of 60 seconds.</p>	model	Specifiable Interfaces	  	lan0, lan1, lan2, lan3		eth0, eth1		lan1
model	Specifiable Interfaces								
  	lan0, lan1, lan2, lan3								
	eth0, eth1								
	lan1								
device poe power	Specify the PoE interface name in IFNAME to enable the power output of the PoE port.								
no device poe power	Specify the PoE interface name in IFNAME to disable the power output of the PoE port.								
device poe icut	<p>Specify the PoE interface name in IFNAME to change the current limit of the PoE port. The current limit value that can be specified varies depending on the model.</p> <table border="1"> <thead> <tr> <th>model</th> <th>Specifiable current limit (mA)</th> </tr> </thead> <tbody> <tr> <td>   </td> <td>110, 204, 374, 592, 645, 754, 920, auto</td> </tr> <tr> <td></td> <td>auto</td> </tr> </tbody> </table> <p> If auto is specified, it is set automatically.</p>	model	Specifiable current limit (mA)	   	110, 204, 374, 592, 645, 754, 920, auto		auto		
model	Specifiable current limit (mA)								
   	110, 204, 374, 592, 645, 754, 920, auto								
	auto								
device poe	Disable shutdown outputs to allow PoE devices to operate.								

Command	Contents
no device poe	<p>Enable shutdown outputs to prevent PoE devices from operating.</p>  <ul style="list-style-type: none"> ● Once the shutdown output is enabled, any PoE devices connected under ON control and located at will be turned off. ● Disabling the shutdown output back with the device poe command will initialize the PoE controller of this device, so the PoE device will not be turned on; to turn the PoE device on, run device poe power <IFNAME> or device poe reset <IFNAME>. ● It is also possible to turn on PoE devices through separately scheduled dead/ alive monitoring. <p>➔ For more information, see " 7.7.3 Set a schedule " for more information.</p>

Execution example

Since PoE port control is involved in the startup control of the device, the settings cannot be displayed in general user mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# device poe reset lan0 120 ↵
amnimo# no device poe power lan0 ↵
amnimo# device poe power lan0 ↵
amnimo# device poe icut lan0 592 ↵
amnimo# device poe ↵
amnimo# no device poe ↵
```

8.2.3 Display PoE settings

To view the PoE configuration, run the *show config poe* command.

Format

```
show config poe [IFNAME].
```

Setting items

Item	Contents
IFNAME	Specify the interface name of the PoE. <ul style="list-style-type: none"> ● Since the PoE control function is implemented on the LAN0-3 side, it is LAN0-3 that can be specified. ● If IFNAME is omitted, the PoE status of all configured interfaces will be displayed.

Output Format

```
# ---- transition to configure mode ----
configure
#
POE IFNAME
# ---- poe IFNAME configure ----
ENABLE
limit-current ICUT
onDeLay ONDELAY
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents																														
IFNAME	The PoE interface name is displayed.																														
ENABLE	Information is displayed when PoE power supply is enabled/disabled. <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.																								
Setting	Display																														
Enable	The message "enable" is displayed.																														
Disable	The message "no enable" is displayed.																														
ICUT	The PoE current limit value is displayed. <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th>Model</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td>110mA</td> <td>Current limit 110mA (PoEPlus disabled)</td> </tr> <tr> <td></td> <td>204mA</td> <td>Current limit 204mA (PoEPlus disabled)</td> </tr> <tr> <td></td> <td>374mA</td> <td>Current limit 374mA (PoEPlus disabled)</td> </tr> <tr> <td></td> <td>592mA</td> <td>Current limit 592mA (PoEPlus enabled)</td> </tr> <tr> <td></td> <td>645mA</td> <td>Current limit 645mA (PoEPlus enabled)</td> </tr> <tr> <td></td> <td>754mA</td> <td>Current limit 754mA (PoEPlus enabled)</td> </tr> <tr> <td></td> <td>920mA</td> <td>Current limit 920mA (PoEPlus enabled)</td> </tr> <tr> <td></td> <td>auto</td> <td>auto-setup mode</td> </tr> <tr> <td></td> <td>auto</td> <td>auto-setup mode</td> </tr> </tbody> </table>	Model	Value	Description		110mA	Current limit 110mA (PoEPlus disabled)		204mA	Current limit 204mA (PoEPlus disabled)		374mA	Current limit 374mA (PoEPlus disabled)		592mA	Current limit 592mA (PoEPlus enabled)		645mA	Current limit 645mA (PoEPlus enabled)		754mA	Current limit 754mA (PoEPlus enabled)		920mA	Current limit 920mA (PoEPlus enabled)		auto	auto-setup mode		auto	auto-setup mode
Model	Value	Description																													
	110mA	Current limit 110mA (PoEPlus disabled)																													
	204mA	Current limit 204mA (PoEPlus disabled)																													
	374mA	Current limit 374mA (PoEPlus disabled)																													
	592mA	Current limit 592mA (PoEPlus enabled)																													
	645mA	Current limit 645mA (PoEPlus enabled)																													
	754mA	Current limit 754mA (PoEPlus enabled)																													
	920mA	Current limit 920mA (PoEPlus enabled)																													
	auto	auto-setup mode																													
	auto	auto-setup mode																													
ONDELAY	The delay time (in seconds) at startup is displayed.																														

Execution example

Since PoE settings are involved in controlling the startup of the device, the settings cannot be displayed in general user mode. Below is an example of running the Edge Gateway in administrator mode.

管理者モード

```
amnimo# show config poe lan0 ↵
# ---- transition to configure mode ----
configure
# ---- Poe lan0 configure ----
POE LAN0
enable
limit-current 592
ondelay 120
exit
# ---- exit configure mode ----
exit
```

設定モード

```
amnimo(cfg)# show config poe lan0 ↵
# ---- Poe lan0 configure ----
POE LAN0
enable
limit-current 592
ondelay 120
exit
amnimo(cfg)#.
```



Running the show config command in PoE advanced configuration mode will display the same information as in configuration mode.

```
amnimo(cfg)# poe lan0↵ ← Go to PoE advanced configuration mode
amnimo(cfg-poe-lan0)# show config ↵ ← Same as setting mode
enable
limit-current 592
(Omitted.)
```

8.2.4 Configure PoE

To configure PoE, go to the PoE advanced configuration mode and execute the configuration commands.

The settings made here are written to a configuration file.

Format (AI Edge Gateway, Edge Gateway Outdoor Type IoT Router)

```
POE [IFNAME].
ondelay <0-3600>.
limit-current <110|204|374|754|592|645|920|auto>
enable
show config
no enable
exit
no poe IFNAME
```

Format (Compact Router Outdoor Type with wireless LAN)

```
POE [IFNAME].
ondelay <0-3600>
limit-current auto
enable
show config
no enable
exit
no poe IFNAME
```

Command

Command	Contents								
POE	<p>Specify the interface name of the PoE in IFNAME and execute the PoE configuration command. The interface to be specified in IFNAME varies depending on the model.</p> <table border="1"> <thead> <tr> <th>Model</th> <th>Specifiable Interfaces</th> </tr> </thead> <tbody> <tr> <td></td> <td>lan0, lan1, lan2, lan3</td> </tr> <tr> <td></td> <td>eth0, eth1</td> </tr> <tr> <td></td> <td>lan1</td> </tr> </tbody> </table> <p> Executing a command in the configuration mode will enter the advanced configuration mode for the specified interface.</p>	Model	Specifiable Interfaces		lan0, lan1, lan2, lan3		eth0, eth1		lan1
Model	Specifiable Interfaces								
	lan0, lan1, lan2, lan3								
	eth0, eth1								
	lan1								
ondelay	Set the delay time (in seconds) at startup from 0 to 3600.								
limit-current	<p>Sets the current limit of the PoE port. The current limit values that can be specified vary depending on the model.</p> <table border="1"> <thead> <tr> <th>Model</th> <th>Specifiable current limit (mA)</th> </tr> </thead> <tbody> <tr> <td></td> <td>110, 204, 374, 592, 645, 754, 920, auto</td> </tr> <tr> <td></td> <td>auto</td> </tr> </tbody> </table> <p> If auto is specified, it is set automatically.</p>	Model	Specifiable current limit (mA)		110, 204, 374, 592, 645, 754, 920, auto		auto		
Model	Specifiable current limit (mA)								
	110, 204, 374, 592, 645, 754, 920, auto								
	auto								
enable	Enable PoE power supply and start the service.								

Command	Contents
show config	Displays PoE settings. → For more information, see " 8.2.3 Display PoE settings " for more information.
no enable	Disable PoE power supply and stop service.
exit	Exit PoE advanced setting mode and enter setting mode.
no poe	Delete the PoE configuration by specifying the PoE interface name in IFNAME.

Execution example

設定モード

```
amnimo(cfg)# poe lan0 ↵
amnimo(cfg-poe-lan0)# ondelay 1200 ↵
amnimo(cfg-poe-lan0)# limit-current 592 ↵
amnimo(cfg-poe-lan0)# enable ↵
amnimo(cfg-poe-lan0)# exit ↵
```

8.3 Manage D IN/D OUT status



Displays the status of the digital input (D IN terminal) and digital output (D OUT terminal) on the rear of the product. It also controls the digital output.

8.3.1 Display the status of D IN

To display the status of the digital input (D IN pin), execute the *show din* command.

Format

```
show din [permanent].
```

Setting items

Item	Contents
permanent	Monitors changes in digital input and outputs status continuously. To stop output, press CTRL+C.

Output Format

```
DI-1: DI-STATUS
DI-2: DI-STATUS
DI-3: DI-STATUS
DI-4: DI-STATUS
```

Output item

Item	Contents						
DI-STATUS	The status of the digital input is displayed. <table border="1" data-bbox="571 1137 1353 1265"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td>ON state</td> </tr> <tr> <td>OFF</td> <td>OFF state</td> </tr> </tbody> </table>	Display	Contents	ON	ON state	OFF	OFF state
Display	Contents						
ON	ON state						
OFF	OFF state						

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```
amnimo$ show din ↵
DI-1: ON
DI-2: ON
DI-3: OFF
DI-4: OFF
```

8.3.2 Display the status of D OUT

To display the status of the digital output (D OUT pin), execute the *show dout* command.

Format

```
show dout
```

Output Format

```
DO-1: DO-STATUS
DO-2: DO-STATUS
```

Output item

Item	Contents						
DO-STATUS	The status of the digital output is displayed.						
	<table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td>ON state</td> </tr> <tr> <td>OFF</td> <td>OFF state</td> </tr> </tbody> </table>	Display	Contents	ON	ON state	OFF	OFF state
Display	Contents						
ON	ON state						
OFF	OFF state						

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```
amnimo$ show dout ↵
DO-1: ON
DO-2: OFF
```

8.3.3 Controls the state of D OUT

To control the digital output, execute the *dout* command.

Format

```
dout <set | set-bit | clr-bit> <0-3>
dout <on | off> <1 | 2>
```

Setting items

Item	Contents						
set	To control multiple digital outputs simultaneously, set one of the following <table border="1" data-bbox="571 539 1353 667"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ON</td> </tr> <tr> <td>0</td> <td>OFF</td> </tr> </tbody> </table>	Setting	Contents	1	ON	0	OFF
Setting	Contents						
1	ON						
0	OFF						
set-bit	Set the digital output to ON by specifying the bit number.						
clr-bit	Set the digital output to OFF by specifying the bit number.						
on	Set the digital output to ON by specifying the digital output number.						
off	Set the digital output to OFF by specifying the digital output number.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# dout set 3↵ ← Set digital output numbers 1 and 2 to ON simultaneously.
amnimo# dout on 1↵ ← Set digital output number 1 to ON
```

8.4 Display DIP switch status



To obtain the status of a DIP switch, run the *show dip-switch* command.



This function is not available on Compact Router.

Format

```
show dip-switch
```

Output Format

```
DSW-1: DSW-STATUS
DSW-2: DSW-STATUS
DSW-3: DSW-STATUS
DSW-4: DSW-STATUS
```

Output item

Item	Contents						
DSW-STATUS	The status of the DIP switch is displayed.						
	<table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td>ON state</td> </tr> <tr> <td>OFF</td> <td>OFF state</td> </tr> </tbody> </table>	Display	Contents	ON	ON state	OFF	OFF state
Display	Contents						
ON	ON state						
OFF	OFF state						

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.



```
amnimo$ show dip-switch ↵
DSW-1: OFF
DSW-2: OFF
DSW-3: OFF
DSW-4: ON
```

Chap 9. Maintenance and Management

This chapter describes how to understand and manage the hardware and network status of the product.

9.1 Display the status of this product

Displays the input voltage of the product and the temperature inside the enclosure.

9.1.1 Display input voltage



To display the input voltage, execute the *show voltage* command.

Format

```
show voltage
```

Output Format

```
Input Voltage: VOLTAGE1
Backup Voltage: VOLTAGE2
```

Output item

Item	Contents
VOLTAGE1	The voltage of the main power supply is displayed.
VOLTAGE2	The voltage of the backup power supply is displayed.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```
amnimo$ show voltage ↵
Input Voltage: +11.93 V
Backup Voltage: +3.53 V
```

9.1.2 Display the temperature inside the enclosure



To display the temperature inside the enclosure, run the *show temperature* command.

Format

```
show temperature
```

Output format (Edge Gateway, IoT Router)

```
CPU area : TEMPERATURE1
PoE area : TEMPERATURE2
```

Output items (Edge Gateway, IoT Router)

Item	Contents
TEMPERATURE1	Displays the temperature around the CPU.
TEMPERATURE2	Displays the temperature around the PoE.  IoT Routers do not show a "PoE area" row.

Output format (Compact Router)

```
NAV area: TEMPERATURE1
WDDAC area: TEMPERATURE2
MODEM area: TEMPERATURE3
IPSS area: TEMPERATURE4
CPU area: TEMPERATURE5
PA0 area: TEMPERATURE6
```

Output items (Compact Router)

Item	Contents
TEMPERATURE1	Displays the temperature around the NAV (GPS/GNSS).
TEMPERATURE2	Displays the temperature around the WDDAC.
TEMPERATURE3	Displays the temperature around the MODEM.
TEMPERATURE4	Displays the temperature around the IPSS.
TEMPERATURE5	Displays the temperature around the CPU.
TEMPERATURE6	Displays the temperature of the PA (PowerAmplifier) and the thermistor near the PMIC.

Execution example

Command input and output is the same in all modes. Below is an example of running the General User mode on an Outdoor Type Edge Gateway.



```
amnimo$ show temperature ↵
CPU area : +38.285 °C
PoE area : +38.071 °C
```

9.2 Configure CPU operation settings.

Displays and sets CPU operation.

9.2.1 Display CPU operation



To view CPU activity, run the *show cpufreq* command.



This function is not available for AI Edge Gateway.

