Yamaha L2 Switch

SWP2 series (SWP2-10SMF, SWP2-10MMF)

Command Reference

Rev.2.03.22

Contents

Preface

Introduction

- Unauthorized reproduction of this document in part or in whole is prohibited.
- The contents of this document are subject to change without notice.
- Yamaha disclaims all responsibility for any damages caused by loss of data or other problems resulting from the use of this product.
  The warranty is limited to this physical product itself. Please be aware of these points.
- The information contained in this document has been carefully checked and is believed to be reliable. However, if you find some of the contents to be missing or have questions regarding the contents, please contact us.
- All the company and product names used in this manual are registered trademarks or trademarks of the companies concerned.

Chapter 1

How to read the command reference

1.1 Applicable firmware revision

This command reference applies to firmware Yamaha L2 Switch SWP2 of Rev.2.03.22.
For the latest firmware released after printing of this command reference, manuals, and items that differ, access the following URL and see the information in the WWW server.
https://www.yamaha.com/proaudio/

1.2 How to read the command reference

This command reference describes the commands that you enter from the console of the Yamaha L2 Switch SWP2.

Each command is described by a combination of the following items.

[Syntax]	Explains the command input syntax. Key input can use either uppercase or lowercase characters.
	Command names are shown in bold (**Bold face**).
	The parameter portion is shown in italic (*Italic face*).
	Keywords are shown in normal characters.
	Parameters that can be omitted are enclosed in square brackets ([ ]).
[Keyword]	Explains the type and significance of keywords that can be specified for the command.
[Parameter]	Explains the type and significance of parameters that can be specified for the command.
[Initial value]	Displays the default setting value for the command.
[Input mode]	Indicates the modes in which the command can be executed.
[Description]	Explains the command.
[Note]	Explains points that you should be aware of when using the command.
[Example]	Provides specific examples of the command.

1.3 Interface names

In the command input syntax, interface names are used to specify each interface of the switch.
The following interface names are handled by the SWP2.

Interface type	Prefix	Description	Examples
LAN/SFP+ port	port	Used to specify a physical port. Specify "1" + "." + "port number" after the port number.	To specify LAN port #1: port1.1
VLAN interface	vlan	Used to specify a VLAN. Specify vlan followed by the "VLAN ID".	To specify VLAN #1: vlan1
static logical interface	sa	Used to specify link aggregation that combines multiple LAN/SFP+ port. Specify sa or po followed by "logical interface ID".	To specify static logical interface #1: sa1
LACP logical interface	po		To specify LACP logical interface #2: po2

1.4 Input syntax for commands starting with the word "no"

Many commands also have a form in which the command input syntax starts with the word **no**. If you use a syntax that with begins with the word **no**, the settings of that command are deleted and returned to the default value, unless explained otherwise.

Chapter 2

How to use the commands

The SWP2 lets you perform command operations in the following two ways.

Type of operation	Method of operation	Description
Operation via console	• Access from a console terminal • Access from a TELNET client • Access from a SSH client	Issue commands one by one to interactively make settings or perform operations.
Operation via a config file	• File transfer via TFTP • File transfer via GUI operation	A file containing a set of necessary commands (called a configuration or "config" file) is used to specify multiple settings, or to obtain multiple settings from the SWP2, in a single operation.

This chapter explains how to use each method.

2.1 Operation via console

2.1.1 Access from a console terminal

Use an RJ-45/DB-9 console cable when making settings from a terminal that is connected to the CONSOLE port of SWP2.

If you are using a computer as a console terminal (serial terminal), you'll need a terminal program to control the computer's serial (COM) port. Set the communication settings of the console terminal as follows.

Setting item	Value
Baud rate	9600bps
Data	8-bit
Parity	none
Stop bit	1-bit
Flow control	Xon/Xoff

For settings related to the console terminal, use the **line con** command to move to line mode.

2.1.2 Access from a TELNET client

You can use a TELNET client on a computer to connect to the TELNET server of the SWP2 and control it. In order to make settings using TELNET, you must first set up a connection environment (IP network) and then make TELNET server settings.

The IP address settings of the SWP2 are as follows.

- The default IPv4 address setting is ip address dhcp for VLAN #1.
- To change the IPv4 address, use the **ip address** command.

The TELNET server settings of the SWP2 are as follows.

- With the default settings of the TELNET server function, it runs on the default port (TCP port 23) and allows access only from VLAN #1 (vlan0.1).
- To change the reception port number, use the **telnet-server** command.
- Access to the TELNET server can be controlled in VLAN units, and can be specified by the **telnet-server interface** command.

A virtual communication port by which a TELNET client connects is called a "virtual terminal (VTY: Virtual TYpewriter) port." The maximum number of simultaneous TELNET client connections depends on the number of VTY ports of the SWP2. The VTY ports of the SWP2 are as follows.

- With the default VTY port settings, eight VTY ports (ID: 0--7) can be used.
- To check the number of VTY ports, use the **show running-config | include line vty** command.
- To change the number of VTY ports, use the **line vty** command. (maximum 8 (ID: 0--7))

To make VTY port settings, use the **line vty** command to specify the target VTY port, and then move to line mode. ID management for virtual terminal ports is handled within the SWP2, but since login session and ID assignments depend on the connection timing, you should normally make the same settings for all VTY ports.

2.1.3 Access from an SSH client

You can use an SSH client on a computer to connect to the SSH server of the SWP2 and control it. In order to make settings using SSH, you must first set up a connection environment (IP network) and then make SSH server settings.

The IP address settings of the SWP2 are as follows.

- The default IPv4 address setting is ip address dhcp for VLAN #1.
- To change the IPv4 address, use the **ip address** command.

The following settings on the SWP2 must be made beforehand when accessing from an SSH client.

- Generate a host key on the SSH server using the **ssh-server host key generate** command.
- Enable the SSH server functions using the **ssh-server** command.
- Register the user name and password using the **username** command.

The SSH server settings of the SWP2 are as follows.

- Access to an SSH server can be controlled for each VLAN, and is set using the **ssh-server interface** command.
- Note that the following functions are not supported.
- SSH protocol version 1
- User authentication aside from password authentication (host response authentication, public key authentication, challenge-response authentication, GSSAPI authentication)
- Port forwarding (X11/TCP forwarding)
- Gateway Ports (Port relay)
- Permitting blank passwords

A virtual communication port by which an SSH client connects is called a "virtual terminal (VTY: Virtual TYpewriter) port." The maximum number of simultaneous SSH client connections depends on the number of VTY ports of the SWP2. The VTY ports of the SWP2 are as follows.

- With the default VTY port settings, eight VTY ports (ID: 0--7) can be used.
- To check the number of VTY ports, use the **show running-config | include line vty** command.
- To change the number of VTY ports, use the **line vty** command. (maximum 8 (ID: 0--7))

To make VTY port settings, use the **line vty** command to specify the target VTY port, and then move to line mode. ID management for virtual terminal ports is handled within the SWP2, but since login session and ID assignments depend on the connection timing, you should normally make the same settings for all VTY ports.

2.1.4 Console terminal/VTY settings

The SWP2 lets you make the following settings for console terminals and VTY.

1. Timeout duration interpreted as no operation
2. Number of lines shown in one page of the terminal screen

Setting item	Content of setting
Timeout duration interpreted as no operation	Specifies the time after which the login session is forcibly ended when there has been no key input from the terminal. With the default setting, the session is forcibly disconnected after ten minutes. To make this setting, use the **exec-timeout** command of the line mode; this takes effect from the next session.

Setting item	Content of setting
Number of lines shown in one page of the terminal screen	Specifies the number of lines shown on one page of the terminal screen. This can be set as 0--512 lines/page, and the default setting is 24 lines/page. When displaying in this state, 23 lines are displayed, then "---More---" is displayed and the system waits for key input. There are two types of this setting, and they are applied to the system starting with the upper type. 1) unprivileged EXEC mode **terminal length** command 2) global configuration mode **service terminal-length** command Setting 1) is a function that temporarily applies to the user who is using the terminal, and is applied as soon as the command is executed. Setting 2) applies starting with the next session.

2.2 Operation via configuration (config) files

A file containing a set of needed commands is called a configuration (config) file.

The settings that have been made on the SWP2 can be read as a configuration file by a host on the LAN via TFTP. A configuration file on the host can also be loaded into the SWP2 to specify its settings.

A configuration file contains all the settings for the entire unit; it is not possible to partially read or write only the settings for a specific area. The configuration file is a text file consisting of ASCII + line-return (CRLF or LF).

The commands and parameters in a configuration file must be in the correct syntax. If the syntax or content are incorrect, that content is ignored and is not applied to operation.

2.2.1 Access from a TFTP client

In order to transfer a configuration file via TFTP, you must first set up a connection environment (IP network) and then make TFTP server settings.

The IP address settings of the SWP2 are as follows.

- The default IPv4 address setting is ip address dhcp for VLAN #1.
- To change the IPv4 address, use the **ip address** command.

The TFTP server settings of the SWP2 are as follows.

- With the default settings of the TFTP server function, it is running on the default port (UDP port 69) and does not allow access from anywhere.
- To change the reception port number, use the **tftp-server** command.
- Access to the TFTP server can be controlled in VLAN units, and can be specified by the **tftp-server interface** command. Specify the VLAN ID for which access is allowed.

2.2.2 Reading/writing a configuration file

Reading/writing a configuration file is performed by executing a TFTP command from the host on the LAN.

The following configuration files are read or written.

- configuration file

Applicable configuration	Applicable file	Description	Remarks
running-config	CONFIG file (.txt)	Setting values for current operation (Basic settings)	
startup-config (USER mode/DANTE mode)	CONFIG file (.txt)	Saved setting values (Basic settings)	USER mode : DIP switch #1 ON DANTE mode : DIP switch #1 OFF
	All setttings (.zip)	Saved setting values (All settings)	

Specify the following as the remote path of the configuration file read (GET) or write (PUT) destination.

- Remote path for applicable files (No automatic restart)

Applicable configuration	Applicable file	Remote path	Load (GET)	Save (PUT)	Automatic restart
running-config	CONFIG file (.txt)	config	✓	✓	-
startup-config (USER mode)	CONFIG file (.txt)	config0	✓	✓	-
	All settings (.zip)	config0-all	✓	✓	-
startup-config (DANTE mode)	CONFIG file (.txt)	config1	✓	-	-
	All settings (.zip)	config1-all	✓	-	-

If you want to restart the system automatically after applying the CONFIG file, specify the following remote path. The currently running configuration is applicable.

- Remote path for applicable files (with automatic restart)

Applicable configuration	Applicable file	Remote path	Load (GET)	Save (PUT)	Automatic restart
startup-config (USER mode)	CONFIG file (.txt)	reconfig	-	✓	✓
	All settings (.zip)	reconfig-all	-	✓	✓

When applying (PUT) a CONFIG file, confirm that the target CONFIG and the type of the target file are correct.

If an incorrect file is specified, it cannot be reflected correctly.

The command syntax used depends on the OS of that host (TFTP client). Keep the following points in mind when executing commands.

- IP address of the SWP2
- Use "binary mode" as the transmission mode.
- You must specify the administrator password after the remote path in the format "/PASSWORD".
  When the admin password is in the default state, you cannot read/write configuration files. The admin password must be changed first.
- If you PUT (write) with "config" specified as the remote path, the changes are added or overwritten to the current operating settings.
  Settings that you do not add or change will remain as the current operating settings.
  Since the setting values are not saved, you must use the **write** command etc. if you want to save them.
- The encrypted password (**password 8** or **enable password 8** command format) is not applied to the settings even if it is PUT to running-config via TFTP.
  And, users are not actually registered when making settings for users that include encrypted passwords (**username** command).

2.3 Login

When the SWP2 has finished starting up, a login screen is displayed.

You can log in by entering the configured user name and password.

By default, a default administrator is configured, and you can log in with the user name:**admin**and password:**admin**.

- Login screen

```
Username:admin
Password:
```

- Console screen following login

```
SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

SWP2>
```

When logging in as the default administrator for the first time, the password change screen is displayed. Change the password.

- Password change screen

```
Username:admin
Password:

SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.
```

```
Please change the default password for admin.
New Password:
New Password(Confirm):
Saving ...
Succeeded to write configuration
```

If the incorrect password is entered three times in a row, you will be restricted from logging in for one minute. After one minute has passed, please enter the correct password.

- Login restriction screen

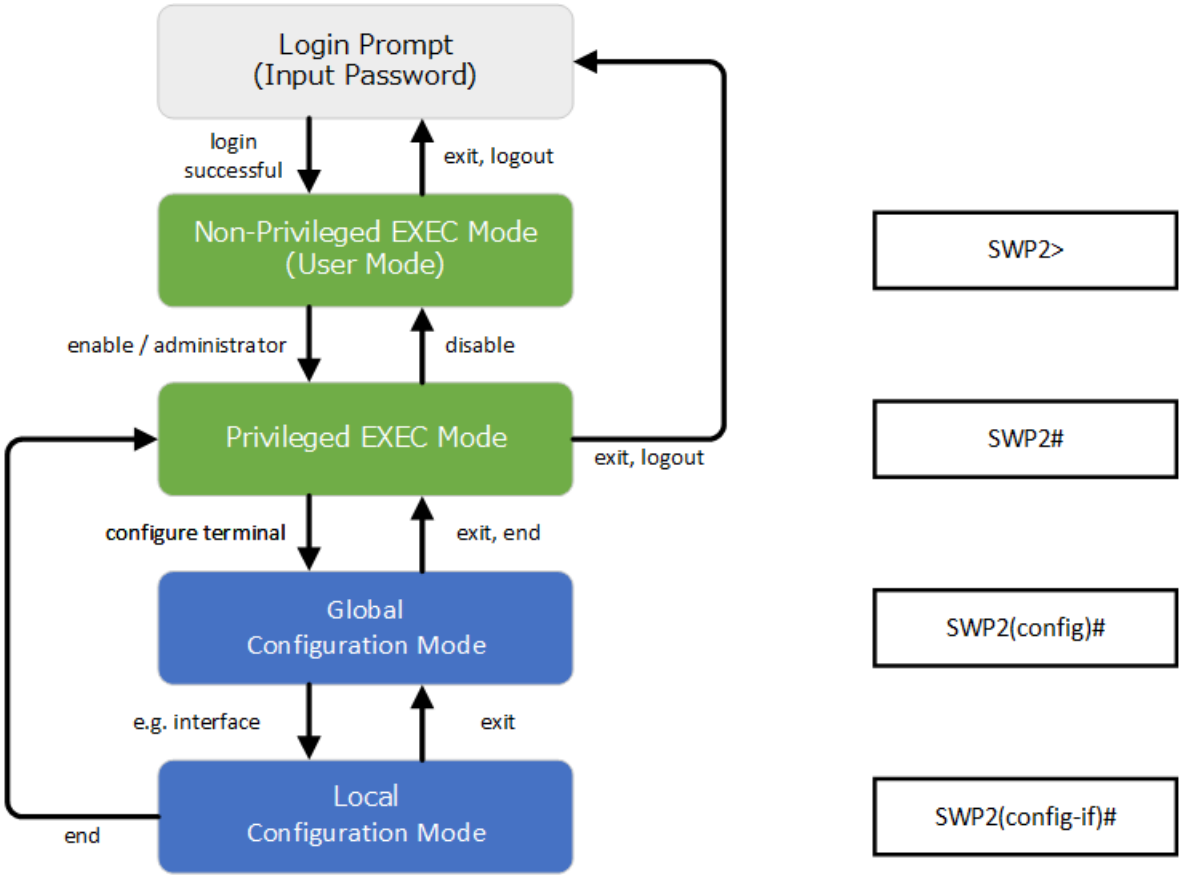
```
Username: user
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or blocked upon 3 failed login attempts for user.
% Please try again later.
```

- If a restricted user enters the wrong password again, the time limit will be refreshed.
- After the restriction time limit expires, you can log in by entering the correct password.

2.4 Command input mode

2.4.1 Command input mode basics

In order to change the settings of the SWP2 or to reference the status, you must move to the appropriate command input mode and then execute the command. Command input mode is divided into hierarchical levels as shown below, and the commands that can be entered in each mode are different. By noting the prompt, the user can see which mode they are currently in.



The basic commands related to moving between command input modes are described below. For commands that move from global configuration mode mode to individual configuration mode, refer to "individual configuration mode."

- **exit** command
- **logout** command
- **enable** command / **administrator**command
- **disable** command
- **configure terminal** command
- **end** command

2.4.2 individual configuration mode

individual configuration mode is the overall name for the mode in which you can make detailed settings for specific items such as LAN/SFP+ port, VLAN interface, and QoS. To enter individual configuration mode, issue the command for transitioning to the respective mode from global configuration mode.

On SWP2, individual configuration mode contains the following modes. Some of the modes within individual configuration mode have a hierarchy. For example, policy map mode → policy map class mode.

individual configuration mode	Transition command	Prompt
interface mode	**interface** command	SWP2(config-if)#
line mode	**line con** command **line vty** command	SWP2(config-line)#
VLAN mode	**vlan database** command	SWP2(config-vlan)#
VLAN access map mode	**vlan access-map** command	SWP2(config-vlan-access-map)#
MST mode	**spanning-tree mst configuration** command	SWP2(config-mst)#
class map mode	**class-map** command	SWP2(config-cmap)#
policy map mode	**policy-map** command	SWP2(config-pmap)#
policy map class mode	**class** command	SWP2(config-pmap-c)#
aggregate policer mode	**aggregate-police** command	SWP2(config-agg-policer)#
LLDP agent mode	**lldp-agent** command	SWP2(lldp-agent)#
E-mail template mode	**mail template** command	SWP2(config-mail)#
Schedule template mode	**schedule template** command	SWP2(config-schedule)#
RADIUS configuration mode	**radius-server local-profile** command	SWP2(config-radius)#

2.4.3 Command prompt prefix

he command prompt prefix indicates the host name. In the default state, the host name is the model name "SWP2". This indication can be changed by using the **hostname** command to specify the host name. In cases where multiple SWP2 units are used, management will be easier if separate names are assigned to each switch.

Changing the host name

```
SWP2(config)# hostname Switch-012
Switch-012(config)#
```

2.4.4 Executing commands of a different input mode

Because the commands that can be used on the SWP2 differ depending on the mode, you must transition to the mode in which a command can be executed before you execute that command. The **do** command is provided as a way to avoid this requirement.

By using the **do** command you can execute priviledged EXEC mode commands from any configuration mode. This allows you to reference the current configuration or save settings from any configuration mode without having to transition to priviledged EXEC mode.

However, since the completion function cannot be used with **do**, you must enter the command that follows either in its full spelling or in its abbreviated form.

- Entry in full spelling

  ```
  SWP2(config)#do show running-config
  ```
- Entry in abbreviated form

  ```
  SWP2(config)#do sh ru
  ```

2.5 Keyboard operations when using the console

2.5.1 Basic operations for console input

The SWP2 allows the following operations in the command line.

- Moving the cursor

Keyboard operation	Description and notes
→	Move right one character
←	Move left one character
Press Esc, then F	Move right one word (move to the character following the end of the word at the cursor location)
Press Esc, then B	Move left one word (move to the first character of the word at the cursor location)
Ctrl + A	Move to the beginning of the line
Ctrl + E	Move to the end of the line

- Deleting an input character

Keyboard operation	Description and notes
Backspace	Delete the character at the left of the cursor
Ctrl + H	
Ctrl + D	Delete the character at the cursor. If this operation is performed when the command line is empty, the result is the same as the **exit** command.
Press Esc, then D	Delete from the cursor position until immediately before the first space
Ctrl + K	Delete from the cursor position until the end of the line
Ctrl + U	Delete all characters that are being entered

- Other

Keyboard operation	Description and notes
Ctrl + T	Exchange the character at the cursor position with the preceding character. If the cursor is at the end of the line, exchange the preceding character with the character that precedes it.
Ctrl + C	In unprivileged EXEC mode and priviledged EXEC mode, discard the command being entered and move to the next line. In individual configuration mode, discard the command line being entered and move to priviledged EXEC mode. Command processing that is currently being executed will be stopped. (ex: **ping** command)
Ctrl + Z	Move from individual configuration mode to priviledged EXEC mode. This is the same operation as the **end** command.

2.5.2 Command help

By entering '?' in the command line you can search for the available commands or parameters.

```
SWP2#show vlan ?
  <1-4094>      VLAN id
  access-map    Show VLAN Access Map
  brief         VLAN information for all bridges (static and dynamic)
  filter        Show VLAN Access Map Filter
  private-vlan  private-vlan information

SWP2#show vlan
```

2.5.3 Input command completion and keyword candidate list display

If you press the "Tab" key while entering a command in the console, the command name is completed. If you press the "Tab" key after entering a keyword, a list of keyword candidates that can be entered next is shown. The same operation can also be performed by pressing the "Ctrl + I" key.

- Command name completion

```
SWP2#con "press the <Tab>key"
      ↓
SWP2#configure
```

- Keyword candidate list display

```
SWP2(config)#vlan "press the <Tab> key"
access-map  database    filter
SWP2(config)#vlan
```

2.5.4 Entering command abbreviations

When you enter commands or parameters in abbreviated form, and the characters you entered can be recognized unambiguously as a command or parameter, that command is executed.

Example of entering a command abbreviation (show running-config)

```
SWP2# sh run
```

2.5.5 Command history

By using the command history function, you can easily re-execute a command that you previously input, or partially modify a previously input command and re-execute it. Command history is shown as a history that is common to all modes.

Operation is shown below.

Keyboard operation	Description and notes
↑	Move backward through command history
Ctrl + P	
↓	Move forward through command history
Ctrl + N	

2.6 Commands that start with the word "show"

2.6.1 Modifiers

Modifiers send the information produced by the **show** command through a filter, restricting the content that is shown in the screen and making it easier for you to see the desired information.

The SWP2 provides the following three modifiers for the **show** command.

Modifiers	Description
include	Output only the lines that include the specified character string
grep	
exclude	Output only the lines that do not include the specified character string

Modifiers can be used only one at a time. You cannot specify more than one modifier.

- (Example) Using **show running-config** to view information that includes VLAN #1 (vlan1).

```
SWP2#show running-config | grep vlan1
interface vlan1
http-server interface vlan1
telnet-server interface vlan1
```

- (Example) Using **show spanning-tree** to view information that includes Role.

```
SWP2# show spanning-tree | include Role
%   po1: Port Number 505 - Ifindex 4601 - Port Id 0x81f9 - Role Disabled - State
Discarding
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Disabled -
```

```
State Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Disabled -
State Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Disabled -
State Forwarding
%   port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled -
State Forwarding
%   port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled -
State Forwarding
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled -
State Forwarding
%   port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled -
State Forwarding
%   port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled -
State Forwarding
```

Chapter 3

Configuration

3.1 Manage setting values

The SWP2 uses the following configurations to manage its settings.

Types of configuration	Description	User operations that can be performed
Running configuration (running-config)	Setting values currently used for operation. Managed in RAM.	Note Save to startup configuration (in USER mode) Save some functions to backup configuration (in DANTE mode)
Startup configuration (startup-config)	In USER mode, setting values saved in Flash ROM. In DANTE mode, the same setting values as the default configuration.	Note Update by running configuration (in USER mode)
Backup configuration (backup-config)	Setting values for some functions saved in DANTE mode. Managed in Flash ROM.	Update by running configuration (in DANTE mode)
Default configuration (default-config)	Default setting values. Managed in Flash ROM. Created based on the VLAN preset that is selected by the settings of DIP switches #2/#3 at start-up.	No operations possible

The start-up flow for the SWP2 system is as follows.

1. Reference DIP switch #1 and determine the CONFIG mode
   - If DIP switch #1 is up (OFF), start up in DANTE mode
   - If DIP switch #1 is down (ON), start up in USER mode
2. Determine the startup configuration for each CONFIG mode
   - For DANTE mode
     - Use the default configuration that was selected according to the settings of DIP switches #2/#3
   - For USER mode
     - If a startup configuration for USER mode exists, use the corresponding data
     - If a startup configuration for USER mode does not exist, use the default configuration that was selected according to the settings of DIP switches #2/#3.
3. Load the startup configuration into RAM as the running configuration
   - If a backup configuration exists in DANTE mode, overwrite the corresponding data onto the running configuration

If commands etc. are used to modify the settings while the SWP2 is running, the modified settings are immediately reflected in the running configuration. After modifying the running configuration, executing the **write** or **copy** command in USER mode will update the startup configuration. In DANTE mode, executing the **backup-config** command will update the backup configuration. If you restart without saving the content that was specified or modified, the settings or modifications are lost. Please be aware of this.

3.2 Default setting values

On the SWP2, the VLAN preset specified by DIP switches #2/#3 will be the default setting values. The VLAN preset types for DIP switch #2/#3 settings are as follows.

Note that the default values listed in this documentation are not applied for the factory settings, but the default settings listed below for each command are used instead.

- DIP switch #2/#3 settings

Setting position		VLAN preset type
#2	#3	
Up (OFF)	Up (OFF)	Normal
Down (ON)	Up (OFF)	A
Up (OFF)	Down (ON)	B
Down (ON)	Down (ON)	C

The common setting values and presets are shown first, and then the specific to the presets setting values are shown.

- Settings common to all presets (system-wide)

Category	Setting item	Default value
Terminal settings	Console timeout	600 sec
	Number of VTYs	8
	Number of lines displayed	24
User account	Default administrator	User name: admin, Password: admin
	Administrator password	admin
	Password encryption	not encrypted
Time management	Time zone	UTC (±0)
	NTP server	none
	NTP update cycle	once per hour
RMON	Behavior	enabled
sFlow	Behavior	disabled
Firmware update	Download URL	firmware-update url http://www.rtpro.yamaha.co.jp/ firmware/revision-up/swp2.bin
	Allow revision-down	don't allow
	Timeout	300 sec
LLDP	Behavior	disabled
	Automatically set function	disabled
L2MS	Behavior	enabled (can not change)
	Role	agent (can not change)
SYSLOG	Debug level log output	OFF
	Information level log output	ON
	Error level log output	ON
	SYSLOG server	none
Access control	Telnet server status	run
	Telnet server access	allow only VLAN #1
	SSH server status	do not run
	TFTP server status	do not run
	HTTP server status	run
	HTTP server access	allow only VLAN #1
	Secure HTTP server status	do not run
Maintenance VLAN	VLAN interface	VLAN #1

Category	Setting item	Default value
L2 switching	Automatic MAC address learning	enabled
	Automatic MAC address learning aging time	300 sec
	Spanning tree	enabled
	Proprietary loop detection	enabled
DNS cliant	Behavior	enabled
Traffic control	QoS	enabled
	QoS DSCP - transmission queue ID conversion table	DSCP: 8 → transmission queue: 2 DSCP: 26 → transmission queue: 3 DSCP: 34 → transmission queue: 4 DSCP: 48 → transmission queue: 5 Other than above → transmission queue: 0
	Flow control (IEEE 802.3x)	disabled
Web GUI	Language setting	English

- Settings common to all models and presets (LAN/SFP+ port)

Category	Setting item	Default value
Common setting	Speed/duplex mode setting	auto
	Cross/straight automatic detection	enabled
	MRU	1,522 Byte
	Port description	none
	EEE	disabled
	Port Mode	depends on preset
	Associated VLAN ID	depends on preset
L2MS	L2MS filter	depends on preset
L2 switching	Spanning tree	depends on preset
	Proprietary loop detection	enabled
Traffic control	QoS trust mode	DSCP
	Flow control (IEEE 802.3x)	disabled
	Storm control	disabled

- Default settings for the Normal VLAN preset of the SWP2 (entire system)

Category	Setting item	Default setting values
IP multicast control	Function to transmit IGMP/MLD query when topology changes	Enabled (wait time 5 sec)

- SWP2's VLAN preset Normal settings (LAN/SFP+ port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	-
port1.2	Disable	-	Access	1(default)	-
port1.3	Disable	-	Access	1(default)	-
port1.4	Disable	-	Access	1(default)	-
port1.5	Disable	-	Access	1(default)	-
port1.6	Disable	-	Access	1(default)	-

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP
port1.7	Disable	-	Access	1(default)	-
port1.8	Disable	-	Access	1(default)	-
port1.9	Disable	-	Access	1(default)	-
port1.10	Disable	-	Access	1(default)	-
port1.11	Disable	-	Access	1(default)	✓
port1.12	Disable	-	Access	1(default)	✓

- SWP2's VLAN preset Normal settings (VLAN interface)
  - VLAN #1(for Dante and Control)
    - IPv4 Address: DHCP
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30 sec
      - Fast-Leave : Disable
      - Check TTL : Disable
- Default settings for the Normal VLAN preset A of the SWP2 (entire system)

Category	Setting item	Default setting values
IP multicast control	Function to transmit IGMP/MLD query when topology changes	Enabled (wait time 5 sec)

- SWP2's VLAN preset A settings (LAN/SFP+ port)

Interface	L2MS Filter	LAG(static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	-
port1.2	Disable	-	Access	1(default)	-
port1.3	Disable	-	Access	1(default)	-
port1.4	Disable	-	Access	1(default)	-
port1.5	Disable	-	Access	2	-
port1.6	Disable	-	Access	2	-
port1.7	Disable	-	Access	1(default)	-
port1.8	Disable	-	Access	1(default)	-
port1.9	Disable	-	Access	2	-
port1.10	Disable	-	Access	2	-
port1.11	Disable	sa1	Trunk	1(native), 2	✓
port1.12	Disable				

- SWP2's VLAN preset A settings (VLAN interface)
  - VLAN #1(for Dante)
    - IPv4 Address: DHCP
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30 sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping: Disable
- Default settings for the Normal VLAN preset B of the SWP2 (entire system)

Category	Setting item	Default setting values
IP multicast control	Function to transmit IGMP/MLD query when topology changes	Enabled (wait time 5 sec)

- SWP2's VLAN preset B settings (LAN/SFP+ port)

Interface	L2MS Filter	LAG(static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	-
port1.2	Disable	-	Access	1(default)	-
port1.3	Disable	-	Access	1(default)	-
port1.4	Disable	-	Access	1(default)	-
port1.5	Disable	-	Access	2	-
port1.6	Disable	-	Access	2	-
port1.7	Disable	-	Access	1(default)	-
port1.8	Disable	-	Access	2	-
port1.9	Disable	sa1	Trunk	1(native), 2	✓
port1.10	Disable				
port1.11	Disable	sa2	Trunk	1(native), 2	✓
port1.12	Disable				

- SWP2's VLAN preset B settings (VLAN interface)
  - VLAN #1(for Dante)
    - IPv4 Address: DHCP
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30 sec
      - Fast-leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping: Disable
- SWP2's VLAN preset C settings (LAN/SFP+ port)

Interface	L2MS Filter	LAG(static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	-
port1.2	Disable	-	Access	1(default)	-
port1.3	Disable	-	Access	1(default)	-
port1.4	Enable	-	Access	2	-
port1.5	Enable	-	Access	2	-
port1.6	Enable	-	Access	2	-
port1.7	Disable	-	Access	1(default)	-
port1.8	Disable	-	Access	1(default)	-
port1.9	Enable	-	Access	2	-
port1.10	Enable	-	Access	2	-
port1.11	Disable	-	Access	1(default)	-
port1.12	Enable	-	Access	2	-

- SWP2's VLAN preset C settings (VLAN interface)
  - VLAN #1(for Dante)
    - IPv4 Address: DHCP

    - IGMP Snooping: Enable
        - Querier : Enable
        - Query Interval : 30 sec
        - Fast-leave : Disable
        - Check TTL : Disable
- VLAN #2(for Control)
    - IGMP Snooping: Enable
        - Querier : Enable
        - Query Interval : 30 sec
        - Fast-leave : Disable
        - Check TTL : Disable

Chapter 4

Maintenance and operation functions

4.1 Passwords

4.1.1 Set administrator password

[Syntax]

enable password *password*

[Parameter]

password : Administrator password

Single-type alphanumeric characters and " and ' and | and > and ? and single-byte symbols other than space characters (32 characters or less)

The first character must be a single-byte alphanumeric character

[Initial value]

enable password admin

[Input mode]

global configuration mode

[Description]

Specifies the administrator password needed to enter priviledged EXEC mode.

You cannot change it to the default password, "admin".

[Note]

If the password was encrypted by the **password-encryption** command, it is shown in the configuration in the form "**enable password** 8 *password*."

The user cannot enter the password in this form when making configuration settings from the command line.

Automatically set the default administrator password (admin) if no administrator password is set at boot.

[Example]

Specify admin1234 as the administrator password.

```
SWP2(config)#enable password admin1234
```

4.1.2 Encrypt password

[Syntax]

password-encryption *switch*
no password-encryption

[Parameter]

switch : Set password encryption

Setting value	Description
enable	Encrypt
disable	Don't encrypt

[Initial value]

password-encryption disable

[Input mode]

global configuration mode

[Description]

Enables password encryption.

If this is enabled, the password entered by the **password** command, the **enable password** command, and the **username** command are saved in the configuration in an encrypted form.

If this command is executed with the "no" syntax, password encryption is disabled, and the password entered by the **password** command, the **enable password** command, and the **username** command are saved in the configuration as plaintext.

[Note]

If password encryption is changed from disabled to enabled, previously-entered passwords are converted from plaintext to an encrypted form; however if it is changed from enabled to disabled, previously-encrypted passwords in a configuration file do not return to plaintext.

[Example]

Enables password encryption.

```
SWP2(config)#password-encryption enable
```

Disabled password encryption.

```
SWP2(config)#no password-encryption
```

4.2 User account maintenance

4.2.1 Set user

[Syntax]

username *username* [privilege *privilege*] password *password*
no username *username*

[Keyword]

privilege	:	Specifies the user's privileges
password	:	Specifies the user's password

[Parameter]

username : User name

Single-byte alphanumeric characters (32 characters or less)

privilege : Whether to grant privilege

Setting value	Description
on	Password input is not requested when moving to privileged EXEC mode Access to Web GUI is allowed with administrator privileges
off	Password input is requested when moving to privileged EXEC mode Access to Web GUI is allowed with guest

password : User's login password

Single-type alphanumeric characters and " and ' and | and > and ? and single-byte symbols other than space characters (32 characters or less)

The first character must be a single-byte alphanumeric character

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets user information.

A maximum of 33 items of user information can be registered. However, while there can be up to 32 privilege off users, 1 privilege on user is required.

The following words cannot be registered as user names.

lp, adm, bin, ftp, gdm, man, rpc, sys, xfs, halt, mail, news, nscd, sync, uucp, root, sshd, games, daemon, gopher, nobody, ftpuser, mtsuser, rpcuser, mailnull, operator, shutdown

The default password of "admin" cannot be used as a password.

[Note]

If the password was encrypted by the **password-encryption** command, it is shown in the configuration in the form "**username** *username* 8 password *password*."

The user cannot enter the password in this form when making configuration settings from the command line.

At boot, if no privilege on user has been set, a default administrator (admin/admin) is added.

At boot, users who do not have a password set will have their password set to the same string as the user name.

[Example]

Set the user "**user1234**".

```
SWP2(config)#username user1234 password user_pass
```

Set the privilege on user **user1234** .

```
SWP2(config)#username user1234 privilege on password user_pass
```

4.2.2 Changing User Permissions

[Syntax]

username *username* privilege *privilege*

[Keyword]

privilege	:	Specifies user permissions

[Parameter]

username	:	User name Up to 32 half-width alphanumeric characters
privilege	:	Whether or not privileges are granted

Setting value	Description
on	Users will not be prompted to enter a password when switching to privileged EXEC mode Web GUI can be accessed with Administrator permissions
off	Users will be prompted to enter a password when switching to privileged EXEC mode Web GUI can be accessed with Guest permissions

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Permissions of a registered users can be changed.

[Note]

Cannot be configured for unregistered users.

[Example]

Grants privileges to **user1234** registered users.

```
SWP2(config)#username user1234 privilege on
```

4.2.3 Show login user information

[Syntax]

show users

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode, global configuration mode

[Description]

Shows information on the current logged-in users.

The following items are shown.

Item	Description
Line	Shows the login method. **con 0** is the serial console port **vty N** is the VTY port **http N** is the Web GUI
Own	An ***** is shown for the line of one's own connection port.
User	Shows the currently logged-in user names.
Status	Shows the login status. If the user is in use, this indicates **Login**.
Login time	Shows the login time.
IP address	Shows the IP address of the connected user.

[Example]

Show login information for the users.

```
SWP2>show users

  Line    Own  User                                Status  Login time  IP address
-------------------------------------------------------------------------------
---------
  con  0       user1234                            Login   02:15:23
  vty  0   *   operators1                           Login   00:12:59    192.168.100.1
  vty  1       abcdefghijklmnopqrstuvwxyzabcdef    Login   00:00:50    192.168.100.24
  vty  2       -                                   Login   00:00:21    192.168.100.10
  vty  3       -                                   -       -
  vty  4       -                                   -       -
  vty  5       -                                   -       -
  vty  6       -                                   -       -
  vty  7       -                                   -       -
  http 0       user1234                            Login   01:12:25    192.168.100.4
  http 1       (noname)                            Login   00:18:04    192.168.100.102
  http 2       -                                   -       -
  http 3       -                                   -       -
```

4.2.4 Set banner

[Syntax]

banner motd *word*

no banner motd

[Parameter]

word : Single-byte alphanumeric characters and single-byte symbols (256 characters or less)

[Initial value]

no banner motd

[Input mode]

global configuration mode

[Description]

Sets the banner that is displayed when logging in to the console.

[Example]

Set the banner display to "Hello World!".

```
Username:
Password:

SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

SWP2>enable
SWP2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWP2(config)#banner motd Hello World!
SWP2(config)#exit
SWP2#exit

Username:
Password:

Hello World!

SWP2>enable
SWP2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWP2(config)#no banner motd
SWP2(config)#exit
SWP2#exit

Username:
Password:

SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

SWP2>
```

4.3 Configuration management

4.3.1 Save running configuration

[Syntax]

copy running-config startup-config

[Input mode]

priviledged EXEC mode

[Description]

Saves the current operating settings (running configuration) as the settings for startup (startup configuration).

[Note]

The save-destination startup configuration is determined by the unit's DIP switch #1 at the time that the unit is started.

The running configuration can also be saved by executing the **write** command and **save** command.

This command can be used to save settings only when in USER mode. When in DANTE mode, the **backup-config** command can be used to save some of the settings.

[Example]

Save the running configuration.

```
SWP2#copy running-config startup-config
Succeeded to write configuration
SWP2#
```

4.3.2 Save running configuration

[Syntax]

write
save

[Input mode]

priviledged EXEC mode, individual configuration mode

[Description]

Saves the current operating settings (running configuration) as the settings for startup (startup configuration).

[Note]

The save-destination startup configuration is determined by the unit's DIP switch #1 at the time that the unit is started.

The running configuration can also be saved by executing the **copy running-config startup-config** command.

This command can be used to save settings only when in USER mode. When in DANTE mode, the **backup-config** command can be used to save some of the settings.

[Example]

Save the running configuration.

```
SWP2#write
Succeeded to write configuration.
SWP2#
```

4.3.3 Save certain functions to the backup configuration

[Syntax]

backup-config

[Input mode]

priviledged EXEC mode

[Description]

Backup the settings of certain functions.

This applies to the following functions.

- Settings related to IPv4 addresses
- Settings related to time zone
- Settings related to user account
- Settings related to firmware updating
- Settings related to SYSLOG
- Settings related to HTTP server functions
- Settings related to Telnet server functions
- Settings related to SSH server functions
- Settings related to TFTP server functions

Saves the settings of certain functions to the backup configuration.

If a backup configuration exists when the SWP2 starts in DANTE mode, those settings are restored to the running configuration.

[Note]

This command can be used only when the configuration mode of the SWP2 is DANTE mode.

[Example]

Save the settings of the applicable functions to the backup configuration.

```
SWP2#backup-config
Succeeded to write backup configuration
SWP2#
```

4.3.4 Show the running configuration

[Syntax]

show running-config [*section*]
show config

[Parameter]

section : Section to be shown

Setting value	Description
access-list	Access list related
http-server	HTTP server related
interface	Interface related
ip	IP related
ipv6	IPv6 related
key	Authentication key related
l2ms	L2MS related
lldp	LLDP related
mail	E-mail notification-related
radius-server	RADIUS server related
schedule	Schedule related
sflow	sFlow-related
snmp	SNMP related
spanning-tree	STP related
ssh-server	SSH server related
telnet-sever	TELNET server related

[Input mode]

priviledged EXEC mode, individual configuration mode

[Description]

Shows the currently-operating settings (running configuration).

If *section* is not specified, all settings are shown.

[Example]

Show the running configuration.

```
SWP2#show running-config
!
interface port1.1
 switchport
...
!
line con 0
line vty 0 7
!
end

SWP2#
```

4.3.5 Show startup configuration

[Syntax]

show startup-config

[Input mode]

priviledged EXEC mode

[Description]

Shows the startup settings (startup configuration).

[Note]

The startup configuration that is shown is determined by the unit's DIP switch #1 at the time that the unit is started.

[Example]

Shows the startup settings (startup configuration) at next startup.

```
SWP2#show startup-config
!
!  Last Modified: Mon Jan 01 00:00:00 UTC 2018
!
qos enable
qos dscp-queue 0 0
qos dscp-queue 1 0
qos dscp-queue 2 0
qos dscp-queue 3 0
qos dscp-queue 4 0

...

!
telnet-server enable
!
line con 0
line vty 0 7
!
end
SWP2#
```

4.3.6 Show backup configuration

[Syntax]

show backup-config

[Input mode]

priviledged EXEC mode

[Description]

Shows the backup settings (backup configuration).

[Note]

Executing this command while operating in USER mode results in an error.

[Example]

Show the backup configuration.

```
SWP2#show backup-config
!
!  Last backup: Fri Sep 7 00:00:00 UTC 2018
!
interface vlan1
 ip address dhcp
!
interface vlan2
!
http-server enable
http-server language english
!
telnet-server enable
!
end
SWP2#
```

4.3.7 Erase startup configuration

[Syntax]

erase startup-config

[Input mode]

priviledged EXEC mode

[Description]

Erase the settings used at startup (startup config) and the information associated with them.

[Note]

The startup configuration that is erased is determined by the unit's DIP switch #1 at the time that the unit is started.

[Example]

Erase the startup configuration.

```
SWP2#erase startup-config
Succeeded to erase configuration.
SWP2#
```

4.3.8 Erase backup of certain functions

[Syntax]

erase backup-config

[Input mode]

priviledged EXEC mode

[Description]

Erase the settings of certain functions (backup config) and the information associated with them.

[Note]

Executing this command while operating in USER mode results in an error.

[Example]

Erase the backup configuration.

```
SWP2#erase backup-config
Succeeded to erase configuration.
SWP2#
```

4.4 Manage boot information

4.4.1 Show boot information

[Syntax]

show boot *num*
show boot all
show boot list

[Keyword]

all	:	Shows up to five entries of the boot information history
list	:	Shows a simplified version of up to five entries of the boot information history

[Parameter]

num	:	<0-4> Shows the boot history entry of the specified number

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Show the boot information.

[Note]

This history is cleared when you execute the **cold start** command or the **clear boot list** command.

[Example]

Show the current boot information.

```
SWP2>show boot
 Running EXEC: SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
Previous EXEC: SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
Restart by reload command
```

Shows a list of the boot history.

```
SWP2>show boot list
No. Date       Time     Info
--- ---------- -------- --------------------------------------------------
  0 2018/03/15 09:50:29 Restart by reload command
  1 2018/03/14 20:24:40 Power-on boot
--- ---------- -------- --------------------------------------------------
```

4.4.2 Clear boot information

[Syntax]

clear boot list

[Input mode]

priviledged EXEC mode

[Description]

Clears the boot information history.

[Example]

Clear the boot information.

```
SWP2#clear boot list
```

4.5 Show unit information

4.5.1 Show inventory information

[Syntax]

show inventory

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows inventory information for this unit and the SFP+ modules.

The following items are shown.

Item	Description
NAME	Name
DESCR	Description
Vendor	Vendor name
PID	Product ID
VID	Version ID, 0 if invalid
SN	Serial number

[Example]

Show inventory information.

```
SWP2>show inventory
NAME  : L2 switch
DESCR : SWP2
Vendor: Yamaha
```

```
PID   : SWP2
VID   : 0000
SN    : SMF00000

NAME  : SFP1
DESCR : 10G Base-LR
Vendor: Yamaha
PID   : YSFP-10G-LR
VID   : V1.0
SN    : Z5H00000YJ

NAME  : SFP2
DESCR : 10G Base-LR
Vendor: Yamaha
PID   : YSFP-10G-LR
VID   : V1.0
SN    : Z5H00001YJ

SWP2>
```

4.5.2 Show operating information

[Syntax]

show environment

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows information about the system's operating environment.

The following items are shown.

- Boot version
- Firmware revision
- Serial number
- MAC address
- CPU usage ratio
- Memory usage ratio
- Firmware file
- CONFIG mode
- VLAN preset (only in DANTE mode)
- Serial baud rate
- Boot time
- Current time
- Elapsed time from boot

[Example]

Show operating information.

```
SWP2>show environment
SWP2 BootROM Ver.1.01
SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
main=SWP2 ver=00 serial=S00000000 MAC-Address=ac44.f200.0000
CPU:   4%(5sec)   5%(1min)   5%(5min)    Memory:  25% used
Startup firmware: exec0
Configration mode: DANTE
VLAN preset: Normal
Serial Baudrate: 9600
Boot time: 2018/10/01 06:14:46 +00:00
Current time: 2018/10/01 06:49:23 +00:00
Elapsed time from boot: 0days 00:34:41

SWP2>
```

4.5.3 Disk usage status

[Syntax]

show disk-usage

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the usage status of the disk used by the system.

- Area used by the system (including settings information)
- Temporary : Temporary area

[Example]

Show the disk usage status.

```
SWP2#show disk-usage
  Category    Total    Used     Free     Used (%)
  ----------- -------- -------- -------- --------
  System       160.6M     1.1M   154.8M       1%
  Temporary     80.0M     2.4M    77.6M       3%
```

4.5.4 Show currently-executing processes

[Syntax]

show process

[Input mode]

priviledged EXEC mode

[Description]

Shows all currently-executing processes.

[Example]

Show currently-executing processes.

```
SWP2#show process
```

4.5.5 Display memory usage

[Syntax]

show memory

[Input mode]

priviledged EXEC mode

[Description]

Shows how much memory is used by each process.

The following items are shown.

Item	Explanation
PID	Process ID
NAME	Process name
%MEM	Percentage of physical memory used
SIZE	Amount of physical memory used (current value)
PEAK	Amount of physical memory used (maximum value until now)
DATA	Size of dynamic virtual memory area
STK	Stack size

[Example]

This shows how much memory is used by each process.

```
SWP2#show memory
```

4.5.6 Show technical support information

[Syntax]

show tech-support

[Input mode]

priviledged EXEC mode

[Description]

Show technical support information. The technical support information includes a list of the results of executing the following commands.

Command	Executable
show running-config	✓
show startup-config	✓
show environment	✓
show system-diagnostics	✓
show clock detail	✓
show disk-usage	✓
show dipsw	✓
show inventory	✓
show boot all	✓
show logging	✓
show process	✓
show users	✓
show interface	✓
show frame-counter	✓
show vlan brief	✓
show spanning-tree mst detail	✓
show etherchannel status detail	✓
show loop-detect	✓
show mac-address-table	✓
show l2ms detail	✓
show qos queue-counters	✓
show ddm status	✓
show errdisable	✓
show auth status	✓
show auth supplicant	✓
show error port-led	✓
show ip interface brief	✓
show ip forwarding	✓
show ipv6 interface brief	✓
show ipv6 dhcp interface	✓
show ipv6 forwarding	✓
show ip route	✓
show ip route database	✓

Command	Executable
show ipv6 route	✓
show ipv6 route database	✓
show arp	✓
show ipv6 neighbors	✓
show ip igmp snooping groups	✓
show ip igmp snooping interface	✓
show ipv6 mld snooping groups	✓
show ipv6 mld snooping interface	✓
show radius-server local certificate status	✓
show radius-server local nas	✓
show radius-server local user	✓
show radius-server local certificate list	✓
show radius-server local certificate revoke	✓
show sflow	✓
show sflow sampling	✓

[Example]

Show technical support information.

```
SWP2#show tech-support
#
# Information for Yamaha Technical Support
#

*** show running-config ***
!
!  - Running Configuration -
!  Current Time:  Fri Jan 1 00:00:00 JST 2021
!
dns-client enable
!
vlan database
 vlan 2 name VLAN0002
 vlan 3 name VLAN0003
!
interface port1.1
 switchport
 switchport mode access
...

*** show startup-config ***
...

*** show environment ***
...

*** show disk-usage ***
...

*** show dipsw ***
...
...
...

#
# End of Information for Yamaha Technical Support
#

SWP2#
```

4.6 System self-diagnostics

4.6.1 Showing system self-diagnostics results

[Syntax]

show system-diagnostics

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows all system self-diagnostics results (bootup diagnostics, on-demand diagnostics, and health-monitoring diagnostics).

[Example]

Shows system self-diagnostics results.

```
SWP2#show system-diagnostics
Test results: (P = Pass, F = Fail, U = Untested, N = Normal, W = Warning)

- Bootup
  Loading Test: Pass

  RTC Test: Pass

   . . .

- On-demand
Last on-demand diagnostics information:
 Date     : 2021/07/07 09:00:00 +09:00
 BootROM  : Ver.1.00
 Firmware : Rev.2.06.07
 . . .

  PHY Test:
    Port   1   2   3   4   5   6   7   8   9  10  11  12
    ------------------------------------------------------
           P   P   P   P   P   P   P   P   P   P   P   P

   . . .

- Health monitoring
   . . .

  SFP Test:
    Port  13  14  15  16
    --------------------
           N   N   N   N
```

4.6.2 Executing on-demand diagnostics

[Syntax]

system-diagnostics on-demand execute [no-confirm]

[Keyword]

no-confirm : Execute on-demand diagnostics immediately without an execution check (y or n)

[Input mode]

priviledged EXEC mode

[Description]

Executes on-demand diagnostics.

Shut down all LAN/SFP+ port during the diagnostics. At the end of the diagnostics, simple diagnostic results are shown and the system is automatically rebooted.

If no parameters are specified, confirmation is requested as to whether to execute on-demand diagnostics.

You must enter "y” to execute diagnostics or "n" to not execute diagnostics.

[Note]

Detailed on-demand diagnostics results can be checked after reboot by using the **show system-diagnostics** command.

[Example]

Executes on-demand diagnostics.

```
SWP2#system-diagnostics on-demand execute
The system will be rebooted after diagnostics. Continue ? (y/n) y
on-demand diagnostics completed (pass). reboot immediately...
```

4.6.3 Clearing the on-demand diagnostics results

[Syntax]

clear system-diagnostics on-demand

[Input mode]

priviledged EXEC mode

[Description]

Clears the on-demand diagnostics results.

[Example]

Clears the on-demand diagnostics results.

```
SWP2#clear system-diagnostics on-demand
```

4.7 Cable diagnostics

4.7.1 Execute cable diagnostics

[Syntax]

cable-diagnostics tdr execute interface *ifname*
test cable-diagnostics tdr interface *ifname*

[Parameter]

ifname	:	LAN port interface name Target interface

[Input mode]

priviledged EXEC mode

[Description]

Execute cable diagnostics. The previous diagnostic result can be viewed with the show cable-diagnostics tdr command.

[Note]

Only the prior diagnostic result is stored, and the result is overwritten when executing the cable diagnostics again.

[Example]

Execute diagnostics on the LAN cable connected to port1.1.

```
SWP2#cable-diagnostics tdr execute interface port1.1
The port will be temporarily down during test. Continue? (y/n): y
% To check result, enter "show cable-diagnostics tdr"
```

4.7.2 Clear cable diagnostic results

[Syntax]

clear cable-diagnostics tdr
clear test cable-diagnostics tdr

[Input mode]

priviledged EXEC mode

[Description]

Clears the results of the prior cable-diagnostics tdr execute interface command execution.

[Example]

Clear the results of the prior cable diagnostic execution.

```
SWP2#clear cable-diagnostics tdr
SWP2#
```

4.7.3 Display cable diagnostic results

[Syntax]

show cable-diagnostics tdr
show test cable-diagnostics tdr

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Displays the result of the prior cable-diagnostics tdr execute interface command execution.

[Example]

Display the result of the last cable diagnostic execution.

```
SWP2#show cable-diagnostics tdr
Last run on Tue May 31 14:29:35 2022
Port      Pair  Status  Fault distance
-----------------------------------------
port1.8   1     OK      -
          2     OK      -
          3     Open    15   m
          4     Open    15   m
```

4.8 Time management

4.8.1 Set clock manually

[Syntax]

clock set *time month day year*

[Parameter]

time	:	hh:mm:ss
		Time
month	:	<1-12> or Jan, Feb, Mar, ... , Dec
		Month or name of month
day	:	<1-31>
		Day
year	:	Year (four digits)

[Input mode]

priviledged EXEC mode

[Description]

Set the system time.

[Example]

Set the time to 0 hours 0 minutes 0 seconds on January 1, 2015.

```
SWP2#clock set 00:00:00 Jan 1 2015
```

4.8.2 Set time zone

[Syntax]

clock timezone *zone*
clock timezone *offset*
no clock timezone

[Parameter]

zone	:	UTC, JST
		Name of the time zone shown when standard time is in effect
offset	:	-12:00, -11:00, ... , -1:00, +1:00, ... , +13:00
		Enter the difference from UTC

[Initial value]

clock timezone UTC

[Input mode]

global configuration mode

[Description]

Sets the time zone.
If this command is executed with the "no" syntax, UTC is specified.

[Example]

Set the time zone to JST.

```
SWP2(config)#clock timezone JST
```

Set the time zone to UTC+9 hours.

```
SWP2(config)#clock timezone +9:00
```

4.8.3 Configuring daylight saving time (recurring)

[Syntax]

clock summer-time *name* **recurring** *week wday month time week wday month time* [*offset*]
no clock summer-time

[Parameter]

name	:	Time zone name to be displayed when daylight saving time is in effect
		Alphanumeric characters (up to 7 characters)
week	:	<1-4> or first, last
		Specifies the week of the month
wday	:	Sun, Mon, Tue, ... , Sat
		Day of the week
month	:	<1-12> or Jan, Feb, Mar, ... , Dec
		Month or month name
time	:	hh:mm
		Time
offset	:	<1-1440>
		Time to add during daylight saving time. Specify in minutes. The default value is 60.

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Configure daylight saving time.

Configure daylight saving time to start and end on a specified week and day of the week every year.

The first part specifies the daylight saving time start period and the second part specifies the end period.

If this command is executed with the "no" syntax, the setting is cleared.

[Note]

Daylight saving times cannot overlap.

[Example]

Set daylight saving time to start at 2 AM on the second Sunday of March and end at 2 AM on the first Sunday of November every year.

```
SWP2(config)#clock summer-time JDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00
```

4.8.4 Configuring daylight saving time (by date)

[Syntax]

clock summer-time *name* **date** *month day year time month day year time* [*offset*]
no clock summer-time

[Parameter]

name	:	Time zone name to be displayed when daylight saving time is in effect
		Alphanumeric characters (up to 7 characters)
month	:	<1-12> or Jan, Feb, Mar, ... , Dec
		Month or month name
day	:	<1-31>
		Day
year	:	Year (4 digits)
time	:	hh:mm
		Time
offset	:	<1-1440>
		Time to add during daylight saving time. Specify in minutes. The default value is 60.

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Configure daylight saving time.

Configure daylight saving time to start and end on specified dates.

The first part specifies the daylight saving time start date and the second part specifies the end date.

If this command is executed with the "no" syntax, the setting is cleared.

[Note]

Daylight saving times cannot overlap.

[Example]

Set daylight saving time to start on March 14, 2021 at 2 AM and end on November 7, 2021 at 2 AM.

```
SWP2(config)#clock summer-time JDT date Mar 14 2021 2:00 Nov 7 2021 2:00
```

4.8.5 Show current time

[Syntax]

show clock [detail]

[Keyword]

detail	:	Also display detailed information

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the current time, year, month, and date.

When detail is specified, detailed information (current time and daylight saving time) is displayed.

If daylight saving time is recurring, it displays the actual date of the next (or currently in effect) daylight saving time period.

[Example]

Show current time.

```
SWP2>show clock
Thu Jan 1 00:00:00 JST 2015
```

Display detailed information about the current time. (If daylight saving time is configured)

```
SWP2>show clock detail
Thu Jan 1 00:00:00 JST 2021

Summer Time
  Type   : Recurring
  Offset : 60 (min)
  From   : Sun Mar 14 02:00:00 JST 2021
  To     : Sun Nov 7 02:00:00 JDT 2021
```

Display detailed information about the current time. (If daylight saving time is not configured)

```
SWP2>show clock detail
SWX3220>show clock detail
Thu Jan 1 00:00:00 JST 2021

Summer Time Disabled
```

4.8.6 Set NTP server

[Syntax]

ntpdate server ipv4 *ipv4_addr*
ntpdate server ipv6 *ipv6_addr*
ntpdate server name *fqdn*
no ntpdate server

[Keyword]

ipv4	:	Specify the NTP server by IPv4 address
ipv6	:	Specify the NTP server by IPv6 address
name	:	Specify the NTP server by host name

[Parameter]

ipv4_addr	:	IPv4 address of the NTP server
ipv6_addr	:	IPv6 address of the NTP server If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)
fqdn	:	Host name of the NTP server As character types, alphabetical characters (uppercase/lowercase), numerals, . (period), and - (hyphen) can be used

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Registers the address or host name of the NTP server.

Up to two instances of this command can be set.

If this command is executed with the "no" syntax, the NTP server setting is deleted.

If time synchronization is performed with two NTP servers specified, they are queried in the order of NTP server 1 and NTP server 2 as shown by the **show ntpdate** command.

The query to NTP server 2 is performed only if synchronization with NTP server 1 fails.

