Yamaha L2 Switch

SWP1 Series(SWP1-8, SWP1-8MMF, SWP1-16MMF)

Command Reference

Rev.2.01.11

Contents

Preface

Introduction

- All copyrights to the software and this command reference are the property of Yamaha Corporation.
- 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.
- 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 products

This command reference applies to the Yamaha SWP1 series of L2 switches (SWP1-8, SWP1-8MMF, SWP1-16MMF).
Refer to the following website for the latest information on firmware.
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 SWP1.

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]	Indicates the default setting 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 SWP1.

Interface type	Prefix	Description	Examples
LAN/SFP port	ge	Used to specify a physical port. Specify ge followed by the port number.	To specify LAN port #1: ge1
VLAN interface	vlan	Used to specify a VLAN. Specify vlan followed by "bridge ID (fixed at 0)" + "." + "VLAN ID".	To specify VLAN #1: vlan0.1
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 SWP1 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	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 SWP1, 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

To make settings from a terminal connected to the CONSOLE port of the SWP1, use an RJ-45/DB-9 serial cable. 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	none

For settings related to the console terminal, use the **line console** 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 SWP1 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 SWP1 are as follows.

- The default IPv4 address setting is automatically specified by DHCP for VLAN #1 (vlan0.1).
- To change the IPv4 address, use the **ip address** command.

The TELNET server settings of the SWP1 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 **service 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 SWP1. The VTY ports of the SWP1 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 SWP1, 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 Console terminal/VTY settings

The SWP1 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.
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 SWP1 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 SWP1 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 SWP1 are as follows.

- The default IPv4 address setting is automatically specified by DHCP for VLAN #1 (vlan0.1).
- To change the IPv4 address, use the **ip address** command.

The TFTP server settings of the SWP1 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.
- The reception port number cannot be changed.
- 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.

- Config file

Applicable config file	Description	Remarks
running-config	Setting values for current operation	
startup-config for USER mode	Saved setting values	Setting values when starting up with DIP switch #1 ON

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 SWP1
- Use "binary mode" as the transmission mode.
- Specify the following as the remote path of the configuration file read (GET) or write (PUT) destination.

Remote path	Applicable config file	Load (GET)	Save (PUT)	Automatic restart
config	running-config	✓	✓	-
config0	startup-config for USER mode	✓	✓	-
reconfig	startup-config for USER mode	-	✓	✓

- You must append the administrator password to the remote path (format: "/PASSWORD"). You cannot read or write the settings file while the default administrator password is still being used. To do this, you must first change the administrator password.
- 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.
- If you want to start operation in USER mode with a completely new config file, specify "reconfig" as the remote path. After updating startup-config, the unit restarts automatically, and begins operating with the new settings.
- 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.

2.3 Login

When the SWP1 has finished starting up, a login screen is displayed.

If a login password has been set, enter that password.

The login password "**admin**" is specified by default, so you can log in with that password.

- Login screen

```
Password:
```

- Console screen after logging in

```
SWP1-16 Rev.2.01.01 (Mon Sep 14 11:28:38 2015)
  Copyright (c) 2015 Yamaha Corporation. All Rights Reserved.

SWP1>
```

A screen appears for changing the login password and admin password only when you've logged in using the default login password for the first time. Change the passwords here.

- Password edit screen

```
Password:

SWP1-16 Rev.2.01.01 (Mon Sep 14 11:28:38 2015)
  Copyright (c) 2015 Yamaha Corporation. All Rights Reserved.
% Please change the default password.
New Login Password:
New Login Password(Confirm):
New Administrator Password:
New Administrator Password(Confirm):
Saving ...
```

```
Building configuration...
[OK]
```

If you have entered the wrong password three times in a row, login is restricted for one minute. After one minute elapses, enter the correct password.

- Login restriction screen

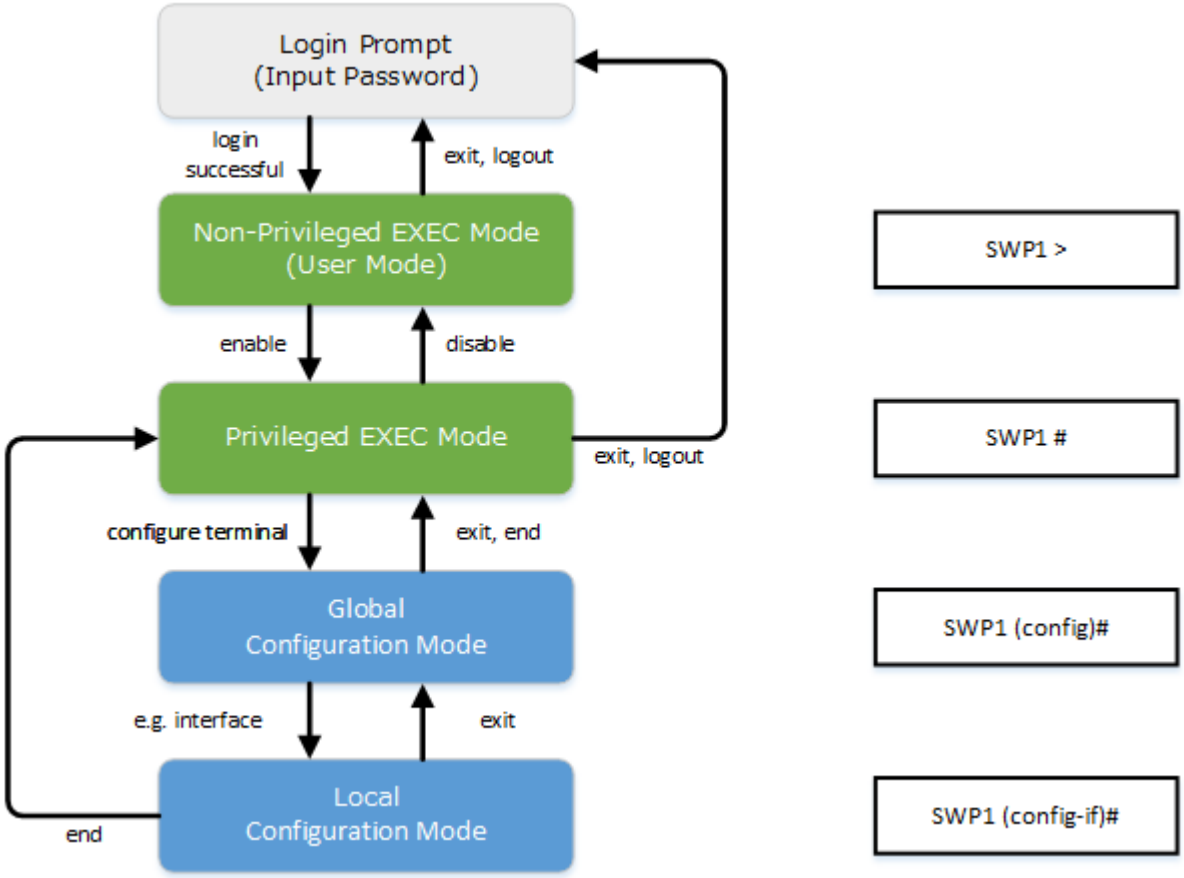
```
Password:
% Incorrect password, or login is restricted.
Password:
% Incorrect password, or login is restricted.
Password:
% Incorrect password, or blocked upon 3 failed login attempts.
% Please try again later.
```

- The restriction time is refreshed if you enter the wrong password again while login is restricted.
- You can log in by entering the correct password after the restriction time elapses.

2.4 Command input mode

2.4.1 Command input mode basics

In order to change the settings of the SWP1 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 to individual configuration mode, refer to "individual configuration mode."

- **exit** command
- **logout** command
- **enable** 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 SWP1, 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	SWP1(config-if)#
line mode	**line console** command **line vty** command	SWP1(config-line)#
VLAN mode	**vlan database** command	SWP1(config-vlan)#
VLAN access map mode	**vlan access-map** command	SWP1(config-vlan-access-map)#
MST mode	**spanning-tree mst configuration** command	SWP1(config-mst)#
class map mode	**class-map** command	SWP1(config-cmap)#
policy map mode	**policy-map** command	SWP1(config-pmap)#
policy map class mode	**class** command	SWP1(config-pmap-c)#
L2MS mode	**l2ms configuration** command	SWP1(config-l2ms)#

2.4.3 Command prompt prefix

The command prompt prefix indicates the host name. In the default state, the host name is the model name "SWP1". This indication can be changed by using the **hostname** command to specify the host name. In cases where multiple SWP1 units are used, management will be easier if separate names are assigned to each switch.

Changing the host name

```
SWP1(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 SWP1 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

  ```
  SWP1(config)#do show running-config
  ```
- Entry in abbreviated form

  ```
  SWP1(config)#do sh ru
  ```

2.5 Keyboard operations when using the console

2.5.1 Basic operations for console input

The SWP1 allows the following operations in the command line.

- Moving the cursor

Keyboard operation	Description and notes
→	Move right one character
←	Move left one character

Keyboard operation	Description and notes
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.

```
SWP1#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

SWP1#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

```
SWP1#con "press the <Tab>key"
      ↓
SWP1#configure
```

- Keyword candidate list display

```
SWP1(config)#vlan "press the <Tab> key"
access-map  database    filter
SWP1(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)

```
SWP1# 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 SWP1 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 (vlan0.1).

```
SWP1#show running-config | grep vlan0.1
interface vlan0.1
snmp-server community public ro interface vlan0.1
http-server interface vlan0.1
telnet-server interface vlan0.1
```

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

```
SWP1# show spanning-tree | include Role
%   ge1: Port Number 1 - Ifindex 1 - Port Id 8001 - Role Disabled - State
Discarding
%   ge2: Port Number 2 - Ifindex 2 - Port Id 8002 - Role Disabled - State
Discarding
%   ge3: Port Number 3 - Ifindex 3 - Port Id 8003 - Role Disabled - State
Discarding
%   ge4: Port Number 4 - Ifindex 4 - Port Id 8004 - Role Disabled - State
Discarding
%   ge5: Port Number 5 - Ifindex 5 - Port Id 8005 - Role Disabled - State
Discarding
```

```
%   ge6: Port Number 6 - Ifindex 6 - Port Id 8006 - Role Disabled - State
Discarding
%   ge7: Port Number 7 - Ifindex 7 - Port Id 8007 - Role Disabled - State
Discarding
%   ge8: Port Number 8 - Ifindex 8 - Port Id 8008 - Role Disabled - State
Discarding
%   ge9: Port Number 9 - Ifindex 9 - Port Id 8009 - Role Disabled - State
Discarding
%   ge10: Port Number 10 - Ifindex 10 - Port Id 800a - Role Disabled - State
Discarding
%   ge11: Port Number 11 - Ifindex 11 - Port Id 800b - Role Disabled - State
Discarding
%   ge12: Port Number 12 - Ifindex 12 - Port Id 800c - Role Disabled - State
Discarding
%   ge13: Port Number 13 - Ifindex 13 - Port Id 800d - Role Disabled - State
Discarding
%   ge14: Port Number 14 - Ifindex 14 - Port Id 800e - Role Disabled - State
Discarding
%   ge15: Port Number 15 - Ifindex 15 - Port Id 800f - Role Disabled - State
Discarding
%   ge16: Port Number 16 - Ifindex 16 - Port Id 8010 - Role Disabled - State
Discarding
%   ge17: Port Number 17 - Ifindex 17 - Port Id 8011 - Role Disabled - State
Forwarding
%   ge18: Port Number 18 - Ifindex 18 - Port Id 8012 - Role Disabled - State
Discarding
```

Chapter 3

Configuration

3.1 Managing settings

The SWP1 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 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 ROM.	Update by running configuration (in DANTE mode)
Default configuration (default-config)	Default setting values. Managed in 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 SWP1 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 SWP1 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 SWP1, 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. 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 setting values that are common between models and presets are shown first, and then the setting values that are specific to the presets of each model are shown.