Format

```
show cpufreq
```

Output Format

CPUFREQ

Output item

Item	Contents																						
CPUFREQ	<p>The current CPU operating frequency will be displayed. The display will show one of the following</p> <ul style="list-style-type: none"> ● Edge Gateways, IoT Routers <table border="1"> <tr><td>200 MHZ</td></tr> <tr><td>250 MHZ</td></tr> <tr><td>500 MHZ</td></tr> <tr><td>1000 MHZ</td></tr> <tr><td>ondemand (200MHZ)</td></tr> <tr><td>ondemand (250MHZ)</td></tr> <tr><td>ondemand (500MHZ)</td></tr> <tr><td>ondemand (1000MHZ)</td></tr> </table> ● Compact Router <table border="1"> <tr><td>400000</td></tr> <tr><td>800000</td></tr> <tr><td>998400</td></tr> <tr><td>1094400</td></tr> <tr><td>1190400</td></tr> <tr><td>1248000</td></tr> <tr><td>1305600</td></tr> <tr><td>interactive(400000)</td></tr> <tr><td>interactive(800000)</td></tr> <tr><td>interactive(998400)</td></tr> <tr><td>interactive(1094400)</td></tr> <tr><td>interactive(1190400)</td></tr> <tr><td>interactive(1248000)</td></tr> <tr><td>interactive(1305600)</td></tr> </table> 	200 MHZ	250 MHZ	500 MHZ	1000 MHZ	ondemand (200MHZ)	ondemand (250MHZ)	ondemand (500MHZ)	ondemand (1000MHZ)	400000	800000	998400	1094400	1190400	1248000	1305600	interactive(400000)	interactive(800000)	interactive(998400)	interactive(1094400)	interactive(1190400)	interactive(1248000)	interactive(1305600)
200 MHZ																							
250 MHZ																							
500 MHZ																							
1000 MHZ																							
ondemand (200MHZ)																							
ondemand (250MHZ)																							
ondemand (500MHZ)																							
ondemand (1000MHZ)																							
400000																							
800000																							
998400																							
1094400																							
1190400																							
1248000																							
1305600																							
interactive(400000)																							
interactive(800000)																							
interactive(998400)																							
interactive(1094400)																							
interactive(1190400)																							
interactive(1248000)																							
interactive(1305600)																							

Execution example (Edge Gateway, IoT Router)

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show cpufreq ↵  
500 MHZ
```

Execution example (Compact Router)

ユーザーモード 管理者モード 設定モード

```
amnimo$ show cpufreq ↵  
1305600
```

9.2.2 Display CPU operation settings



To display CPU operating settings, run the ***show config cpufreq*** command.



This function is not available on AI Edge Gateways and Compact Router.

Format

```
show config cpufreq
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- cpufreq configure ----
cpufreq CPUFREQ
# ---- exit configure mode ----
exit
```

Output items (Edge Gateway, IoT Router)

Item	Contents
CPUFREQ	The current CPU operating frequency will be displayed. The display will show one of the following <ul style="list-style-type: none">● 200 MHZ● 250 MHZ● 500 MHZ● 1000 MHZ● ondemand

Output items (Compact Router)

Item	Contents
CPUFREQ	The current CPU operating frequency will be displayed. The display will show one of the following <ul style="list-style-type: none">● 200 MHZ● 250 MHZ● 500 MHZ● 1000 MHZ● ondemand

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# show config cpufreq ↵
# ---- transition to configure mode ----
configure
# ---- cpufreq configure ----
cpufreq 500MHZ
# ---- exit configure mode ----
exit
```

9.2.3 Configure CPU operation



To set the CPU operating frequency during normal operation, execute the *cpufreq* command.

➔ For information on setting the CPU operating frequency at high and low temperatures, see "9.3 Set high and low temperature protection" for more information.



This function is not available on AI Edge Gateways and Compact Router.

Format

```
cpufreq <ondemand | 200MHZ | 250MHZ | 500MHZ | 1000MHZ>
```

Setting items

Item	Contents
ondemand	Dynamically change CPU operating frequency based on CPU load status.
200 MHz	Set the operating frequency to 200 MHz fixed.
250MHz	Set the operating frequency to 250 MHz fixed.
500MHz	Set the operating frequency to 500 MHz fixed.
1000 MHz	Sets the operating frequency to 1000 MHz fixed. (Default value)



The default value up to version 1.5.0 is ondemand. After version 1.5.1, the default value is 1000 MHz (fixed).

Execution example

設定 モード

```
amnimo(cfg)# cpufreq 500MHZ ↵
```

9.3 Set high and low temperature protection



Configure settings to change the CPU operating frequency, mobile module, and interface status when the enclosure is hot or cold.



This function is not available on Compact Router.

9.3.1 Display high and low temperature protection settings

To view the high and low temperature protection settings, run the *show config thermal* command.

Format

```
show config thermal
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- thermal configure ----
thermal polling POLLING
# ---- cpufreq COND-NAME configure ---- ← CPU operating frequency setting is displayed
thermal cpufreq COND-NAME
ENABLE
mode MODE
temperature TEMPERATURE
hysteresis HYSTERESIS
LOG-DETECTION
LOG-RESTORATION
state STATE
exit
# ---- mobile COND-NAME configure ---- ← Mobile module configuration will be displayed.
thermal mobile COND-NAME
ENABLE
mode MODE
temperature TEMPERATURE
hysteresis HYSTERESIS
LOG-DETECTION
LOG-RESTORATION
state STATE
exit
# ---- interface COND-NAME configure ---- ← Interface configuration will be displayed.
thermal interface COND-NAME
ENABLE
mode MODE
temperature TEMPERATURE
hysteresis HYSTERESIS
LOG-DETECTION
LOG-RESTORATION
state STATE
exit
# ---- exit configure mode ----
```

Output item

Item	Contents						
POLLING	The interval (in milliseconds) at which polling is performed is displayed.						
COND-NAME	The condition name is displayed.						
ENABLE	Information is displayed when each condition is enabled/disabled. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
MODE	mode is displayed.						
TEMPERATURE	The temperature at which the unit enters the high/low temperature protection control is displayed.						
HYSTERESIS	The hysteresis temperature to return from high/low temperature protection control is displayed.						
LOG-DETECTION	Displays whether or not logging is output when a control condition is activated. If so, the log level is displayed. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Log output enabled</td> <td>The message "log detection {log level}" is displayed.</td> </tr> <tr> <td>Log output disabled</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Log output enabled	The message "log detection {log level}" is displayed.	Log output disabled	Not displayed.
Setting	Display						
Log output enabled	The message "log detection {log level}" is displayed.						
Log output disabled	Not displayed.						
LOG-RESTORATION	Displays whether or not logging is output when a control condition is disabled. If so, the log level is displayed. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Log output enabled</td> <td>The message "log restoration {log level}" is displayed.</td> </tr> <tr> <td>Log output disabled</td> <td>Not displayed.</td> </tr> </tbody> </table>	Setting	Display	Log output enabled	The message "log restoration {log level}" is displayed.	Log output disabled	Not displayed.
Setting	Display						
Log output enabled	The message "log restoration {log level}" is displayed.						
Log output disabled	Not displayed.						
STATE	The control status when the high/low temperature protection control is entered is displayed.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# show config thermal ↵
# ---- transition to configure mode. ----
configure
# ---- thermal configure ----
thermal polling 1000
# ---- cpufreq high configure ----
thermal cpufreq high
enable
mode high
temperature 100.0
hysteresis 10.0
log detection warnings
log restoration notifications
state 200MHZ
exit
# ---- cpufreq low configure ----
```

```
thermal cpufreq low
enable
mode low
temperature -10.0
hysteresis 5.0
log detection warnings
log restoration notifications
state 1000MHZ
exit
# ---- mobile high configure ----
thermal mobile high
enable
mode high
temperature 100.0
hysteresis 10.0
log detection warnings
log restoration notifications
state enable
exit
# ---- interface high configure ----
thermal interface high
enable
mode high
temperature 100.0
hysteresis 10.0
log detection warnings
log restoration notifications
state 100baseT-Auto
exit
# ---- exit configure mode. ----
exit
```

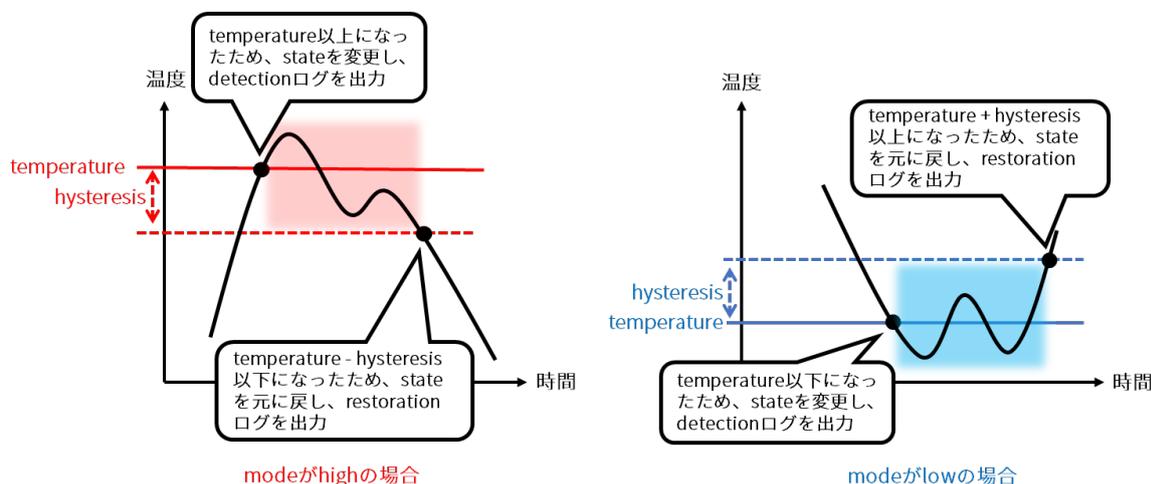
9.3.2 Set high and low temperature protection

To configure high and low temperature protection, go to the advanced configuration mode and execute the configuration command.

High and low temperature protection settings include advanced setting modes for configuring CPU operating frequency, mobile modules, and interfaces. Each of these advanced setting modes can be entered by executing the *thermal* command with options.

The settings made here are written to a configuration file.

The following figure outlines the operation and settings for high temperature (mode=high) and low temperature (mode=low).



Format

```
thermal polling POLLING
thermal < cpufreq | mobile | interface > COND-NAME
no thermal < cpufreq | mobile | interface > COND-NAME
enable
no enable
mode MODE
temperature TEMPERATURE
hysteresis HYSTERESIS
log detection LEVEL
no log detection
log restoration LEVEL
no log restoration
show config
state STATE
```

Command

Command	Contents
thermal polling	Specify the temperature polling interval (in milliseconds) in the range of 100 to 3600000 in POLLING. Temperatures are acquired at the time intervals set here and control conditions are checked.
thermal cpufreq thermal mobile thermal interface	Specify the name of the condition in COND-NAME. <ul style="list-style-type: none"> ● Executing a command in the setting mode shifts to the detailed setting mode for each function. ● COND-NAME specifies a name that uniquely identifies the control condition, using up to 32 alphanumeric and minus characters. ● Entering the "Tab" key completes the entry of the condition name.

Command	Contents						
enable	Enable control conditions.						
no enable	Disables the control condition.						
mode	<p>Specify the mode of the control condition in MODE.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>high</td> <td>Specify if this is a control condition at high temperature.</td> </tr> <tr> <td>low</td> <td>Specify if this is a control condition at low temperatures.</td> </tr> </tbody> </table>	Setting	Display	high	Specify if this is a control condition at high temperature.	low	Specify if this is a control condition at low temperatures.
Setting	Display						
high	Specify if this is a control condition at high temperature.						
low	Specify if this is a control condition at low temperatures.						
temperature	<p>Specify in TEMPERATURE the temperature (°C) at which the state is to be changed, in the range of -100.0 to 200.0. This is a required field.</p>  <ul style="list-style-type: none"> It is not possible to specify control conditions with overlapping temperature ranges for temperature and hysteresis. If low is specified for mode, a higher temperature range than the control condition of high cannot be specified. 						
hysteresis	<p>Specify a temperature hysteresis (°C) in the range of 0 to 100.0 for HYSTERESIS.</p>  <ul style="list-style-type: none"> If "high" is specified for mode, when the temperature falls below "temperature - hysteresis", it is out of the control condition range. When "low" is specified for mode, the temperature is out of the control condition range when the temperature becomes "temperature + hysteresis" or higher. 						
log	<p>Enables the specified log output.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>destination</td> <td>Specify a Syslog level in LEVEL to enable log output when a control condition occurs.</td> </tr> <tr> <td>restoration</td> <td>Specify a Syslog level for LEVEL to enable log output when recovering from a control condition in progress.</td> </tr> </tbody> </table>  <p>The following Syslogs can be specified</p> <ul style="list-style-type: none"> emergencies alerts criticals errors warnings notifications informational debugging  <p>When a control condition is enabled/disabled, the following log is output:</p> <ul style="list-style-type: none"> When a control condition is activated: COND-NAME is active When a control condition is disabled: COND-NAME is inactive 	Setting	Display	destination	Specify a Syslog level in LEVEL to enable log output when a control condition occurs.	restoration	Specify a Syslog level for LEVEL to enable log output when recovering from a control condition in progress.
Setting	Display						
destination	Specify a Syslog level in LEVEL to enable log output when a control condition occurs.						
restoration	Specify a Syslog level for LEVEL to enable log output when recovering from a control condition in progress.						

Command	Contents																																				
no log	<p>Disables the specified log output.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>display</th> </tr> </thead> <tbody> <tr> <td>destination</td> <td>Disables log output when a control condition occurs.</td> </tr> <tr> <td>restoration</td> <td>Disables log output when a control condition is recovered from occurring.</td> </tr> </tbody> </table>	Setting	display	destination	Disables log output when a control condition occurs.	restoration	Disables log output when a control condition is recovered from occurring.																														
Setting	display																																				
destination	Disables log output when a control condition occurs.																																				
restoration	Disables log output when a control condition is recovered from occurring.																																				
show config	<p>Displays settings for high and low temperature protection.</p> <p>➔ Refer to " 9.3.1 Display high and low temperature protection settings " for more information.</p>																																				
state	<p>Specifies the state when the control condition is in range. The values that can be set vary depending on which function is in advanced setting mode.</p> <ul style="list-style-type: none"> ● For CPU operating frequency <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>200 MHZ</td> <td>Set the CPU operating frequency to 200 MHZ fixed.</td> </tr> <tr> <td>250 MHZ</td> <td>Set the CPU operating frequency to 250 MHZ fixed.</td> </tr> <tr> <td>500 MHZ</td> <td>Set the CPU operating frequency to 500 MHZ fixed.</td> </tr> <tr> <td>1000 MHZ</td> <td>Set the CPU operating frequency to 1000 MHZ fixed.</td> </tr> <tr> <td>ondemand</td> <td>Dynamically change CPU operating frequency based on CPU load status.</td> </tr> </tbody> </table> <p> AI Edge Gateway does not support specification of CPU operating frequency.</p> <ul style="list-style-type: none"> ● For mobile modules <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the mobile module.</td> </tr> <tr> <td>disable</td> <td>Disable the mobile module.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> ● For interface <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>10baseT-Half</td> <td>Set the mode to 10baseT-Half.</td> </tr> <tr> <td>10baseT-Full</td> <td>Set the mode to 10baseT-Full.</td> </tr> <tr> <td>100baseT-Auto</td> <td>Set the mode to 100baseT-Auto.</td> </tr> <tr> <td>100baseT-Half</td> <td>Set the mode to 100baseT-Half.</td> </tr> <tr> <td>100baseT-Full</td> <td>Set the mode to 100baseT-Full.</td> </tr> <tr> <td>1000baseT-Auto</td> <td>Set the mode to 1000baseT-Auto.</td> </tr> <tr> <td>1000baseT-Full</td> <td>Set the mode to 1000baseT-Full.</td> </tr> <tr> <td>disable</td> <td>Disables the interface.</td> </tr> </tbody> </table>	Setting	Contents	200 MHZ	Set the CPU operating frequency to 200 MHZ fixed.	250 MHZ	Set the CPU operating frequency to 250 MHZ fixed.	500 MHZ	Set the CPU operating frequency to 500 MHZ fixed.	1000 MHZ	Set the CPU operating frequency to 1000 MHZ fixed.	ondemand	Dynamically change CPU operating frequency based on CPU load status.	Setting	Contents	enable	Enable the mobile module.	disable	Disable the mobile module.	Setting	Contents	10baseT-Half	Set the mode to 10baseT-Half.	10baseT-Full	Set the mode to 10baseT-Full.	100baseT-Auto	Set the mode to 100baseT-Auto.	100baseT-Half	Set the mode to 100baseT-Half.	100baseT-Full	Set the mode to 100baseT-Full.	1000baseT-Auto	Set the mode to 1000baseT-Auto.	1000baseT-Full	Set the mode to 1000baseT-Full.	disable	Disables the interface.
Setting	Contents																																				
200 MHZ	Set the CPU operating frequency to 200 MHZ fixed.																																				
250 MHZ	Set the CPU operating frequency to 250 MHZ fixed.																																				
500 MHZ	Set the CPU operating frequency to 500 MHZ fixed.																																				
1000 MHZ	Set the CPU operating frequency to 1000 MHZ fixed.																																				
ondemand	Dynamically change CPU operating frequency based on CPU load status.																																				
Setting	Contents																																				
enable	Enable the mobile module.																																				
disable	Disable the mobile module.																																				
Setting	Contents																																				
10baseT-Half	Set the mode to 10baseT-Half.																																				
10baseT-Full	Set the mode to 10baseT-Full.																																				
100baseT-Auto	Set the mode to 100baseT-Auto.																																				
100baseT-Half	Set the mode to 100baseT-Half.																																				
100baseT-Full	Set the mode to 100baseT-Full.																																				
1000baseT-Auto	Set the mode to 1000baseT-Auto.																																				
1000baseT-Full	Set the mode to 1000baseT-Full.																																				
disable	Disables the interface.																																				
no thermal cpufreq no thermal mobile no thermal interface	Deletes a control condition by specifying the condition name in COND-NAME.																																				
exit	Exit the detailed setting mode and enter the setting mode.																																				

Execution example

設定モード