[Example]

Specify 192.168.1.1 as the NTP server.

```
SWP2(config)#ntpdate server ipv4 192.168.1.1
```

Specify fe80::2a0:deff:fe11:2233%vlan1 as the NTP server.

```
SWP2(config)#ntpdate server ipv6 fe80::2a0:deff:fe11:2233%vlan1
```

Specify ntp.example.com as the NTP server.

```
SWP2(config)#ntpdate server name ntp.example.com
```

4.8.7 Synchronize time from NTP server (one-shot update)

[Syntax]

ntpdate oneshot

[Input mode]

priviledged EXEC mode

[Description]

Attempts to obtain time information from the registered NTP server.

This is performed only once when this command is executed.

[Example]

Obtain time information from the NTP server.

```
SWP2#ntpdate oneshot
```

4.8.8 Synchronize time from NTP server (update interval)

[Syntax]

ntpdate interval *interval-time*
no ntpdate interval

[Parameter]

interval-time : <0-24>

Interval (hours) for time synchronization. If this is set to 0 hours, periodic synchronization will not occur.

[Initial value]

ntpdate interval 1

[Input mode]

global configuration mode

[Description]

Specifies the interval (in one-hour units) at which time information is periodically obtained from the registered NTP server.

If this command is executed with the "no" syntax, the setting returns to the default.

When this command is executed, the time is updated immediately, and is subsequently updated at the specified interval.

[Example]

Request the time every two hours.

```
SWP2(config)#ntpdate interval 2
```

Disable periodic time synchronization.

```
SWP2(config)#ntpdate interval 0
```

4.8.9 Show NTP server time synchronization settings

[Syntax]

show ntpdate

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the settings that are related to time synchronization from an NTP server.

[Example]

Show time synchronization settings. *If the synchronization update interval is one hour

```
SWP2#show ntpdate
NTP Server 1 : ntp.nict.jp
NTP Server 2 : none
adjust time : Thu Jan 1 09:00:00 2015 + interval 1 hour
sync server : ntp.nict.jp
```

Show time synchronization settings. *If periodic synchronization is not being performed

```
SWP2#show ntpdate
NTP Server 1 : ntp.nict.jp
NTP Server 2 : none
adjust time : Thu Jan 1 09:00:00 2015
sync server : ntp.nict.jp
```

4.9 Terminal settings

4.9.1 Move to line mode (console terminal)

[Syntax]

line con *port*

[Parameter]

port : 0

Serial console port number

[Initial value]

line con 0

[Input mode]

global configuration mode

[Description]

Moves to line mode in order to make console terminal settings.

[Note]

To return from line mode to global configuration mode, use the **exit** command. To return to priviledged EXEC mode, use the **end** command.

[Example]

Move to line mode in order to make console terminal settings.

```
SWP2(config)#line con 0
SWP2(config-line)#
```

4.9.2 Set VTY port and move to line mode (VTY port)

[Syntax]

line vty *port1* [*port2*]
no line vty *port1* [*port2*]

[Parameter]

port1	:	<0-7>
		VTY port number
port2	:	<0-7>
		Last VTY port number when specifying a range

[Initial value]

no line vty 0 7

[Input mode]

global configuration mode

[Description]

After enabling the specified VTY ports, moves to line mode for making VTY port settings.

If this command is executed with the "no" syntax, the specified VTY ports are disabled.

If you specify *port2*, a range of ports is specified; all VTY ports from *port1* through *port2* are specified. *port2* must be a number greater than *port1*.

[Note]

The maximum number of simultaneous Telnet client connections depends on the number of VTY ports that are enabled.

To return from line mode to global configuration mode, use the **exit** command. To return to priviledged EXEC mode, use the **end** command.

[Example]

Enable VTY port #0 and then move to line mode.

```
SWP2(config)#line vty 0
SWP2(config-line)#
```

4.9.3 Set terminal login timeout

[Syntax]

exec-timeout *min* [*sec*]
no exec-timeout

[Parameter]

min	:	<0-35791>
		Timeout time (minutes)
sec	:	<0-2147483>
		Timeout time (seconds)

[Initial value]

exec-timeout 10

[Input mode]

line mode

[Description]

Sets the time after which automatic logout occurs if there has been no key input from the console terminal or VTY.

If *sec* is omitted, 0 is specified. If *min* and *sec* are both set to 0, automatic logout does not occur.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

After this command is executed, the setting is applied starting at the next login.

[Example]

Set the console timeout time to five minutes.

```
SWP2(config)#line con 0
SWP2(config-line)#exec-timeout 5 0
SWP2(config-line)#
```

4.9.4 Change the number of lines displayed per page for the terminal in use

[Syntax]

terminal length *line*
terminal no length

[Parameter]

line : <0-512>

Number of lines displayed per page on the terminal

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Changes the number of lines displayed per page for the terminal in use.

If *line* is set to 0, the display is not paused per page.

If the **terminal no length** command is executed, the number of lines is set to 24 in the case of a serial console, or to the window size when connected in the case of VTY.

[Note]

When this command is executed, the change applies immediately.

The result of executing this command takes priority over the setting applied by the **service terminal-length** command.

[Example]

Change the number of lines displayed per page for the terminal in use to 100 lines.

```
SWP2>terminal length 100
SWP2>
```

4.9.5 Set the number of lines displayed per page on the terminal

[Syntax]

service terminal-length *line*
no service terminal-length

[Parameter]

line : <0-512>

Number of lines displayed per page on the terminal

[Initial value]

no service terminal-length

[Input mode]

global configuration mode

[Description]

Sets the number of lines displayed per page on the terminal.

If *line* is set to 0, the display is not paused per page.

If this command is executed with the "no" syntax, the number of lines is set to 24 in the case of a serial console, or to the window size when connected in the case of VTY.

[Note]

After this command is executed, the setting is applied starting at the next login.

If the **terminal length** command is executed, the result of executing the **terminal length** command takes priority.

[Example]

Change the number of lines displayed per page for the terminal in use to 100 lines.

```
SWP2(config)#service terminal-length 100
SWP2(config)#
```

4.10 Management

4.10.1 Set management VLAN

[Syntax]

management interface *interface*
no management interface

[Parameter]

interface : VLAN interface name

[Initial value]

management interface vlan1

[Input mode]

global configuration mode

[Description]

Set the VLAN that is used for management.

By setting this command, it will be possible to set and acquire the IP address assigned by the L2MS manager to the corresponding VLAN when operating as an L2MS agent.

If this is executed with the "no" syntax, or if the VLAN is deleted, this command also returns to the default settings.

[Example]

Set VLAN #2 as the management VLAN.

```
SWP2(config)#management interface vlan2
```

4.11 SYSLOG

4.11.1 Set log notification destination (SYSLOG server)

[Syntax]

logging host *host*
no logging host *host*

[Parameter]

host : A.B.C.D

IPv4 address of the SYSLOG server

: X:X::X:X

IPv6 address of the SYSLOG server

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

[Initial value]

no logging host

[Input mode]

global configuration mode

[Description]

Specifies the IP address of the SYSLOG server to which log notifications are sent.

Up to 2 entries can be specified.

If this command is executed with the "no" syntax, the setting returns to its default value, and notifications are not sent.

[Example]

Set the SYSLOG server IPv4 address to 192.168.100.1.

```
SWP2(config)#logging host 192.168.100.1
```

Set the SYSLOG server IPv6 address to fe80::2a0:deff:fe11:2233.

```
SWP2(config)#logging host fe80::2a0:deff:fe11:2233%vlan1
```

4.11.2 Setting the notification format of the log

[Syntax]

logging format *type*
no logging format

[Parameter]

type : Log format type

Setting value	Description
legacy	Proprietary format that does not include the header section (time stamp, host name)

[Initial value]

no logging format

[Input mode]

global configuration mode

[Description]

Change the format of messages sent to the SYSLOG server.

If this command is executed with the "no" syntax, the header (time stamp, host name) is included in the SYSLOG message.

[Example]

Sets the format of the SYSLOG message to no header.

```
SWP2(config)#logging format legacy
```

4.11.3 Setting the log facility value

[Syntax]

logging facility *facility*
no logging facility

[Parameter]

facility : Log facility value

Setting value	Description
0..23	facility value
user	1
local0..local7	16..23

[Initial value]

logging facility local0

[Input mode]

global configuration mode

[Description]

Change the facility value of messages sent to the SYSLOG server.

[Note]

The meanings of the facility values are assigned independently on each SYSLOG server.

[Example]

Set the facility value of the SYSLOG message to 10.

```
SWP2(config)#logging facility 10
```

4.11.4 Set log output level (debug)

[Syntax]

logging trap debug
no logging trap debug

[Initial value]

no logging trap debug

[Input mode]

global configuration mode

[Description]

Output the debug level log to SYSLOG. If this command is executed with the "no" syntax, the log is not output.

Since enabling debug level will output a large volume of log data, you should enable this only if necessary.

If you use the **logging host** command to send notifications to the SYSYLOG server, you should ensure that there is sufficient disk space on the host. With the default setting, this is not output.

[Example]

Output the debug level log to SYSLOG.

```
SWP2(config)#logging trap debug
```

4.11.5 Set log output level (informational)

[Syntax]

logging trap informational
no logging trap informational

[Initial value]

logging trap informational

[Input mode]

global configuration mode

[Description]

Outputs the informational level log to SYSLOG.

If this command is executed with the "no" syntax, the log is not output.

[Note]

This can be output to the console by executing the **logging stdout info** command.

[Example]

Output the informational level log to SYSLOG.

```
SWP2(config)#logging trap informational
```

4.11.6 Set log output level (error)

[Syntax]

logging trap error
no logging trap error

[Initial value]

logging trap error

[Input mode]

global configuration mode

[Description]

Outputs the error level log to SYSLOG.

If this command is executed with the "no" syntax, the log is not output.

[Example]

Output the error level log to SYSLOG.

```
SWP2(config)#logging trap error
```

4.11.7 Set log console output

[Syntax]

logging stdout info
no logging stdout info

[Initial value]

no logging stdout info

[Input mode]

global configuration mode

[Description]

Outputs the informational level SYSLOG to the console.

If this command is executed with the "no" syntax, the log is not output.

[Example]

Output the informational level SYSLOG to the console.

```
SWP2(config)#logging stdout info
```

4.11.8 Back up log

[Syntax]

save logging

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Saves all logs accumulated in RAM to Flash ROM.

Logs are accumulated in RAM, and are periodically backed up automatically to Flash ROM, but you can use this command to back up this data manually.

[Example]

Back up the log.

```
SWP2#save logging
```

4.11.9 Clear log

[Syntax]

clear logging

[Input mode]

priviledged EXEC mode

[Description]

Clears the log.

[Example]

Clear the log.

```
SWP2#clear logging
```

4.11.10 Show log

[Syntax]

show logging [reverse]

[Keyword]

reverse	:	Shows the log in reverse order

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the log that records the operating status of the unit. Normally the log is shown starting with the oldest events, but the display order is reversed if "reverse" is specified.

The log contains a maximum of 10,000 events. If this maximum number is exceeded, the oldest events are successively deleted. In order to save more than the maximum number of logs, you must use the **logging host** command to forward the log to the SYSLOG server and save it on the host.

The level of log events to be output can be specified by the **logging trap** command.

[Note]

Log events are accumulated in RAM, and are automatically backed up to Flash ROM at regular intervals. When the power is turned off, log entries that are not backed up will not be saved, so you must back them up manually if you want to save the log.

The log is maintained when the **reload** command or a firmware update etc. cause a reboot.

[Example]

Show the log.

```
SWP2#show logging
```

4.12 SNMP

4.12.1 Set host that receives SNMP notifications

[Syntax]

snmp-server host *host_address type* **version** *version community*
snmp-server host *host_address type* **version** *version seclevel user*
no snmp-server host *host_address*
no snmp-server host *host_address type* **version** *version community*
no snmp-server host *host_address type* **version** *version seclevel user*

[Parameter]

host_address	:	Destination IPv4 address or IPv6 address for notifications If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)
type	:	Notification message

Setting value	Description
traps	Send notifications as traps (without response confirmation)
informs	Send notifications as inform requests (with response confirmation). This can be specified if *version* is '2c' or '3'.

version : SNMP version

Setting value	Description
1	Use SNMPv1
2c	Use SNMPv2c
3	Use SNMPv3

community : Community name (maximum 32 characters)

This can be specified if *version* is '1' or '2c'

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

seclevel : Security level requested for authenticating the notification

This can be specified only if *version* is '3'

Setting value	Description
noauth	No authentication / No encryption (noAuthNoPriv)
auth	Authentication / No encryption (authNoPriv)
priv	Authentication / Encryption (authPriv)

user : User name (maximum 32 characters)

This can be specified only if *version* is '3'

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Set the destination of SNMP notifications.

Up to 8 entries can be specified.

If this command is executed with the "no" syntax, the specified destination hosts are deleted.

[Note]

Note that if this is specified as an IPv6 link local address, and you add a setting that specifies a different transmitting interface for the same address, the combination of address and transmitting interface is considered to have changed, and all settings of the old combination are deleted. For example if there are multiple settings that specify "fe80::10%vlan1" and you newly add the setting "fe80::10%vlan2," all settings for "fe80::10%vlan1" are deleted, and only the settings of the added "fe80::10%vlan2" will remain.

[Example]

Using SNMPv1, set 192.168.100.11 as the destination for traps. Set "snmptrapname" as the trap community name.

```
SWP2(config)#snmp-server host 192.168.100.11 traps version 1 snmptrapname
```

Using SNMPv2c, set 192.168.100.12 as the destination for notifications. Specify the notification type as informs, and the notification screen community name as "snmpinformsname".

```
SWP2(config)#snmp-server host 192.168.100.12 informs version 2c snmpinformsname
```

Using SNMPv3, set 192.168.10.13 as the destination for notifications. Set the notification type to traps, set the security level for transmission to priv, and set the user name to "admin1".

```
SWP2(config)#snmp-server host 192.168.10.13 traps version 3 priv admin1
```

4.12.2 Setting the time to wait before sending a notification message at system boot

[Syntax]

snmp-server startup-trap-delay *sec*
no snmp-server startup-trap-delay

[Parameter]

sec : <10-600>
Wait time (seconds)

[Initial value]

snmp-server startup-trap-delay 10

[Input mode]

global configuration mode

[Description]

Sets the time to wait before sending an SNMP notification message (trap) at system startup.

SNMP notification messages generated after system boot and before the wait time has elapsed will be sent after the wait time has elapsed.

If this command is executed with the "no" syntax, the setting is cleared.

[Note]

The wait time measurement starts and ends at the timing at which the following logs are output.

```
[    SNMP]:dbg: SNMP startup trap delay timer start (delay_sec : XX)
[    SNMP]:dbg: SNMP startup trap delay timer end (delay_sec : XX)
```

[Example]

Set the time to wait before sending an SNMP notification message at system startup to 30 seconds.

```
SWP2(config)#snmp-server startup-trap-delay 30
```

4.12.3 Set notification type to transmit

[Syntax]

snmp-server enable trap *trap_type* [*trap_type*]
no snmp-server enable trap

[Parameter]

trap_type : Type of trap

Setting value	Description
coldstart	When the power is turned on/off, or when firmware is updated
warmstart	When reload command is executed
linkdown	At linkdown
linkup	At linkup
authentication	When authentication fails
l2ms	When L2MS agent is detected or lost
errdisable	When ErrorDisable is detected or canceled
rmon	When RMON event is executed
termmonitor	When terminal monitoring is detected
bridge	When spanning tree root is detected / When topology is changed
loopdetect	During loop detection/clearing
all	All trap types. All of the above trap types are specified in the config.

[Initial value]

no snmp-server enable trap

[Input mode]

global configuration mode

[Description]

Specifies the type of trap notification that is sent.

If this command is executed with the "no" syntax, traps are disabled.

[Example]

Enable coldstart trap.

```
SWP2(config)#snmp-server enable trap coldstart
```

Disable traps.

```
SWP2(config)#no snmp-server enable trap
```

4.12.4 Set system contact

[Syntax]

snmp-server contact *contact*
no snmp-server contact

[Parameter]

contact : Name (maximum 255 characters) to register as the system contact

[Initial value]

no snmp-server contact

[Input mode]

global configuration mode

[Description]

Sets the MIB variable sysContact.

sysContact is a variable that is typically used to enter the name of the administrator or contact.

If this command is executed with the "no" syntax, the setting is deleted.

[Example]

Set the system contact to "swx_admin@sample.com".

```
SWP2(config)#snmp-server contact swx_admin@sample.com
```

4.12.5 Set system location

[Syntax]

snmp-server location *location*
no snmp-server location

[Parameter]

location : Name to register as the system location (255 characters or less)

[Initial value]

no snmp-server location

[Input mode]

global configuration mode

[Description]

Sets the MIB variable sysLocation.

sysLocation is a variable that is generally used to enter the installed location of the unit.

If this command is executed with the "no" syntax, the setting is deleted.

[Example]

Set the system location as "MainOffice-1F".

```
SWP2(config)#snmp-server location MainOffice-1F
```

4.12.6 Set SNMP community

[Syntax]

snmp-server community *community ro_rw*
no snmp-server community *community*

[Parameter]

community : Community name (maximum 32 characters)

When both ends are enclosed in "" or ", the "" and " at both ends are not included in the number of characters

ro_rw : Access restriction

Setting value	Description
ro	Read only
rw	Write allowed

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the SNMP community.

Up to 16 communities can be registered.

If this is executed with the "no" syntax, the specified community is deleted.

[Example]

Set the read-only community name to "public".

```
SWP2(config)#snmp-server community public ro
```

Delete the "public" community.

```
SWP2(config)#no snmp-server community public
```

4.12.7 Set SNMP view

[Syntax]

snmp-server view *view oid type*
no snmp-server view *view*

[Parameter]

view : View name (maximum 32 characters)

oid : MIB object ID

type : Type

Setting value	Description
include	Include the specified object ID in management
exclude	Exclude the specified object ID from management

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the SNMP MIB view.

The MIB view is the set of MIB objects to specify when allowing access rights.

Up to 16 MIB views can be registered.

The combination of the *oid* parameter and the *type* parameter indicates whether the MIB sub-tree following the specified object ID is or is not subject to management. Taking the *oid* parameter and the *type* parameter together as one entry, you can specify multiple entries for each MIB view, up to a maximum of 8.

When multiple entries are specified, the *type* parameter for the specified object ID takes priority for entries that are contained at a lower level within the specified object ID.

If this command is executed with the "no" syntax, the MIB view is deleted. It is not possible to delete individual entries.

[Example]

Specify the "most" view which shows the internet node (1.3.6.1) and below.

```
SWP2(config)#snmp-server view most 1.3.6.1 include
```

Specify the "standard" view which shows the mib-2 node (1.3.6.1.2.1) and below.

```
SWP2(config)#snmp-server view standard 1.3.6.1.2.1 include
```

4.12.8 Set SNMP group

[Syntax]

snmp-server group *group seclevel* read *read_view* [write *write_view*]
snmp-server group *group seclevel* write *write_view* [read *read_view*]
no snmp-server group *group*

[Keyword]

read : Specify the MIB view that can be read by users belonging to this group

write : Specify the MIB view that can be written by users belonging to this group

[Parameter]

group : Group name (maximum 32 characters)

seclevel : Security level required of users belonging to this group

Setting value	Description
noauth	No authentication / No encryption (noAuthNoPriv)
auth	Authentication / No encryption (authNoPriv)
priv	Authentication / Encryption (authPriv)

read_view : Name of the MIB view (maximum 32 characters) that can be read by users belonging to this group

write_view : Name of the MIB view (maximum 32 characters) that can be written by users belonging to this group

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the user group.

Access to MIB objects not included in the MIB view specified by this command is prohibited.

The MIB view is defined by the **snmp-server view** command.

The maximum number of entries is 16.

If this command is executed with the "no" syntax, the specified group setting is deleted.

[Example]

Create the user group "admins," and grant users belonging to the "admins" group full access rights to the "most" view.

```
SWP2(config)#snmp-server group admins priv read most write most
```

Create the user group "users," and grant users belonging to the "users" group read access rights to the "standard" view.

```
SWP2(config)#snmp-server group users auth read standard
```

4.12.9 Set SNMP user

[Syntax]

snmp-server user *user group* [auth *auth auth_pass* [priv *priv priv_pass*]]
no snmp-server user *user*

[Keyword]

auth : Set the authentication algorithm

priv : Set the encryption algorithm

[Parameter]

user : User name (maximum 32 characters)

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

group : Group name (maximum 32 characters)

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

auth : Authentication algorithm

Setting value	Description
md5	HMAC-MD5-96
sha	HMAC-SHA-96

auth_pass : Authentication password (8 or more characters, maximum 32 characters)

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

priv : Encryption algorithm

Setting value	Description
des	DES-CBC
aes	AES128-CFB

priv_pass : Encryption password (8 or more characters, maximum 32 characters)

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Specifies a user.

The group name of this command specifies the name defined by the snmp-server group command; according to the security level specified by the group setting, it specifies the algorithm and password that are used to authenticate and encrypt the content of communication.

It is not possible to only encrypt without authentication.

The maximum number of entries is 16.

The setting as to whether authentication and encryption are used, the algorithm, and the password, must match the user setting of the SNMP manager that is the other party.

If this command is executed with the "no" syntax, the setting of the specified user is deleted.

[Example]

Create "admin1" as a user. According to the specified group and the security level prescribed for that group, specify the protocol (SHA, AES) and password (passwd1234) used for authentication and encryption.

```
SWP2(config)#snmp-server user admin1 admins auth sha passwd1234 priv aes passwd1234
```

Create "user1" as a user. According to the specified group and the security level prescribed for that group, specify the protocol (SHA) and password (passwd5678) used for authentication and encryption.

```
SWP2(config)#snmp-server user user1 users auth sha passwd5678
```

4.12.10 IP address restrictions for clients that can access the SNMP server

[Syntax]

snmp-server access *action info* [community *community*]
no snmp-server access [*action info* [community *community*]]

[Keyword]

community : Specify a community

[Parameter]

action : Specify behavior for access conditions

Setting value	Description
permit	"Permit" the condition

info : Sets the sending source IPv4/IPv6 address information used as a condition

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with a subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with a subnet mask length (Mbit)
any	Specifies all IPv4/IPv6 addresses

community : Community name (up to 32 characters)

Community to which the access conditions apply

If the community specification is omitted, the access conditions will apply to all communities

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters.

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Restrict client terminals that are permitted to access the SNMP server by IPv4/IPv6 address.

Up to 32 items can be set with this command, and those applied first are given priority.

When this command is set, all access that does not meet the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is cleared.

If community is omitted in the “no” syntax, all settings for the specified info are cleared.

If all parameters are omitted in the “no” syntax, all settings are cleared.

[Note]

The access restrictions of this command apply only to SNMPv1 and SNMPv2c access.

It does not apply to SNMPv3 access.

[Example]

Permit SNMP server access only from the 192.168.100.0/24 segment.

```
SWP2(config)#snmp-server access permit 192.168.100.0/24
```

Restrict access to only 192.168.100.0/24 hosts with the ‘public’ community name and to only 192.168.100.12 hosts with the 'private’ community name.

```
SWP2(config)#snmp-server access permit 192.168.100.0/24 community public
SWP2(config)#snmp-server access permit 192.168.100.12 community private
```

4.12.11 Show SNMP community information

[Syntax]

show snmp community

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows SNMP community information.

Shows the community name, and access mode.

[Example]

Show SNMP community information.

```
SWP2#show snmp community
SNMP Community information
  Community Name: public
  Access: Read-Only


  Community Name: private
  Access: Read-Write
```

4.12.12 Show SNMP view settings

[Syntax]

show snmp view

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the contents of the SNMP view settings.

Shows the view name, object ID, and type.

[Example]

Show the contents of the SNMP view settings.

```
SWP2#show snmp view
SNMP View information
  View Name: most
  OID: 1.6.1
  Type: include

  View Name: standard
  OID: 1.3.6.1.2.1
  Type: include
```

4.12.13 Show SNMP group settings

[Syntax]

show snmp group

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the contents of the SNMP group settings.

Shows the group name, security level, reading view, and writing view.

[Example]

Show the contents of the SNMP group settings.

```
SWP2#show snmp group
SNMP Group information
  Group Name: admins
  Security Level: priv
  Read View: most
  Write View: most

  Group Name: users
  Security Level: auth
  Read View: standard
  Write View: standard
```

4.12.14 Show SNMP user settings

[Syntax]

show snmp user

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the contents of the SNMP user settings.

Shows the engine ID, user name, affiliated group name, authentication method, and encryption method.

[Example]

Show the contents of the SNMP user settings.

```
SWP2#show snmp user
SNMP User information
  EngineID: 0x8000049e0300a0deaeb90e

  User Name: admin1
  Group Name: admins
  Auth: sha
  Priv: aes

  User Name: user1
  Group Name: users
  Auth: sha
  Priv: none
```

4.13 RMON

4.13.1 Set RMON function

[Syntax]

rmon *switch*

no rmon

[Parameter]

switch : RMON function operation

Setting value	Description
enable	Enable RMON function
disable	Disable RMON function

[Initial value]

rmon enable

[Input mode]

global configuration mode

[Description]

Sets the system-wide operation of the RMON function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If this command is used to disable the system-wide RMON function, the following RMON group operations are disabled.

- Ethernet statistical information group
- History group
- Alarm group
- Event group

This command can be set using the private MIB ysrmonSetting (1.3.6.1.4.1.1182.3.7.1).

[Example]

Enable RMON function.

```
SWP2(config)#rmon enable
```

Disable RMON function.

```
SWP2(config)#rmon disable
```

4.13.2 Set RMON Ethernet statistical information group

[Syntax]

rmon statistics *index* [owner *owner*]
no rmon statistics *index*

[Parameter]

index	:	<1 - 65535>
		Index of the Ethernet statistical information group (etherStatsIndex)
owner	:	Name of the Ethernet statistical information group owner (etherStatsOwner)
		Maximum 127 characters
		(if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the RMON Ethernet statistical information group setting for the applicable interface.

If this command is set, statistical information is collected, and the RMON MIB's etherStatsTable can be acquired.

This command can be specified a maximum number of eight times for the same interface.

If this command is executed with the "no" syntax, selete the setting and the collected statistical information.

[Note]

To enable the Ethernet statistical information group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

If this command is overwritten, the previously collected statistical information is deleted, and collection is once again started.

If the system-wide RMON function is disabled, collection of statistical information is interrupted. Subsequently, if the system-wide RMON function is enabled, the previously collected statistical data is deleted, and collection is once again started.

[Example]

Enable the RMON Ethernet statistical information group settings for port1.1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#rmon statistics 1
```

4.13.3 Set RMON history group

[Syntax]

rmon history *index* [buckets *buckets*] [interval *interval*] [owner *owner*]
no rmon history *index*

[Parameter]

index	:	<1 - 65535>
		Index of history group (historyControlIndex)
buckets	:	<1 - 65535>
		Number of history group items to maintain (historyControlBucketsRequested)
		(if omitted : 50)

interval : <1 - 3600>

Interval at which to save history group items (seconds) (historyControlInterval)

(if omitted : 1800)

owner : Name of history group owner (historyControlOwner)

Maximum 127 characters

(if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables RMON history group settings for the applicable interface.

If this command is set, it will be possible to acquire the RMON MIB's historyControlTable. After setting this command, history information is collected at the specified interval, and the RMON MIB's etherHistoryTable can be acquired.

This command can be specified a maximum number of eight times for the same interface.

If this command is executed with the "no" syntax, delete the setting and the collected historical information.

[Note]

To enable the history group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

If this command is overwritten, the previously collected historical information is deleted, and collection is once again started.

If the system-wide RMON function is disabled, collection of historical information is interrupted. Subsequently, if the system-wide RMON function is enabled, the previously collected historical data is deleted, and collection is once again started.

[Example]

Enable the RMON historical group settings for port1.1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#rmon history 1
```

4.13.4 Set RMON event group

[Syntax]

rmon event *index type community* [description *description*] [owner *owner*]
no rmon event *index*

[Parameter]

index : <1 - 65535>

Index of event group (eventIndex)

type : Event type (eventType)

Setting value	Description
log	Record in log
trap	Send SNMP trap
log-trap	Record in log and send SNMP trap

community : Community name (eventCommunity)

Maximum 127 characters

This can be specified if *type* is "trap" or "log-trap".

description : Description of event (eventDescription)

Maximum 127 characters

(if omitted : RMON_SNMP)

owner : Name of event group owner (eventOwner)

Maximum 127 characters

(if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enables the RMON event group settings.

If this command is set, it will be possible to acquire the RMON MIB's eventTable. Use the **rmon alarm** command to set the event group for this command.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

To enable the event group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

In order for RMON to send an SNMP trap, you must have made SNMP trap transmission settings.

[Example]

After making SNMP trap settings, enable the RMON event group setting. Set the type of event as "log-trap", and the community name of the trap as "public".

```
SWP2(config)#snmp-server host 192.168.100.3 traps version 2c public
SWP2(config)#snmp-server enable trap rmon
SWP2(config)#rmon event 1 log-trap public
```

4.13.5 Set RMON alarm group

[Syntax]

rmon alarm *index variable* interval *interval* [*type*] rising-threshold *rising_threshold* event *rising_event-index* falling-threshold *falling_threshold* event *falling_event_index* [alarmstartup *startup*] [owner *owner*]

rmon alarm *index variable* interval *interval* [*type*] rising-threshold *rising_threshold* event *rising_event-index* [owner *owner*]

rmon alarm *index variable* interval *interval* [*type*] falling-threshold *falling_threshold* event *falling_event_index* [owner *owner*]

no rmon alarm *index*

[Parameter]

index : <1-65535>

Index of alarm group (alarmIndex)

variable : MIB object to be monitored (alarmVariable)

interval : <1-2147483647>

Sampling interval (seconds)(alarmInterval)

type : Sampling type (alarmSampleType)

Setting value	Description
absolute	Compare by absolute value. Directly compare sample value and threshold value
delta	Compare by relative value. Compare the difference between the latest sample value and the previous sample value

(if omitted : absolute)

rising_threshold : <1-2147483647>

Upper threshold value (alarmRisingThreshold)

rising_event_index : <1-65535>

Event index (alarmRisingEventIndex)

falling_threshold : <1-2147483647>

Lower threshold value (alarmFallingThreshold)

falling_event_index : <1-65535>

Event index (alarmFallingEventIndex)

startup : <1-3>

Threshold value used for first alarm decision (alarmStartupAlarm)

Setting value	Description
1	Use only upper threshold value (risingAlarm)
2	Use only lower threshold value (fallingAlarm)
3	Use both upper threshold value and lower threshold value (risingOrFallingAlarm)

(if omitted : 3)

owner : Name of alarm group owner (alarmOwner)

maximum 127 characters

(if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enables the RMON alarm group settings.

Set *variable* as the MIB object that will be the target of monitoring by the RMON alarm group. Of the etherStatsEntry(.1.3.6.1.2.1.16.1.1.1) MIB objects, *variable* can be specified only as a MIB object that has a counter type. This can be specified in the following three formats.

- etherStatsEntry.X.Y
- (OID name under etherStatsEntry).Y
- .1.3.6.1.2.1.16.1.1.1.X.Y

For example, if specifying etherStatsPkts.1(.1.3.6.1.2.1.16.1.1.1.5.1), it can be specified in any of the following formats.

Format	Description
etherStatsEntry.X.Y	etherStatsEntry.5.1
(OID name under etherStatsEntry).Y	etherStatsPkts.1
.1.3.6.1.2.1.16.1.1.1.X.Y	.1.3.6.1.2.1.16.1.1.1.5.1

You can use a format that specifies either *rising_threshold* or *falling_threshold*, not both. In this case, the following values are used for parameters whose setting is omitted.

- Use only *rising_threshold*
  - *falling_threshold* : Same value as *rising_threshold*
  - *falling_event_index* : Same value as *rising_event_index*
  - *startup* : 1 (Use only upper_threshold)
- Use only *falling_threshold*
  - *rising_threshold* : Same value as *falling_threshold*
  - *rising_event_index* : Same value as *falling_event_index*
  - *startup* : 2 (Use only lower_threshold)

If this command is set, it will be possible to acquire the RMON MIB's alarmTable.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

To enable the alarm group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

The MIB object specified in *variable* is a MIB object of the Ethernet statistical information group. If an Ethernet statistical information group possessing the applicable index has not been created, this command returns an error.

The Ethernet statistical information group can be created by the **rmon statistics** command. If the Ethernet statistical information group being used by this command is deleted, this command is also deleted.

The event index specifies the index that is set by the **rmon event** command. If the event group being used by this command is deleted, this command is also deleted.

The *rising_threshold* value must be a higher value than the *falling_threshold* value.

If this command is overwritten, the previous sampling data is deleted, and sampling is once again started.

If the system-wide RMON function is disabled, sampling is interrupted. Subsequently, if the system-wide RMON function is enabled, the previous sampling data is deleted, and sampling is once again started.

[Example]

Enable the RMON alarm group settings with the following conditions.

- The MIB object to be monitored is etherStatsPkts.1.
- The sampling interval is 180 seconds.
- The sampling type is delta.
- The upper threshold value is 3000, and the event when rising above the upper threshold value is 1.
- The lower threshold value is 2000, and the event when falling below the lower threshold value is 1.

```
SWP2(config)#rmon alarm 1 etherStatsPkts.1 interval 180 delta rising-threshold 3000
event 1 falling-threshold 2000 event 1
```

4.13.6 Show RMON function status

[Syntax]

show rmon

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the settings and status of the RMON function.

The following items are shown.

- System-wide RMON function settings
- RMON function settings for each group
  - Ethernet statistical information group
  - History group
  - Alarm group
  - Event group

[Example]

```
SWP2>show rmon
rmon: Enable

statistics:
    rmon collection index 1
    stats->ifindex = 5001
    input packets 7, bytes 600, drop events 0, multicast packets 4
    output packets 17, bytes 2091, multicast packets 17 broadcast packets 0

history:
    history index = 1
    data source ifindex = 5001
    buckets requested = 50
    buckets granted = 50
    Interval = 1800
```

```
    Owner RMON_SNMP

event:
    event Index = 1
       Description RMON_SNMP
       Event type Log
       Event community name RMON_SNMP
       Last Time Sent = 00:00:58
       Owner  RMON_SNMP

alarm:
    alarm Index = 1
      alarm status = VALID
        alarm Interval = 15
        alarm Type is Absolute
        alarm Value  = 0
        alarm Rising Threshold = 10
        alarm Rising Event = 1
        alarm Falling Threshold = 7
        alarm Falling Event = 1
        alarm Startup Alarm = 3
        alarm Owner is RMON_SNMP
```

4.13.7 Show RMON Ethernet statistical information group status

[Syntax]

show rmon statistics

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the settings and status of the RMON Ethernet statistical information group.

The following items are shown.

- Index
- Applicable interface
- Input packets
- Output packets

[Example]

```
SWP2>show rmon statistics
    rmon collection index 1
    stats->ifindex = 5001
    input packets 7, bytes 600, drop events 0, multicast packets 4
    output packets 17, bytes 2091, multicast packets 17 broadcast packets 0
```

4.13.8 Show RMON history group status

[Syntax]

show rmon history

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the settings and status of the RMON history group.

The following items are shown.

- Index
- Applicable interface
- Number of history group items to maintain
- Interval at which to save history group items
- Owner name

[Example]

```
SWP2>show rmon history
```

```
        history index = 1
        data source ifindex = 5001
        buckets requested = 50
        buckets granted = 50
        Interval = 1800
        Owner RMON_SNMP
```

4.13.9 Show RMON event group status

[Syntax]

show rmon event

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the settings and status of the RMON event group.

The following items are shown.

- Index
- Description of event
- Type of event
- Community name when sending trap
- Time of executing event
- Owner name

[Example]

```
SWP2>show rmon event
    event Index = 1
       Description RMON_SNMP
       Event type Log
       Event community name RMON_SNMP
       Last Time Sent = 00:00:58
       Owner  RMON_SNMP
```

4.13.10 Show RMON alarm group status

[Syntax]

show rmon alarm

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the settings and status of the RMON alarm group.

The following items are shown.

- Index
- Alarm status
- MIB object to be monitored
- Sampling interval
- Sampling type
- Measured value
- Upper threshold value
- Event for upper threshold value
- Lower threshold value
- Event for lower threshold value
- Startup alarm
- Owner name

[Example]

```
SWP2>show rmon alarm
      alarm Index = 1
        alarm status = VALID
          alarm Interval = 15
```

```
          alarm Type is Absolute
          alarm Value  = 0
          alarm Rising Threshold = 10
          alarm Rising Event = 1
          alarm Falling Threshold = 7
          alarm Falling Event = 1
          alarm Startup Alarm = 3
          alarm Owner is RMON_SNMP
```

4.13.11 Clear counters of the RMON Ethernet statistical information group

[Syntax]

rmon clear counters

[Input mode]

interface mode

[Description]

Clears the counters of the RMON Ethernet statistical information group for the applicable interface.

[Example]

Clear the counters of the RMON Ethernet statistical information group for port1.1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#rmon clear counters
```

4.14 sFlow

4.14.1 Set sFlow function

[Syntax]

sflow *switch*
no sflow

[Parameter]

switch : sFlow function operation

Setting value	Description
enable	Enable sFlow function
disable	Disable sFlow function

[Initial value]

sflow disable

[Input mode]

global configuration mode

[Description]

This sets the sFlow function operation.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Enable the sFlow function.

```
SWP2(config)#sflow enable
```

4.14.2 Set sFlow agent

[Syntax]

sflow agent *address*
no sflow agent

[Parameter]

address	:	A.B.C.D
		IPv4 address
	:	X:X::X:X
		IPv6 address

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the IP address for the sFlow agent.

The IP address set with this command is used in the sFlow header of the sFlow datagram.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

An IPv6 address cannot specified if the stack function is enabled.

[Example]

Sets the IP address for the sFlow agent to "192.168.100.240".

```
SWP2(config)#sflow agent 192.168.100.240
```

4.14.3 Set sFlow collector

[Syntax]

sflow collector *address* [*port*]
no sflow collector

[Parameter]

address	:	A.B.C.D
		IPv4 address
	:	X:X::X:X
		IPv6 address
port	:	<1 - 65535>
		Destination UDP port number for sFlow collector
		Default value is 6343

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the IP address and destination UDP port number for the sFlow collector.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

An IPv6 address cannot specified if the stack function is enabled.

[Example]

Sets the IP address for the sFlow collector to "192.168.100.240".

```
SWP2(config)#sflow collector 192.168.100.240
```

4.14.4 Set maximum size of sFlow datagram

[Syntax]

sflow collector max-datagram-size *size*
no sflow collector max-datagram-size

[Parameter]

size : <512 - 1452> (bytes)

[Initial value]

sflow collector max-datagram-size 1400

[Input mode]

global configuration mode

[Description]

This sets the maximum size of datagrams transmitted from the sFlow agent to the sFlow collector.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set maximum size to 1000 bytes for sFlow datagrams.

```
SWP2(config)#sflow collector max-datagram-size 1000
```

4.14.5 Set sampling rate of packet flow sampling

[Syntax]

sflow sampling-rate *rate*
no sflow sampling-rate

[Parameter]

rate : <256 - 1000000000>

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the sampling rate used for packet flow on the applicable port when executing packet flow sampling.

If this command is not set, packet flow sampling is not implemented.

This command can be specified only for LAN/SFP+ port.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Sets the sampling rate of packet flow sampling to 10000.

```
SWP2(config-if)#sflow sampling-rate 10000
```

4.14.6 Set maximum Ethernet frame header size for packet flow sampling

[Syntax]

sflow max-header-size *size*
no sflow max-header-size

[Parameter]

size : <14 - 256> (bytes)

[Initial value]

sflow max-header-size 128

[Input mode]

interface mode

[Description]

Sets the maximum Ethernet frame header size used for packet flow sampling on the applicable port.

If this command is executed with the "no" syntax, the setting returns to the default.

This command can be specified only for LAN/SFP+ port.

[Example]

This sets the maximum Ethernet frame header size for packet flow sampling to 100.

```
SWP2(config-if)#sflow max-header-size 100
```

4.14.7 Set polling interval for counter sampling

[Syntax]

sflow polling-interval *interval*
no sflow polling-interval

[Parameter]

interval : <1 - 86400> (seconds)

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the polling interval used when executing counter sampling on the applicable port.

If this command is not set, counter sampling is not implemented.

This command can be specified only for LAN/SFP+ port.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Sets the counter sampling interval to 100 seconds.

```
SWP2(config-if)#sflow polling-interval 100
```

4.14.8 Show sFlow status

[Syntax]

show sflow

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the status of sFlow.

[Example]

This shows the status of sFlow.

```
SWP2#show sflow
sFlow Global Configuration:
  sFlow Feature      : Enabled
  Agent Address      : 192.168.100.240
  Collector Address  : 192.168.100.2
  Collector UDP Port : 6343
  Max Datagram Size  : 1400(bytes)
```

```
sFlow Port Configuration:

           Sampling-Rate    Polling-Interval
  Port     (1 in N pkts)    (secs)
  ---------------------------------------------------------
  port1.1   300             30
  port1.5   500             (NOT SET)

sFlow Drop Sampling Count : 0
```

4.14.9 Show sFlow sampling information

[Syntax]

show sflow sampling [*ifname*]

[Parameter]

ifname : LAN/SFP+ port interface name
Interface to show

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows sFlow sampling information for the interface specified by *ifname*.

If *ifname* is omitted, information is shown for all interfaces.

[Note]

This command cannot be executed on non-main member switches when the stack function is enabled.

When the stack function is enabled, this information is not synchronized between main and members.

[Example]

Shows the sFlow sampling information.

```
SWP2#show sflow sampling
sFlow sampling information:

  Interface port1.1:
    Packet-Flow-Samping:
      Samping count : 40
      Number of packets remaining until next sampling:
        Ingress : 208
        Egress  : 590
    Counter-Samping:
      Samping count : 65
      Number of seconds remaining until next sampling : 15

  Interface port1.5:
    Packet-Flow-Samping:
      Samping count : 15
      Number of packets remaining until next sampling:
        Ingress : 876
        Egress  : 870
    Counter-Samping:
      (NOT SET)
```

4.15 Telnet server

4.15.1 Start Telnet server and change listening port number

[Syntax]

telnet-server enable [*port*]
telnet-server disable
no telnet-server

[Keyword]

enable	:	Telnet server is enabled
disable	:	Telnet server is disable

[Parameter]

port	:	<1-65535> Listening port of the Telnet server (if omitted: 23)

[Initial value]

telnet-server disable

[Input mode]

global configuration mode

[Description]

Enables the Telnet server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the function is disabled.

[Example]

Start the Telnet server with 12345 as the listening port number.

```
SWP2(config)#telnet-server enable 12345
```

4.15.2 Show Telnet server settings

[Syntax]

show telnet-server

[Input mode]

priviledged EXEC mode

[Description]

Shows the settings of the Telnet server. The following items are shown.

- Telnet server function enabled/disabled status
- Listening port number
- VLAN interface that is permitted to access the TELNET server
- Filter that controls access to the TELNET server

[Example]

Show the settings of the Telnet server.

```
SWP2#show telnet-server
Service:Enable
Port:23
Management interface(vlan): 1
Interface(vlan):1, 2, 3
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

4.15.3 Set host that can access the Telnet server

[Syntax]

telnet-server interface *interface*
no telnet-server interface *interface*

[Parameter]

interface	:	VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the Telnet server.

If this command is executed with the "no" syntax, the specified interface is deleted.

This command can be used to specify up to eight items, which are applied in the order that they are specified.

If this command is not set, access is permitted only from the management VLAN.

[Note]

If **telnet-server enable** is not specified, this command does not function.

[Example]

Allow access to the Telnet server from the hosts connected to VLAN #1 and VLAN #2.

```
SWP2(config)#telnet-server interface vlan1
SWP2(config)#telnet-server interface vlan2
```

4.15.4 Restrict access to the TELNET server according to the IP address of the client

[Syntax]

telnet-server access *action info*
no telnet-server access [*action info*]

[Parameter]

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

info : Specifies the transmission-source IPv4 address or IPv6 address that is the condition.

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv4 addresses and IPv6 addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Restrict access to the TELNET server according to the client terminal's IPv4/IPv6 address.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is set, all access that does not satisfy the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is deleted.

If this command is executed with the "no" syntax, and parameter is omitted, all settings are deleted.

[Note]

If **telnet-server enable** is not specified, this command does not function.

[Example]

Permit access to the TELNET server only from 192.168.1.1 and the 192.168.10.0/24 segment.

```
SWP2(config)#telnet-server access permit 192.168.1.1
SWP2(config)#telnet-server access permit 192.168.10.0/24
```

Deny only access to the TELNET server from the segment 192.168.10.0/24.

```
SWP2(config)#telnet-server access deny 192.168.10.0/24
SWP2(config)#telnet-server access permit any
```

4.16 Telnet client

4.16.1 Start Telnet client

[Syntax]

telnet *host* [*port*]

[Parameter]

host : Remote host name, IPv4 address (A.B.C.D), or IPv6 address(X:X::X:X)

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

port : <1-65535>

Port number to use (if omitted: 23)

[Initial value]

none

[Input mode]

priviledged EXEC mode

[Description]

Connects to the specified host via Telnet.

[Example]

Connect via Telnet to port number 12345 of the host at IPv4 address 192.168.100.1.

```
SWP2#telnet 192.168.100.1 12345
```

Connect via Telnet to port number 12345 of the host at IPv6 address fe80::2a0:deff:fe11:2233.

```
SWP2#telnet fe80::2a0:deff:fe11:2233%vlan1 12345
```

4.16.2 Enable Telnet client

[Syntax]

telnet-client *switch*
no telnet-client

[Parameter]

switch : Whether to enable TELNET client

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

telnet-client disable

[Input mode]

global configuration mode

[Description]

Enables use of the telnet command as a Telnet client.

If this command is executed with the "no" syntax, the Telnet client is disabled.

[Example]

Enable the Telnet client.

```
SWP2(config)#telnet-client enable
```

4.17 TFTP server

4.17.1 Start TFTP server and change listening port number

[Syntax]

tftp-server enable [*port*]
tftp-server disable
no tftp-server

[Keyword]

enable	:	TFTP server is enabled
disable	:	TFTP server is disable

[Parameter]

port	:	<1-65535> Listening port number of the TFTP server (if omitted: 69)

[Initial value]

tftp-server disable

[Input mode]

global configuration mode

[Description]

Enables the TFTP server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the TFTP server is disabled.

[Example]

Start the TFTP server with 12345 as the listening port number.

```
SWP2(config)#tftp-server enable 12345
```

4.17.2 Show TFTP server settings

[Syntax]

show tftp-server

[Input mode]

priviledged EXEC mode

[Description]

Shows the settings of the TFTP server. The following items are shown.

- TFTP server function enabled/disabled status
- Listening port number
- VLAN interface that is permitted to access the TFTP server

[Example]

Show the settings of the TFTP server.

```
SWP2#show tftp-server
Service:Enable
Port:69
Management interface(vlan): 1
Interface(vlan):1, 2, 3
```

4.17.3 Set hosts that can access the TFTP server

[Syntax]

tftp-server interface *interface*
no tftp-server interface *interface*

[Parameter]

interface	:	VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the TFTP server.

If this command is executed with the "no" syntax, the specified interface is deleted

This command can be used to specify up to eight items, which are applied in the order that they are specified.

If this command is not set, access is permitted only from the management VLAN.

[Example]

Allow access to the TFTP server from the hosts connected to VLAN #1 and VLAN #2.

```
SWP2(config)#tftp-server interface vlan1
SWP2(config)#tftp-server interface vlan2
```

4.18 HTTP server

4.18.1 Start HTTP server and change listening port number

[Syntax]

http-server enable [*port*]
http-server disable
no http-server

[Keyword]

enable	:	HTTP server is enabled
disable	:	HTTP server is disabled

[Parameter]

port	:	<1-65535> Listening port number of the HTTP server (if omitted: 80)

[Initial value]

http-server disable

[Input mode]

global configuration mode

[Description]

Enables the HTTP server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the function is disabled.

[Example]

Start the HTTP server with 8080 as the listening port number.

```
SWP2(config)#http-server enable 8080
```

4.18.2 Start secure HTTP server and change listening port number

[Syntax]

http-server secure enable [*port*]
http-server secure disable
no http-server secure

[Keyword]

enable	:	Enable the secure HTTP server
disable	:	Disable the secure HTTP server

[Parameter]

port	:	<1-65535> Listening port number of the secure HTTP server (if omitted: 443)

[Initial value]

http-server secure disable

[Input mode]

global configuration mode

[Description]

Enables the secure HTTP server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the function is disabled.

If the secure HTTP server is enabled, encryption is performed in software, meaning that depending on the amount of traffic, the CPU usage rate will rise.

To avoid a high usage rate, it is desirable to avoid access by multiple users to an automatically updated web page such as the dashboard or the LAN map.

[Example]

Start the secure HTTP server with 8080 as the listening port number.

```
SWP2(config)#http-server secure enable 8080
```

4.18.3 Show HTTP server settings

[Syntax]

show http-server

[Input mode]

priviledged EXEC mode

[Description]

Shows the settings of the HTTP server. The following items are shown.

- HTTP server function enabled/disabled status
- HTTP server's listening port number
- VLAN interface that is permitted to access the HTTP server
- Filter that controls access to the HTTP server
- Secure HTTP server function enabled/disabled status
- Log-in timeout time

[Example]

Show the settings of the HTTP server.

```
SWP2#show http-server
HTTP :Enable(80)
HTTPS:Disable
Management interface(vlan): 1
Interface(vlan):1
Access:None
Login timeout:30 min 51 sec
```

4.18.4 Set hosts that can access the HTTP server

[Syntax]

http-server interface *interface*
no http-server interface *interface*

[Parameter]

interface : VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the HTTP server.

If this command is executed with the "no" syntax, the specified interface is deleted.

This command can be used to specify up to eight items, which are applied in the order that they are specified.

If this command is not set, access is permitted only from the management VLAN.

[Example]

Allow access to the HTTP server from the hosts connected to VLAN #1 and VLAN #2.

```
SWP2(config)#http-server interface vlan1
SWP2(config)#http-server interface vlan2
```

4.18.5 Restrict access to the HTTP server according to the IP address of the client

[Syntax]

http-server access *action info*
no http-server access [*action info*]

[Parameter]

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

info : Specifies the transmission-source IPv4 address or IPv6 address that is the condition.

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv4 addresses and IPv6 addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Restrict access to the HTTP server according to the client terminal's IPv4/IPv6 address.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is set, all access that does not satisfy the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is deleted.

If this command is executed with the "no" syntax, and parameter is omitted, all settings are deleted.

[Note]

If **http-server enable** or **http-server secure enable** are not specified, this command does not function.

[Example]

Permit access to the HTTP server only from 192.168.1.1 and the 192.168.10.0/24 segment.

```
SWP2(config)#http-server access permit 192.168.1.1
SWP2(config)#http-server access permit 192.168.10.0/24
```

Deny access to the HTTP server only from 192.168.10.0/24 segment.

```
SWP2(config)#http-server access deny 192.168.10.0/24
SWP2(config)#http-server access permit any
```

4.18.6 Web GUI display language

[Syntax]

http-server language *lang*
no http-server language

[Parameter]

lang : Specify the language

Setting value	Description
japanese	Japanese
english	English

[Initial value]

http-server language japanese

[Input mode]

global configuration mode

[Description]

Sets the Web GUI display language.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the Web GUI display language to English.

```
SWP2(config)#http-server language english
```

4.18.7 Set log-in timeout time for HTTP server

[Syntax]

http-server login-timeout *min* [*sec*]
no http-server login-timeout

[Parameter]

min : <0-35791>

Timeout time (minutes)

sec : <0-2147483>

Timeout time (seconds)

[Initial value]

http-server login-timeout 5

[Input mode]

global configuration mode

[Description]

Specify the time until automatic logout when there has been no access to the HTTP server.

If sec is omitted, 0 is specified.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The smallest value that can be specified is one minute.

[Example]

Set the timeout time for the HTTP server to 2 minutes 30 seconds.

```
SWP2(config)#http-server login-timeout 2 30
```

4.19 SSH server

4.19.1 Start SSH server and change listening port number

[Syntax]

ssh-server enable [*port*]
ssh-server disable
no ssh-server

[Keyword]

enable	:	SSH server is enabled
disable	:	SSH server is disable

[Parameter]

port	:	<1-65535> Listening port of the SSH server (if omitted: 22)

[Initial value]

ssh-server disable

[Input mode]

global configuration mode

[Description]

Enables the SSH server. You can also specify the listening TCP port number.

In order to enable the SSH server, the host key must be created in advance (ssh-server host key generate).

If this command is executed with the "no" syntax, disable the SSH server.

[Note]

In order to log in from the SSH client, the user name and password must be registered in advance (username).

[Example]

Start the SSH server with 12345 as the listening port number.

```
SWP2#ssh-server host key generate
SWP2#configure terminal
SWP2(config)#ssh-server enable 12345
```

4.19.2 Show SSH server settings

[Syntax]

show ssh-server

[Input mode]

priviledged EXEC mode

[Description]

Shows the settings of the SSH server.

The following items are shown.

- SSH server function enabled/disabled status
- Listening port number
- Whether SSH server host key exists
- VLAN interface permitted to access the SSH server
- Filter that controls access to the SSH server

[Example]

Show the settings of the SSH server.

```
SWP2#show ssh-server
Service:Enable
Port:23
Hostkey:Generated
Management interface(vlan): 1
Interface(vlan):1, 2, 3
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

4.19.3 Set host that can access the SSH server

[Syntax]

ssh-server interface *ifname*
no ssh-server interface *ifname*

[Parameter]

ifname : VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the SSH server.

If this command is executed with the "no" syntax, delete the specified interface.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is not set, access is permitted only from the maintenance VLAN.

[Example]

Allow access to the SSH server from the hosts connected to VLAN #1 and VLAN #2.

```
SWP2(config)#ssh-server interface vlan1
SWP2(config)#ssh-server interface vlan2
```

4.19.4 Set client that can access the SSH server

[Syntax]

ssh-server access *action info*
no ssh-server access [*action info*]

[Parameter]

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

info : Specifies the transmission-source IPv4 address or IPv6 address that is the condition

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv4 addresses and IPv6 address

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Restrict access to the SSH according to the client terminal's IPv4/IPv6 address.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is set, all access that does not satisfy the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is deleted.

If parameters are omitted with the "no" syntax, the all setting are deleted.

[Note]

If **ssh-server enable** command is not specified, this command does not function.

[Example]

Permit access to the SSH server only from 192.168.1.1 and the 192.168.10.0/24 segment.

```
SWP2(config)#ssh-server access permit 192.168.1.1
SWP2(config)#ssh-server access permit 192.168.10.0/24
```

Deny only access to the SSH server from the segment 192.168.10.0/24.

```
SWP2(config)#ssh-server access deny 192.168.10.0/24
SWP2(config)#ssh-server access permit any
```

4.19.5 Generate SSH server host key

[Syntax]

ssh-server host key generate [bit *bit*]

[Parameter]

bit : 1024, 2048

Bit length of RSA key

[Initial value]

none

[Input mode]

priviledged EXEC mode

[Description]

Sets the host RSA key and host DSA key of the SSH server.

For the RSA key, the *bit* parameter can be used to specify the number of bits in the generated key. The DSA key generates a 1024-bit key.

[Note]

In order to use the SSH server function, this command must be executed in advance to generate the host keys.

If this command is executed when the host keys have already been specified, the user is asked to confirm whether to update the host keys.

It might take several minutes of time to generate the host keys.

This command can be executed only if the SSH server is disabled.

[Example]

Generate a 2048-bit RSA key and a DSA key.

```
SWP2#ssh-server host key generate bit 2048
```

4.19.6 Clear SSH server host key

[Syntax]

clear ssh-server host key

[Input mode]

priviledged EXEC mode

[Description]

Deletes the host RSA key and host DSA key of the SSH server.

[Note]

This command can be executed only if the SSH server is disabled.

[Example]

Delete the host RSA key and host DSA key.

```
SWP2#clear ssh-server host key
```

4.19.7 Show SSH server public key

[Syntax]

show ssh-server host key [fingerprint]

[Keyword]

fingerprint : Show key fingerprint

[Input mode]

priviledged EXEC mode

[Description]

Shows the public key of the SSH server.

If the "fingerprint" keyword is specified, the public key's key length, key fingerprint, and ASCII art are shown.

[Note]

Both the MD5 and SHA256 key fingerprint hash algorithms are shown.

[Example]

Show the public key.

```
SWP2#show ssh-server host key
ssh-dss XXXXXXXXXX1kc3MAAAEBAPTB9YYdgvE+4bbhF4mtoIJri+ujdAIfgr4hL/0w7Jlvc50eXg
sXJoCqlPlsLRGHOOzxVYbOouPCUV/jPFCatgOIii8eJNzUqSB1e6MOFtGjmESrdYiafyIUhps+YWqd
TlIo0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKWk1ChbatWnT/Z7RcmEVEou0qlOyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok8lL5qFhCHmGOGtqJTKZsqb5VnPz8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9alGo/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
PXUgrLf5HAAABAQCnnPO+ZjWZcZwGa6LxTGMczAjDy5uwD4DWBbRxsPKaXlsicJGC0aridnTthIGa8
```

```
ARypDjhpL1a37SDezx8yClQ5vh+4SPLdS1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAn3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RerToZ4vSgodskv7nyXX
XXXXXXX

ssh-rsa XXXXXXXXXX1yc2EAAAABIwAAAQEAwvAZK18jKTCHIHQfRV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3Knb7LX2SfymQYJ7XYIqMjmU0oziv/zi+De/z3M7wJHQUwfMZEDAdR6Mx39w
6Q04/ehQcaszjXi+0Al2wG/kk56lAU23CW/i21o//5GZTzkFKyEJUtWauHWEW9glF5Yy7F64PesqoH
6h5oDNK7LhlT7s4QXRnUJphIlINrW278Dnvyry3liR+tgTJAq3cGHfYsaQCdankDilQhUazUY0vJO
/gjYCjMuWH6Ek/cst+PCtgnt0XV5Bl079uRUmcACs2pDX5EWrwbPXXXXXXXXX==
```

Show the key fingerprint of the public key.