- Settings common to all models and presets (system-wide)

Category	Setting item	Setting value
Terminal settings	Number of VTYs	8
	VTY Timeout	600sec
	Console Timeout	600sec
	Number of lines displayed	24
Password	Login password	admin
	Administrator password	admin
	Password encryption	not encrypted
Time management	Time zone	UTC (±0)
	NTP server	ntp.nict.jp
	NTP update cycle	once per hour
SYSLOG	Debug level log output	OFF
	Information level log output	ON
	Error level log output	ON
	SYSLOG server	none
Firmware update	Download URL	http://www.rtpro.yamaha.co.jp/firmware/revision-up/swp1.bin
	Allow revision-down	don't allow
	Timeout	300 sec
L2 switching	Automatic MAC address learning	enabled
	Automatic MAC address learning aging time	300 sec
	Spanning tree	enabled
	Proprietary loop detection	enabled
Access control	Telnet server status	run
	Telnet server access	allow only VLAN #1
	HTTP server status	run
	HTTP server access	allow only VLAN #1
	TFTP server access	deny all

Category	Setting item	Setting value
Traffic control	QoS	enabled
	QoS DSCP - transmission queue ID conversion table	DSCP: 8 → transmission queue: 2 DSCP:46 → transmission queue: 5 DSCP:56 → transmission queue: 7 Other than above → transmission queue: 0
	Flow control (IEEE 802.3x) threshold value	Start control: 80%, Return from control: 60%

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

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

- SWP1-8/8MMF's VLAN preset Normal settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Disable	-	Access	1(default)	-	✓
etherCON4	Disable	-	Access	1(default)	-	✓
etherCON5	Disable	-	Access	1(default)	-	✓
etherCON6	Disable	-	Access	1(default)	-	✓
etherCON7	Disable	-	Access	1(default)	-	✓
etherCON8	Disable	-	Access	1(default)	-	✓
opticalCON9	Disable	sa1	Access	1(default)	✓	-
opticalCON10	Disable					

- SWP1-8/8MMF's VLAN preset Normal settings (VLAN interface)
  - VLAN #1(for Dante and Control)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
- SWP1-8/8MMF's VLAN preset A settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Disable	-	Access	2	-	✓
etherCON4	Disable	-	Access	2	-	✓
etherCON5	Disable	-	Access	1(default)	-	✓
etherCON6	Disable	-	Access	1(default)	-	✓
etherCON7	Disable	-	Access	2	-	✓
etherCON8	Disable	-	Access	2	-	✓
opticalCON9	Disable	sa1	Trunk	1(native), 2	✓	-
opticalCON10	Disable					

- SWP1-8/8MMF's VLAN preset A settings (VLAN interface)
  - VLAN #1(for Dante)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping : Disable
- SWP1-8/8MMF's VLAN preset B settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Disable	-	Access	2	-	✓
etherCON4	Disable	-	Access	2	-	✓
etherCON5	Disable	-	Access	1(default)	-	✓
etherCON6	Disable	-	Access	2	-	✓
etherCON7	Disable	sa1	Trunk	1(native), 2	✓	-
etherCON8	Disable					
opticalCON9	Disable	sa2	Trunk	1(native), 2	✓	-
opticalCON10	Disable					

- SWP1-8/8MMF's VLAN preset B settings (VLAN interface)
  - VLAN #1(for Dante)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping : Disable
- SWP1-8/8MMF's VLAN preset C settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Enable	-	Access	2	-	✓
etherCON4	Enable	-	Access	2	-	✓
etherCON5	Disable	-	Access	1(default)	-	✓
etherCON6	Disable	-	Access	1(default)	-	✓
etherCON7	Enable	-	Access	2	-	✓
etherCON8	Enable	-	Access	2	-	✓
opticalCON9	Disable	-	Access	1(default)	-	✓
opticalCON10	Enable	-	Access	2	-	✓

- SWP1-8/8MMF's VLAN preset C settings (VLAN interface)
  - VLAN #1(for Primary Dante and Control)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Secondary Dante and Control)
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
- SWP1-16MMF's VLAN preset Normal settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Disable	-	Access	1(default)	-	✓
etherCON4	Disable	-	Access	1(default)	-	✓
etherCON5	Disable	-	Access	1(default)	-	✓
etherCON6	Disable	-	Access	1(default)	-	✓
etherCON7	Disable	-	Access	1(default)	-	✓
etherCON8	Disable	-	Access	1(default)	-	✓
RJ45 9	Disable	-	Access	1(default)	-	✓
RJ45 10	Disable	-	Access	1(default)	-	✓
RJ45 11	Disable	-	Access	1(default)	-	✓
RJ45 12	Disable	-	Access	1(default)	-	✓
etherCON13	Disable	-	Access	1(default)	-	✓
etherCON14	Disable	-	Access	1(default)	-	✓
etherCON15	Disable	-	Access	1(default)	-	✓
etherCON16	Disable	-	Access	1(default)	-	✓

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
opticalCON17	Disable	sa1	Access	1(default)	✓	-
opticalCON18	Disable					

- SWP1-16MMF's VLAN preset Normal settings (VLAN interface)
  - VLAN #1(for Dante and Control)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
- SWP1-16MMF's VLAN preset A settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Disable	-	Access	1(default)	-	✓
etherCON4	Disable	-	Access	1(default)	-	✓
etherCON5	Disable	-	Access	1(default)	-	✓
etherCON6	Disable	-	Access	1(default)	-	✓
etherCON7	Disable	-	Access	2	-	✓
etherCON8	Disable	-	Access	2	-	✓
RJ45 9	Disable	-	Access	1(default)	-	✓
RJ45 10	Disable	-	Access	1(default)	-	✓
RJ45 11	Disable	-	Access	2	-	✓
RJ45 12	Disable	-	Access	2	-	✓
etherCON13	Disable	-	Access	1(default)	-	✓
etherCON14	Disable	-	Access	1(default)	-	✓
etherCON15	Disable	-	Access	2	-	✓
etherCON16	Disable	-	Access	2	-	✓
opticalCON17	Disable	sa1	Trunk	1(native), 2	✓	-
opticalCON18	Disable					

- SWP1-16MMF's VLAN preset A settings (VLAN interface)
  - VLAN #1(for Dante)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping : Disable
- SWP1-16MMF's VLAN preset B settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Disable	-	Access	1(default)	-	✓
etherCON4	Disable	-	Access	1(default)	-	✓
etherCON5	Disable	-	Access	1(default)	-	✓
etherCON6	Disable	-	Access	1(default)	-	✓
etherCON7	Disable	-	Access	2	-	✓
etherCON8	Disable	-	Access	2	-	✓
RJ45 9	Disable	-	Access	1(default)	-	✓
RJ45 10	Disable	-	Access	1(default)	-	✓
RJ45 11	Disable	-	Access	2	-	✓
RJ45 12	Disable	-	Access	2	-	✓
etherCON13	Disable	-	Access	1(default)	-	✓
etherCON14	Disable	-	Access	2	-	✓
etherCON15	Disable	sa1	Trunk	1(native), 2	✓	-
etherCON16	Disable					
opticalCON17	Disable	sa2	Trunk	1(native), 2	✓	-
opticalCON18	Disable					

- SWP1-16MMF's VLAN preset B settings (VLAN interface)
  - VLAN #1(for Dante and Control)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping : Disable
- SWP1-16MMF's VLAN preset C settings (LAN/SFP port)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
etherCON1	Disable	-	Access	1(default)	-	✓
etherCON2	Disable	-	Access	1(default)	-	✓
etherCON3	Disable	-	Access	1(default)	-	✓
etherCON4	Disable	-	Access	1(default)	-	✓
etherCON5	Enable	-	Access	2	-	✓
etherCON6	Enable	-	Access	2	-	✓
etherCON7	Enable	-	Access	2	-	✓
etherCON8	Enable	-	Access	2	-	✓
RJ45 9	Disable	-	Access	1(default)	-	✓
RJ45 10	Disable	-	Access	1(default)	-	✓
RJ45 11	Enable	-	Access	2	-	✓

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP	Loop Detection
RJ45 12	Enable	-	Access	2	-	✓
etherCON13	Disable	-	Access	1(default)	-	✓
etherCON14	Disable	-	Access	1(default)	-	✓
etherCON15	Enable	-	Access	2	-	✓
etherCON16	Enable	-	Access	2	-	✓
opticalCON17	Disable	-	Access	1(default)	-	✓
opticalCON18	Enable	-	Access	2	-	✓

- SWP1-16MMF's VLAN preset C settings (VLAN interface)
  - VLAN #1(for Primary Dante and Control)
    - IPv4 Address : DHCP
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Secondary Dante and Control)
    - IGMP Snooping : Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable

Chapter 4

Maintenance and operation functions

4.1 Passwords

4.1.1 Setting the login password

[Syntax]

password *password*

[Parameter]

password	:	Single-byte alphanumeric characters, and symbols other than the single-byte characters '|', '>', and '?' (32 characters or less) User password to set The first character must be a single-byte alphanumeric character

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets a login password for logging on to the SWP1.

You cannot change this to the default password ("admin").

[Note]

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

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

If the login password has not been set on startup, the default login password ("admin") is automatically set.

[Example]

Specifies "user1234" as the login password.

```
SWP1(config)#password user1234
SWP1(config)#
```

4.1.2 Set administrator password

[Syntax]

enable password *password*

[Parameter]

password	:	Single-byte alphanumeric characters, and symbols other than the single-byte characters '|', '>', and '?' (32 characters or less) Administrator password to set The first character must be a single-byte alphanumeric character

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Specifies the administrator password needed to enter privileged EXEC mode.

You cannot change this to the default password ("admin").

[Note]

If the password was encrypted by the **service 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.

If the administrator password has not been set when the unit starts up, the default administrator password ("admin") is automatically set.

[Example]

Specify admin1234 as the administrator password.

```
SWP1(config)#enable password admin1234
SWP1(config)#
```

4.1.3 Encrypt password

[Syntax]

service password-encryption
no service password-encryption

[Initial value]

no service password-encryption

[Input mode]

global configuration mode

[Description]

Enables password encryption.

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

If this is executed with the "no" syntax, password encryption is disabled, and the password entered by the **password** command or the **enable password** command is 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.

```
SWP1(config)#service password-encryption
SWP1(config)#
```

Disabled password encryption.

```
SWP1(config)#no service password-encryption
SWP1(config)#
```

4.2 Configuration management

4.2.1 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.

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.

```
SWP1#copy running-config startup-config
Building configuration...
[OK]
SWP1#
```

4.2.2 Save running configuration

[Syntax]

write

[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.

```
SWP1#write
Building configuration...
[OK]
SWP1#
```

4.2.3 Save certain functions to the backup configuration

[Syntax]

backup-config

[Input mode]

priviledged EXEC mode

[Description]

Saves the settings of certain functions to the backup configuration.

This applies to the following functions.

- Settings related to IPv4 addresses
- Settings related to time zone and NTP
- Login password setting
- Administrator password setting
- Settings related to firmware updating
- Settings related to SYSLOG
- Settings related to HTTP server functions
- Settings related to Telnet server functions
- Settings for the load balance function

[Note]

This command can be used only when the configuration mode of the SWP1 is DANTE mode.

If a backup configuration exists when the SWP1 starts in DANTE mode, those settings are restored to the running configuration.

The **erase startup-config** command can be used to delete the saved backup configuration.

[Example]

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

```
SWP1#backup-config
```

4.2.4 Show the running configuration

[Syntax]

show running-config [*section*]

[Parameter]

section : Section to be shown

Setting value	Description
access-list	Access list related
igmp	IGMP related
interface	Interface related
ip	IP related
ipv6	IPv6 related
l2ms	L2MS related
mld	MLD related
mstp	MSTP related
snmp	SNMP related
switch	LACP, VLAN related
telnet-server	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.

```
SWP1#show running-config
!
ip domain-lookup
!
spanning-tree mode mstp
loop-detect enable
mls qos enable
mls qos dscp-queue 0 0
mls qos dscp-queue 1 0
mls qos dscp-queue 2 0
mls qos dscp-queue 3 0
mls qos dscp-queue 4 0
mls qos dscp-queue 5 0
mls qos dscp-queue 6 0
mls qos dscp-queue 7 0
mls qos dscp-queue 8 2

...

!
snmp-server community public ro interface vlan0.1
```

```
!
service http-server
http-server interface vlan0.1
!
service telnet-server
telnet-server interface vlan0.1
!
line con 0
line vty 0 7
!
end

SWP1#
```

4.2.5 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]

Show the startup configuration.

```
SWP1#show startup-config
!
!  Last Modified: 00:00:00 UTC Thu Jan 01 1970
!
ip domain-lookup
!
spanning-tree mode mstp
loop-detect enable
mls qos enable
mls qos dscp-queue 0 0
mls qos dscp-queue 1 0
mls qos dscp-queue 2 0
mls qos dscp-queue 3 0
mls qos dscp-queue 4 0
mls qos dscp-queue 5 0
mls qos dscp-queue 6 0
mls qos dscp-queue 7 0
mls qos dscp-queue 8 2

...

!
snmp-server community public ro interface vlan0.1
!
service http-server
http-server interface vlan0.1
!
service telnet-server
telnet-server interface vlan0.1
!
line con 0
line vty 0 7
!
end

SWP1#
```

4.2.6 Erase startup configuration

[Syntax]

erase startup-config

[Input mode]

priviledged EXEC mode

[Description]

Erases the startup settings (startup configuration).