```
amnimo(cfg)# thermal polling 1000 ↵

amnimo(cfg)# thermal cpufreq high↵ ← Go to detailed CPU operating frequency setting mode
amnimo(cfg-th-cpu-high)# enable ↵
amnimo(cfg-th-cpu-high)# mode high ↵
amnimo(cfg-th-cpu-high)# temperature 100.0 ↵
amnimo(cfg-th-cpu-high)# hysteresis 10.0 ↵
amnimo(cfg-th-cpu-high)# log detection warnings ↵
amnimo(cfg-th-cpu-high)# log restoration notifications ↵
amnimo(cfg-th-cpu-high)# state ondemand ↵
amnimo(cfg-th-cpu-high)# exit ↵

amnimo(cfg)# thermal mobile high↵ ← Go to mobile advanced configuration mode
amnimo(cfg-th-mob-high)# enable ↵
amnimo(cfg-th-mob-high)# mode high ↵
amnimo(cfg-th-mob-high)# temperature 100.0 ↵
amnimo(cfg-th-mob-high)# hysteresis 10.0 ↵
amnimo(cfg-th-mob-high)# log detection warnings ↵
amnimo(cfg-th-mob-high)# log restoration notifications ↵
amnimo(cfg-th-mob-high)# state disable ↵
amnimo(cfg-th-mob-high)# exit ↵

amnimo(cfg)# thermal interface high↵ ← Go to detailed interface configuration mode
amnimo(cfg-th-if-high)# enable ↵
amnimo(cfg-th-if-high)# mode high ↵
amnimo(cfg-th-if-high)# temperature 100.0 ↵
amnimo(cfg-th-if-high)# hysteresis 10.0 ↵
amnimo(cfg-th-if-high)# log detection warnings ↵
amnimo(cfg-th-if-high)# log restoration notifications ↵
amnimo(cfg-th-if-high)# state 100baseT-Auto ↵
amnimo(cfg-th-if-high)# exit ↵
```

9.4 Check network status

If there is a possible problem with the network, it examines information such as reachability, routes, destinations, and contents of communications.

9.4.1 Examine network reachability



To check the reachability of a network, run the *ping* command.

Format

```
ping <DEST_IP_ADDR> [ ipver <v4 | v6> ] [ repeat REPEAT ] [ size SIZE ] [ interval INTERVAL ] [ src SRC_IP_ADDR ] [ tos TOS ] [ pmtud <do | want | dont> ] [ pattern PATTERN ] [ ttl TTL ] [ ttl ]
```

Setting items

Item	Contents								
DEST_IP_ADDR	Specify the IP address of the ping destination. This is a required field.								
ipver (computer security protocol)	Specifies the version of the Internet Protocol. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>v4</td> <td>Use IPv4 only. This is set by default.</td> </tr> <tr> <td>v6</td> <td>Use IPv6 only.</td> </tr> </tbody> </table>	Setting	Display	v4	Use IPv4 only. This is set by default.	v6	Use IPv6 only.		
Setting	Display								
v4	Use IPv4 only. This is set by default.								
v6	Use IPv6 only.								
repeat	Specify the number of pings to REPEAT. If repeat is omitted, , a permanent ping will be sent.								
size	Specify the ping transmit packet size in the range of 0 to 65507 for SIZE. The default setting is "64".								
interval	Specify the interval between ping transmissions in the range of 1 to 3600 for INTERVAL. The default setting is "1".								
src	Specify the source IP address in SRC_IP_ADDR. You can also specify an interface or FQDN. By default, it is set to its own address.								
tos	Specify the ToS (Type of Service) field in the TOS as a hexadecimal number. The default setting is "0".								
pmtud	Configure the Path MTU Discovery execution settings. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>do</td> <td>Pragmentation is prohibited. DF (Don't fragment) is set.</td> </tr> <tr> <td>want</td> <td>The minimum MTU size on the route is detected by Path MTU Discovery and if it is larger than that size, it is fragmented. It is set by default.</td> </tr> <tr> <td>dont</td> <td>No pragmentation is prohibited. DF (Don't fragment) is not set.</td> </tr> </tbody> </table>	Setting	Display	do	Pragmentation is prohibited. DF (Don't fragment) is set.	want	The minimum MTU size on the route is detected by Path MTU Discovery and if it is larger than that size, it is fragmented. It is set by default.	dont	No pragmentation is prohibited. DF (Don't fragment) is not set.
Setting	Display								
do	Pragmentation is prohibited. DF (Don't fragment) is set.								
want	The minimum MTU size on the route is detected by Path MTU Discovery and if it is larger than that size, it is fragmented. It is set by default.								
dont	No pragmentation is prohibited. DF (Don't fragment) is not set.								
pattern	Specify the data pattern of the packet to be specified in 16 bytes in the range of 0x0 to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (hexadecimal) in PATTERN. It is used to find data dependency problems on the network.								
ttl	Specify a Time to Live (TTL) value for TTL.								

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ ping 192.168.0.106 repeat 10 size 1472 ↵
PING 192.168.0.106 (192.168.0.106) 1472(1500) bytes of data.
1480 bytes from 192.168.0.106: icmp_seq=1 ttl=64 time=0.467 ms
1480 bytes from 192.168.0.106: icmp_seq=2 ttl=64 time=0.370 ms
1480 bytes from 192.168.0.106: icmp_seq=3 ttl=64 time=0.365 ms
1480 bytes from 192.168.0.106: icmp_seq=4 ttl=64 time=0.358 ms
1480 bytes from 192.168.0.106: icmp_seq=5 ttl=64 time=0.348 ms
1480 bytes from 192.168.0.106: icmp_seq=6 ttl=64 time=0.356 ms
1480 bytes from 192.168.0.106: icmp_seq=7 ttl=64 time=0.351 ms
1480 bytes from 192.168.0.106: icmp_seq=8 ttl=64 time=0.347 ms
1480 bytes from 192.168.0.106: icmp_seq=9 ttl=64 time=0.366 ms
1480 bytes from 192.168.0.106: icmp_seq=10 ttl=64 time=0.353 ms

--- 192.168.0.106 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9207ms
rtt min/avg/max/mdev = 0.347/0.368/0.467/0.034 ms
```

9.4.2 Examine network routes



To examine the network routes, run the *tracert* command.

Format (Edge Gateway, IoT Router)



```
tracert <DEST_IP_ADDR> [ipver <v4 | v6> ] [ first-hop FIRST-HOP max-hop MAX-HOP ] [ no
resolve ] [ src SRC_IP_ADDR ] [ tos TOS ] [ queries queries ] [ protocol < icmp | udp[:POR
T] | tcp[:PORT] | any[:PORT] > ] [ timeout TIMEOUT ] [ timeout ]
```

Format (Compact Router)



```
tracert <DEST_IP_ADDR> [ipver <v4 | v6> ] [ first-hop FIRST-HOP max-hop MAX-HOP ] [ no
resolve ] [ src SRC_IP_ADDR ] [ tos TOS ] [ queries QUERIES ] [ protocol < icmp | any[:POR
T] > ] [ timeout TIMEOUT ] [ timeout ]
```

Setting items

Item	Contents						
DEST_IP_ADDR	Specify the IP address of the target host for route search. This is a required field.						
ipver (computer security protocol)	Specifies the version of the Internet Protocol. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>v4</td> <td>Use IPv4 only. This is set by default.</td> </tr> <tr> <td>v6</td> <td>Use IPv6 only.</td> </tr> </tbody> </table>	Setting	Display	v4	Use IPv4 only. This is set by default.	v6	Use IPv6 only.
Setting	Display						
v4	Use IPv4 only. This is set by default.						
v6	Use IPv6 only.						
first-hop	Specify the initial TTL hop in the range of 1 to 254 for FIRST-HOP. The default setting is "1".						
max-hop	Specify the maximum number of hops, in the range of 2 to 255, for MAX-HOP. The default setting is "30". If FIRST-HOP is specified, a number greater than FIRST-HOP must be specified.						
noresolve	Specify if IP address name resolution is not used. By default, it is configured to perform name resolution.						
src	Specify the source IP address in SRC_IP_ADDR. You can also specify an interface or FQDN. By default, it is set to its own address.						
tos	Specify the ToS (Type of Service) field in the TOS as a hexadecimal number. The default setting is "0".						
queries	Specify the number of probes per hop in the range of 1 to 9. The default setting is "3".						

Item	Contents										
protocol	<p>Specifies the protocol to be used for traceroute. The default setting is "udp:33434-33435".</p> <p>The port number can be specified following ":". A range of ports can also be specified by including a "-" character. (e.g. tcp:80-1024)</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>icmp</td> <td>Specifies the ICMP protocol.</td> </tr> <tr> <td>udp[:1-65535]]</td> <td>Specifies the UDP protocol.</td> </tr> <tr> <td>tcp[:1-65535].</td> <td>Specifies the TCP protocol.</td> </tr> <tr> <td>any[:1-65535]]</td> <td>Specified without distinguishing between TCP and UDP protocols.</td> </tr> </tbody> </table> <p> On Compact Router, only icmp and any can be specified for configuration, not a range of ports.</p>	Setting	Display	icmp	Specifies the ICMP protocol.	udp[:1-65535]]	Specifies the UDP protocol.	tcp[:1-65535].	Specifies the TCP protocol.	any[:1-65535]]	Specified without distinguishing between TCP and UDP protocols.
Setting	Display										
icmp	Specifies the ICMP protocol.										
udp[:1-65535]]	Specifies the UDP protocol.										
tcp[:1-65535].	Specifies the TCP protocol.										
any[:1-65535]]	Specified without distinguishing between TCP and UDP protocols.										
timeout	<p>Specify a timeout period (s: seconds) in the range of 1s to 600s for TIMEOUT. The default setting is "5s".</p>										

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード
管理者モード
設定モード

```

amnimo$ traceroute www.google.com protocol udp:80 tos 0xA0 first-hop 1 max-hop 255 que
ries 5 ↵
traceroute to www.google.com (172.217.26.4), 255 hops max, 60 byte packets
 1 _gateway (172.16.10.1) 1.257 ms 1.381 ms 1.304 ms 1.389 ms 1.347 ms
 2 ex10.example.or.jp (124.155.80.121) 28.621 ms 29.186 ms 29.163 ms 29.125 ms 29.199 m
s
 3 ex10-v1.example.or.jp (124.155.80.69) 29.389 ms 29.390 ms 29.548 ms 29.260 ms 29.458
ms
(omitted)
 8 001.example.or.jp (202.224.51.158) 36.211 ms 38.756 ms 36.620 ms 36.462 ms 36.219 ms
 9 209.85.174.82 (209.85.174.82) 36.153 ms 39.213 ms 40.888 ms 40.953 ms 40.916 ms
10 108.170.243.67 (108.170.243.67) 41.282 ms 108.170.243.131 (108.170.243.131) 41.046
ms 108.170.243.67 (108.170.243.67) 40.703 ms 108.170.243. 35 (108.170.243.35) 38.841 m
s 108.170.243.131 (108.170.243.131) 39.662 ms
11 172.253.70.43 (172.253.70.43) 37.652 ms 40.043 ms 61.698 ms 40.725 ms 108.177.3.255
(108.177.3.255) 40.599 ms
12 72.14.234.66 (72.14.234.66) 39.938 ms 39.947 ms 209.85.244.63 (209.85.244.63) 46.98
0 ms 72.14.234.66 (72.14.234.66) 45.782 ms 209.85.244.3 (209 .85.244.3) 46.583 ms
13 108.170.242.161 (108.170.242.161) 45.936 ms 108.170.242.193 (108.170.242.193) 46.88
3 ms 108.170.242.161 (108.170.242.161) 46.400 ms 46.024 ms 108.170.242.193 (108.170.24
2.193) 29.662 ms
14 66.249.95.89 (66.249.95.89) 26.951 ms 26.667 ms 28.706 ms 66.249.95.155 (66.249.95.
155) 27.995 ms 28.408 ms
15 nrt20s02-in-f4.1e100.net (172.217.26.4) 28.598 ms 28.480 ms 28.358 ms 24.998 ms 25.
580 ms

```

9.4.3 Find out which MAC address corresponds to an IP address



To retrieve information about the ARP table, which uses the Address Resolution Protocol (ARP) and manages the association between IP addresses and MAC addresses, use the `show arp` command.

■ Display ARP table

To view the ARP table, run the `show arp` command.

Format

```
show arp
```

Output format (Edge Gateway, IoT Router)



```
Address HWtype HWaddress Flags Mask Iface
IP-ADDRESS HW-TYPE MAC-ADDRESS FLAGS-MASK IFACE
IP-ADDRESS HW-TYPE MAC-ADDRESS FLAGS-MASK IFACE
IP-ADDRESS HW-TYPE MAC-ADDRESS FLAGS-MASK IFACE
(Omitted.)
```

Output format (Compact Router)



```
? (IP-ADDRESS) at MAC-ADDRESS [ether] on IFACE
? (IP-ADDRESS) at MAC-ADDRESS [ether] on IFACE
? (IP-ADDRESS) at MAC-ADDRESS [ether] on IFACE
(Omitted.)
```

Output item

Item	Contents														
IP-ADDRESS	The IP addresses registered in the ARP table are displayed.														
HW-TYPE	The hardware type of the network interface is displayed.														
MAC-ADDRESS	The MAC address corresponding to the IP address is displayed.														
FLAG-MASK	<p>A flag mask indicating the MAC address entry status is displayed.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>C</td> <td>Entry Completed</td> </tr> <tr> <td></td> <td> If the table is not reused for a certain period of time, it is subject to deletion from the table.</td> </tr> <tr> <td>M</td> <td>Permanent entry completed</td> </tr> <tr> <td>P</td> <td>Public Entry</td> </tr> <tr> <td>A</td> <td>Entry status automatically added</td> </tr> <tr> <td>!</td> <td>non-responsive address</td> </tr> </tbody> </table>	Setting	Display	C	Entry Completed		 If the table is not reused for a certain period of time, it is subject to deletion from the table.	M	Permanent entry completed	P	Public Entry	A	Entry status automatically added	!	non-responsive address
Setting	Display														
C	Entry Completed														
	 If the table is not reused for a certain period of time, it is subject to deletion from the table.														
M	Permanent entry completed														
P	Public Entry														
A	Entry status automatically added														
!	non-responsive address														
IFACE	The network interface is displayed.														