```
SWP2#show ssh-server host key fingerprint
ssh-dss
1024 MD5:XX:XX:a8:b9:51:93:9d:d2:ec:40:1a:43:66:3a:XX:XX
+---[DSA 1024]----+
|   .* .          |
|=*=+. o          |
|E+X+   o         |
| o . + = + .     |
|.. ..O X .       |
|oo=.B.*.o        |
|  o +   S o      |
|   . o           |
|    E            |
+------[MD5]------+
1024 SHA256:XXXXearwsCXvYTfIKrS6yYSrjMh0fW6W0Bw7aAOXXXX
+---[DSA 1024]----+
|  . +E.          |
|   o o           |
|    o X S        |
|   + = * .       |
|  o . B * .      |
|       + o .     |
|      * * +      |
|X+.@ +o=         |
|@*o.= o.         |
+----[SHA256]-----+

ssh-rsa
2048 MD5:XX:XX:b8:07:e3:5e:57:b8:80:e3:fc:b3:24:17:XX:XX
+---[RSA 2048]----+
|                 |
|...*             |
|*+.              |
|    .            |
|   .   +         |
|                 |
|        E        |
|     . B..       |
|      . oo       |
+------[MD5]------+
2048 SHA256:XXXXMkUuEbkJggPD68UoR+gobWPhgu7qqXzE8iUXXXX
+---[RSA 2048]----+
|*.==+            |
|*o+= . .         |
|*=o.  . S        |
|      * S . .    |
|     + B * o     |
| = = . . .       |
|    o            |
|     .           |
|. * *            |
+----[SHA256]-----+
```

4.19.8 Set SSH client alive checking

[Syntax]

ssh-server client alive enable [*interval* [*count*]]
ssh-server client alive disable
no ssh-server client alive

[Parameter]

interval	:	<1-2147483647> Client alive checking interval (seconds, if omitted: 100)
count	:	<1-2147483647> Maximum count for client alive checking (if omitted: 3)

[Initial value]

ssh-server client alive disable

[Input mode]

global configuration mode

[Description]

Sets whether to perform client alive checking.

A message requesting a response is sent to the client at intervals of the number of seconds specified by "interval". If there is no response for a successive number of times specified by "count", the connection with this client is cut and the session is ended.

If this command is executed with the "no" syntax, the setting returns to the default.

4.20 SSH client

4.20.1 Start SSH client

[Syntax]

ssh [*user@*] *host* [*port*]

[Parameter]

user	:	User name used when logging in to the remote host
host	:	Remote host name, IPv4 address (A.B.C.D), or IPv6 address (X:X::X:X) If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)
port	:	<1-65535> Port number to use (if omitted: 22)

[Initial value]

none

[Input mode]

priviledged EXEC mode

[Description]

Connects to the specified host via SSH.

If *user* is omitted, access the SSH server using the currently logged-in user name.

If *user* is omitted when logged in as an unnamed user, "root" is used.

[Note]

The escape character is the tilde (~). The escape character is recognized only if it is input at the beginning of the line.

If the escape character is input twice in succession at the beginning of the line, the escape character is used as input to the server.

If the escape character followed by a period (.) is input, the connection is forcibly closed.

If the escape character followed by a question mark (?) is input, a list of escape inputs is shown.

[Example]

To the host at IPv4 address 192.168.100.1, connect via SSH using user name "uname" and port number 12345.

```
SWP2#ssh uname@192.168.100.1 12345
```

To the host at IPv6 address fe80::2a0:deff:fe11:2233, connect via SSH using user name "uname" and port number 12345.

```
SWP2#ssh uname@fe80::2a0:deff:fe11:2233%vlan1 12345
```

4.20.2 Enable SSH client

[Syntax]

ssh-client *switch*
no ssh-client

[Parameter]

switch : Whether to enable SSH client

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ssh-client disable

[Input mode]

global configuration mode

[Description]

Enables use of the **ssh** command as an SSH client.
If this command is executed with the "no" syntax, the SSH client is disabled.

[Example]

Enable the SSH client.

```
SWP2(config)#ssh-client enable
```

4.20.3 Clear SSH host information

[Syntax]

clear ssh host *host*

[Parameter]

host : Remote host name, IPv4 address (A.B.C.D), or IPv6 address (X:X::X:X)

[Input mode]

priviledged EXEC mode

[Description]

Delete the public key of the SSH server that is connected as an SSH client.

[Example]

Clear the SSH host information.

```
SWP2#clear ssh host 192.168.100.1
```

4.21 E-mail notification

4.21.1 SMTP e-mail server settings

[Syntax]

mail server smtp *id* **host** *host* [**port** *port*] [**encrypt** *method*] [**auth** *username password*]
no mail server smtp *id*

[Keyword]

port : Specifying a port number for the e-mail server

encrypt : Specifying an encryption method

auth : Specifying the account information to use for SMTP authentication

[Parameter]

id : <1-10>

Mail server ID

host : Mail server address or host name

IPv4 address (A.B.C.D), IPv6 address (X:X::X:X)

When specifying an IPv6 link local address, the transmitting interface also needs to be specified (in fe80::X%vlanN format).

Host name (64 characters or less, Single-byte alphanumeric characters - . and :)

port : <1-65535>

Port number for e-mail server (this is 25 when omitted, and 465 when over-ssl is specified as *method*)

method : Encryption method

Setting value	Description
over-ssl	Encrypting communication (over SSL)
starttls	Encrypting communication (STARTTLS)

username : User name used for SMTP authentication

(64 characters or less, ? " | > and aingle-byte alphanumeric characters and symbols other than spaces)

password : Passwords used for SMTP authentication

(64 characters or less,? " | > and aingle-byte alphanumeric characters and symbols other than spaces)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets server information used when sending e-mails.

[Note]

When performing SMTP authentication, the AUTH LOGIN command is used for authentication.

For the SSL/TLS version, TLSv1, TLSv1.1 and TLSv1.2 are supported.

When setting an IPv6 address as the e-mail server address, encryption using SSL/TLS cannot be used.

[Example]

Sets the e-mail transmission server to “smtp-server-test.com”.

```
SWP2(config)#mail server smtp 1 host smtp-server-test.com
```

Specify “smtp-server-test2.com” as the e-mail transmission server, and configures settings for using encryption and SMTP authentication.

```
SWP2(config)#mail server smtp 1 host smtp-server-test2.com encrypt over-ssl auth
test_user test_password
```

4.21.2 SMTP e-mail server name settings

[Syntax]

mail server smtp *id* **name** *server_name*
no mail server smtp *id*

[Parameter]

id : <1-10>

E-mail server ID

server_name : Mail server name

(64 characters or less, single-byte alphanumeric characters and symbols other than ?)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the name of the server used when sending e-mails.

[Example]

Sets the e-mail transmission server name to “test_mail_server”.

```
SWP2(config)#mail server smtp 1 name test_mail_server
```

4.21.3 E-mail notification trigger settings

[Syntax]

mail notify *temp-id* **trigger** terminal
no mail notify *temp-id* **trigger** terminal

[Keyword]

terminal : Notify events related to the terminal monitoring function

[Parameter]

temp-id : <1-10>

E-mail template ID

Specify a template to use for event notification

[Initial value]

no mail notify

[Input mode]

global configuration mode

[Description]

Configures the settings for e-mail notification of event information for the specified function.

[Example]

Sets the terminal monitoring function event trigger for e-mail template #1.

```
SWP2(config)#mail notify 1 trigger terminal
```

4.21.4 E-mail transmission template settings mode

[Syntax]

mail template *temp-id*
no template

[Parameter]

temp-id : <1-10>

E-mail template ID

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Switches to the mode for setting the template used when sending e-mails.

The following items can be configured after switching to template mode. Up to 10 templates can be created.

- E-mail transmission destination address
- E-mail transmission source address
- Subject of e-mails sent
- Wait time settings for e-mail transmission (only event notification used)

[Example]

Switches to the mode for setting e-mail template #1.

```
SWP2(config)#mail template 1
SWP2(config-mail)#
```

4.21.5 E-mail transmission server ID settings

[Syntax]

send server *server-id*
no send server

[Parameter]

server-id : <1-10>
E-mail template ID

[Initial value]

no send server

[Input mode]

E-mail template mode

[Description]

Sets the ID of the e-mail server to be used.

[Example]

Specifies server ID #1 for the e-mail server used in e-mail template #1.

```
SWP2(config)#mail template 1
SWP2(config-mail)#send server 1
```

4.21.6 E-mail transmission source address setting

[Syntax]

send from *address*
no send from *address*

[Parameter]

address : Source e-mail address
(256 characters or less, single-byte alphanumeric characters and _ - . @)

[Initial value]

no send from

[Input mode]

E-mail template mode

[Description]

Sets the source e-mail address.

[Example]

Specifies “sample@test.com” as the source e-mail address for e-mail template #1.

```
SWP2(config)#mail template 1
SWP2(config-mail)#send from sample@test.com
```

4.21.7 Destination e-mail address setting for e-mail transmission

[Syntax]

send to *address*
no send to

[Parameter]

address	:	Destination e-mail address (256 characters or less, single-byte alphanumeric characters and _ - . @)

[Initial value]

no send to

[Input mode]

E-mail template mode

[Description]

Sets the destination e-mail addresses (maximum of four).

[Note]

This setting is used as the destination for event notifications, and is not used for the destinations when distributing certificates or sending notifications.

[Example]

Specifies “user@test.com” as the destination e-mail address for e-mail template #1.

```
SWP2(config)#mail template 1
SWP2(config-mail)#send to user@test.com
```

4.21.8 Setting for subject used when sending e-mails

[Syntax]

send subject *subject*
no send subject

[Parameter]

temp-id	:	Subject used when sending e-mails (128 characters or less, single-byte alphanumeric characters and symbols other than the characters ? | >)

[Initial value]

no send subject

[Input mode]

E-mail template mode

[Description]

Specifies the subject for e-mails that are sent.

[Note]

The subject shown below will be used if this is not set.

- Event notification : Notification from SWP2
- Certificate distribution : Certification publishment
- Certificate notification : Certification expiration

[Example]

Sets the subject to “TestMail” for e-mails sent using e-mail template #1.

```
SWP2(config)#mail template 1
SWP2(config-mail)#send subject TestMail
```

4.21.9 Wait time settings for e-mail transmission

[Syntax]

send notify wait-time *time*
no send notify wait-time

[Parameter]

time : <1-86400>
Transmission wait time (seconds)

[Initial value]

send notify wait-time 30

[Input mode]

E-mail template mode

[Description]

Sets the wait time before actually sending event-related notification e-mails.

[Note]

This setting is used as the wait time before event-related notification e-mails are sent.

[Example]

Sets the transmission wait time for e-mail template #1 to 60 seconds.

```
SWP2(config)#mail template 1
SWP2(config-mail)#send notify wait-time 60
```

4.21.10 E-mail settings when sending certificates

[Syntax]

mail send certificate *temp-id*
no mail send certificate

[Parameter]

temp-id : <1-10>
E-mail template ID

[Initial value]

no mail send certificate

[Input mode]

RADIUS configuration mode

[Description]

Specifies the template ID to use when sending RADIUS server client certificates.

The RADIUS server client certificate is sent to the e-mail address specified by the “user” command of the RADIUS server function.

[Note]

Example of e-mail body text used when sending RADIUS server client certificates
---
Certification is published.
Name : [Name] - Setting value for the NAME option in the “user” command
Account : [User name] - USERID value for the “user” command
MAC address : XX:XX:XX:XX:XX:XX
Expire : YYYY/MM/DD

[Example]

Specifies “#1” for the template ID to use when sending RADIUS server client certificates.

```
SWP2(config-radius)#mail send certificate 1
```

4.21.11 E-mail settings for certificate notification

[Syntax]

mail send certificate-notify *temp-id*
no mail send certificate-notify

[Parameter]

temp-id : <1-10>
E-mail template ID

[Initial value]

no mail send certificate-notify

[Input mode]

RADIUS configuration mode

[Description]

Specifies the template to use when sending notifications of RADIUS server client certificates by e-mail.

[Note]

Example of e-mail body text used when sending notifications beforehand about expired term of validity for RADIUS server client certificates
---
Your certificate will expire in [X] days.
Name : [Name] - Setting value for the NAME option in the “user” command
Account : [User name] - USERID value for the “user” command
MAC address : XX:XX:XX:XX:XX:XX
Expire : YYYY/MM/DD

[Example]

Specifies “#2” for the template to use when sending notifications of RADIUS server client certificates by e-mail.

```
SWP2(config-radius)#mail send certificate-notify 2
```

4.21.12 Notification timing settings for expired certificates

[Syntax]

mail certificate expire-notify *day* [*day*] [*day*]
no mail certificate expire-notify

[Parameter]

day : <1-90>
No. of days remaining for notification of expired term of validity

[Initial value]

mail certificate expire-notify 30

[Input mode]

RADIUS configuration mode

[Description]

Specifies the number of days to notify beforehand about expired term of validity for RADIUS server client certificates.

Up to three numbers of days for notifications can be specified.

[Note]

The *day* is displayed in descending order, regardless of the order in which it was inputted.

[Example]

Sets the number of days to notify beforehand about expired term of validity for RADIUS server client certificates to “50 days before” and “10 days before”.

```
SWP2(config-radius)#mail certificate expire-notify 50 10
```

4.21.13 Show e-mail transmission information

[Syntax]

show mail information [*temp-id*]

[Parameter]

temp-id : <1-10>
E-mail template ID

[Input mode]

priviledged EXEC mode

[Description]

Shows e-mail transmission information for the specified template ID.

If the template ID is omitted, this displays all e-mail information.

[Example]

Shows e-mail information for e-mail template #1.

```
SWP2#show mail information 1
 Template ID          : 1
 Notify trigger       : lan-map, terminal, stack
 LAN map notices      : hardware/loop/sfp-power/queue-usage/poe/snapshot/l2ms
 Server host          : smtp-server.com
 Server port          : 25
 Encryption           : STARTTLS
 Wait time            : 30 sec
 Mail address (from)  : sample@test.com
 Mail address (to)    : user1@test.com
                        user2@test.com
                        user3@test.com
                        user4@test.com
```

4.22 Yamaha Unified Network Operation Service (Y-UNOS)

4.22.1 Set Y-UNOS function

[Syntax]

y-unos enable
y-unos disable
no y-unos

[Keyword]

enable : Enable Y-UNOS function

disable : Disable Y-UNOS function

[Initial value]

y-unos enable

[Input mode]

global configuration mode

[Description]

Enables or disables Y-UNOS (Yamaha Unified Network Operation Service: a service which links devices together via a network).

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The Y-UNOS function operates only with the management VLAN. When no IPv4 address is set in the management VLAN or the management VLAN is linked down, the Y-UNOS function is stopped.

If the management VLAN has been changed, the multicast frame forwarding settings (**l2-mcast flood 239.192.128.250**) of the Y-UNOS mutual automatic recognition function are applied to the maintenance VLAN.

It may take up to one second to enable or disable the Y-UNOS function.

This command cannot be used if the stack function is enabled.

[Example]

This enables the Y-UNOS function.

```
SWP2(config)#y-unos enable
```

This disables the Y-UNOS function.

```
SWP2(config)#y-unos disable
```

4.22.2 Show Y-UNOS information

[Syntax]

show y-unos

[Input mode]

priviledged EXEC mode

[Description]

Shows Y-UNOS-related settings and status information.

The following content is displayed.

- Y-UNOS function settings (Y-UNOS)
- Y-UNOS function status (Status)
- Y-UNOS function IPv4 address (IPv4-Address)
  - View management VLAN IPv4 address and ID
- List of detected devices
  - Model name (Model)
  - Serial number (Serial)
  - Firmware version (Version)
  - MAC address (MAC-Address)
  - IPv4 address (IPv4-Address)
  - Host name (HostName)

One of the following items is displayed in the status (Status) for Y-UNOS.

Status	Description
Active	Operational status of Y-UNOS function
Inactive(stack enable)	Non-operational status of Y-UNOS function (stack function is enabled) *Only for devices that support stack functionality
Inactive(no ipv4 address)	Non-operational status of Y-UNOS function (IPv4 address not set for management VLAN, or management VLAN is linked down)
Disable	Y-UNOS function is disabled

[Example]

This shows the Y-UNOS information.

```
SWP2>show y-unos
Y-UNOS       : Enable
Status       : Active
IPv4 address : 192.168.10.6 (vlan1)

Model          Serial     Version     MAC-Address    IPv4-Address    HostName
-------------------------------------------------------------------------------
RM-CR          RMCR00001  V2.0.0      0000.0000.0000 192.168.10.5    RMCR-hostname
SWX3220-16MT   Z740000000 Rev.4.02.11 0000.0000.0000 192.168.10.4    SWX3220
SWX2310-28GT   Z610000000 Rev.2.04.15 0000.0000.0000 192.168.10.28   SW-Hostname002
```

4.23 LLDP

4.23.1 Enable LLDP function

[Syntax]

lldp run
no lldp run

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enable the LLDP function for the entire system.

If this command is executed with the "no" syntax, disable the LLDP function for the entire system.

[Note]

In order to enable the LLDP function for a port, the following command must be set.

Set the **set lldp enable** command's *type* (LLDP agent mode) to "txrx", "txonly", or "rxonly" as necessary.

- **lldp run** (global configuration mode)
- **lldp-agent** (interface mode)
- **set lldp enable** *type* (LLDP agent mode)

[Example]

Enable LLDP function transmission and reception for LAN port #1.

```
SWP2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set lldp enable txrx
```

4.23.2 Set system description

[Syntax]

lldp system-description *line*
no lldp system-description

[Parameter]

line : System description text string (255 characters or less)

[Initial value]

no lldp system-description

[Input mode]

global configuration mode

[Description]

Sets the system description used by the LLDP function.

If this command is executed with the "no" syntax, the setting returns to the default.

By default, this is "model name + firmware revision".

[Example]

Set the system description to SWITCH1_POINT_A.

```
SWP2(config)#lldp system-description SWITCH1_POINT_A
```

4.23.3 Set system name

[Syntax]

lldp system-name *name*
no lldp system-name

[Parameter]

name : System name text string (255 characters or less)

[Initial value]

no lldp system-name

[Input mode]

global configuration mode

[Description]

Sets the system name used by the LLDP function.

If this command is executed with the "no" syntax, the setting returns to the default.

By default, this is "model name".

The specified value is set in "LLDP System Name TLV".

[Example]

Set the system name to SWITCH1.

```
SWP2(config)#lldp system-name SWITCH1
```

4.23.4 Create LLDP agent

[Syntax]

lldp-agent
no lldp-agent

[Initial value]

none

[Input mode]

interface mode

[Description]

Create an LLDP agent, and transition to LLDP agent mode.

If this command is executed with the "no" syntax, delete the LLDP agent.

[Note]

When you delete the LLDP agent, the commands specified in LLDP agent mode are also deleted.

[Example]

Create an LLDP agent on port1.1, and transition to LLDP agent mode.

```
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#
```

4.23.5 Set automatic setting function by LLDP

[Syntax]

lldp auto-setting *switch*
no lldp auto-setting

[Parameter]

switch : Set automatic setting function by LLDP

Setting value	Description
enable	Enable automatic setting function by LLDP
disable	Disable automatic setting function by LLDP

[Initial value]

lldp auto-setting disable

[Input mode]

global configuration mode

[Description]

Enables the function by which LLDP frames transmitted by specific Yamaha devices can automatically modify the settings of a switch.

Also enables the notification function of the power supply stop timing for the **power-inline disable delay** command.

The following features are configured in LLDP frames.

- Flow control
- QoS
- IGMP snooping
- EEE
- RADIUS server host
- Terminal monitoring

If this command is executed with the "no" syntax, the setting returns to the default.

This can be set only for a physical interface.

[Note]

In order to use this function, you must use the **set lldp enable** command to enable reception of LLDP frames.

[Example]

Enable automatic setting function by LLDP.

```
SWP2(config)#lldp auto-setting enable
```

4.23.6 Set LLDP transmission/reception mode

[Syntax]

set lldp enable *type*
set lldp disable
no set lldp enable

[Parameter]

type : Transmission/reception mode

Setting value	Description
rxonly	Set receive-only mode
txonly	Set transmit-only mode
txrx	Set transmit and receive

[Initial value]

set lldp disable

[Input mode]

LLDP agent mode

[Description]

Sets the LLDP frame transmission/reception mode for the applicable interface.

If you specify **set lldp disable**, LLDP frames are not transmitted or received.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the LLDP transmission/reception mode of LAN port #1 to receive-only.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set lldp enable rxonly
```

4.23.7 Set type of management address

[Syntax]

set management-address-tlv *type*
no set management-address-tlv

[Parameter]

type : Type of management address

Setting value	Description
ip-address	Set IP address as the management address
mac-address	Set MAC address as the management address

[Initial value]

set management-address-tlv ip-address

[Input mode]

LLDP agent mode

[Description]

Sets the type of port management address used by LLDP.

If this command is executed with the "no" syntax, the setting returns to the default.

The specified value is set in "LLDP Management Address TLV".

[Example]

Set the MAC address as the type of management address for LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set management-address mac-address
```

4.23.8 Set basic management TLVs

[Syntax]

tlv-select basic-mgmt
no tlv-select basic-mgmt

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

Adds basic management TLVs to transmitted frames.

If this command is executed with the "no" syntax, exclude basic management TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<Basic management TLV>

(1) Port Description TLV : Description of port

(2) System Name TLV : Name of system

(3) System Description TLV : Description of system

(4) System Capabilities TLV : System capabilities

(5) Management Address TLV : Management address of port (MAC address or IP address)

[Example]

Add basic management TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select basic-mgmt
```

4.23.9 Set IEEE-802.1 TLV

[Syntax]

tlv-select ieee-8021-org-specific
no tlv-select ieee-8021-org-specific

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

Adds IEEE-802.1 TLVs to transmitted frames.

If this command is executed with the "no" syntax, exclude IEEE-802.1 TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<IEEE-802.1 TLV>

(1) Port VLAN ID : ID of port VLAN

(2) Port and Protocol VLAN ID : ID of protocool VLAN

(3) Protocol Identity : List of supported protocols

(4) Link Aggregation : Link aggregation information

(5) VLAN Name : Name of port VLAN

[Example]

Add IEEE-802.1 TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select ieee-8021-org-specific
```

4.23.10 Set IEEE-802.3 TLV

[Syntax]

tlv-select ieee-8023-org-specific
no tlv-select ieee-8023-org-specific

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

Adds IEEE-802.3 TLVs to transmitted frames.

If this command is executed with the "no" syntax, exclude IEEE-802.3 TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<IEEE-802.3 TLV>

(1) MAC/PHY Configuration/Status : Auto-negotiation support information

(2) Power Via MDI : PoE information (only for models with PoE function)

(3) Link Aggregation : Link aggregation information

(4) Maximum Frame Size : Maximum frame size

[Example]

Add IEEE-802.3 TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select ieee-8023-org-specific
```

4.23.11 Set LLDP-MED TLV

[Syntax]

tlv-select med
no tlv-select med

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

If this command is executed with the "no" syntax, exclude LLDP-MED TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<LLDP-MED TLV>

(1) Media Capabilities : Type of LLDP-MED TLV transmitted

(2) Network Policy : Voice VLAN information (Only ports for which voice VLAN is specified)

(3) Extended Power-via-MDI : Extended PoE information (only for models with PoE function)

[Note]

Location Identification TLV is set to a value of "Location".

[Example]

Add LLDP-MED TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select med
```

4.23.12 Set LLDP frame transmission interval

[Syntax]

set timer msg-tx-interval *tx_interval*
no set timer msg-tx-interval

[Parameter]

tx_interval : <5-3600>
LLDP frame transmission interval (seconds)

[Initial value]

set timer msg-tx-interval 30

[Input mode]

LLDP agent mode

[Description]

Sets LLDP frame transmission interval.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set 60 seconds as the LLDP frame transmission interval on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
```

```
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set timer msg-tx-interval 60
```

4.23.13 Set LLDP frame transmission interval for high speed transmission period

[Syntax]

set timer msg-fast-tx *fast_tx*
no set timer msg-fast-tx

[Parameter]

fast_tx : <1-3600>

LLDP frame transmission interval for high speed transmission period (seconds)

[Initial value]

set timer msg-fast-tx 1

[Input mode]

LLDP agent mode

[Description]

Sets the LLDP frame transmission interval during the high speed transmission period.

If this command is executed with the "no" syntax, the setting returns to the default.

The high speed transmission period is the period immediately after a port's connected device was newly found, and LLDP frames are transmitted according to the following commands for making high speed transmission period settings.

- **set timerx msg-fast-tx** *fast_tx* : Sets the transmission interval (seconds) during the high speed transmission period.
- **set tx-fast-init** *value* : Sets the number of LLDP frames transmitted during the high speed transmission period.

[Example]

Set 2 seconds as the LLDP frame transmission interval during the high speed transmission period on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set timer msg-fast-tx 2
```

4.23.14 Set time from LLDP frame transmission stop until re-initialization

[Syntax]

set timer reinit-delay *reinit_delay*
no set timer reinit-delay

[Parameter]

reinit_delay : <1-10>

Time from LLDP frame transmission stop until re-initialization (seconds)

[Initial value]

set timer reinit-delay 2

[Input mode]

LLDP agent mode

[Description]

Sets the time from when LLDP frame transmission stops until re-initialization occurs.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set 10 seconds as the time from when LLDP frame transmission stops on LAN port #1 until re-initialization occurs.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set timer reinit-delay 10
```

4.23.15 Set multiplier for calculating time to live (TTL) of device information

[Syntax]

set msg-tx-hold *value*
no set msg-tx-hold

[Parameter]

value : <1-100>

Multiplier for calculating the time to live (TTL) value of device information

[Initial value]

set msg-tx-hold 4

[Input mode]

LLDP agent mode

[Description]

Sets the multiplier for calculating the time to live (TTL) of device information.

If this command is executed with the "no" syntax, the setting returns to the default.

This setting is multiplied with the LLDP frame transmission interval (msg-tx-interval), and then increased by +1 to become the TTL value (seconds).

The TTL value is set in "Time To Live TLV".

TTL = msg-tx-interval x msg-tx-hold + 1 (seconds)

[Example]

Set 2 as the multiplier used to calculate the time to live (TTL) for device information on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set msg-tx-hold 2
```

4.23.16 Set number of LLDP frames transmitted during the high speed transmission period

[Syntax]

set tx-fast-init *value*
no set tx-fast-init

[Parameter]

value : <1-8>

Number of LLDP frames transmitted during the high speed transmission period

[Initial value]

set tx-fast-init 4

[Input mode]

LLDP agent mode

[Description]

Sets the number of LLDP frames transmitted during the high speed transmission period.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set 2 as the number of LLDP frames transmitted during the high speed transmission period on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set tx-fast-init 2
```

4.23.17 Set maximum number of connected devices manageable by a port

[Syntax]

set too-many-neighbors limit *max_value*
no set too-many-neighbors limit

[Parameter]

max_value : <1-1000>
Maximum number of connected devices manageable by a port

[Initial value]

set too-many-neighbors limit 5

[Input mode]

LLDP agent mode

[Description]

Sets the maximum number of connected devices that can be managed by a port.

If this command is executed with the "no" syntax, the setting returns to the default.

If the maximum number of connected device for a port is exceeded, LLDP frames sent from new devices are ignored.

[Note]

When this command is set, the remote device management table is cleared once when the first LLDP frame is received on the applicable port.

[Example]

Set 10 as the maximum number of connected devices that can be managed by a port on LAN port #1.

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set too-many-neighbors limit 10
```

4.23.18 Global interface setting for LLDP function

[Syntax]

lldp interface enable *type*
lldp interface disable

[Keyword]

enable : Enable LLDP function

disable : Disable LLDP function

[Parameter]

type : Transmission/reception mode

Setting value	Description
rxonly	Set receive-only mode
txonly	Set transmit-only mode
txrx	Set transmit and receive

[Input mode]

global configuration mode

[Description]

Enables or disables the LLDP function for all LAN/SFP+ port in a single operation.

If this setting is enabled, set the transmission and reception mode of the specified LLDP frames.

[Note]

This command can be executed only for global configuration mode.

This command is for making the LLDP setting of each interface, and is not shown in running-config.

[Example]

Enable the LLDP function of all LAN/SFP+ port, and set a mode that allows transmission and reception of LLDP frames.

```
SWP2(config)#lldp interface enable txrx
```

4.23.19 Show interface status

[Syntax]

show lldp interface *ifname* [neighbor]

[Keyword]

neighbor : Shows information for connected devices.

[Parameter]

ifname : Interface name of the LAN/SFP+ port

Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows LLDP information for the interface specified by *ifname*.

If "neighbor" is specified, information for the device connected to the interface is shown.

The following items are shown.

For **show lldp interface** *ifname*

- Interface and its statistical information

Agent Mode	Bridge mode (fixed as nearest bridge)
Enable (tx/rx)	Transmission mode/Reception mode (Y:enable, N:disable)
Message fast transmit time	LLDP frame transmission interval for high speed transmission period (seconds)
Message transmission interval	LLDP frame transmission interval (seconds)
Reinitialisation delay	Time from LLDP frame transmission stop until re-initialization (seconds)
MED Enabled	LLDP-MED TLV transmission enable/disable
Device Type	Device type (fixed as NETWORK_CONNECTIVITY)
Total frames transmitted	Number of LLDP frames transmitted
Total entries aged	Number of devices not received for more than TTL seconds, and deleted from management table
Total frames received	Number of LLDP frames received
Total frames received in error	Number of LLDP frame reception errors
Total frames discarded	Number of LLDP frames discarded
Total discarded TLVs	Number of TLV discarded
Total unrecognised TLVs	Number of TLVs that could not be recognized

For **show lldp interface** *ifname* neighbor

- Basic management information

Interface Name	Received interface name
System Name	System name
System Description	System description
Port Description	Port description
System Capabilities	System capabilities

Interface Numbering	Type of interface number
Interface Number	Number of interface
OID Number	OID number
Management Address	MAC address os IP addresss

- Mandatory TLV information

CHASSIS ID TYPE	CHASSIS ID TLV type and value
PORT ID TYPE	PORT ID TLV type and value
TTL (Time To Live)	Time to maintain device information (seconds)

- 8021 ORIGIN SPECIFIC TLV information

Port Vlan id	ID of port VLAN
PP Vlan id	ID of protocol VLAN
VLAN ID	ID of port VLAN
VLAN Name	Name of port VLAN
Remote Protocols Advertised	List of supported protocols
Remote VID Usage Digestt	VID Usage Digestt value
Remote Management Vlan	Name of management VLAN
Link Aggregation Status	Link aggregation enabled/disabled
Link Aggregation Port ID	ID of link aggregation port

- 8023 ORIGIN SPECIFIC TLV information

AutoNego Support	Auto negotiation enabled/disabled
AutoNego Capability	Communication methods that can be auto-negotiate
Operational MAU Type	Communication speed and duplex mode
MDI power support	Whether PoE function is supported
PSE power pair	PSE power pair
Power class	PoE power supply class
Type/source/priority	PoE power supply type, source, and priority order
PD requested power value	Power requested by PD device (0.1 mW units)
PSE allocated power value	Power that can be supplied by PSE device (0.1 mW units)
Link Aggregation Status	Link aggregation enabled/disabled
Link Aggregation Port ID	ID of link aggregation port
Max Frame Size	Maximum frame size

- LLDP-MED TLV information (shown if LLDP-MED TLV is received)

MED Capabilities	LLDP-MED TLV type list
MED Capabilities Dev Type	LLDP-MED media device type
MED Application Type	Application type
MED Vlan id	ID of VLAN
MED Tag/Untag	VLAN tagged or untagged
MED L2 Priority	L2 priority order
MED DSCP Val	DSCP value priority order
MED Location Data Format	Format of location data

Latitude Res	Resolution of latitude (number of significant upper bits)
Latitude	Latitude (34 bits)
Longitude Res	Resolution of longitude (number of significant upper bits)
Longitude	Longitude (34 bits)
AT	Altitude type
	1: meter
	2: floor of building
Altitude Res	Resolution of altitude (number of significant upper bits)
Altitude	Altitude (30 bits)
Datum	Geodetic datum
	0: USA's World Geodetic System (WGS 84)
	1: North American Datum (NAD 83)
	2: Average historical minimum sea level of North American Datum (NAD 83)
LCI length	Length of location information data
What	Place of reference location
	0: Location of the DHCP server
	1: Position of the network element thought to be nearest the client
	2: Location of client
Country Code	Country code
CA type	CA (Civic Address) type
MED Inventory	Inventory information list

Refer to RFC 3825 for details on location information.

[Example]

Show LLDP information for LAN port #1.

```
SWP2#show lldp interface port1.1
Agent Mode                    : Nearest bridge
Enable (tx/rx)                : Y/Y
Message fast transmit time    : 1
Message transmission interval : 30
Reinitialisation delay        : 2
MED Enabled                   : Y
Device Type                   : NETWORK_CONNECTIVITY
LLDP Agent traffic statistics
  Total frames transmitted       : 0
  Total entries aged             : 0
  Total frames received          : 0
  Total frames received in error : 0
  Total frames discarded         : 0
  Total discarded TLVs           : 0
  Total unrecognised TLVs        : 0
SWP2#
```

4.23.20 Show information for connected devices of all interfaces

[Syntax]

show lldp neighbors

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows information for connected devices of all interfaces.

(For the display format, refer to the **show lldp interface** *ifname neighbor* command)

[Example]

Show information for connected devices.

```
SWP2#show lldp neighbors
Interface Name           : port1.1
System Name              : SWP2-10MMF
System Description       : SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
Port Description         : port1.3
System Capabilities      : L2 Switching
Interface Numbering      : 2
Interface Number         : 5003
OID Number               :
Management MAC Address   : ac44.f230.0000
Mandatory TLVs
  CHASSIS ID TYPE
    IP ADDRESS           : 0.0.0.0
  PORT ID TYPE
    INTERFACE NAME       : port1.3
  TTL (Time To Live)     : 41
8021 ORIGIN SPECIFIC TLVs
  Port Vlan id               : 1
  PP Vlan id                 : 0
  Remote VLANs Configured
    VLAN ID                  : 1
    VLAN Name                : default
  Remote Protocols Advertised :
    Multiple Spanning Tree Protocol
  Remote VID Usage Digestt   : 0
  Remote Management Vlan     : 0
  Link Aggregation Status    :
  Link Aggregation Port ID   :
8023 ORIGIN SPECIFIC TLVs
  AutoNego Support           : Supported Enabled
  AutoNego Capability        : 27649
  Operational MAU Type       : 30
  Power via MDI Capability (raw data)
    MDI power support        : 0x0
    PSE power pair           : 0x0
    Power class              : 0x0
    Type/source/priority     : 0x0
    PD requested power value : 0x0
    PSE allocated power value : 0x0
  Link Aggregation Status    :
  Link Aggregation Port ID   :
  Max Frame Size             : 1522
LLDP-MED TLVs
  MED Capabilities           :
    Capabilities
    Network Policy
  MED Capabilities Dev Type  : End Point Class-3
  MED Application Type       : Reserved
  MED Vlan id                : 0
  MED Tag/Untag              : Untagged
  MED L2 Priority            : 0
  MED DSCP Val               : 0
  MED Location Data Format   : ECS ELIN
    Latitude Res      : 0
    Latitude          : 0
    Longitude Res     : 0
    Longitude         : 0
    AT                : 0
    Altitude Res      : 0
    Altitude          : 0
    Datum             : 0
    LCI length        : 0
    What              : 0
    Country Code      : 0
    CA type           : 0
  MED Inventory
```

```
SWP2#
```

4.23.21 Clear LLDP frame counters

[Syntax]

clear lldp counters

[Input mode]

priviledged EXEC mode

[Description]

Clear the LLDP frame counter of all ports.

[Example]

Clear the LLDP frame counter.

```
SWP2>clear lldp counters
```

4.24 L2MS (Layer 2 management service) settings

4.24.1 Set L2MS control frame transmit/receive

[Syntax]

l2ms filter enable
l2ms filter disable
no l2ms filter

[Keyword]

enable	:	L2MS control frames cannot be transmitted or received
disable	:	L2MS control frames can be transmitted or received

[Initial value]

l2ms filter disable

[Input mode]

interface mode

[Description]

Prevents L2MS control frames from being transmitted or received.

If this command is executed with the "no" syntax, L2MS control frames can be transmitted and received.

[Note]

This command cannot be specified for the following interfaces.

- VLAN interface
- A physical interface inside a logical interface

A physical interface inside a logical interface operates according to the setting of this command on the interface inside which it exists. If the physical interface is inside the logical interface, the setting of the physical interface returns to the default.

Regardless of the setting of this command, L2MS control frames might not be transmitted or received if any of the following conditions exist.

- The interface is in the Blocking status due to STP or the loop detection function
- The **switchport trunk native vlan none** command has been specified
- It is inside a logical interface

[Example]

Prevent port1.5 from transmitting or receiving L2MS control frames.

```
SWP2(config)#interface port1.5
SWP2(config-if)#l2ms filter enable
```

4.24.2 Show L2MS information

[Syntax]

show l2ms [detail]

[Keyword]

detail	:	Also show detailed information

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the following information.

- Whether managed by the L2MS manager
- MAC address of L2MS manager (if managed)

[Note]

Information is not shown if L2MS is not operating.

Specifying "detail" is valid only if L2MS is operating as manager.

[Example]

If operating as a agent, L2MS information is shown.

```
SWP2>show l2ms
Role : Agent

Status : Managed by Manager (ac44.f23d.0bb9)
```

4.25 Snapshot

4.25.1 Set snapshot function

[Syntax]

snapshot enable
snapshot disable
no snapshot

[Keyword]

enable	:	Snapshot function is enabled
disable	:	Snapshot function is disable

[Initial value]

snapshot disable

[Input mode]

global configuration mode

[Description]

Enables the snapshot function.

If this command is executed with the "no" syntax, disables the snapshot function.

[Note]

This command is valid only if L2MS is operating as manager.

[Example]

Enable the snapshot function.

```
SWP2(config)#snapshot enable
```

4.25.2 Set whether to include terminals in the snapshot comparison

[Syntax]

snapshot trap terminal [except-wireless]
no snapshot trap terminal

[Keyword]

except-wireless : Information for wirelessly connected terminals is excluded from the snapshot comparison.

[Initial value]

no snapshot trap terminal

[Input mode]

global configuration mode

[Description]

Terminal information is included in the snapshot comparison.

If the except-wireless option is specified, information for terminals that are wirelessly connected below a wireless access point are excluded from the snapshot comparison.

If this command is executed with the "no" syntax, terminal information is excluded from the snapshot comparison.

[Note]

This command is valid only when operating as the manager and the **terminal-watch enable** command and **snapshot enable** command have also been set.

[Example]

Include terminal information in the snapshot comparison.

```
SWP2(config)#snapshot trap terminal
```

4.25.3 Create snapshot

[Syntax]

snapshot save [after-update]

[Keyword]

after-update : After updating the network's connection state, save it as a snapshot

[Input mode]

priviledged EXEC mode

[Description]

Saves a snapshot file that is the base for the LAN map's snapshot function.

If the after-update option is not included, the network connection state currently maintained by the manager is saved as the snapshot file.

If the after-update option is included, the network connection state information is updated to the latest information, and then saved as the snapshot file.

[Note]

If the after-update option is included, the network connection state information is updated to the latest information, but depending on the configuration of the network, it might take some time for this update to be completed.

[Example]

After updating the network's connection state, save the snapshot file.

```
SWP2#snapshot save after-update
```

4.25.4 Delete snapshot

[Syntax]

snapshot delete

[Input mode]

priviledged EXEC mode

[Description]

Deletes the snapshot file.

[Example]

Delete the snapshot file.

```
SWP2#snapshot delete
```

4.26 Firmware update

4.26.1 Set firmware update site

[Syntax]

firmware-update url *url*
no firmware-update url

[Parameter]

url	:	Single-byte alphanumeric characters and single-byte symbols (255 characters or less) URL at which the firmware is located

[Initial value]

firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swp2.bin

[Input mode]

global configuration mode

[Description]

Specify the download source URL used when updating the firmware from a firmware file located on a web server.

The input syntax is "http://server IP address or hostname/pathname".

IPv6 addresses must be enclosed in "[]", as shown here: "[IPv6 address]".

When specifying an IPv6 link-local address, the sending interface must also be specified (fe80::X%vlanN syntax).

If the server's port number is other than 80, you must specify this within the URL, using the syntax "http://server IP address or hostname:port number/path name".

[Example]

Specify http://192.168.100.1/swp2.bin as the firmware download URL.

```
SWP2(config)#firmware-update url http://192.168.100.1/swp2.bin
SWP2(config)#
```

4.26.2 Configure the HTTP proxy server used for firmware updates

[Syntax]

firmware-update http-proxy *server port*
no firmware-update http-proxy

[Parameter]

server	:	A.B.C.D IPv4 address of the HTTP proxy server
server	:	[X:X::X:X] IPv6 address of the HTTP proxy server Must be enclosed in "[]", as shown here: "[X:X::X:X]" When specifying an IPv6 link-local address, the sending interface must also be specified (fe80::X%vlanN syntax).
	:	Alphanumeric characters and symbols (up to 255 characters) The HTTP proxy server FQDN
port	:	<1-65535> The HTTP proxy server listening port number

[Initial value]

no firmware-update http-proxy

[Input mode]

global configuration mode

[Description]

Configure the HTTP proxy server used when updating firmware using a firmware file located on the web server.

If no HTTP proxy server is configured, the firmware update will be performed without going through the HTTP proxy server.

The port number must also be explicitly configured.

If this command is executed with the "no" syntax, the HTTP proxy server setting is cleared.

[Example]

Set the HTTP proxy server to 192.168.100.1 (port number 8080).

```
SWP2(config)#firmware-update http-proxy 192.168.100.1 8080
SWP2(config)#
```

4.26.3 Execute firmware update

[Syntax]

firmware-update execute [no-confirm] [no-reboot]

[Keyword]

no-confirm	:	Don't confirm the firmware update
no-reboot	:	Does not reboot after updating firmware

[Input mode]

priviledged EXEC mode

[Description]

Compares the firmware file located on the web server with the revision of the currently-running firmware, and executes the update if rewriting is possible.

If firmware of a revision that can be rewritten exists, you will be asked for confirmation; enter "y" if you want to update, or enter "n" if you don't want to update.

If you specify "no-confirm," the update is executed without asking you for confirmation.

When no-reboot is specified, the system does not reboot after performing a revision update. It will boot with the updated firmware on the next boot.

[Note]

You can use the **firmware-update url** command to change the download source URL.

If you execute the **firmware-update revision-down enable** command, it will be possible to downgrade to an older revision.

When no-reboot is specified, the system will not reboot at the specified time, even if the **firmware-update revision-time** command is configured.

[Example]

Update the firmware using a firmware file located on a web server.

```
SWP2#firmware-update execute
Found the new revision firmware
Current Revision: Rev.2.03.01
New Revision:     Rev.2.03.03
Downloading...
Update to this firmware? (y/n)y
Updating...
Finish
SWP2#
```

4.26.4 Set firmware download timeout duration

[Syntax]

firmware-update timeout *time*
no firmware-update timeout

[Parameter]

time	:	<100-86400>
		Timeout time (seconds)

[Initial value]

firmware-update timeout 300

[Input mode]

global configuration mode

[Description]

Specifies the timeout duration when downloading firmware from a web server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the firmware download timeout duration to 120 seconds.

```
SWP2(config)#firmware-update timeout 120
SWP2(config)#
```

4.26.5 Allow revision-down

[Syntax]

firmware-update revision-down enable
no firmware-update revision-down

[Initial value]

no firmware-update revision-down

[Input mode]

global configuration mode

[Description]

When using a firmware file from a web server to update the firmware, this allows the firmware to be changed to a revision that is older than the current revision.

If this is executed with the "no" syntax, revision-down is not allowed.

[Example]

Allow revision-down.

```
SWP2(config)#firmware-update revision-down enable
SWP2(config)#
```

4.26.6 Show firmware update function settings

[Syntax]

show firmware-update

[Input mode]

priviledged EXEC mode

[Description]

Shows the current settings of the firmware update function.

The following items are shown.

- Download source URL
- Proxy server URL
- Download timeout duration
- Allow revision-down
- Firmware revision on next boot
- Reboot time after update

[Example]

Show the current settings of the firmware update function.

```
SWP2#show firmware-update
url: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swp2.bin
http-proxy: -
timeout: 300 (seconds)
revision-down: Disable
firmware revision for next boot: -
```

```
reload-time: -
SWP2#
```

4.26.7 Set firmware update reload time

[Syntax]

firmware-update reload-time *hour* [*min*]
no firmware-update reload-time

[Parameter]

hour : <0-23>

Firmware update reload time (hour)

min : <0-59>

Firmware update reload time (minutes)

[Input mode]

global configuration mode

[Description]

Sets the time at which the new firmware is applied by restarting after a firmware update.

If this command is executed with the "no" syntax, the new firmware is applied by restarting immediately after the firmware is updated.

[Example]

Specify AM 1:30 as the restart time for updating the firmware.

```
SWP2(config)#firmware-update reload-time 1 30
SWP2(config)#
```

4.27 Schedule

4.27.1 Schedule settings

[Syntax]

schedule *id* **time** *date time template_id*
schedule *id* **event** *event template_id*
no schedule *id*

[Parameter]

id : <1-10>

Schedule number

date : <1-12> or * / <1-12> or sun, mon, ... , sat or *

Month/day

Month setting examples	**Setting contents**
1	January
1.2	January and February
2-	From February to December
2-7	From February to July
-7	From January to July
*	Monthly

Day setting examples	**Setting contents**
1	One day
1.2	The 1st and the 2nd
2-	From the 2nd to the 12th
2-7	From the 2nd to the 7th
-7	From the 1st to the 7th
mon	Monday
sat,sun	Saturday and Sunday
mon-fri	From Monday to Friday
-fri	From Sunday to Friday
*	Monthly

time : <0-23> or * : <0-59> or * : <0-59>

h:m:s (the seconds can be omitted)

Hour setting examples	**Setting contents**
12	12:00
12.13	12:00 and 13:00
12-	From 12:00 to 23:00
10-20	From 10:00 to 20:00
-20	From 0:00 to 20:00
*	Hourly

Minute setting examples	**Setting contents**
30	30 minutes
15.45	15 minutes and 45 minutes
30-	From 30 minutes to 59 minutes
15-45	From 15 minutes to 45 minutes
-45	From 0 minutes to 45 minutes
*	Each minute

event : Event

Setting value	**Description**
startup	When booting

template_id : <1-10>

Schedule template number

[Initial value]

None

[Input mode]

global configuration mode

[Description]

When setting the schedule using “time,” this executes the actions listed in the specified schedule template at the specified time(s).

When setting the schedule using “event,” this executes the actions listed in the specified schedule template when the specified events occur.

If this command is executed with the "no" syntax, the schedule with the specified ID is deleted.

[Note]

When multiple schedules are executed at the same time, they are executed beginning with the schedule with the smallest ID.

When specifying the day, you cannot specify using a mix of numbers and weekdays.

If the seconds are omitted, the settings will be the same as when specifying “00” seconds.

For the month and days settings, you can specify ranges using “-” and “,” characters, and you can specify all dates using the “*” character. Note that for the seconds setting, you cannot specify ranges using “-” and “,” characters, nor can you specify all dates using the “*” character.

[Example]

This sets schedule #1 to execute schedule template #1 every Monday at exactly 0:00, 1:00, 2:00, 12:00, 21:00, 22:00 and 23:00.

```
SWP2(config)#schedule time */mon -2,12-14,21-:0 1
```

4.27.2 Schedule template description text settings

[Syntax]

description *line*
no description

[Parameter]

line : Single-byte alphanumeric characters and single-byte symbols (64 characters or less)

Schedule template description text

[Initial value]

no description

[Input mode]

Schedule template mode

[Description]

Sets the schedule template description text.

If this command is executed with the "no" syntax, the description text in the specified schedule template is deleted.

[Example]

This sets the description text for schedule template #1.

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#description Get tech-support
```

4.27.3 Settings to enable/disable schedule template

[Syntax]

action *switch*
no action

[Parameter]

switch : Schedule template settings

Setting value	Description
enable	Enable schedule template
disable	Disable schedule template

[Initial value]

action enable

[Input mode]

Schedule template mode

[Description]

This enables or disables the schedule template.

Specifying “disable” with this command makes it possible to stop execution of actions due to trigger startup.

If this command is executed with the "no" syntax, the schedule template is enabled.

[Example]

Disables schedule template #1.

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#action disable
```

4.27.4 Schedule template settings

[Syntax]

schedule template *template_id*
no schedule template

[Parameter]

template_id : <1-10>

Schedule template number

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Switches to the mode for setting the schedule template.

If this command is executed with the "no" syntax, the specified schedule template is deleted.

[Example]

This switches to the mode for setting schedule template #1.

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#
```

4.27.5 Schedule template command execution settings

[Syntax]

cli-command *id command*
no cli-command *id*

[Parameter]

id : <1-20>

Command no.

command : Command

[Initial value]

None

[Input mode]

Schedule template mode

[Description]

This sets the commands to be executed when the trigger for a schedule function starts.

If this command is executed with the "no" syntax, commands with the specified numbers are deleted.

[Note]

If both the “cli-command” command and “script” command are configured for the same schedule template, the “script” command will be executed, and the “cli-command” will not operate.

If multiple commands are specified, the commands are executed beginning with the command with the smallest command number.

If multiple commands are specified, the remaining commands will still be executed even if the command results in an execution error while running.

As commands are executed in privileged EXEC mode when the trigger starts, some commands may need to be configured along with commands that switch to an appropriate mode.

The last “write” command must be executed to save the settings.

Commands cannot be specified in abbreviated form. For instance, you must write “interface port1.1” and not “int port1.1” when entering the input mode for Port1.1 of the interface.

The following commands cannot be executed.

backup system, boot prioritize sd, no boot prioritize sd, certificate user, commands beginning with “clock,” cold start, copy radius-server local, crypto pki generate ca, no crypto pki generate ca, disable, enable password, exit, firmware-update execute, firmware-update sd execute, logout, commands beginning with “ntpdate,” commands beginning with “no ntpdate,” password-encryption, no password-encryption, ping, ping6, quit, reload, restart, restore system, schedule, no schedule, schedule template, no schedule template, commands beginning with “show,” ssh , ssh-server host key generate, startup-config select, no startup-config select, system-diagnostics on-demand execute(*1), telnet, traceroute, traceroute6

(*1): system-diagnostics on-demand execute no-confirm can be executed

[Example]

This registers the “copy tech-support sd” command in number #1 of schedule template #1.

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#cli-command 1 copy tech-support sd
```

4.28 General maintenance and operation functions

4.28.1 Set host name

[Syntax]

hostname *hostname*
no hostname [*hostname*]

[Parameter]

hostname : Single-byte alphanumeric characters and single-byte symbols (63characters or less)

Host name

[Initial value]

hostname SWP2

[Input mode]

global configuration mode

[Description]

Specifies the host name.

The host name specified by this command is used as the command prompt. If SNMP access is possible, this is used as the value of the MIB variable sysName.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Example]

Set the host name as "yamaha."

```
SWP2(config)#hostname yamaha
yamaha(config)#
```

4.28.2 Reload system

[Syntax]

reload
restart

[Input mode]

priviledged EXEC mode

[Description]

Reboots the system.

[Note]

If the currently-running settings (running configuration) have been changed from the settings at the time of boot (startup configuration), reboot will discard those changes. Therefore, if necessary, you should execute the **copy running-config startup-config** command, the **write** command or the **save** command before you execute the **reload** command.

[Example]

Reboot the system.

```
SWP2#reload
reboot system? (y/n): y
```

4.28.3 Initialize settings

[Syntax]

cold start

[Input mode]

priviledged EXEC mode

[Description]

Reboots with the factory settings. SYSLOG is also initialized.

[Note]

You must enter the administrator password when executing this command.

This command cannot be executed when the admin password is in the default state. The admin password must be changed first.

[Example]

Initialize the settings.

```
SWP2#cold start
Password:
```

4.28.4 Set default LED mode

[Syntax]

led-mode default *mode*
no led-mode default

[Parameter]

mode : Default LED mode

Setting value	Description
link-act	LINK/ACT mode
vlan	VLAN mode
off	OFF mode

[Initial value]

led-mode default link-act

[Input mode]

global configuration mode

[Description]

Set the default LED mode.

When you execute this command, the LEDs are lit in the specified mode. The LEDs are lit in the specified mode even when a loop is detected in STATUS mode and the loop status has been resolved.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the default LED mode to OFF mode.

```
SWP2(config)#led-mode default off
```

4.28.5 Show LED mode

[Syntax]

show led-mode

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the LED mode setting and status.

The following items are shown.

- Default LED mode setting
- Current LED mode status

[Example]

Show the LED mode setting and status.

```
SWP2>show led-mode
default mode : off
current mode : link-act
```

4.28.6 Starting the "Find this switch" function

[Syntax]

find switch start *sec method*

[Parameter]

sec : <5-3600>

“Find this switch” time (seconds)

method : Method

Parameter	Description
led	Blinks the port LED in amber.

[Input mode]

priviledged EXEC mode

[Description]

Executes the “Find this switch” function with the specified number of seconds and method.

[Note]

If the current LED mode is OFF mode, the LED cannot blink.

[Example]

Start the "Find this switch" function with LED for 10 seconds only.

```
SWP2#find switch start 10 led
```

4.28.7 Stop the “Find this switch” function

[Syntax]

find switch stop

[Input mode]

priviledged EXEC mode

[Description]

Stops the 'Find this switch' function.

[Example]

Stops the 'Find this switch' function.

```
SWP2#find switch stop
```

4.28.8 Show DIP switches status

[Syntax]

show dipsw

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Show status of the DIP switches at startup and the current status.

[Example]

Show the status of the DIP switches.

```
SWP2>show dipsw
 DIPSW              SW1   SW2   SW3   SW4
--------------------------------------
 Startup status :   ON    OFF   OFF   ON
 Current status :   ON    OFF   OFF   ON
```

4.28.9 Show port error LED status

[Syntax]

show error port-led

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the ID of ports that are generating an error, and the following error causes.

Item	Description
loop-detected (blocking)	Detected a loop, and are currently blocking
loop-detected (shutdown)	Detected a loop, and are currently shutdown
sfp rx-power error (low)	SFP optical reception level is below the normal range
sfp rx-power error (high)	SFP optical reception level is above the normal range

[Example]

Show the port error status.

```
SWP2>show error port-led
 ID             error
----------------------------------------
 port1.1        loop-detected (blocking)
```

4.28.10 Set ProAV profile type

[Syntax]

proav profile-type *type*
no proav profile-type

[Parameter]

type : ProAV profile type

Setting value	Description
dante-primary	Dante primary
dante-primary	Dante secondary
ndi	NDI
sdvoe	SDVoE

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the ProAV profile type.

This command is used with the the ProAV settings page in the Web GUI, to select the compatible ProAV profile type for the VLAN.

[Note]

Executing this command via CLI does not apply the ProAV profile settings.

Chapter 5

Interface control

5.1 Interface basic settings

5.1.1 Set description

[Syntax]

description *line*
no description

[Parameter]

line : Single-byte alphanumeric characters and single-byte symbols (80characters or less)
Description of the applicable interface

[Initial value]

no description

[Input mode]

interface mode

[Description]

Specifies a description of the applicable interface. If this command is executed with the "no" syntax, the description is deleted.

[Example]

Specify a description for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#description Connected to rtx1210-router
```

5.1.2 Shutdown

[Syntax]

shutdown
no shutdown

[Initial value]

no shutdown

[Input mode]

interface mode

[Description]

Shut down the applicable interface so that it is not used.

An interface for which this command is specified will not link-up even if it is connected.

If this command is executed with the "no" syntax, the applicable interface can be used.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

If this command is applied to logical interface, the settings of all LAN/SFP+ port units belonging to that interface are changed.

[Example]

Shut down LAN port #1 so that it is not used.

```
SWP2(config)#interface port1.1
SWP2(config-if)#shutdown
```

5.1.3 Set speed and duplex mode

[Syntax]

speed-duplex *type*

no speed-duplex

[Parameter]

type : Speed and duplex mode types

Speed and duplex mode types	Description
auto	Auto negotiation
10000-full	10Gbps/Full
1000-full	1000Mbps/Full
100-full	100Mbps/Full
100-half	100Mbps/Half
10-full	10Mbps/Full
10-half	10Mbps/Half

[Initial value]

speed-duplex auto

[Input mode]

interface mode

[Description]

Sets the speed and duplex mode.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

This command can be specified only for LAN/SFP+ port.

*type*10000-full cannot be set for the LAN port.

The only *type* that can be specified for SFP+ port is auto or 10000-full.

[Example]

Set the speed and duplex mode for LAN port #1 to 100Mbps/Full.

```
SWP2(config)#interface port1.1
SWP2(config-if)#speed-duplex 100-full
```

5.1.4 Set MRU

[Syntax]

mru *mru*

no mru

[Parameter]

mru : <64-10240>

Maximum frame size that can be received (the specified value must be an even number)

[Initial value]

mru 1522

[Input mode]

interface mode

[Description]

Specifies the maximum frame size that can be received.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port.

[Example]

Set the LAN port #1 mru to 9000 bytes.

```
SWP2(config)#interface port1.1
SWP2(config-if)#mru 9000
```

5.1.5 Set cross/straight automatic detection

[Syntax]

mdix auto *action*
no mdix auto

[Parameter]

type : Cross/straight automatic detection operations

Setting value	Description
enable	Enable cross/straight automatic detection
disable	Disable cross/straight automatic detection

[Initial value]

mdix auto enable

[Input mode]

interface mode

[Description]

Enables cross/straight automatic detection. If this is enabled, the necessary cable connection type (straight or cross) is automatically detected, and the connection is specified appropriately.