[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.

```
SWP1#erase startup-config
erasing...[OK]
SWP1#
```

4.3 Manage boot information

4.3.1 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 (if this is omitted, boot history number 0 (current) is shown)

[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.

```
SWP1>show boot
 Running EXEC: SWP1-16 Rev.2.01.01 (Mon Sep 14 11:28:38 2015)
Previous EXEC: SWP1-16 Rev.2.01.01 (Mon Sep 14 11:28:38 2015)
Restart by reload command
```

Shows a list of the boot history.

```
SWP1>show boot list
No. Date       Time     Info
--- ---------- -------- --------------------------------------------------
  0 2015/01/01 00:00:00 Restart by reload command
  1 2015/01/01 00:00:00 Power-on boot
--- ---------- -------- --------------------------------------------------
```

4.3.2 Clear boot information

[Syntax]

clear boot list

[Input mode]

priviledged EXEC mode

[Description]

Clears the boot information history.

[Example]

Clear the boot information.

```
SWP1#clear boot list
```

4.4 Show unit information

4.4.1 Show version information

[Syntax]

show version

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the system version.

The following items are shown.

- Boot version
- Firmware revision
- MAC address

[Example]

Show the version information.

```
SWP1>show version
SWP1-16 BootROM Ver.1.00
SWP1-16 Rev.2.01.01 (Mon Sep 14 11:28:38 2015)
Base ethernet MAC Address: 00a0.de00.0000
SWP1>
```

4.4.2 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 (only for SFP modules)

[Example]

Show inventory information.

```
SWP1>show inventory
NAME: L2 switch
DESCR: SWP1-16
Vendor: Yamaha
PID: SWP1-16
VID: 0000

NAME: SFP1
DESCR: 1000BASE-SX
Vendor: AVAGO
PID: AFBR-5715APZ
VID:
SN: 00000000000

NAME: SFP2
DESCR: 1000BASE-SX
Vendor: AVAGO
PID: AFBR-5715APZ
VID:
SN: 00000000000

SWP1>
```

4.4.3 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
- MAC address
- CPU usage ratio
- Memory usage ratio
- CONFIG mode
- VLAN preset (only in DANTE mode)
- Serial baud rate
- Boot time
- Current time
- Elapsed time from boot

[Example]

Show operating information.

```
SWP1>show environment
SWP1-16 BootROM Ver.1.00
SWP1-16 Rev.2.01.01 (Mon Sep 14 11:28:38 2015)
main=SWP1-16 ver=00 MAC-Address=00a0.de00.0000
CPU:   0%(5sec)   1%(1min)   1%(5min)    Memory:  45% used
Configuration mode: DANTE
VLAN preset: NORMAL
Serial Baudrate: 9600
Boot time: 1970/01/01 00:00:00 +09:00
Current time: 1970/01/01 00:00:00 +09:00
Elapsed time from boot: 0days 00:00:00

SWP1>
```

4.4.4 Show currently-executing processes

[Syntax]

show process

[Input mode]

priviledged EXEC mode

[Description]

Shows all currently-executing processes.

[Example]

Show currently-executing processes.

```
SWP1#show process
```

4.4.5 Show technical support information

[Syntax]

show tech-support

[Input mode]

priviledged EXEC mode

[Description]

Shows a list of the results of executing the following commands useful for technical support.

- show running-config
- show environment
- show dipsw
- show inventory
- show boot all
- show logging
- show process
- show interface
- show frame-counter
- show vlan brief
- show spanning-tree mst detail
- show loop-detect
- show mac-address-table
- show l2ms detail
- show mls qos queue-counters
- show ddm status
- show errdisable

[Example]

Show technical support information.

```
SWP1#show tech-support
#
# Information for Yamaha Technical Support
#

*** show running-config ***
!
ip domain-lookup
!
spanning-tree mode mstp
!

...

#
# End of Information for Yamaha Technical Support
#
```

```
SWP1#
```

4.5 Time management

4.5.1 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.

```
SWP1#clock set 00:00:00 Jan 1 2015
```

4.5.2 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.

```
SWP1(config)#clock timezone JST
```

Set the time zone to UTC+9 hours.

```
SWP1(config)#clock timezone +9:00
```

4.5.3 Show current time

[Syntax]

show clock

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the current time and date.

[Example]

Show the current time.

```
SWP1>show clock
00:00:00 JST Thu Jan 1 2015
```

4.5.4 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%vlan0.N format)
fqdn	:	Host name of the NTP server

[Initial value]

ntpdate server name ntp.nict.jp

[Input mode]

global configuration mode

[Description]

Registers the address or host name of the NTP server.

If this command is executed when the NTP server is already registered, the information is overwritten.

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

[Example]

Specify 192.168.1.1 as the NTP server.

```
SWP1(config)#ntpdate server ipv4 192.168.1.1
```

Specify ntp.example.com as the NTP server.

```
SWP1(config)#ntpdate server name ntp.example.com
```

4.5.5 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.

```
SWP1#ntpdate oneshot
```

4.5.6 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.

```
SWP1(config)#ntpdate interval 2
```

Disable periodic time synchronization.

```
SWP1(config)#ntpdate interval 0
```

4.5.7 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

```
SWP1(config)#show ntpdate
```

```
NTP Server  : ntp.nict.jp
adjust time : Thu Jan 1 09:00:00 2015 + interval 1 hour
```

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

```
SWP1(config)#show ntpdate
NTP Server  : ntp.nict.jp
adjust time : Thu Jan 1 09:00:00 2015
```

4.6 Terminal settings

4.6.1 Move to line mode (console terminal)

[Syntax]

line console *port*

[Parameter]

port : 0

Serial console port number

[Initial value]

line console 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 privileged EXEC mode, use the **end** command.

[Example]

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

```
SWP1(config)#line console 0
SWP1(config-line)#
```

4.6.2 Set VTP 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]

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 privileged EXEC mode, use the **end** command.

[Example]

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

```
SWP1(config)#line vty 0
SWP1(config-line)#
```

4.6.3 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.

```
SWP1(config)#line console 0
SWP1(config-line)#exec-timeout 5 0
SWP1(config-line)#
```

4.6.4 Show terminal login information

[Syntax]

show line

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows terminal login information.

The following items are shown.

Item	Description
Line	Console and VTY ports that are enabled. "con 0" is the serial console port. "vty N" is a VTY port.
Own	The user's own connection port. The user's own connection port is indicated by an "*" symbol.

Item	Description
Status	Login status. If a user is using a terminal, this indicates "Login".

[Example]

Log in via Telnet and show terminal login information.

```
SWP1>show line

  Line   Own  Status
----------------------
  con 0         -
  vty 0   *   Login
  vty 1         -
  vty 2         -
  vty 3         -
  vty 4         -
  vty 5         -
  vty 6         -
  vty 7         -

SWP1>
```

4.6.5 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.

```
SWP1>terminal length 100
SWP1>
```

4.6.6 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]

Set the number of lines displayed per page on the terminal to 100 lines.

```
SWP1(config)#service terminal-length 100
SWP1(config)#
```

4.7 SYSLOG

4.7.1 Set log notification destination (SYSLOG server)

[Syntax]

logging host *host*
no logging 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%vlan0.N 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.

```
SWP1(config)#logging host 192.168.100.1
```

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

```
SWP1(config)#logging host fe80::2a0:deff:fe11:2233%vlan0.1
```

4.7.2 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.

```
SWP1(config)#logging trap debug
```

4.7.3 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.

```
SWP1(config)#logging trap informational
```

4.7.4 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.

```
SWP1(config)#logging trap error
```

4.7.5 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.

```
SWP1(config)#logging stdout info
```

4.7.6 Clear log

[Syntax]

clear logging

[Input mode]

priviledged EXEC mode

[Description]

Clears the log.

[Example]

Clear the log.

```
SWP1#clear logging
```

4.7.7 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 1,500 events. If this maximum number is exceeded, the oldest events are successively deleted.

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

[Example]

Show the log.

```
SWP1#show logging
```

4.8 L2MS (Layer 2 management service) settings

4.8.1 Set L2MS control frame transmit/receive

[Syntax]

l2ms filter enable
no l2ms filter

[Initial value]

Depends on VLAN preset. Refer to Default setting values.

[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 ge5 from transmitting or receiving L2MS control frames.

```
SWP1(config)#interface ge5
SWP1(config-if)#l2ms filter enable
```

4.8.2 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 according to the L2MS operating state.

- Whether managed by the manager
- MAC address of manager (if managed)

[Note]

The "detail" keyword is valid only if operating as a manager.

[Example]

L2MS information is shown.

```
SWP1>show l2ms
Role : Agent

Status : Managed by Manager (00a0.de00.0000)
```

4.9 Firmware update

4.9.1 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/swp1.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".

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/swp1.bin as the firmware download URL.

```
SWP1(config)#firmware-update url http://192.168.100.1/swp1.bin
SWP1(config)#
```

4.9.2 Execute firmware update

[Syntax]

firmware-update execute [no-confirm]

[Keyword]

no-confirm : Don't confirm the firmware update

[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.

[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.

[Example]

Update the firmware using a firmware file located on a web server.

```
SWP1#firmware-update execute
Found the new revision firmware
Current Revision: Rev.2.01.01
New Revision:     Rev.2.01.02
Downloading...
Update to this firmware? (Y/N)y
Updating...
Finish
SWP1#
```

4.9.3 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.

```
SWP1(config)#firmware-update timeout 120
SWP1(config)#
```

4.9.4 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.

```
SWP1(config)#firmware-update revision-down enable
SWP1(config)#
```

4.9.5 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
- Download timeout duration
- Allow revision-down

[Example]

Show the current settings of the firmware update function.

```
SWP1#show firmware-update
url:http://www.rtpro.yamaha.co.jp/firmware/revision-up/swp1.bin
timeout:300 (seconds)
revision-down:disable
SWP1#
```

4.10 General maintenance and operation functions

4.10.1 Set host name

[Syntax]

hostname *hostname*
no hostname [*hostname*]

[Parameter]

hostname	:	Single-byte alphanumeric characters and single-byte symbols (63 characters or less) Host name

[Initial value]

hostname SWP1

[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."

```
SWP1(config)#hostname yamaha
yamaha(config)#
```

4.10.2 Reload system

[Syntax]

reload

[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 or the **write** command before you execute the **reload** command.

[Example]

Reboot the system.

```
SWP1#reload
reboot system? (y/n): y
```

4.10.3 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.

You cannot execute this command when using the default administrator password setting. You must change the administrator password beforehand.

[Example]

Initialize the settings.

```
SWP1#cold start
Password:
```

4.10.4 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
status	STATUS mode
vlan	VLAN mode
eco	ECO 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 ECO mode.

```
SWP1(config)#led-mode default eco
```

4.10.5 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.

```
SWP1>show led-mode
default mode : eco
current mode : link-act
```

4.10.6 Show dip switches status

[Syntax]

show dipsw

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Show the status of the DIP switches at startup and the current status.

[Example]

Show the status of the DIP switches.

```
SWP1>show dipsw

 DIPSW             SW1   SW2   SW3   SW4
---------------------------------------
 Startup status :  ON    OFF   OFF   ON
 Current status :  ON    OFF   OFF   ON
```

Chapter 5

IPv4/IPv6 common setting

5.1 DNS client

5.1.1 Set DNS lookup function

[Syntax]

ip domain-lookup
no ip domain-lookup

[Initial value]

ip domain-lookup

[Input mode]

global configuration mode

[Description]

Enables the DNS lookup function.

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

[Note]

When the **no ip domain-lookup** command is executed, it disables only the settings of the **ip domain-name**, **ip domain-list**, and **ip name-server** commands; it does not disable the list of found domains obtained from the DHCP server by the **ip address dhcp** command, or the DNS server IP address.

[Example]

Enable the DNS lookup function.

```
SWP1(config)#ip domain-lookup
```

5.1.2 Set default domain name

[Syntax]

ip domain-name *name*
no ip 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]

If the **ip address dhcp** command was used to obtain the default domain name from the DHCP server, the setting of this command takes priority.

[Example]

Set the default domain name to "example.com".

```
SWP1(config)#ip domain-name example.com
```

5.1.3 Show default domain name

[Syntax]

show ip domain-name

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the default domain name that was specified by the **ip domain-name** command.

[Example]

Show the default domain name.

```
SWP1>show ip domain-name
example.com
```

5.1.4 Set search domain list

[Syntax]

ip domain-list *name*
no ip 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 the **ip address dhcp** command was used to obtain the search domain list from the DHCP server, the setting of this command takes priority.

However if fewer than six items were registered by this command in the search domain list, up to six items from the search 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.

```
SWP1(config)#ip domain-list example1.com
SWP1(config)#ip domain-list example2.com
```

5.1.5 Show search domain list

[Syntax]

show ip domain-list

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows a list of the search domains that were specified by the **ip domain-list** command.