Execution example (Edge Gateway, IoT Router)

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show arp ←
Address HWtype HWaddress Flags Mask Iface
192.168.0.204 ether 00:11:22:33:44:55 C eth0
192.168.0.205 ether 00:11:22:33:44:56 C eth0
```

Execution example (Compact Router)

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ show arp ←
? (192.168.0.204) at 00:11:22:33:44:55 [ether] on eth0
? (192.168.0.205) at 00:11:22:33:44:56 [ether] on eth0
```

9.4.4 Control ARP table information



Registers information in the ARP table and deletes information from the ARP table.

Register in the ARP table

To register information in the ARP table, run the *arp* command.

Format

```
arp <IP-ADDRESS> <MAC-ADDRESS>
```

Setting items

Item	Contents
IP-ADDRESS	Specifies the IP address to be registered in the ARP table.
MAC-ADDRESS	Specify the MAC address to be mapped to the IP address.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ arp 192.168.0.206 00:11:22:33:44:57 ↵
```

Delete from ARP table

To remove information from the ARP table, execute the *no arp* command.

Format

```
no arp <IP-ADDRESS>.
```

Setting items

Item	Contents
IP-ADDRESS	Specifies IP addresses to be removed from the ARP table.

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.

ユーザーモード 管理者モード 設定モード

```
amnimo$ no arp 192.168.0.204 ↵
```

9.4.5 Dump packets to examine communication contents



To dump packets and examine their communication contents, run the *packet-dump* command.

Format (AI Edge Gateway, Edge Gateway, IoT Router)



```
packet-dump <iface IFNAME > [file PCAP-FILE ] [src IP-ADDRESS | dst IP-ADDRESS | proto
col [not] <udp | tcp | all> ] [port PORT_NO ] [[rotate SIZE:NUM] [ limit-size LIMIT_SIZ
E ]][ limit-time LIMIT_TIME ] [silent < true | false > ]
```

Format (Compact Router)



```
packet-dump <iface IFNAME > [src IP-ADDRESS | dst IP-ADDRESS | protocol [not] <udp | t
cp | all> ] [port PORT_NO ]
```

Setting items

Item	Contents								
iface	<p>As a filter, specify a network interface in IFNAME. The interface names that can be specified are as follows eth0, lan<0-3>, br<0-9>, ecm0, ppp<0-9>, tun<0-9>, tap<0-9></p>  <ul style="list-style-type: none"> ● This function is required. ● Only one interface can be specified. 								
file	<p>Specify in PCAP-FILE the pcap format file in which the captures will be saved.</p>  <ul style="list-style-type: none"> ● The file is created under the /tmp/packet-dump directory. ● The maximum size of a file that can be saved with this function is 100Mbytes and the maximum number of files is 999. ● Since the file size increases according to the log volume, care should be taken not to overwhelm the size of tmpfs by factors other than this function. The results of the previous dump remain intact, so if they are not needed, delete them to increase the remaining space in tmpfs as much as possible. <p>➔ “ 9.4.7 Delete the results of dumping packets “</p> <ul style="list-style-type: none"> ● Cannot be used with Compact Router. 								
src	Specify the source IP address in IP-ADDRESS as the filter.								
dst	Specify the destination IP address in IP-ADDRESS as the filter.								
protocol	<p>Specifies the protocol as a filter; set the port number in the range of 0 to 65535 in PORT_NO.</p> <table border="1" data-bbox="336 1608 1347 1843"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>udp</td> <td>Specifies the UDP protocol. You can also specify "protocol not tcp".</td> </tr> <tr> <td>tcp</td> <td>Specifies the TCP protocol. You can also specify "protocol not udp".</td> </tr> <tr> <td>all</td> <td>Specify both UDP and TCP protocols.</td> </tr> </tbody> </table>	Setting	Display	udp	Specifies the UDP protocol. You can also specify "protocol not tcp".	tcp	Specifies the TCP protocol. You can also specify "protocol not udp".	all	Specify both UDP and TCP protocols.
Setting	Display								
udp	Specifies the UDP protocol. You can also specify "protocol not tcp".								
tcp	Specifies the TCP protocol. You can also specify "protocol not udp".								
all	Specify both UDP and TCP protocols.								
port	As a filter, specify a port number in PORT_NO.								

Item	Contents						
rotate	<p>SIZE:NUM is specified when pcap files are to be rotated and saved. The numbers 0, 1, 2, 3... are added to the end of the rotated file name.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>SIZE</td> <td>Specify the size per file in the range of 1 to 100 (in Mbytes).</td> </tr> <tr> <td>NUM</td> <td>Specify the number of files to rotate in the range of 1 to 100.</td> </tr> </tbody> </table> <p> Cannot be used with Compact Router.</p>	Setting	Display	SIZE	Specify the size per file in the range of 1 to 100 (in Mbytes).	NUM	Specify the number of files to rotate in the range of 1 to 100.
Setting	Display						
SIZE	Specify the size per file in the range of 1 to 100 (in Mbytes).						
NUM	Specify the number of files to rotate in the range of 1 to 100.						
limit-size	<p>Specify in LIMIT_SIZE the size (in Mbytes) from 1 to 100 at which file capture will be automatically stopped.</p> <p> Cannot be used with Compact Router.</p>						
limit-time	<p>If you want to rotate files when the time limit is exceeded, specify in LIMIT_TIME a time (in seconds per file) from 60 to 3600 seconds to automatically stop file capture.</p> <p> Cannot be used with Compact Router.</p>						
silent	<p>Specifies that the pcap file be recorded and the packet log be displayed on the console at the same time.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>true</td> <td>Records pcap files and displays packet logs on the console at the same time.</td> </tr> <tr> <td>false</td> <td>Do not display the packet log on the console at the same time as recording the pcap file.</td> </tr> </tbody> </table> <p> Cannot be used with Compact Router.</p>	Setting	Display	true	Records pcap files and displays packet logs on the console at the same time.	false	Do not display the packet log on the console at the same time as recording the pcap file.
Setting	Display						
true	Records pcap files and displays packet logs on the console at the same time.						
false	Do not display the packet log on the console at the same time as recording the pcap file.						



If both rotate and limit-size are not set, the default value is set to rotate 10:10 (10 Mbytes per file, 10 rotated files).

Execution example

In the packets on the br0 side, get the packets on TCP port 80 and save them in dumpfile.pcap as a file of maximum 1Mbyte in 3 rotating files. The input and output of the command is the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# packet-dump interface br0 file dumpfile.pcap protocol tcp port 80 rotate 1:3 ↵
```

Capture results are saved as follows

```
admin@amnimo$ ls -lh /tmp/packet-dump ↵
total 2.7M
-rw----- 1 root root 1001K Aug 4 14:38 dumpfile_00001_20210804143821.pcap
-rw----- 1 root root 1001K Aug 4 14:39 dumpfile_00002_20210804143847.pcap
-rw----- 1 root root 751K Aug 4 14:39 dumpfile_00003_20210804143914.pcap
```

9.4.6 Display the results of dumping packets



To view the results of dumping packets, run the *show packet-dump* command.



This function is not available on Compact Router.

Format

```
show packet-dump file <PCAP-FILE>.
```

Setting items

Item	Contents
PCAP-FILE	Specifies the pcap format file in which the capture was saved.

Execution example

Displays the contents of one file of the dump result of the example run in "9.4.5 Dump packets to examine communication contents". Command input and output are the same in administrator mode and configuration mode. The following is an example of administrator mode execution.

管理者 モード 設定 モード

```
amnimo# show packet-dump file dumpfile_00001_20210804143821.pcap ↵
Running as user "root" and group "root". This could be dangerous.
  1 0.000000000 192.168.0.1 → 192.168.0.254 UDP 108 31234 → 22 Len=66
  2 0.038015493 192.168.0.254 → 192.168.0.1 UDP 117 22 → 31234 Len=75
  3 0.059774154 192.168.0.254 → 192.168.0.1 UDP 127 22 → 31234 Len=85
  4 0.103200831 192.168.0.254 → 192.168.0.1 UDP 123 22 → 31234 Len=81
  5 0.132931219 192.168.0.254 → 192.168.0.1 UDP 763 22 → 31234 Len=721
  6 0.134194090 192.168.0.1 → 192.168.0.254 UDP 120 31234 → 22 Len=78
  7 0.135167345 192.168.0.254 → 192.168.0.1 UDP 123 22 → 31234 Len=81
      .
      .
      .
```

9.4.7 Delete the results of dumping packets



To delete the results of a packet dump, execute the *no packet-dump* command.



This function is not available on Compact Router.

Format

```
no packet-dump [file PCAP-FILE].
```

Setting items

Item	Contents				
file	Specify and delete the pcap format file in which the capture was saved.  If not specified, all packet files are deleted.				
	<table border="1"><thead><tr><th>Setting</th><th>Contents</th></tr></thead><tbody><tr><td>PCAP-FILE</td><td>Name of the pcap format file in which the capture was saved</td></tr></tbody></table>	Setting	Contents	PCAP-FILE	Name of the pcap format file in which the capture was saved
Setting	Contents				
PCAP-FILE	Name of the pcap format file in which the capture was saved				

Execution example 1

Deletes one file from the dump result of the example in " 9.4.5 Dump packets to examine communication contents". Command input and output are the same in administrator mode and configuration mode. The following is an example of execution in administrator mode.

管理者 モード 設定 モード

```
amnimo# no packet-dump file dumpfile_00001_20210804143821.pcap ↵  
Are you sure you want to delete dumpfile_00001_20210804143821.pcap (y/N): ← Enter y
```

Execution example 2

Deletes all dump results in the example execution of " 9.4.5 Dump packets to examine communication contents". Command input and output are the same in administrator mode and configuration mode. The following is an example of execution in administrator mode.

管理者 モード 設定 モード

```
amnimo# no packet-dump ↵  
Are you sure you want to delete ALL pcap files? (y/N): ← Enter y
```

Chap 10. Applications for this product

This chapter describes commands for managing the Device Management System (DMS) and Nx Witness.

10.1 Configure DMS settings.



When using the Device Management System (DMS) to monitor and maintain a remote Edge Gateway series, the CLI is used to view and configure DMS information.

10.1.1 Display DMS status

To view the status of DMS services, run the *show service dms* command.

Format

```
show service dms
```

Output Format

```
SERVICE-STATUS
```

Output item

Item	Contents						
SERVICE-STATUS	The status of the DMS service is displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Running</td> <td>The message "active" will be displayed.</td> </tr> <tr> <td>Stopped</td> <td>The message "inactive" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Running	The message "active" will be displayed.	Stopped	The message "inactive" is displayed.
Setting	Display						
Running	The message "active" will be displayed.						
Stopped	The message "inactive" is displayed.						

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.



```
amnimo$ show service dms ↵
active
```

10.1.2 Control DMS

To start, stop, or restart DMS services, run the *service dms* command with options.

Format

```
service dms <start | stop | restart>
```

Output item

Item	Contents
start	Start the DMS service.
stop	Stop the DMS service.
restart	Restart the DMS service.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# service dms start ↵
amnimo# service dms stop ↵
amnimo# service dms restart ↵
```

10.1.3 Display DMS settings

To view the DMS configuration, run the *show config dms* command.

Format

```
show config dms
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- dms configure ----
dms
ENABLE
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLE	Information is displayed when DMS is enabled/disabled.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# show config dms ↵
# ---- transition to configure mode ----
configure
# ---- dms configure ----
dms
enable
exit
# ---- exit configure mode ----
exit
```

10.1.4 Configure DMS settings.

To configure the DMS, enter the advanced configuration mode and execute the configuration commands.

The settings made here are written to a configuration file.

Format

```
dms
enable
no enable
exit
```

Command

Command	Contents
dms	Execute DMS configuration commands.  Executing a command in the setting mode shifts to the detailed setting mode.
enable	Start the DMS service.
no enable	Stop the DMS service.
exit	Exit the DMS advanced setting mode and enter the setting mode.

Execution example

設定モード

```
amnimo(cfg)# dms ↵
amnimo(cfg-dms)# enable ↵
amnimo(cfg-dms)# no enable ↵
amnimo(cfg-dms)# exit ↵
```

10.2 Configure Nx Witness settings.



When using Nx Witness as a management tool for network cameras, the CLI is used to view and configure Nx Witness information.



Nx Witness settings must be saved at the Edge Gateway.

→ How to save your Nx Witness settings in " 10.2.4 Configure Nx Witness settings. ", " 10.2.5 Write Nx Witness settings" for more information on how to configure Nx Witness.

If you do not save your settings, camera settings and other settings may disappear and revert to their original settings. Therefore, if you change the settings of Nx Witness, be sure to save the Nx Witness settings. Also, by saving the settings, the settings will be reflected correctly when starting from the redundant area side.

10.2.1 Display Nx Witness status

To view the status of Nx Witness services, run the ***show service nxwitness*** command.

Format

```
show service nxwitness
```

Output Format

```
SERVICE-STATUS
```

Output item

Item	Contents						
SERVICE-STATUS	The status of the Nx Witness service is displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>in operation</td> <td>The message "active" will be displayed.</td> </tr> <tr> <td>at a standstill</td> <td>The message "inactive" is displayed.</td> </tr> </tbody> </table>	Setting	Display	in operation	The message "active" will be displayed.	at a standstill	The message "inactive" is displayed.
Setting	Display						
in operation	The message "active" will be displayed.						
at a standstill	The message "inactive" is displayed.						

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.



```
amnimo$ show service nxwitness ↵
active
```

10.2.2 Controlling Nx Witness

To start, stop, or restart the Nx Witness service, run the ***service nxwitness*** command with options.

Format

```
service nxwitness <start | stop | restart>
```

Output item

Item	Contents
start	Start the Nx Witness service.
stop	Stop the Nx Witness service.
restart	Restart the Nx Witness service.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# service nxwitness start ↵
amnimo# service nxwitness stop ↵
amnimo# service nxwitness restart ↵
```

10.2.3 View Nx Witness settings

To view the Nx Witness configuration, run the *show config nxwitness* command.

Format

```
show config nxwitness
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- nxwitness configure ----
nxwitness
ENABLE
port PORT_NUM
database DATABASE_FILE_PATH
password secret ENCRYPT-PASSWORD
exit
# ---- exit configure mode ----
exit
```

Output item

Item	Contents						
ENABLE	Information is displayed when Nx Witness is enabled/disabled. <table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
PORT_NUM	The port number configured for Nx Witness is displayed. By default, "7001" is set.						
DATABASE_FILE_PATH	The location of the database backup file is displayed. By default, "/mnt/share/nxwitness/database/file.db" is set. <div data-bbox="571 1220 646 1288" style="display: inline-block; vertical-align: middle;">  </div> If you change the location of the backup files, you must set up an area that can be accessed from both boot 0 and boot 1.						
ENCRYPT-PASSWORD	The encrypted password is displayed.						

管理者モード

```
amnimo# show config nxwitness ↵
# ---- transition to configure mode ----
configure
# ---- nxwitness configure ----
nxwitness
enable
port 7001
database /mnt/share/nxwitness/database/file.db
password secret 1sxWjNj/NBbdEfGFmP6vrw==
exit
# ---- exit configure mode ----
exit
```

設定モード

```
amnimo(cfg)# show config nxwitness ↵
# ---- nxwitness configure ----
nxwitness (abbreviated)
enable
port 7001
database /mnt/share/nxwitness/database/file.db
password secret 1sxWjNj/NBbdEfGFmP6vrw==
exit
```



Running the *show config* command in the advanced configuration mode of Nx Witness will display the same information as in the configuration mode.

```
amnimo(cfg)# nxwitness↵    ← Go to NxWitness advanced configuration mode
amnimo(cfg-nxwitness)# show config ↵
enable                      ← Same as setting mode
(Omitted.)
```

10.2.4 Configure Nx Witness settings.

To configure Nx Witness, enter the advanced configuration mode and execute the configuration command.