If this is executed with the "no" syntax, automatic detection is disabled, and MDI is used.

[Note]

This command can be specified only for LAN port.

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

[Example]

Disable cross/straight automatic detection for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#mdix auto disable
```

5.1.6 Set EEE

[Syntax]

eee *action*
no eee

[Parameter]

type : Behavior of the EEE

Setting value	Description
enable	Enable EEE
disable	Disable EEE

[Initial value]

eee disable

[Input mode]

interface mode

[Description]

Enables Energy Efficient Ethernet (EEE).

If this command is executed with the "no" syntax, EEE is disabled.

[Note]

This command can be specified only for LAN port.

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

[Example]

Enable EEE for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#eee enable
```

5.1.7 Show EEE capabilities

[Syntax]

show eee capabilities interface *ifname*

[Parameter]

ifname	:	LAN port interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows whether the specified interface supports EEE.

The following items are shown.

Item	Description
interface	Interface name
EEE(efficient-ethernet)	Whether the unit supports EEE
Link Partner	Whether the other unit supports EEE

[Note]

If another unit is not connected, the display indicates that EEE is not supported.

[Example]

Show EEE capabilities for LAN port #1.

[If the other unit supports EEE]

```
SWP2#show eee capabilities interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  yes (1000-T, 100-TX)
  Link Partner           :  yes (1000-T, 100-TX)
```

[If the other unit does not support EEE]

```
SWP2#show eee capabilities interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  yes (1000-T, 100-TX)
  Link Partner           :  not enabled
```

5.1.8 Show EEE status

[Syntax]

show eee status interface *ifname*

[Parameter]

ifname	:	LAN port interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the EEE status of the specified interface.

The following items are shown.

Item	Description
interface	Interface name
EEE(efficient-ethernet)	Whether EEE is enabled
Rx LPI Status	Low-power mode status of the receiving unit
Tx LPI Status	Low-power mode status of the transmitting unit
Wake Error Count	Error count

[Example]

Show EEE status of LAN port #1.

[If EEE is disabled]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Disabled
  Rx LPI Status           :  None
  Tx LPI Status           :  None
  Wake Error Count        :  0
```

[If EEE is enabled]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status           :  Received
  Tx LPI Status           :  Received
  Wake Error Count        :  0
```

[If EEE is enabled and is transitioning to low-power mode]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status           :  Interrupted
  Tx LPI Status           :  Interrupted
  Wake Error Count        :  0
```

[If EEE is enabled and has transitioned to low-power mode]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status           :  Low Power
  Tx LPI Status           :  Low Power
  Wake Error Count        :  0
```

5.1.9 Set port mirroring

[Syntax]

mirror interface *ifname* direction *direct*
no mirror interface *ifname* [direction *direct*]

[Keyword]

direction : Specify the direction of traffic that is mirrored

[Parameter]

ifname : LAN/SFP+ port interface name
Interface whose traffic is mirrored

direct : Direction of traffic that is mirrored

Traffic direction	Description
both	Both receiver and transmitter
receive	Receiver
transmit	Transmitter

[Initial value]

none

[Input mode]

interface mode

[Description]

Mirrors the traffic specified by *direct*, with the applicable interface as the sniffer port and *ifname* as the monitored port.

If this command is executed with the "no" syntax, the mirroring setting is deleted.

[Note]

This command can be specified only for LAN/SFP+ port.

Only one interface can be specified as the sniffer port.

[Example]

With LAN port #1 as the sniffer port, mirror the transmitted and received frames of LAN port #4 and the transmitted frames of LAN port #5.

```
SWP2(config)#interface port1.1
SWP2(config-if)#mirror interface port1.4 direction both
SWP2(config-if)#mirror interface port1.5 direction transmit
```

5.1.10 Show port mirroring status

[Syntax]

show mirror [interface *ifname*]

[Keyword]

interface : Specify the monitored port to show

[Parameter]

ifname : Interface name of the LAN/SFP+ port

Monitored port to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the port mirroring setting. If interface is omitted, the settings for all monitored ports are shown.

The following items are shown for each monitored port.

Item	Description
Monitored Port	Interface name of the monitored port
Sniffer Port	Interface name of the sniffer port
Direction	>Direction of traffic that is mirrored

[Example]

Show the mirroring port settings.

```
SWP2#show mirror
Sniffer Port   Monitored Port  Direction
=============  ==============  ==========
port1.1        port1.4         both
port1.1        port1.5         transmit
```

5.1.11 Show interface status

[Syntax]

show interface [*type* [*index*]]

[Parameter]

type : Interface type

Interface type	Description
port	Physical interface
vlan	VLAN interface
sa	Static logical interface
po	LACP logical interface

index : Index number

Interface ID	Description
1.X	Specifies the number printed on the chassis (X).
<1－4094>	Specify the VLAN ID.
<1－96>	Speciffy the static logical interface number.
<1－127>	Specify the LACP logical interface number.

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the status of the interface specified by *ifname*. If *ifname* is omitted, shows the status of all interfaces.

The following items are shown.

Item	Description
Interface	Interface name
Link is	Link status *2 (if shutdown, shows the cause) • If shutdown is specified : (by shutdown) • If port error is detected : (by err-disable)
Hardware is	Interface type (e.g., Ethernet, VLAN)
HW addr	Physical (MAC) address *1
Description	Description of interface
ifIndex	Interface index number
MRU	Maximum Receive Unit *4
ARP ageing timeout	ARP timeout time (time that ARP entries are maintained) *3
Speed-Duplex	Speed and duplex mode settings, and operating status *1
Auto MDI/MDIX	Auto MDI/MDIX enabled/disabled *1
IPv4 address	IP address/mask length *3 (shown only if IP address is set)
broadcast	IP broadcast address *3 (shown only if IP address is set)

Item		Description
Switchport mode		Mode of the switchport • access : untagged • trunk : tagged
Ingress filter		Status of ingress filtering • enable : enabled • disable : disabled
Acceptable frame types		Frame types that can be received • all : All frames are received (regardless of whether they are tagged or untagged) • vlan-tagged only : Only frames with a VLAN tag are received
Default Vlan		VLAN ID that handles untagged frames • For an untagged port: VLAN specified by the **switchport access vlan** command • For a tagged port: Native VLAN • For a tagged port and set to receive only tagged packets: None • If unspecified: vlan1
Configured Vlans		List of the VLAN IDs that belong to the corresponding interface
input	packets	Number of received packets *2
	bytes	Number of received bytes *2
	multicast packets	Number of received multicast packets *2
	drop packets	Number of overflowed packets received *2, *5
output	packets	Number of transmitted packets *2
	bytes	Number of transmitted bytes *2
	multicast packets	Number of transmitted multicast packets *2
	broadcast packets	Number of transmitted broadcast packets *2
	drop packets	Number of tail-dropped packets transmitted *2, *5

*1 Shown only for physical interface
*2 Shown only for physical interface and logical interface
*3 Shown only for VLAN interface
*4 In the case of logical interface and VLAN interface, shows the minimum value for the physical interface belonging to that interface
*5 Shows the transmission information when tail dropping is enabled, and the information only for reception when tail dropping is disabled.

[Example]

Show the status of LAN port #1.

```
SWP2# show interface port 1.1
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: 00a0.de00.0000
  Description: Connected to router
  ifIndex 5001, MRU 1522
  Speed-Duplex: auto(configured), 1000-full(current)
```

```
  Auto MDI/MDIX: on
  Vlan info:
    Switchport mode         : access
    Ingress filter          : enable
    Acceptable frame types  : all
    Default Vlan            :    1
    Configured Vlans        :    1
  Interface counter:
    input  packets          : 320
           bytes            : 25875
           multicast packets: 301
    output packets          : 628
           bytes            : 129895
           multicast packets: 628
           broadcast packets: 0
           drop packets     : 0
```

Show the status of VLAN #1.

```
SWP2#show interface vlan 1
Interface vlan1
  Hardware is VLAN
  Description: Connected to router(VLAN)
  ifIndex 301, ARP ageing timeout 1200
  IPv4 address 192.168.100.240/24 broadcast 192.168.100.255
                                                  (u)-Untagged, (t)-Tagged
VLAN ID  Name                             State   Member ports
======= ================================ ======= ====================
1       default                          ACTIVE  port1.1(u) port1.2(u)
                                                 port1.3(u) port1.4(u)
                                                 port1.5(u) port1.6(u)
                                                 port1.7(u) port1.8(u)
```

5.1.12 Show brief interface status

[Syntax]

show interface brief

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode, individual configuration mode

[Description]

Shows brief interface status.

The following items are shown.

Item	Description
Interface	Interface name
Type	Interface type *2
PVID	VLAN ID that handles untagged frames *2
Mode	Mode of the switchport *2 • access : untagged • trunk : tagged
Status	Link status
Reason	Cause of link down • AD: If shutdown is specified • ED: If port error is detected • PD: Other than above
Speed	Communication speed operating status *2

Item	Description
Port Ch	Type of associated logical interface *1 • (S) : Static logical interface • (P) : LACP logical interface ID of associated logical interface
Description	Description of interface

*1 Shown only for physical interface
*2 hown only for physical interface and logical interface

[Example]

Show brief interface status.

```
SWP2#show interface brief

Codes: ETH - Ethernet, AGG - Aggregate , PVID - Port Vlan-id
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down



--------------------------------------------------------------------------------
Ethernet   Type  PVID  Mode       Status  Reason  Speed Port    Description
Interface                                           Ch #
--------------------------------------------------------------------------------
port1.1    ETH   1     access     up      --      1g    (S)1    --
port1.2    ETH   1     access     up      --      1g    --      --
port1.3    ETH   1     access     down    PD      auto  --      --
port1.4    ETH   1     access     down    AD      auto  --      --
port1.5    ETH   1     access     up      --      1g    --      --
port1.6    ETH   1     access     up      --      1g    --      --
port1.7    ETH   1     access     up      --      1g    --      --
port1.8    ETH   1     access     up      --      1g    --      --


--------------------------------------------------------------------------------
Interface    Status   Reason  Description
--------------------------------------------------------------------------------
vlan1        up       --      --
vlan2        down     PD      --


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode       Status   Reason  Speed  Description
Interface
--------------------------------------------------------------------------------
sa1           AGG   1     access     up       --      1g     --
```

5.1.13 Resetting an interface

[Syntax]

interface reset *ifname*

[Parameter]

ifname : LAN/SFP+ port or logical interface
Interface to reset

[Input mode]

priviledged EXEC mode

[Description]

This resets the specified interface.

[Note]

The link status for the specified interface will be reset, and the link is re-established.

Note that linkdown will momentarily occur in order to reset.

This cannot be executed for LAN/SFP+ port that belong to logical interface

[Example]

Reset LAN port #1

```
SWP2#interface reset port1.1
```

5.1.14 Show frame counter

[Syntax]

show frame-counter [*ifname*]

[Parameter]

ifname : Interface name of the LAN/SFP+ port

Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows frame counter information for the interface specified by *ifname*. If *ifname* is omitted, shows information for all interfaces.

The following items are shown.

Item	Description
Packets	Number of packets transmitted/received
Octets	Number of octets transmitted/received
Broadcast packets	Number of broadcast packets transmitted/received
Multicast packets	Number of multicast packets transmitted/received
Unicast packets	Number of unicast packets transmitted/received
Undersize packets	Number of undersize packets received (packets smaller than 64 octets)
Oversize packets	Number of oversize packets received (packets larger than 1523 octets*1)
Fragments	Number of fragment packets received (packs smaller than 64 octets with abnormal CRC)
Jabbers	Number of jabber packets received (packs larger than 1523 octets with abnormal CRC*1)
FCS errors	Number of FCS error packets received
RX errors	Number of reception errors
TX errors	Number of transmission errors
Collisions	Number of collision occurrences
Drop packets	Number of tail-dropped packets transmitted, number of packets not received due to buffer overflow *2
64octet packets	Number of packets with 64 octet length transmitted/received
65-127octet packets	Number of packets with 65--127 octet length transmitted/ received
128-255octet packets	Number of packets with 128--255 octet length transmitted/ received
256-511octet packets	Number of packets with 256--511 octet length transmitted/ received
512-1023octet packets	Number of packets with 512--1023 octet length transmitted/ received
1024-MAXoctet packets	Number of packets with 1024--maximum octet length (*1) transmitted/received

*1 Varies depending on the MRU of each interface.
*2 Shows the transmission information when tail dropping is enabled, and the information only for reception when tail dropping is disabled.

[Example]

Show the frame counter of LAN port #1.

```
SWP2#show frame-counter port1.1
Interface port1.1 Ethernet MAC counters:
  Received:
    Packets               : 84
    Octets                : 6721
    Broadcast packets     : 8
    Multicast packets     : 76
    Unicast   packets     : 0
    Undersize packets     : 0
    Oversize  packets     : 0
    Fragments             : 0
    Jabbers               : 0
    FCS errors            : 0
    RX errors             : 0

  Transmitted:
    Packets               : 91
    Octets                : 11193
    Broadcast packets     : 0
    Multicast packets     : 91
    Unicast   packets     : 0
    TX errors             : 0
    Collisions            : 0
    Drop packets          : 0

  Received and Transmitted:
    64octet       packets : 1
    65-127octet   packets : 166
    128-255octet  packets : 7
    256-511octet  packets : 1
    512-1023octet packets : 0
    1024-MAXoctet packets : 0
```

5.1.15 Clear frame counters

[Syntax]

clear counters *ifname*
clear counters all

[Keyword]

all	:	Clearing the frame counter information for all interfaces

[Parameter]

ifname	:	Interface name of LAN/SFP+ port or logical interface Applicable interface

[Input mode]

priviledged EXEC mode

[Description]

This clears the frame counter for the interfaces.

If *ifname* is specified, the frame counter for that interface is cleared.

If logical interface is specified as the *ifname*, the frame counters of all LAN/SFP+ port port units associated with that interface are cleared.

[Example]

Clear the frame counters of LAN port #1.

```
SWP2#clear counters port1.1
```

5.1.16 Show SFP+ module status

[Syntax]

show ddm status

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the status of the SFP+ module.

For each item, shows the current value, upper threshold value, and lower threshold value for each SFP+ port.

Item	Description
Temperature	Internal temperature of the module (°C)
Voltage	Voltage value (V)
Current	Current value (mA)
TX-Power	Strength of light produced (dBm)
RX-Power	Strength of light received (dBm)

[Example]

Show the status of the SFP+ module.

```
SWP2#show ddm status
             Temperature  High Alarm   High Warning Low Warning  Low Alarm
Interface    (Celsius)    Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11     42.7         100.0         85.0        -40.0        -55.0
 port1.12     40.7          95.0         90.0        -20.0        -25.0

             Voltage      High Alarm   High Warning Low Warning  Low Alarm
Interface    (V)          Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11    3.37         3.62         3.46         3.13         2.97
 port1.12    3.34         3.89         3.70         2.89         2.70

             Current      High Alarm   High Warning Low Warning  Low Alarm
Interface    (mA)         Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11      4.0         16.0          15.0          2.0          2.0
 port1.12      6.2         17.0          14.0          2.0          1.0

             TX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11     -5.4806       0.4139       0.0000     -10.7058     -12.2184
 port1.12     -5.4714      -1.9997      -1.9997     -11.0237     -11.7392

             RX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11     -7.5696       2.5527       0.0000     -16.9897     -40.0000
 port1.12     -8.7614       1.0002      -1.0017     -18.0134     -20.0000
```

5.1.17 Set SFP+ module optical reception level monitoring

[Syntax]

sfp-monitor rx-power *action*
no sfp-monitor rx-power

[Parameter]

action : Operations for SFP+ module optical reception level monitoring

Setting value	Description
enable	Enables SFP+ module optical reception level monitoring
disable	Disables SFP+ module optical reception level monitoring

[Initial value]

sfp-monitor rx-power enable

[Input mode]

global configuration mode

[Description]

Sets the monitoring of SFP+ module optical reception levels.

[Example]

Disable SFP+ module optical reception level monitoring.

```
SWP2(config)#sfp-monitor rx-power disable
```

5.1.18 Configuring transmission queue usage rate monitoring (system)

[Syntax]

tx-queue-monitor usage-rate *action*
no tx-queue-monitor usage-rate

[Parameter]

action : Configuration for system-wide transmission queue usage rate monitoring

Setting value	Description
enable	Enable system-wide transmission queue usage rate monitoring
disable	Disable system-wide transmission queue usage rate monitoring

[Initial value]

tx-queue-monitor usage-rate enable

[Input mode]

global configuration mode

[Description]

Enable or disable system-wide transmission queue usage rate monitoring.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable transmission queue usage rate monitoring, in addition to this command, transmission queue usage rate monitoring must also be enabled on the interface.

[Example]

Disable system-wide transmission queue usage rate monitoring.

```
SWP2(config)#tx-queue-monitor usage-rate disable
```

5.1.19 Configuring transmission queue usage rate monitoring (interface)

[Syntax]

tx-queue-monitor usage-rate *action*
no tx-queue-monitor usage-rate

[Parameter]

action : Configuration for transmission queue usage rate monitoring of the target interface

Setting value	Description
enable	Enable transmission queue usage rate monitoring of the target interface
disable	Disable transmission queue usage rate monitoring of the target interface

[Initial value]

tx-queue-monitor usage-rate enable

[Input mode]

interface mode

[Description]

Enable or disable transmission queue usage rate monitoring of the target interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can only be set for LAN/SFP+ port.

To enable transmission queue usage rate monitoring, in addition to this command, system-wide transmission queue usage rate monitoring must also be enabled.

[Example]

Disable transmission queue usage rate monitoring for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#tx-queue-monitor usage-rate disable
```

5.1.20 Display configuration for transmission queue usage rate monitoring

[Syntax]

show tx-queue-monitor

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Displays the transmission queue usage rate monitoring configuration.

The display details are as follows.

- Configuration for system-wide transmission queue usage rate monitoring
- Configuration by LAN/SFP+ port
  - Interface name (port)
  - Configure transmission queue usage rate monitoring for LAN/SFP+ port (usage-rate).

[Example]

Displays the transmission queue usage rate monitoring configuration.

```
SWP2>show tx-queue-monitor
usage-rate: Enable

port      usage-rate
-------------------
port1.1       enable
port1.2       enable
port1.3       enable
port1.4       enable
port1.5       enable
port1.6       enable
port1.7      disable
   :            :
port2.1       enable
   :            :
```

5.2 Link aggregation

5.2.1 Set static logical interface

[Syntax]

static-channel-group *link-id*
no static-channel-group

[Parameter]

link-id : <1-96>
static logical interface number

[Input mode]

interface mode

[Description]

Associates the applicable interface with the static logical interface specified by *link-id*.

If this command is executed with the "no" syntax, the applicable interface is dissociated from the static logical interface.

[Note]

This command can be specified only for LAN/SFP+ port.

If a LAN/SFP+ port is associated to a *link-id* for which a static logical interface does not exist, the static logical interface is newly generated.

If the associated LAN/SFP+ port is no longer present because it was removed from the static logical interface, the static logical interface is deleted.

Up to eight LAN/SFP+ port units can be associated with one static logical interface.

If it is to be associated with an already-existing static logical interface, all of the following settings must match between the LAN/SFP+ port and the static logical interface. If the settings differ, an error occurs.

- VLAN setting
- Set QoS trust mode (including default CoS value and port priority)
- Set loop detection (enable/disable loop detection, enable/disable port blocking)

If a static logical interface is newly generated, the above settings of the LAN/SFP+ port are set to the default settings of the static logical interface.

If a LAN/SFP+ port is associated with a static logical interface, the MSTP settings return to the default values. The MSTP settings also return to the default values if the LAN/SFP+ port is removed from the static logical interface.

It is not possible to associate a single LAN/SFP+ port with multiple logical interface units. You must use the "no" syntax to first remove it before associating it with a different logical interface.

[Example]

Associate LAN port #1 with static logical interface #5.

```
SWP2(config)#interface port1.1
SWP2(config-if)#static-channel-group 5
```

5.2.2 Show static logical interface status

[Syntax]

show static-channel-group

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the static logical interface status.

The following items are shown for each static logical interface that exists.

- static logical interface name
- Load balance function rules
- Interface name of associated LAN/SFP+ port

For details on the load balance function rules, refer to the *type* parameter of the **port-channel load-balance** command.

[Example]

Show the static logical interface status.

```
SWP2#show static-channel-group
% Static Aggregator: sa5
% Load balancing: src-dst-mac
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
```

5.2.3 Set LACP logical interface

[Syntax]

channel-group *link-id* **mode** *mode*
no channel-group

[Parameter]

link-id : <1-127>

LACP logical interface number

mode : Operation mode

mode	**Description**
active	Operate LACP in active mode. In active mode, it actively sends LACP frames to the other device.
passive	Operate LACP in passive mode. In passive mode, it sends LACP frames only if LACP frames are received from the other device.

[Input mode]

interface mode

[Description]

Associates the applicable interface with the LACP logical interface specified by *link-id*.

If this command is executed with the "no" syntax, the applicable interface is dissociated from the LACP logical interface.

[Note]

This command can be specified only for LAN/SFP+ port.

If a LAN/SFP+ port is associated with a LACP logical interface, **lacp timeout long** command is specified for the corresponding LAN/SFP+ port.

If it is dissociated from the LACP logical interface, the **lacp timeout** command setting of the corresponding LAN/SFP+ port is deleted.

If you associate a LAN/SFP+ port to a *link-id* for which a LACP logical interface does not exist, the LACP logical interface is newly generated.

If the associated LAN/SFP+ port is no longer present because it was removed from the LACP logical interface, the LACP logical interface is deleted.

Up to twenty LAN/SFP+ port units can be associated with one LACP logical interface.

If up to eight associated LAN/SFP+ ports are combined into an LACP logical interface, they are immediately combined into the LACP logical interface; ports in excess of eight are standby ports used in case of a malfunction.

LAN/SFP+ port whose communication mode is half duplex do not support LACP link aggregation. (They can be assigned, but do not function as LACP link aggregation.)

If LAN/SFP+ port with different communication speeds are assigned to the same LACP logical interface, the operation depends on the settings for different-speed link aggregation. See the **lacp multi-speed** command for details.

If a LAN/SFP+ port is to be associated with an already-existing LACP logical interface, all of the following settings must match between the LAN/SFP+ port and the LACP logical interface. If the settings differ, an error occurs.

- Setting of VLAN
- Set QoS trust mode (including default CoS value and port priority)
- Loop detection settings (enable/disable loop detection, enable/disable port blocking)

If a LACP logical interface is newly generated, the above settings of the LAN/SFP+ port are set to the default settings of the LACP logical interface.

If a LAN/SFP+ port is associated with an LACP logical interface, the MSTP settings return to the default values.

The MSTP settings also return to the default values if the LAN/SFP+ port is removed from the LACP logical interface.

It is not possible to associate a single LAN/SFP+ port with multiple logical interface units.

You must use the "no" syntax to first remove it before associating it with a different logical interface.

[Example]

Associate LAN port #1 in ACTIVE mode with LACP logical interface #10.

```
SWP2(config)#interface port1.1
SWP2(config-if)#channel-group 10 mode active
```

5.2.4 Show LACP logical interface status

[Syntax]

show etherchannel [*ifname*]

[Parameter]

ifname	:	Interface name of the LAN/SFP+ port Interfaces that make up the LACP logical interface

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

If *ifname* is omitted, shows the status of the LACP logical interface.

The following items are shown for each LACP logical interface that exists.

- LACP logical interface name
- Load balance function rules
- Interface name of associated LAN/SFP+ port

For details on the load balance function rules, refer to the *type* parameter of the **port-channel load-balance** command.

If *ifname* is specified, shows the status of the LAN/SFP+ port that make up the LACP logical interface.

The following items are shown.

Item	Description
Etherchannel portN.N	LAN/SFP+ port name
Physical admin key	Key that identifies physical characteristics (created from bandwidth, duplex, mru, and VLAN structure)
Receive machine state	Status of the LACP protocol Receive machine transition variable • "Invalid" • "Initialize" • "Port disabled" • "LACP disabled" • "Expired" • "Defaulted" • "Current"
Periodic Transmission machine state	Status of the LACP protocol Periodic Transmission transition variable • "Invalid" • "No periodic" • "Fast periodic" (transmitted at one-second intervals) • "Slow periodic" (transmitted at 30 second intervals) • "Periodic"

Item	Description
Mux machine state	Status of the LACP protocol Receive machine transition variable • "Detached" • "Waiting" • "Attached" • "Collecting/Distributing"
Selection	Usage status • "Selected" • "Unselectedic" • "Standby"
Information	Refer to the table below (Actor is self, Partner is other party)
Aggregator ID	Distinguishing ID on LACP

Information shows the following items.

Item	Description
LAG	LACP system ID (priority, MAC address)
Admin Key	ID that is the basis of the LACP key (logical port number)
Port priority	LACP port priority order
Ifindex	Interface number
Timeout	Timeout value ("Long"=90 seconds, "Short"=3 seconds)
Active	LACP operation mode("Active", "Passive")
Synchronized	Synchronization flag
Collecting	Collecting flag
Distributing	Distributing flag
Defaulted	Defaulted flag
Expired	Expired flag

[Example]

Shows the status of LACP logical interface.

```
SWP2#show etherchannel
% Lacp Aggregator: po10
% Load balancing: src-dst-mac
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
```

Shows the status of the LAN/SFP+ ports that make up the LACP logical interface.

```
SWP2#show etherchannel port1.1
Etherchannel port1.1
 Physical admin key                        3
 Receive machine state                  Current
 Periodic Transmission machine state    Slow periodic
 Mux machine state                      Collecting/Distributing
 Selection                              Selected
 Information    Actor                        Partner
  LAG           0x8000, 00-a0-de-e0-e0-e0    0x8000, 00-a0-de-11-11-11
  Admin Key       0001                         0001
  Port Priority  32768                        32768
  Ifindex         5001                         5001
  Timeout       Long                         Long
  Active             1                            1
  Synchronized       1                            1
  Collecting         1                            1
  Distributing       1                            1
```

```
  Defaulted          0                                 0
  Expired            0                                 0
```

5.2.5 Set LACP system priority order

[Syntax]

lacp system-priority *priority*
no lacp system-priority

[Parameter]

priority : <1-65535>

LACP system priority irder
Lower numbers have higher priority

[Initial value]

lacp system-priority 32768

[Input mode]

global configuration mode

[Description]

Sets the LACP system priority order.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Note]

If an LACP logical interface is connected to the other device, the system priorities are compared, and control privilege is given to the device with the higher priority.

[Example]

Set the LACP system priority order to 100.

```
SWP2(config)#lacp system-priority 100
```

5.2.6 Show LACP system priority

[Syntax]

show lacp sys-id

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the LACP system priority and the LACP system ID.

The following items are shown.

- LACP system priority (hexadecimal number starting with 0x)
- LACP system ID

[Note]

The LACP system priority can be set by the **lacp system-priority** command.

The LACP system ID is generated from the MAC address.

[Example]

Show the LACP system priority.

```
SWP2>show lacp sys-id
% System 0x8000, 00-a0-de-e0-e0-e0
```

5.2.7 LACP different-speed link aggregation settings

[Syntax]

lacp multi-speed *switch*
no lacp multi-speed

[Parameter]

switch : Different-speed link aggregation function enable/disable settings

Setting value	Description
enable	Enabling different-speed link aggregation
disable	Disabling different-speed link aggregation

[Initial value]

lacp multi-speed disable

[Input mode]

global configuration mode

[Description]

Enables or disables different-speed link aggregation in an LACP.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Note]

Operations when different-speed link aggregation is enabled

- All associated ports up to the maximum (eight ports) are set to active, regardless of communication speed.
- Load balancing is handled the same for all associated ports.
- If the opposing device does not accept a different communication speed, a list of associated ports is exchanged between this device and the opposing device, and the ports usable by both devices are enabled.

Operations when different-speed link aggregation is disabled

- Amongst the associated ports, only those with the same communication speed as the port initially linked up are made active.
  - Other ports with different communication speeds are left on standby.
  - When set to auto negotiation, only those ports amongst the associated ports with the same communication speed as that which resulted from the initial auto negotiation are made active.
- When the first group of linked-up ports all link down, the LACP logical interface also links down.

[Example]

This sets different-speed link aggregation to enabled.

```
SWP2(config)#lacp multi-speed enable
```

5.2.8 Set LACP timeout

[Syntax]

lacp timeout *duration*

[Parameter]

duration : Specify the timeout

duration	Description
short	Sets the timeout to 3 seconds
long	Sets the timeout to 90 seconds

[Input mode]

interface mode

[Description]

Sets the LACP timeout.

[Note]

This command can be set only for a LAN/SFP+ port that is associated with an LACP logical interface.

If a LAN/SFP+ port is associated with an LACP logical interface, **lacp timeout long** command is specified for the corresponding LAN/SFP+ port.

If it is dissociated from the LACP logical interface, the **lacp timeout** command setting of the corresponding LAN/SFP+ port is deleted.

LACP timeout indicates the time since the last LACP frame received from the other device, after which it is determined that the link has gone down.

The LACP timeout setting is placed in a LACP frame and sent to the other device; after receiving this, the other device will transmit LACP frames at intervals of 1/3 of this LACP timeout.

The interval at which the device itself transmits LACP frames depends on the LACP timeout value inside the LACP frame sent from the other device.

[Example]

Set the LACP timeout of LAN port #1 to short.

```
SWP2(config)#interface port1.1
SWP2(config-if)#lacp timeout short
```

5.2.9 Clear LACP frame counters

[Syntax]

clear lacp [*link-id*] **counters**

[Parameter]

link-id : <1-127>

LACP logical interface number

[Input mode]

priviledged EXEC mode

[Description]

Clears the LACP frame counters.

If *link-id* is omitted, the frame counter of every existing LACP logical interface is cleared.

[Example]

Clear the frame counter for every LACP logical interface.

```
SWP2#clear lacp counters
```

5.2.10 Show LACP frame counter

[Syntax]

show lacp-counter [*link-id*]

[Parameter]

link-id : <1-127>

LACP logical interface number

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Show the LACP frame counter.

If *link-id* is omitted, the frame counter of every existing LACP logical interface is shown.

The following items are shown for each associated LAN/SFP+ port.

- LACP frames sent and received
- Marker protocol frames sent and received
- Error frames sent and received

[Example]

Show the frame counter for every LACP logical interface.

```
SWP2#show lacp-counter
% Traffic statistics
Port       LACPDUs         Marker         Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po1 , ID 4601
port1.1  297     298     0       0       0       0
port1.2  306     299     0       0       0       0
port1.3  305     298     0       0       0       0
```

```
port1.4  309     1350    0       0       0       0
port1.5  186     186     0       0       0       0
```

5.2.11 Set load balance function rules

[Syntax]

port-channel load-balance *type*
no port-channel load-balance

[Parameter]

type : Rules to specify the forwarding destination interface

type	Description
dst-ip	Destination IPv4/IPv6 address
dst-mac	Destination MAC address
dst-port	Destination TCP/UDP port number
src-dst-ip	Source and destination IPv4/IPv6 address
src-dst-mac	Source and destination MAC address
src-dst-port	Source and destination TCP/UDP port number
src-ip	Source IPv4/IPv6 address
src-mac	Source MAC address
src-port	Source TCP/UDP port number

[Initial value]

port-channel load-balance dst-ip

[Input mode]

global configuration mode

[Description]

Sets rules to specify the forwarding destination interface of the load balance function.

This uses the L2/L3/L4 information in the received frames to determine the forwarding destination.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command is a system-wide setting.

In the case of a frame that is not an IPv4/IPv6 packet, the forwarding destination interface is determined according to the forwarding source and destination MAC addresses, regardless of the rules that were specified.

[Example]

With the load balance function, set the system to determine the forwarding destination interface based on the transmission-source and destination IPv4/IPv6 address.

```
SWP2(config)#port-channel load-balance src-dst-ip
```

5.2.12 Show protocol status of LACP logical interface

[Syntax]

show etherchannel status [*link-id*] [summary | detail]

[Keyword]

summary : Abbreviated display

detail : Detailed display

[Parameter]

link-id : <1-127>

LACP logical interface number

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the status of the LACP logical interface specified by *link-id*.

If *link-id* is omitted, shows the status of all LACP logical interface.

If summary is specified, an abbreviated display is shown; if detail is specified, details are shown.

sIf both summary and detail are omitted, the result is as though summary was specified.

The following items are shown.

Item	Description
Aggregator	LACP logical interface
ID	Distinguishing ID on the LACP logical interface
Actor LAG	The actor's own LACP system ID (priority, MAC address)
Admin Key	The ID that is the basis of the actor's own LACP key (logical port number)
Status	Link aggregation status ("Not ready"/"Ready")
Partner LAG	The partner's LACP system ID (priority, MAC address)
Partner Key	The ID that is the basis of the partner's LACP key
Link count	Number of ports currently conveying data / Number of ports able to convey data
Link	List of the constituent LAN/SFP+ port (see table below for details)

Link shows the following items.

Usage status	Description
"Unselected"	Currently communicating with LACP control protocol.
"Selected"	Selected as a LAN/SFP+ port with LACP enabled.
"Standby"	Specified as a standby LAN/SFP+ port with LACP enabled.

Synchronization flag	Description
"no"	Synchronization flag is not set.
"yes"	Synchronization flag is set.

The state of the linked-up LAN/SFP+ ports are known from the usage status and the Synchronization flag.

Usage status	Synchronization	State of the linked-up LAN/SFP+ port
Unselected	no	Currently communicating with LACP control protocol.
Selected	no	Selected as a LAN/SFP+ port with LACP enabled. Currently negotiating to combine for link aggregation.
Standby	no	Selected as a LAN/SFP+ port with LACP enabled, and specified as a standby port.
Selected	yes	Selected as a LAN/SFP+ port with LACP enabled. Combined as link aggregation,

[Example]

Show the status of the LACP logical interface.

```
SWP2#show etherchannel status summary
```

```
Aggregator po1
 ID          4601
 Status       Ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    1/  1
Aggregator po2
 ID          4602
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
Aggregator po127
 ID          4727
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1


SWP2#show etherchannel status detail
Aggregator po1
 ID          4601
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0001
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    1/  1
 Link
  port1.1     Selected     Synchronized  yes
Aggregator po2
 ID          4602
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0002
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
 Link
  port1.2     Selected     Synchronized  no
  port1.3     Unselected   Synchronized  no
Aggregator po127
 ID          4727
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0127
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
 Link
  port1.4     Selected     Synchronized  no
```

5.2.13 Set LACP port priority order

[Syntax]

lacp port-priority *priority*
no lacp port-priority

[Parameter]

priority : <1-65535>

LACP port priority order
Lower numbers have higher priority

[Initial value]

lacp port-priority 32768

[Input mode]

interface mode

[Description]

Sets the LACP port priority order.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Note]

If up to eight LAN/SFP+ ports are combined into an LACP logical interface, they are immediately combined into the LACP logical interface; ports in excess of eight are standby ports used in case of a malfunction.

In such cases, the priority order between the LAN/SFP+ ports are evaluated, and they are combined starting with the highestpriority port.

The priority order is evaluated as follows.

1) Priority is given to ports with a lower LACP port priority.

2) If the LACP port priority is the same, priority is given to the lower interface number.

If an SFP+ port is to be given priority, its LACP port priority must be set lower than other ports.

[Example]

Set the LACP port priority order to 1024.

```
SWP2(config-if)#channel-group 1 mode active
SWP2(config-if)#lacp port-priority 1024
```

5.3 Port authentication

5.3.1 Configuring the IEEE 802.1X authentication function for the entire system

[Syntax]

aaa authentication dot1x
no aaa authentication dot1x

[Initial value]

no aaa authentication dot1x

[Input mode]

global configuration mode

[Description]

Enables IEEE 802.1X authentication for the entire system.

If this command is executed with the "no" syntax, disables IEEE 802.1X authentication for the entire system.

Use a RADIUS server for authentication on which the **radius-server host** command has been configured.

[Note]

In order to actually use IEEE 802.1X authentication, you need to enable IEEE 802.1X authentication on the applicable interface as well.(**dot1x port-control** command)

[Example]

Enable IEEE 802.1X authentication for the entire system.

```
SWP2(config)#aaa authentication dot1x
```

5.3.2 Configuring the MAC authentication function for the entire system

[Syntax]

aaa authentication auth-mac
no aaa authentication auth-mac

[Initial value]

no aaa authentication auth-mac

[Input mode]

global configuration mode

[Description]

Enables MAC authentication for the entire system.

If this command is executed with the "no" syntax, disables MAC authentication for the entire system.

Use a RADIUS server for authentication on which the **radius-server host** command has been configured.

[Note]

In order to actually use MAC authentication, you need to enable MAC authentication on the applicable interface as well. (**auth-mac enable** command)

[Example]

Enable MAC authentication for the entire system.

```
SWP2(config)#aaa authentication auth-mac
```

5.3.3 Configuring the Web authentication function for the entire system

[Syntax]

aaa authentication auth-web
no aaa authentication auth-web

[Initial value]

no aaa authentication auth-web

[Input mode]

global configuration mode

[Description]

Enables Web authentication for the entire system.

If this command is executed with the "no" syntax, Disables Web authentication for the entire system.

Use a RADIUS server for authentication on which the **radius-server host** command has been configured.

[Note]

In order to actually use Web authentication, you need to enable Web authentication on the applicable interface as well. (**auth-web enable** command)

[Example]

Enable Web authentication for the entire system.

```
SWP2(config)#aaa authentication auth-web
```

5.3.4 Set operation mode for the IEEE 802.1X authentication function

[Syntax]

dot1x port-control *mode*
no dot1x port-control

[Parameter]

mode : Operation mode for IEEE 802.1X authentication

Operation mode	Description
auto	Operates as an authenticator for IEEE 802.1X authentication
force-authorized	Sets the authenticated port for IEEE 802.1X authentication to a fixed port
force-unauthorized	Sets the unauthenticated port for IEEE 802.1X authentication to a fixed port

[Initial value]

no dot1x port-control

[Input mode]

interface mode

[Description]

Configures the IEEE 802.1X authentication operation mode for the applicable interface.

If this command is executed with the "no" syntax, the IEEE 802.1X authentication function will be disabled for the applicable interface.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

[Example]

This command can be specified only for LAN/SFP+ port.

```
SWP2(config)#interface port1.1
SWP2(config-if)#dot1x port-control auto
```

5.3.5 Set for forwarding control on an unauthenticated port for IEEE 802.1X authentication

[Syntax]

dot1x control-direction *direction*
no dot1x control-direction

[Parameter]

direction : Sets the packet forwarding operation for unauthenticated ports

Forwarding operation	Description
both	Both send and receive packets are discarded.
in	Only receive packets are discarded.

[Initial value]

dot1x control-direction both

[Input mode]

interface mode

[Description]

Changes the packet forwarding operation for the applicable interface when the IEEE 802.1X authentication is unauthenticated.

If this command is executed with the "no" syntax, the setting returns to the default.

When "both" is specified, the packets received from the supplicant are discarded, and the broadcast/multicast packets to the interface to which the supplicant is connected from other ports are also discarded.

When "in" is specified, only packets received from the supplicant are discarded, and the broadcast/multicast packets to the interface to which the supplicant is connected from other ports are forwarded.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

If the host mode is set as multi-supplicant mode for the corresponding interface, or if it is used in conjunction with MAC authentication, the "in" setting is automatic.

When the guest VLAN is configured using the applicable interface, the settings for this command will be disabled.

Changing the settings for this command will make the authentication state return to the default.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command)

[Example]

Discard received packets only for the packet forwarding operation on an unauthenticated port of LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#dot1x control-direction in
```

5.3.6 Set the EAPOL packet transmission count

[Syntax]

dot1x max-auth-req *count*
no dot1x max-auth-req

[Parameter]

count : <1-10>

Maximum number of times EAPOL packets are transmitted

[Initial value]

dot1x max-auth-req 2

[Input mode]

interface mode

[Description]

Sets the maximum value for the EAPOL packet transmission count for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command)

[Example]

Set the EAPOL packet transmission count for LAN port #1 to "3".

```
SWP2(config)#interface port1.1
SWP2(config-if)#dot1x max-auth-req 3
```

5.3.7 Set the MAC authentication function

[Syntax]

auth-mac enable
auth-mac disable
no auth-mac

[Keyword]

enable	:	Enable MAC authentication
disable	:	Disable MAC authentication

[Initial value]

auth-mac disable

[Input mode]

interface mode

[Description]

Enables MAC authentication for the applicable interface.

When this command is executed with the "no" syntax or when disable is specified, MAC authentication is disabled.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

In order to actually use MAC authentication, you need to enable MAC authentication for the entire system as well. (**aaa authentication auth-mac** command)

[Example]

Enable the LAN port #1 MAC authentication function.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth-mac enable
```

5.3.8 Set MAC address format during MAC authentication

[Syntax]

auth-mac auth-user *type case*
no auth-mac auth-user

[Parameter]

type	:	Specify the format

Setting value	Format
hyphen	xx-xx-xx-xx-xx-xx
colon	xx:xx:xx:xx:xx:xx
unformatted	xxxxxxxxxxxx

case : Specify upper or lowercase

Setting value	Description
lower-case	Lower case(a～f)
upper-case	Upper case(A～F)

[Initial value]

auth-mac auth-user hyphen lower-case

[Input mode]

global configuration mode

[Description]

Changes the format of the user name and password used for authentication during MAC authentication.

During MAC authentication, the MAC address of the supplicant is used as a user name and password, and a request is sent to the RADIUS server for authentication.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To use this command, you must enable the MAC authentication function for the applicable interface. (**auth-mac enable** command)

[Example]

Change the MAC address format used for MAC authentication to all uppercase format without hyphens.

```
SWP2(config)#auth-mac auth-user unformatted upper-case
```

5.3.9 Configuring static registration for MAC authentication

[Syntax]

auth-mac static enable
auth-mac static disable
no auth-mac static

[Keyword]

enable : Enable static registration

disable : Disable static registration

[Initial value]

auth-mac static disable

[Input mode]

interface mode

[Description]

The MAC authentication feature registers the MAC address of a supplicant that has passed authentication as a static entry in the FDB.

Static registration is disabled when executed with the "no" syntax or when specified as disable.

[Note]

This command can only be set for LAN/SFP+ port and logical interface.

When the configuration of this command is changed, the authentication state returns to default.

Normally, MAC authentication is subject to aging timeout because it is registered as a dynamic entry in the FDB, but when this command is enabled, it is not subject to aging timeout because it is registered as a static entry.

Static registrations (authentication information) can be cleared with the **clear auth state** command or the **auth clear-state time** command.

To use this command, the MAC authentication function must be enabled on the target interface. (**auth-mac enable** command)

[Example]

Enable static registration of MAC authentication for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth-mac static enable
```

5.3.10 Set the Web authentication function

[Syntax]

auth-web enable
auth-web disable
no auth-web

[Keyword]

enable	:	Enable Web authentication
disable	:	Disable Web authentication

[Initial value]

auth-web disable

[Input mode]

interface mode

[Description]

Enables Web authentication for the applicable interface.

When this command is executed with the "no" syntax or when disable is specified, Web authentication is disabled.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

In order to actually use Web authentication, you need to enable Web authentication for the entire system as well. (**aaa authentication auth-web** command)

You cannot enable the Web authentication function from any other mode besides multi-supplicant mode.

You cannot use this together with guest VLAN.

[Example]

Enable the LAN port #1 Web authentication function.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth-web enable
```

5.3.11 Set host mode

[Syntax]

auth host-mode *mode*
no auth host-mode

[Parameter]

mode	:	Operating mode for port authentication

Operation mode	Description
single-host	This mode allows communications for only one supplicant per port. Only the first supplicant that passes authentication is allowed.
multi-host	This mode allows communication with multiple supplicants for each port. If the first supplicant passes authentication, all other supplicants of the same port will be allowed to communicate without authentication.
multi-supplicant	This mode allows communication with multiple supplicants for each port. Communication is allowed or denied on a per-supplicant basis.

[Initial value]

auth host-mode single-host

[Input mode]

interface mode

[Description]

Changes the port authentication operation mode for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

Changing the settings for this command will make the authentication state return to the default.

When using dynamic VLAN in multi-supplicant mode, the VLAN can be specified for individual supplicants.

When using dynamic VLAN in multi-host, the VLAN ID applied by the first supplicant will be applied to supplicants from the second onwards.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Change the LAN port #1 to multi supplicant mode.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth host-mode multi-supplicant
```

5.3.12 Configuring the authentication order

[Syntax]

auth order dot1x auth-mac
auth order auth-mac dot1x
no auth order

[Keyword]

dot1x	:	IEEE 802.1x authentication method
auth-mac	:	MAC authentication method

[Initial value]

auth order dot1x auth-mac

[Input mode]

interface mode

[Description]

Sets the order in which authentication occurs when authentication methods are used together in the port authentication function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can only be set for LAN/SFP+ port and logical interface.

Regardless of this setting, Web authentication is performed when an ID/Password is entered on the Web authentication screen.

If the IEEE 802.1X authentication, MAC authentication, or Web authentication setting is disabled, that authentication method is not performed.

To use this command, the port authentication function must be enabled on the target interface. (**dot1x port-control** command,**auth-mac enable** command, **auth-web enable** command)

[Example]

Set the authentication method order for LAN port #1 as MAC authentication -> IEEE 802.1X authentication.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth order auth-mac dot1x
```

5.3.13 Set re-authentication

[Syntax]

auth reauthentication
no auth reauthentication

[Initial value]

no auth reauthentication

[Input mode]

interface mode

[Description]

Enables reauthentication of supplicants for the applicable interface.

If this is executed with the "no" syntax, the re-authentication is disabled.

When this setting is enabled, this periodically reauthenticates supplicants that have been successfully authenticated.

The reauthentication interval can be changed using the **auth timeout reauth-period** command.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

During IEEE 802.1X authentication, an EAPOL packet is transmitted to the supplicant at the timing for reauthentication to once again retrieve the user information, and an authentication request is sent to the RADIUS server.

During MAC authentication, the supplicant's MAC address is regarded as a user name and password at the timing for reauthentication, and a request is sent to the RADIUS server for authentication.

During Web authentication, the supplicant's authentication state is shifted to unauthorized at the timing of reauthentication.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Enable re-authenticatio of LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth reauthentication
```

5.3.14 Set dynamic VLAN

[Syntax]

auth dynamic-vlan-creation
no auth dynamic-vlan-creation

[Initial value]

no auth dynamic-vlan-creation

[Input mode]

interface mode

[Description]

Sets dynamic VLAN for the applicable interface.

If this is executed with the "no" syntax, the dynamic VLAN is disabled.

For interfaces on which dynamic VLAN is enabled, the associated VLAN is actively changed based on the property (Tunnel-Private-Group-ID) specified by the RADIUS server.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

Changing the settings for this command will make the authentication state return to the default.

When using dynamic VLAN in multi-supplicant mode, the VLAN can be specified for individual supplicants.

When using dynamic VLAN in multi-host, the VLAN ID applied by the first supplicant will be applied to supplicants from the second onwards.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Enable dynamic VLAN on LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth dynamic-vlan-creation
```

5.3.15 Set the guest VLAN

[Syntax]

auth guest-vlan *vlan-id*
no auth guest-vlan

[Parameter]

vlan-id	:	<1-4094>
		VLAN ID for guest VLAN

[Initial value]

no auth guest-vlan

[Input mode]

interface mode

[Description]

If the supplicant connected to the applicable interface is unauthorized or if authorization has failed, this specifies the guest VLAN to which the supplicant is associated.

If this command is executed with the "no" syntax, the guest VLAN setting is deleted.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

Changing the settings for this command will make the authentication state return to the default.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command)

This command cannot be set when Web authentication is enabled.

[Example]

This specifies guest VLAN #10 for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth guest-vlan 10
```

5.3.16 Suppression period settings following failed authentication

[Syntax]

auth timeout quiet-period *time*
no auth timeout quiet-period

[Parameter]

time	:	<1-65535>
		Period during which communication with a supplicant is refused after authentication fails (seconds)

[Initial value]

auth timeout quiet-period 60

[Input mode]

interface mode

[Description]

Sets the period during which authentication is suppressed for the applicable interface after authentication fails.

If this command is executed with the "no" syntax, the setting returns to the default.

All packets received during the authentication suppression period will be discarded.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Set the suppression period for LAN port #1 to 300.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout quiet-period 300
```

5.3.17 Set reauthentication interval

[Syntax]

auth timeout reauth-period *time*
no auth timeout reauth-period

[Parameter]

time : <300-86400>

Supplication reauthentication interval (seconds)

[Initial value]

auth timeout reauth-period 3600

[Input mode]

interface mode

[Description]

Sets the reauthentication interval of the supplicant for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

To use this command, you must enable the port authorization function and the reauthentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command, **auth reauthentication** command)

[Example]

Set the reauthentication period for LAN port #1 to 1200.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout reauth-period 1200
```

5.3.18 Set the reply wait time for the RADIUS server overall

[Syntax]

auth timeout server-timeout *time*
no auth timeout server-timeout

[Parameter]

time : <1-65535>

Reply wait time from the authentication server for the authentication request (seconds)

[Initial value]

auth timeout server-timeout 30

[Input mode]

interface mode

[Description]

Sets the reply wait time for the RADIUS server overall when authenticating a port of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

The value for this setting must be at least equal to (setting of **radius-server timeout** command) x (setting of **radius-server retransmit** command + 1) x (number of radius servers).

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

This sets the reply wait time to the RADIUS server overall to 180 seconds, for authentication requests from LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout server-timeout 180
```

5.3.19 Set supplicant reply wait time

[Syntax]

auth timeout supp-timeout *time*
no auth timeout supp-timeout

[Parameter]

time : <1-65535>
Supplicant reply wait time (seconds)

[Initial value]

auth timeout supp-timeout 30

[Input mode]

interface mode

[Description]

Sets the reply wait time from the supplicant during port authentication for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Set the reply wait time from the supplicant of LAN port #1 to 180 seconds.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout supp-timeout 180
```

5.3.20 Set RADIUS server host

[Syntax]

radius-server host *host* [auth-port *port*] [timeout *time*] [retransmit *count*] [key *secret*]
no radius-server host

[Keyword]

auth-port : Sets the UDP port number used for authenticating the RADIUS server

timeout	:	Sets the reply standby time for requests sent to the RADIUS server
retransmit	:	Sets the number of times to resend the request to the RADIUS server
key	:	Sets the password used for communicating with the RADIUS server

[Parameter]

host	:	IPv4 address (A.B.C.D) or IPv6 address (X:X::X:X) When specifying an IPv6 link local address, the transmitting interface also needs to be specified (fe80::X%vlanN format).
port	:	<0-65535> UDP port number used for authentication (the default value of 1812 is used when this is omitted)
time	:	<1-1000> Reply standby time (in seconds; the settings for the radius-server timeout command--5 sec. at default are used if this is omitted)
count	:	<0-100> Number of times to resend (the settings for the radius-server retransmit command--3 times. at default are used if this is omitted)
secret	:	Single-byte alphanumeric characters, and single-byte symbols other than the characters '?' and spaces (128 characters or less) Shared password (the settings for the radius-server key command are used if this is omitted)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a server to the authentication server list.

The maximum number of entries is 8.

If this command is executed with the "no" syntax, this deletes the specified server from the authentication server list.

[Note]

The setting values should be adjusted so that the value of (setting value of **radius-server timeout** command) x (setting value of **radius-server retransmit** command + 1) x (number of RADIUS servers) is within the setting value of the **auth timeout server-timeout** command.

The **radius-server host** command configured with the LLDP auto-configuration feature is suffixed with the "dynamic" option that indicates it is a temporary setting. When the "dynamic" option is added, it will not be saved to the startup configuration even if the **write** command is executed.

[Example]

Add the server at IP address 192.168.100.100, with a reply standby time of 10 seconds and a number of times to resend requests of 5 seconds to the authentication server list.

```
SWP2(config)#radius-server host 192.168.100.100 timeout 10 retransmit 5
```

Add the server at IP address 192.168.100.101, with an authentication UDP port of 1645 and a shared password of "abcde" to the authentication server list.

```
SWP2(config)#radius-server host 192.168.100.101 auth-port 1645 key abcde
```

Adds the local RADIUS server to the authentication server list.

```
SWP2(config)#radius-server host 127.0.0.1 key secret_local
```

5.3.21 Set the reply wait time for each RADIUS server

[Syntax]

radius-server timeout *time*
no radius-server timeout

[Parameter]

time : <1-1000>

Standby time for replying to requests (seconds)

[Initial value]

radius-server timeout 5

[Input mode]

global configuration mode

[Description]

Sets the reply wait time for each RADIUS server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a server-specific wait time for replying to requests has been set using the **radius-server host** command, the **radius-server host** command settings are used.

The setting needs to be adjusted so that the value of (Setting of **radius-server timeout** command) x (Setting of **radius-server retransmit** command + 1) x (Number of RADIUS servers) falls within the number set in the auth timeout server-timeout command.

[Example]

Set the reply wait time for each RADIUS server to 10 seconds.

```
SWP2(config)#radius-server timeout 10
```

5.3.22 Set number of times to resend requests to RADIUS server

[Syntax]

radius-server retransmit *count*
no radius-server retransmit

[Parameter]

count : <0-100>

Number of times to resend request

[Initial value]

radius-server retransmit 3

[Input mode]

global configuration mode

[Description]

Sets the number of times to resend requests to a RADIUS server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a server-specific number of resends for requests has been set using the **radius-server host** command, the **radius-server host** command settings are used.

[Example]

Set the number of times to resend requests to a RADIUS server to 5.

```
SWP2(config)#radius-server retransmit 5
```

5.3.23 Set RADIUS server shared password

[Syntax]

radius-server key *secret*
no radius-server key

[Parameter]

secret	:	Shared password Single-byte alphanumeric characters, and single-byte symbols other than the characters '?' and spaces (128 characters or less)

[Initial value]

no radius-server key

[Input mode]

global configuration mode

[Description]

Sets the shared password used when communicating with a RADIUS server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a server-specific shared password has been set using the **radius-server host** command, the **radius-server host** command settings are used.

[Example]

The shared password used with the RADIUS server is "abcde".

```
SWP2(config)#radius-server key abcde
```

5.3.24 Set time of RADIUS server usage prevention

[Syntax]

radius-server deadtime *time*
no radius-server deadtime

[Parameter]

time	:	<0-1440> RADIUS server usage prevention time (minutes)

[Initial value]

radius-server deadtime 0

[Input mode]

global configuration mode

[Description]

Sets the time during which the usage of the relevant server is prevented, when a request to the RADIUS server has timed out.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This sets the usage prevention for the RADIUS server to 1 minute.

```
SWP2(config)#radius-server deadtime 1
```

5.3.25 Set NAS-Identifier attribute sent to RADIUS server

[Syntax]

auth radius attribute nas-identifier *line*
no auth radius attribute nas-identifier

[Parameter]

line	:	Identifying text (253 characters or fewer) The desired text string to be set as the NAS-Identifier attribute

[Initial value]

no auth radius attribute nas-identifier

[Input mode]

global configuration mode

[Description]

Specifies a desired text string that is sent as the NAS-Identifier attribute to the RADIUS server for port authentication.

If this setting is made, it is notified to RADIUS server as the NAS-Identifier attribute. If this setting is deleted, notification is stopped.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set "Nas-ID-001" as the NAS-Identifier attribute that is sent to the RADIUS server.

```
SWP2(config)#auth radius attribute nas-identifier Nas-ID-001
```

5.3.26 Show port authentication information

[Syntax]

show auth status [interface *ifname*]

[Keyword]

interface	:	Show information for only a specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the setting status for port authentication as well as the current authentication state.

[Example]

Show the port authentication information.

```
SWP2#show auth status
[System information]
  802.1X Port-Based Authentication : Enabled
  MAC-Based Authentication         : Disabled
  WEB-Based Authentication         : Enabled

  Clear-state time : Not configured

  Redirect URL :
    Not configured

  Auth-web custom-file :
    There is no custom-file

  RADIUS server address :
    192.168.100.101 (port:1812)

[Interface information]
  Interface port1.1 (up)
    802.1X Authentication   : Auto (configured:auto)
    MAC Authentication      : Disabled (configured:disable)
    WEB Authentication      : Disabled (configured:disable)
    Host mode               : Single-host
    Dynamic VLAN creation   : Disabled
    Guest VLAN              : Disabled
    Reauthentication        : Disabled
    Reauthentication period : 60 sec
    MAX request             : 2 times
    Supplicant timeout      : 30 sec
    Quiet period            : 60 sec
    Controlled directions   : Both (configured:both)
    Protocol version        : 2
    Authentication status   : Authorized
    Clear-state time        : Not configured
```

```
Interface port1.4 (down)
  802.1X Authentication   : Force Authorized (configured:-)
  MAC Authentication      : Disabled (configured:disable)
  WEB Authentication      : Enabled (configured:enable)
  Host mode               : Multi-supplicant
  Dynamic VLAN creation   : Disabled
  Guest VLAN              : Disabled
  Reauthentication        : Disabled
  Reauthentication period : 3600 sec
  MAX request             : 2 times
  Supplicant timeout      : 30 sec
  Server timeout          : 30 sec
  Quiet period            : 60 sec
  Controlled directions   : In (configured:both)
  Protocol version        : 2
  Clear-state time        : Not configured
```

5.3.27 Show supplicant information

[Syntax]

show auth supplicant [interface *ifname*]

[Keyword]

interface	:	Show information for only a specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

priviledged EXEC mode

[Description]

Shows the supplicant information for port authentication.

[Example]

Show supplicant information for LAN port #1.

```
SWP2#show auth supplicant interface port1.1
Port     MAC address       User name         Status          VLAN Method
-------- ----------------- ----------------- --------------- ---- ------
port1.1  0011.2233.4455    user              Authorized         1 802.1X
```

5.3.28 Show statistical information

[Syntax]

show auth statistics [interface *ifname*]

[Keyword]

interface	:	Shows statistical information for only the specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows statistical information for packets during port authentication.