[Example]

Show the search domain list.

```
SWP1>show ip domain-list
example1.com
example2.com
```

5.1.6 Set DNS server list

[Syntax]

ip name-server *server*
no ip name-server *server*

[Parameter]

server : A.B.C.D

IPv4 address 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%vlan0.N 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** command was used to obtain the DNS server list from the DHCP server, the setting of this command takes 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.

```
SWP1(config)#ip name-server 192.168.100.1
SWP1(config)#ip name-server 2001:db8::1234
SWP1(config)#ip name-server fe80::2a0:deff:fe11:2233%vlan0.1
```

5.1.7 Show DNS server list

[Syntax]

show ip name-server

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the DNS server list that was specified by the **ip name-server** command.

[Example]

Show the DNS server list.

```
SWP1>show ip name-server
192.168.100.1
2001:db8::1234
fe80::2a0:deff:fe11:2233%vlan0.1
```

Chapter 6

IPv4

6.1 IPv4 address management

6.1.1 Set IP address

[Syntax]

ip address *ip_address*/*mask* [label *textline*]
no ip address

[Keyword]

label	:	Set label as IP address

[Parameter]

ip_address	:	A.B.C.D
		IP address
mask	:	<1-31>
		Number of mask bits
textline	:	Label (maximum 64 characters)

[Initial value]

no ip address

[Input mode]

interface mode

[Description]

Specifies the IP address and net mask for the VLAN interface.

An IP address can be specified for only one VLAN interface.

If the **ip address** or **ip address dhcp** command has already been specified for a certain VLAN interface, and you then specify the **ip address** or **ip address dhcp** command for a different VLAN interface, the old setting is automatically deleted.

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

If a label is specified, it is shown in the "IPv4 address" field by the **show interface** command.

[Example]

Specify 192.168.1.100 as the IP address for VLAN #1.

```
SWP1(config)#interface vlan0.1
SWP1(config-if)#ip address 192.168.1.100/24
```

6.1.2 Show IP address

[Syntax]

show ip interface [*interface*] **brief**

[Parameter]

interface	:	VLAN interface name
		Interface to show

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IP address of the interface.

- IP address

  - If the IP address was set automatically by DHCP, "(DHCP)" is appended following the IP address.
  - If an IP 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 IP address can be specified.

[Note]

An error occurs if the specified interface is one to which an IP address cannot be assigned.

[Example]

Shows the IP address of every VLAN interface.

```
SWP1>show ip interface brief
Interface            IP-Address            Status                Protocol
vlan0.1              192.168.1.100/24      up                    up
vlan0.2              unassigned            up                    down
```

6.1.3 Automatically set IP 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 IP address (A.B.C.D)

[Initial value]

ip address dhcp *VLAN #1 only

[Input mode]

interface mode

[Description]

Using the DHCP client, assigns the 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 IP address has been obtained, you can execute the **no ip address dhcp** command to send a release message for the obtained IP address to the DHCP server.

An IP address can be specified for only one VLAN interface.

If the **ip address** or **ip address dhcp** command has already been specified for a certain VLAN interface, and you then specify the **ip address** or **ip address dhcp** command for a different VLAN interface, the old setting is automatically canceled.

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.

The **no ip address** command can also be used to cancel the **ip address dhcp** command.

If an IP address cannot be obtained from the DHCP server when this command is specified, an IPv4 link local address is generated by the Auto IP function.
If an IP address is obtained from the DHCP server after the IPv4 link local address was generated, the IPv4 link local address is discarded, and the IP address obtained from the DHCP server is used.

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 IP address to VLAN #100.

```
SWP1(config)#interface vlan0.100
SWP1(config-if)#ip address dhcp
```

6.1.4 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 IP 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

[Example]

Show the current DHCP client status.

```
SWP1>show dhcp lease
Interface vlan0.1
------------------------------------------------------------------------------
IP Address:                    192.168.100.2
Expires:                       2015/01/01 00:00:00
Renew:                         2015/01/01 00:00:00
Rebind:                        2015/01/01 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
```

6.2 IPv4 route control

6.2.1 Set static 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

IP 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

IP 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 IP.

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

[Example]

Set the default gateway to 192.168.1.1.

```
SWP1(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.

```
SWP1(config)#ip route 172.16.0.0 255.255.0.0 192.168.2.1
```

6.2.2 Show IP Forwarding Information Base

[Syntax]

show ip route [*ip_address*[/*mask*]]

[Parameter]

ip_address : A.B.C.D

IP address

mask : <0-32>

Number of mask bits (if omitted: 32)

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IP Forwarding Information Base (FIB).

If the IP address is omitted, the entire content of the FIB is shown.

If the IP address or network address is specified, detailed information for the routing entry that matches the destination is shown.

[Example]

Show the entire IP forwarding information base.

```
SWP1>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, vlan0.1
S       172.16.0.0/16 [1/0] via 192.168.200.240, vlan0.100
S       192.168.1.1/32 [1/0] is directly connected, vlan0.100
C       192.168.100.0/24 is directly connected, vlan0.1
C       192.168.200.0/24 is directly connected, vlan0.100
```

Show the route used for sending packets that are addressed to 192.168.100.10.

```
SWP1>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, vlan0.1
```

6.2.3 Show IP Routing Information Base

[Syntax]

show ip route database

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the IP Routing Information Base (RIB).

[Example]

Show the IP routing information base.

```
SWP1>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, vlan0.1
S    *> 172.16.0.0/16 [1/0] via 192.168.200.240, vlan0.100
S    *> 192.168.1.1/32 [1/0] is directly connected, vlan0.100
C    *> 192.168.100.0/24 is directly connected, vlan0.1
C    *> 192.168.200.0/24 is directly connected, vlan0.100

Gateway of last resort is not set
```

6.2.4 Show summary of the route entries registered in the IP 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 IP Routing Information Base (RIB).

[Example]

Show a summary of the route entries that are registered in the IP Routing Information Base.

```
SWP1>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
```

6.3 ARP

6.3.1 Show ARP table

[Syntax]

show arp

[Input mode]

unprivileged EXEC mode, priviledged EXEC mode

[Description]

Shows the ARP cache.

The ARP cache stores up to 1023 entries (total of dynamic entries and static entries).

[Example]

Show the ARP cache.

```
SWP1>show arp
 IP Address      MAC Address   Interface  Type
192.168.100.10  00a0.de00.0000 vlan0.1    dynamic
192.168.100.100 00a0.de00.0001 vlan0.1    static
```

6.3.2 Clear ARP table

[Syntax]

clear arp-cache

[Input mode]

priviledged EXEC mode

[Description]

Clears the ARP cache.

[Example]

Clear the ARP cache.

```
SWP1#clear arp-cache
```

6.3.3 Set static ARP entry

[Syntax]

arp *ip_address mac_address*
no arp *ip_address*

[Parameter]

ip_address	:	A.B.C.D
		IP address
mac_address	:	HHHH.HHHH.HHHH
		MAC address

[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 with the IP address 192.168.100.100 and MAC address 00a0.de00.0000.

```
SWP1(config)#arp 192.168.100.100 00a0.de00.0000
```

6.3.4 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 1200

[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 1200 seconds.

[Example]

Change the ARP entry ageing timeout for VLAN #1 to five minutes.

```
SWP1(config)#interface vlan0.1
SWP1(config)#arp-aging-timeout 300
```

6.4 Ping

6.4.1 Ping

[Syntax]

ping *host* [repeat *count*] [size *datalen*] [timeout *timeout*]

[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

[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"

[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.

```
SWP1#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
```

Chapter 7

IPv6

7.1 IPv6 address management

7.1.1 Set enable/disable IPv6

[Syntax]

ipv6 enable
no ipv6

[Initial value]

no ipv6

[Input mode]

interface mode

[Description]

Enables IPv6 for the VLAN interface and automatically sets the link local address.

IPv6 can be enabled only for one VLAN interface.

If the **ipv6 enable** command has already been specified for a certain VLAN interface, and you then specify the **ipv6 enable** command for a different VLAN interface, the old setting is automatically deleted.

If this command is executed with the "no" syntax, IPv6 is disabled. At this time, the related settings are also deleted.

[Note]

The automatically-specified link local address can be viewed by using the **show ipv6 interface brief** command.

IPv6 is enabled for VLAN #1 by default.

[Example]

Enable IPv6 for VLAN #1.

```
SWP1(config)#interface vlan0.1
SWP1(config-if)#ipv6 enable
```

7.1.2 Set IPv6 address

[Syntax]

ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
prefix_len	:	<1-127> IPv6 prefix length

[Input mode]

interface mode

[Description]

Specifies the IPv6 address and prefix length for the VLAN interface.

The IPv6 address can be specified only for the **ipv6 enable** for which the ipv6 enable command has been specified.

Only one IPv6 address can be specified for a single VLAN interface.

If the ipv6 address autoconfig command was executed before executing this command, the setting of the ipv6 address autoconfig command is automatically deleted

If this command is executed with the "no" syntax, the specified IPv6 address is deleted.

[Example]

Specify 2001:db8:1::2 as the IPv6 address for VLAN #1.

```
SWP1(config)#interface vlan0.1
SWP1(config-if)#ipv6 address 2001:db8:1::2/64
```

7.1.3 Set RA for IPv6 address

[Syntax]

ipv6 address autoconfig
no ipv6 address

[Initial value]

no ipv6 address

[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.

If the ipv6 address ipv6_address/prefix_len command was executed before executing this command, the setting of the ipv6 address ipv6_address/prefix_len command is automatically deleted.

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

[Example]

Use RA to set the IPv6 address for VLAN #1.

```
SWP1(config)#interface vlan0.1
SWP1(config-if)#ipv6 address autoconfig
```

7.1.4 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 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.

```
SWP1>show ipv6 interface brief
Interface        IP-Address                                Status
Protocol
vlan0.1          2001:db8:1::2/64                          up                    up
                 fe80::2a0:deff:fe:2/64
vlan0.2          unassigned                                up
down
```

7.2 IPv6 route control

7.2.1 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%vlan0.N 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.

```
SWP1(config)#ipv6 route 2001:db8:2::/64 2001:db8:1::1
```

Set the default gateway to fe80::2a0:deff:fe:1 on VLAN #1.

```
SWP1(config)#ipv6 route ::/0 fe80::2a0:deff:fe:1%vlan0.1
```

7.2.2 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.

[Example]

Show the entire IPv6 forwarding information base.

```
SWP1>show ipv6 route
Codes: C - connected, S - static
Timers: Uptime

S      ::/0 [1/0] via fe80::2a0:deff:fe:1, vlan0.1, 00:03:08
C      2001:db8:1::/64 via ::, vlan0.1, 00:01:10
S      2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan0.1, 00:01:52
C      fe80::/64 via ::, vlan0.1, 00:03:08
```

Show the route used for sending packets that are addressed to 2001:db8:1::2

```
SWP1>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, vlan0.1
```

7.2.3 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).

[Example]

Show the IPv6 routing information base.

```
SWP1>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, vlan0.1, 00:21:39
C   *> 2001:db8:1::/64 via ::, vlan0.1, 00:19:41
S   *> 2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan0.1, 00:20:23
C   *> fe80::/64 via ::, vlan0.1, 00:21:39
```

7.2.4 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).

[Example]

Show a summary of the IPv6 Routing Information Base.

```
SWP1>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
```

7.3 Neighbor cache

7.3.1 Set static neighbor cache entry

[Syntax]

ipv6 neighbor *ipv6_address interface mac_address*
no ipv6 neighbor *ipv6_address interface*

[Parameter]

ipv6_address	:	X:X::X:X
		IPv6 address
interface	:	vlan0.N
		VLAN interface name
mac_address	:	HHHH.HHHH.HHHH
		MAC address

[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.

[Example]

Add the MAC address of the IPv6 address 2001:db8:cafe::1 on VLAN #1 to the Neighbor cache.

```
SWP1(config)#ipv6 neighbor 2001:db8:cafe::1 vlan0.1 00a0.de80.cafe
```

7.3.2 Show neighbor cache table

[Syntax]

show ipv6 neighbors

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the neighbor cache table.

[Example]

Shows the neighbor cache table.

```
SWP1>show ipv neighbors
 IPv6 Address                              MAC Address     Interface  Type
2001:db8:1:0:3538:5dc7:6bc4:1a23          0011.2233.4455   vlan0.1    dynamic
2001:db8:cafe::1                          00a0.de80.cafe   vlan0.1    static
fe80::0211:22ff:fe33:4455                 0011.2233.4455   vlan0.1    dynamic
fe80::6477:88ff:fe99:aabb                 6677.8899.aabb   vlan0.1    dynamic
```

7.3.3 Clear neighbor cache table

[Syntax]

clear ipv6 neighbors

[Input mode]

priviledged EXEC mode

[Description]

Clears the neighbor cache.

[Example]

Clears the neighbor cache.

```
SWP1#clear ipv6 neighbors
```

7.4 Ping

7.4.1 IPv6 ping

[Syntax]

ping6 *host* [repeat *count*] [size *datalen*] [timeout *timeout*]

[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

[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%vlan0.N 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"

[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.

[Example]

Ping fe80::2a0:deff:fe11:2233.