The settings made here are written to a configuration file.

Format

```
nxwitness
enable
no enable
password
password secret ENCRYPT-PASSWORD
port PORT_NUM
database DATABASE_FILE_PATH
exit
```

Command

Command	Contents
nxwitness	Execute the Nx Witness configuration command.  Executing a command in the setting mode shifts to the detailed setting mode.
enable	Start the Nx Witness service.
no enable	Stop the Nx Witness service.
password	Save the admin password set for Nx Witness. Used for functions such as writing Nx Witness settings and reading Nx Witness settings. If the password change is successful, the encrypted password is saved.
password secret	Specify an encrypted password string in ENCRYPT-PASSWORD to update the password.
port	Saves the port number configured for Nx Witness. The default setting is "7001". Used for functions such as writing Nx Witness settings and reading Nx Witness settings.
database	Sets the location of the database backup file. By default, "/mnt/share/nxwitness/database/file.db" is set.  If you change the location of the backup files, you must set up an area that can be accessed from both boot 0 and boot 1.
exit	Exit Nx Witness advanced setting mode and enter setting mode.

Execution example

設定モード

```
amnimo(cfg)# nxwitness ↵
amnimo(cfg-nxwitness)# enable ↵
amnimo(cfg-nxwitness)# no enable ↵
amnimo(cfg-nxwitness)# password ↵
Enter new password: Enter          ← Enter password and press Enter
Retype new password:                ← Enter password again and press Enter
amnimo(cfg-nxwitness)# port 7001 ↵
amnimo(cfg-nxwitness)# database /mnt/share/nxwitness/database/file.db ↵
amnimo(cfg-nxwitness)# exit ↵
amnimo(cfg)#.
```

10.2.5 Write Nx Witness settings

Saves Nx Witness settings. Saved settings can be reflected in the system by loading the Nx Witness settings.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# config nxwitness save ↵
```

10.2.6 Load Nx Witness settings

Nx Witness settings are reflected in the system.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者 モード 設定 モード

```
amnimo# config nxwitness load ↵
```

10.3 Configure remote.it settings



When using remote.it to securely access this product from a remote location away from your PC or other devices, you can use the CLI to view, control, view and configure remote.it information and settings.

10.3.1 Display the status of remote.it

To view the status of the remote.it service, run the *show service remoteit* command.

Format

```
show service remoteit
```

Output Format

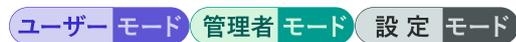
```
SERVICE-STATUS
```

Output item

Item	Contents						
SERVICE-STATUS	The status of the remote.it service is displayed.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>in operation</td> <td>The message "active" will be displayed.</td> </tr> <tr> <td>at a standstill</td> <td>The message "inactive" is displayed.</td> </tr> </tbody> </table>	Setting	Display	in operation	The message "active" will be displayed.	at a standstill	The message "inactive" is displayed.
Setting	Display						
in operation	The message "active" will be displayed.						
at a standstill	The message "inactive" is displayed.						

Execution example

Command input and output is the same in all modes. Below is an example of execution in general user mode.



```
amnimo$ show service remoteit ↵
active
```

10.3.2 Controlling remote.it

To start, stop, or restart the remote.it service, run the ***service remoteit*** command with the option

Format

```
service remoteit <start | stop | restart>
```

Output item

Item	Contents
start	Start the remote.it service.
stop	Stop the remote.it service.
restart	Restart the remote.it service.

Execution example

Command input and output are the same in administrator mode and configuration mode. An example of administrator mode execution is shown below.

管理者モード 設定モード

```
amnimo# service remoteit start ↵
amnimo# service remoteit stop ↵
amnimo# service remoteit restart ↵
```

10.3.3 View remote.it settings

To view the remote.it configuration, run the *show config remoteit* command.

Format

```
show config remoteit
```

Output Format

```
# ---- transition to configure mode ----
configure
# ---- remoteit configure ----
remoteit
ENABLED
registration REGISTRATION_CODE
exit
# ---- exit configure mode ----
Exit
```

Output item

Item	Contents						
ENABLE	Information is displayed when remote.it is enabled/disabled. <table border="1" data-bbox="448 869 1227 994"> <thead> <tr> <th>Setting</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>The message "enable" is displayed.</td> </tr> <tr> <td>Disable</td> <td>The message "no enable" is displayed.</td> </tr> </tbody> </table>	Setting	Display	Enable	The message "enable" is displayed.	Disable	The message "no enable" is displayed.
Setting	Display						
Enable	The message "enable" is displayed.						
Disable	The message "no enable" is displayed.						
registration	Displays the license key or bulk code for remote.it. REGISTRATION_CODE displays a hexadecimal string of type uuid as defined in RFC4122.  This function is available on Compact Router only.						

Execution example

管理者 モード

```
amnimo# show config remoteit ↵
# ---- transition to configure mode ----
configure
# ---- remoteit configure ----
remoteit
enable
registration 01234567-89ab-cdef-0123-456789abcdef
exit
# ---- exit configure mode ----
exit
```

```
amnimo(cfg)# show config remoteit ↵  
# ---- remoteit configure ----  
remoteit  
enable  
registration 01234567-89ab-cdef-0123-456789abcdef  
exit
```



Running the *show config* command in the advanced configuration mode of remote.it will display the same information as in the configuration mode.

```
amnimo(cfg)# remoteit↵      ← Go to remote.it advanced configuration mode  
amnimo(cfg-remoteit)# show config ↵  
enable                      ← Same as setting mode  
(Omitted.)
```

10.3.4 Configure remote.it settings

To configure remote.it, go to advanced configuration mode and execute the configuration command.

The settings made here are written to a configuration file.

Format

```
remoteit
enable
no enable
registration REGISTRATION_CODE
no registration
exit
```

Command

Command	Contents
remoteit	Execute the remote.it configuration command.  Executing a command in the setting mode will shift to the detailed setting mode.
enable	Start the remote.it service.
no enable	Stop the remote.it service.
registration	Set the license key or bulk code for remote.it. REGISTRATION_CODE is set to a hexadecimal string of type uuid as defined in RFC4122.  This function is available on Compact Router only.
no registration	Delete the configured remote.it license key or bulk code.  This function is available on Compact Router only.
exit	Exit the advanced setting mode of remote.it and enter the setting mode.

Execution example

設定モード

```
amnimo(cfg)# remoteit ↵
amnimo(cfg-remoteit)# enable ↵
amnimo(cfg-remoteit)# no enable ↵
amnimo(cfg-remoteit)# registration 01234567-89ab-cdef-0123-456789abcdef ↵
amnimo(cfg-remoteit)# no registration ↵
amnimo(cfg-remoteit)# exit ↵
```

10.4 Execute application commands



Execute commands for applications installed on the product. Enter the advanced setting mode and execute the command.



- This function is supported only for the *remoteit* command.
- This function is not available on Compact Router. (To be supported in the next version)

Format

```
execute remoteit < remoteit command >
```

Execution example

The command is executed with root privileges, so there is no need to use sudo to execute the remoteit command.

設定モード

```
amnimo(cfg)# execute remoteit version ↵  
amnimo(cfg)# execute remoteit signin ↵  
amnimo(cfg)# execute remoteit status ↵
```



After completing the various settings related to the remote.it application, execute the command to save the configuration file (config file save) and save it as the configuration of this device.

- ➔ "11.1.4 Save the configuration file "
- ➔ Please refer to the startup guide for each device for basic remote.it setup instructions.

Chap 11. external command

This chapter describes the CLI's external commands, which allow you to manipulate the product's configuration files and hardware without launching amsh.



- The IoT Router does not support operation via external commands.
- Compact Router cannot be operated by external commands.

11.1 Controlling configuration files



Setup To control the configuration file, use the **amcfg** command.

11.1.1 Basics of configuration file control commands

This section describes the basic format of the amcfg command.

Format

```
amcfg [<OPTIONS>] <COMMAND>.
```

Setting items

Item	Contents																
OPTIONS	Specify command line options.																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>-V, --verbose</td> <td>Outputs more detailed information to the console.</td> </tr> <tr> <td>-v</td> <td>Displays the version number.</td> </tr> <tr> <td>-h, --help</td> <td>Displays help information.</td> </tr> </tbody> </table>	Option	Contents	-V, --verbose	Outputs more detailed information to the console.	-v	Displays the version number.	-h, --help	Displays help information.								
	Option	Contents															
	-V, --verbose	Outputs more detailed information to the console.															
-v	Displays the version number.																
-h, --help	Displays help information.																
COMMAND	Specifies commands to control the configuration file.																
	<table border="1"> <thead> <tr> <th>Command</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>init</td> <td>Initialize the configuration file.</td> </tr> <tr> <td>load</td> <td>Loads a configuration file.</td> </tr> <tr> <td>save</td> <td>Save the configuration file.</td> </tr> <tr> <td>move</td> <td>Move the configuration file.</td> </tr> <tr> <td>copy</td> <td>Copy the configuration file.</td> </tr> <tr> <td>delete</td> <td>Delete the configuration file.</td> </tr> <tr> <td>list</td> <td>Displays a list of configuration files.</td> </tr> </tbody> </table>	Command	Contents	init	Initialize the configuration file.	load	Loads a configuration file.	save	Save the configuration file.	move	Move the configuration file.	copy	Copy the configuration file.	delete	Delete the configuration file.	list	Displays a list of configuration files.
Command	Contents																
init	Initialize the configuration file.																
load	Loads a configuration file.																
save	Save the configuration file.																
move	Move the configuration file.																
copy	Copy the configuration file.																
delete	Delete the configuration file.																
list	Displays a list of configuration files.																

11.1.2 Initialize the configuration file

To initialize the configuration file, run the **amcfg init** command.

Execution example

To initialize the configuration file, the **sudo** command must be used.

```
admin@amnimo:~# sudo amcfg init ↵
Do you want to initialize the settings?   ←Enter the "y" key followed by Enter
```



To cancel execution of the command, type Enter or press the "n" key followed by Enter.

11.1.3 Read the configuration file

To load the configuration file, run the *amcfg load* command.

Format

```
amcfg load [FILENAME].
```

Setting items

Item	Contents
FILE	<p>Enter the name of the configuration file.</p> <ul style="list-style-type: none"> ● A maximum file name of 32 characters can be set. ● The characters that can be used as file names are "alphanumeric characters" (case-sensitive) and "-" (hyphen) (cannot be used at the beginning or end). <p> If you omit entering a configuration file name, "startup-config" will be set.</p>

Execution example

To read the configuration file, you must use the *sudo* command.

```
admin@amnimo:~# sudo amcfg load startup-config2 ↵
```

11.1.4 Save the configuration file

To save the configuration file, run the *amcfg save* command.

Format

```
amcfg save [FILENAME].
```

Setting items

Item	Contents
FILENAME	<p>Enter the name of the configuration file.</p> <ul style="list-style-type: none"> ● A maximum file name of 32 characters can be set. ● The characters that can be used as file names are "alphanumeric characters" (case-sensitive) and "-" (hyphen) (cannot be used at the beginning or end). <p> If you omit entering a configuration file name, "startup-config" will be set.</p>

Execution example

To save the configuration file, you must use the *sudo* command.

```
admin@amnimo:~# sudo amcfg save startup-config2 ↵
```

11.1.5 Rename the configuration file

To rename the configuration file, run the *amcfg move* command.

Format

```
amcfg move SRC-FILENAME DST-FILENAME
```

Setting items

Item	Contents
SRC-FILENAME	Enter the name of the configuration file before the change.
DST-FILENAME	Enter the name of the modified configuration file.

Execution example

To rename the configuration file, you must use the *sudo* command.

```
admin@amnimo:~# sudo amcfg move backup-20200101 backup-20200101-2 ↵
```

11.1.6 Copy the configuration file

To copy the configuration file, run the *amcfg copy* command.

➔ For more information on the setting items, please refer to "11.1.4 Save the configuration file".

Format

```
amcfg copy SRC-FILENAME DST-FILENAME
```

Execution example

To copy the configuration file, you must use the *sudo* command.

```
admin@amnimo:~# sudo amcfg copy startup-config_2 backup-20200101-3 ↵
```

11.1.7 Delete configuration files

To delete a configuration file, run the *amcfg delete* command.

➔ For more information on the setting items, please refer to " 11.1.4 Save the configuration file".

Format

```
amcfg delete [FILE].
```

Execution example

To delete a configuration file, you must use the *sudo* command.

```
admin@amnimo:~# sudo amcfg delete startup-config_2 ↵
Are you sure you want to delete the startup-config_2 file?    ←Enter the "y" key followed by Enter
```

11.1.8 Display a list of configuration files

To view a list of configuration files, run the *amcfg list* command.

Execution example

To view a list of configuration files, you must use the *sudo* command.

```
admin@amnimo:~# sudo amcfg list ↵
startup-config 2020-01-02T00:00:00+09:00
backup-20200101 2020-01-01T00:00:00+09:00
backup-20200202 2020-01-02T00:00:00Z+09:00
```

11.2 Control hardware

To control the hardware, use the *amctrl* command.

11.2.1 Basics of Hardware Control Commands



This section describes the basic format of the amctrl command.

Format

```
amctrl COMMAND [--help].
```

Setting items

Item	Contents																										
COMMAND	<p>Specifies commands to control hardware.</p> <table border="1"> <thead> <tr> <th>Command</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>information</td> <td>Displays hardware information such as device-specific information.</td> </tr> <tr> <td>dip-switch</td> <td>Displays the status of the DIP switches.</td> </tr> <tr> <td>push-switch</td> <td>Displays the status of the PUSH switch.</td> </tr> <tr> <td>boot</td> <td>Controls the startup area.</td> </tr> <tr> <td>led</td> <td>Controls LEDs.</td> </tr> <tr> <td>POE</td> <td>Controls the PoE controller.</td> </tr> <tr> <td>usb</td> <td>Controls the USB port.</td> </tr> <tr> <td>di</td> <td>Controls digital inputs.</td> </tr> <tr> <td>do</td> <td>Controls digital output.</td> </tr> <tr> <td>reboot</td> <td>Execute the reboot process.</td> </tr> <tr> <td>version</td> <td>Displays version information for the amcfg command.</td> </tr> <tr> <td>help</td> <td>Displays help for the amcfg command.</td> </tr> </tbody> </table> <p> Information about the commands described in this table is displayed.</p>	Command	Contents	information	Displays hardware information such as device-specific information.	dip-switch	Displays the status of the DIP switches.	push-switch	Displays the status of the PUSH switch.	boot	Controls the startup area.	led	Controls LEDs.	POE	Controls the PoE controller.	usb	Controls the USB port.	di	Controls digital inputs.	do	Controls digital output.	reboot	Execute the reboot process.	version	Displays version information for the amcfg command.	help	Displays help for the amcfg command.
Command	Contents																										
information	Displays hardware information such as device-specific information.																										
dip-switch	Displays the status of the DIP switches.																										
push-switch	Displays the status of the PUSH switch.																										
boot	Controls the startup area.																										
led	Controls LEDs.																										
POE	Controls the PoE controller.																										
usb	Controls the USB port.																										
di	Controls digital inputs.																										
do	Controls digital output.																										
reboot	Execute the reboot process.																										
version	Displays version information for the amcfg command.																										
help	Displays help for the amcfg command.																										
--help	<p>Running the command with "--help" or "-h" after it will display detailed information about the command.</p> <p>Example:</p> <pre>admin@amnimo:~# amctrl di --help ↵</pre>																										

Command common options

The following common options exist for all commands except *information*, *version*, and *help*.

option	Contents																
-S, --syslog LOG_LEVEL	Specify the console output level for messages in LOG_LEVEL.																
-V, --verbose LOG_LEVEL	Specify the message output level for the message in LOG_LEVEL.																
LEVEL	Specify the log level as a number in LOG_LEVEL. Logs below the log level specified here will be displayed. By default, "informational" is set.																
	<table border="1"><thead><tr><th>Setting</th><th>Contents</th></tr></thead><tbody><tr><td>emerg</td><td>This log indicates that the system is unstable.</td></tr><tr><td>alert</td><td>This is a level of logging that requires immediate action.</td></tr><tr><td>crit</td><td>Logs indicating fatal errors.</td></tr><tr><td>err</td><td>Error log.</td></tr><tr><td>warning</td><td>Warning Log.</td></tr><tr><td>info</td><td>Information Log.</td></tr><tr><td>debug</td><td>Debug level logs.</td></tr></tbody></table>	Setting	Contents	emerg	This log indicates that the system is unstable.	alert	This is a level of logging that requires immediate action.	crit	Logs indicating fatal errors.	err	Error log.	warning	Warning Log.	info	Information Log.	debug	Debug level logs.
Setting	Contents																
emerg	This log indicates that the system is unstable.																
alert	This is a level of logging that requires immediate action.																
crit	Logs indicating fatal errors.																
err	Error log.																
warning	Warning Log.																
info	Information Log.																
debug	Debug level logs.																

11.2.2 Display hardware information



To view hardware information, run the *amctrl information* command.

Format

```
amctrl information
```

Execution example

The following is an example of execution at an Edge Gateway.