[Example]

Show statistical information for LAN port #1.

```
SWP2#show auth statistics interface port1.1
Interface port1.1
  EAPOL frames:
    Received frames      : 11
      EAPOL Start        : 1
      EAPOL Logoff       : 0
      EAP Response ID    : 1
      EAP Response       : 9
      Invalid EAPOL      : 0
      EAP Length error   : 0
      Last EAPOL version : 1
      Last EAPOL source  : 0011.2233.4455
    Transmitted frames   : 11
      EAP Request ID     : 1
      EAP Request        : 9
      EAP Success        : 1
      EAP Fail           : 0

  RADIUS packets:
    Received packets     : 10
      Access Request     : 0
      Access Challenge   : 9
      Access Accept      : 1
      Access Reject      : 0
    Transmitted packets  : 10
      Access Request     : 10
```

5.3.29 Clear statistical information

[Syntax]

clear auth statistics [interface *ifname*]

[Keyword]

interface	:	Clears statistical information for only the specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

priviledged EXEC mode

[Description]

Clears the packet statistical information during port authentication.

[Example]

Clear the statistical information for LAN port #1.

```
SWP2#clear auth statistics interface port1.1
```

5.3.30 Show RADIUS server setting information

[Syntax]

show radius-server

[Input mode]

priviledged EXEC mode

[Description]

Shows setting information related to the RADIUS server.

Shows setting information (server host, UDP port number for authentication, shared password, wait time for replying to requests, number of times to resend requests, server usage prevention time) for RADIUS servers registered in the authentication server list.

[Example]

Show setting information related to the RADIUS server.

```
SWP2#show radius-server
Server Host : 192.168.100.101
```

```
  Authentication Port : 1812
  Secret Key          : abcde
  Timeout             : 10 sec
  Retransmit Count    : 5
  Deadtime            : 0 min

Server Host : 192.168.100.102
  Authentication Port : 1645
  Secret Key          : fghij
  Timeout             : 5 sec
  Retransmit Count    : 3
  Deadtime            : 0 min
```

5.3.31 Settings for redirect destination URL following successful Web authentication

[Syntax]

auth-web redirect-url *url*
no auth-web redirect-url

[Parameter]

url	:	Single-byte alphanumeric characters and single-byte symbols (maximum 255 characters) Redirect destination URL

[Initial value]

no auth-web redirect-url

[Input mode]

global configuration mode

[Description]

Specifies the URL to redirect to after successful Web authentication.

If this is executed with the "no" syntax, disables the redirect function after authentication.

[Note]

URLs that include question marks ("?") cannot be specified.

[Example]

Specify the redirect destination after successful Web authentication as http://192.168.100.200.

```
SWP2(config)#auth-web redirect-url http://192.168.100.200
```

5.3.32 Clear the authentication state

[Syntax]

clear auth state [all] [interface *ifname*] [supplicant *mac-addr*]

[Keyword]

all	:	Clears the authentication state for all supplicants
interface	:	Clears the authentication state for supplicants connected to specific interfaces
supplicant	:	Clear the authentication state for specific supplicant

[Parameter]

ifname	:	Interfacee name Interface to clear
mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal) Applicable MAC address

[Input mode]

priviledged EXEC mode

[Description]

Clears the supplicant authentication state.

[Example]

Clear the authentication state for supplicants connected to LAN port #1.

```
SWP2#clear auth state interface port1.1
```

5.3.33 Setting the time for clearing the authentication state (system)

[Syntax]

auth clear-state time *time*
no auth clear-state time

[Parameter]

time : <0-23>
Time at which the authentication state is cleared

[Initial value]

no auth clear-state time

[Input mode]

global configuration mode

[Description]

Sets the time at which the authentication state for the supplicant is cleared for the entire system.

If this command is executed with the "no" syntax, deletes the time setting for clearing the authentication state.

[Note]

If a time has been set to clear the interface authentication state, this will clear the authentication state at the time specified in the interface.

[Example]

This sets the time at which the authentication state for the supplicant is cleared for the entire system to 12:00.

```
SWP2(config)#auth clear-state time 12
```

5.3.34 Setting the time for clearing the authentication state (interface)

[Syntax]

auth clear-state time *time*
no auth clear-state time

[Parameter]

time : <0-23>
Time at which the authentication state is cleared

[Initial value]

no auth clear-state time

[Input mode]

interface mode

[Description]

Sets the time at which the authentication state of the supplicant is cleared for the applicable interface.

If this command is executed with the "no" syntax, deletes the time setting for clearing the authentication state.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

Even if a time has been set to clear the interface authentication state for the applicable interface system-wide, the authentication state will be cleared at the time specified by this command.

[Example]

This sets the time at which the authentication state of the supplicant connected to LAN port #1 is cleared to 12:00.

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth clear-state time 12
```

5.3.35 Set EAP pass through

[Syntax]

pass-through eap *switch*
no pass-through eap

[Parameter]

switch : Behavior EAP pass through

Setting value	Description
enable	Enable the EAP pass through
disable	Disable the EAP pass through

[Initial value]

pass-through eap enable

[Input mode]

global configuration mode

[Description]

Enables/disables EAP pass-through, specifying whether EAPOL frames are forwarded.

If "disable" is specified, EAP frames are discarded.

If this is executed with the "no" syntax, or if "enable" is specified, EAPOL frames are forwarded.

[Note]

For interfaces on which 802.1X authentication is enabled, authentication functionality is given priority, and EAP pass-through settings are not applied.

[Example]

Disable the EAP pass through.

```
SWP2(config)#pass-through eap disable
```

5.4 Port security

5.4.1 Set port security function

[Syntax]

port-security enable
port-security disable
no port-security

[Keyword]

enable : Enables port security function

disable : Disables port security function

[Initial value]

port-security disable

[Input mode]

interface mode

[Description]

Enables the port security function for the applicable interface.

If this is executed with the "no" syntax, or disable is specified, port security will be disabled for the applicable interface.

[Note]

This command can be specified only for both LAN/SFP+ port and logical interface.

Any unregistered terminals will be discarded at the time when the port security function is enabled.

[Example]

Enable port security for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#port-security enable
```

5.4.2 Register permitted MAC addresses

[Syntax]

port-security mac-address
no port-security mac-address

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Registers MAC addresses that are allowed to communicate on ports for which port security has been enabled.

If this command is executed with the "no" syntax, deletes the registered address.

[Example]

Register MAC address 00:A0:DE:00:00:01 as a permitted address for LAN port #1.

```
SWP2(config)#port-security mac-address 00a0.de00.0001 forward port1.1 vlan 1
```

5.4.3 Set operations used for security violations

[Syntax]

port-security violation *action*
no port-security violation

[Parameter]

action : Operation used for port security violations

Operation mode	Description
discard	Discards packets
shutdown	Shuts down the port

[Initial value]

port-security violation discard

[Input mode]

interface mode

[Description]

Sets the action to be taken during a port security violation for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When restoring ports in shutdown mode that have been shut down, use the no shutdown command.

This command can be specified only for both LAN/SFP+ port and logical interface.

[Example]

Change the operation used for a violation on LAN port #1 to "port shutdown."

```
SWP2(config)#interface port1.1
SWP2(config-if)#port-security violation shutdown
```

5.4.4 Show port security information

[Syntax]

show port-security status

[Input mode]

priviledged EXEC mode

[Description]

Shows the port security information.

[Example]

Show the port security information.

```
SWP2#show port-security status
 Port     Security  Action    Status    Last violation
 -------- --------- --------- --------- -----------------
 port1.1  Enabled   Discard   Blocking  00a0.de00.0003
 port1.2  Disabled  Discard   Normal
 port1.3  Disabled  Discard   Normal
 port1.4  Disabled  Discard   Normal
 port1.5  Disabled  Discard   Normal
 port1.6  Disabled  Discard   Normal
 port1.7  Disabled  Discard   Normal
 port1.8  Disabled  Discard   Normal
 port1.9  Disabled  Discard   Normal
 port1.10 Disabled  Discard   Normal
```

5.5 Error detection function

5.5.1 Set automatic recovery from errdisable state

[Syntax]

errdisable auto-recovery *function* [interval *interval*]
no errdisable auto-recovery *function*

[Keyword]

interval : Automatic recovery time setting

[Parameter]

function : Functions that can be the cause of errdisable

Setting value	Description
bpduguard	BPDU guard function
loop-detect	Loop detection function

interval : <10-1000000>

Time (seconds) until auto-recovery

[Initial value]

no errdisable auto-recovery bpduguard (BPDU guard function)

errdisable auto-recovery loop-detect interval 300 (Loop detection function)

[Input mode]

global configuration mode

[Description]

Enables the function that automatically recovers after the error detection function causes the errdisable state, and specifies the time until automatic recovery.

If interval is omitted, 300 seconds is specified.

this is executed with the "no" syntax, the automatic recovery function is disabled.

[Note]

For a LAN/SFP+ port that was put in the errdisable state by the BPDU guard function before this command was executed, the change in the setting is applied the next time BPDU is detected.

[Example]

Enable automatic recovery after BPDU guard has caused the errdisable state, and set the recovery time to 600 seconds.

```
SWP2(config)#errdisable auto-recovery bpduguard interval 600
```

Disable automatic recovery after loop detection has caused the errdisable state.

```
SWP2(config)#no errdisable auto-recovery loop-detect
```

5.5.2 Show error detection function information

[Syntax]

show errdisable

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows information for the error detection function.

The following items are shown.

- Whether automatic recovery from the errdisable state is enabled or disabled
- The interface that is in the errdisable state, and the function that detected the error

[Example]

Show information for the error detection function.

```
SWP2>show errdisable

function        auto recovery          interval
-----------------------------------------------
BPDU guard      disable
Loop detect     enable                      300
Port-security   disable

port            reason
----------------------------
port1.1         BPDU guard
port1.7         Loop detect
sa1             Loop detect
```

Chapter 6

Layer 2 functions

6.1 FDB (Forwarding Data Base)

6.1.1 Set MAC address acquisition function

[Syntax]

mac-address-table learning enable
mac-address-table learning disable
no mac-address-table learning

[Keyword]

enable	:	Enables MAC address learning function
disable	:	Disables MAC address learning function

[Initial value]

mac-address-table learning enable

[Input mode]

global configuration mode

[Description]

Enables/disables the MAC address learning function.

If this is executed with the "no"syntax, the MAC address acquisition function is enabled.

[Note]

If the MAC address acquisition function is disabled, a dynamic entry is not registered in the MAC address table even if a frame is received.

[Example]

Enable the MAC address acquisition function.

```
SWP2(config)#mac-address-table learning enable
```

6.1.2 Set dynamic entry ageing time

[Syntax]

mac-address-table ageing-time *time*
no mac-address-table ageing-time

[Parameter]

time	:	<10-400> Ageing time (seconds)

[Initial value]

mac-address-table ageing-time 300

[Input mode]

global configuration mode

[Description]

Sets the dynamic entry ageing time.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In some cases, there might be a discrepancy between the time specified by this command and the time until the dynamic entry is actually deleted from the MAC address table.

[Example]

Set the dynamic entry ageing time to 400 seconds.

```
SWP2(config)#mac-address-table ageing-time 400
```

6.1.3 Clear dynamic entry

[Syntax]

clear mac-address-table dynamic
clear mac-address-table dynamic address *mac-addr*
clear mac-address-table dynamic vlan *vlan-id*
clear mac-address-table dynamic interface *ifname* [instance *inst*]

[Keyword]

address	:	Specifies the MAC address
vlan	:	Specifies the VLAN ID
interface	:	Specifies the interface
instance	:	Specifies the MST instance

[Parameter]

mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal)
		Applicable MAC address
ifname	:	Name of LAN/SFP+ port or logical interface
		Applicable interface
vlan-id	:	<1-4094>
		Applicable VLAN ID
inst	:	<1-63>
		Applicable MST instance ID

[Input mode]

priviledged EXEC mode

[Description]

Deletes a dynamic entry from the MAC address table.

If a keyword is specified, only the entries that match the applicable conditions are deleted.

If no keyword is specified, all dynamic entries are deleted.

[Example]

Delete the dynamic entry whose MAC address is 00a0.de11.2233.

```
SWP2#clear mac-address-table dynamic address 00a0.de11.2233
```

6.1.4 Set static entry

[Syntax]

mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]
no mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]

[Keyword]

vlan	:	Specifies the VLAN ID

[Parameter]

mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal)
		Applicable MAC address
action	:	Action applied to frames addressed to mac-addr

Setting value	Description
forward	Forward
discard	Discard

ifname : Name of LAN/SFP+ port or logical interface

Applicable interface

vlan-id : <1-4094>

Applicable VLAN ID

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Registers a static entry in the MAC address table.

If

action is specified as "forward," received frames that match the specified MAC address and VLAN ID are forwarded to the specified interface.
If *action* is specified as "discard," received frames that match the specified MAC address and VLAN ID are discarded.

If this command is executed with the "no" syntax, the static entry is deleted from the MAC address table.

If "vlan" is omitted, VLAN #1 is specified.

[Note]

If *action* is specified as "discard," a multicast MAC address cannot be specified as *mac-addr*.

The following MAC addresses cannot be specified as *mac-addr*.

- 0000.0000.0000
- 0100.5e00.0000 - 0100.5eff.ffff
- 0180.c200.0000 - 0180.c200.000f
- 0180.c200.0020 - 0180.c200.002f
- ffff.ffff.ffff

[Example]

Specify that frames addressed to 00a0.de11.2233 are forwarded to LAN port #2.

```
SWP2(config)#mac-address-table static 00a0.de11.2233 forward port1.2
```

6.1.5 Show MAC address table

[Syntax]

show mac-address-table

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the MAC address table.

The following items are shown.

- VLAN ID
- Interface name
- MAC address
- Action applied to frames
- Entry type
- Ageing time

[Example]

Show the MAC address table.

```
SWP2>show mac-address-table
VLAN  port      mac              fwd      type     timeout
   1  port1.1   00a0.de11.2233  forward  static         0
   1  sa1       1803.731e.8c2b  forward  dynamic      300
   1  sa2       782b.cbcb.218d  forward  dynamic      300
```

6.1.6 Show number of MAC addresses

[Syntax]

show mac-address-table count
show mac-address-table count interface *ifname*
show mac-address-table count vlan *vlan-id*

[Keyword]

interface	:	Show the number of MAC addresses for only a specified interface
vlan	:	Show the number of MAC addresses for only a specific VLAN

[Parameter]

ifname	:	Name of interface to show Only LAN/SFP+ port or logical interface can be specified
vlan-id	:	<1-4094> VLAN ID to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the number of MAC addresses that are registered in the FDB entries.

The number of dynamic addresses registered by automatic learning and of manually registered static addresses are shown.

[Example]

Show the number of MAC addresses that are registered in the FDB entries.

```
SWP2>show mac-address-table count
 MAC Entries for all vlans
  Dynamic Address   : 20
  Static Address    : 10
  Total MAC Address : 30
```

6.2 VLAN

6.2.1 Move to VLAN mode

[Syntax]

vlan database

[Input mode]

global configuration mode

[Description]

Moves to VLAN mode in order to make VLAN interface settings.

[Note]

To return from VLAN mode to global configuration mode, use the **exit** command. To return to priviledged EXEC mode, use the **end** command.

[Example]

Move to VLAN mode.

```
SWP2(config)#vlan database
SWP2(config-vlan)#
```

6.2.2 Set VLAN interface

[Syntax]

vlan *vlan-id* [name *name*] [state *state*]
no vlan *vlan-id*

[Keyword]

name	:	Specifies the name of the VLAN
state	:	Specifies the state of the VLAN

[Parameter]

vlan-id	:	<2-4094> VLAN ID
name	:	Single-byte alphanumeric characters and single-byte symbols(32characters or less) Name of the VLAN
state	:	Whether frame forwarding is enabled or disabled

Setting value	Description
enable	Frames are forwarded
disable	Frames are not forwarded

[Initial value]

none

[Input mode]

VLAN mode

[Description]

Sets the VLAN interface.

If this command is executed with the "no" syntax, the VLAN interface is deleted.

If "name" is omitted, the name of the VLAN is specified as "VLANxxxx" (xxxx is the four-digit VLAN ID).

If "state" is omitted, "enable" is specified.

If "disable" is specified, all settings of the VLAN interface are deleted.

[Note]

If this command is executed with "name" omitted for a VLAN ID for which *name* is already specified, the already-specified *name* is not changed.

Multiple VLAN IDs can be specified for *vlan-id*. However, if multiple VLAN IDs are specified, the name cannot be specified.

To specify multiple items, use "-" or "," as shown below

- To select from VLAN #2 through VLAN #4: 2-4
- To select VLAN #2 and VLAN #4: 2,4

[Example]

Set VLAN #1000 with the name "Sales".

```
SWP2(config-vlan)#vlan 1000 name Sales
```

6.2.3 Set private VLAN

[Syntax]

private-vlan *vlan-id type*
no private-vlan *vlan-id type*

[Parameter]

vlan-id	:	<2-4094> VLAN ID set by the **vlan** command

type : Type of private VLAN

Setting value	Description
primary	Primary VLAN
community	Secondary VLAN (community VLAN)
isolated	Secondary VLAN (isolated VLAN)

[Initial value]

none

[Input mode]

VLAN mode

[Description]

Uses *vlan-id* as a private VLAN.

If this command is executed with the "no" syntax, the private VLAN setting is deleted, and it is used as a conventional VLAN.

[Note]

If this is set as a community VLAN, it can communicate with the promiscuous port of the primary VLAN and with another interface that is associated with the same community VLAN, but cannot communicate with a different community VLAN or with an interface that is associated with an isolated VLAN.

If this is set as an isolated VLAN, it can communicate with the promiscuous port of the primary VLAN, but cannot communicate with the community VLAN or with another interface that is associated with an isolated VLAN.

[Example]

Set the following private VLANs.

- VLAN #100 : Primary VLAN
- VLAN #101 : Secondary VLAN (community VLAN)
- VLAN #102 : Secondary VLAN (community VLAN)
- VLAN #103 : Secondary VLAN (isolated VLAN)

```
SWP2(config-vlan)#vlan 100
SWP2(config-vlan)#vlan 101
SWP2(config-vlan)#vlan 102
SWP2(config-vlan)#vlan 103
SWP2(config-vlan)#private-vlan 100 primary
SWP2(config-vlan)#private-vlan 101 community
SWP2(config-vlan)#private-vlan 102 community
SWP2(config-vlan)#private-vlan 103 isolated
```

6.2.4 Set secondary VLAN for primary VLAN

[Syntax]

private-vlan *vlan-id* **association** add *2nd-vlan-ids*
private-vlan *vlan-id* **association** remove *2nd-vlan-ids*
no private-vlan *vlan-id* **association**

[Keyword]

add : Associate the specified VLAN

remove : Remove the association of the specified VLAN

[Parameter]

vlan-id : <2-4094>

VLAN ID specified for the primary VLAN

2nd-vlan-ids : <2-4094>

VLAN ID specified for the secondary VLAN

To specify multiple items, use "-" or "," as shown below

- To select from VLAN #2 through VLAN #4: 2-4
- To select VLAN #2 and VLAN #4: 2,4

[Initial value]

none

[Input mode]

VLAN mode

[Description]

Specify the association of the secondary VLAN (isolated VLAN, community VLAN) with the primary VLAN of the private VLAN.

By specifying "add," specify the association of the *vlan-id* with the *2nd-vlan-ids*.

By specifying "remove," remove the association of the *vlan-id* and the *2nd-vlan-ids*.

If this command is executed with the "no" syntax, all associations to the primary VLAN are deleted.

[Example]

After specifying the following private VLAN, associate the secondary VLANs to the primary VLAN.

- VLAN #100 : Primary VLAN
- VLAN #101 : Secondary VLAN (community VLAN)
- VLAN #102 : Secondary VLAN (community VLAN)
- VLAN #103 : Secondary VLAN (isolated VLAN)

```
SWP2(config-vlan)#vlan 100
SWP2(config-vlan)#vlan 101
SWP2(config-vlan)#vlan 102
SWP2(config-vlan)#vlan 103
SWP2(config-vlan)#private-vlan 100 primary
SWP2(config-vlan)#private-vlan 101 community
SWP2(config-vlan)#private-vlan 102 community
SWP2(config-vlan)#private-vlan 103 isolated
SWP2(config-vlan)#private-vlan 100 association add 101
SWP2(config-vlan)#private-vlan 100 association add 102
SWP2(config-vlan)#private-vlan 100 association add 103
```

6.2.5 Set access port (untagged port)

[Syntax]

switchport mode access

[Initial value]

switchport mode access

[Input mode]

interface mode

[Description]

Specifies the port type of the applicable interface as an access port.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

If this command is applied to a logical interface, the settings of every LAN/SFP+ port associated with that interface are changed.

If the port type is changed from a trunk port to an access port, the setting of the **switchport trunk allowed vlan** command and the **switchport trunk native vlan** command return to their default settings.

To specify the VLAN that is associated as an access port, use the **switchport access vlan** command.

[Example]

Set LAN port #1 as an access port.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode access
```

6.2.6 Set associated VLAN of an access port (untagged port)

[Syntax]

switchport access vlan *vlan-id*
no switchport access vlan

[Parameter]

vlan-id : <1-4094>

Associated VLAN ID

[Initial value]

switchport access vlan 1

[Input mode]

interface mode

[Description]

Sets the VLAN ID that is associated as an access port with the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only for a LAN/SFP+ port or logical interface for which the **switchport mode access** command is set.

If this command is applied to a logical interface, the settings of every LAN/SFP+ port associated with that interface are changed.

If the port type is changed to a trunk port, the setting of this command returns to the default setting.

[Example]

Set VLAN #10 as the VLAN to which LAN port #1 is associated as the access port.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport access vlan 10
```

6.2.7 Set trunk port (tagged port)

[Syntax]

switchport mode trunk [ingress-filter *action*]

[Keyword]

ingress-filter : Specifies the behavior of the ingress filter

[Parameter]

action : Behavior of the ingress filter

Setting value	Description
enable	Enable the ingress filter
disable	Disable the ingress filter

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the port type of the applicable interface as an trunk port.

If "ingress-filter" is omitted, "enable" is specified.

If ingress filtering is enabled, frames are forwarded only if the VLAN ID of the received frame matches the VLAN associated with the interface.

If ingress filtering is disabled, all frames are forwarded.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

If this command is applied to a logical interface, the settings of every LAN/SFP+ port associated with that interface are changed.

If the port type is changed from an access port to a trunk port, the setting of the **switchport access vlan** command returns to the default setting.

To specify the VLAN ID that is associated as a trunk port, use the **switchport trunk allowed vlan** command. To specify the native VLAN, use the **switchport trunk native vlan** command.

[Example]

Set LAN port #1 as a trunk port.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode trunk
```

6.2.8 Set associated VLAN for trunk port (tagged port)

[Syntax]

switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add *vlan-ids*
switchport trunk allowed vlan except *vlan-ids*
switchport trunk allowed vlan remove *vlan-ids*
no switchport trunk

[Keyword]

all	:	vlanAssociate to all VLANs that are set by the vlan command
none	:	Dissociate from all VLANs
add	:	Associate to the specified VLAN
except	:	Associate to all VLANs that are set by the vlan command except for the specified
remove	:	Dissociate from the specified VLAN

[Parameter]

vlan-ids	:	<1-4094> VLAN ID set by the **vlan** command To specify multiple items, use "-" or "," as shown below • To select from VLAN #2 through VLAN #4: 2-4 • To select VLAN #2 and VLAN #4: 2,4

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the VLAN ID that is associated as a trunk port with the applicable interface.

If this is executed with the "no" syntax, all associated VLAN IDs are deleted and the port type is changed to access port.

[Note]

This command can be set only for a LAN/SFP+ port or logical interface for which the **switchport mode trunk** command is set.

If this command is applied to a logical interface, the settings of every LAN/SFP+ port associated with that interface are changed.

If the port type is changed to access port, the setting of this command returns to the default setting.

If this is set with "all" or "except" specified, the content of a subsequently changed **vlan** command is always applied.

If this is set with "all" or "except" specified, making the following settings will change the remaining affiliated VLAN IDs to the settings that were specified by "add."

- If you specify "remove" to delete a VLAN ID that is associated
- If you use the **switchport trunk native vlan** command to specify an associated VLAN ID

If you make this setting with "except" specified, and then associate the VLAN ID that had been excluded by specifying "add", the associated VLAN ID is changed to the setting specified by "add".

If you specify "remove" and then specify an unassociated VLAN ID, an error occurs.

For the setting of this command and the **switchport trunk native vlan** command, the last-specified command takes priority.

- If you use the **switchport trunk native vlan** command to specify a VLAN ID that was associated by this command, it is removed from the specified VLAN ID.
- If you specify and associate a VLAN ID that was set by the **switchport trunk native vlan** command, **switchport trunk native vlan none** is set.

If you specify the **switchport trunk allowed vlan add** command with a combination of "-" or "," in the *vlan-ids*, the command setting will fail if you revert to an older version (Rev.2.00.08 or earlier). As a result, normal communication might become impossible. (Example setting: switchport trunk allowed vlan add 101,103-105)

[Example]

Set LAN port #1 as the trunk port, and associate it to VLAN #2.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode trunk
SWP2(config-if)#switchport trunk allowed vlan add 2
```

6.2.9 Set native VLAN for trunk port (tagged port)

[Syntax]

switchport trunk native vlan *vlan-id*
switchport trunk native vlan none
no switchport trunk native vlan

[Keyword]

none	:	Disables the native VLAN

[Parameter]

vlan-id	:	<1-4094>
		VLAN ID set by the **vlan** command

[Initial value]

switchport trunk native vlan 1

[Input mode]

interface mode

[Description]

Sets the native VLAN for the applicable interface.

If "none" is specified, the native VLAN is disabled. This means that untagged frames received by the applicable interface are discarded.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only for a LAN/SFP+ port or logical interface for which the **switchport mode trunk** command is set.

If this command is applied to a logical interface, the settings of every LAN/SFP+ port associated with that interface are changed.

If the port type is changed to access port, the setting of this command returns to the default setting.

For the setting of this command and the setting of the **switchport trunk allowed vlan** command, the last-specified command takes priority.

- If you use the **switchport trunk allowed vlan** command to specify the associated VLAN ID, and then specify this command, it is removed from the specified VLAN ID.
- If the VLAN ID specified by this command is associated using the **switchport trunk allowed vlan** command, **switchport trunk native vlan none** is specified.

[Example]

Set LAN port #1 as the trunk port, and specify VLAN #2 as the native VLAN.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode trunk
SWP2(config-if)#switchport trunk native vlan 2
```

6.2.10 Set private VLAN port type

[Syntax]

switchport mode private-vlan *port-type*
no switchport mode private-vlan *port-type*

[Parameter]

port-type : Port mode

Setting value	Description
promiscuous	Promiscuous port
host	Host port

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the private VLAN port type for the applicable interface.

If this is executed with the "no" syntax, the setting of the private VLAN specified for the applicable interface is deleted.

[Note]

This command can be set only for a LAN/SFP+ port for which the **switchport mode access** command is set.

In addition, promiscuous can be specified for the following interfaces.

- Interface that is operating as a trunk port
- logical interface

[Example]

Set LAN port #1 as a promiscuous port, and LAN port #2 as a host port.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode private-vlan promiscuous
SWP2(config-if)#exit
SWP2(config)#interface port1.2
SWP2(config-if)#switchport mode private-vlan host
```

6.2.11 Set private VLAN host port

[Syntax]

switchport private-vlan host-association *pri-vlan-id* add *2nd-vlan-id*
no switchport private-vlan host-association

[Keyword]

add : Sets the secondary VLAN for the primary VLAN

[Parameter]

pri-vlan-id : <2-4094>

VLAN ID specified as the primary VLAN

2nd-vlan-id : <2-4094>

VLAN ID specified as the secondary VLAN

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the primary VLAN that is associated as the host port of the private VLAN for the applicable interface, and associates the secondary VLAN.

If this is executed with the "no" syntax, the setting of the primary VLAN associated as the host port of the applicable interface, and the association of the secondary VLAN, are deleted.

[Note]

This command can be set only for a LAN/SFP+ port that has been set as the host port by the **switchport mode private-vlan** command.

pri-vlan-id and *2nd-vlan-id* must be associated by the **private-vlan association** command.

If the **switchport mode private-vlan** command is used to set the port type to something other than host port, the setting of this command is deleted.

[Example]

Specify the following private VLAN for each interface.

- LAN port #1 : Primary VLAN #100, Secondary VLAN #101
- LAN port #2 : Primary VLAN #100, Secondary VLAN #102
- LAN port #3 : Primary VLAN #100, Secondary VLAN #103

```
SWP2(config)# interface port1.1
SWP2(config-if)# switchport mode private-vlan host
SWP2(config-if)# switchport private-vlan host-association 100 add 101
SWP2(config-if)# interface port1.2
SWP2(config-if)# switchport mode private-vlan host
SWP2(config-if)# switchport private-vlan host-association 100 add 102
SWP2(config-if)# interface port1.3
SWP2(config-if)# switchport mode private-vlan host
SWP2(config-if)# switchport private-vlan host-association 100 add 103
```

6.2.12 Set promiscuous port for private VLAN

[Syntax]

switchport private-vlan mapping *pri-vlan-id* add *2nd-vlan-ids*
switchport private-vlan mapping *pri-vlan-id* remove *2nd-vlan-ids*
no switchport private-vlan mapping

[Keyword]

add	:	Sets the secondary VLAN for the primary VLAN
remove	:	Deletes the secondary VLAN for the primary VLAN

[Parameter]

pri-vlan-id	:	<2-4094> VLAN ID specified as the primary VLAN
2nd-vlan-ids	:	<2-4094> VLAN ID specified as the secondary To specify multiple items, use "-" or "," as shown below • To select from VLAN #2 through VLAN #4: 2-4 • select VLAN #2 and VLAN #4: 2,4

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the primary VLAN that is associated with the applicable interface as the promiscuous port, and associates the secondary VLAN.

If this is executed with the "no" syntax, the setting of the primary VLAN that is associated with the applicable interface as the promiscuous port, and the association of the secondary VLAN, are deleted.

[Note]

This command can be set only for a LAN/SFP+ port that has been set as a promiscuous port by the **switchport mode private-vlan** command.

In addition, it can also be set for the following interfaces that are specified as promiscuous ports.

- Interface that is operating as a trunk port
- logical interface

pri-vlan-id and *2nd-vlan-ids* must be associated by the **private-vlan association** command.

If this command is applied to a logical interface, the settings of every LAN/SFP+ port associated with that interface are changed.

If the **switchport mode private-vlan** command is used to set the port type to something other than promiscuous port, the setting of this command is deleted.

A community VLAN can be associated with multiple promiscuous ports.

Multiple promiscuous ports can be specified for one primary VLAN.

Since an interface in an isolated VLAN can communicate only with one promiscuous port, only one promiscuous port can be associated with one isolated VLAN.

[Example]

Make LAN port #1 operate as a promiscuous port, specify primary VLAN #100, and associate the secondary VLANs #101, #102, and #103.

```
SWP2(config)# interface port1.1
SWP2(config-if)# switchport mode private-vlan promiscuous
SWP2(config-if)# switchport private-vlan mapping 100 add 101
SWP2(config-if)# switchport private-vlan mapping 100 add 102
SWP2(config-if)# switchport private-vlan mapping 100 add 103
```

6.2.13 Set voice VLAN

[Syntax]

switchport voice vlan *type*
no switchport voice vlan

[Parameter]

type : Type

Setting value	Description
<1-4094>	VLAN ID
dot1p	Use priority tagged frames
untagged	Use untagged frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets voice VLAN. This can be specified only for a physical interface that is specified as an access port.

If a VLAN ID is specified, frames with an 802.1p tag of the specified VLAN are used as voice traffic.

If dot1p is specified, priority tag frames (VLAN ID of 0, and CoS value of the specified 802.1p tag) are used as voice traffic.

If untagged is specified, untagged frames are used as voice traffic.

[Example]

Assign LAN port #1 as voice VLAN to VLAN #100.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport voice vlan 100
```

6.2.14 Set CoS value for voice VLAN

[Syntax]

switchport voice cos *value*
no switchport voice cos

[Parameter]

value : <0-7>
CoS value to specify for connected device

[Initial value]

switchport voice cos 5

[Input mode]

interface mode

[Description]

Specify the CoS value to use for voice traffic by the connected device.

The connected device is notified of the setting via LLDP-MED in the following cases.

- Voice VLAN is specified for the corresponding port.
- LLDP-MED transmission and reception is possible for the corresponding port.

[Example]

Set the CoS value to 6 for using LAN port #1 as voice VLAN.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport voice cos 6
```

6.2.15 Set DSCP value for voice VLAN

[Syntax]

switchport voice dscp *value*
no switchport voice dscp

[Parameter]

value : <0-63>
DSCP value to specify for connected device

[Initial value]

switchport voice dscp 0

[Input mode]

interface mode

[Description]

Specify the DSCP value to use for voice traffic by the connected device.

The connected device is notified of the setting via LLDP-MED in the following cases.

- Voice VLAN is specified for the corresponding port.
- LLDP-MED transmission and reception is possible for the corresponding port.

[Example]

Set the DSCP value to 63 for using LAN port #1 as voice VLAN.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport voice dscp 63
```

6.2.16 Set multiple VALN group

[Syntax]

switchport multiple-vlan group *group-ids*
no switchport multiple-vlan group

[Parameter]

group-ids : <1-256>

Multiple VLAN group ID

To specify multiple items, use "-" or "," as shown below

- To select from group #2 through group #4: 2-4
- To select group #2 and group #4: 2,4

[Initial value]

none

[Input mode]

interface mode

[Description]

Specify the group of multiple VLAN.

If a group is specified for the interface, the corresponding interface can communicate only with interfaces of the same multiple VLAN group. Even if the VLAN is the same, communication is not possible if the multiple VLAN group differs.

This can be specified only for a physical interface or for a link aggregation logical interface.

By default, each interface is not associated with a multiple VLAN group.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This cannot be used in conjunction with the private VLAN.

Ports that are associated with a link aggregation logical interface must be set to the same multiple VLAN group.

The multiple VLAN group is applied only to forwarding between ports. Self-originating packets are not affected by multiple VLAN group settings.

Even if multiple VLAN is specified, correct communication might not be possible due to the following.

- Spanning tree block status
- IGMP snooping or MLD snooping status
- Loop detection block status

[Example]

Assign LAN port #1 to multiple VLAN group #10.

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport multiple-vlan group 10
SWP2(config-if)#exit
```

6.2.17 Set name of multiple VLAN group

[Syntax]

multiple-vlan group *group-id* **name** *name*
no multiple-vlan group *group-id*

[Parameter]

group-id : <1-256>

Multiple VLAN group ID

name : Single-byte alphanumeric characters and single-byte symbols(32characters or less)

Name of mulitiple VLAN group

[Initial value]

multiple-vlan group *group-id* name GROUPxxxx (xxxx is the four-digit group ID)

[Input mode]

global configuration mode

[Description]

Sets the name of multiple VLAN group.

If this command is executed with the "no" syntax, the setting returns to the default.

The name that was set is shown with the **show vlan multiple-vlan** command.

[Example]

Set multiple VLAN group #10 with the name "Network1".

```
SWP2(config)#multiple-vlan group 10 name Network1
```

6.2.18 Configuring the YMPI frame transmission when multiple VLANs are configured

[Syntax]

multiple-vlan transfer ympi *switch*
no multiple-vlan transfer ympi

[Parameter]

switch : Behavior of the YMPI frame transmission when multiple VLANs are configured

Setting value	Description
enable	Enable transmission
disable	Disable transmission

[Initial value]

multiple-vlan transfer ympi enable

[Input mode]

global configuration mode

[Description]

Sets whether YMPI frames, the management frames for Yamaha wireless access points, are transmitted when multiple VLANs are configured.

This must be enabled if you want to use cluster management or wireless LAN controller functionality with multiple Yamaha wireless access points belonging to different multiple VLAN groups.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Disable YMPI frame transmission when multiple VLANs are configured.

```
SWP2(config)#multiple-vlan transfer ympi disable
```

6.2.19 Show VLAN information

[Syntax]

show vlan *vlan-id*
show vlan brief

[Keyword]

brief : Show all VLAN information

[Parameter]

vlan-id : <1-4094>

VLAN ID to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows information for the specified VLAN ID.

The following items are shown.

Item	Description
VLAN ID	VLAN ID

Item	Description
Name	Name of the VLAN
State	VLAN status (whether frames are forwarded) • ACTIVE : forwarded • SUSPEND : not forwarded
Member ports	Interfaces associated with the VLAN ID • (u) : Access port (untagged port) • (t) : Trunk port (tagged port)

[Example]

Show all VLAN information.

```
SWP2>show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID  Name                             State   Member ports
======= ================================ ======= ======================
1       default                          ACTIVE  port1.1(u) port1.2(u)
                                                 port1.3(u) port1.4(u)
                                                 port1.5(u) port1.6(u)
                                                 port1.7(u) port1.8(u)
```

6.2.20 Show private VLAN information

[Syntax]

show vlan private-vlan

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows private VLAN information.

The following items are shown.

Item	Description
PRIMARY	VLAN ID of primary VLAN
SECONDARY	VLAN ID of secondary VLAN
TYPE	Type of secondary VLAN • isolated : Isolated VLAN • community : Community VLAN
INTERFACES	Interfaces that are associated as a host port

[Example]

Show private VLAN information.

```
SWP2>show vlan private-vlan
PRIMARY       SECONDARY          TYPE         INTERFACES
-------        ---------       ----------      ----------
      2              21         isolated
      2              22         community
```

6.2.21 Show multiple VLAN group setting information

[Syntax]

show vlan multiple-vlan [**group** *group-id*]

[Keyword]

group : Show information for specific multiple VLAN groups

[Parameter]

group-id : <1-256>

Multiple VLAN group ID

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the setting status for multiple VLAN groups.

If the "group" specification is omitted, all groups that are actually assigned to the interface are shown.

The setting state of the YMPI frame transmission function is also displayed.

[Example]

Shows the setting status for multiple VLAN groups.

```
SWP2>show vlan multiple-vlan
GROUP ID  Name                             Member ports
========= ================================ ======================
1         GROUP0001                        port1.1 port1.2
                                           port1.5

YMPI transfer: Enable
```

6.3 STP (Spanning Tree Protocol)

6.3.1 Set spanning tree for the system

[Syntax]

spanning-tree shutdown
no spanning-tree shutdown

[Initial value]

no spanning-tree shutdown

[Input mode]

global configuration mode

[Description]

Disables spanning tree for the entire system.

If this command is executed with the "no" syntax, spanning tree is enabled for the entire system.

[Note]

In order to enable spanning tree, spanning tree must be enabled on the interface in addition to this command.

[Example]

Disable spanning tree for the entire system.

```
SWP2(config)#spanning-tree shutdown
```

6.3.2 Set forward delay time

[Syntax]

spanning-tree forward-time *time*
no spanning-tree forward-time

[Parameter]

time : <4-30>

Forward delay time (seconds)

[Initial value]

spanning-tree forward-time 15

[Input mode]

global configuration mode

[Description]

Sets the forward delay time.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The setting of this command must satisfy the following conditions.
2 x (hello time + 1) <= maximum aging time <= 2 x (forward delay time - 1)

The maximum aging time can be set by the **spanning-tree max-age** command.

The hello time is always 2 seconds, and cannot be changed.

[Example]

Set the forward delay time to 10 seconds.

```
SWP2(config)#spanning-tree forward-time 10
```

6.3.3 Set maximum aging time

[Syntax]

spanning-tree max-age *time*
no spanning-tree max-age

[Parameter]

time : <6-40>
Maximum aging time (seconds)

[Initial value]

spanning-tree max-age 20

[Input mode]

global configuration mode

[Description]

Sets the maximum aging time.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The maximum aging time is the time that the L2 switch waits without receiving a spanning tree configuration message, and after which time it attempts to reconfigure.

The setting of this command must satisfy the following conditions.
2 x (hello time + 1) <= maximum aging time <= 2 x (forward delay time - 1)

The forward delay time can be set by the **spanning-tree forward-time** command.

The hello time is always 2 seconds, and cannot be changed.

[Example]

Set the maximum aging time to 25 seconds.

```
SWP2(config)#spanning-tree max-age 25
```

6.3.4 Set bridge priority

[Syntax]

spanning-tree priority *priority*
no spanning-tree priority

[Parameter]

priority : <0-61440> (multiple of 4096)
Priority value

[Initial value]

spanning-tree priority 32768

[Input mode]

global configuration mode

[Description]

Sets the bridge priority. Lower numbers have higher priority.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In the case of MSTP, this is the setting for CIST (instance #0).

[Example]

Set the bridge priority to 4096.

```
SWP2(config)#spanning-tree priority 4096
```

6.3.5 Set spanning tree for an interface

[Syntax]

spanning-tree *switch*

[Parameter]

switch : Spanning tree operation

Setting value	Description
enable	Enable spanning tree
disable	Disable spanning tree

[Initial value]

spanning-tree enable

[Input mode]

interface mode

[Description]

Sets spanning tree operation for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

[Example]

Disable spanning tree for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree disable
```

6.3.6 Set spanning tree link type

[Syntax]

spanning-tree link-type *type*
no spanning-tree link-type

[Parameter]

type : Link type

Setting value	Description
point-to-point	Point-to-point link
shared	Shared link

[Initial value]

spanning-tree link-type point-to-point

[Input mode]

interface mode

[Description]

Sets the link type for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Set the LAN port #1 link type to "shared."

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree link-type shared
```

6.3.7 Set interface BPDU filtering

[Syntax]

spanning-tree bpdu-filter *filter*
no spanning-tree bpdu-filter

[Parameter]

filter : BPDU filtering operation

Setting value	Description
enable	Enables BPDU filtering
disable	Disables BPDU filtering

[Initial value]

spanning-tree bpdu-filter disable

[Input mode]

interface mode

[Description]

Sets BPDU filtering for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Enable BPDU filtering for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree bpdu-filter enable
```

6.3.8 Set interface BPDU guard

[Syntax]

spanning-tree bpdu-guard *guard*
no spanning-tree bpdu-guard

[Parameter]

guard : BPDU guard operation

Setting value	Description
enable	Enables BPDU guard
disable	Disables BPDU guard

[Initial value]

spanning-tree bpdu-guard disable

[Input mode]

interface mode

[Description]

Sets BPDU guard for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

If a LAN/SFP+ port is **shutdown** by BPDU guard, it can be brought back by executing the **no shutdown** command for that interface.

If a logical interface is **shutdown** by BPDU guard, it can be brought back by executing the **shutdown** command for that interface and then executing the **no shutdown** command.

[Example]

Enable BPDU guard for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree bpdu-guard enable
```

6.3.9 Set interface path cost

[Syntax]

spanning-tree path-cost *path-cost*
no spanning-tree path-cost

[Parameter]

path-cost : <1-200000000>
Path cost value

[Initial value]

Use the following values according to the link speed of the interface.

Link speed	Path cost value
1000Mbps	20000
100Mbps	200000
10Mbps	2000000

For a logical interface, the path cost value is calculated based on totaling the link speed of each associated LAN/SFP+ port.

[Input mode]

interface mode

[Description]

Sets the path cost of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In the case of MSTP, this is the setting for CIST (instance #0).

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Set the path cost of LAN port #1 to 100000.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree path-cost 100000
```

6.3.10 Set interface priority

[Syntax]

spanning-tree priority *priority*
no spanning-tree priority

[Parameter]

priority : <0-240> (multiple of 16)
Priority value

[Initial value]

spanning-tree priority 128

[Input mode]

interface mode

[Description]

Sets the priority of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

Lower numeric values indicate a higher priority, increasing the probability that the other interface will become the root port.

[Note]

In the case of MSTP, this is the setting for CIST (instance #0).

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Set the LAN port #1 priority to 64.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree priority 64
```

6.3.11 Set edge port for interface

[Syntax]

spanning-tree edgeport
no spanning-tree edgeport

[Initial value]

no spanning-tree edgeport

[Input mode]

interface mode

[Description]

Sets the edge port of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Set LAN port #1 as the edge port.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree edgeport
```

6.3.12 Show spanning tree status

[Syntax]

show spanning-tree [interface *ifname*]

[Keyword]

interface	:	Specifies the interface to show

[Parameter]

ifname	:	Name of LAN/SFP+ port or logical interface Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the spanning tree status.

If "interface" is omitted, the status of all interfaces is shown.

In the case of MSTP, shows CIST (instance #0) information.

The following items are shown.

Item	Description
Bridge up	Spanning tree protocol enabled/disabled
Root Path Cost	Path cost of the root bridge
Root Port	Interface index number of the root port. Shows 0 if it is the root bridge. In the case of a logical interface, this is shown as the interface index number of the logical interface.
Bridge Priority	Bridge priority
Forward Delay	Root bridge forwarding delay time setting
Hello Time	Hello time setting of the root bridge
Max Age	Maximum ageing time setting of the root bridge
Root Id	Root bridge identifier. This consists of the root bridge priority (the first four hexadecimal digits) and MAC address
Bridge Id	Bridge identifier. This consists of the bridge priority (the first four hexadecimal digits) and MAC address
topology change(s)	Number of times that a topology change has occurred (to be precise, this indicates the number of BPDU that have the TC flag)
last topology change	Date and time at which the last topology change occurred
Ifindex	Interface index number
Port Id	Interface's port ID
Role	Role of the interface. This is either Disabled, Designated, Rootport, or Alternate
State	State of the interface. This is either Listening, Learning, Forwarding, or Discarding
Designated Path Cost	Path cost

Item	Description
Configured Path Cost	Path cost setting of the interface
Add type Explicit ref count	Number of STP domains associated with the interface
Designated Port Id	ID of the designated port
Priority	Priority of the interface
Root	Root bridge identifier. This consists of the root bridge priority (the first four hexadecimal digits) and MAC address
Designated Bridge	Bridge identifier. This consists of the bridge priority (the first four hexadecimal digits) and MAC address
Message Age	Elapsed time of message
Hello Time	Hello time setting value
Forward Delay	Forward delay time setting value
Forward Timer	Actual forward delay timer
Msg Age Timer	Timer at which the interface destroys BPDU information. With the default setting, count down from 20 seconds for STP, or count down Hello Time x 3 for RSTP/MSTP.
Hello Timer	Timer used to send hello. Hello packet is sent when 0 is reached
topo change timer	Topology change timer
forward-transitions	Number of times that the interface has entered Forward State
Version	Spanning tree protocol operating mode (version)
Received	Type of BPDU that was received
Send	Type of BPDU to transmit
portfast configured	Edge port setting value and current status. This will be either portfast off, portfast on, or edgeport on
bpdu-guard	Setting and current status of the interface's BPDU guard function
bpdu-filter	Setting and current status of the interface's BPDU filtering function
root guard configured	Setting and current status of the root guard function
Configured Link Type	Setting and current status of the interface's link type. Either point-to-point or shared
auto-edge configured	Auto-edge setting and current status

[Example]

Show the spanning tree status for LAN port #1.

```
SWP2>show spanning-tree interface port1.1
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 6 topology change(s)  - last topology change Tue Feb 27 19:52:52 2018

%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated -
State Forwarding
%   port1.1: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.1: Configured Path Cost 20000  - Add type Explicit ref count 1
%   port1.1: Designated Port Id 0x8389 - CIST Priority 128  -
%   port1.1: CIST Root 8000ac44f2300110
%   port1.1: Regional Root 8000ac44f2300110
```

```
%   port1.1: Designated Bridge 8000ac44f2300110
%   port1.1: Message Age 0 - Max Age 20
%   port1.1: CIST Hello Time 2 - Forward Delay 15
%   port1.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   port1.1: forward-transitions 1
%   port1.1: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   port1.1: No portfast configured - Current  portfast off
%   port1.1: bpdu-guard  disabled  - Current bpdu-guard off
%   port1.1: bpdu-filter disabled  - Current bpdu-filter off
%   port1.1: no root guard configured     - Current root guard off
%   port1.1: Configured Link Type point-to-point - Current point-to-point
%   port1.1: No auto-edge configured - Current port Auto Edge off
```

6.3.13 Show spanning tree BPDU statistics

[Syntax]

show spanning-tree statistics [interface *ifname*]

[Keyword]

interface	:	Specifies the interface to show

[Parameter]

ifname	:	Name of LAN/SFP+ port or logical interface Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows spanning tree BPDU statistics.

If "interface" is omitted, the status of all interfaces is shown.

[Example]

Show the BPDU statistics for LAN port #1.

```
SWP2>show spanning-tree statistics interface port1.1
                 Port number = 905 Interface = port1.1
                 ================================
% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Enable
% Spanning Tree Type                : Multiple Spanning Tree Protocol
% Current Port State                : Forwarding
% Port ID                           : 8389
% Port Number                       : 389
% Path Cost                         : 20000
% Message Age                       : 0
% Designated Root                   : ac:44:f2:30:01:10
% Designated Cost                   : 0
% Designated Bridge                 : ac:44:f2:30:01:10
% Designated Port Id                : 0x8389
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE

% PORT Based Information & Statistics
% ----------------------------------
% Config Bpdu's xmitted             : 3
% Config Bpdu's received            : 0
% TCN Bpdu's xmitted                : 2
% TCN Bpdu's received               : 3
% Forward Trans Count               : 1

% STATUS of Port Timers
% --------------------
% Hello Time Configured             : 2
% Hello timer                       : ACTIVE
% Hello Time Value                  : 0
% Forward Delay Timer               : INACTIVE
% Forward Delay Timer Value         : 0
```

```
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 3
% Next State                         : Discard/Blocking
% Topology Change Time               : 0

% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : ac:44:f2:30:01:10
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 5001
% Last Topology Change Occured       : Tue Feb 27 19:52:52 2018
% Topology Change                    : FALSE
% Topology Change Detected           : TRUE
% Topology Change Count              : 6
% Topology Change Last Recvd from    : 00:a0:de:ae:b8:79
```

6.3.14 Clear protocol compatibility mode

[Syntax]

clear spanning-tree detected protocols [interface *ifname*]

[Keyword]

interface	:	Specifies the interface to clear

[Parameter]

ifname	:	Name of LAN/SFP+ port or logical interface Interface to clear

[Input mode]

priviledged EXEC mode

[Description]

Returns an interface that had been operating in STP compatibility mode to normal mode.

If "interface" is omitted, the status of all interfaces is cleared.

[Note]

If a STP BPDU is received, the interface that received it will operate in STP compatibility mode. However even if STP BPDU is no longer received subsequently, the corresponding interface continues to operate in STP compatibility mode. In such cases, you can execute this command to make the interface return from STP compatibility mode to normal mode.

[Example]

Return LAN port #1 from STP compatibility to normal mode.

```
SWP2#clear spanning-tree detected protocols interface port1.1
```

6.3.15 Move to MST mode

[Syntax]

spanning-tree mst configuration

[Input mode]

global configuration mode

[Description]

Moves to MST mode in order to make MST instance and MST region settings.

[Note]

To return from MST mode to global configuration mode, use the **exit** command. To return to priviledged EXEC mode, use the **end** command.

[Example]

Move to MST mode.

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#
```

6.3.16 Generate MST instance

[Syntax]

instance *instance-id*
no instance

[Parameter]

instance-id : <1-15>
Instance ID

[Initial value]

none

[Input mode]

MST mode

[Description]

Generates an MST instance.

If this command is executed with the "no" syntax, the MST instance is deleted.

[Note]

MST instance generation and association with a VLAN is specified by the **instance vlan** command.

[Example]

Generate MST instance #1.

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#instance 1
```

6.3.17 Set VLAN for MST instance

[Syntax]

instance *instance-id* **vlan** *vlan-id*
no instance *instance-id* **vlan** *vlan-id*

[Parameter]

instance-id : <1-15>
Instance ID

vlan-id : <2-4094>
VLAN ID set by the **vlan** command

[Initial value]

none

[Input mode]

MST mode

[Description]

Associates a VLAN with an MST instance.

If this command is executed with the "no" syntax, the VLAN association for the MST instance is deleted. If as a result of this deletion, not even one VLAN is associated with the MST instance, the MST instance is deleted.

If you specify an MST instance that has not been generated, the MST instance will also be generated.

[Note]

You cannot specify a VLAN ID that is associated with another MST instance.

[Example]

Associate VLAN #2 with MST instance #1.

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#instance 1 vlan 2
```

6.3.18 Set priority of MST instance

[Syntax]

instance *instance-id* **priority** *priority*
no instance *instance-id* **priority**

[Parameter]

instance-id	:	<1-15>
		Instance ID
priority	:	<0-61440> (multiple of 4096)
		Priority value

[Initial value]

instance *instance-id* priority 32768

[Input mode]

MST mode

[Description]

Sets the priority of the MST instance.

Lower numeric values indicate a higher priority, increasing the probability that this MST instance will become the root bridge.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set MST instance #2 to a priority of 4096.

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#instance 2
SWP2(config-mst)#instance 2 priority 4096
```

6.3.19 Set MST region name

[Syntax]

region *region-name*
no region

[Parameter]

region-name	:	Single-byte alphanumeric characters and single-byte symbols(32characters or less)
		Region name

[Initial value]

region Default

[Input mode]

MST mode

[Description]

Sets the MST region name.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the MST region name to "Test1".

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#region Test1
```

6.3.20 Set revision number of MST region

[Syntax]

revision *revision*

[Parameter]

revision : <0-65535>

Revision number

[Initial value]

revision 0

[Input mode]

MST mode

[Description]

Sets the revision number of the MST region.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the revision number as 2 for the MST region.

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#revision 2
```

6.3.21 Set MST instance for interface

[Syntax]

spanning-tree instance *instance-id*
no spanning-tree instance

[Parameter]

instance-id : <1-15>

ID of generated MST interface

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets MST instance for the applicable interface.

If this command is executed with the "no" syntax, the MST instance setting is deleted.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Set MST instance #2 for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree instance 2
```

6.3.22 Set interface priority for MST instance

[Syntax]

spanning-tree instance *instance-id* **priority** *priority*
no spanning-tree instance *instance-id* **priority**

[Parameter]

instance-id : <1-15>
ID of MST instance specified for the applicable interface

priority : <0-240> (multiple of 16)
Priority value

[Initial value]

spanning-tree instance *instance-id* priority 128

[Input mode]

interface mode

[Description]

Sets the priority for the applicable interface in the MST instance.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Set LAN port #1 MST instance #2 to a priority of 16.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree instance 2
SWP2(config-if)#spanning-tree instance 2 priority 16
```

6.3.23 Set interface path cost for MST instance

[Syntax]

spanning-tree instance *instance-id* **path-cost** *path-cost*
no spanning-tree instance *instance-id* **path-cost**

[Parameter]

instance-id : <1-15>
ID of MST instance specified for the applicable interface

path-cost : <1-200000000>
Path cost value

[Initial value]

Use the following values according to the link speed of the interface.

Link speed	Path cost value
1000Mbps	20000
100Mbps	200000
10Mbps	2000000

For a logical interface, the path cost value is calculated based on totaling the link speed of each associated LAN/SFP+ port.

[Input mode]

interface mode

[Description]

Sets the path cost of the applicable interface on an MST instance.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP+ port and logical interface.

It is not possible to specify this command for a LAN/SFP+ port that is associated to a logical interface.

If a LAN/SFP+ port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP+ port returns to the default.

[Example]

Set LAN port #1 MST instance #2 to a path cost of 100000.

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree instance 2
SWP2(config-if)#spanning-tree instance 2 path-cost 100000
```

6.3.24 Show MST region information

[Syntax]

show spanning-tree mst config

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode, interface mode

[Description]

Shows distinguishing information for the MST region.

[Example]

Show distinguishing information for the MST region.

```
SWP2>show spanning-tree mst config
%
%  MSTP Configuration Information for bridge Default :
%----------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0xAC36177F50283CD4B83821D8AB26DE62
%----------------------------------------------------
```

6.3.25 Show MSTP information

[Syntax]

show spanning-tree mst [detail] [interface *ifname*]

[Keyword]

detail	:	Shows detailed information
interface	:	Specifies the interface to show

[Parameter]

ifname	:	Name of LAN/SFP+ port or logical interface Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode, interface mode

[Description]

Shows MSTP information.

Normally, this shows association information for the MST instance and VLAN and interface.

If "detail" is specified, this shows detailed information for the interface and MST instance.

If "interface" is omitted, information for all interfaces is shown.

[Note]

A LAN/SFP+ port that is associated with a logical interface cannot be specified as *ifname*.

[Example]

Show MSTP information.

```
SWP2>show spanning-tree mst
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 9 topology change(s)  - last topology change Tue Feb 27 20:14:35 2018

%
%   Instance        VLAN
%   0:              1
%   1:              100 (port1.8)
```

Show detailed MSTP information for LAN port #8.

```
SWP2>show spanning-tree mst detail interface port1.8
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 9 topology change(s)  - last topology change Tue Feb 27 20:14:35 2018

%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.8: Configured Path Cost 20000  - Add type Explicit ref count 2
%   port1.8: Designated Port Id 0x8390 - CIST Priority 128  -
%   port1.8: CIST Root 8000ac44f2300110
%   port1.8: Regional Root 8000ac44f2300110
%   port1.8: Designated Bridge 8000ac44f2300110
%   port1.8: Message Age 0 - Max Age 20
%   port1.8: CIST Hello Time 2 - Forward Delay 15
%   port1.8: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.8: forward-transitions 1
%   port1.8: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   port1.8: No portfast configured - Current  portfast off
%   port1.8: bpdu-guard  disabled  - Current bpdu-guard off
%   port1.8: bpdu-filter disabled  - Current bpdu-filter off
%   port1.8: no root guard configured     - Current root guard off
%   port1.8: Configured Link Type point-to-point - Current point-to-point
%   port1.8: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 100
% Default: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 8001ac44f2300110
% Default: MSTI Bridge Id 8001ac44f2300110
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated Internal Path Cost 0  - Designated Port Id 0x8390
%   port1.8: Configured Internal Path Cost 20000
%   port1.8: Configured CST External Path cost 20000
%   port1.8: CST Priority 128  - MSTI Priority 128
%   port1.8: Designated Root 8001ac44f2300110
%   port1.8: Designated Bridge 8001ac44f2300110
%   port1.8: Message Age 0
%   port1.8: Hello Time 2 - Forward Delay 15
%   port1.8: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

6.3.26 Show MST instance information

[Syntax]

show spanning-tree mst instance *instance-id* [interface *ifname*]

[Keyword]

interface	:	Specifies the interface to show

[Parameter]

instance-id	:	<1-15> ID of generated MST interface
ifname	:	Name of LAN/SFP+ port or logical interface Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode, interface mode

[Description]

Shows information for the specified MST instance.

If "interface" is omitted, information is shown for all interfaces that are assigned the specified MST instance.

[Note]

A LAN/SFP+ port that is associated with a logical interface cannot be specified as *ifname*.

[Example]

Show information for MST instance #1.