```
SWP1#ping6 fe80::2a0:deff:fe11:2233%vlan0.1
PING fe80::2a0:deff:fe11:2233%vlan0.1 (fe80::2a0:deff:fe11:2233%vlan0.1): 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%vlan0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.681/7.554/10.210 ms
```

Chapter 8

Remote access functions

8.1 Telnet server

8.1.1 Start Telnet server and change listening port number

[Syntax]

service telnet-server [*port*]
no service telnet-server

[Parameter]

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

[Initial value]

service telnet-server

[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.

```
SWP1(config)#service telnet-server 12345
```

8.1.2 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.

```
SWP1#show telnet-server
Service:Enable
Port:23
Interface(vlan):1, 2, 3
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

8.1.3 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]

telnet-server interface vlan0.1

[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 has not been used, all access is prohibited.

[Note]

If **service telnet-server** 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.

```
SWP1(config)#telnet-server interface vlan0.1
SWP1(config)#telnet-server interface vlan0.2
```

8.1.4 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 **service telnet-server** and **telnet-server interface** are 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.

```
SWP1(config)#telnet-server access permit 192.168.1.1
SWP1(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.

```
SWP1(config)#telnet-server access deny 192.168.10.0/24
SWP1(config)#telnet-server access permit any
```

8.2 Telnet client

8.2.1 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%vlan0.N 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.

```
SWP1#telnet 192.168.100.1 12345
```

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

```
SWP1#telnet fe80::2a0:deff:fe11:2233%vlan0.1 12345
```

8.2.2 Enable Telnet client

[Syntax]

service telnet-client
no service telnet-client

[Initial value]

no service telnet-client

[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.

```
SWP1(config)#service telnet-client
```

8.3 TFTP server

8.3.1 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 has not been used, all access is prohibited.

[Example]

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

```
SWP1(config)#tftp-server interface vlan0.1
SWP1(config)#tftp-server interface vlan0.2
```

8.4 HTTP server

8.4.1 Start HTTP server and change listening port number

[Syntax]

service http-server [*port*]
no service http-server

[Parameter]

port : <1-65535>

Listening port number of the HTTP server (if omitted: 80)

[Initial value]

service http-server

[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.

```
SWP1(config)#service http-server 8080
```

8.4.2 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
- Listening port number

[Example]

Show the settings of the HTTP server.

```
SWP1#show http-server
Service:Enable
Port:80
```

8.4.3 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]

http-server interface vlan0.1

[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 has not been used, all access is prohibited.

[Example]

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

```
SWP1(config)#http-server interface vlan0.1
SWP1(config)#http-server interface vlan0.2
```

8.4.4 Set Web GUI display language

[Syntax]

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

[Parameter]

language : Web GUI display language

Setting value	Description
english	English
japanese	Japanese

[Initial value]

http-server language english

[Input mode]

global configuration mode

[Description]

Sets the Web GUI display language.

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

[Example]

Set the Web GUI display language to English.

```
SWP1(config)#http-server language english
```

Chapter 9

Network monitoring

9.1 SNMP

9.1.1 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%vlan0.N 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'

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'

[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%vlan0.1" and you newly add the setting "fe80::10%vlan0.2," all settings for "fe80::10%vlan0.1" are deleted, and only the settings of the added "fe80::10%vlan0.2" will remain.

[Example]

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

```
SWP1(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".

```
SWP1(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".

```
SWP1(config)#snmp-server host 192.168.10.13 traps version 3 priv admin1
```

9.1.2 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, when firmware is updated
warmstart	At restart
linkdown	At linkdown
linkup	At linkup
authentication	When authentication fails
errdisable	When ErrorDisable is detected or canceled

[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.

```
SWP1(config)#snmp-server enable trap coldstart
```

Disable traps.

```
SWP1(config)#no snmp-server enable trap
```

9.1.3 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 "swp1admin@sample.com".

```
SWP1(config)#snmp-server contact swp1admin@sample.com
```

9.1.4 Set system location

[Syntax]

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

[Parameter]

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

[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".

```
SWP1(config)#snmp-server location MainOffice-1F
```

9.1.5 Set SNMP community

[Syntax]

snmp-server community *community ro_rw* [**interface** *ifname*]
no snmp-server community *community*

[Parameter]

community : Community name (maximum 32 characters)

ro_rw : Access restriction

Setting value	Description
ro	Read only
rw	Write allowed

ifname : (Obsolete parameter)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the SNMP community.

Up to 16 communities can be registered.

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

[Note]

Specifying the interface does not affect SNMP operation.

Setting the **snmp-server community** command will fail if you roll back to an older version (Rev.2.00.08 or earlier). As a result, it will no longer be possible to show or set the MIB variables via SNMP.

[Example]

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

```
SWP1(config)#snmp-server community public ro
```

Delete the "public" community.

```
SWP1(config)#no snmp-server community public
```

9.1.6 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.

```
SWP1(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.

```
SWP1(config)#snmp-server view standard 1.3.6.1.2.1 include
```

9.1.7 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.

```
SWP1(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.

```
SWP1(config)#snmp-server group users auth read standard
```

9.1.8 Set SNMP user

[Syntax]

snmp-server user *user group* [auth *auth auth_path* [priv *priv priv_path*]]
no snmp-server user *user*

[Keyword]

auth : Set the authentication algorithm

priv : Set the encryption algorithm

[Parameter]

user : User name (maximum 32 characters)

group : Group name (maximum 32 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)

priv : Encryption algorithm

Setting value	Description
des	DES-CBC
aes	AES128-CFB

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

```
SWP1(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.

```
SWP1(config)#snmp-server user user1 users auth sha passwd5678
```

9.1.9 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, access mode, and the name of the VLAN interface that can be accessed.

[Example]

Show SNMP community information.

```
SWP1#show snmp community
SNMP Community information
  Community Name: public
  Access: Read-Only
  Acceptable Interface: vlan0.1

  Community Name: private
  Access: Read-Write
  Acceptable Interface: vlan0.1
```

9.1.10 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.

```
SWP1#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
```

9.1.11 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.

```
SWP1#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
```

9.1.12 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 user name, affiliated group name, authentication method, and encryption method.

[Example]

Shows the contents of the SNMP user settings.

```
SWP1#show snmp user
SNMP User information
  User Name: admin1
  Group Name: admins
  Auth: sha
  Priv: aes

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

Chapter 10

LAN/SFP port control

10.1 Basic settings

10.1.1 Set description

[Syntax]

description *line*
no description

[Parameter]

line : Single-byte alphanumeric characters and single-byte symbols (80 characters 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#description Connected to rtx1210-router
```

10.1.2 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.

It is not possible to change a VLAN interface when it is in the **no shutdown** state.

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.

```
SWP1(config)#interface ge1
SWP1(config-if)#shutdown
```

10.1.3 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
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.

The only *type* that can be specified for SFP port is auto or 1000-full.

[Example]

Set the speed and duplex mode for LAN port #1 to 100Mbps/Full.

```
SWP1(config)#interface ge1
SWP1(config-if)#speed-duplex 100-full
```

10.1.4 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#mru 9000
```

10.1.5 Set cross/straight automatic detection

[Syntax]

mdix auto
no mdix auto

[Initial value]

mdix auto

[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.

```
SWP1(config)#interface ge1
SWP1(config-if)#no mdix auto
```

10.1.6 Set EEE

[Syntax]

power efficient-ethernet auto
no power efficient-ethernet auto

[Initial value]

no power efficient-ethernet auto

[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.

```
SWP1(config)#interface ge1
SWP1(config-if)#power efficient-ethernet auto
```

10.1.7 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
  SWP1#show eee capabilities interface ge1
  interface:ge1
    EEE(efficient-ethernet):  yes (1000-T, 100-TX)
    Link Partner           :  yes (1000-T, 100-TX)

・If the other unit does not support EEE
  SWP1#show eee capabilities interface ge1
  interface:ge1
    EEE(efficient-ethernet):  yes (1000-T, 100-TX)
    Link Partner           :  not enabled
```

10.1.8 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
  SWP1#show eee status interface ge1
  interface:ge1
    EEE(efficient-ethernet):  Disabled
    Rx LPI Status          :  None
    Tx LPI Status          :  None
    Wake Error Count       :  0

・If EEE is enabled
  SWP1#show eee status interface ge1
  interface:ge1
    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
  SWP1#show eee status interface ge1
  interface:ge1
    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
  SWP1#show eee status interface ge1
  interface:ge1
    EEE(efficient-ethernet):  Operational
    Rx LPI Status          :  Low Power
    Tx LPI Status          :  Low Power
    Wake Error Count       :  0
```

10.1.9 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]

no mirror interface

[Input mode]

interface mode

[Description]

Mirrors the traffic specified by *direct*, with the applicable interface as the mirror port and *ifname*as the monitor 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 mirror port.

[Example]

With LAN port #1 as the mirror port, mirror the transmitted and received frames of LAN port #4 and the transmitted frames of LAN port #5.

```
SWP1(config)#interface ge1
SWP1(config-if)#mirror interface ge4 direction both
SWP1(config-if)#mirror interface ge5 direction transmit
```

10.1.10 Show port mirroring status

[Syntax]

show mirror [interface *ifname*]

[Keyword]

interface	:	Specify the monitor port to show

[Parameter]

ifname	:	Interface name of the LAN/SFP port Monitor 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 monitor ports are shown.

The following items are shown for each monitor port.

Item	Description
Mirror Test Port Name	Interface name of the mirror port
Mirror option	Whether port mirroring is enabled or disabled
Mirror direction	Direction of traffic that is mirrored
Monitored Port Name	Interface name of the monitor port

[Example]

Show the mirroring port settings.

```
SWP1#show mirror
Mirror Test Port Name: ge1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: ge3
Mirror Test Port Name: ge1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: ge4
Mirror Test Port Name: ge1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: ge5
```

10.1.11 Show interface status

[Syntax]

show interface [*ifname*]

[Parameter]

ifname	:	Interface name Interface to show

[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)
input	packets	Number of packets received *2
	bytes	Number of bytes received *2
	multicast packets	Number of multicast packets received *2
	drop packets	Number of overflowed packets received *2, *5
output	packets	Number of packets transmitted *2
	bytes	Number of bytes transmitted *2
	multicast packets	Number of multicast packets transmitted *2
	broadcast packets	Number of broadcast packets transmitted *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.

```
SWP1#show interface ge1
Interface ge1
```

```
  Link is UP
  Hardware is Ethernet
  HW addr: 00a0.de00.0000
  Description: Connected to router
  ifIndex 1, MRU 1522
  Speed-Duplex: auto(configured), 1000-full(current)
  Auto MDI/MDIX: on
  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.

```
SWP1#show interface vlan0.1
Interface vlan0.1
  Hardware is VLAN
  Description: Connected to router(VLAN)
  ifIndex 10001, ARP ageing timeout 1200
  IPv4 address 192.168.100.240/24 broadcast 192.168.100.255
```

10.1.12 Show VLAN information for switchport

[Syntax]

show interface switchport info [*ifname*]

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

unprivileged EXEC mode、 priviledged EXEC mode

[Description]

Shows VLAN-related information of the interface specified by *ifname*. If ifname is omitted, shows information for all interfaces. If *ifname* is omitted, shows information for all interfaces.

The following items are shown.

Item	Description
Interface name	Interface name
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

Item	Description
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 : vlan0.1
Configured Vlans	List of the VLAN IDs that belong to the corresponding interface

[Example]

Show VLAN-related information for the LAN port #1.

```
SWP1#show interface switchport info ge1
Interface name          : ge1
Switchport mode         : access
Ingress filter          : enable
Acceptable frame types : all
Default Vlan            :    1
Configured Vlans        :    1
```

10.1.13 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

Item	Description
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.

```
SWP1#show frame-counter ge1
Interface ge1 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
```

10.1.14 Clear frame counters

[Syntax]

clear counters *ifname*

[Parameter]

ifname : Interface name of LAN/SFP port or logical interface

Applicable interface

[Input mode]

priviledged EXEC mode

[Description]

Clears frame counter information for the interface specified by *ifname*.

If logical interface is specified as the *ifname*, the frame counters of all LAN/SFP port units associated with that interface are cleared.

[Example]

Clear the frame counters of LAN port #1.

```
SWP1#clear counters ge1
```

10.1.15 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.

```
SWP1#show ddm status
             Temperature  High Alarm   High Warning Low Warning  Low Alarm
Interface    (Celsius)    Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 ge9          31.1        100.0         85.0        -40.0        -55.0
 ge10             -            -            -            -            -

             Voltage      High Alarm   High Warning Low Warning  Low Alarm
Interface    (V)          Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 ge9         3.34         3.62         3.46         3.13         2.97
 ge10             -            -            -            -            -

             Current      High Alarm   High Warning Low Warning  Low Alarm
Interface    (mA)         Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 ge9           3.8         16.0         15.0           2.0          2.0
 ge10             -            -            -            -            -

             TX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 ge9          -5.5160       0.4139       0.0000     -10.7058     -12.2184
 ge10             -            -            -            -            -

             RX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 ge9          -5.9226       2.5527       0.0000     -16.9897     -40.0000
 ge10             -            -            -            -            -
```

10.2 Link aggregation

10.2.1 Set static logical interface

[Syntax]

static-channel-group *link-id*
no static-channel-group

[Parameter]

link-id : <1-12>
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.