```
admin@amnimo:~$ amctrl information ↵
manufacturer  amnimo
board         AG10
series        G
model         AG10-010JP-10-512G
serial        012345
revision      0
date:         2020-01-01t00:00:00z
```



If the model is different, the contents specific to the model are displayed in board, series, and model.

11.2.3 Display DIP switch status



To obtain the status of a DIP switch, run the *amctrl dip-switch* command.

Format

```
amctrl dip-switch
```

Output Format

```
DSW-1: DSW-STATUS
DSW-2: DSW-STATUS
DSW-3: DSW-STATUS
DSW-4: DSW-STATUS
```

Output item

Item	Contents						
DSW-STATUS	The status of each DIP switch is displayed. <table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td>ON state</td> </tr> <tr> <td>OFF</td> <td>OFF state</td> </tr> </tbody> </table>	Display	Contents	ON	ON state	OFF	OFF state
Display	Contents						
ON	ON state						
OFF	OFF state						

Execution example

To obtain the status of the DIP switches, the *sudo* command must be used.

```
admin@amnimo:~$ sudo amctrl dip-switch ↵
DSW-1: OFF
DSW-2: ON
DSW-3: ON
DSW-4: ON
```

11.2.4 Display the status of the PUSH switch



To display the status of the PUSH switch, run the *push-switch* command.

Format

```
amctrl push-switch
```

Output Format

```
PSW: PSW-STATUS
```

Output item

Item	Contents						
PSW -STATUS	The status of the PUSH switch is displayed.						
	<table border="1"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td>ON state</td> </tr> <tr> <td>OFF</td> <td>OFF state</td> </tr> </tbody> </table>	Display	Contents	ON	ON state	OFF	OFF state
Display	Contents						
ON	ON state						
OFF	OFF state						

Execution example

To display the status of the PUSH switch, the *sudo* command must be used.

```
admin@amnimo:~$ sudo amctrl push-switch ↵
PSW: OFF
```

11.2.5 Controlling the startup area



To control the boot area, run the *amctrl boot* command.

Format

```
amctrl boot
```

Output Format

```
AREA: AREA_NO
```

Output item

Item	Contents						
AREA_NO	The number of the startup area is displayed. <table border="1"><thead><tr><th>Display</th><th>Contents</th></tr></thead><tbody><tr><td>0</td><td>Area 0 Configuration storage area: /dev/mmcblk0boot0 rootfs: /dev/mmcblk0p1 userfs: /dev/mmcblk0p3</td></tr><tr><td>1</td><td>Area 1 Configuration storage area: /dev/mmcblk0boot1 rootfs: /dev/mmcblk0p2 userfs: /dev/mmcblk0p4</td></tr></tbody></table>	Display	Contents	0	Area 0 Configuration storage area: /dev/mmcblk0boot0 rootfs: /dev/mmcblk0p1 userfs: /dev/mmcblk0p3	1	Area 1 Configuration storage area: /dev/mmcblk0boot1 rootfs: /dev/mmcblk0p2 userfs: /dev/mmcblk0p4
Display	Contents						
0	Area 0 Configuration storage area: /dev/mmcblk0boot0 rootfs: /dev/mmcblk0p1 userfs: /dev/mmcblk0p3						
1	Area 1 Configuration storage area: /dev/mmcblk0boot1 rootfs: /dev/mmcblk0p2 userfs: /dev/mmcblk0p4						

Setting items

Item	Contents				
--set AREA_NO	Switches the startup area. <table border="1"><thead><tr><th>Display</th><th>Contents</th></tr></thead><tbody><tr><td>AREA_NO</td><td>startup area</td></tr></tbody></table>	Display	Contents	AREA_NO	startup area
Display	Contents				
AREA_NO	startup area				
-V, --verbose	Specify the console output level of the message in LEVEL.				
-h, --help	Displays help messages.				

Execution example

To control the boot area, the *sudo* command must be used.

```
admin@amnimo:~$ sudo amctrl boot -set 1↵
admin@amnimo:~$ sudo amctrl boot ↵
AREA: 1
```



To control the lighting of LEDs, run the *amctrl led* command with the option

Format

```
amctrl led [--number <1-5>]
          [--color <green | red>]
          [--trigger <none | timer >]
          [--brightness <off | on>]
          [--delay <125 | 500>]
          [--syslog LEVEL].
          [--verbose LEVEL].
          [-h]
```

Setting items

Item	Contents												
--number	<p>Specify the number of the LED to be controlled in the range of 1 to 5.</p> <p> Do not use 1 and 2 as they are reserved for the system.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ANT</td> </tr> <tr> <td>2</td> <td>MOB</td> </tr> <tr> <td>3</td> <td>ST1</td> </tr> <tr> <td>4</td> <td>ST2</td> </tr> <tr> <td>5</td> <td>ST3</td> </tr> </tbody> </table>	Setting	Contents	1	ANT	2	MOB	3	ST1	4	ST2	5	ST3
Setting	Contents												
1	ANT												
2	MOB												
3	ST1												
4	ST2												
5	ST3												
--color	<p>Specifies the LED color to be controlled.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>green</td> <td>green</td> </tr> <tr> <td>red</td> <td>red</td> </tr> </tbody> </table>	Setting	Contents	green	green	red	red						
Setting	Contents												
green	green												
red	red												
--trigger	<p>Specify the trigger for LED control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>none</td> <td>nashi (Pyrus pyrifolia, esp. var. culta)</td> </tr> <tr> <td>timer</td> <td>Flashes at the cycle specified by --delay.</td> </tr> </tbody> </table>	Setting	Contents	none	nashi (Pyrus pyrifolia, esp. var. culta)	timer	Flashes at the cycle specified by --delay.						
Setting	Contents												
none	nashi (Pyrus pyrifolia, esp. var. culta)												
timer	Flashes at the cycle specified by --delay.												
--brightness	<p>LED lighting control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>on</td> <td>lighting (a lamp)</td> </tr> <tr> <td>off</td> <td>switching off the light</td> </tr> </tbody> </table>	Setting	Contents	on	lighting (a lamp)	off	switching off the light						
Setting	Contents												
on	lighting (a lamp)												
off	switching off the light												
-delay	<p>Specifies the lighting cycle for LED blinking control.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>125</td> <td>125ms cycle</td> </tr> <tr> <td>500</td> <td>500ms cycle</td> </tr> </tbody> </table>	Setting	Contents	125	125ms cycle	500	500ms cycle						
Setting	Contents												
125	125ms cycle												
500	500ms cycle												
-S , --syslog	LEVEL specifies the level at which messages are output to syslog.												
-V, --verbose	Specify the console output level of the message in LEVEL.												
-h, --help	Displays help messages.												



If the option is omitted, the control settings for all LEDs are displayed.

Execution example

To control the lighting of the LEDs, the *sudo* command must be used. Below is an example of how to do this at the Edge Gateway.

```
admin@amnimo:~# sudo amctrl led ↵
LED-1: color=green,trigger=none,brightness=on,delay=125
LED-1: color=red,trigger=none,brightness=off,delay=125
LED-2: color=green,trigger=none,brightness=off,delay=125
LED-2: color=red,trigger=none,brightness=off,delay=125
LED-3: color=green,trigger=none,brightness=off,delay=125
LED-3: color=red,trigger=none,brightness=off,delay=125
LED-4: color=green,trigger=none,brightness=off,delay=125
LED-4: color=red,trigger=none,brightness=off,delay=125
LED-5: color=green,trigger=none,brightness=off,delay=125
LED-5: color=red,trigger=none,brightness=off,delay=125
```



To control the PoE controller, run the *amctrl poe* command with parameters.

Format

```
amctrl poe <power [-i <lan0-lan3>] [-p <on|off>] |
reset [-i <lan0-lan3>] [-d <0-3600>] |
status | (default)
shutdown [-p <on|off>] |
limitcurrent [-L <110|204|374|592|645|754|920|auto>] >
```

Setting items

Item	Contents						
power	Controls the power supply to each PoE port.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>-i</td> <td>Specify the PoE interface in the range of lan0 to lan3.</td> </tr> <tr> <td>-p</td> <td>Specify power ON/OFF.</td> </tr> </tbody> </table>	Setting	Contents	-i	Specify the PoE interface in the range of lan0 to lan3.	-p	Specify power ON/OFF.
	Setting	Contents					
-i	Specify the PoE interface in the range of lan0 to lan3.						
-p	Specify power ON/OFF.						
reset	Reset each PoE port.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>-i</td> <td>Specify the PoE interface in the range of lan0 to lan3.</td> </tr> <tr> <td>-d</td> <td>Specify the startup delay time (in seconds) in the range of 0 to 3600.</td> </tr> </tbody> </table>	Setting	Contents	-i	Specify the PoE interface in the range of lan0 to lan3.	-d	Specify the startup delay time (in seconds) in the range of 0 to 3600.
	Setting	Contents					
-i	Specify the PoE interface in the range of lan0 to lan3.						
-d	Specify the startup delay time (in seconds) in the range of 0 to 3600.						
status	Obtains the control status of the PoE.						
shutdown	Shut down the PoE controller.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>-p</td> <td>Specify shutdown ON/OFF. <ul style="list-style-type: none"> ● on Enables shutdown output (PoE device activated). ● off Disables shutdown output (PoE device stops). </td> </tr> </tbody> </table>	Setting	Contents	-p	Specify shutdown ON/OFF. <ul style="list-style-type: none"> ● on Enables shutdown output (PoE device activated). ● off Disables shutdown output (PoE device stops). 		
	Setting	Contents					
-p	Specify shutdown ON/OFF. <ul style="list-style-type: none"> ● on Enables shutdown output (PoE device activated). ● off Disables shutdown output (PoE device stops). 						
limitcurrent	Changes the current limit when supplying power to each PoE port.						
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>-L</td> <td>Specify one of the following current limit values 110, 204, 374, 592, 645, 754, 920, auto</td> </tr> </tbody> </table>	Setting	Contents	-L	Specify one of the following current limit values 110, 204, 374, 592, 645, 754, 920, auto		
	Setting	Contents					
-L	Specify one of the following current limit values 110, 204, 374, 592, 645, 754, 920, auto						

Execution example

To control the PoE controller, the *sudo* command must be used. The following is an example of connecting a Class 1 power receiving device (PD) to lan0 and lan2.

```
admin@amnimo:~# sudo amctrl poe status
state 0:1,1:0,2:1,3:0
class 0:Class1,1:Unknown,2:Class1,3:Unknown
poeplus 0:0,1:0,2:0,3:0
limit-current 0:204mA,1:592mA,2:754mA,3:920mA
Voltage 0:53.293V,1:0.000V,2:53.432V,3:0.000V
Current 0:43.765mA,1:0.000mA,2:45.169mA,3:0.000mA
Watt 0:2.332W,1:0.000W,2:2.413W,3:0.000W
Temperature 52.8deg
```



To control the USB port, run the ***amctrl usb*** command.

Format

```
amctrl usb [<-b|--bus> <1-2>] [<-w|--wait> <0s-600s|<0m-10m>] USB-CTRL
```

Setting items

Item	Contents								
-b --bus	Specifies the USB bus number. The range is 1 or 2.								
-w --wait	Specifies the OFF time during reset control. The default is 0 seconds. Seconds specified (s): 0 to 600 seconds Time specified (m): 0 to 10 minutes								
USB-CTRL	Specifies USB port control. <table border="1" data-bbox="571 801 1353 974"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>on</td> <td>Turn on the USB port.</td> </tr> <tr> <td>off</td> <td>Turn off the USB port.</td> </tr> <tr> <td>reset</td> <td>Reset the USB port.</td> </tr> </tbody> </table>	Setting	Contents	on	Turn on the USB port.	off	Turn off the USB port.	reset	Reset the USB port.
Setting	Contents								
on	Turn on the USB port.								
off	Turn off the USB port.								
reset	Reset the USB port.								
-V, --verbose	Specify the console output level of the message in LEVEL.								
-h, --help	Displays help messages.								

Execution example

To control the USB port, the ***sudo*** command must be used.

```
admin@amnimo:~# sudo amctrl usb --bus 1 --wait 10m reset ↵
```



To control the digital inputs, execute the *amctrl di* command.

Format

```
amctrl di [-p] [-V LEVEL] [-h]
```

Setting items

Item	Contents
-p, --permanent	This mode continuously outputs digital input changes.
-V, --verbose	Specify the console output level of the message in LEVEL.
-h, --help	Displays help messages.

Output Format

```
DI-1: DI-STATUS
DI-2: DI-STATUS
DI-3: DI-STATUS
DI-4: DI-STATUS
```

Output item

Item	Contents						
DI-STATUS	The status of the digital input is displayed. <table border="1" data-bbox="571 1019 1353 1151"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td>ON state</td> </tr> <tr> <td>OFF</td> <td>OFF state</td> </tr> </tbody> </table>	Display	Contents	ON	ON state	OFF	OFF state
Display	Contents						
ON	ON state						
OFF	OFF state						



If the option is omitted, the status of all digital inputs is displayed.

Execution example

To control the digital inputs, the *sudo* command must be used.

```
admin@amnimo:~# sudo amctrl di ↵
DI-1: OFF
DI-2: OFF
DI-3: OFF
DI-4: OFF
```



To control the digital output, execute the *amctrl do* command.

Format

```
amctrl do [--set HEX].
          [--set-bit HEX].
          [--clr-bit HEX].
          [--on <1|2>]]
          [--off <1|2>]]
          -V LEVEL
          -h
```

Setting items

Item	Contents						
--set	Hexadecimal value to control multiple bits of digital output simultaneously. <table border="1" data-bbox="571 779 1353 913"> <thead> <tr> <th>Setting</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ON</td> </tr> <tr> <td>0</td> <td>OFF</td> </tr> </tbody> </table>	Setting	Contents	1	ON	0	OFF
Setting	Contents						
1	ON						
0	OFF						
--set-bit	Specify bit number (1 or 2) to control digital output ON. When 3 is specified, the digital outputs of DO-1 and DO-2 are controlled ON.						
--clr-bit	Specify the bit number (1 or 2) to control the digital output OFF. When 3 is specified, the digital outputs of DO-1 and DO-2 are controlled OFF.						
--on	Controls digital output ON by specifying the digital output number (1 or 2).						
--off	Controls the digital output OFF by specifying the digital output number (1 or 2).						
-V, --verbose	Specify the console output level of the message in LEVEL.						
-h, --help	Displays help messages.						

Output Format

```
DO-1: DO-STATUS
DO-2: DO-STATUS
```

Output item

Item	Contents						
DO-STATUS	The status of the digital output is displayed. <table border="1" data-bbox="571 1697 1353 1823"> <thead> <tr> <th>Display</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td>ON state</td> </tr> <tr> <td>OFF</td> <td>OFF state</td> </tr> </tbody> </table>	Display	Contents	ON	ON state	OFF	OFF state
Display	Contents						
ON	ON state						
OFF	OFF state						



If the option is omitted, the status of all digital outputs is displayed.

Execution example

To control the digital output, the *sudo* command must be used.