```
SWP2>show spanning-tree mst instance 1
% Default: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 8001ac44f2300110
% Default: MSTI Bridge Id 8001ac44f2300110
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated Internal Path Cost 0  - Designated Port Id 0x8390
%   port1.8: Configured Internal Path Cost 20000
%   port1.8: Configured CST External Path cost 20000
%   port1.8: CST Priority 128  - MSTI Priority 128
%   port1.8: Designated Root 8001ac44f2300110
%   port1.8: Designated Bridge 8001ac44f2300110
%   port1.8: Message Age 0
%   port1.8: Hello Time 2 - Forward Delay 15
%   port1.8: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

6.4 Loop detection

6.4.1 Set loop detection function (system)

[Syntax]

loop-detect *switch*
no loop-detect

[Parameter]

switch : Set system-wide loop detection function

Setting value	Description
enable	Enables system-wide loop detection function
disable	Disables system-wide loop detection function

[Initial value]

loop-detect disable

[Input mode]

global configuration mode

[Description]

Enables or disables the system-wide loop detection function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The spanning tree function and the loop detection function can be used together on the entire system.

In order to enable the loop detection function, the loop detection function must be enabled on the interface in addition to this command.

Even if the loop detection function is enabled, the loop detection function does not operate on the following interfaces.

- LAN/SFP+ port and logical interface on which the spanning tree function is operating However, because a Forwarding port transmits and receives LDF, the loop detection will operate if misconnection or another issue causes a loop to occur.
- LAN/SFP+ port that is operating as a mirror port for the mirroring function

[Example]

Enable the loop detection function for the entire system.

```
SWP2(config)#loop-detect enable
```

Disable the loop detection function for the entire system.

```
SWP2(config)#loop-detect disable
```

6.4.2 Set loop detection function (interface)

[Syntax]

loop-detect *switch*
no loop-detect

[Parameter]

switch : Set loop detection function for the applicable interface

Setting value	Description
enable	Enables loop detection function for the applicable interface
disable	Disables loop detection function for the applicable interface

[Initial value]

loop-detect enable

[Input mode]

interface mode

[Description]

Enables or disables loop detection function for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In order to enable the loop detection function, the loop detection function must be enabled on the entire system in addition to this command.

An LAN/SFP+ port whose settings of this command differ cannot be aggregated as a logical interface. However, in the case of settings for an LAN/SFP+ port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

This command cannot be executed for LAN/SFP+ port that belong to logical interface.

Even if the loop detection function is enabled, the loop detection function does not operate on the following interfaces.

- LAN/SFP+ port and logical interface on which the spanning tree function is operating However, because a forwarding port transmits and receives LDF, the loop detection will operate if misconnection or another issue causes a loop to occur.
- LAN/SFP+ port that is operating as a mirror port for the mirroring function

The following table shows which function is enabled depending on the settings of the spanning tree function (STP) and the loop detection function (LPD).

			Interface			
			LPD disabled		LPD enabled	
			STP disabled	STP enabled	STP disabled	STP enaabled
System	LPD disabled	STP disabled	-	-	-	-
		STP enabled	-	STP	-	STP
	LPD enabled	STP disabled	-	-	LPD	LPD
		STP enabled	-	STP	LPD	STP

[Example]

Enable the loop detection function of LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect enable
```

Enables the loop detection function of static logical interface #1.

```
SWP2(config)#interface sa1
SWP2(config-if)#loop-detect enable
```

Enables the loop detection function of LACP logical interface #1.

```
SWP2(config)#interface po1
SWP2(config-if)#loop-detect enable
```

Disable the loop detection function of LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect disable
```

6.4.3 Set port blocking for loop detection

[Syntax]

loop-detect blocking *switch*
no loop-detect blocking

[Parameter]

switch : Set port blocking for the applicable interface

Setting value	Description
enable	Enables port blocking for the applicable interface
disable	Disables port blocking for the applicable interface

[Initial value]

loop-detect blocking enable

[Input mode]

interface mode

[Description]

Enables or disables blocking when a loop is detected for the applicable interface.

If this is executed with the "no" syntax, the setting returns to the default.

[Note]

An LAN/SFP+ port whose settings of this command differ cannot be aggregated as a logical interface. However, in the case of settings for an LAN/SFP+ port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

This command cannot be executed for LAN/SFP+ port that belong to logical interface.

[Example]

Block if a loop is detected on LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect blocking enable
```

This executes blocking if a loop is detected on static logical interface #1.

```
SWP2(config)#interface sa1
SWP2(config-if)#loop-detect blocking enable
```

This executes blocking if a loop is detected on LACP logical interface #1.

```
SWP2(config)#interface po1
SWP2(config-if)#loop-detect blocking enable
```

Do not block if a loop is detected on LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect blocking disable
```

6.4.4 Detects Port Blocking loop clearing at regular intervals

[Syntax]

loop-detect blocking interval *interval*
no loop-detect blocking interval

[Parameter]

interval : <10-3600>
Time between loop clearing detection (seconds)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Normally, Blocking is released immediately when the loop is cleared.

When this command is configured, it detects if the loop is cleared at regular intervals.

If the loop is cleared, Blocking is released, but if the loop is not cleared, Blocking continues until that time passes again.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a port in the Port Blocking state goes link down, the Port Blocking is removed immediately.

[Example]

Set the Port Blocking loop clearing detection interval to 300 seconds.

```
SWP2(config)#loop-detect blocking interval 300
```

6.4.5 Reset loop detection status

[Syntax]

loop-detect reset

[Input mode]

priviledged EXEC mode

[Description]

Resets the loop detection status of all interfaces.

[Note]

This command can be executed only if the system-wide loop detection function is enabled.

[Example]

Reset the loop detection status.

```
SWP2#loop-detect reset
```

6.4.6 Show loop detection function status

[Syntax]

show loop-detect

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the settings and status of the loop detection function.

The following items are shown.

- Setting of the system-wide loop detection function
- Port Blocking loop clearing detection interval ("auto" or "N seconds")
- Loop detection status for each LAN/SFP+ port and logical interface
  - Interface name (port, sa, po)
  - Setting of the loop detection function (loop-detect) for LAN/SFP+ port and logical interface. If the loop detection function is operating, (*) is added
  - Status of the Port Blocking setting (port-blocking)
  - Loop detection status (status)

[Note]

This is not shown for LAN/SFP+ port that belong to a logical interface.

[Example]

Show the loop detection status.

```
SWP2>show loop-detect
loop-detect: Enable
port-blocking interval: 300 seconds

port      loop-detect    port-blocking           status
-------------------------------------------------------
port1.1        enable(*)        enable         Detected
port1.2        enable(*)        enable         Blocking
port1.3        enable(*)        enable           Normal
port1.4        enable(*)       disable           Normal
port1.5        enable(*)        enable           Normal
port1.6        enable(*)        enable         Shutdown
port1.7       disable           enable           ------
   :             :                :                :
sa1            enable(*)        enable         Blocking
   :             :                :                :
po1            enable(*)        enable           Normal
   :             :                :                :
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

6.5 DHCP snooping

6.5.1 Enable/disable setting for DHCP snooping (system)

[Syntax]

ip dhcp snooping *switch*
no ip dhcp snooping

[Parameter]

switch : System-wide DHCP snooping function setting

Setting value	Description
enable	Enables settings of the DHCP snooping function for the entire system
disable	Disables settings of the DHCP snooping function for the entire system

[Initial value]

ip dhcp snooping disable

[Input mode]

global configuration mode

[Description]

Enables or disables settings of the system-wide DHCP snooping function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DHCP snooping function, you must enable the DHCP snooping function for the VLAN interface in addition to using this command.

Also, you must use the **ip dhcp snooping trust** command to set the port that is connected to the DHCP server.

[Example]

This enables the DHCP snooping function for the entire system.

```
SWP2(config)#ip dhcp snooping enable
```

This disables the DHCP snooping function for the entire system.

```
SWP2(config)#ip dhcp snooping disable
```

6.5.2 Enable/disable DHCP snooping (VLAN) setting

[Syntax]

ip dhcp snooping *switch*
no ip dhcp snooping

[Parameter]

switch : Setting for the DHCP snooping function of the applicable interface

Setting value	Description
enable	Enables the DHCP snooping detection function setting for the applicable interface
disable	Disables the DHCP snooping detection function setting for the applicable interface

[Initial value]

ip dhcp snooping disable

[Input mode]

interface mode

[Description]

Enables or disables the DHCP snooping function settings for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces.

To enable the DHCP snooping function, you must enable the DHCP snooping function for the entire system in addition to using this command.

Also, you must use the **ip dhcp snooping trust** command to set the port that is connected to the DHCP server.

[Example]

This enables the DHCP snooping function for VLAN1.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping enable
```

This disables the DHCP snooping function for VLAN1.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping disable
```

6.5.3 DHCP snooping port type setting

[Syntax]

ip dhcp snooping trust
no ip dhcp snooping trust

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the applicable interface as a trusted port for DHCP snooping.

If this command is executed with the "no" syntax, the setting returns to the default.

All ports are set as untrusted ports by default.

[Note]

This command can be specified only for the LAN/SFP ports and for logical interfaces.

This cannot be set for LAN/SFP ports that belong to a logical interface.

DHCP packet filtering is not performed with trusted ports, and trusted ports are set as ports to which trusted DHCP servers are connected.

DHCP packet filtering is processed for untrusted ports as follows.

- DHCP packets transmitted from the DHCP server are discarded.
- Discard IP address release requests (DHCP RELEASE) and IP address duplicate detection notifications (DHCP DECLINE) received from an interface whose MAC address is registered in the binding database and which is also different from the registered interface.
- When MAC address verification is enabled, the MAC address for the DHCP packet transmission source is compared with the client hardware database (chaddr). If the two do not match, the relevant DHCP packet is discarded.
- When Option 82 is enabled and the Option 82 information is already added to the DHCP packet received from the DHCP client, the relevant DHCP packet is discarded.

[Example]

This specifies port1.5 as a trusted port.

```
SWP2(config)#interface port1.5
SWP2(config-if)#ip dhcp snooping trust
```

6.5.4 Enable/disable setting for MAC address verification

[Syntax]

ip dhcp snooping verify mac-address *switch*
no ip dhcp snooping verify mac-address

[Parameter]

switch : MAC address verification setting

Setting value	Description
enable	Enables MAC address verification setting
disable	Disables MAC address verification setting

[Initial value]

ip dhcp snooping verify mac-address enable

[Input mode]

global configuration mode

[Description]

The MAC address for the transmission source of the DHCP packet received from an untrusted port is compared with the client hardware database (chaddr). If the two do not match, the relevant DHCP packet is discarded.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Disables MAC address verification setting.

```
SWP2(config)#ip dhcp snooping verify mac-address disable
```

6.5.5 Enable/disable Option 82 setting

[Syntax]

ip dhcp snooping information option *switch*
no ip dhcp snooping information option

[Parameter]

switch : Option 82 setting

Setting value	Description
enable	Enable setting for Option 82
disable	Disable setting for Option 82

[Initial value]

ip dhcp snooping information option enable

[Input mode]

global configuration mode

[Description]

Enables/disables the settings for adding, inspecting and deleting Option 82 information in DHCP packets.

If this command is executed with the "no" syntax, the setting returns to the default.

When Option 82 is enabled, the Option 82 information is added to DHCP packets received from the DHCP client on the untrusted port,

and the return packets are forwarded to the DHCP client from the DHCP server with the Option 82 information deleted.

The Option 82 information is as follows.

- Remote-ID
  - The MAC address of this device is added by default.
  - You can use the **ip dhcp snooping information option format remote-id** command to add a desired text string (single-byte alphanumeric characters and single-byte symbols) to the Remote-ID.
- Circuit-ID
  - The VLAN ID that received the DHCP packet from the DHCP client as well as the interface number are added by default.
  - Use the **ip dhcp snooping vlan vlan-id information option format-type circuit-id** command to change the Circuit-ID information to the VLAN ID that received the DHCP packet from the DHCP client as well as the port number.
- Subscriber-ID
  - Not added by default.
  - You can use the **ip dhcp snooping subscriber-id** command to set the desired text string for the Subscriber-ID of the applicable port.

When a DHCP packet to which Option 82 information has already been added is received, that DHCP packet is discarded.

You can use the **ip dhcp snooping information option allow-untrusted** command to permit forwarding of DHCP packets that include Option 82 information at the untrusted port.

[Example]

This disables Option 82 settings.

```
SWP2(config)#ip dhcp snooping information option disable
```

6.5.6 Settings for permitting receipt of packets on an untrusted port, including Option 82 information

[Syntax]

ip dhcp snooping information option allow-untrusted
no ip dhcp snooping information option allow-untrusted

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Enables forwarding of DHCP packets to which Option 82 information has been added at an untrusted port.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This enables forwarding of DHCP packets to which Option 82 information has been added at an untrusted port.

```
SWP2(config)#ip dhcp snooping information option allow-untrusted
```

6.5.7 Option 82 Remote-ID settings

[Syntax]

ip dhcp snooping information option format remote-id string *remoteid*
ip dhcp snooping information option format remote-id hostname
no ip dhcp snooping information option format remote-id

[Keyword]

string	:	Specifies the REMOTEID text string
hostname	:	Sets the REMOTEID host name

[Parameter]

remoteid	:	Desired text string (single-byte alphanumeric characters and single-byte symbols, 63 characters or less)

[Initial value]

None

[Input mode]

interface mode

[Description]

Lets you add a desired text string to an Option 82 Remote-ID.

Note that "?" cannot be included in the desired text string.

If this command is executed with the "no" syntax, this unit’s MAC address is added to the Remote-ID.

[Note]

This command can be specified only for VLAN interfaces.

[Example]

This lets you add desired characters to a Remote-ID.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping information option format remote-id pc1
```

6.5.8 Option 82 Circuit-ID settings

[Syntax]

ip dhcp snooping information option format-type circuit-id vlan-port
ip dhcp snooping information option format-type circuit-id string *string*
ip dhcp snooping information option format-type circuit-id vlan-ifindex
no ip dhcp snooping information option format-type circuit-id

[Keyword]

vlan-port	:	Use Circuit-ID type 0 VLAN ID, Module (stack ID), port number
string	:	Use Circuit-ID type 1 desired text string

vlan-ifindex : Use Circuit-ID type 2 VLAN ID, ifindex

[Parameter]

string : Desired text string (single-byte alphanumeric characters and single-byte symbols, 63 characters or less)

[Initial value]

ip dhcp snooping information option format-type circuit-id vlan-ifindex

[Input mode]

interface mode

[Description]

Specifies the information used for Option 82 Circuit-ID.

When "vlan-port" is specified, this adds the VLAN ID that received the DHCP packet from the DHCP client, as well as the stack number and port number.

When "string" is specified, a desired text string is added. Note that "?" cannot be included in the desired text string.

When "vlan-ifindex" is specified, this adds the VLAN ID that received the DHCP packet from the DHCP client, as well as the interface number.

If this command is executed with the "no" syntax, the setting is returned to the default.

[Note]

This command can be specified only for VLAN interfaces.

[Example]

Adds the VLAN ID that received the DHCP packet from the DHCP client to the Circuit ID, as well as the port number.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping information option format-type circuit-id vlan-port
```

6.5.9 Option 82 Subscriber-ID settings

[Syntax]

ip dhcp snooping subscriber-id *subid*
no ip dhcp snooping subscriber-id

[Parameter]

subid : Desired text string (single-byte alphanumeric characters and single-byte symbols, 50 characters or less)

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the desired text string (1–50 characters) for the Subscriber-ID of the applicable port. Note that "?" cannot be included in the text string.

If this command is executed with the "no" syntax, the Subscriber-ID is not added to the Option 82 information.

[Note]

This command can be specified only for the LAN/SFP ports and for logical interfaces.

This cannot be set for LAN/SFP ports that belong to a logical interface.

[Example]

This sets the Subscriber-ID for port1.1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#ip dhcp snooping subscriber-id a_room
```

6.5.10 DHCP packet reception rate limitation setting

[Syntax]

ip dhcp snooping limit rate *limit*
no ip dhcp snooping limit rate

[Parameter]

limit : 10 - 125
Number of DHCP packets that can be received per second (pps)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the number of DHCP packets that can be received per second (pps) for the entire system.

If this exceeds the reception rate limitation, the received DHCP packets that exceed the rate are discarded.

If this command is executed with the "no" syntax, the DHCP packet reception rate is not limited.

[Example]

This sets the DHCP packet reception rate to 100 pps for the entire system.

```
SWP2(config)#ip dhcp snooping limit rate 100
```

6.5.11 Setting to enable/disable SYSLOG output when DHCP packets are discarded

[Syntax]

ip dhcp snooping logging *switch*
no ip dhcp snooping logging

[Parameter]

switch : SYSLOG output setting when DHCP packets are discarded

Setting value	Description
enable	Outputs to SYSLOG when DHCP packets are discarded
disable	Does not output to SYSLOG when DHCP packets are discarded

[Initial value]

ip dhcp snooping logging enable

[Input mode]

global configuration mode

[Description]

Outputs the reason why DHCP packets were discarded to SYSLOG.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This outputs to SYSLOG when DHCP packets are discarded.

```
SWP2(config)#ip dhcp snooping logging enable
```

6.5.12 Show DHCP snooping system setting information

[Syntax]

show ip dhcp snooping

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows DHCP snooping system setting information.

[Example]

This shows the DHCP snooping system setting information.

```
SWP2>show ip dhcp snooping
DHCP Snooping Information for system:
  DHCP Snooping service ............. Enabled
  Option 82 insertion ............... Enabled
  Option 82 on untrusted ports ...... Disabled
  Verify MAC address ................ Enabled
  Rate limit ........................ 100 pps
  Logging ........................... Enabled
```

6.5.13 Show interface setting information for DHCP snooping

[Syntax]

show ip dhcp snooping interface

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the interface setting information for DHCP snooping.

[Example]

This shows the interface setting information for DHCP snooping.

```
SWP2>show ip dhcp snooping interface
DHCP Snooping information for vlan1:
  DHCP snooping ... Enabled
  Remote-ID ....... 00a0.de00.0001
  Circuit-ID ...... vlan-ifindex
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.1     Trusted
  port1.2     Untrusted   a_room
  port1.10    Untrusted   b_room

DHCP Snooping information for vlan2:
  DHCP snooping ... Enabled
  Remote-ID ....... yamaha
  Circuit-ID ...... vlan-port
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.3     Trusted
  port1.4     Untrusted   c_room
  port1.5     Untrusted   d_room

DHCP Snooping information for vlan3:
  DHCP snooping ... Disabled

DHCP Snooping information for vlan4:
  DHCP snooping ... Enabled
  Remote-ID ....... yamaha
  Circuit-ID ...... torakusu
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.8     Untrusted   e_room
  port1.9     Trusted
```

6.5.14 View the binding database

[Syntax]

show ip dhcp snooping binding

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows information for the entries that are registered in the binding database.

The entry information is as follows.

- VLAN ID that received a DHCP message from a DHCP client
- Information on the interface that received a DHCP message from a DHCP client
- MAC addresses of DHCP clients
- IP addresses of DHCP clients
- Lease time

[Example]

Shows the contents of the binding database.

```
SWP2>show ip dhcp snooping binding
DHCP Snooping Bindings:
Total number of bindings in database: 4

VLAN  Interface  MAC address     IP address       Expires(sec)
----  ---------  --------------  ---------------  ------------
   1  port1.1    0000.1111.2222  192.168.100.2          259170
   1  port1.2    0000.3333.4444  192.168.100.3          112000
   2  sa1        0000.5555.6666  192.168.200.2          100000
   2  port1.10   0000.7777.8888  192.168.200.3        infinite
```

6.5.15 Show DHCP snooping statistics

[Syntax]

show ip dhcp snooping statistics

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows DHCP snooping statistics.

Shows the number of received and discarded DHCP packets for each interface.

[Note]

The packets that are discarded as a result of DHCP packet reception rate limitation settings are not counted.

[Example]

Shows DHCP snooping statistics.

```
SWP2>show ip dhcp snooping statistics
DHCP Snooping Statistics:

VLAN  Interface  IN-Packets  IN-Discards
----  ---------  ----------  -----------
   1  port1.1           200          100
   1  port1.2           300            0
   1  port1.5             0            0
   2  port1.3             0            0
   2  port1.4             0            0
   2  sa1                50            2
```

6.5.16 Clear the binding database

[Syntax]

clear ip dhcp snooping binding

[Input mode]

priviledged EXEC mode

[Description]

Clears the binding database.

[Example]

This clears the binding database.

```
SWP2#clear ip dhcp snooping binding
```

6.5.17 Clear the DHCP snooping statistics

[Syntax]

clear ip dhcp snooping statistics

[Input mode]

priviledged EXEC mode

[Description]

Clears the DHCP snooping statistics.

[Example]

This clears the DHCP snooping statistics.

```
SWP2#clear ip dhcp snooping statistics
```

Chapter 7

Layer 3 functions

7.1 IPv4 address management

7.1.1 Set IPv4 address

[Syntax]

ip address *ip_address*/*mask* [secondary] [label *textline*]
ip address *ip_address netmask* [secondary] [label *textline*]
no ip address *ip_address*/*mask* [secondary]
no ip address *ip_address netmask* [secondary]
no ip address

[Keyword]

label	:	Set label as IPv4 address
secondary	:	Set as the secondary address

[Parameter]

ip_address	:	A.B.C.D
		IPv4 address
mask	:	<1-31>
		Number of mask bits
netmask	:	A.B.C.D
		Netmask in IPv4 address format
textline	:	Label (maximum 64 characters)

[Initial value]

None

[Input mode]

interface mode

[Description]

Specifies the IPv4 address and net mask for the VLAN interface.

For IPv4 addresses, one primary address and four secondary addresses can be set in one VLAN interface.

Up to 8 IPv4 addresses can be configured for the system overall.

A primary address must be set before configuring a secondary address.

If this command is executed with the "no" syntax, the specified IPv4 address is deleted. If no IPv4 address is specified, all IPv4 addresses are deleted.

You cannot delete a primary address while a secondary address is set.

If a label is specified, it is shown in the "IPv4 address" field by the **show interface** command.

[Note]

It is not possible to assign an IPv4 address of the same subnet to multiple interfaces.

[Example]

Specify 192.168.1.100 as the IP address for VLAN #1.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip address 192.168.1.100/24
```

7.1.2 Show IPv4 address

[Syntax]

show ip interface [*interface*] **brief**

[Parameter]

interface : VLAN interface name

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv4 address for each interface.

The following content is shown.

- IPv4 address
  - For secondary addresses, “(secondary)” is appended to the end of IPv4 addresses.
  - If an IPv4 address has been specified by the **ip address dhcp** command, an "*" is shown added before the displayed IPv4 address.
  - If the IPv4 address is not specified after setting the **ip address dhcp** command (such as while searching for the server), then "searching" is shown.
  - If the **ip address** command has not been set, the indication "unassigned" is shown.
- Physical layer status
- Data link layer status

If an interface is specified, information for that interface is shown. If the interface is omitted, information is shown for all interfaces for which an IPv4 address can be specified.

[Note]

An error occurs if the specified interface is one to which an IP address cannot be assigned.

[Example]

Show the IP address of every VLAN interface.

```
SWP2>show ip interface brief
Interface      IP-Address                      Admin-Status          Link-Status
vlan1          192.168.1.100/24
               192.168.101.100/24 (secondary)  up                    up
vlan2          192.168.2.100/24                up                    down
vlan3          unassigned                      up                    down
```

7.1.3 Automatically set IPv4 address by DHCP client

[Syntax]

ip address dhcp [hostname *hostname*]
no ip address

[Keyword]

hostname : Set host name of DHCP server

[Parameter]

hostname : Host name or IPv4 address (A.B.C.D)

[Initial value]

none

[Input mode]

interface mode

[Description]

Using the DHCP client, assigns the IPv4 address granted by the DHCP server to the VLAN interface.

If the DHCP server is specified, the HostName option (option code 12) can be added to the Discover/Request message.

If an IPv4 address has been obtained, you can execute the **no ip address** command to send a release message for the obtained IP address to the DHCP server.

A secondary address cannot be set for interfaces that are set as DHCP clients.

If this command is executed with the "no" syntax, the DHCP client setting is deleted.

[Note]

The lease time requested from the DHCP server is fixed at 72 hours. However, the actual lease time will depend on the setting of the DHCP server.

Even if this command is used to obtain the default gateway, DNS server, and default domain name from the DHCP server, the settings of the **ip route, dns-client name-server, dns-client domain-name** commands take priority.

If an IPv4 address cannot be obtained from the DHCP server even by using this command, then an IPv4 link local address (169.254.xxx.xxx/16) is automatically assigned only to VLAN interfaces for which the Auto IP function is enabled.

[Example]

Use the DHCP client to assign an IPv4 address to VLAN #100.

```
SWP2(config)#interface vlan100
SWP2(config-if)#ip address dhcp
```

7.1.4 Show DHCP client status

[Syntax]

show dhcp lease

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the DHCP client status. The following items are shown.

- Interface that is operating as a DHCP client
- Assigned IPv4 address
- Lease expiration time
- Lease renewal request time
- Lease rebinding time
- DHCP server name
- Information obtained as DHCP options
  - Net mask
  - Default gateway
  - Lease time
  - DNS server
  - DHCP server ID
  - Domain name

[Note]

[Example]

Show the current DHCP client status.

```
SWP2>show dhcp lease
Interface vlan1
-------------------------------------------------------------------------------
IP Address:                   192.168.100.2
Expires:                      2018/01/01 00:00:00
Renew:                        2018/01/01 00:00:00
Rebind:                       2018/01/01 00:00:00
Server:
Options:
  subnet-mask                 255.255.255.0
  default-gateway             192.168.100.1
  dhcp-lease-time             259200
  domain-name-servers         192.168.100.1
  dhcp-server-identifier      192.168.100.1
  domain-name                 example.com
```

7.1.5 Set auto IP function

[Syntax]

auto-ip *switch*

no auto-ip

[Parameter]

switch : Behavior of the auto IP function

Setting value	Description
enable	Enable the auto IP function
disable	Disable the auto IP function

[Initial value]

auto-ip disable

[Input mode]

interface mode

[Description]

For the VLAN interface, enables the Auto IP function which automatically generates the IPv4 link local address (169.254.xxx.xxx/16).

The Auto IP function works only if an IPv4 address cannot be obtained from the DHCP server after the **ip address dhcp** command is specified.

The Auto IP function can be enabled for only one VLAN interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If an IPv4 address could be obtained from the DHCP server after the IPv4 link local address was determined, the IPv4 link local address is discarded, and the IPv4 address obtained from the DHCP server is used.

[Example]

Enable the Auto IP function for VLAN #2.

```
SWP2(config)#interface vlan2
SWP2(config-if)#auto-ip enable
```

7.2 IPv4 route control

7.2.1 Set static IPv4 route

[Syntax]

ip route *ip_address*/*mask gateway* [*number*]
ip route *ip_address*/*mask* null [*number*]
ip route *ip_address netmask gateway* [*number*]
ip route *ip_address netmask* null [*number*]
no ip route *ip_address*/*mask* [*gateway* [*number*]]
no ip route *ip_address*/*mask* [null [*number*]]
no ip route *ip_address netmask* [*gateway* [*number*]]
no ip route *ip_address netmask* [null [*number*]]

[Keyword]

null : Discard packet without forwarding it

[Parameter]

ip_address : A.B.C.D

IPv4 address

Set this to 0.0.0.0 if specifying the default gateway

mask : <1-31>

Number of mask bits

Set this to 0 if specifying the default gateway

netmask : A.B.C.D

Netmask in address format

Set this to 0.0.0.0 if specifying the default gateway

gateway : A.B.C.D

IPv4 address of gateway

number : <1-255>

Administrative distance (priority order when selecting route) (if omitted: 1)

Lower numbers have higher priority.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a static route for IPv4.

If this command is executed with the "no" syntax, the specified route is deleted.

[Example]

Set the default gateway to 192.168.1.1.

```
SWP2(config)#ip route 0.0.0.0/0 192.168.1.1
```

For the destination 172.16.0.0/16, set the gateway to 192.168.2.1.

```
SWP2(config)#ip route 172.16.0.0 255.255.0.0 192.168.2.1
```

7.2.2 Show IPv4 Forwarding Information Base

[Syntax]

show ip route [*ip_address*[/*mask*]]

[Parameter]

ip_address : A.B.C.D

IPv4 address

mask : <0-32>

Number of mask bits (if omitted: 32)

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv4 Forwarding Information Base (FIB).

If the IPv4 address is omitted, the entire content of the FIB is shown.

If the IPv4 address or network address is specified, detailed information for the routing entry that matches the destination is shown.

[Example]

Show the entire IPv4 forwarding information base.

```
SWP2>show ip route
Codes: C - connected, S - static
       * - candidate default

Gateway of last resort is 192.168.100.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.100.1, vlan1
S       172.16.0.0/16 [1/0] via 192.168.200.240, vlan100
S       192.168.1.1/32 [1/0] is directly connected, vlan100
C       192.168.100.0/24 is directly connected, vlan1
C       192.168.200.0/24 is directly connected, vlan100
```

Show the route used for sending packets that are addressed to 192.168.100.10.

```
SWP2>show ip route 192.168.100.10
Routing entry for 192.168.100.0/24
  Known via "connected", distance 0, metric 0, best
  * is directly connected, vlan1
```

7.2.3 Show IPv4 Routing Information Base

[Syntax]

show ip route database

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv4 Routing Information Base (RIB).

[Example]

Show the IPv4 routing information base.

```
SWP2>show ip route database
Codes: C - connected, S - static
       > - selected route, * - FIB route

S    *> 0.0.0.0/0 [1/0] via 192.168.100.1, vlan1
S    *> 172.16.0.0/16 [1/0] via 192.168.200.240, vlan100
S    *> 192.168.1.1/32 [1/0] is directly connected, vlan100
C    *> 192.168.100.0/24 is directly connected, vlan1
C    *> 192.168.200.0/24 is directly connected, vlan100

Gateway of last resort is not set
```

7.2.4 Show summary of the route entries registered in the IPv4 Routing Information Base

[Syntax]

show ip route summary

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows a summary of the route entries that are registered in the IPv4 Routing Information Base (RIB).

[Example]

Show a summary of the route entries that are registered in the IPv4 Routing Information Base.

```
SWP2>show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 1
Route Source    Networks
connected       2
static          3
Total           5
```

7.3 ARP

7.3.1 Show ARP table

[Syntax]

show arp

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the ARP cache.

[Example]

Show the ARP cache.

```
SWP2>show arp
 IP Address      MAC Address   Interface  Type
192.168.100.10  00a0.de00.0000 vlan1    dynamic
192.168.100.100 00a0.de00.0001 vlan1    static
```

7.3.2 Clear ARP table

[Syntax]

clear arp-cache

[Input mode]

priviledged EXEC mode

[Description]

Clears the ARP cache.

[Example]

Clear the ARP cache.

```
SWP2#clear arp-cache
```

7.3.3 Set static ARP entry

[Syntax]

arp *ip_address mac_address interface*
no arp *ip_address*

[Parameter]

ip_address	:	A.B.C.D
		IP address
mac_address	:	HHHH.HHHH.HHHH
		MAC address
interface	:	portN.M
		Physical interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Creates a static group ARP entry.

If this command is executed with the "no" syntax, the specified entry is deleted.

[Example]

Create a static ARP entry of IP address 192.168.100.100 and MAC address 00a0.de00.0000 connected to port1.1.

```
SWP2(config)#arp 192.168.100.100 00a0.de00.0000 port1.1
```

7.3.4 Set ARP timeout

[Syntax]

arp-ageing-timeout *time*
no arp-ageing-timeout [*time*]

[Parameter]

time	:	<1-3000>
		ARP entry ageing timeout (seconds)

[Initial value]

arp-ageing-timeout 300

[Input mode]

interface mode

[Description]

Changes the length of time that ARP entries are maintained in the applicable VLAN interface. ARP entries that are not received within this length of time are deleted.

If this command is executed with the "no" syntax, the ARP entry timeout is set to 300 seconds.

[Example]

Change the ARP entry ageing timeout for VLAN #1 to ten minutes.

```
SWP2(config)#interface vlan1
SWP2(config)#arp-aging-timeout 600
```

7.3.5 ARP request transmission method settings during ARP timeout

[Syntax]

arp-ageing-timeout request *mode*
no arp-ageing-timeout request

[Parameter]

mode : ARP request transmission method

Setting value	Description
unicast	Transmits ARP request that is transmitted during ARP timeout, via unicast
broadcast	Transmits ARP request that is transmitted during ARP timeout via broadcast

[Initial value]

arp-ageing-timeout request unicast

[Input mode]

interface mode

[Description]

Sets the ARP request method that is transmitted when the ARP entry timeout has expired for the target VLAN interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Transmits the ARP request that is transmitted when ARP entry timeout for VLAN #1 has expired, via broadcast.

```
SWP2(config)#interface vlan1
SWP2(config)#arp-aging-timeout request broadcast
```

7.4 IPv4 forwarding control

7.4.1 IPv4 forwarding settings

[Syntax]

ip forwarding *switch*
no ip forwarding [*switch*]

[Parameter]

switch : IPv4 packet forwarding settings

Setting value	Description
enable	Enable forwarding of IPv4 packets
disable	Disable forwarding of IPv4 packets

[Initial value]

ip forwarding disable

[Input mode]

global configuration mode

[Description]

Enables or disables forwarding of IPv4 packets.

If this is executed with the "no" syntax, the setting returns to the default.

7.4.2 Show IPv4 forwarding settings

[Syntax]

show ip forwarding

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv4 packet forwarding settings.

[Example]

Shows the IPv4 packet forwarding settings.

```
SWP2>show ip forwarding
IP forwarding is on
```

7.4.3 MTU setting

[Syntax]

mtu *mtu*
no mtu

[Parameter]

mtu : <68-9216>
Maximum packet size that can be transmitted

[Initial value]

mtu 1500

[Input mode]

interface mode

[Description]

Sets the maximum value (MTU) for the size of packets that can be transmitted from the VLAN interface.

Eligible packets are those which are transmitted from this product, as well as those which are L3 forwarded (routing). Ethernet frames that are L2 forwarded by this product are not eligible.

When L3 forwarding packets for which the total length of the IPv4 header exceeds the MTU value, the packets are IP fragmented and then transmitted.

When L3 forwarding packets for which the payload length of the IPv6 header exceeds the MTU value, an ICMPv6 error is sent back and the packets are discarded.

Since packets that fit into the Ethernet frame length set by the mru command are eligible for routing, you must use the mru command to adjust the length of Ethernet frames that can be received when routing jumbo frames.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interface.

You can specify up to seven different values for the MTU besides the default value.

On VLAN interfaces for which ipv6 enable has been specified, the MTU can be set within a range of <1280-9216>.

You cannot specify the ipv6 enable command for a VLAN interface that is set to an MTU value less than 1280.

[Example]

This allows jumbo frames of up to 10240 bytes between the LAN port #1 belonging to VLAN interface #1 and the LAN port #2 belonging to VLAN interface #2, and sets the MTU to 2000 bytes.

```
SWP2(config)#interface port1.1-2
SWP2(config-if)#mru 10240
SWP2(config-if)#interface vlan1-2
SWP2(config-if)#mtu 2000
```

7.5 IPv4 ping

7.5.1 IPv4 ping

[Syntax]

ping *host* [repeat *count*] [size *datalen*] [timeout *timeout*] [source *ip_address*]

[Keyword]

repeat	:	Specifies the number of times to execute
size	:	Specifies the length of the ICMP payload (byte units)
timeout	:	Specifies the time to wait for a reply after transmitting the specified number of Echo requests
source	:	Sets the source address for ICMP packets

[Parameter]

host : Target to which ICMP Echo is sent

Host name, or target IP address (A.B.C.D)

count : Number of times to execute (if omitted: 5)

Setting value	Description
<1-2147483647>	Execute the specified number of times
continuous	Execute repeatedly until Ctrl+C is entered

datalen : <36-18024>

Length of the ICMP payload (if omitted: 56)

timeout : <1-65535>

Time to wait for a reply (if omitted: 2)

This is ignored if the number of times to execute is specified as "continuous"

ip_address : A.B.C.D

IPv4 address

[Input mode]

priviledged EXEC mode

[Description]

Send ICMP Echo to the specified host, and wait for ICMP Echo Reply.

If there is a reply, show it. Show statistical information when the command ends.

[Example]

Ping the IP address 192.168.100.254 three times with a data size of 120 bytes.

```
SWP2#ping 192.168.100.254 repeat 3 size 120
PING 192.168.100.254 (192.168.100.254): 120 data bytes
128 bytes from 192.168.100.254: seq=0 ttl=255 time=8.368 ms
128 bytes from 192.168.100.254: seq=1 ttl=255 time=9.946 ms
128 bytes from 192.168.100.254: seq=2 ttl=255 time=10.069 ms

--- 192.168.100.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 8.368/9.461/10.069 ms
```

7.5.2 Check IPv4 route

[Syntax]

traceroute *host*

[Parameter]

host : Destination for which to check the route

Host name, or target IP address (A.B.C.D)

[Input mode]

priviledged EXEC mode

[Description]

Shows information for the route to the specified host.

[Example]

Check the route to 192.168.100.1.

```
SWP2#traceroute 192.168.100.1
traceroute to 192.168.100.1 (192.168.100.1), 30 hops max
 1  192.168.10.1 (192.168.10.1)  0.563 ms  0.412 ms  0.428 ms
 2  192.168.20.1 (192.168.20.1)  0.561 ms  0.485 ms  0.476 ms
 3  192.168.30.1 (192.168.30.1)  0.864 ms  0.693 ms  21.104 ms
 4  192.168.40.1 (192.168.40.1)  0.751 ms  0.783 ms  0.673 ms
 5  192.168.50.1 (192.168.50.1)  7.689 ms  7.527 ms  7.168 ms
 6  192.168.100.1 (192.168.100.1)  33.948 ms  10.413 ms  7.681 ms
```

7.6 IPv6 address management

7.6.1 Set IPv6

[Syntax]

ipv6 *switch*

no ipv6

[Parameter]

switch : Behavior of the IPv6

Setting value	Description
enable	Enable the IPv6
disable	Disable the IPv6

[Initial value]

ipv6 disable

[Input mode]

interface mode

[Description]

Enables IPv6 for the VLAN interface and automatically sets the link local address.

IPv6 addresses can be assigned to a maximum of 8 VLAN interfaces.

If IPv6 is disabled, related settings are also simultaneously deleted.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The automatically-specified link local address can be viewed by using the **show ipv6 interface brief** command.

[Example]

Enable IPv6 for VLAN #1.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 enable
```

7.6.2 Set IPv6 address

[Syntax]

ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
prefix_len	:	<0-127> IPv6 prefix length

[Input mode]

interface mode

[Description]

Specifies the IPv6 address and prefix length for the VLAN interface.

An IPv6 address can be set for a VLAN interface for which the **ipv6 enable** command has been set.

This command can be used with the **ipv6 address autoconfig**, **ipv6 address dhcp** and **ipv6 address pd** commands.

For IPv6 addresses, up to five global addresses (including RA settings, DHCPv6 clients and the settings for IPv6 addresses that use DHCPv6-PD) and one link local address can be set in one VLAN interface.

Up to 8 IPv6 addresses can be configured for the system overall (excepting link local addresses that are automatically assigned).

If this command is executed with the "no" syntax, the specified IPv6 address is deleted. If no IPv6 address is specified, all IPv6 addresses (including RA settings, DHCPv6 clients and the settings for IPv6 addresses that use DHCPv6-PD) are deleted.

[Note]

It is not possible to assign an IPv6 address of the same subnet to multiple interfaces.

[Example]

Specify 2001:db8:1::2 as the IPv6 address for VLAN #1.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 address 2001:db8:1::2/64
```

7.6.3 Set RA for IPv6 address

[Syntax]

ipv6 address autoconfig [stateless]
no ipv6 address autoconfig

[Keyword]

stateless	:	Operates a stateless DHCPv6.

[Initial value]

none

[Input mode]

interface mode

[Description]

Uses RA to specify an IPv6 address for the VLAN interface.

RA can be specified only for the VLAN interface for which the **ipv6 enable** command has been specified.

This command can be used with the **ipv6 address** and **ipv6 address pd** commands.

This cannot be set for VLAN interface that has already been set using the **ipv6 address dhcp** or **dhcpv6-server** commands (only for models that support a DHCPv6 server).

If an RA with a valid router lifetime is received after enabling this command, the address of the device that transmitted the RA is added to the default gateway.

Also, if an RA with a router lifetime of "0" is received, the address of the device that transmitted the RA is deleted from the default gateway.

However, if the **ipv6 nd accept-ra-default-routes disable** command has been set, nothing is added to the default gateway based on the RA.

If "stateless" is specified, a DHCPv6 "Information-request" is sent and the unit operates in DHCPv6 stateless mode.

If "stateless" is specified, this cannot be set for a VLAN interface for which the **ipv6 dhcp client pd** command has already been set.

Only one DHCPv6 stateless can be set for one VLAN interface.

This command for which "stateless" has been specified can be set for a maximum of 8 VLAN interface.

If you overwrite the **ipv6 address autoconfig stateless** command after setting it with the **ipv6 address autoconfig** command, the DHCPv6 stateless mode is stopped.

If this command is executed with the "no" syntax, the RA setting is deleted.

[Note]

If "stateless" is specified regardless of whether the received RA "O" flag is on or off, DHCPv6 stateless operations are enabled.

This requests "OPTION_DNS_SERVERS" (option code 23) and "OPTION_DOMAIN_LIST" (option code 24) to the DHCPv6 server during stateless operations.

When multiple options are returned from the DHCPv6 server, up to three can be obtained for a DNS server and up to six can be obtained for a domain list.

You can use the **show ipv6 dhcp interface** to confirm the DNS servers or domain lists obtained due to requests made when operating in stateless mode.

If there is no period (dot) at the end of the domain name of a domain list that was obtained, "." is appended.

Even when this command is used to obtain the DNS server or query domain list from the DHCPv6 server, the settings of the **dns-client name-server** and **dns-client domain-list** commands take priority.

You can use the **show dns-client** command to confirm the DNS servers or domain lists configured in the system.

[Example]

Use RA to set the IPv6 address for VLAN #1.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 address autoconfig
```

7.6.4 Set dynamic IPv6 addresses with a DHCPv6 client

[Syntax]

ipv6 address dhcp
no ipv6 address dhcp

[Initial value]

None

[Input mode]

interface mode

[Description]

Using the DHCPv6 client, this sets the IPv6 address granted by the DHCPv6 server for the VLAN interface.

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

Only one address can be set with this command for one VLAN interface.

This command can be used with the **ipv6 address** and **ipv6 address pd** commands.

This command can be specified for a maximum of eight VLAN interface.

This cannot be set for VLAN interface that has already been set using the **ipv6 dhcp client pd**, **ipv6 address autoconfig** or **dhcpv6-server** commands (only for models that support a DHCPv6 server).

If an IPv6 address has been obtained, you can execute the **no ipv6 address dhcp** command to send a release message for the obtained IPv6 address to the DHCPv6 server.

If this command is executed with the "no" syntax, the DHCPv6 client setting is deleted.

If the **ipv6** command is set to "disable", this command is also deleted.

[Note]

If the IPv6 address is automatically set using this command, the prefix length is set to "/128".

If this command is set regardless of whether the received RA "M" flag is on or off, DHCPv6 stateful operations (IA_NA) are enabled.

The DHCPv6 client requests "OPTION_DNS_SERVERS" (option code 23) and "OPTION_DOMAIN_LIST" (option code 24) to the DHCPv6 server.

When multiple options are returned from the DHCPv6 server, up to three can be obtained for a DNS server and up to six can be obtained for a domain list.

You can use the **show ipv6 dhcp interface** command to confirm the DNS servers or domain lists obtained due to requests made by the DHCPv6 client.

If there is no period (dot) at the end of the domain name of a domain list that was obtained, "." is appended.

Even when this command is used to obtain the DNS server or query domain list from the DHCPv6 server, the settings of the **dns-client name-server** and **dns-client domain-list** commands take priority.

You can use the **show dns-client** command to confirm the DNS servers or domain lists configured in the system.

If an RA with a valid router lifetime is received after enabling this command, the address of the device that transmitted the RA is added to the default gateway.

Also, if an RA with a router lifetime of "0" is received, the address of the device that transmitted the RA is deleted from the default gateway.

However, if the **ipv6 nd accept-ra-default-routes disable** command has been set, nothing is added to the default gateway based on the RA.

[Example]

This assigns an IPv6 address to VLAN #100 via the DHCPv6 client.

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 address dhcp
```

7.6.5 Set an IPv6 address using DHCPv6-PD

[Syntax]

ipv6 address pd *pd_prefixname pd_ipv6_address*/*prefix_len*
no ipv6 address pd *pd_prefixname pd_ipv6_address*/*prefix_len*

[Parameter]

pd_prefixname	:	Prefix name set on the DHCPv6-PD client (ipv6 dhcp client pd command)
		Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores
pd_ipv6_address	:	X:X::X:X
		IPv6 address based on prefix obtained from DHCPv6-PD client
		Sets the lower level (remaining) portion for the prefix obtained from a DHCPv6-PD client
		"0" must be specified for the prefix obtained from DHCPv6-PD client
prefix_len	:	<0-127>
		IPv6 prefix length

[Initial value]

None

[Input mode]

interface mode

[Description]

Specifies the IPv6 address and prefix length for the VLAN interface.

An IPv6 address can be set for a VLAN interface for which the **ipv6 enable** command has been set.

This generates an IPv6 address based on the prefix obtained using the DHCPv6-PD client function.

The generated IPv6 address can be checked by using the **show ipv6 interface** command.

This command can be used with the **ipv6 address**, **ipv6 address autoconfig** and **ipv6 address dhcp** commands.

For IPv6 addresses, up to five global addresses (including RA settings and DHCPv6 client) and one link local address can be set in one VLAN interface.

Up to 8 IPv6 addresses can be configured for the system overall (excepting link local addresses that are automatically assigned).

If this command is executed with the "no" syntax, the specified IPv6 address is deleted.

[Note]

If prefix information cannot be obtained via the DHCPv6-PD client function, the IPv6 address is not generated.

The IPv6 address is not generated if the combination of the prefix information and lower (host) part of the address is incorrect, or if the subnet is duplicated across interfaces.

[Example]

This obtains the IPv6 prefix for VLAN #100 via the DHCPv6-PD client.

The prefix name "PD_VLAN100" that was obtained is used to set the IPv6 address for VLAN #200.

In this example, we assume that "2001:db8:1:aaf0::/60" is obtained with "PD_VLAN100".

The following settings are used to set "2001:db8:1:aaf2::1/64" for VLAN #200.

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 dhcp client pd PD_VLAN100
SWP2(config)#interface vlan200
SWP2(config-if)#ipv6 address pd PD_VLAN100 ::2:0:0:0:1/64
```

7.6.6 Set DHCPv6-PD client

[Syntax]

ipv6 dhcp client pd *prefixname*
no ipv6 dhcp client pd

[Parameter]

prefixname	:	Internal name attached to assigned prefix Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores

[Initial value]

None

[Input mode]

interface mode

[Description]

Enables the DHCPv6-PD client function on the applicable interface, and configures the client to request prefix assignments.

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

The prefix obtained using the *prefixname* of this command can be used as shown below.

- Use the prefix obtained with the **ipv6 address pd** command to set a IPv6 address.
- Use the prefix obtained with the **range** command in DHCPv6 mode to set an IPv6 address range for dynamic assignment on a DHCPv6 server. (Only for models that support a DHCPv6 server.)
- Use the prefix obtained with the **prefix-delegation** command in DHCPv6 mode to reassign a prefix on a DHCPv6 server. (Only for models that support a DHCPv6 server.)

Only one address can be set with this command for one VLAN interface.

This command can be specified for a maximum of eight VLAN interface.

This cannot be set for a VLAN interface that has already been set using the **ipv6 address dhcp**, **ipv6 address autoconfig stateless** or **dhcpv6-server** commands (only for models that support a DHCPv6 server).

If an IPv6 prefix has been obtained, you can execute the **no ipv6 dhcp client pd** command to send a release message for the obtained prefix to the DHCPv6 server.

If this command is executed with the "no" syntax, the DHCPv6-PD client setting is deleted.

If the **ipv6** command is set to "disable", this command is also deleted.

[Note]

If this command is set regardless of whether the received RA "M" flag is on or off, DHCPv6-PD stateful operations (IA_PD) are enabled.

The DHCPv6-PD client requests "OPTION_DNS_SERVERS" (option code 23) and "OPTION_DOMAIN_LIST" (option code 24) to the DHCPv6 server.

When multiple options are returned from the DHCPv6 server, up to three can be obtained for a DNS server and up to six can be obtained for a domain list.

You can use the **dns-server** and **domain-name** commands in DHCPv6 mode for DNS servers and domain lists obtained by a DHCPv6-PD client. (Only for models that support a DHCPv6 server.)

You can use the **show ipv6 dhcp interface** command to confirm the DNS servers or domain lists obtained due to requests made by the DHCPv6-PD client.

If there is no period (dot) at the end of the domain name of a domain list that was obtained, "." is appended.

Even when this command is used to obtain a DNS server or query domain list from the DHCPv6-PD server, the settings of the **dns-client name-server** and **dns-client domain-list** commands take priority.

You can use the **show dns-client** command to confirm the DNS servers or domain lists configured in the system.

If an RA with a valid router lifetime is received after enabling this command, the address of the device that transmitted the RA is added to the default gateway.

Also, if an RA with a router lifetime of "0" is received, the address of the device that transmitted the RA is deleted from the default gateway.

However, if the **ipv6 nd accept-ra-default-routes disable** command has been set, nothing is added to the default gateway based on the RA.

[Example]

This obtains the IPv6 prefix for VLAN #100 via the DHCPv6-PD client.

The prefix name "PD_VLAN100" that was obtained is used to set the IPv6 address for VLAN #200.

In this example, we assume that "2001:db8:1:aaf0::/60" is obtained with "PD_VLAN100".

The following settings are used to set "2001:db8:1:aaf2::1/64" for VLAN #200.

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 dhcp client pd PD_VLAN100
SWP2(config)#interface vlan200
SWP2(config-if)#ipv6 address pd PD_VLAN100 ::2:0:0:0:1/64
```

7.6.7 Set automatic registration of default gateway using RA

[Syntax]

ipv6 nd accept-ra-default-routes *switch*
no ipv6 nd accept-ra-default-routes

[Parameter]

switch : Settings for automatic registration of default gateway using RA

Setting value	Description
enable	Enable setting of automatic registration for the default gateway using RA
disable	Disable setting of automatic registration for the default gateway using RA

[Initial value]

ipv6 nd accept-ra-default-routes enable

[Input mode]

interface mode

[Description]

Enables/disables the setting of automatic registration of a IPv6 default gateway, based on the starting address of the router advertisement (RA) received by the applicable interface.

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

If this command is executed with the "no" syntax, the setting returns to the default value.

If the **ipv6** command is set to "disable", this command is also deleted.

[Note]

If an RA was received when the **ipv6 address dhcp**, **ipv6 dhcp client pd** or **ipv6 address autoconfig** command was set, the setting for this command takes priority.

If these commands have not been set, default gateways are not automatically registered, even if this command is set to "enable".

[Example]

Disables setting of automatic registration for the default gateway using RA on VLAN #100.

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 nd accept-ra-default-routes disable
```

7.6.8 Show IPv6 address

[Syntax]

show ipv6 interface [*interface*] **brief**

[Parameter]

interface : VLAN interface name

Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv6 address for each interface.

- IPv6 address
  - If an IPv6 address has been dynamically specified by the **ipv6 address dhcp** command, an asterisk is shown added before the displayed IPv6 address.
  - If the IPv6 address is not specified after setting the **ipv6 address dhcp** command (such as while searching for the server), "searching" is shown.
  - If the address uses *pd_prefixname* as set by the **ipv6 address pd** command, an asterisk is shown added before the displayed IPv6 address.
  - If an IPv6 address has not been set, this will be "unassigned."
- Physical layer status
- Data link layer status

If an interface is specified, information for that interface is shown. If the interface is omitted, information is shown for all interfaces for which an IPv6 address is specified.

[Note]

An error occurs if the specified interface is one to which an IPv6 address cannot be assigned.

[Example]

Show the IPv6 address for all VLAN interface.

```
SWP2>show ipv6 interface brief
Interface        IPv6-Address                                Admin-Status
Link-Status
vlan1            2001:db8:1::2/64
                 2001:db8:2::2/64
                 fe80::2a0:deff:fe:2/64                      up                      up
vlan2            2001:db8:2::2/64
                 fe80::2a0:deff:fe:2/64                      up
down
vlan3            unassigned                                  up
down
```

7.6.9 Show DHCPv6 client status

[Syntax]

show ipv6 dhcp interface [*ifname*]

[Parameter]

ifname : VLAN interface name

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the DHCPv6 client status.

If *ifname* is not specified, this shows information for all VLAN interface.

[Note]

[Example]

Shows the DHCPv6 client status for all VLAN interface.

```
SWP2#show ipv6 dhcp interface
Interface vlan1
  Client Type        : IA_NA
  Address            : 2001:db8:1:aa10::dd2d
  IAID               : 0f28924a
  DUID               : 000100010000000000a0de000000
  preferred lifetime : 604800
  valid lifetime     : 2592000
  expires            : 2023/4/19 07:25:48

Interface vlan2
  Client Type        : Stateless
  DUID               : 000100012ce737dbac44f284efdd
  DNS Server         : 2001:db8:1:bb10::100
  DNS Server         : 2001:db8:1:bb10::200
  Domain Name        : example.com.

Interface vlan100
  Client Type        : IA_PD
  Prefix name        : PD_VLAN100
  prefix             : 2001:db8:1:aaf0::/60
  IAID               : 0f28924a
  DUID               : 000100010000000000a0de000000
  preferred lifetime : 604800
  valid lifetime     : 2592000
  expires            : 2023/4/19 08:08:04
  DNS Server         : 2001:db8:2::100
  DNS Server         : 2001:db8:2::200
  Domain Name        : example.com.
```

7.6.10 Reset DHCPv6 client

[Syntax]

clear ipv6 dhcp client *ifname*

[Parameter]

ifname : VLAN interface name

[Input mode]

priviledged EXEC mode

[Description]

Clears the DHCPv6 client that's operating on the applicable interface.

When you execute this command, the DHCPv6 information that was acquired on the applicable interface is erased.

At this time, release messages acquired for the IPv6 address are sent to the DHCPv6 server.

After this, the request to the DHCPv6 server is transmitted again, to make the settings again for the DHCPv6 client.

When using a DHCPv6-PD client, if the prefix acquired via the **ipv6 address pd** command is used,the interface address that was set is configured again.

When the information acquired via the DHCPv6 mode **range** command, **prefix-delegation** command, **dns-server** command or **domain-name** command by means of the DHCPv6 server function is used, the DHCPv6 server function is also reconfigured. (Only for models that support a DHCPv6 server.)

[Note]

[Example]

Clears the DHCPv6 client for VLAN #100.

```
SWP2#clear ipv6 dhcp client vlan100
```

7.6.11 Set ND prefix received when configuring a DHCPv6 client

[Syntax]

ipv6 dhcp client nd-prefix *prefix_len*
no ipv6 dhcp client nd-prefix

[Parameter]

prefix_len : <1-127>

Length of ND prefix received

[Initial value]

None

[Input mode]

interface mode

[Description]

For a VLAN interface on which an IPv6 address (prefix /128) is automatically set via the **ipv6 address dhcp** command, all ND (Neighbor Discovery) packets are received regardless of the IPv6 address from which they are transmitted.

When this command is set, both addresses listed below are compared within the set prefix range when the ND packets are received. For identical segments, the ND packet is received. For differing segments, the ND packet is discarded.

- IPv6 addresses automatically configured via the **ipv6 address dhcp** command
- Source IPv6 addresses for ND packets received

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

The ND packets targeted by this command are limited to NS (Neighbor Solicitation) and NA (Neighbor Advertisement).

If this command is executed with the "no" syntax, the ND prefix received when the DHCPv6 client is set is deleted.

[Note]

This only works for a VLAN interface on which an IPv6 address (prefix /128) is automatically set via the **ipv6 address dhcp** command.

[Example]

This allows the receipt of only ND packets from subnet /64, on VLAN #1 for which an IPv6 address has been set automatically via the **ipv6 address dhcp** command.

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 dhcp client nd-prefix 64
```

7.7 IPv6 route control

7.7.1 Set IPv6 static route

[Syntax]

ipv6 route *ipv6_address*/*prefix_len gateway* [*number*]
ipv6 route *ipv6_address*/*prefix_len* null [*number*]
no ipv6 route *ipv6_address*/*prefix_len* [*gateway* [*number*]]
no ipv6 route *ipv6_address*/*prefix_len* [null [*number*]]

[Keyword]

null : Discard packet without forwarding it

[Parameter]

ipv6_address : X:X::X:X

IPv6 address

Set this to :: (abbreviated 0:0:0:0:0:0:0:0) if specifying the default gateway

prefix_len : <1-127>

IPv6 prefix

Set this to 0 if specifying the default gateway

gateway : X:X::X:X

IPv6 address of gateway

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

number : <1-255>

Management route (priority order when selecting route) (if omitted: 1)

Lower numbers have higher priority.

[Input mode]

global configuration mode

[Description]

Adds a static route for IPv6.

If this command is executed with the "no" syntax, the specified route is deleted.

[Note]

For the default gateway setting, the static route setting takes priority over the RA setting.

[Example]

For the destination 2001:db8:2::/64, set the gateway to 2001:db8:1::1.