- speed-duplex command setting
- VLAN setting

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 #9 with static logical interface #5.

```
SWP1(config)#interface ge9
SWP1(config-if)#static-channel-group 5
```

10.2.2 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.

```
SWP1#show static-channel-group
% Static Aggregator: sa5
% Load balancing: src-dst-mac
% Member:
   ge9
   ge11
   ge13
   ge15
```

10.2.3 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.

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.

- **speed-duplex** command setting
- VLAN setting

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 a 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 #17 in ACTIVE mode with LACP logical interface #10

```
SWP1(config)#interface ge17
SWP1(config-if)#channel-group 10 mode active
```

10.2.4 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 geNN	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"
Mux machine state	Status of the LACP protocol Receive machine transition variable • "Detached" • "Waiting" • "Attached" • "Collecting/Distributing"

Item	Description
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.

```
SWP1#show etherchannel
% Lacp Aggregator: po10
% Load balancing: src-dst-mac
% Member:
   ge17
   ge19
   ge21
   ge23
```

Shows the status of the LAN/SFP ports that make up the LACP logical interface.

```
SWP1#show etherchannel ge17
Etherchannel ge17
 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           17                             17
  Timeout         Long                           Long
  Active             1                              1
  Synchronized       1                              1
  Collecting         1                              1
  Distributing       1                              1
  Defaulted          0                              0
  Expired            0                              0
 Aggregator ID  1000000
```

10.2.5 Set LACP system priority

[Syntax]

lacp system-priority *priority*
no lacp system-priority

[Parameter]

priority : <1-65535>

LACP system priority
Lower numbers have higher priority

[Initial value]

lacp system-priority 32768

[Input mode]

global configuration mode

[Description]

Sets the LACP system priority.

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

[Note]

If a 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 to 100.

```
SWP1(config)#lacp system-priority 100
```

10.2.6 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.

```
SWP1>show lacp sys-id
% System 0x8000, 00-a0-de-ae-b8-7e
```

10.2.7 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 a LACP logical interface.

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.

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 #17 to short.

```
SWP1(config)#interface ge17
SWP1(config-if)#lacp timeout short
```

10.2.8 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.

```
SWP1#clear lacp counters
```

10.2.9 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.

```
SWP1#show lacp-counter
% Traffic statistics
Port       LACPDUs         Marker         Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po1 129
ge25     297     298     0       0       0       0
ge21     306     299     0       0       0       0
ge19     305     298     0       0       0       0
ge17     309     1350    0       0       0       0
ge23     186     186     0       0       0       0
```

10.2.10 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]

interface mode

[Description]

Sets rules to specify the forwarding destination interface of the load balance function.

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

[Note]

This command can be specified only for logical interface.

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]

For the load balance function of the LACP logical interface #1, specify that the forwarding destination interface is determined according to the source and destination IPv4/IPv6 addresses.

```
SWP1(config)#interface po1
SWP1(config-if)#port-channel load-balance src-dst-ip
```

10.2.11 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 interfaces.

If summary is specified, an abbreviated display is shown; if detail is specified, details are shown.

If 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 is 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 portt 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, and data communication is possible.

[Example]

Show the status of the LACP logical interface.

```
SWP1#show etherchannel status summary
Aggregator po1
 ID          1000000
 Status       Ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    1/  1
Aggregator po2
 ID          1000001
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
Aggregator po127
 ID          1000002
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1


SWP1#show etherchannel status detail
Aggregator po1
 ID          1000000
 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
  ge17    Selected     Synchronized  yes
Aggregator po2
 ID          1000001
 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
  ge23    Selected     Synchronized  no
  ge24    Unselected   Synchronized  no
Aggregator po127
 ID          1000002
 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
 ge25    Selected     Synchronized  no
```

10.2.12 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 is evaluated, and they are combined starting with the highest-priority 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.

```
SWP1(config-if)#channel-group 1 mode active
SWP1(config-if)#lacp port-priority 1024
```

10.3 Port authentication

10.3.1 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)

Since MAC authentication and IEEE 802.1X authentication are exclusive control systems, it is necessary to invalidate MAC authentication in order to enable IEEE 802.1X authentication. (**no aaa authentication auth-mac** command)

[Example]

Enable IEEE 802.1X authentication for the entire system.

```
SWP1(config)#aaa authentication dot1x
```

10.3.2 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)

Since MAC authentication and IEEE 802.1X authentication are exclusive control systems, it is necessary to invalidate IEEE 802.1X authentication in order to enable MAC authentication. (**no aaa authentication dot1x** command)

[Example]

Enable MAC authentication for the entire system.

```
SWP1(config)#aaa authentication auth-mac
```

10.3.3 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 LAN/SFP port.

[Example]

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

```
SWP1(config)#interface ge1
SWP1(config-if)#dot1x port-control auto
```

10.3.4 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 LAN/SFP port.

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.

```
SWP1(config)#interface ge1
SWP1(config-if)#dot1x control-direction in
```

10.3.5 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 LAN/SFP port.

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".

```
SWP1(config)#interface ge1
SWP1(config-if)#dot1x max-auth-req 3
```

10.3.6 Set the MAC authentication function

[Syntax]

auth-mac enable
auth-mac disable
no auth-mac enable

[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 LAN/SFP port.

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.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth-mac enable
```

10.3.7 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 port 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.

```
SWP1(config)#auth-mac auth-user unformatted upper-case
```

10.3.8 Set host mode

[Syntax]

auth host-mode *mode*
no auth host-mode

[Parameter]

mode : Operating mode for port authentication

Operation mode for port authentication	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.

[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 LAN/SFP port.

Changing the settings for this command will make the authentication state return to the default.

When using dynamic VLAN in multi-host mode, 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)

[Example]

Change the LAN port #1 to multi host mode.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth host-mode multi-host
```

10.3.9 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 LAN/SFP port.

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.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command)

[Example]

Enable re-authenticatio of LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth reauthentication
```

10.3.10 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 LAN/SFP port.

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)

[Example]

Enable dynamic VLAN on LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth dynamic-vlan-creation
```

10.3.11 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 LAN/SFP port.

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)

[Example]

This specifies guest VLAN #10 for LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth guest-vlan 10
```

10.3.12 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 LAN/SFP port.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command)

[Example]

Set the suppression period for LAN port #1 to 300.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth timeout quiet-period 300
```

10.3.13 Set reauthentication interval

[Syntax]

auth timeout reauth-period *time*
no auth timeout reauth-period

[Parameter]

time : <60-86400>

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 LAN/SFP port.

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 reauthentication** command)

[Example]

Set the reauthentication period for LAN port #1 to 120.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth timeout reauth-period 120
```

10.3.14 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 LAN/SFP port.

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)

[Example]

This sets the reply wait time to the RADIUS server overall to 180 seconds, for authentication requests from LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth timeout server-timeout 180
```

10.3.15 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 LAN/SFP port.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command)

[Example]

Set the reply wait time from the supplicant of LAN port #1 to 180 seconds.

```
SWP1(config)#interface ge1
SWP1(config-if)#auth timeout supp-timeout 180
```

10.3.16 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 (A:B:C:D:E:F:G:H) When specifying an IPv6 link local address, the transmitting interface also needs to be specified (fe80::X%vlan0.N 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 (64 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.

[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.

```
SWP1(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.

```
SWP1(config)#radius-server host 192.168.100.101 auth-port 1645 key abcde
```

10.3.17 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.

```
SWP1(config)#radius-server timeout 10
```

10.3.18 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.

```
SWP1(config)#radius-server retransmit 5
```

10.3.19 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 (64 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".

```
SWP1(config)#radius-server key abcde
```

10.3.20 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.

```
SWP1(config)#radius-server deadtime 1
```

10.3.21 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.

```
SWP1#show auth status
[System information]
  802.1X Port-Based Authentication : Enabled
  MAC-Based Authentication         : Disabled

  RADIUS server address :
    192.168.100.101 (port:1812)

[Interface information]
  Interface ge1 (up)
    802.1X Authentication   : Auto (configured:auto)
```

```
    MAC 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

  Interface ge4 (down)
    802.1X Authentication   : Auto (configured:auto)
    MAC Authentication      : Disabled (configured:disable)
    Host mode               : Multi-host
    Dynamic VLAN creation   : Enabled
    Guest VLAN              : Disabled
    Reauthentication        : Enabled
    Reauthentication period : 120 sec
    MAX request             : 2 times
    Supplicant timeout      : 180 sec
    Server timeout          : 120 sec
    Quiet period            : 60 sec
    Controlled directions   : In (configured:in)
    Protocol version        : 2
    Authentication status   : Unauthorized
```

10.3.22 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.

```
SWP1#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
```

10.4 Error detection function

10.4.1 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 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.

If 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.

```
SWP1(config)#errdisable auto-recovery bpduguard interval 600
```

Disable automatic recovery after loop detection has caused the errdisable state.

```
SWP1(config)#no errdisable auto-recovery loop-detect
```

10.4.2 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.

```
SWP1>show errdisable

function        auto recovery          interval
-----------------------------------------------
BPDU guard      disable
Loop detect     enable                      300

port            reason
----------------------------
```

```
ge1             BPDU guard
ge7             Loop detect
```

Chapter 11

L2 switching function

11.1 VLAN

11.1.1 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.

```
SWP1(config)#vlan database
SWP1(config-vlan)#
```

11.1.2 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 (32 characters 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]

Depends on VLAN preset. Refer to Default setting values.

[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.

[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. Also, multiple VLAN IDs cannot be specified when using the "no" syntax.

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".

```
SWP1(config-vlan)#vlan 1000 name Sales
```

11.1.3 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 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)

```
SWP1(config-vlan)#vlan 100
SWP1(config-vlan)#vlan 101
SWP1(config-vlan)#vlan 102
SWP1(config-vlan)#vlan 103
```

```
SWP1(config-vlan)#private-vlan 100 primary
SWP1(config-vlan)#private-vlan 101 community
SWP1(config-vlan)#private-vlan 102 community
SWP1(config-vlan)#private-vlan 103 isolated
```

11.1.4 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-id*.

By specifying "remove," remove the association of the *vlan-id* and the *2nd-vlan-id*.

If this command is executed with the "no" syntax, all associations to the primary VLAN are deleted.

[Note]

If you specify the **private-vlan association add** command with a combination of "-" or "," in the *2nd-vlan-ids*, the command setting will fail if you revert to an older version (Rev.2.01.04 or earlier). As a result, normal communication might become impossible. (Example setting: private-vlan 100 association add 101,103-105)

[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)

```
SWP1(config-vlan)#vlan 100
SWP1(config-vlan)#vlan 101
SWP1(config-vlan)#vlan 102
SWP1(config-vlan)#vlan 103
SWP1(config-vlan)#private-vlan 100 primary
SWP1(config-vlan)#private-vlan 101 community
SWP1(config-vlan)#private-vlan 102 community
SWP1(config-vlan)#private-vlan 103 isolated
SWP1(config-vlan)#private-vlan 100 association add 101
SWP1(config-vlan)#private-vlan 100 association add 102
SWP1(config-vlan)#private-vlan 100 association add 103
```

11.1.5 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 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.

```
SWP1(config)#vlan access-map VAM001
SWP1(config-vlan-access-map)#
```

11.1.6 Set access list for VLAN access map

[Syntax]

match *type* **access-list** *list-id*
no match *type* **access-list** *list-id*

[Parameter]

type : Type of access list to use

Setting value	Description
ip	Use an IPv4 access list
mac	Use a MAC access list

list-id : <1-99>, <1300-1999>, <100-199>, <2000-2699>

Access list number specified by the **access-list** command
You must specify the number used by the access list specified by *type*

[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 allows packets from 192.168.0.1.

```
SWP1(config)#access-list 2 permit 192.168.0.1 0.0.0.255
SWP1(config)#vlan access-map VAM001
SWP1(config-vlan-access-map)#match ip access-list 2
```

11.1.7 Set VLAN access map filter

[Syntax]

vlan filter *access-map-name vlan-id*
no vlan filter *access-map-name vlan-id*

[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

[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.

[Example]

Create a VLAN access map named "VAM001", specify an access list that allows packets from 192.168.0.1, and then specify VAM001 for VLAN #1000.