```
admin@amnimo:~# sudo amctrl do --set 0x03 ↵
admin@amnimo:~# sudo amctrl do ↵
DO-1: ON
DO-2: ON
admin@amnimo:~# sudo amctrl do --set 0x0 ↵
admin@amnimo:~# sudo amctrl do ↵
DO-1: OFF
DO-2: OFF
admin@amnimo:~# sudo amctrl do --set-bit 1 ↵
admin@amnimo:~# sudo amctrl do ↵
DO-1: ON
DO-2: OFF
admin@amnimo:~# sudo amctrl do --set-bit 2 ↵
admin@amnimo:~# sudo amctrl do ↵
DO-1: ON
DO-2: ON
admin@amnimo:~# sudo amctrl do --clr-bit 1 ↵
admin@amnimo:~# sudo amctrl do ↵
DO-1: OFF
DO-2: ON
admin@amnimo:~# sudo amctrl do --on 1 ↵
admin@amnimo:~# sudo amctrl do ↵
DO-1: ON
DO-2: ON
admin@amnimo:~# sudo amctrl do --off 2 ↵
admin@amnimo:~# sudo amctrl do ↵
DO-1: ON
DO-2: OFF
```

11.2.11 Controls the reboot process



To control the reboot process, run the *amctrl reboot* command.

Format

```
amctrl reboot -t <soft | hard> [--wait SEC] [-V LEVEL] [-h]
```

Setting items

Item	Contents						
-t	Specifies the restart type. Required field. <table border="1"><thead><tr><th>Setting</th><th>Contents</th></tr></thead><tbody><tr><td>soft</td><td>Perform a software reboot. It is set as the default value.</td></tr><tr><td>hard</td><td>Perform a hardware reboot. Turns the entire hardware from OFF to ON.</td></tr></tbody></table>	Setting	Contents	soft	Perform a software reboot. It is set as the default value.	hard	Perform a hardware reboot. Turns the entire hardware from OFF to ON.
Setting	Contents						
soft	Perform a software reboot. It is set as the default value.						
hard	Perform a hardware reboot. Turns the entire hardware from OFF to ON.						
--wait	Specify the time (in seconds) to wait for a reset, in the range of 0 to 3600. The default setting is "0".						
-V, --verbose	Specify the console output level of the message in LEVEL.						
-h, --help	Displays help messages.						

Execution example

To control the reboot process, the *sudo* command must be used.

```
admin@amnimo:~# sudo amctrl reboot ↵
```

11.2.12 Display command version

To view the version of the amctrl command, run *amctrl version*.

Execution example