```
SWP2(config)#ipv6 route 2001:db8:2::/64 2001:db8:1::1
```

Set the default gateway to fe80::2a0:deff:fe:1 on VLAN #1.

```
SWP2(config)#ipv6 route ::/0 fe80::2a0:deff:fe:1%vlan1
```

7.7.2 Show IPv6 Forwarding Information Base

[Syntax]

show ipv6 route [*ipv6_address*[/*prefix_len*]]

[Parameter]

ipv6_address : X:X::X:X

IPv6 address

mask : <0-128>

IPv6 prefix length (if omitted: 128)

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv6 Forwarding Information Base (FIB).

If the IPv6 address is omitted, the entire content of the FIB is shown.

If the IPv6 address or network address is specified, detailed information for the routing entry that matches the destination is shown.

[Note]

[Example]

Show the entire IPv6 forwarding information base.

```
SWP2>show ipv6 route
Codes: C - connected, S - static
Timers: Uptime

S      ::/0 [1/0] via fe80::2a0:deff:fe:1, vlan1, 00:03:08
C      2001:db8:1::/64 via ::, vlan1, 00:01:10
S      2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan1, 00:01:52
C      fe80::/64 via ::, vlan1, 00:03:08
```

Show the route used for sending packets that are addressed to 2001:db8:1::2.

```
SWP2>show ipv6 route 2001:db8:1::2
Routing entry for 2001:db8:1::/64
  Known via "connected", distance 0, metric 0, best
  Last update 00:18:27 ago
  * directly connected, vlan1
```

7.7.3 Show IPv6 Routing Information Base

[Syntax]

show ipv6 route database

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv6 Routing Information Base (RIB).

[Note]

[Example]

Show the IPv6 routing information base.

```
SWP2>show ipv6 route database
Codes: C - connected, S - static
       > - selected route, * - FIB route
Timers: Uptime

S   *> ::/0 [1/0] via fe80::2a0:deff:fe:1, vlan1, 00:21:39
C   *> 2001:db8:1::/64 via ::, vlan1, 00:19:41
S   *> 2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan1, 00:20:23
C   *> fe80::/64 via ::, vlan1, 00:21:39
```

7.7.4 Show summary of the route entries registered in the IPv6 Routing Information Base

[Syntax]

show ipv6 route summary

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows a summary of the route entries that are registered in the IPv6 Routing Information Base (RIB).

[Note]

[Example]

Show a summary of the IPv6 Routing Information Base.

```
SWP2>show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 1
Route Source    Networks
connected       2
static          2
Total           4
```

7.8 Neighbor cache

7.8.1 Set static neighbor cache entry

[Syntax]

ipv6 neighbor *ipv6_address interface mac_address interface*
no ipv6 neighbor *ipv6_address interface*

[Parameter]

ipv6_address	:	X:X::X:X
		IPv6 address
interface	:	vlanN
		VLAN interface name
mac_address	:	HHHH.HHHH.HHHH
		MAC address

interface : portN.M

Physical interface name

[Input mode]

global configuration mode

[Description]

Adds a static entry to the neighbor cache.

If this command is executed with the "no" syntax, the specified static entry is deleted.

[Note]

[Example]

Set the MAC address of IPv6 2001:db8:cafe::1 located at port1.1 of VLAN #1, in the Neighbor cache.

```
SWP2(config)#ipv6 neighbor 2001:db8:cafe::1 vlan1 00a0.de80.cafe port1.1
```

7.8.2 Show neighbor cache table

[Syntax]

show ipv6 neighbors

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the neighbor cache table.

[Note]

[Example]

Show the neighbor cache table.

```
SWP2>show ipv neighbors
 IPv6 Address                              MAC Address     Interface  Type
2001:db8:1:0:3538:5dc7:6bc4:1a23          0011.2233.4455   vlan1      dynamic
2001:db8:cafe::1                          00a0.de80.cafe   vlan1      static
fe80::0211:22ff:fe33:4455                 0011.2233.4455   vlan1      dynamic
fe80::6477:88ff:fe99:aabb                 6677.8899.aabb   vlan1      dynamic
```

7.8.3 Clear neighbor cache table

[Syntax]

clear ipv6 neighbors

[Input mode]

priviledged EXEC mode

[Description]

Clears the neighbor cache.

[Note]

[Example]

Clear the neighbor cache.

```
SWP2#clear ipv6 neighbors
```

7.9 IPv6 forwarding control

7.9.1 IPv6 forwarding settings

[Syntax]

ipv6 forwarding *switch*

no ipv6 forwarding [*switch*]

[Parameter]

switch : IPv6 packet forwarding settings

Setting value	Description
enable	Enable forwarding of IPv6 packets
disable	Disable forwarding of IPv6 packets

[Initial value]

ipv6 forwarding disable

[Input mode]

global configuration mode

[Description]

Enables or disables forwarding of IPv6 packets.

If this is executed with the "no" syntax, the setting returns to the default.

7.9.2 Show IPv6 forwarding settings

[Syntax]

show ipv6 forwarding

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IPv6 packet forwarding settings.

[Example]

Shows the IPv6 packet forwarding settings.

```
SWP2>show ipv6 forwarding
IPv6 forwarding is on
```

7.10 IPv6 ping

7.10.1 IPv6 ping

[Syntax]

ping6 *host* [repeat *count*] [size *datalen*] [timeout *timeout*] [source *ipv6_address*]

[Keyword]

repeat : Specifies the number of times to execute

size : Specifies the length of the ICMPv6 payload (byte units)

timeout : Specifies the time to wait for a reply after transmitting the specified number of Echo requests

source : Sets the source address for ICMPv6 packets

[Parameter]

host : Host name, or target IPv6 address (X:X::X:X)

Target to which ICMPv6 Echo is sent

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

count : Number of times to execute (if omitted: 5)

Setting value	Description
<1-2147483647>	Execute the specified number of times
continuous	Execute repeatedly until Ctrl+C is entered

datalen : <36-18024>

Length of ICMP payload (if omitted: 56)

timeout : <1-65535>

Time to wait for a reply (if omitted: 2)

Ignored if count is specified as "continuous"

ipv6_address : X:X::X:X

IPv6 address

[Input mode]

priviledged EXEC mode

[Description]

Send ICMPv6 Echo to the specified host, and wait for ICMPv6 Echo Reply.

When it is received, indicate this. Show simple statistical information when the command ends.

[Note]

[Example]

Ping fe80::2a0:deff:fe11:2233.

```
SWP2#ping6 fe80::2a0:deff:fe11:2233%vlan1
PING fe80::2a0:deff:fe11:2233%vlan1 (fe80::2a0:deff:fe11:2233%vlan1): 56 data bytes
64 bytes from fe80::2a0:deff:fe11:2233: seq=0 ttl=64 time=2.681 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=1 ttl=64 time=4.760 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=2 ttl=64 time=10.045 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=3 ttl=64 time=10.078 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=4 ttl=64 time=10.210 ms

--- fe80::2a0:deff:fe11:2233%vlan1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.681/7.554/10.210 ms
```

7.10.2 Check IPv6 route

[Syntax]

traceroute6 *host*

[Parameter]

host : Destination for which to check the route

Host name, or target IPv6 address (X:X::X:X)

[Input mode]

priviledged EXEC mode

[Description]

Shows information for the route to the specified host.

[Note]

[Example]

Check the route to 2001:db8:1::2.

```
SWP2#traceroute6 2001:db8:1::2
traceroute to 2001:db8:1::2 (2001:db8:1::2), 30 hops max
 1  2001:db8:10::1 (2001:db8:10::1)  0.563 ms  0.412 ms  0.428 ms
 2  2001:db8:20::1 (2001:db8:20::1)  0.561 ms  0.485 ms  0.476 ms
 3  2001:db8:30::1 (2001:db8:30::1)  0.864 ms  0.693 ms  21.104 ms
 4  2001:db8:40::1 (2001:db8:40::1)  0.751 ms  0.783 ms  0.673 ms
 5  2001:db8:50::1 (2001:db8:50::1)  7.689 ms  7.527 ms  7.168 ms
 6  2001:db8:1::2 (2001:db8:1::2)  33.948 ms  10.413 ms  7.681 ms
```

7.11 DNS client

7.11.1 Set DNS lookup function

[Syntax]

dns-client *switch*
no dns-client

[Parameter]

switch : Behavior of the DNS client

Setting value	Description
enable	Enable the DNS client
disable	Disable the DNS client

[Initial value]

dns-client disable

[Input mode]

global configuration mode

[Description]

Enables or disables the DNS lookup function.

If this command is executed with the "no" syntax, the function is disabled.

[Example]

Enable the DNS lookup function.

```
SWP2(config)#dns-client enable
```

7.11.2 Set DNS server list

[Syntax]

dns-client name-server *server*
no dns-client name-server *server*

[Parameter]

server : A.B.C.D

IPv4 addtess of the DNS server

: X:X::X:X

IPv6 address of the DNS server

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a server to the DNS server list.

Up to three servers can be specified.

If this command is executed with the "no" syntax, the specified server is deleted from the DNS server list.

[Note]

If the **ip address dhcp**, **ipv6 address dhcp**, **ipv6 dhcp client pd** or **ipv6 address autoconfig stateless** command was used to obtain the DNS server list from the DHCP server, the settings of this command take priority.

However if fewer than three items were registered to the DNS server list by this command, up to a total of three items of the DNS server list obtained from the DHCP server are added to the end of this list.

[Example]

Add the IP addresses 192.168.100.1, 2001:db8::1234, and fe80::2a0:deff:fe11:2233 to the DNS server list.

```
SWP2(config)#dns-client name-server 192.168.100.1
SWP2(config)#dns-client name-server 2001:db8::1234
SWP2(config)#dns-client name-server fe80::2a0:deff:fe11:2233%vlan1
```

7.11.3 Set default domain name

[Syntax]

dns-client domain-name *name*
no dns-client domain-name *name*

[Parameter]

name : Domain name (maximum 255 characters)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Specifies the default domain name used for DNS queries.

If this command is executed with the "no" syntax, the default domain name is deleted.

[Note]

The setting of this command takes priority if the default domain name (option code 15) was obtained from the DHCP server by the **ip address dhcp** command.

If a search domain list is specified by the **dns-client domain-list** command, the default domain name specified by this command and the default domain name automatically specified by the **ip address dhcp** command are not used.

[Example]

Set the default domain name to "example.com".

```
SWP2(config)#dns-client domain-name example.com
```

7.11.4 Set search domain list

[Syntax]

dns-client domain-list *name*
no dns-client domain-list *name*

[Parameter]

name : Domain name (maximum 255 characters)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a domain name to the list of domain names used for DNS queries.

Up to six domains can be registered in the search domain list.

If this command is executed with the "no" syntax, the specified domain name is deleted from the search domain list.

[Note]

If a search domain list is specified by this command, the default domain name specified by the **dns-client domain-name** command and the default domain name automatically specified by the **ip address dhcp** command are not used.

If the **ipv6 address dhcp**, **ipv6 dhcp client pd** or **ipv6 address autoconfig stateless** command was used to obtain the query domain list from the DHCP server, the setting for this command takes priority.

However if fewer than six items were registered by this command in the query domain list, up to six items from the query domain list obtained by the DHCP server are added to the end of this list.

[Example]

Add the domain names "example1.com" and "example2.com" to the search domain list.

```
SWP2(config)#dns-client domain-list example1.com
SWP2(config)#dns-client domain-list example2.com
```

7.11.5 Show DNS client information

[Syntax]

show dns-client

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the DNS client information.

The following content is shown.

Item	Description
DNS Client is enabled	Enable the DNS client
DNS Client is disabled	Disable the DNS client
Default domain	Default domain name
Domain list	Search domain list
Name Servers	DNS server list (IP address)

[Example]

Show the DNS client information.

```
SWP2>show dns-client

DNS client is enabled
 Default domain  : example.com
 Domain list     : example1.com example2.com
 Name Servers    : 192.168.100.1 2001:db8::1234 fe80::2a0:deff:fe11:2233%vlan1

 * - Values assigned by DHCP or DHCPv6 Client.
```

Chapter 8

IP multicast control

8.1 IP multicast basic settings

8.1.1 Set processing method for unknown multicast frames

[Syntax]

l2-unknown-mcast *mode*

[Parameter]

mode : Sets the processing method for multicast frames

Setting value	Description
discard	Discard
flood	Flood

[Initial value]

l2-unknown-mcast flood

[Input mode]

global configuration mode

[Description]

Specifies the processing method for multicast frames that are not registered in the MAC address table.

[Example]

Discard unknown multicast.

```
SWP2(config)#l2-unknown-mcast discard
```

8.1.2 Setting the processing method for unknown multicast frames (interface)

[Syntax]

l2-unknown-mcast *mode*
no l2-unknown-mcast

[Parameter]

mode : Sets the processing method for multicast frames

Setting value	Description
discard	Discard
flood	Flood

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the processing method for multicast frames received by the VLAN interface, which are not registered in the MAC address table.

If this command is executed with the "no" syntax, the setting returns to its default value, the system-wide processing method for unknown multicast frames is used.

[Note]

This command can be specified only for VLAN interfaces.

This command is prioritized over the settings for the system-wide processing method for unknown multicast frames.

[Example]

This discards the multicast frames received by VLAN #1 that are not registered in the MAC address table.

```
SWP2(config)#interface vlan1
SWP2(config-if)#l2-unknown-mcast discard
```

8.1.3 Forwarding setting for link local multicast frames

[Syntax]

l2-unknown-mcast forward link-local
no l2-unknown-mcast forward link-local

[Initial value]

None

[Input mode]

global configuration mode

[Description]

When l2-unknown-mcast discard is set, the frame for the link local multicast address is forwarded without being discarded.

If this command is executed with the "no" syntax, the specified setting is deleted.

[Note]

The link local multicast address for this command falls within the ranges shown below.

- IPv4: 224.0.0.0/24
- IPv6: ff02::/112

The format for specifying the IPv4 multicast address has been discontinued. When you load a config that includes this format, the config is automatically replaced with the **l2-mcast flood** command.

[Example]

This forwards frames for the link local multicast address as unknown multicasts without discarding them.

```
SWP2(config)#l2-unknown-mcast discard
SWP2(config)#l2-unknown-mcast forward link-local
```

8.1.4 Forwarding setting for multicast frames

[Syntax]

l2-mcast flood *ipv4_addr*
no l2-mcast flood *ipv4_addr*

[Parameter]

ipv4_addr	:	A.B.C.D IPv4 multicast address

[Initial value]

None

[Input mode]

interface mode

[Description]

Floods the frames with the IPv4 multicast address specified by the destination in multicast traffic received by the VLAN interface.

Up to 100 instances of this command can be set system-wide.

If this command is executed with the "no" syntax, the specified IPv4 multicast address settings are deleted.

If no IPv4 multicast address is specified, all settings are deleted.

[Note]

This command can be specified only for VLAN interfaces.

The IPv4 multicast address specified by this command is excluded from IGMP snooping.

[Example]

Floods the frame 239.0.0.251 with the destination IPv4 address received by VLAN #1.

```
SWP2(config)#interface vlan1
SWP2(config-if)#l2-mcast flood 239.0.0.251
```

8.1.5 Enable/disable function to transmit IGMP/MLD query when topology changes

[Syntax]

l2-mcast snooping tcn-query enable *time*
l2-mcast snooping tcn-query disable
no l2-mcast snooping tcn-query

[Parameter]

time : <1-30>
Wait time for transmitting IGMP/MLD query (seconds)

[Initial value]

l2-mcast snooping tcn-query disable

[Input mode]

global configuration mode

[Description]

Specifies operation of the function that transmits an IGMP/MLD query when the topology changes due to spanning tree.

If this command is executed with the "no" syntax, the setting returns to the default.

When both IGMP/MLD snooping and spanning tree are used together, multicast communication might stop temporarily due to a change in topology, but that interval can be shortened by using this function.

If this is enabled, when a change in topology is detected, an IGMP/MLD query is transmitted after waiting the specified time.

If this is disabled, an IGMP/MLD query is not transmitted even if the topology changes.

[Example]

Enable transmission of an IGMP/MLD query when topology changes, and set the wait time to 5 seconds.

```
SWP2(config)#l2-mcast snooping tcn-query enable 5
```

Disable transmission of an IGMP/MLD query when topology changes.

```
SWP2(config)#l2-mcast snooping tcn-query disable
```

8.2 IGMP snooping

8.2.1 Set enable/disable IGMP snooping

[Syntax]

ip igmp snooping *switch*
no ip igmp snooping

[Parameter]

switch : IGMP snooping operations

Setting value	Description
enable	Enable IGMP snooping
disable	Disable IGMP snooping

[Initial value]

ip igmp snooping enable

[Input mode]

interface mode

[Description]

Enables the IGMP snooping setting of the interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interface.

[Example]

Enable IGMP snooping for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping enable
```

Disable IGMP snooping for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping disable
```

8.2.2 Set IGMP snooping fast-leave

[Syntax]

ip igmp snooping fast-leave [auto-assignment]
no ip igmp snooping fast-leave

[Keyword]

auto-assignment : If the switch is connected to and controlled by the LAN/SFP port, the fast-leave function is disabled.

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables IGMP snooping fast-leave for the interface.

If this is executed with the "no" syntax, IGMP snooping fast-leave is disabled.

If the switch is connected to and controlled by the LAN/SFP port when the auto-assignment option is specified, the fast-leave function is automatically disabled only for that port.

If it cannot be determined whether there is a switch connected to and controlled by the LAN/SFP port, the determination is made based on whether "Bridge" is included in the "System Capabilities" of the basic management TLV for the LLDP frame that's received at the relevant port.

[Note]

This command can be specified only for VLAN interface.

On a VLAN interface for which multiple hosts are connected to the LAN/SFP+ port, use this command to either enable the auto-assignment option or disable the fast-leave function altogether.

[Example]

Enable IGMP snooping fast-leave for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping fast-leave
```

Disable IGMP snooping fast-leave for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping fast-leave
```

8.2.3 Set multicast router connection destination

[Syntax]

ip igmp snooping mrouter interface *ifname*
no ip igmp snooping mrouter interface *ifname*

[Parameter]

ifname	:	LAN/SFP+ port interface name Interface to set

[Initial value]

none

[Input mode]

interface mode

[Description]

Statically sets the LAN/SFP+ port to which the multicast router is connected.

If this command is executed with the "no" syntax, the setting is discarded.

[Note]

This command can be specified only for VLAN interface.

The multicast router must be connected to the specified LAN/SFP+ port. If an IGMP report is received from the receiver, it is forwarded to the specified LAN/SFP+ port.

[Example]

Specify LAN port #8 as a connection destination of the multicast router.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping mrouter interface port1.8
```

Remove LAN port #8 as a connection destination of the multicast router.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping mrouter interface port1.8
```

8.2.4 Set query transmission function

[Syntax]

ip igmp snooping querier
no ip igmp snooping querier

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the IGMP query transmission function.

If this is executed with the "no" syntax, the IGMP query transmission function is disabled.

[Note]

This command can be specified only for VLAN interface.

Note that if you change the IP address while leaving this command enabled, queries will no longer be sent with the correct IP address following the change.

[Example]

Enable the transmission function for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping querier
```

Disable the transmission function for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping querier
```

8.2.5 Set IGMP query transmission interval

[Syntax]

ip igmp snooping query-interval *interval*
no ip igmp snooping query-interval

[Parameter]

interval : <20-18000>
Query transmission interval (seconds)

[Initial value]

ip igmp snooping query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for IGMP queries.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interface.

[Example]

Set the VLAN #2 query transmission interval to 30 seconds.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping query-interval 30
```

Return the VLAN #2 query transmission interval to the default setting.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping query-interval
```

8.2.6 Set TTL value verification function for IGMP packets

[Syntax]

ip igmp snooping check ttl *switch*
no ip igmp snooping check ttl

[Parameter]

switch : TTL value verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check ttl enable

[Input mode]

interface mode

[Description]

Sets the TTL value verification function for IGMP packets.

If this command is executed with the "no" syntax, the setting returns to the default.

When this is enabled, IGMP packets with illegal TTL values in the IP header (besides 1) will be discarded.

When disabled, the relevant packet will be discarded, and the TTL value will be corrected to 1 and forwarded.

[Note]

This command can be specified only for VLAN interface.

[Example]

Enable the TTL value verification function of IGMP packets for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ttl enable
```

Disnable the TTL value verification function of IGMP packets for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ttl disable
```

8.2.7 Set RA verification function for IGMP packets

[Syntax]

ip igmp snooping check ra *switch*
no ip igmp snooping check ra

[Parameter]

switch : RA verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check ra disable

[Input mode]

interface mode

[Description]

Configures the RA verification function for IGMPv2/IGMPv3 packets.

If this command is executed with the "no" syntax, the setting returns to the default.

If this is enabled, IGMPv2/IGMPv3 packets whose IP headers do not include an RA (Router Alert) option are discarded.

When disabled, the relevant packet is not discarded; instead, an RA option is added to the IP header and the packet is forwarded.

[Note]

This command can only be specified for VLAN interface.

[Example]

This enables the RA verification function of IGMP packets for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ra enable
```

This disables the RA verification function of IGMP packets for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ra disable
```

8.2.8 Set ToS verification function for IGMP packets

[Syntax]

ip igmp snooping check tos *switch*
no ip igmp snooping check tos

[Parameter]

switch : ToS verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check tos disable

[Input mode]

interface mode

[Description]

Configures the ToS verification function for IGMP packets.

If this command is executed with the "no" syntax, the setting returns to the default.

When this is enabled, IGMPv3 packets with illegal ToS IP Precedence values (3 bits) in the IP header (besides B'110) will be discarded. For all other packets, the ToS is rewritten to 0xc0 and forwarded.

When disabled, the IGMP packet is not discarded; instead, the ToS will be corrected to 0xc0 and the packet is forwarded.

[Note]

This command can only be specified for VLAN interface.

[Example]

This enables the ToS verification function of IGMP packets for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check tos enable
```

This disables the ToS verification function of IGMP packets for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check tos disable
```

8.2.9 Set IGMP version

[Syntax]

ip igmp snooping version *version*
no ip igmp snooping version

[Parameter]

version : <2-3>
IGMP version

[Initial value]

ip igmp snooping version 3

[Input mode]

interface mode

[Description]

Sets the IGMP version.

If this command is executed with the "no" syntax, the IGMP version returns to the default setting (V3).

[Note]

This command can be specified only for VLAN interface.

If an IGMP packet of a different version than this setting is received, the following action occurs.

- When set to V2
  - If a V3 query is received, it is forwarded as a V2 query
  - If a V3 report is received, it is discarded
- When set to V3
  - If a V2 query is received, it is forwarded as a V2 query

- If a V2 report is received, it is forwarded as a V3 report

[Example]

On VLAN #2, set the IGMP version to 2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping version 2
```

On VLAN #2, return the IGMP version to the default setting.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping version
```

8.2.10 Settings for IGMP Report Suppression

[Syntax]

ip igmp snooping report-suppression *switch*
no ip igmp snooping report-suppression

[Parameter]

switch : IGMP report suppression

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping report-suppression enable

[Input mode]

interface mode

[Description]

Configures IGMP report suppression.

If this command is executed with the "no" syntax, the setting returns to the default.

When enabled, the minimum number of messages will be sent to the multicast router ports based on the information obtained from the received Report messages and Leave messages.

When disabled, the received Report messages and Leave messages will be sequentially transmitted to the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables IGMP report suppression at VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-suppression enable
```

Disables IGMP report suppression at VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-suppression disable
```

8.2.11 Set the IGMP report forwarding function

[Syntax]

ip igmp snooping report-forward *switch*
no ip igmp snooping report-forward

[Parameter]

switch : IGMP report forwarding function

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping report-forward disable

[Input mode]

interface mode

[Description]

This configures the IGMP report forwarding function.

If this command is executed with the "no" syntax, the setting returns to the default.

When this is enabled and a switch is connected to and controlled by LAN/SFP+ port, an IGMP Report message or a Leave message is forwarded to that port, in addition to the multicast router port.

When disabled, the IGMP Report messages and Leave messages will be forwarded only to the multicast router port.

If it cannot be determined whether there is a switch connected to and controlled by LAN/SFP+ port, the determination is made based on whether "Bridge" is included in the "System Capabilities" of the basic management TLV for the LLDP frame that's received at the relevant port.

[Note]

This command can only be specified for VLAN interface.

When this function is enabled, disable the IGMP report suppression function.

[Example]

Enables the IGMP report forwarding function for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-forward enable
```

Disables the IGMP report forwarding function for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-forward disable
```

8.2.12 Settings for Suppression of Data Transmission to Multicast Router Ports

[Syntax]

ip igmp snooping mrouter-port data-suppression *switch*
no ip igmp snooping mrouter-port data-suppression

[Parameter]

switch : Suppression of data transmission to multicast router ports

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping mrouter-port data-suppression disable

[Input mode]

interface mode

[Description]

Configures suppression of data transmission to multicast router ports.

If this command is executed with the "no" syntax, the setting returns to the default.

When enabled, the relevant data will be transmitted to the multicast router ports only when Report messages are received by the multicast router ports.

When disabled, the relevant data will be transmitted to the multicast router ports when Report messages are received by any of the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables suppression of data transmission to multicast router ports at VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping mrouter-port data-suppression enable
```

Disables suppression of data transmission to multicast router ports in VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping mrouter-port data-suppression disable
```

8.2.13 Show multicast router connection port information

[Syntax]

show ip igmp snooping mrouter *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the multicast router connection port information that was dynamically learned or statically set.

[Example]

Show multicast router connection port information for VLAN #2.

```
SWP2#show ip igmp snooping mrouter vlan2
VLAN    Interface             IP-address    Expires
2       port1.8(dynamic)          192.168.100.216        00:00:49
```

8.2.14 Show IGMP group membership information

[Syntax]

show ip igmp snooping groups [detail]
show ip igmp snooping groups *A.B.C.D* [detail]
show ip igmp snooping groups *ifname* [detail]

[Keyword]

detail	:	Detailed information

[Parameter]

A.B.C.D	:	Multicast group address
ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows IGMP group membership information.

[Example]

Show IGMP group membership information.

```
SWP2#show ip igmp snooping groups
IGMP Snooping Group Membership
```

```
Group source list: (R - Remote, S - Static)
Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
1      239.255.255.250          port1.5        R      01:06:02   00:03:45
192.168.100.11    V3
```

Show detailed IGMP group membership information.

```
SWP2#show ip igmp snooping groups detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      port1.5
Group:          239.255.255.250
Flags:          R
Uptime:         01:07:10
Group mode:     Exclude (Expires: 00:04:13)
Last reporter:  192.168.100.11
Source list is empty
```

8.2.15 Show an interface's IGMP-related information

[Syntax]

show ip igmp snooping interface *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows IGMP-related information for a VLAN interface.

[Example]

Show IGMP-related information for VLAN #1.

```
SWP2#show ip igmp snooping interface vlan1

IGMP Snooping information for vlan1
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2/v3 fast-leave is enabled
 IGMPv1/v2 Report suppression enabled
 IGMPv2/v3 fast-leave auto-assignment is enabled
 IGMPv3 Report suppression enabled
 IGMPv1/v2/v3 Report forwarding enabled
 IGMP Snooping check TTL is enabled
 IGMP Snooping check RA is enabled
 IGMP Snooping check ToS is enabled
 IGMP Snooping Mrouter-port Data suppression disabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 1
 Number of v1-reports: 0
 Number of v2-reports: 6
 Number of v2-leaves: 0
 Number of v3-reports: 127
 Active Ports:
  port1.1 (F,R)
  port1.2

  F - Fast-leave auto-assignment is enabled
  R - Report forwarding is enabled
```

8.2.16 Clear IGMP group membership entries

[Syntax]

clear ip igmp snooping
clear ip igmp snooping group *A.B.C.D*
clear ip igmp snooping interface *ifname*

[Keyword]

group	:	Specifies the multicast group address to be cleared
interface	:	Specifies the VLAN interface to be cleared

[Parameter]

A.B.C.D	:	Multicast group address "*" indicates all entries
ifname	:	VLAN interface name Interface to clear

[Input mode]

priviledged EXEC mode

[Description]

Clears IGMP group membership entries.

[Example]

Clear IGMP group membership entries for VLAN #1.

```
SWP2#clear ip igmp snooping interface vlan1
```

8.3 MLD snooping

8.3.1 Enable/disable MLD snooping

[Syntax]

ipv6 mld snooping *switch*
no ipv6 mld snooping

[Parameter]

switch : MLD snooping operations

Setting value	Description
enable	Enable MLD snooping
disable	Disable MLD snooping

[Initial value]

ipv6 mld snooping enable

[Input mode]

interface mode

[Description]

Configures the operations of the MLD snooping setting of the interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces.

[Example]

Enable MLD snooping for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping enable
```

Disnable MLD snooping for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping disable
```

8.3.2 Set MLD snooping fast-leave

[Syntax]

ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables MLD snooping fast-leave for the interface.

If this is executed with the "no" syntax, MLD snooping fast-leave is disabled.

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

Do not enable this command on a VLAN interface for which multiple hosts are connected to the LAN/SFP+ port.

[Example]

Enable MLD snooping fast-leave for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping fast-leave
```

Disable MLD snooping fast-leave for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping fast-leave
```

8.3.3 Set multicast router connection destination

[Syntax]

ipv6 mld snooping mrouter interface *ifname*
no ipv6 mld snooping mrouter interface *ifname*

[Parameter]

ifname	:	Interface name of LAN/SFP+ port Interface to set

[Initial value]

none

[Input mode]

interface mode

[Description]

Statically sets the LAN/SFP+ port to which the multicast router is connected.

If this command is executed with the "no" syntax, the setting is discarded.

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

The multicast router must be connected to the specified LAN/SFP+ port. If an MLD report is received from the receiver, it is forwarded to the specified LAN/SFP+ port.

[Example]

Specify LAN port #8 as a connection destination of the multicast router.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping mrouter interface port1.8
```

Remove LAN port #8 as a connection destination of the multicast router.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping mrouter interface port1.8
```

8.3.4 Set query transmission function

[Syntax]

ipv6 mld snooping querier
no ipv6 mld snooping querier

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the MLD query transmission function.

If this command is executed with the "no" syntax, the MLD query transmission function is disabled.

[Note]

This command can be specified only forVLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

When using this command, you must specify the **ipv6 enable** command for one of the VLAN interfaces. Note that if the **ipv6 enable** command has not been specified, MLD query is not transmitted.

[Example]

Enable the MLD query transmission function for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping querier
```

Disable the MLD query transmission function for VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping querier
```

8.3.5 Set MLD query transmission interval

[Syntax]

ipv6 mld snooping query-interval *interval*
no ipv6 mld snooping query-interval

[Parameter]

interval : <20-18000>

Query transmission interval (seconds)

[Initial value]

ipv6 mld snooping query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for MLD queries.

If this command is executed with the "no" syntax, the MLD query transmission interval is returned to the default setting.

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

[Example]

Set the VLAN #2 query transmission interval to 30 seconds.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping query-interval 30
```

Return the VLAN #2 query transmission interval to the default setting.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping query-interval
```

8.3.6 Set MLD version

[Syntax]

ipv6 mld snooping version *version*
no ipv6 mld snooping version

[Parameter]

version : <1-2>
MLD version

[Initial value]

ipv6 mld snooping version 2

[Input mode]

interface mode

[Description]

Sets the MLD version.

If this command is executed with the "no" syntax, the MLD version returns to the default setting (V2).

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

If an MLD packet of a different version than this setting is received, the following action occurs.

- If V1 is specified
  - If a V2 query is received, it is forwarded as a V1 query
  - If a V2 report is received, it is discarded
- If V2 is specified
  - If a V1 query is received, it is forwarded as a V1 query
  - If a V1 report is received, it is forwarded as a V2 report

[Example]

On VLAN #2, set the MLD version to 1.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping version 1
```

On VLAN #2, return the MLD version to the default setting.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping version
```

8.3.7 Settings for MLD Report Suppression

[Syntax]

ipv6 mld snooping report-suppression *switch*
no ipv6 mld snooping report-suppression

[Parameter]

switch : MLD report suppression

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ipv6 mld snooping report-suppression enable

[Input mode]

interface mode

[Description]

Configures MLD report suppression.

If this command is executed with the "no" syntax, the setting returns to the default.

When enabled, the minimum number of messages will be sent to the multicast router ports based on the information obtained from the received Report messages and Leave messages.

When disabled, the received Report messages and Leave messages will be sequentially transmitted to the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables MLD report suppression at VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping report-suppression enable
```

Disables MLD report suppression at VLAN #2.

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping report-suppression disable
```

8.3.8 Show multicast router connection port information

[Syntax]

show ipv6 mld snooping mrouter *ifname*

[Parameter]

ifname : VLAN interface name

Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the multicast router connection port information that was dynamically learned or statically set.

[Example]

Show multicast router connection port information for VLAN #2.

```
SWP2#show ipv6 mld snooping mrouter vlan2
VLAN    Interface             IP-address    Expires
2       port1.11(dynamic)         fe80::ae44:f2ff:fe30:291        00:01:04
```

8.3.9 Show MLD group membership information

[Syntax]

show ipv6 mld snooping groups [detail]
show ipv6 mld snooping groups *X*:*X*::*X*:*X* [detail]
show ipv6 mld snooping groups *ifname* [detail]

[Keyword]

detail : Detailed information

[Parameter]

X:X::X:X	:	Multicast group address
ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows MLD group membership information.

[Example]

Show MLD group membership information.

```
SWP2#show ipv6 mld snooping groups
MLD Connected Group Membership
Group Address                              Interface            Uptime   Expires  Last
Reporter
ff15::1                                    port1.3              00:00:44 00:01:07
fe80::a00:27ff:fe8b:87e3
```

Show detailed MLD group membership information.

```
SWP2#show ipv6 mld snooping groups detail
MLD Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      port1.3
Group:          ff15::1
Uptime:         00:00:03
Group mode:     Include ()
Last reporter:  fe80::a00:27ff:fe8b:87e3
Group source list: (R - Remote, M - SSM Mapping, S - Static )
    Source Address                           Uptime    v2 Exp    Fwd  Flags
    fe80::221:70ff:fef9:8a39               00:00:03  00:01:06  Yes  R
```

8.3.10 Show an interface's MLD-related information

[Syntax]

show ipv6 mld snooping interface *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Show a VLAN interface's MLD-related information.

[Example]

Show MLD-related information for VLAN #1.

```
SWP2#show ipv6 mld snooping interface vlan1

MLD Snooping information for vlan1
 MLD Snooping enabled
 Snooping Querier none
 MLD Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 MLDv1 fast-leave is disabled
 MLDv1 Report suppression enabled
 MLDv2 Report suppression enabled
 Router port detection using MLD Queries
 Number of router-ports: 0
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v1-leaves: 0
```

```
Number of v2-reports: 127
Number of v1-query-warnings: 0
Number of v2-query-warnings: 0
Active Ports:
 port1.1
 port1.2
```

8.3.11 Clear MLD group membership entries

[Syntax]

clear ipv6 mld snooping
clear ipv6 mld snooping group *X*:*X*::*X*:*X*
clear ipv6 mld snooping interface *ifname*

[Keyword]

group	:	Specifies the multicast group address to be cleared
interface	:	Specifies the VLAN interface to clear

[Parameter]

X:*X*::*X*:*X*	:	Multicast group address
		"*" indicates all entries
ifname	:	VLAN interface name
		Interface to clear

[Input mode]

priviledged EXEC mode

[Description]

Clears MLD group membership entries.

[Example]

Clear MLD group membership entries for VLAN #1.

```
SWP2#clear ipv6 mld snooping interface vlan1
```

Chapter 9

Traffic control

9.1 ACL

9.1.1 Generate IPv4 access list

[Syntax]

access-list *ipv4-acl-id* [*seq_num*] *action protocol src-info* [*src-port*] *dst-info* [*dst-port*] [**ack**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**]
no access-list *ipv4-acl-id* [*seq_num*] [*action protocol src-info* [*src-port*] *dst-info* [*dst-port*] [**ack**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**]]

[Keyword]

ack : If tcp is specified as the protocol, the ACK flag of the TCP header is specified as a condition.

fin : If tcp is specified as the protocol, the FIN flag of the TCP header is specified as a condition.

psh : If tcp is specified as the protocol, the PSH flag of the TCP header is specified as a condition.

rst : If tcp is specified as the protocol, the RST flag of the TCP header is specified as a condition.

syn : If tcp is specified as the protocol, the SYN flag of the TCP header is specified as a condition.

urg : If tcp is specified as the protocol, the URG flag of the TCP header is specified as a condition.

[Parameter]

ipv4-acl-id : <1-2000>

ID of IPv4 access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

protocol : Specifies the applicable protocol type

Setting value	Description
<0-255>	Protocol number of the IP header
any	All IPv4 packets
tcp	TCP packets
udp	UDP packets

src-info : Specifies the transmission-source IPv4 address that is the condition

Setting value	Description
A.B.C.D E.F.G.H	Specifies an IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
host A.B.C.D	Specifies a single IPv4 address (A.B.C.D)
any	Applies to all IPv4 addresses

src-port : <0-65535>

If protocol is specified as tcp or udp, this specifies the transmission source port number <0-65535> that is the condition. This can also be omitted.

Method of specifying	Description
eq X	Specify port number (X)
range X Y	Specify port numbers (X) through (Y)

dst-info : Specifies the destination IPv4 address information that is the condition

Setting value	Description
A.B.C.D E.F.G.H	Specifies an IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
host A.B.C.D	Specifies a single IPv4 address (A.B.C.D)
any	Applies to all IPv4 addresses

dst-port : <0-65535>

If protocol is specified as tcp or udp, this specifies the destination port number <0-65535> that is the condition. This can also be omitted.

Method of specifying	Description
eq X	Specify port number (X)
range X Y	Specify port numbers (X) through (Y)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates an IPv4 access list.

Multiple conditions (maximum 256) can be specified for the generated access list.

To apply the generated access list, use the **access-group** command of interface mode.

If the "no" syntax is used to specify "action" and following, the IPv4 access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and following, the IPv4 access list of the matching ID of access list is deleted.

[Note]

An access list that is applied to LAN/SFP+ port and logical interface cannot be deleted using the "no" syntax. You must first cancel the application, and then delete the access list.

For both src-port and dst-port, you can use "range" to specify a range; however for the entire system, only one IPv4 access list that specifies a range in this way can be applied to the interface by using the **access-group** command.

[Example]

Create access list #1 that denies communication from the source segment 192.168.1.0/24 to the destination 172.16.1.1.

```
SWP2(config)#access-list 1 deny any 192.168.1.0 0.0.0.255 host 172.16.1.1
```

Delete IPv4 access list #1.

```
SWP2(config)#no access-list 1
```

9.1.2 Adding a description for IPv4 access list

[Syntax]

access-list *ipv4-acl-id* **description** *line*
no access-list *ipv4-acl-id* **description**

[Parameter]

ipv4-acl-id	:	<1-2000> ID of the IPv4 access list to which to add a description
line	:	Description to add. Can be up to 32 ASCII characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Add a description to the generated IPv4 access list.

If this command is executed with the "no" syntax, the IPv4 description is cleared.

[Note]

A description can be added with this command even after applying an access list to LAN/SFP+ port and logical interface. (The later description will overwrite it)

[Example]

Create IPv4 access list #1 that denies communication from the 192.168.1.0/24 sending source segment to 172.16.1.1, and add the description of "Test".

```
SWP2(config)#access-list 1 deny any 192.168.1.0 0.0.0.255 host 172.16.1.1
SWP2(config)#access-list 1 description Test
```

9.1.3 Apply IPv4 access list

[Syntax]

access-group *ipv4-acl-id direction*
no access-group *ipv4-acl-id direction*

[Parameter]

ipv4-acl-id	:	<1-2000> ID of IPv4 access list to apply
direction	:	Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames
out	Apply to transmitted frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Applies an IPv4 access list to both LAN/SFP+ port and logical interface.

If the received/transmitted frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the corresponding frame.

If this command is executed with the "no" syntax, the applied access list is deleted from both LAN/SFP+ port and logical interface.

[Note]

Only one access list for each direction can be registered for incoming frames (in) and for outgoing frames (out) on the same interface.

The access list for transmitted frames can only be applied to LAN/SFP+ port.

The following restrictions apply.

An IPv4 access list for which the port number range (range X Y) is specified cannot be applied to transmitted frames (out).

An LAN/SFP+ port for which an incoming frames access list is specified cannot be associated to an logical interface.

An incoming frames access list cannot be applied to an LAN/SFP+ port that is associated with an logical interface. However, if an access list setting for incoming frames is specified for an LAN/SFP+ port that is associated with an logical interface in the startup config, then the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Apply extended IPv4 access list #1 to received frames of LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#access-group 1 in
```

9.1.4 Generate IPv6 access list

[Syntax]

access-list *ipv6-acl-id* [*seq_num*] *action src-info*
no access-list *ipv6-acl-id* [*seq_num*] [*action src-info*]

[Parameter]

ipv6-acl-id : <3001-4000>

ID of IPv6 access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

src-info : Specifies the transmission-source IPv6 address that is the condition

Setting value	Description
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv6 addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates an IPv6 access list.

Multiple conditions (maximum 256) can be specified for the generated access list.

To apply the generated access list, use the **access-group** command of interface mode.

If the "no" syntax is used to specify "action" and following, the IPv6 access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and following, the IPv6 access list of the matching ID of access list is deleted.

[Note]

An access list that is applied to LAN/SFP+ port and logical interface cannot be deleted using the "no" syntax. Before you can delete the access list, you must rescind the application of that list.

[Example]

Create IPv6 access list #3002 which will deny frames from 3ffe:506::/32.

```
SWP2(config)#access-list 3002 deny 3ffe:506::/32
```

Delete IPv6 access list #3002.

```
SWP2(config)#no access-list 3002
```

9.1.5 Adding a description for IPv6 access list

[Syntax]

access-list *ipv6-acl-id* **description** *line*
no access-list *ipv6-acl-id* **description**

[Parameter]

ipv6-acl-id	:	<3001-4000>
		ID of the IPv6 access list to which to add a description
line	:	Description to add. Can be up to 32 ASCII characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Add a description to the generated IPv6 access list.

If this command is executed with the "no" syntax, the IPv6 descriptive text is cleared.

[Note]

A description can be added with this command even after applying an access list to LAN/SFP+ port and logical interface. (It will be overwritten with the later description)

[Example]

Create IPv6 access list #3002 that denies packets from 3ffe:506::/32, and add the description of "Test".

```
SWP2(config)#access-list 3002 deny 3ffe:506::/32
SWP2(config)#access-list 3002 description Test
```

9.1.6 Apply IPv6 access list

[Syntax]

access-group *ipv6-acl-id direction*
no access-group *ipv6-acl-id direction*

[Parameter]

ipv6-acl-id : <3001-4000>

ID of IPv6 access list to apply

direction : Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames
out	Apply to transmitted frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Applies an IPv6 access list to both LAN/SFP+ port and logical interface.

If the received/transmitted frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the corresponding frame.

If this command is executed with the "no" syntax, the applied access list is deleted from both LAN/SFP+ port and logical interface.

[Note]

Only one access list for each direction can be registered for incoming frames (in) and for outgoing frames (out) on the same interface.

The access list for transmitted frames can only be applied to LAN/SFP+ port.

The following restrictions apply.

An LAN/SFP+ port for which an incoming frames access list is specified cannot be associated to an logical interface.

An incoming frames access list cannot be applied to an LAN/SFP+ port that is associated with an logical interface. However, if an access list setting for incoming frames is specified for an LAN/SFP+ port that is associated with an logical interface in the startup config, then the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Apply IPv6 access list #3002 to received frames of LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#access-group 3002 in
```

9.1.7 Generate MAC access list

[Syntax]

access-list *mac-acl-id* [*seq_num*] *action src-info dst-info*
no access-list *mac-acl-id* [*seq_num*] [*action src-info dst-info*]

[Parameter]

mac-acl-id : <2001-3000>

ID of MAC access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

src-info : Specifies the transmission-source MAC address information that is the condition

Setting value	Description
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	Specifies the MAC address (HHHH.HHHH.HHHH) with wildcard bits (WWWW.WWWW.WWWW)
host HHHH.HHHH.HHHH	Specifies an individual MAC address (HHHH.HHHH.HHHH)
any	Applies to all MAC addresses

dst-info : Specifies the destination MAC address information that is the condition

Setting value	Description
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	Specifies the MAC address (HHHH.HHHH.HHHH) with wildcard bits (WWWW.WWWW.WWWW)
host HHHH.HHHH.HHHH	Specifies an individual MAC address (HHHH.HHHH.HHHH)
any	Applies to all MAC addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates a MAC access list.

Multiple conditions (maximum 256) can be specified for the generated access list.

To apply the generated access list, execute the **access-group** command in interface mode.

If the "no" syntax is used to specify "action" and following, the MAC access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and following, the MAC access list of the matching ID of access list is deleted.

[Note]

An access list that is applied to LAN/SFP+ port and logical interface cannot be deleted using the "no" syntax. You must first cancel the application, and then delete the access list.

"W" and "H" represent a single character from the range 0-9, a-f, and A-F.

[Example]

Create MAC access list #2001 which denies frames from MAC address 00-A0-DE-12-34-56.

```
SWP2(config)#access-list 2001 deny mac 00A0.DE12.3456 0000.0000.0000 any
```

Delete MAC access list #2001.

```
SWP2(config)#no access-list 2001
```

9.1.8 Adding a description for MAC access lists

[Syntax]

access-list *mac-acl-id* **description** *line*
no access-list *mac-acl-id* **description**

[Parameter]

mac-acl-id	:	<2001-3000> ID of the MAC access list to which to add a description
line	:	Description to add. Can be up to 32 ASCII characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Add a description to the generated MAC access list.

If this command is executed with the "no" syntax, the MAC description is cleared.

[Note]

A description can be added with this command even after applying an access list to LAN/SFP+ port and logical interface. (The later description will overwrite it)

[Example]

Create MAC access list #2001 that denies frames from MAC address 00-A0-DE-12-34-56, and add the description of "Test".

```
SWP2(config)#access-list 2001 deny mac 00A0.DE12.3456 0000.0000.0000 any
SWP2(config)#access-list 2001 description Test
```

9.1.9 Apply MAC access list

[Syntax]

access-group *mac-acl-id direction*
no access-group *mac-acl-id direction*

[Parameter]

mac-acl-id	:	<2001-3000> ID of MAC access list to apply
direction	:	Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Applies a MAC access list to both LAN/SFP+ port and logical interface.

If the received frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the corresponding frame.

If this is executed with the "no" syntax, the applied access list is deleted from both LAN/SFP+ port and logical interface.

[Note]

It is not possible to register multiple access lists for a single interface.

The following restrictions apply.

An LAN/SFP+ port for which an incoming frames access list is specified cannot be associated to an logical interface.

An incoming frames access list cannot be applied to an LAN/SFP+ port that is associated with an logical interface. However, if an access list setting for incoming frames is specified for an LAN/SFP+ port that is associated with an logical interface in the startup config, then the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Apply access list #2001 to received frames of LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#access-group 2001 in
```

9.1.10 Show generated access list

[Syntax]

show access-list [*acl_id*]

[Parameter]

acl-id : <1-2000>, <2001-3000>, <3001-4000>

ID of access list

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the registered access list.

If acl-id is omitted, all access lists are shown.

If an access list is applied to an interface, and one or more frames that match the conditions are received or forwarded, the total number (match) of those frames is also shown.

[Note]

The total number (match) of frames that match the traffic category (QoS) conditions is also incremented.

[Example]

Show all lists.

```
SWP2>show access-list
IPv4 access list 1
    10 deny any 192.168.1.0/24 host 172.16.1.1 [match= 62]
MAC access list 2001
    10 deny host 00A0.DE12.3456 any [match= 123]
IPv6 access list 3002
    10 deny 3ffe:506::/32
```

9.1.11 Clear counters

[Syntax]

clear access-list counters [*acl_id*]

[Parameter]

acl-id : <1-2000>, <2001-3000>, <3001-4000>

ID of access list

[Input mode]

priviledged EXEC mode

[Description]

Clears the counters (match) that are shown by the "show access-list" command.

[Example]

Clear counters.

```
SWP2>clear access-list counters
```

9.1.12 Show access list applied to interface

[Syntax]

show access-group

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

For each interface, shows the ID of all access lists that are applied.

[Example]

Show a list.

```
SWP2>show access-group
Interface port1.1 : IPv4 access group 1 in
Interface port1.7 : IPv6 access group 3002 in
Interface port1.8 : MAC access group 2001 in
```

9.1.13 Set VLAN access map and move to VLAN access map mode

[Syntax]

vlan access-map *access-map-name*
no vlan access-map *access-map-name*

[Parameter]

access-map-name	:	Single-byte alphanumeric characters and single-byte symbols(256 characters or less) Access map name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Create a VLAN access map with the name specified by *access-map-name*, and then move to VLAN access map mode in order to make VLAN access map settings.

If this command is executed with the "no" syntax, the specified VLAN access map is deleted.

[Note]

To return from VLAN access map mode mode to global configuration mode, use the **exit** command. To return to priviledged EXEC mode, use the **end** command.

[Example]

Create a VLAN access map named "VAM001", and move to VLAN access map mode.

```
SWP2(config)#vlan access-map VAM001
SWP2(config-vlan-access-map)#
```

9.1.14 Set access list for VLAN access map

[Syntax]

match access-list *list-id*
no match access-list *list-id*

[Parameter]

list-id	:	<1-2000>, <2001-3000>, <3001-4000> Access list number specified by the access-list command

[Initial value]

none

[Input mode]

VLAN access map mode

[Description]

Sets the access list that is applied to the corresponding VLAN access map.

If this command is executed with the "no" syntax, the specified access list is deleted from the corresponding VLAN access map.

[Note]

Only one access list can be specified for one VLAN access map.

You can use the **show vlan access-map** command to view the setting.

[Example]

Create a VLAN access map named "VAM001", and specify an access list that denies packets from 192.168.0.1.

```
SWP2(config)#access-list 2 deny any 192.168.0.1/32 any
SWP2(config)#vlan access-map VAM001
SWP2(config-vlan-access-map)#match access-list 2
```

9.1.15 Set VLAN access map filter

[Syntax]

vlan filter *access-map-name vlan-id* [*direction*]
no vlan filter *access-map-name vlan-id* [*direction*]

[Parameter]

access-map-name : Single-byte alphanumeric characters and single-byte symbols(256 characters or less)

Access map name specified by the vlan access-map command

vlan-id : <1-4094>

VLAN ID set to the "enable" status by the vlan command

direction : Specifies the direction of applicable frames. Applied to incoming frames when omitted

Setting value	Description
in	Apply to received frames
out	Apply to transmitted frames

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN access map filter for the specified VLAN.

If this command is executed with the "no" syntax, the VLAN access map filter for the specified VLAN is deleted.

[Note]

It is not possible to specify this command for a VLAN ID that is set to the "disable" state.

Only one VLAN access map for each direction can be registered for incoming frames (in) and for outgoing frames (out) on the same interface.

Note that VLAN access maps for which the following access list is set cannot be applied to outgoing frames (out).

- MAC access list
- As a restriction, an IPv4 access list for which the port number range (range X Y) is specified cannot be applied to transmitted frames (out).

[Example]

Creates a VLAN access map named VAM001, specifies an access list that denies packets beginning from 192.168.0.1, and then applies VAM001 to incoming frames of VLAN #1000.

```
SWP2(config)#vlan database
SWP2(config-vlan)#vlan 1000
SWP2(config-vlan)#exit
SWP2(config)#access-list 2 deny any 192.168.0.1/32 any
SWP2(config)#vlan access-map VAM001
SWP2(config-vlan-access-map)#match access-list 2
SWP2(config-vlan-access-map)#exit
SWP2(config)#vlan filter VAM001 1000 in
```

9.1.16 Show VLAN access map

[Syntax]

show vlan access-map

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the registered VLAN access map.

The following items are shown.

- Name of the VLAN access map
- Access list applied to VLAN access map

[Example]

Show VLAN access map information.

```
SWP2>show vlan access-map
Vlan access-map VAM001
    match ipv4 access-list 2
```

9.1.17 Show VLAN access map filter

[Syntax]

show vlan filter

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Show VLAN access map filter application information.

The following items are shown.

- Name of the VLAN access map
- VLAN ID applied to VLAN access map
- Frame direction (in/out) for which a VLAN access map is applied

[Example]

Show VLAN access map filter information.

```
SWP2>show vlan filter
Vlan Filter VAM001 is applied to vlan 1000 in
Vlan Filter VAM001 is applied to vlan 1001 out
Vlan Filter VAM002 is applied to vlan 2000-2001 in
```

9.2 QoS (Quality of Service)

9.2.1 Enable/disable QoS

[Syntax]

qos *action*
qos_disable

[Parameter]

action : Operation for Qos

Setting value	Description
enable	Qos is enabled
disable	Qos is disabled

[Initial value]

no qos

[Input mode]

global configuration mode

[Description]

Enables QoS.

If this is executed with the "no" syntax, QoS is disabled. At this time, the related QoS settings are also deleted.

[Note]

If the flow control system setting is enabled, it is not possible to enable QoS.

Many of the commands related to QoS cannot be executed unless QoS is left enabled.

[Example]

Enable QoS.

```
SWP2(config)#qos enable
```

Disable QoS.

```
SWP2(config)#qos disable
```

9.2.2 Set default CoS

[Syntax]

qos cos *value*
no qos cos

[Parameter]

value : <0-7>
Default CoS value

[Initial value]

qos cos 0

[Input mode]

interface mode

[Description]

Sets the default CoS of LAN/SFP+ port and logical interface.

If this is executed with the "no" syntax, the default value (CoS=0) is specified.

The default CoS is used if untagged frames are received when the interface's trust mode is set to CoS. (Since CoS is not specified for the frame)

[Note]

In order to execute this command, QoS must be enabled.

If this is executed for an interface whose trust mode is CoS, the command results in an execution error.

An LAN/SFP+ port whose default CoS differs cannot be aggregated as an logical interface.

If the interface for which this is executed is an LAN/SFP+ port that is associated with an logical interface, then this command produces an execution error. However, in the case of settings for an LAN/SFP+ port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Set the default CoS value to 2.

```
SWP2(config-if)#qos cos 2
```

Return the default CoS value to the default value.

```
SWP2(config-if)#no qos cos
```

9.2.3 Set trust mode

[Syntax]

qos trust *mode*
no qos trust

[Parameter]

mode : Trust mode

Setting value	Description
cos	Determines the egress queue based on the CoS value
dscp	Determines the egress queue based on the DSCP value
port-priority	Applies the specified priority to the receiving port

[Initial value]

qos trust cos

[Input mode]

interface mode

[Description]

Specifies the trust mode of LAN/SFP+ port and logical interface.

If this is executed with the "no" syntax, the default value (CoS trust mode) is specified.

In the case of "CoS" trust mode, the CoS value of incoming frames is used to determine the egress queue. In the case of "DSCP," the DSCP value of incoming frames is used to determine the egress queue. In the case of "port priority," the priority specified for the receiving interface is used to determine the egress queue.

The CoS value and DSCP value, and the egress queue that is associated with the receiving port, can be changed by using the following commands.

Trust mode	Setting value used for egress queue determination	Corresponding command
CoS	CoS - egress queue ID conversion table	**qos cos-queue**
DSCP	DSCP - egress queue ID conversion table	**qos dscp-queue**
Port Priority	Priority specified for each receiving port	**qos port-priority-queue**

Within the various QoS processes, there are four types of timing that determine (change) the egress queue.

1. When assigning the egress queue
2. Specifying the egress queue by class map
3. Specifying pre-marking by class map
4. Specifying remarking by class map

Types 2, 3, and 4 can be specified whether the trust mode is "CoS" or "DSCP"; in either case, the egress queue is assigned by referencing the "egress queue ID conversion table" that corresponds to its own trust mode.

[Note]

In order to execute this command, QoS must be enabled.

If a policy map is applied to LAN/SFP+ port and logical interface, the trust mode cannot be changed.

An LAN/SFP+ port whose trust mode differs cannot be aggregated as an logical interface.

The trust mode cannot be changed for an LAN/SFP+ port that is associated with an logical interface. However, in the case of settings for an LAN/SFP+ port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

Some QoS functions have limitations on execution depending on the trust mode, or may show different results.

[Example]

Set the trust mode of LAN/SFP+ port and logical interface to DSCP.

```
SWP2(config-if)#qos trust dscp
```

Set the trust mode of LAN/SFP+ port and logical interface to the default setting (CoS).

```
SWP2(config-if)#no qos trust
```

9.2.4 Show status of QoS function setting

[Syntax]

show qos

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the enabled (Enable) or disabled (Disable) status of the QoS function.

[Example]

Show the status of the system's QoS setting.

```
SWP2#show qos
  Enable
```

9.2.5 Show QoS information for interface

[Syntax]

show qos interface [*ifname*]

[Parameter]

ifname : Name of the LAN/SFP+ port or logical interface. If this is omitted, the command applies to all ports.
Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows QoS settings for the specified interface. The following content is shown.

Item	Description
Port Trust Mode	Trust mode of interface (CoS/DSCP/Port-Priority)
Input Policy-Map Name	Name of policy map already applied to the interface class map information (note 1)
Port Default CoS Priority	Default CoS value (note 2)
Port-Priority-Queue	Port priority order (note 3)
Egress Traffic Shaping	Traffic shaping (individual port)
Egress Traffic Queue Shaping	Traffic shaping (individual queue)
Queue Scheduling	Egress queue scheduling format and weight
CoS (Queue)	CoS - egress queue ID conversion table (note 2)
DSCP (Queue)	DSCP - egress queue ID conversion table (note 4)
Special Queue Assignment: Sent From CPU	Specify the egress queue of the frames transmitted from the CPU

Note 1) Not shown if no policy map is applied. For details on class map information, refer to the **show class-map** command.