```
SWP1(config)#vlan database
SWP1(config-vlan)#vlan 1000
SWP1(config-vlan)#exit
SWP1(config)#access-list 2 permit 192.168.0.1 0.0.0.255
SWP1(config)#vlan access-map VAM001
SWP1(config-vlan-access-map)#match ip access-list 2
SWP1(config-vlan-access-map)#exit
SWP1(config)#vlan filter VAM001 1000
```

11.1.8 Set access port (untagged port)

[Syntax]

switchport mode access

[Initial value]

Depends on VLAN preset. Refer to Default setting values.

[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.

```
SWP1(config)#interface ge1
SWP1(config-if)#switchport mode access
```

11.1.9 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]

Depends on VLAN preset. Refer to Default setting values.

[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.

```
SWP1(config)#interface ge1
SWP1(config-if)#switchport access vlan 10
```

11.1.10 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]

Depends on VLAN preset. Refer to Default setting values.

[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.

```
SWP1(config)#interface ge1
SWP1(config-if)#switchport mode trunk
```

11.1.11 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]

Depends on VLAN preset. Refer to Default setting values.

[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 setting of 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.2.01.04 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#switchport mode trunk
SWP1(config-if)#switchport trunk allowed vlan add 2
```

11.1.12 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#switchport mode trunk
SWP1(config-if)#switchport trunk native vlan 2
```

11.1.13 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#switchport mode private-vlan promiscuous
SWP1(config-if)#exit
SWP1(config)#interface ge2
SWP1(config-if)#switchport mode private-vlan host
```

11.1.14 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

```
SWP1(config)# interface ge1
SWP1(config-if)# switchport mode private-vlan host
SWP1(config-if)# switchport private-vlan host-association 100 add 101
SWP1(config-if)# interface ge2
SWP1(config-if)# switchport mode private-vlan host
SWP1(config-if)# switchport private-vlan host-association 100 add 102
SWP1(config-if)# interface ge3
SWP1(config-if)# switchport mode private-vlan host
SWP1(config-if)# switchport private-vlan host-association 100 add 103
```

11.1.15 Set promiscuous port for private VLAN

[Syntax]

switchport private-vlan mapping *pri-vlan-id* add *2nd-vlan-id*
switchport private-vlan mapping *pri-vlan-id* remove *2nd-vlan-id*
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-id : <2-4094>

VLAN ID specified as 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]

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-id* 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.

If you specify the **switchport private-vlan mapping add** command with a combination of "-" or "," in the *2nd-vlan-ids*, the command setting will fail if you revert to an older version (Rev.2.01.04 or earlier). As a result, normal communication might become impossible. (Example setting: switchport private-vlan mapping 100 add 101,103-105)

[Example]

Make LAN port #1 operate as a promiscuous port, specify primary VLAN #100, and associate the secondary VLANs #101, #102, and #103.

```
SWP1(config)# interface ge1
SWP1(config-if)# switchport mode private-vlan promiscuous
SWP1(config-if)# switchport private-vlan mapping 100 add 101
SWP1(config-if)# switchport private-vlan mapping 100 add 102
SWP1(config-if)# switchport private-vlan mapping 100 add 103
```

11.1.16 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
Name	Name of the VLAN

Item	Description
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.

```
SWP1>show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID  Name                             State   Member ports
======= ================================ ======= ====================
1       default                          ACTIVE  ge1(u) ge2(u) ge3(u)
                                                 ge4(u) ge5(u) ge6(u)
                                                 ge7(u) ge8(u) ge9(u)
                                                 ge10(u)
```

11.1.17 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.

```
SWP1>show vlan private-vlan
PRIMARY       SECONDARY          TYPE         INTERFACES
-------        ---------       ----------      ----------
      2              21         isolated
      2              22         community
```

11.1.18 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.

```
SWP1>show vlan access-map
VLAN-ACCESS-MAP: VAM001
match ip access-list 2
```

11.1.19 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

[Example]

Show VLAN access map filter information.

```
SWP1>show vlan filter
Vlan Filter VAM001 is applied to vlan 1000
```

11.2 STP (Spanning Tree Protocol)

11.2.1 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 is executed with the "no" syntax, spanning tree is enabled for the entire system.

[Note]

The spanning tree function and the loop detection function can be used together on the entire system. Enabling spanning tree does not set the **no loop-detect** command.

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.

```
SWP1(config)#spanning-tree shutdown
```

11.2.2 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.

```
SWP1(config)#spanning-tree forward-time 10
```

11.2.3 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.

```
SWP1(config)#spanning-tree max-age 25
```

11.2.4 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.

```
SWP1(config)#spanning-tree priority 4096
```

11.2.5 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]

Depends on VLAN preset. Refer to Default setting values.

[Input mode]

interface mode

[Description]

Sets spanning tree operation for the applicable interface.

[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 this command is used to enable spanning tree, the loop detection function is disabled for the applicable interface.

[Example]

Disable spanning tree for LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree disable
```

11.2.6 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."

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree link-type shared
```

11.2.7 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree bpdu-filter enable
```

11.2.8 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree bpdu-guard enable
```

11.2.9 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree path-cost 100000
```

11.2.10 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree priority 64
```

11.2.11 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.

spanning-tree portfast and **no spanning-tree portfast** have been abolished.

If there is a **spanning-tree portfast** in the config, it is changed to **spanning-tree edgeport**

[Example]

Sets LAN port #1 as the edge port.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree edgeport
```

11.2.12 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

Item	Description
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
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.

```
SWP1>show spanning-tree interface ge1
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 13 -  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 800100a0deaeb83d
% Default: CIST Reg Root Id 800100a0deaeb83d
% Default: CIST Bridge Id 800100a0deaeb879
% Default: 4 topology change(s)  - last topology change Thu Jan  1 09:01:05 1970

%   ge1: Port Number 1 - Ifindex 1 - Port Id 8001 - Role Disabled - State Discarding
%   ge1: Designated External Path Cost 0 -Internal Path Cost 0
%   ge1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge1: Designated Port Id 0 - CIST Priority 128  -
%   ge1: Message Age 0 - Max Age 0
%   ge1: CIST Hello Time 0 - Forward Delay 0
%   ge1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   ge1: forward-transitions 0
%   ge1: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   ge1: No portfast configured - Current  portfast off
%   ge1: bpdu-guard  disabled  - Current bpdu-guard off
%   ge1: bpdu-filter disabled  - Current bpdu-filter off
%   ge1: no root guard configured     - Current root guard off
%   ge1: Configured Link Type point-to-point - Current point-to-point
%   ge1: No auto-edge configured - Current port Auto Edge off
```

11.2.13 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.

```
SWP1>show spanning-tree statistics interface ge1

                 Port number = 1 Interface = ge1
                 ================================
% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Enable
% Spanning Tree Type                : Multiple Spanning Tree Protocol
% Current Port State                : Forwarding
% Port ID                           : 8001
% Port Number                       : 1
% Path Cost                         : 20000
% Message Age                       : 1
% Designated Root                   : c4:64:13:00:00:00
% Designated Cost                   : 20000
% Designated Bridge                 : 00:a0:de:00:00:00
% Designated Port Id                : 8001
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE

% PORT Based Information & Statistics
% ----------------------------------
```

```
% Config Bpdu's xmitted              : 1
% Config Bpdu's received             : 1
% TCN Bpdu's xmitted                 : 4
% TCN Bpdu's received                : 2
% 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              : ACTIVE
% Topology Change Timer Value        : 1
% 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               : 3


% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : 00:a0:de:00:00:00
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 2
% Last Topology Change Occured       : Thu Jan  1 00:00:00 2015
% Topology Change                    : TRUE
% Topology Change Detected           : TRUE
% Topology Change Count              : 42
% Topology Change Last Recvd from    : c4:64:13:00:00:00
```

11.2.14 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 an 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.

```
SWP1#clear spanning-tree detected protocols interface ge1
```

11.2.15 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.

```
SWP1(config)#spanning-tree mst configuration
SWP1(config-mst)#
```

11.2.16 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.

```
SWP1(config)#spanning-tree mst configuration
SWP1(config-mst)#instance 1
```

11.2.17 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.

```
SWP1(config)#spanning-tree mst configuration
SWP1(config-mst)#instance 1 vlan 2
```

11.2.18 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.

```
SWP1(config)#spanning-tree mst configuration
SWP1(config-mst)#instance 2
SWP1(config-mst)#instance 2 priority 4096
```

11.2.19 Set MST region name

[Syntax]

region *region-name*
no region

[Parameter]

region-name : Single-byte alphanumeric characters and single-byte symbols (32 characters 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".

```
SWP1(config)#spanning-tree mst configuration
SWP1(config-mst)#region Test1
```

11.2.20 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.

[Example]

Set the revision number as 2 for the MST region.

```
SWP1(config)#spanning-tree mst configuration
SWP1(config-mst)#revision 2
```

11.2.21 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree instance 2
```

11.2.22 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree instance 2
SWP1(config-if)#spanning-tree instance 2 priority 16
```

11.2.23 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.

```
SWP1(config)#interface ge1
SWP1(config-if)#spanning-tree instance 2
SWP1(config-if)#spanning-tree instance 2 path-cost 100000
```

11.2.24 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.

```
SWP1>show spanning-tree mst config
%
%  MSTP Configuration Information for bridge 0 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0x919CA1A4907081530782879A411E6994
%-------------------------------------------------------
```

11.2.25 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.

```
SWP1>show spanning-tree mst
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 40000 - CIST Root Port 2 -  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 8000c46413a93de0
% Default: CIST Reg Root Id 800100a0deaeb920
% Default: CIST Bridge Id 800100a0deaeb920
% Default: 896 topology change(s)  - last topology change Fri Jan 16 08:04:20 1970

%
%   Instance        VLAN
%   0:              1
%   1:              10 (ge18)
%   5:              20, 30 (ge19)
%   6:              40 (ge20)
%   7:              50 (ge21)
```

Show detailed MSTP information for LAN port #19.

```
SWP1>show spanning-tree mst detail interface ge19
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 40000 - CIST Root Port 2 -  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 8000c46413a93de0
% Default: CIST Reg Root Id 800100a0deaeb920
% Default: CIST Bridge Id 800100a0deaeb920
% Default: 896 topology change(s)  - last topology change Fri Jan 16 08:04:20 1970

%   ge19: Port Number 19 - Ifindex 19 - Port Id 8013 - Role Disabled - State
Discarding
%   ge19: Designated External Path Cost 0 -Internal Path Cost 0
%   ge19: Configured Path Cost 20000000  - Add type Explicit ref count 2
%   ge19: Designated Port Id 0 - CIST Priority 128  -
%   ge19: Message Age 0 - Max Age 0
%   ge19: CIST Hello Time 0 - Forward Delay 0
%   ge19: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer
0
%   ge19: forward-transitions 0
%   ge19: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   ge19: No portfast configured - Current  portfast off
%   ge19: bpdu-guard  disabled  - Current bpdu-guard off
%   ge19: bpdu-filter disabled  - Current bpdu-filter off
%   ge19: no root guard configured     - Current root guard off
%   ge19: Configured Link Type point-to-point - Current point-to-point
%   ge19: No auto-edge configured - Current port Auto Edge off
%

% Instance  5:  Vlans: 20, 30
% Default: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 800500a0deaeb920
% Default: MSTI Bridge Id 800500a0deaeb920
%   ge19: Port Number 19 - Ifindex 19 - Port Id 8013 - Role Disabled - State
Discarding
%   ge19: Designated Internal Path Cost 0  - Designated Port Id 0
%   ge19: Configured Internal Path Cost 20000000
%   ge19: Configured CST External Path cost 20000000
```

```
%   ge19: CST Priority 128  - MSTI Priority 128
%   ge19: Designated Root 000000a0deaeb920
%   ge19: Designated Bridge 000000a0deaeb920
%   ge19: Message Age 0 - Max Age 0
%   ge19: Hello Time 0 - Forward Delay 0
%   ge19: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

11.2.26 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 #5.

```
SWP1>show spanning-tree mst instance 5
% Default: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 800500a0deaeb920
% Default: MSTI Bridge Id 800500a0deaeb920
%   ge19: Port Number 19 - Ifindex 19 - Port Id 8013 - Role Disabled - State
Discarding
%   ge19: Designated Internal Path Cost 0  - Designated Port Id 0
%   ge19: Configured Internal Path Cost 20000000
%   ge19: Configured CST External Path cost 20000000
%   ge19: CST Priority 128  - MSTI Priority 128
%   ge19: Designated Root 000000a0deaeb920
%   ge19: Designated Bridge 000000a0deaeb920
%   ge19: Message Age 0 - Max Age 0
%   ge19: Hello Time 0 - Forward Delay 0
%   ge19: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

11.3 Loop detection

11.3.1 Set loop detection function (system)

[Syntax]

loop-detect enable
no loop-detect

[Initial value]

loop-detect enable

[Input mode]

global configuration mode

[Description]

Enables the loop detection function for the entire system.

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

[Note]

The spanning tree function and the loop detection function can be used together on the entire system. Enabling the loop detection function does not specify the **spanning-tree shutdown** command.

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 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
- LAN/SFP port that is inside a logical interface

[Example]

Enable the loop detection function for the entire system.