```
admin@amnimo:~$ amctrl version ↵  
amnimo Inc.  
amnimo G series control program version 1.0.0
```

12.1 CLI functions supported in each mode



All features of this product series are listed here as items in a table.

Some functions are not supported by some products.

➔ For a description of the differences in functionality between products, please refer to " 12.2 CLI functions supported by each product ".

Item	General User Mode	Administrator mode	Setup mode
Equipment restart control	-	✓	-
Equipment power-down possible state transition ※1	-	✓	-
Device Information Display	✓	✓	✓
FW version display	✓	✓	-
FW file confirmation	-	✓	-
FW file deletion	-	✓	-
FW Update	-	✓	-
Redundant area synchronization	-	✓	-
Startup area display	✓	✓	✓
Startup area setting	-	✓	✓
Package Update	-	✓	-
Package Information Deletion	-	✓	-
Add credentials for package repositories	-	-	✓
Delete credentials in package repositories	-	-	✓
Display of package repository authentication information settings	-	✓	✓
initialization	-	✓	✓
Setting list display	-	✓	✓
Configuration file list display	-	✓	✓
Setting file writing	-	✓	✓
Configuration file read	-	✓	✓
Configuration file name change	-	✓	✓
Configuration file copy	-	✓	✓
Configuration file deletion	-	✓	✓
file list view	-	✓	✓
File movement control (e.g., basic configuration files)	-	✓	✓
File copy control (e.g., basic configuration files)	-	✓	✓
file deletion control	-	✓	✓
Host Name Display	✓	✓	✓
Host Name Change	-	-	✓
Time Zone Display	✓	✓	✓
Time Zone Setting	-	-	✓
Change User Password	✓※2	✓	✓
Account Listing	-	✓	✓
Login Account Display	✓	✓	✓
Account (user and group) settings display	-	✓	✓

Item	General User Mode	Administrator mode	Setup mode
Account (user, group) setting control	-	-	✓
Mobile Module Display	✓	✓	✓
Mobile Module Control	-	✓	✓
Mobile Status Display	✓	✓	✓
Mobile connection control (manual connection mode)	-	✓	✓
Mobile disconnection control	-	✓	✓
Mobile Settings Display	-	✓	✓
Mobile Configuration Control	-	-	✓
PPP status display	✓	✓	✓
PPP connection control (manual connection)	-	✓	✓
PPP Disconnection Control	-	✓	✓
PPP setting display	-	✓	✓
PPP configuration control	-	-	✓
interface status indication	✓	✓	✓
Interface setting display	-	✓	✓
Interface setting control	-	-	✓
routing table display	✓	✓	✓
Routing setting display	-	✓	✓
routing configuration control	-	-	✓
Packet filtering setting display	-	✓	✓
packet filtering configuration control	-	-	✓
NAT setting display	-	✓	✓
NAT configuration control	-	-	✓
DNS (forward and reverse lookup) search	✓	✓	✓
DNS status display	✓	✓	✓
DNS Settings Display	-	✓	✓
DNS configuration control	-	-	✓
DHCP lease list display	✓	✓	✓
DHCP status display	✓	✓	✓
DHCP setting display	-	✓	✓
DHCP setting control	-	-	✓
IPsec status display	✓	✓	✓
IPsec connection control (manual connection)	-	✓	✓
IPsec disconnection control	-	✓	✓
IPsec setting display	-	✓	✓
IPsec Configuration Control	-	-	✓
NTP status display	✓	✓	✓
NTP setting display	-	✓	✓
NTP setting control	-	-	✓
SSH setting display	-	✓	✓
SSH Configuration Control	-	✓	✓
Storage Device Display	✓	✓	✓
Storage partition control	-	✓	✓
Storage Format Control	-	✓	✓
Storage mount display	✓	✓	✓

Item	General User Mode	Administrator mode	Setup mode
Storage mount control	-	✓	✓
Storage Unmount Control	-	✓	✓
Storage Check Control	-	✓	✓
Storage Usage Status Display	✓	✓	✓
Storage Settings Display	✓	✓	✓
Storage Configuration Control	-	✓	✓
Storage Format Information Attitude Display	✓	✓	✓
Schedule operation status display	✓	✓	✓
Schedule setting display	-	✓	✓
Schedule setting control	-	-	✓
PoE status display	✓	✓	✓
PoE port control (power on/off, reset)	-	✓	✓
PoE setting display	-	✓	✓
PoE setting control	-	-	✓
USB Device Display	✓	✓	✓
USB device control (power on/off, reset)	-	✓	✓
Syslog message display	-	✓	✓
Syslog configuration display	-	✓	✓
Syslog configuration control	-	-	✓
amlog message display	-	✓	✓
amlog control	-	✓	✓
PING control	✓	✓	✓
TRACEROUTE Control	✓	✓	✓
ARP Information Display	✓	✓	✓
ARP Information Control	-	✓	✓
packet dump indication	-	✓	✓
packet dump save	-	✓	✓
packet dumpster deletion	-	✓	✓
CPU status display	✓	✓	✓
CPU operation setting display	-	✓	✓
CPU operation setting control	-	-	✓
Input voltage indication	✓	✓	✓
Temperature display inside the enclosure	✓	✓	✓
High/low temperature protection setting display	-	✓	✓
High/low temperature protection setting control	-	-	✓
Time display	✓	✓	✓
Time setting (manual)	-	✓	✓
Time setting (ntpddate)	-	✓	✓
DIN status indication	✓	✓	✓
DOUT status display	✓	✓	✓
DOUT Control	-	✓	✓
DIP switch status indication	✓	✓	✓
DMS setting display	✓	✓	✓
DMS setting control	-	✓	✓
NxWitness status display	✓	✓	✓
NxWitness Control	-	✓	✓

Item	General User Mode	Administrator mode	Setup mode
NxWitness Settings Display	-	✓	✓
NxWitness setting control	-	✓	✓
NxWitness setting write	-	✓	✓
Loading NxWitness Settings	-	✓	✓
remote.it status display	✓	✓	✓
remote.it control	-	✓	✓
remote.it setting display	-	-	✓
remote.it setting control	-	-	✓
Application Command Execution	-	-	✓
GUI setting display	-	✓	✓
GUI setting control	-	-	✓
DHCP relay setting display	-	✓	✓
DHCP relay setting control	-	-	✓
Proxy server setting display	-	✓	✓
Proxy server configuration control	-	-	✓
Wireless LAN access point status display	✓	✓	✓
Wireless LAN Access Point Connection Station List Display	✓	✓	✓
Wireless LAN Access Point Connection Station disconnection control	-	✓	✓
Wireless LAN access point setting display	-	✓	✓
Wireless LAN access point setting control	-	-	✓
Wireless LAN station status display	✓	✓	✓
Wireless LAN station connection switching control	-	✓	✓
Wireless LAN station setting display	-	✓	✓
Wireless LAN station configuration control	-	-	✓
WPS connection control	-	-	✓
WPS setting display	-	✓	✓
WPS setting control	-	-	✓

*1 The system will enter a state where the power can be disconnected. However, if the same state is maintained for a certain period of time (approximately 10 minutes), the system will automatically reboot through a cold reboot.

*2 The password is only the password for your own account.

12.2 CLI functions supported by each product

Item	AI	GW	GW	RT	RT	CR	CR	CR
Equipment restart control		✓	✓	✓	✓	✓	✓	✓
Equipment power-down possible state transition		✓	✓	✓	✓	-	-	-
Device Information Display	✓	✓	✓	✓	✓	✓	✓	✓
FW version display	✓	✓	✓	✓	✓	✓	✓	✓
FW file confirmation	✓	✓	✓	✓	✓	✓	✓	✓
FW file deletion	✓	✓	✓	✓	✓	✓	✓	✓

Item								
FW Update	✓	✓	✓	✓	✓	✓	✓	✓
Redundant area synchronization	✓	✓	✓	✓	✓	✓	✓	✓
Startup area display	✓	✓	✓	✓	✓	✓	✓	✓
Startup area setting	✓	✓	✓	✓	✓	✓	✓	✓
Package Update	✓	✓	✓	✓	✓	-	-	-
Package Information Deletion	✓	✓	✓	✓	✓	-	-	-
package repository. Additional authentication information	✓	✓	✓	✓	✓	-	-	-
package repository. Deletion of authentication information	✓	✓	✓	✓	✓	-	-	-
package repository. Authentication information setting display	✓	✓	✓	✓	✓	-	-	-
initialization	✓	✓	✓	✓	✓	✓	✓	✓
Setting list display	✓	✓	✓	✓	✓	✓	✓	✓
Configuration file list display	✓	✓	✓	✓	✓	✓	✓	✓
Setting file writing	✓	✓	✓	✓	✓	✓	✓	✓
Configuration file read	✓	✓	✓	✓	✓	✓	✓	✓
Configuration file name change	✓	✓	✓	✓	✓	✓	✓	✓
Configuration file copy	✓	✓	✓	✓	✓	✓	✓	✓
Configuration file deletion	✓	✓	✓	✓	✓	✓	✓	✓
file list view	✓	✓	✓	✓	✓	✓	✓	✓
File Movement Control (Basic configuration file, etc.)	✓	✓	✓	✓	✓	✓	✓	✓
file copy control (Basic configuration file, etc.)	✓	✓	✓	✓	✓	✓	✓	✓
file deletion control	✓	✓	✓	✓	✓	✓	✓	✓
Host Name Display	✓	✓	✓	✓	✓	✓	✓	✓
Host Name Change	✓	✓	✓	✓	✓	✓	✓	✓
Time Zone Display	✓	✓	✓	✓	✓	✓	✓	✓
Time Zone Setting	✓	✓	✓	✓	✓	✓	✓	✓
Change User Password	✓	✓	✓	✓	✓	✓	✓	✓
Account Listing	✓	✓	✓	✓	✓	✓	✓	✓
Login Account Display	✓	✓	✓	✓	✓	✓	✓	✓
Account Settings Display	✓	✓	✓	✓	✓	✓	✓	✓
account setup control	✓	✓	✓	✓	✓	✓	✓	✓
group settings indication	-	-	-	-	-	✓	✓	✓
group setting control	-	-	-	-	-	✓	✓	✓
Mobile Module Display	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Module Control	✓	✓	✓	✓	✓	✓	✓	✓

Item								
Mobile Status Display	✓	✓	✓	✓	✓	✓	✓	✓
Mobile connection control (manual connection mode)	✓	✓	✓	✓	✓	✓	✓	✓
Mobile disconnection control	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Settings Display	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Configuration Control	✓	✓	✓	✓	✓	✓	✓	✓
PPP status display	✓	✓	✓	✓	✓	-	✓	✓
PPP connection control (manual connection)	✓	✓	✓	✓	✓	-	✓	✓
PPP Disconnection Control	✓	✓	✓	✓	✓	-	✓	✓
PPP setting display	✓	✓	✓	✓	✓	-	✓	✓
PPP configuration control	✓	✓	✓	✓	✓	-	✓	✓
interface status indication	✓	✓	✓	period ※1	period ※1	period ※1	period ※1	period ※1
Interface setting display	✓	✓	✓	period ※1	period ※1	period ※1	period ※1	period ※1
Interface setting control	✓	✓	✓	period ※1	period ※1	period ※1	period ※1	period ※1
routing table display	✓	✓	✓	✓	✓	✓	✓	✓
Routing setting display	✓	✓	✓	✓	✓	✓	✓	✓
routing configuration control	✓	✓	✓	✓	✓	✓	✓	✓
Packet filtering setting display	✓	✓	✓	✓	✓	✓	✓	✓
packet filtering configuration control	✓	✓	✓	✓	✓	✓	✓	✓
NAT setting display	✓	✓	✓	✓	✓	✓	✓	✓
NAT configuration control	✓	✓	✓	✓	✓	✓	✓	✓
DNS (forward and reverse lookup) search	✓	✓	✓	✓	✓	✓	✓	✓
DNS status display	✓	✓	✓	✓	✓	✓	✓	✓
DNS Settings Display	✓	✓	✓	✓	✓	✓	✓	✓
DNS configuration control	✓	✓	✓	✓	✓	✓	✓	✓
DHCP lease list display	✓	✓	✓	✓	✓	✓	✓	✓
DHCP status display	✓	✓	✓	✓	✓	✓	✓	✓
DHCP setting display	✓	✓	✓	✓	✓	✓	✓	✓
DHCP setting control	✓	✓	✓	✓	✓	✓	✓	✓
IPsec status display	✓	✓	✓	✓	✓	✓	✓	✓
IPsec connection control (manual connection)	✓	✓	✓	✓	✓	✓	✓	✓
IPsec disconnection control	✓	✓	✓	✓	✓	✓	✓	✓
IPsec setting display	✓	✓	✓	✓	✓	✓	✓	✓
IPsec Configuration Control	✓	✓	✓	✓	✓	✓	✓	✓

Item								
NTP status display	✓	✓	✓	✓※3	✓※3	✓※3	✓	✓※3
NTP setting display	✓	✓	✓	✓※3	✓※3	✓※3	✓	✓※3
NTP setting control	✓	✓	✓	✓※3	✓※3	✓※3	✓	✓※3
SSH setting display	✓	✓	✓	✓	✓	✓	✓	✓
SSH Configuration Control	✓	✓	✓	✓	✓	✓	✓	✓
Storage Device Display	✓	✓	✓	-	-	-	-	-
Storage partition control	✓	✓	✓	-	-	-	-	-
Storage Format Control	✓	✓	✓	-	-	-	-	-
Storage mount display	✓	✓	✓	-	-	-	-	-
Storage mount control	✓	✓	✓	-	-	-	-	-
Storage Unmount Control	✓	✓	✓	-	-	-	-	-
Storage Check Control	✓	✓	✓	-	-	-	-	-
Storage Usage Status Display	✓	✓	✓	-	-	-	-	-
Storage Settings Display	✓	✓	✓	-	-	-	-	-
Storage Configuration Control	✓	✓	✓	-	-	-	-	-
storage format information display	✓	✓	✓	-	-	-	-	-
Schedule operation status display	✓	✓	✓	✓	✓	✓	✓	✓
Schedule setting display	✓	✓	✓	✓※4	✓	✓※4,5	✓※4,5	✓※4,5
Schedule setting control	✓	✓	✓	✓※4	✓	✓※4,5	✓※4,5	✓※4,5
PoE status display	✓	✓	✓	-	✓	-	-	✓
PoE port control (power on/off, reset)	✓	✓	✓	-	✓	-	-	✓
PoE setting display	✓	✓	✓	-	✓	-	-	✓
PoE setting control	✓	✓	✓	-	✓	-	-	✓
USB Device Display	✓	✓	✓	-	-	-	-	-
USB Device Control (Power ON/OFF, reset)	✓	✓	✓	-	-	-	-	-
Input voltage indication	✓	✓	✓	✓	✓	-	-	-
Syslog message display	✓	✓	✓	✓	✓	✓	✓	✓
Syslog configuration display	✓	✓	✓	✓	✓	✓	✓	✓
Syslog configuration control	✓	✓	✓	✓	✓	✓	✓	✓
amlog message display	✓	✓	✓	✓	✓	-	-	-
amlog control	✓	✓	✓	✓	✓	-	-	-
PING control	✓	✓	✓	✓	✓	✓	✓	✓
TRACEROUTE Control	✓	✓	✓	✓	✓	✓	✓	✓
ARP Information Display	✓	✓	✓	✓	✓	✓	✓	✓
ARP Information Control	✓	✓	✓	✓	✓	✓	✓	✓
packet dump indication	✓	✓	✓	✓	✓	✓	✓	✓
packet dump save	✓	✓	✓	✓	✓	-	-	-
packet dumpster deletion	✓	✓	✓	✓	✓	-	-	-

Item								
CPU status display	-	✓	✓	✓	✓	✓	✓	✓
CPU operation setting display	-	✓	✓	✓	✓	-	-	-
CPU operation setting control	-	✓	✓	✓	✓	-	-	-
Input voltage indication	✓	✓	✓	✓	✓	-	-	-
Temperature display inside the enclosure	✓	✓	✓	✓	✓	✓	✓	✓
High/low temperature protection setting display	✓	✓	✓	✓	✓	-	-	-
High/low temperature protection setting control	✓	✓	✓	✓	✓	-	-	-
Time display	✓	✓	✓	✓	✓	✓	✓	✓
Time setting (manual)	✓	✓	✓	✓	✓	✓	✓	✓
Time setting (ntpdate)	✓	✓	✓	✓	✓	✓	✓	✓
DIN status indication	✓	✓	✓	-	-	-	-	-
DOUT status display	✓	✓	✓	-	-	-	-	-
DOUT Control	✓	✓	✓	-	-	-	-	-
DIP switch status indication	✓	✓	✓	✓	✓	-	-	-
DMS setting display	✓	✓	✓	✓	✓	✓	✓	✓
DMS setting control	✓	✓	✓	✓	✓	✓	✓	✓
NxWitness status display	✓	✓	✓	-	-	-	-	-
NxWitness Control	✓	✓	✓	-	-	-	-	-
NxWitness Settings Display	✓	✓	✓	-	-	-	-	-
NxWitness setting control	✓	✓	✓	-	-	-	-	-
NxWitness setting write	✓	✓	✓	-	-	-	-	-
Loading NxWitness Settings	✓	✓	✓	-	-	-	-	-
remote.it status display	✓	✓	✓	✓	✓	✓	✓	✓
remote.it control	✓	✓	✓	✓	✓	✓	✓	✓
remote.it setting display	✓	✓	✓	✓	✓	✓	✓	✓
remote.it setting control	✓	✓	✓	✓	✓	✓	✓	✓
Application Command Execution	✓	✓	✓	✓	✓	-	-	-
GUI setting display	✓	✓	✓	✓	✓	✓	✓	✓
GUI setting control	✓	✓	✓	✓	✓	✓	✓	✓
DHCP Relay Display	✓	✓	✓	✓	✓	✓	✓	✓
DHCP relay setting control	✓	✓	✓	✓	✓	✓	✓	✓
Proxy server setting display	✓	✓	✓	✓	✓	✓	✓	✓
Proxy server configuration control	✓	✓	✓	✓	✓	✓	✓	✓
Wireless LAN access point status display	-	-	-	-	-	-	✓	✓

Item								
Wireless LAN Access Point Connection Station List Display	-	-	-	-	-	-	✓	✓
Wireless LAN Access Point Connection Station disconnection control	-	-	-	-	-	-	✓	✓
Wireless LAN access point setting display	-	-	-	-	-	-	✓	✓
Wireless LAN access point setting control	-	-	-	-	-	-	✓	✓
Wireless LAN station status display	-	-	-	-	-	-	✓	✓
Wireless LAN station connection switching control	-	-	-	-	-	-	✓	✓
Wireless LAN station setting display	-	-	-	-	-	-	✓	✓
Wireless LAN station configuration control	-	-	-	-	-	-	✓	✓
WPS connection control	-	-	-	-	-	-	✓	✓
WPS setting display	-	-	-	-	-	-	✓	✓
WPS setting control	-	-	-	-	-	-	✓	✓

- 1 The number of Ethernet ports differs from that of the Edge Gateway.
- 2 Will be supported in a future release.
- 3 GPS function is not available.
- 4 poe-reset-supply is not available.
- 5 Functions related to ppp are not available.

12.3 fail-safe

Fail-safe is a system that provides 24-hour continuous operation by restarting equipment in the event of equipment failure or malfunction. Fail-safe settings exist for mobile, storage, scheduling, and DHCP server functions. The DMS function also has a failsafe feature.

■ failsafe retention function

Feature				Abnormality detection details	Recovery process
Storage Functions ➔ " 4.9.7 Handle fail-safe in case of fsck/mount/read/write process failure "				Storage access failure	storage access execution
Mobile Function ➔ " 5.7 Set up a mobile line "				Communication failure	Mobile Module Reset
Schedule Feature ➔ "7.7.3 Set a schedule "	Schedule Type	"keep-alive".	action	"disconnect ecm ECM-IFNAME reset enable".	● ping resend ● Mobile Module Reset
				"disconnect ecm ECM-IFNAME reset disable".	ping resend
				"wifi ap reset enable". or "wifi sta reset enable".	● ping resend ● Wireless LAN chip reset
				"wifi ap reset disable". or "wifi sta reset disable".	ping resend
				"soft-reboot". or "hard-reboot".	Action Operation (soft or hard reboot) ※2
	"general-control".	"soft-reboot". or "hard-reboot".	(Schedule timing) ※1		
DHCP server function ➔ " 7.6.3 Configure DHCP server settings "				Receipt of DHCP DISCOVER more than the specified number of times in a certain period of time	Restart DHCP server
DMS Function ➔ " 10.1 Configure DMS settings "				Timeout for keep-alive to DMS server※3	Mobile Module Reset※3

- 1 The table describes the contents of abnormality detection, but these are the contents to be set.
- 2 Recovery operation becomes a reboot process.
- 3 Detailed specifications are described in "Fail-safe Operation of DMS Function" on the next page.

Common setting items

Item	Contents
retry ^{*4}	Maximum number of retries to perform recovery processing when an abnormality is detected
reboot	Maximum number of reboots to be performed when the maximum number of resets is reached

*4 For the schedule function only, the maximum number of retries cannot be changed. 3 retries is the fixed value.

Fail-safe operation of DMS functions

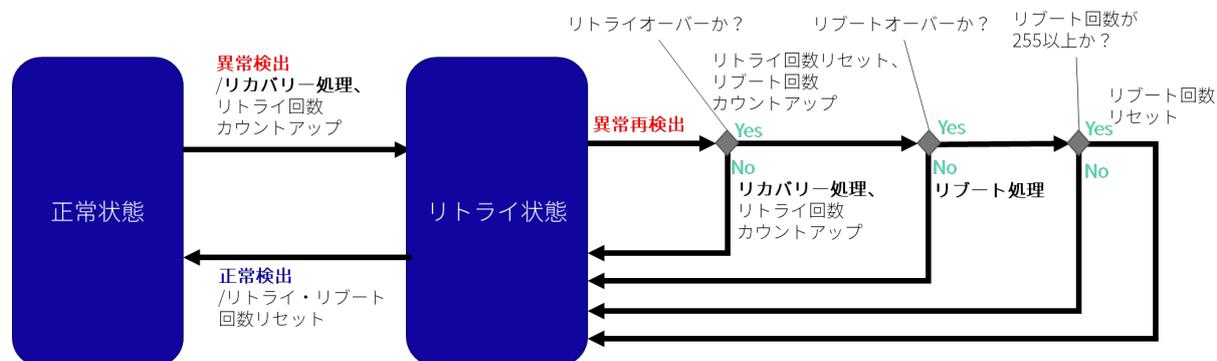
Item	Contents
Abnormality detection conditions	When the DMS function is enabled, reconnection after communication failure between the device and the cloud fails two or more times in a row.
recovery process	<ul style="list-style-type: none"> ● If the mobile line is routed to the Internet side and used as a route for DMS, reset the communication module^{*5}. ● When the failsafe is executed four times in a row, the device is rebooted.

*5 Compact Router resets only the communication module control process.

functional overview

- ③ If an abnormality (e.g., a communication error in the case of the mobile function) is detected, recovery processing is performed. At that time, the number of retries is counted up.
- ④ If reconnection is successful within the number of retries, the number of retries and reboots are reset.
- ⑤ If more than the set maximum number of retries are performed, the number of retries is reset, the reboot counts up, and the equipment is hardware rebooted.
- ⑥ If you reboot more than the configured maximum number of reboots, the reboot process will stop, although the number of reboots will be counted up. However, if the number of reboots exceeds 255, it will return to 0 again.*

*Scheduling and storage functions will not revert to 0 after 255 times. This will be addressed in a future release.



Revision History

Version number	Date of issue	Revision details
1st ed.	July 1, 2020	First Edition
2nd ed.	October 1, 2020	<p>Due to additional functionality with the release of amnimo G series firmware V1.1.0.</p> <ul style="list-style-type: none"> ● Addition of temperature control function ● CPU clock control function added ● DNS setting function added ● Added DHCP (IPv4) setting function ● GPS-linked control function added to NTP function ● Addition of file control functions ● USB control function added ● Add PPP control function ● Added time zone and host name setting functions ● Added IPSec configuration functionality ● Addition of DMS setting function ● Addition of NxWitness configuration functionality ● Added some functions of mobile module control function ● Added some PoE control functions
3rd ed.	April 1, 2021	<p>To add functionality with the release of amnimo G/R series firmware V1.2.0.</p> <ul style="list-style-type: none"> ● Addition of GUI setting function ● Addition of remote.it setting function ● Addition of D IN/D OUT control function
4th ed.	September 10, 2021	<p>Due to additional functions and specification changes with the release of amnimo G/R series firmware V1.3.0.</p> <ul style="list-style-type: none"> ● Changes and additions to mobile module-related functions ● Addition of network confirmation function ● Change of password setting input specification
5th ed.	October 18, 2021	<p>To add functionality with the release of amnimo G/R series firmware V1.4.0.</p> <ul style="list-style-type: none"> ● Outdoor Type Edge Gateway and Outdoor Type IoT Router Outdoor Type Router were added as target devices.
6th ed.	May 20, 2022	<p>To add functionality due to the release of amnimo G/R/C series firmware V1.5.0.</p> <ul style="list-style-type: none"> ● Compact Router added as a target device.
7th ed.	June 15, 2022	<p>Due to specification change by amnimo G/R series firmware V1.5.1 release.</p> <ul style="list-style-type: none"> ● Changed the default value of CPU operating frequency setting to the specification.
8 ed.	July 15, 2022	<p>Due to specification change by amnimo G/R series firmware V1.5.2 release.</p> <ul style="list-style-type: none"> ● Corrected no-communication state monitoring packets. ● To add functionality with the release of amnimo C series firmware V1.6.0. ● Add GUI functionality for Compact Router.

Version number	Date of issue	Revision details
9th ed.	October 1, 2022	<p>Due to additional functionality with the release of amnimo C series firmware V1.7.0.</p> <ul style="list-style-type: none"> ● DHCP relay function, IPsec function, and remote.it function added. ● Corrected a typo in the IPsec command specification. (pre-shared-key => pre-shared-key)
10 ed.	December 2, 2022	<p>To add functionality with the release of amnimo C series firmware V1.8.0.</p> <ul style="list-style-type: none"> ● Added proxy server functionality. ● Added functionality for setting group privileges. (With the addition of this function, some specifications of the user setting function have been changed.) ● Added alias definition function to DNS function. ● Added pass-through mode (the ability to not perform IPsec communications to a specified subnet) for the IPsec function.
11th ed.	January 13, 2023	Updated description with amnimo C series firmware V1.8.1 release and amnimo G/R series firmware V1.8.2 release.
12 ed.	January 23, 2023	Added a condition regarding the input character for passwords.
13th ed.	March 6, 2023	<p>To add functionality with the release of amnimo C series firmware V1.9.0.</p> <ul style="list-style-type: none"> ● Added fail-safe function for DHCP server
14th ed.	May 31, 2023	<p>Due to additional functionality with the release of amnimo C series firmware V1.10.0.</p> <ul style="list-style-type: none"> ● Compact Router Indoor Type with wireless LAN is added as a target device.
15th ed.	June 30, 2023	<p>Due to additional functionality with the release of amnimo C series firmware V1.11.0.</p> <ul style="list-style-type: none"> ● In the "general-control" schedule type of the schedule function, added the ability to execute software reboot and hardware reboot by setting random execution time and startup elapsed time.
16th ed.	September 1, 2023	<p>To add functions by amnimo C series firmware V1.12.0 release and amnimo X series firmware V2.0.0 (to be released).</p> <ul style="list-style-type: none"> ● Compact Router Indoor Type with wireless LAN and AI Edge Gateway Indoor Type were added as target devices.
17th ed.	September 29, 2023	To add functions and specification details by amnimo C series firmware V1.13.0 release and amnimo G/R series firmware V1.9.7.
18th ed.	November 10, 2023	<p>Due to the release of amnimo G series firmware V2.1.0, functionality additions and limitations.</p> <ul style="list-style-type: none"> ● Added the ability to display storage format information. ● Added a specification change that prevents the use of only one-byte numbers for user and group names. ● For amnimo G series only, the maximum MTU value that can be set by the interface function has been changed from 9676 to 9668.
19 ed.	November 15, 2023	Corrected description of scheduling function.



Edge Gateway Series
CLI User's Manual

November 15, 2023 19th ed.

IM AMF03A01-01EN

All Rights Reserved. Copyright © 2020-2023, amnimo Inc.