Note 2) Shown only for CoS trust mode.

Note 3) Shown only if the trust mode is "port priority."

Note 4) Shown only for DSCP trust mode.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the QoS settings of LAN port #1. (trust mode CoS)

```
SWP2#show qos interface port1.1

  Port Trust Mode: CoS
```

```
  Port Default CoS Priority: 0

  Egress Traffic Shaping: Rate 30016 Kbps, Burst 1876 KByte

  Queue Scheduling:
  Queue0 : Weight  1 ( 5.3%)
  Queue1 : Weight  1 ( 5.3%)
  Queue2 : Weight  2 (10.5%)
  Queue3 : Weight  5 (26.3%)
  Queue4 : Weight  5 (26.3%)
  Queue5 : Weight  5 (26.3%)
  Queue6 : SP
  Queue7 : SP

  Cos (Queue): 0(2), 1(0), 2(1), 3(3), 4(4), 5(5), 6(6), 7(7)

  Special Queue Assignment:
    Sent From CPU: Queue7
```

Show the QoS settings of LAN port #1. (trust mode DSCP)

```
SWP2#show qos interface port1.1

  Port Trust Mode: DSCP

  Egress Traffic Shaping: Not Configured

  Queue Scheduling:
  Queue0 : SP
  Queue1 : SP
  Queue2 : SP
  Queue3 : SP
  Queue4 : SP
  Queue5 : SP
  Queue6 : SP
  Queue7 : SP

  DSCP (Queue):  0(2),  1(2),  2(2),  3(2),  4(2),  5(2),  6(2),  7(2)
                 8(0),  9(0), 10(0), 11(0), 12(0), 13(0), 14(0), 15(0)
                16(1), 17(1), 18(1), 19(1), 20(1), 21(1), 22(1), 23(1)
                24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
                32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
                40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
                48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
                56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)

  Special Queue Assignment:
    Sent From CPU: Queue7
```

9.2.6 Show egress queue usage ratio

[Syntax]

show qos queue-counters [*ifname*]

[Parameter]

ifname : Name of the LAN/SFP+ port. If this is omitted, the command applies to all ports.

Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the usage ratio for each egress queue of the specified LAN/SFP+ port. The queue usage ratio is calculated as follows.

(queue usage ratio) = (number of buffers held in the queue) / (maximum length of the queue)

[Note]

This command can be used regardless of the QoS status (enabled/disabled).

[Example]

Show the queue usage ratio of LAN port #1.

```
SWP2#show qos queue-counters port1.1
QoS: Enable
Interface port1.1 Queue Counters:
  Queue 0          59.4 %
  Queue 1          15.0 %
  Queue 2           0.0 %
  Queue 3           0.0 %
  Queue 4           0.0 %
  Queue 5           3.6 %
  Queue 6           0.0 %
  Queue 7           0.1 %
```

9.2.7 Set CoS - egress queue ID conversion table

[Syntax]

qos cos-queue *cos-value queue-id*
no qos cos-queue *cos-value*

[Parameter]

cos-value : <0-7>

CoS value of conversion source

queue-id : <0-7>

Egress queue ID corresponding to CoS value

[Initial value]

See [Note]

[Input mode]

global configuration mode

[Description]

Specifies the values of the CoS - egress queue ID conversion table that is used to determine the egress queue.

If this is executed with the "no" syntax, the egress queue ID for the specified CoS value is returned to the default setting.

The CoS - egress queue ID conversion table is used when the trust mode is set to CoS.

[Note]

In order to execute this command, QoS must be enabled.

The following table shows the default settings of the CoS - egress queue ID conversion table.

CoS value	Egress queue
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

[Example]

Assign egress queue #4 to CoS value "0".

```
SWP2(config)#qos cos-queue 0 4
```

Return the egress queue ID of CoS value "0" to the default value.

```
SWP2(config)#no qos cos-queue 0
```

9.2.8 Set DSCP - egress queue ID conversion tabl

[Syntax]

qos dscp-queue *dscp-value queue-id*
no qos dscp-queue *dscp-value*

[Parameter]

dscp-value : <0-63>
DSCP value of the conversion source

queue-id : <0-7>
Egress queue ID corresponding to DSCP value

[Initial value]

See [Note]

[Input mode]

global configuration mode

[Description]

Specifies the values of the DSCP - egress queue ID conversion table that is used to determine the egress queue.
If this is executed with the "no" syntax, the egress queue ID for the specified DSCP value is returned to the default setting.
The DSCP - egress queue ID conversion table is used when the trust mode is set to DSCP.

[Note]

In order to execute this command, QoS must be enabled.
The following table shows the default settings of the DSCP - egress queue ID conversion table.

DSCP value	Egress queue
0-7	2
8-15	0
16-23	1
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

[Example]

Assign egress queue #4 to DSCP value "0."

```
SWP2(config)#qos dscp-queue 0 4
```

Return the egress queue ID of DSCP value "23" to the default value.

```
SWP2(config)#no qos dscp-queue 23
```

9.2.9 Set port priority order

[Syntax]

qos port-priority-queue *queue-id*
no qos port-priority-queue

[Parameter]

queue-id : <0-7>
Egress queue ID assigned to LAN/SFP+ port

[Initial value]

qos port-priority-queue 2

[Input mode]

interface mode

[Description]

Specifies the priority (egress queue ID) for the receiving interface to LAN/SFP+ port and logical interface.

If this is executed with the "no" syntax, the egress queue ID for the specified interface is returned to the default setting (2).

The port priority is used to determine the egress queue when the trust mode is set to "port priority."

[Note]

In order to execute this command, QoS must be enabled.

If this is executed for an interface whose trust mode is not "port priority," the command results in an execution error.

An LAN/SFP+ port whose port priority differs cannot be aggregated as an logical interface.

If the interface for which this is executed is an LAN/SFP+ port that is associated with an logical interface, then this command produces an execution error. However, in the case of settings for an LAN/SFP+ port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Assign egress queue ID #4 as the port priority for LAN port #1.

```
SWP2#interface port1.1
SWP2(config-if)#qos port-priority-queue 4
```

9.2.10 Specify egress queue of frames transmitted from the switch itself

[Syntax]

qos queue sent-from-cpu *queue-id*
no qos queue sent-from-cpu

[Parameter]

queue-id : <0-7>
Egress queue ID

[Initial value]

qos queue sent-from-cpu 7

[Input mode]

global configuration mode

[Description]

Specifies the egress queue for the storage destination of frames sent to each LAN/SFP+ port from the switch itself (CPU).

If this is executed with the "no" syntax, the default value (7) is specified.

[Note]

In order to execute this command, QoS must be enabled.

If the priority order of frames sent from the CPU is lowered, transmission from a higher-priority queue takes priority; this means that under conditions of high load, functions such as L2MS or loop detection might stop working. For this reason, we recommend that you set this setting to as high a value (priority) as possible.

[Example]

Specify #5 as the storage destination egress queue for frames sent from the CPU.

```
SWP2(config)#qos queue sent-from-cpu 5
```

9.2.11 Generate class map (traffic category conditions)

[Syntax]

class-map *name*
no class-map *name*

[Parameter]

name : Name of class map (maximum 20 characters; uppercase and lowercase are distinguished)

[Input mode]

global configuration mode

[Description]

Generates a class map.

A class map defines the conditions used to classify received frames into traffic classes, and consists of conditions defined by the **match** command and the corresponding action (permit/deny).Class map actions are handled as follows. Class map actions are handled as follows.

- If an access list (ACL) is specified (execute the **match access-group** command)

  The class map action will be the action for the ACL.
- If other than an access list (ACL) is specified

  Permit.

After generating the class map, move to class map mode to specify its content.

If this command is executed with the "no" syntax, the specified class map is deleted.

[Note]

In order to execute this command, QoS must be enabled.

If the specified class map has already been generated, the change is applied to the previous settings. However, if a policy map has been applied to LAN/SFP+ port and logical interface, then the class map that is associated with the policy map cannot be edited or deleted.

[Example]

Create class map "class1."

```
SWP2(config)#class-map class1
SWP2(config-cmap)#
```

9.2.12 Associate class map

[Syntax]

class *name*
no class *name*

[Parameter]

name	:	Class map name

[Input mode]

policy map mode

[Description]

Associates a class map to a policy map.

When the class map association succeeds, move to policy map class mode. In policy map class mode, you can make the following settings for each traffic class.

- Pre-marking or specifying the egress queue
- Metering
- Policing
- Remarking

If this command is executed with the "no" syntax, the association of the class map to the policy map is canceled.

For LAN/SFP+ port and logical interface to which a policy map is applied, received frames are classified into traffic classes according to the conditions of the associated class map. If the action in the class map is "permit," the QoS processing specified by the user for that traffic class is performed.

Up to eight class maps can be associated to one policy map.

[Note]

In order to execute this command, QoS must be enabled.

It is meaningless to specify QoS processing settings for a traffic class for which the action is "deny."

[Example]

Make the following settings for received frames to LAN port #1.

- Permit traffic from the 10.1.0.0 network

- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.13 Set traffic classification conditions (access-list)

[Syntax]

match access-list *acl-id*
no match access-list *acl-id*

[Parameter]

acl-id : <1 - 2000>
IPv4 access list ID
: <2001 - 3000>
MAC access list ID
: <3001 - 4000>
IPv6 access list ID

[Input mode]

class map mode

[Description]

Uses the access list as the conditions to classify the traffic class.

If the received frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the traffic class.

If this is executed with the "no" syntax, the condition settings of the access list are deleted.

[Note]

In order to execute this command, QoS must be enabled.

A maximum of 39 conditions can be specified for traffic categorization in an access list.

[Example]

Specify access list #1 as the classification conditions for class map "class1."

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
```

9.2.14 Set traffic classification conditions (CoS)

[Syntax]

match cos *cos-list*
no match cos

[Parameter]

cos-list : <0 - 7>
CoS value used as classification condition. Up to eight can be registered.

[Input mode]

class map mode

[Description]

Uses the CoS value of the VLAN tag header as the condition to classify the traffic class.

If this is executed with the "no" syntax, the CoS condition setting is deleted.

The setting can be repeated up to the maximum number (eight) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify CoS values "1" and "2" as the classification conditions for class map "class1."

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match cos 1 2
```

9.2.15 Set traffic classification conditions (TOS precedence)

[Syntax]

match ip-precedence *tos-list*
no match ip-precedence

[Parameter]

tos-list : <0 - 7>

Value of the IP header's TOS precedence field used as a classification condition. Up to eight can be registered.

[Input mode]

class map mode

[Description]

Uses the value of the IP header's TOS precedence field as a condition to classify the traffic class.

If this is executed with the "no" syntax, the classification conditions using TOS precedence are deleted.

The setting can be repeated up to the maximum number (eight) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify TOS precedence values "3" and "4" as the classification conditions for class map "class1".

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match ip-precedence 3 4
```

9.2.16 Set traffic classification conditions (DSCP)

[Syntax]

match ip-dscp *dscp-list*
no match ip-dscp

[Parameter]

dscp-list : <0 - 63>

Value of the IP header's DSCP (DiffServ Code Point) field used as a classification condition. Up to eight can be registered.

[Input mode]

class map mode

[Description]

Uses the value of the IP header's DSCP (DiffServ Code Point) field as a condition to classify the traffic class.

If this is executed with the "no" syntax, the classification conditions using DSCP precedence are deleted.

The setting can be repeated up to the maximum number (eight) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify DSCP values "48" and "56" as the classification conditions for class map "class1."

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match ip-dscp 48 56
```

9.2.17 Set traffic classification conditions (Ethernet Type)

[Syntax]

match ethertype *type*
match ethertype *type* tagged
match ethertype *type* untagged
no match ethertype

[Keyword]

tagged	:	Set conditional VLAN tagging
untagged	:	Set conditional VLAN untagging

[Parameter]

type :

Specifies the type of the Ethernet frame.

Setting value	Description
0xXXXX	Hexadecimal expression of type value
any	All frame

[Input mode]

class map mode

[Description]

Uses the Ethernet frame's type value and the presence of a VLAN tag as the conditions to classify the traffic class.

If this command is executed with the "no" syntax, deletes conditional settings based on the Ethernet frame's type value and the presence of a VLAN tag.

If this setting has already been made by the **match ethertype** command, the content of the setting is changed.

[Note]

In order to execute this command, QoS must be enabled.

If applied to an access port, the "tagged" specification is invalid (because tagged frames are not handled by an access port).

[Example]

Set Ethernet frame type value "0x0800" as the classification condition for class map "class1."

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match ethertype 0x0800
```

9.2.18 13.2.22 Set traffic classification conditions (VLAN ID)

[Syntax]

match vlan *id*
no match vlan

[Parameter]

id : <1 - 4094>

VLAN ID used as classification condition

[Input mode]

class map mode

[Description]

Uses the VLAN ID as the condition to classify the traffic class.

If this is executed with the "no" syntax, the classification conditions using VLAN ID are deleted.

The setting can be repeated up to the maximum number (30) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify VLAN #20 as the classification conditions for class map "class1".

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match vlan 20
```

9.2.19 Set traffic classification conditions (VLAN ID range)

[Syntax]

match vlan-range *id-start* **to** *id-end*

[Parameter]

id-start : <1 - 4094>

Starting VLAN ID value used as classification condition.

id-end : <1 - 4094>

Ending VLAN ID value used as classification condition. The range from the specified starting value to the ending value can be a maximum of 30.

[Input mode]

class map mode

[Description]

Uses the VLAN ID as the condition to classify the traffic class.

To delete the classification condition, use the **no match vlan** command.

This can be used in conjunction with the setting of the **match vlan** command.

The **match vlan** command or **match vlan-range** command settings can be repeated up to the maximum number that can be registered (30).

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify VLAN #20 through #30 as the classification conditions for class map "class1".

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match vlan-range 20 to 30
```

9.2.20 Show class map information

[Syntax]

show class-map [*name*]

[Parameter]

name : Class map name. If this is omitted, all class map information is shown.

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows information for the specified class map. The following information is shown for each class map.

Section	Item	Description
Classification conditions (match)	Match Access-List	Access list ID
	Match ethertype	Ethernet Type
	Match vlan	VLAN ID
	Match vlan-range	
	Match CoS	CoS value
	Match IP precedence	TOS precedence
	Match IP DSCP	DSCP value

- The classification condition is shown only once for each type that is specified.
- A classification condition for which a corresponding command (match) is not set will not be shown.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show information for class map "class1".

```
SWP2#show class-map class1

    Class-Map Name: class1
      Match vlan 10
```

9.2.21 Generate policy map for received frames

[Syntax]

policy-map *name*
no policy-map *name*

[Parameter]

name : Name of policy map (maximum 32 characters; uppercase and lowercase are distinguished)

[Input mode]

global configuration mode

[Description]

Generates a policy map. The policy map combines the following processing for received frames, for each traffic class.

- Traffic classification
- Pre-marking
- Metering
- Policing
- Remarking

The policy map generated by this command can be applied to LAN/SFP+ port and logical interface by the **service-policy input** command. This classifies received frames into traffic classes according to each class map in the policy map, and applies the QoS process specified by the user to each class of traffic.

After generating the policy map, move to policy map mode to specify its content.

If this is executed with the "no" syntax, the specified policy map is deleted.

[Note]

In order to execute this command, QoS must be enabled.

If the specified policy map has already been generated, the change is applied to the previous settings. However, if the policy map is already applied to LAN/SFP+ port and logical interface, it cannot be edited or deleted.

[Example]

Make the following settings for received frames to LAN port #1.

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.22 Apply policy map for received frames

[Syntax]

service-policy input *name*
no service-policy *name*

[Parameter]

name : Name of policy map to apply

[Input mode]

interface mode

[Description]

Applies the policy map to the corresponding LAN/SFP+ port and logical interface.

If this is executed with the "no" syntax, the policy map is deleted from the LAN/SFP+ port and logical interface.

[Note]

In order to execute this command, QoS must be enabled.

If a policy map has already been applied to the LAN/SFP+ port and logical interface, an error occurs.

For a class map that is associated with a policy map, an error occurs if there is not even one setting that corresponds to the trust mode of the LAN/SFP+ port and logical interface. Of the class map settings, the following commands are limited in their applicability by the trust mode.

Trust mode	Command	Restrictions
CoS	**set ip-dscp-queue**	Cannot be used
DSCP	**set cos-queue**	Cannot be used
Port Priority	**set cos**	Cannot be used
	set ip-precedence	
	set ip-dscp	
	set cos-queue	
	set ip-dscp-queue	
	police, remark-map	Cannot use a combination for which remarking is enabled (*1)

*1) A combination for which remarking is enabled refers to when the yellow-action or red-action of the **police** command is set to "remark" and the **remark-map** of the corresponding color is specified.

An LAN/SFP+ port to which a policy map is applied cannot be associated with an logical interface.

A policy map cannot be applied to an LAN/SFP+ port that is associated with an logical interface. However, in the case of settings for an LAN/SFP+ port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Apply policy map "policy1" to LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

Remove policy map "policy1" from LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#no service-policy input policy1
```

9.2.23 Set pre-marking (CoS)

[Syntax]

set cos *value*
no set cos

[Parameter]

value : <0 - 7>

CoS value set by pre-marking

[Input mode]

policy map class mode

[Description]

Changes the CoS value of the classified traffic class to the specified CoS value. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

If this is executed with the "no" syntax, pre-marking processing of the CoS value corresponding to the traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Pre-marking cannot be used in conjunction with the set egress queue function.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to the CoS value "2"

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set cos 2
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.24 Set pre-marking (TOS precedence)

[Syntax]

set ip-precedence *value*
no set ip-precedence

[Parameter]

value : <0 - 7>

TOS precedence to specify by pre-marking

[Input mode]

policy map class mode

[Description]

Changes the value of the IP header's TOS precedence field of the classified traffic class to the specified TOS value. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

If this is executed with the "no" syntax, pre-marking processing of the TOS precedence corresponding to the traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Pre-marking cannot be used in conjunction with the set egress queue function.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to TOS precedence "5".

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set ip-precedence 5
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.25 Set pre-marking (DSCP)

[Syntax]

set ip-dscp *value*
no set dscp

[Parameter]

value : <0 - 63>

DSCP value specified by pre-marking

[Input mode]

policy map class mode

[Description]

Changes the DSCP value of the classified traffic class to the specified DSCP value. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

If this is executed with the "no" syntax, pre-marking processing of the DSCP value corresponding to the traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Pre-marking cannot be used in conjunction with the set egress queue function.

Up to four values may be used for pre-marking/remarking to a DSCP value not recommended in the RFC. The following table shows the DSCP values that are recommended in the RFC.

PHB	DSCP value	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to the DSCP value "10."

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.26 Set individual policers (single rate)

[Syntax]

police [single-rate] *CIR CBS EBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

single-rate	:	Use single-rate policer

[Parameter]

CIR	:	<1 - 102300000>
		Traffic rate (kbps)
CBS	:	<11 - 2097120>
		Burst size of conformant token bucket (kbyte)
EBS	:	<11 - 2097120>
		Burst size of excess token bucket (kbyte)
action	:	Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

policy map class mode

[Description]

Specifies individual policers (single rate) for the categorized traffic classes.

If the setting was already made by the **police** command, its content is changed.

Metering on the SWP2 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : Choose discard or remark

  However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (policy map class mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

This cannot be used in conjunction with the aggregate policer (**police-aggregate** command).

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.27 Set individual policers (twin rate)

[Syntax]

police twin-rate *CIR PIR CBS PBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

twin-rate : Use twin rate policers

[Parameter]

CIR : <1 - 102300000>

Traffic rate (kbps)

PIR : <1 - 102300000>

Peak traffic rate (kbps). A value less than CIR cannot be specified.

CBS : <11 - 2097120>

Burst size of conformant token bucket (kbyte)

PBS : <11 - 2097120>

Burst size of peak token bucket (kbyte)

action : Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

policy map class mode

[Description]

Specifies individual policers (twin rate) for the categorized traffic classes.

If the setting was already made by the **police** command, its content is changed.

Metering on the SWP2 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : Choose discard or remark

However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (policy map class mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

This cannot be used in conjunction with the aggregate policer (**police-aggregate** command).

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, PIR:96kbps, CBS:12kbyte, and PBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWP2(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-group 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police twin-rate 48 96 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.28 Set remarking of individual policers

[Syntax]

remark-map *color type value*
no remark-map

[Parameter]

color : Bandwidth class to remark

Setting value	Description
yellow	Make remarking settings for bandwidth class Yellow
red	Make remarking settings for bandwidth class Red

type : Type of remarking

Setting value	Description
cos	CoS remarking
ip-precedence	TOS precedence remarking
ip-dscp	DSCP remarking

value : <0 - 7>

CoS or TOS precedence remarking value

: <0 - 63>

DSCP remarking value

[Input mode]

policy map class mode

[Description]

Specifies remarking operations for bandwidth classes Yellow and Red that were classified by individual policers. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

For remarking, you can select either CoS value, TOS precedence, or DSCP value.

If this is executed with the "no" syntax, the remarking setting is deleted.

In order to perform remarking, you must specify this command and additionally use the **police** command (policy map class mode)) to specify "remark" as the action for the corresponding bandwidth class.

[Note]

In order to execute this command, QoS must be enabled.

Remarking can be used in conjunction with pre-marking and specifying the egress queue.

Up to four user-defined values may be used for pre-marking/remarking to a DSCP value not recommended in the RFC. The following table shows the DSCP values that are recommended in the RFC.

PHB	DSCP value	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[Example]

Make the following settings for received frames of LAN port #1@

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.29 Generate aggregate policer

[Syntax]

aggregate-police *name*
no aggregate-police *name*

[Parameter]

name : Name of aggregate policer (maximum 20 characters; uppercase and lowercase are distinguished)

[Input mode]

global configuration mode

[Description]

Generates an aggregate policer. If the policer has already been generated, this command edits its content.

When the command succeeds, you transition to aggregate policer mode, where you can edit the content of the aggregate policer.

If this command is executed with the "no" syntax, the aggregate policer is deleted.

In the following case, the content of the aggregate policer cannot be changed (you will not transition to aggregate policer mode).

- A policy map that includes a class map specified by the aggregate policer is applied to LAN/SFP+ port and logical interface.

In the following case, the aggregate policer cannot be deleted.

- The **police-aggregate** command was used to set the aggregate policer to a traffic class

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Generate aggregate policer "AGP-01".

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#
```

9.2.30 Set aggregate policer (single rate)

[Syntax]

police [single-rate] *CIR CBS EBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

single-rate : Use single-rate policer

[Parameter]

CIR : <1 - 102300000>

Traffic rate (kbps)

CBS : <11 - 2097120>

Burst size of conformant token bucket (kbyte)

EBS : <11 - 2097120>

Burst size of excess token bucket (kbyte)

action : Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

aggregate policer mode

[Description]

Specifies a single rate policer as an aggregate policer.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

Metering on the SWP2 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : : Choose discard or remark

  However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (aggregate policer mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Create an aggregate policer "AGP-01".

- Executing metering by SrTCM with CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

[Aggregate policer creating]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-action
drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

9.2.31 Set aggregate policer (twin rate)

[Syntax]

police twin-rate *CIR PIR CBS PBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

twin-rate	:	Use twin rate policers

[Parameter]

CIR	:	<1 - 102300000>
		Traffic rate (kbps)
PIR	:	<1 - 102300000>
		Peak traffic rate (kbps). A value less than CIR cannot be specified.
CBS	:	<11 - 2097120>
		Burst size of conformant token bucket (kbyte)
PBS	:	<11 - 2097120>
		Burst size of peak token bucket (kbyte)
action	:	Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

aggregate policer mode

[Description]

Specifies a twin rate policer as an aggregate policer.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

Metering on the SWP2 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : Choose discard or remark

  However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (aggregate policer mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Create an aggregate policer "AGP-01".

- Executing metering by TrTCM with CIR:48kbps, PIR:96kbps, CBS:12kbyte, and EBS:12kbyte

- Yellow: rewrite DSCP value to 10, Red: discard

[Aggregate policer creating]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

9.2.32 Set remarking of aggregate policers

[Syntax]

remark-map *color type value*
no remark-map

[Parameter]

color : Bandwidth class to remark

Setting value	Description
yellow	Make remarking settings for bandwidth class Yellow
red	Make remarking settings for bandwidth class Red

type : Type of remarking

Setting value	Description
cos	CoS remarking
ip-precedence	TOS precedence remarking
ip-dscp	DSCP remarking

value : <0 - 7>

CoS or TOS precedence remarking value

: <0 - 63>

DSCP remarking value

[Input mode]

aggregate policer mode

[Description]

Specifies remarking operations for bandwidth classes Yellow and Red that were classified by aggregate policers. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

For remarking, you can select either CoS value, TOS precedence, or DSCP value.

If this is executed with the "no" syntax, the remarking setting is deleted.

In order to perform remarking, you must specify this command and additionally use the **police** command (aggregate policer mode) to specify "remark" as the action for the corresponding bandwidth class.

[Note]

In order to execute this command, QoS must be enabled.

Remarking can be used in conjunction with pre-marking and specifying the egress queue.

Up to four user-defined values may be used for pre-marking/remarking to a DSCP value not recommended in the RFC. The following table shows the DSCP values that are recommended in the RFC.

PHB	DSCP value	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597

PHB	DSCP value	RFC
Expedited Forwarding(EF)	46	2598

[Example]

Make the following settings for aggregate policer "AGP-01".

- Executing metering by TrTCM with CIR:48kbps, PIR:96kbps, CBS:12kbyte, and PBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

[Aggregate policer creating]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

9.2.33 Show aggregate policers

[Syntax]

show aggregate-police [*name*]

[Parameter]

name : Aggregate policer name. If this is omitted, the command applies to all aggregate policers.

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the contents of an aggregate policer. The contents shown are the same as in the police section shown by the **show class-map** command.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the contents of aggregate policer "AGP-01".

```
SWP2#show aggregate-police AGP-01

      Aggregator-Police Name: AGP-01
          Mode: TrTCM
          average rate (48 Kbits/sec)
          peak rate (96 Kbits/sec)
          burst size (12 KBytes)
          peak burst size (16 KBytes)
          yellow-action (Transmit)
          red-action (Drop)
```

9.2.34 Apply aggregate policer

[Syntax]

police-aggregate *name*
no police-aggregate *name*

[Parameter]

name : Aggregate policer to apply

[Input mode]

policy map class mode

[Description]

Specifies an aggregate policer for a traffic class.

If this is executed with the "no" syntax, the aggregate policer settings for the traffic class are removed.

This cannot be used in conjunction with an individual policer (the **police single-rate and police twin-rate** commands of policy map class mode).

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Apply aggregate policer "AGP-01" to the two traffic classes "class1" and "class2" of policy map "policy1."

- Executing metering by SrTCM with CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

[Create an aggregate policer]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-action
drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

[Set policy]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police-aggregate AGP-01
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#class class2
SWP2(config-pmap-c)#police-aggregate AGP-01
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.35 Show metering counters

[Syntax]

show qos metering-counters [*ifname*]

[Parameter]

ifname : LAN/SFP+ port name or logical interface name. If this is omitted, the command applies to all ports.

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the metering totals for all policers (individual policers / aggregate policers) on the specified LAN/SFP+ port or logical interface.

The following totals are shown.

Item	Description
Green Bytes	Number of bytes categorized as bandwidth class Green
Yellow Bytes	Number of bytes categorized as bandwidth class Yellow
Red Bytes	Number of bytes categorized as bandwidth class Red

The count starts when the policy map is applied to the LAN/SFP+ port or logical interface.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the metering totals for LAN port #1.

```
SWP2#show qos metering-counters port1.1
Interface: port1.1(policy1)

  ****** Individual ******
  Class-map        : class1
      Green Bytes  : 178345
      Yellow Bytes : 0
      Red Bytes    : 0

  ****** Aggregate *******
  Aggregate-policer: AGP-01
```

```
 Class-map        : class2
                    class3
     Green Bytes  : 28672
     Yellow Bytes : 2048
     Red Bytes    : 51552
```

9.2.36 Clear metering counters

[Syntax]

clear qos metering-counters [*ifname*]

[Parameter]

ifname : LAN/SFP+ port name or logical interface name. If this is omitted, the command applies to all ports.

[Input mode]

priviledged EXEC mode

[Description]

Clears the metering totals for all policers (individual policers / aggregate policers) on the specified LAN/SFP+ port or logical interface.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Clear the metering totals for LAN port #1.

```
SWP2#clear qos metering-counter port1.1
```

9.2.37 Set egress queue (CoS-Queue)

[Syntax]

set cos-queue *value*
no set cos-queue

[Parameter]

value : <0 - 7>

CoS value corresponding to egress queue

[Input mode]

policy map class mode

[Description]

Assigns an egress queue to the classified traffic class.

Use the CoS value to specify the egress queue; the egress queue that is assigned is based on the "CoS-egress queue ID conversion table."

If this is executed with the "no" syntax, the specification of egress queue based on traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Egress queue specification cannot be used in conjunction with pre-marking.

Egress queue specification based on CoS is only for CoS trust mode. If a policy map contains even one class map that includes this command, that policy map cannot be applied to a port that uses DSCP trust mode.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to egress queue 3 (CoS:3)

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set cos-queue 3
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.38 Set egress queue (DSCP-Queue)

[Syntax]

set ip-dscp-queue *value*
no set ip-dscp-queue

[Parameter]

value : <0 - 63>

DSCP value corresponding to egress queue

[Input mode]

policy map class mode

[Description]

Assigns an egress queue to the classified traffic class.

Use the DSCP value to specify the egress queue; the egress queue that is assigned is based on the "DSCP-egress queue ID conversion table."

If this is executed with the "no" syntax, the specification of egress queue based on traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Egress queue specification cannot be used in conjunction with pre-marking.

Egress queue specification based on DSCP is only for DSCP trust mode. If a policy map contains even one class map that includes this command, that policy map cannot be applied to a port that uses DSCP trust mode.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to egress queue 3 (DSCP:24)

[Traffic class definition]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[Policy settings]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set ip-dscp-queue 24
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.39 Show policy map information

[Syntax]

show policy-map [*name*]

[Parameter]

name : Policy map name. If this is omitted, all policy map information is shown.

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows information for the specified policy map. The following content is shown.

Item	Description
Policy-Map Name	Policy map name
State	Application status of the policy map (attached/detached)
Class-Map Name	Class map information. For details, refer to the **show class-map** command.
Match	Classification conditions - Match Access-List (Access list ID) - Match ethertype (Ethernet Type) - Match vlan (VLAN ID) - Match vlan-range (VLAN ID) - Match CoS (CoS value) - Match IP precedence (TOS precedence) - Match IP DSCP (DSCP value)
Set	Pre-marking setting, egress queue setting - Set CoS (Pre-marking setting : CoS value) - Set IP precedence (Pre-marking setting : TOS precedence) - Set IP DSCP (Pre-marking setting : DSCP value) - Set CoS-Queue (Specify egress queue : CoS - Set IP-DSCP-Queue (Specify egress queue : DSCP)
Police	Metering/policing/remarking setting * For details, refer to the following

Details of metering, policing, and remarking settings are as follows.

Item		Description
Aggregator-Police Name		Name of aggregate policer (only if specified)
Mode		Metering algorithm (SrTCM/TrTCM)
Shown only for SrTCM	average rate	Traffic rate (kbits/sec)
	burst size	Burst size of conformant token bucket (kBytes)
	excess burst size	Burst size of excess token bucket (kBytes)
Shown only for TrTCM	average rate	Traffic rate (kbits/sec)
	peak rate	Peak traffic rate (kbits/sec)
	burst size	Burst size of conformant token bucket (kBytes)
	peak burst size	Burst size of peak token bucket (kBytes)
yellow-action		Action for bandwidth class Yellow (transmit/drop/remark)
red-action		Action for bandwidth class Red (drop/remark)

- Of the various items in the "Match" and the "Set", only the single item that has been specified is shown.
- The "Match", the "Set", and the "Police" are not shown if the corresponding command (match, set, police) has not been specified.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show information for policy map "policy1".

```
SWP2#show policy-map policy1

  Policy-Map Name: policy1
    State: attached

    Class-Map Name: class1
      Qos-Access-List Name: 1
      Police: Mode: SrTCM
              average rate (48 Kbits/sec)
              burst size (12 KBytes)
              excess burst size (12 KBytes)
              yellow-action (Remark [DSCP:10])
              red-action (Drop)
```

9.2.40 Show map status

[Syntax]

show qos map-status *type* [*name*]

[Parameter]

type : Type of map to show

Setting value	Description
policy	Show policy map status information
class	Show class map status information

name : The name of the policy map (or class map) to show. If this is omitted, all policy maps (or class maps)

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows policy map or class map status information.

By using this command, you can obtain information about the combination of policy maps or class maps, such as the LAN/SFP+ ports and logical interfaces to which a policy map is applied, or the policy maps to which a class map is registered.

The following content is displayed.

policy-map

Item	Display information
input port	List of LAN/SFP+ ports and logical interfaces to which the policy map is applied
edit/erase	Whether **policy-map**/**no policy-map** can be executed
attach limitation	Whether attachment is possible for each trust mode

class-map

Item	Display information
policy-map asociation	List of policy maps to which the class map is associated
edit/erase	Whether **class-map**/**no class-map** can be executed
attach limitation	Whether attachment is possible for each trust mode

Use the **show policy-map** and **show class-map** commands to check the settings of the policy map or class map.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the status of policy map "policy1".

```
SWP2#show qos map-status policy policy1
policy1 status
  input port            : port1.3

  edit/erase            : Disable

  attach limitation
    CoS trust mode           : Enable
    DSCP trust mode          : Enable
    Port-Priority trust mode : Disable
```

Show the status of class map "class1".

```
SWP2#show qos map-status class class1
class1 status
  policy-map association : policy1 (Detached)

  edit/erase             : Disable

  attach limitation
    CoS trust mode           : Enable
    DSCP trust mode          : Enable
    Port-Priority trust mode : Disable
```

9.2.41 Set egress queue scheduling

[Syntax]

qos wrr-weight *queue-id weight*
no qos wrr-weight *queue-id*

[Parameter]

queue-id : <0-7>
Egress queue ID

weight : <1-32>
Weight of WRR

[Initial value]

no qos wrr-weight 0

no qos wrr-weight 1

no qos wrr-weight 2

no qos wrr-weight 3

no qos wrr-weight 4

no qos wrr-weight 5

no qos wrr-weight 6

no qos wrr-weight 7

[Input mode]

global configuration mode

[Description]

Specifies the WRR (weighted round robin) weight for the egress queue.

The scheduling method setting is common to all LAN/SFP+ ports and logical interfaces.

If this is executed with the "no" syntax, the egress queue uses the strict priority (SP) method.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Set egress queues #7 and #6 to the SP method (7 has priority), and set #5, #4, #3, #2, #1, and #0 to the WRR method (5:5:5:2:1:1).

```
SWP2(config)#no qos wrr-weight 7
SWP2(config)#no qos wrr-weight 6
SWP2(config)#qos wrr-weight 5 5
SWP2(config)#qos wrr-weight 4 5
SWP2(config)#qos wrr-weight 3 5
SWP2(config)#qos wrr-weight 2 2
SWP2(config)#qos wrr-weight 1 1
SWP2(config)#qos wrr-weight 0 1
```

9.2.42 Set traffic shaping (individual port)

[Syntax]

traffic-shape rate kbps *CIR* **burst** *BC*
no traffic-shape rate

[Parameter]

CIR : <18-1000000>

Traffic rate (kbps). Due to rounding, the actual value applied may differ from the input value (see [note])

BC : <4-16000>

Burst size (kbyte). Specified in 4-kbyte units.

[Initial value]

no traffic-shape rate

[Input mode]

interface mode

[Description]

Specifies shaping for the port.

If this is executed with the "no" syntax, the port shaping setting is disabled.

[Note]

In order to execute this command, QoS must be enabled.

Due to the rounding of traffic rates, the actual value applied may differ from the input value.

[Example]

Reduce transmission from LAN port #1 down to CIR:30016 kbps, Bc:1876000 byte.

```
SWP2(config)#interface port1.1
SWP2(config-if)#traffic-shape rate kbps 30016 burst 1876
```

9.2.43 Set traffic-shaping (queue units)

[Syntax]

traffic-shape queue *queue-id* **rate kbps** *CIR* **burst** *BC*
no traffic-shape queue *queue-id* **rate**

[Parameter]

queue-id : <0-7>

Egress queue ID

CIR : <18-1000000>

Traffic rate (kbps). Due to rounding, the actual value applied may differ from the input value (see [note])

BC : <4-16000>

Burst size (kbyte). Specified in 4-kbyte units.

[Initial value]

no traffic-shpe queue 0 rate

no traffic-shpe queue 1 rate

no traffic-shpe queue 2 rate

no traffic-shpe queue 3 rate

no traffic-shpe queue 4 rate

no traffic-shpe queue 5 rate

no traffic-shpe queue 6 rate

no traffic-shpe queue 7 rate

[Input mode]

interface mode

[Description]

Specifies shaping for the egress queue of the port.

If this is executed with the "no" syntax, the egress queue shaping setting is disabled.

[Note]

In order to execute this command, QoS must be enabled.

Due to the rounding of traffic rates, the actual value applied may differ from the input value.

[Example]

Reduce transmission from queue #0 of LAN port #1 down to CIR:10 Mbps and Bc:64000 byte.

```
SWP2(config)#interface port1.1
SWP2(config-if)#traffic-shape queue 0 rate kbps 10000 burst 64
```

9.3 Flow control

9.3.1 Set flow control (IEEE 802.3x PAUSE send/receive) (system)

[Syntax]

flowcontrol *type*
no flowcontrol

[Parameter]

type : Flow control operation

Setting value	Description
enable	Enables flow control
disable	Disables flow control

[Initial value]

flowcontrol disable

[Input mode]

global configuration mode

[Description]

Enables flow control for the entire system (IEEE 802.3x PAUSE frames send/receive).

If this is executed with the "no" syntax, flow control is disabled.

[Note]

If the QoS function is enabled, it is not possible to enable flow control for the system.

If flow control is enabled, the tail drop function is automatically disabled.

Flow control for each interface operates only if the flow control settings of the system and of the interface are each enabled.

[Example]

Enable flow control for system.

```
SWP2(config)#flowcontrol enable
```

9.3.2 Set flow control (IEEE 802.3x PAUSE send/receive) (interface)

[Syntax]

flowcontrol *type*
no flowcontrol

[Parameter]

type : Flow control operation

Setting value	Description
auto	Enable flow control auto negotiation
both	Enable transmission/reception of Pause frames
disable	Disable flow control

[Initial value]

flowcontrol disable

[Input mode]

interface mode

[Description]

Enables flow control for the LAN/SFP+ port (IEEE 802.3x PAUSE frames send/receive).

If this command is executed with the "no" syntax, flow control is disabled.

[Note]

This command can be specified only for LAN/SFP+ port.

This will not operate if flow control is disabled for the system.

Sending and receiving of PAUSE frames are enabled or disabled as a set. (It is not possible to enable only send or receive.)

The period of pause time requested when the SWP2 transmits a PAUSE frame is 0xFFFF (65535).

[Example]

Enable flow control for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#flowcontrol both
```

Disable flow control for LAN port #1.

```
SWP2(config)#interface port1.1
SWP2(config-if)#no flowcontrol
```

9.3.3 Show flow control operating status

[Syntax]

show flowcontrol [inteface *ifname*]

[Keyword]

interface : Specifies the interface to show

[Parameter]

ifname : Name of LAN/SFP+ port. If this is omitted, the command applies to all interfaces.

Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows information related to flow control (enabled/disabled, number of PAUSE frames sent/received).

[Note]

The number of PAUSE frames sent and received are shown only if flow control is enabled on the corresponding port.

The number of PAUSE frames sent and received is cleared when you execute the **clear frame-counters** command.

[Example]

Show flow control information for LAN port #1.

```
SWP2#show flowcontrol port1.1
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Both                 4337       0
```

Show flow control information for all ports.

```
SWP2#show flowcontrol
System flow-control: Enable
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Both                 4337       0
port1.2     Disable                 -       -
port1.3     Both                    0    1732
port1.4     Disable                 -       -
port1.5     Disable                 -       -
port1.6     Disable                 -       -
port1.7     Disable                 -       -
port1.8     Disable                 -       -
```

9.4 Storm control

9.4.1 Set storm control

[Syntax]

storm-control *type* [*type*..] **level** *level*
no storm-control

[Parameter]

type : Storm control type

Storm control type	Description
broadcast	Enables broadcast storm control
multicast	Enables multicast storm control
unicast	Enables control for unicast frames with unknown address

level : <0.00-100.00>

Specifies the threshold value as a percentage of the bandwidth
The threshold value can be specified to the second decimal place

[Initial value]

no storm-control

[Input mode]

interface mode

[Description]

Applies reception restrictions to a LAN/SFP+ port, enabling broadcast storm control, multicast storm control, and control of unicast frames with unknown address.

Incoming frames that exceed the threshold value are discarded. However, no reception restrictions are applied if the threshold value is 100%. The threshold value is common to all frames, and cannot be specified individually.

[Example]

Enable broadcast storm control and multicast storm control for LAN port #1, and set the threshold value to 30%.

```
SWP2(config)#interface port1.1
SWP2(config-if)#storm-control broadcast multicast level 30
```

9.4.2 Show storm control reception upper limit

[Syntax]

show storm-control [*ifname*]

[Parameter]

ifname	:	LAN/SFP+ port interface name Interface to show

[Initial value]

none

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the upper limit value for frame reception.

If the interface name is omitted, all interfaces are shown.

[Example]

Show the setting status of all interfaces.

```
SWP2#show storm-control
Port      BcastLevel    McastLevel    UcastLevel
port1.1     30.00%        30.00%       100.00%
port1.2     20.00%        20.00%        20.00%
port1.3    100.00%       100.00%       100.00%
port1.4    100.00%       100.00%       100.00%
port1.5     50.00%        50.00%       100.00%
port1.6    100.00%       100.00%       100.00%
port1.7    100.00%       100.00%        30.00%
port1.8    100.00%       100.00%        30.00%
```

Chapter 10

Application

10.1 Local RADIUS server

10.1.1 Local RADIUS server function settings

[Syntax]

radius-server local enable [*port*]
radius-server local disable
no radius-server local

[Parameter]

port : <1024-65535>
UDP port number used for authentication (the default value of 1812 is used when this is omitted)

[Initial value]

radius-server local disable

[Input mode]

global configuration mode

[Description]

Enables/disables the settings for the local RADIUS server function.

You can also change the authentication UDP port number.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To use the local RADIUS server functions, you must first use the **crypto pki generate ca** command to generate a route certificate authority.

[Example]

Enables the local RADIUS server function.

```
SWP2(config)#radius-server local enable
```

10.1.2 Set access interface

[Syntax]

radius-server local interface *interface*
no radius-server local interface

[Parameter]

interface : VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the local RADIUS server.

Up to seven access interfaces can be specified.

If the command is executed with the "no" syntax, the specified interface is deleted.

[Example]

Allows access to the RADIUS client (NAS) connected to VLAN #1 and VLAN #100.

```
SWP2(config)#radius-server local interface vlan1
SWP2(config)#radius-server local interface vlan100
```

10.1.3 Generate a route certificate authority

[Syntax]

crypto pki generate ca [*ca-name*]
no crypto pki generate ca

[Parameter]

ca-name : Certificate authority name

Characters that can be inputted for the certificate authority name

- Within 3–32 characters
- Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
- Cannot specify “DEFAULT”

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates a route certificate authority to issue a client certificate.

“YAMAHA_SWITCH” will be used when the certificate authority is omitted.

If this command is executed with the "no" syntax, the specified route certificate authority is deleted.

[Note]

If a route certificate authority has not been generated, the functions of the local RADIUS server cannot be used.

When setting a different route certificate authority name when a route certificate authority has already been generated, the route certificate authority will be overwritten.

When the route certificate authority is deleted or overwritten, all client certificates already issued will become invalid.

Even if a route certificate authority exists, it cannot be used as such unless the **crypto pki generate ca** settings have not been made.

[Example]

This generates a route certificate authority with the name “MY RADIUS”.

```
SWP2(config)#crypto pki generate ca MYRADIUS
```

10.1.4 RADIUS configuration mode

[Syntax]

radius-server local-profile

[Input mode]

global configuration mode

[Description]

Switches to the RADIUS configuration mode.

This mode is used to configure the operating specifications for the local RADIUS server function.

[Example]

Switches to the RADIUS configuration mode.

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#
```

10.1.5 Authentication method settings

[Syntax]

authentication *mode* [*mode*...]
no authentication

[Parameter]

mode : Authentication method

Setting value	Description
pap	PAP authentication method
peap	PEAP authentication method
eap-md5	EAP-MD5 authentication method
eap-tls	EAP-TLS authentication method
eap-ttls	EAP-TTLS authentication method

[Initial value]

authentication pap peap eap-md5 eap-tls eap-ttls

[Input mode]

RADIUS configuration mode

[Description]

Specifies the authentication method used for the local RADIUS server.

If this command is executed with the "no" syntax, the setting is returned to its default, and all authentication methods will be enabled.

[Note]

As an internal authentication method for PEAP and EAP-TTLS, this supports MSCHAPv2 and MD5.

The authentication method must be set to “eap-md5” when using MD5.

[Example]

This restricts the authentication method to PEAP and EAP-MD5.

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#authentication peap eap-md5
```

10.1.6 RADIUS client (NAS) settings

[Syntax]

nas *host* key *secret*
no nas *host*

[Keyword]

key : Sets the password used for communicating with the RADIUS client (NAS)

[Parameter]

host : IP address, or IP network address

Setting value	Description
IPv4 address (A.B.C.D)	Range from 0.0.0.1 to 223.255.255.255, except for 127.0.0.1
IPv4 network address (A.B.C.D/M)	The network mask range is from 8 to 32, and the IP address host part will be “0”
IPv6 address (A:B:C::D)	Out of all unicast addresses, the exceptions are unspecified addresses (::/128), default root addresses (::/0) and loopback addresses (::1/128)
IPv6 network address (A:B:C::D/M)	The prefix length is 1–128

secret : Shared password

(128 characters or less, single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces)

[Initial value]

nas 127.0.0.1 key secret_local

[Input mode]

RADIUS configuration mode

[Description]

Adds a RADIUS client (NAS) to the RADIUS client list.

The maximum number of registered entries is 100.

If this command is executed with the "no" syntax, the specified RADIUS client setting is deleted.

[Note]

RADIUS client (NAS) information configured using this command will not display in running-config or startup-config.

Also, this is different from the regular settings command, in that it will be saved as setting data when this command is executed.

Information for the RADIUS client (NAS) that was set can be checked using the **show radius-server local nas** command.

The following settings must be made when specifying a local RADIUS server using the port authentication function of this device.

```
SWP2(config)#radius-server host 127.0.0.1 key secret_local
```

[Example]

Add the RADIUS client (NAS) at IP address 192.168.100.101, with a shared password of "abcde".

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#nas 192.168.100.101 key abcde
```

10.1.7 Authenticated user settings

[Syntax]

user *userid password* [vlan *vlan-id*] [mac *mac-address*] [ssid *ssid*] [name *name*] [mail *mail-address*] [auth *type*] [expire *date*]

no user *userid*

[Keyword]

vlan	:	Set the VLAN for dynamic VLAN
mac	:	Specify the terminal's MAC address when you want to specify an authentication terminal
ssid	:	Specify the SSID when you want to specify a connected SSID
name	:	Specify the user name
mail	:	Set the e-mail addresses to which client certificates will be distributed
auth	:	Set the authentication method type
expire	:	Set the term of validity for the client certificate (this is enabled only when the authentication method is EAP-TLS)

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify "DEFAULT")

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces

password : Password

(32 characters or less, single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces)

vlan-id : <1-4094>

VLAN number for dynamic VLAN

mac-address : hhhh.hhhh.hhhh (h is hexadecimal)

MAC address for terminal (user) to authenticate

ssid : SSID connection point

(32 characters or less, single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces)

name : User name

(32 characters or less, single-byte alphanumeric characters and symbols other than the characters " ? and spaces

mail-address : Mail address

(256 characters or less, single-byte alphanumeric characters and _ - . @)

type : Type of authentication method

Setting value	Description
pap	PAP authentication method (this type uses the user ID and password)
peap	PEAP, EAP-MD5, EAP-TTLS authentication method (this type uses the user ID and password)
eap-tls	EAP-TLS authentication method (this type uses the user ID and password)

When abbreviating, use “eap-tls”

date : Date (“2037/12/31” is used when omitted)

(YYYY/MM/DD from current date to 2037/12/31)

[Initial value]

none

[Input mode]

RADIUS configuration mode

[Description]

This registers the user to be authenticated with the RADIUS server.

The maximum number of registered entries is 2000.

If this command is executed with the "no" syntax, the specified user is deleted.

When the authentication method is EAP-TLS, client certificates need to be issued by executing the **certificate user** command.

Client certificates must be reissued for users for whom the term of validity has been changed on their password or client certificate.

When deleting a user whose client certificate has already been issued, the client certificate will automatically be processed for revocation.

[Note]

Information configured using this command will not display in running-config or startup-config.

Also, this is different from the regular settings command, in that it will be saved as setting data when this command is executed.

User information that was set can be checked using the **show radius-server local user** command.

MAC addresses specified using the “mac” keyword are used when the RADIUS client (NAS) notifies its Calling-Station-Id.

SSID specified using the “ssid” keyword are used when the RADIUS client (NAS) notifies its Calling-Station-Id.

[Example]

This registers the authenticated user.

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#user yamaha secretpassword mac 00a0.de00.0001 auth peap name
YamahaTaro
```

10.1.8 Reauthentication interval setting

[Syntax]

reauth interval *time*
no reauth interval

[Parameter]

time : <3600,43200,86400,604800>
Reauthentication interval (no. of seconds)

[Initial value]

reauth interval 3600

[Input mode]

RADIUS configuration mode

[Description]

Sets the reauthentication interval that is notified to the RADIUS client (NAS).

The RADIUS client (NAS) determines whether the reauthentication interval will be used.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This sets the reauthentication interval to 604800 seconds.

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#reauth interval 604800
```

10.1.9 Apply setting data to local RADIUS server

[Syntax]

radius-server local refresh

[Input mode]

priviledged EXEC mode

[Description]

This applies the current settings to the local RADIUS server.

If the RADIUS-related settings have been modified, this command must be executed to update the data of the local RADIUS server.

[Note]

When this command is executed, operations will be temporarily halted and restarted afterwards, so that the data can be applied to the local RADIUS server.

[Example]

Applies the current settings to the local RADIUS server.

```
SWP2#radius-server local refresh
```

10.1.10 Issuing a client certificate

[Syntax]

certificate [mail] **user** [*userid*]

[Keyword]

mail : This issues a client certificate and sends the certificate to the user via e-mail attachment.

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

priviledged EXEC mode

[Description]

This issues client certificates to users for which the EAP-TLS certification method is specified.

If the user ID is omitted, client certificates will be sent for all users who meet the following conditions.

- Users to whom a client certificate has never been issued
- Users whose passwords or client certificate’s term of validity has been changed
- Users whose authentication method has been changed to EAP-TLS

This automatically revokes the client certificates for users whose authentication methods have been changed from EAP-TLS to a method other than EAP-TLS.

When the “mail” keyword is specified, this sends a client certificate to the e-mail address set using the **user** command.

The e-mail subject and body text follow the e-mail settings template (**mail send certificate** command) used when the certificate was sent.

E-mails cannot be sent if an e-mail address has not been set.

[Note]

Up to two client certificates may be issued per user. If two or more client certificates are issued, the older ones will be revoked.

As bulk issuance of client certificates takes time, this is performed in the background, and other commands may be executed while the certificates are being issued.

However, note that the following commands may not be executed due to restrictions.

- crypto pki generate ca
- no crypto pki generate ca
- nas
- user
- certificate user
- certificate mail user
- certificate revoke

[Example]

Bulk issuance of client certificates.

```
SWP2#certificate user
```

10.1.11 Aborting the issue of a client certificate

[Syntax]

certificate abort

[Input mode]

priviledged EXEC mode

[Description]

This aborts the bulk issuance of client certificates.

The issuance of client certificates can be restarted by executing the **certificate user** command once more.

[Example]

Aborts the bulk issuance of client certificates.

```
SWP2#certificate abort
```

10.1.12 Revoking client certificates

[Syntax]

certificate revoke user *userid*
certificate revoke id *certificate-id*

[Keyword]

user	:	Revoking client certificates for specified users
id	:	Revoking client certificates for specified client certificate IDs

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

certificate-id : Client certificate ID

Combination of “user ID” and “serial number”

[Input mode]

priviledged EXEC mode

[Description]

This revokes client certificates for specified users or client certificate IDs.

In the event that a client certificate is revoked, the authorization using that certificate will fail.

[Note]

Client certificate IDs (certificate-id) can be checked using the **show radius-server local certificate list** command.

[Example]

This revokes the client certificate for user ID “Taro”.

```
SWP2#certificate revoke user Taro
```

This revokes the client certificate for client certificate ID “Taro-DF598EE9B44D22CC”.

```
SWP2#certificate revoke id Taro-DF598EE9B44D22CC
```

10.1.13 Exporting of client certificates (sending via e-mail)

[Syntax]

certificate export mail all compress
certificate export mail user *userid* **compress**

[Keyword]

all	:	Send client certificates for all users via e-mail
user	:	Send client certificates for specified users via e-mail
compress	:	Compress into a ZIP file

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted:
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

priviledged EXEC mode

[Description]

Sends client certificates to each user via e-mail attachment.

Client certificates to be sent are ZIP files, compressed using the passwords for each user.

E-mail cannot be sent to users whose e-mail addresses have not been set.

To send e-mail, the e-mail destination server and e-mail recipient name must be configured in the e-mail template, and an e-mail template ID for use when sending the e-mail must be set using the **mail send certificate** command.

[Note]

Only the newest client certificate (1) can be sent via e-mail.

[Example]

This sends a client certificate via e-mail to the user with the “Yamaha” user ID.

```
SWP2#certificate export mail user Yamaha
```

10.1.14 Show RADIUS client (NAS) status

[Syntax]

show radius-server local nas *host*

[Parameter]

host : IP address or IP network address

Setting value	Description
IPv4 address (A.B.C.D)	Range from 0.0.0.1 to 223.255.255.255, except for 127.0.0.1
IPv4 network address (A.B.C.D/M)	The network mask range is from 8 to 32, and the IP address host part will be “0”
IPv6 address (A:B:C::D)	Out of all unicast addresses, the exceptions are unspecified addresses (::/128), default root addresses (::/0) and loopback addresses (::1/128)
IPv6 network address (A:B:C::D/M)	The prefix length is 1–128

[Input mode]

priviledged EXEC mode

[Description]

Shows a list of RADIUS clients (NAS).

[Example]

Shows the RADIUS clients (NAS) with an IP address of “192.168.100.0/24”.

```
SWP2#show radius-server local nas 192.168.100.0/24
host                                    key
------------------------------------------------------------------------------
------------------
192.168.100.0/24                        abcde
```

10.1.15 Show authenticated user information

[Syntax]

show radius-server local user [detail *userid*]

[Keyword]

detail	:	Show detailed information for the specified user

[Parameter]

userid	:	User ID (within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

priviledged EXEC mode

[Description]

This shows the user information.

[Example]

Shows the user information list.

```
SWP2#show radius-server local user
Total     1

userid                          name                                vlan mode
-------------------------------------------------------------------------------
00a0de001080                    YamahaTaro                             1 eap-md5
```

Shows user information for user ID “00a0de000001”.

```
SWP2#show radius-server local user detail 00a0de000001
Total     1

userid      : 00a0de000001
password    : secretpassword
mode        : eap-tls
vlan        : 10
MAC         : 00a0.de00.0001
SSID        :
name        : YamahaTaro
mail-address: test.com
expire date : 2037/12/31
certificated: Not
```

10.1.16 Client certificate issuance status display

[Syntax]

show radius-server local certificate status

[Input mode]

priviledged EXEC mode

[Description]

Shows the issuance status for client certificates.

Issuance status	Contents
done	Client certificate issuance completed, or not issued
processing	Now issuing client certificate

Issuance status	Contents
aborted	Issuance of client certificate aborted by executing “certificate abort” or other command

[Example]

Shows the issuance status for client certificates.

```
SWP2#show radius-server local certificate status
certificate process: done.
```

10.1.17 Client certificate list display

[Syntax]

show radius-server local certificate list [**detail** *userid*]

[Keyword]

detail : Output the list of details

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

priviledged EXEC mode

[Description]

This shows the list of client certificates that have been issued.

Specifying *userid* will show detailed information for that user.

[Example]

This displays client certificates that have been issued for specific users.

```
SWP2#show radius-server local certificate list detail Yamaha

userid                          certificate number
enddate
-------------------------------------------------------------------------------
--------
Yamaha                          Yamaha-DF598EE9B44D22CC
2018/12/31
                                Yamaha-DF598EE9B44D22CD
2019/12/31
```

10.1.18 Revoked client certificate list display

[Syntax]

show radius-server local certificate revoke

[Input mode]

priviledged EXEC mode

[Description]

This shows a list of client certificates that have been processed for revocation.

Reason for revocation	Contents
revoked	Manual revocation

Reason for revocation	Contents
expired	Revocation due to expired term of validity

[Example]

Displays the list of revoked client certificates.

```
SWP2#show radius-server local certificate revoke

userid                          certificate number
reason
--------------------------------------------------------------------------------
--------
Yamaha                          Yamaha-DF598EE9B44D22CC
expired
                                Yamaha-DF598EE9B44D22CD
revoked
```

Index

L

M

N

P

Q

R

S

T

U

V

W

Y