```
SWP1(config)#loop-detect enable
```

Disable the loop detection function for the entire system.

```
SWP1(config)#no loop-detect
```

11.3.2 Set loop detection function (interface)

[Syntax]

loop-detect enable
no loop-detect

[Initial value]

Depends on VLAN preset. Refer to Default setting values.

[Input mode]

interface mode

[Description]

Enables the loop detection function for the corresponding interface.

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

[Note]

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

In order to enable the loop detection function, the loop detection function must be enabled on the entire system 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 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 trunk port for which native VLAN is not specified
- LAN/SFP port that is inside a logical interface

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 enabled
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.

```
SWP1(config)#interface ge1
SWP1(config-if)#loop-detect enable
```

Disable the loop detection function of LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#no loop-detect
```

11.3.3 Set port blocking for loop detection

[Syntax]

loop-detect blocking
no loop-detect blocking

[Initial value]

loop-detect blocking

[Input mode]

interface mode

[Description]

Enables blocking if a loop is detected on the applicable interface.

If this is executed with the "no" syntax, blocking does not occur if a loop is detected.

[Note]

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

[Example]

Block if a loop is detected on LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#loop-detect blocking
```

Do not block if a loop is detected on LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#no loop-detect blocking
```

11.3.4 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.

```
SWP1#loop-detect reset
```

11.3.5 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
- Loop detection status for each LAN/SFP port
  - Interface name (port)
  - Setting of the loop detection function (loop-detect) for LAN/SFP port. If the loop detection function is operating, (*) is added
  - Status of the Port Blocking setting (port-blocking)
  - Loop detection status (status)

[Example]

Shows the loop detection status.

```
SWP1>show loop-detect
loop-detect: Enable

port      loop-detect    port-blocking           status
-------------------------------------------------------
ge1            enable(*)        enable         Detected
ge2            enable(*)        enable         Blocking
ge3            enable(*)        enable           Normal
ge4            enable(*)        enable           Normal
ge5            enable(*)       disable           Normal
ge6            enable(*)        enable           Normal
ge7            enable(*)        enable         Shutdown
ge8           disable           enable           ------
ge9            enable           enable           Normal
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

11.4 FDB (Forwarding Data Base)

11.4.1 Set MAC address acquisition function

[Syntax]

mac-address-table acquire
no mac-address-table acquire

[Initial value]

mac-address-table acquire

[Input mode]

global configuration mode

[Description]

Enables the MAC address acquisition function.

If this is executed with the "no"syntax, the MAC address acquisition function is disabled.

[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.

```
SWP1(config)#mac-address-table acquire
```

11.4.2 Set dynamic entry ageing time

[Syntax]

mac-address-table ageing-time *time*
no mac-address-table ageing-time

[Parameter]

time : <10-634>
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 600 seconds.

```
SWP1(config)#mac-address-table ageing-time 600
```

11.4.3 Clear dynamic entry

[Syntax]

clear mac-address-table dynamic
clear mac-address-table dynamic adress *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	:	<1-15>
		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.

```
SWP1#clear mac-address-table dynamic address 00a0.de11.2233
```

11.4.4 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*.

- 0180.c200.0000～0180.c200.000f
- 0180.c200.0020～0180.c200.002f

[Example]

Specify that frames addressed to 00a0.de11.2233 are forwarded to LAN port #2.

```
SWP1(config)#mac-address-table static 00a0.de11.2233 forward ge2
```

11.4.5 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.

```
SWP1>show mac-address-table
VLAN  port   mac              fwd      type     timeout
   1  ge2    00a0.de11.2233  forward  static         0
   1  ge1    1803.731e.8c2b  forward  dynamic      300
   1  ge1    782b.cbcb.218d  forward  dynamic      300
```

Chapter 12

IP multicast control

12.1 Basic settings

12.1.1 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.

```
SWP1(config)#l2-unknown-mcast discard
```

12.1.2 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

[Example]

This forwards frames for the link local multicast address as unknown multicasts without discarding them.

```
SWP1(config)#l2-unknown-mcast discard
SWP1(config)#l2-unknown-mcast forward link-local
```

12.1.3 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 224.0.0.251 with the destination IPv4 address received by VLAN #1.

```
SWP1(config)#interface vlan0.1
SWP1(config-if)#l2-mcast flood 224.0.0.251
```

12.2 IGMP snooping

12.2.1 Enable/disable IGMP snooping

[Syntax]

igmp snooping
no igmp snooping

[Initial value]

Depends on VLAN preset. Refer to Default setting values.

[Input mode]

interface mode

[Description]

Enables the IGMP snooping setting of the interface.

If this is executed with the "no" syntax, the IGMP snooping setting is disabled.

[Note]

This command can be specified only for VLAN interface.

[Example]

Enable IGMP snooping for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping
```

Disable IGMP snooping for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no igmp snooping
```

12.2.2 Set IGMP snooping fast-leave

[Syntax]

igmp snooping fast-leave
no igmp snooping fast-leave

[Initial value]

no igmp snooping fast-leave

[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.

[Note]

This command can be specified only for VLAN interface. Also, this can be specified only if IGMP 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 IGMP snooping fast-leave for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping fast-leave
```

Disable IGMP snooping fast-leave for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no igmp snooping fast-leave
```

12.2.3 Set multicast router connection destination

[Syntax]

igmp snooping mrouter interface *ifname*
no igmp snooping mrouter interface *ifname*

[Parameter]

ifname	:	LAN/SFP port interface name Interface to set

[Initial value]

no igmp snooping mrouter interface (all LAN/SFP port)

[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. Also, this can be specified only if IGMP snooping is enabled.

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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping mrouter interface ge8
```

Remove LAN port #8 as a connection destination of the multicast router.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no igmp snooping mrouter interface ge8
```

12.2.4 Set query transmission function

[Syntax]

igmp snooping querier
no igmp snooping querier

[Initial value]

Depends on VLAN preset. Refer to Default setting values.

[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. Also, this can be specified only if IGMP snooping is enabled.

[Example]

Enable the transmission function for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping querier
```

Disable the transmission function for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no igmp snooping querier
```

12.2.5 Set IGMP query transmission interval

[Syntax]

igmp snooping query-interval *interval*
no igmp snooping query-interval

[Parameter]

interval	:	<20-18000>
		Query transmission interval (seconds)

[Initial value]

Depends on VLAN preset. Refer to Default setting values.

[Input mode]

interface mode

[Description]

Sets the transmission interval for IGMP queries.

If this command is executed with the "no" syntax, this is set to 125 seconds.

[Note]

This command can be specified only for VLAN interface. Also, this can be specified only if IGMP snooping is enabled.

[Example]

Set the VLAN #2 query transmission interval to 30 seconds.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping query-interval 30
```

Return the VLAN #2 query transmission interval to the default setting.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no igmp snooping query-interval
```

12.2.6 Set discarding of IGMP packets with invalid TTL values

[Syntax]

igmp snooping check ttl
no igmp snooping check ttl

[Initial value]

Depends on VLAN preset. Refer to Default setting values.

[Input mode]

interface mode

[Description]

Discards IGMP packets for which the IP header's TTL value is invalid (other than 1).

If this is executed with the "no" syntax, IGMP packets are not discarded even if the TTL value is invalid (other than 1).

If the applicable packet is not discarded but forwarded, the TTL value is corrected to 1 when forwarding.

[Note]

This command can be specified only for VLAN interface. Also, this can be specified only if IGMP snooping is enabled.

[Example]

Discard IGMP packets on VLAN #2 whose TTL value is invalid.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping check ttl
```

Do not discard IGMP packets on VLAN #2 whose TTL value is invalid.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no igmp snooping check ttl
```

12.2.7 Set IGMP version

[Syntax]

igmp snooping version *version*
no igmp snooping version

[Parameter]

version : <2-3>
IGMP version

[Initial value]

igmp snooping version 3

[Input mode]

interface mode

[Description]

Sets the IGMP version.

If this command is executed with the "no" syntax, the IVMP version returns to the default setting (V3).

[Note]

This command can be specified only for VLAN interface. Also, this can be specified only if IGMP snooping is enabled.

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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping version 2
```

On VLAN #2, return the IGMP version to the default setting.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no igmp snooping version
```

12.2.8 Settings for IGMP Report Suppression

[Syntax]

igmp snooping report-suppression *switch*
no igmp snooping report-suppression

[Parameter]

switch : IGMP report suppression

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping report-suppression enable
```

Disables IGMP report suppression at VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#igmp snooping report-suppression disable
```

12.2.9 Show multicast router connection port information

[Syntax]

show 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.

```
SWP1#show igmp snooping mrouter vlan0.2
VLAN     Interface
2         ge9
2         ge11
```

12.2.10 Show IGMP group membership information

[Syntax]

show igmp snooping groups [detail]
show igmp snooping groups *A.B.C.D* [detail]
show 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.

```
SWP1#show igmp snooping groups
IGMP Connected Group Membership
Group Address    Interface            Uptime   Expires  Last Reporter
239.0.0.1        ge2                  00:00:01 00:04:19 192.168.1.3
```

Show detailed IGMP group membership information.

```
SWP1#show igmp snooping groups detail
Interface:      ge2
Group:          239.0.0.1
Uptime:         00:00:05
Group mode:     Exclude (Expires: 00:04:14)
Last reporter:  192.168.1.3
Source list is empty
```

12.2.11 Show an interface's IGMP-related information

[Syntax]

show 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.

```
SWP1#show igmp snooping interface vlan0.1
Interface vlan0.1 (Index 10001)
 IGMP Active, Non-Querier, Version 3 (default)
 Internet address is 192.168.1.150
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP querying router is 0.0.0.0
 IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Group Membership interval is 260 seconds
 IGMP Last member query count is 2
 Last member query response interval is 1000 milliseconds
 IGMP Snooping is globally enabled
 IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
 IGMP Snooping check TTL is enabled
```

12.2.12 Clear IGMP group membership entries

[Syntax]

clear igmp snooping
clear igmp snooping group *A.B.C.D*
clear 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.

```
SWP1#clear igmp snooping interface vlan0.1
```

12.3 MLD snooping

12.3.1 Enable/disable MLD snooping

[Syntax]

mld snooping

no mld snooping

[Initial value]

mld snooping

[Input mode]

interface mode

[Description]

Enables the MLD snooping setting of the interface.

If this is executed with the "no" syntax, the MLD snooping setting is disabled.

[Note]

This command can be specified only for VLAN interfaces.

[Example]

Enable MLD snooping for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#mld snooping
```

Disnable MLD snooping for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no mld snooping
```

12.3.2 Set MLD snooping fast-leave

[Syntax]

mld snooping fast-leave
no mld snooping fast-leave

[Initial value]

no mld snooping fast-leave

[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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#mld snooping fast-leave
```

Disable MLD snooping fast-leave for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no mld snooping fast-leave
```

12.3.3 Set multicast router connection destination

[Syntax]

mld snooping mrouter interface *ifname*
no mld snooping mrouter interface *ifname*

[Parameter]

ifname : Interface name of LAN/SFP port

Interface to set

[Initial value]

no mld snooping mrouter interface (all LAN/SFP port)

[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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#mld snooping mrouter interface ge8
```

Remove LAN port #8 as a connection destination of the multicast router.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no mld snooping mrouter interface ge8
```

12.3.4 Set query transmission function

[Syntax]

mld snooping querier
no mld snooping querier

[Initial value]

no mld snooping querier

[Input mode]

interface mode

[Description]

Enables the MLD query transmission function.

If this 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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#mld snooping querier
```

Disable the MLD query transmission function for VLAN #2.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no mld snooping querier
```

12.3.5 Set MLD query transmission interval

[Syntax]

mld snooping query-interval *interval*
no mld snooping query-interval

[Parameter]

interval : <20-18000>
Query transmission interval (seconds)

[Initial value]

mld snooping query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for MLD queries.

If this 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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#mld snooping query-interval 30
```

Return the VLAN #2 query transmission interval to the default setting.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no mld snooping query-interval
```

12.3.6 Set MLD version

[Syntax]

mld snooping version *version*
no mld snooping version

[Parameter]

version : <1-2>
MLD version

[Initial value]

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.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#mld snooping version 1
```

On VLAN #2, return the MLD version to the default setting.

```
SWP1#configure terminal
SWP1(config)#interface vlan0.2
SWP1(config-if)#no mld snooping version
```

12.3.7 Show multicast router connection port information

[Syntax]

show 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.

```
SWP1#show mld snooping mrouter vlan0.2
VLAN     Interface
2         ge9
2         ge11
```

12.3.8 Show MLD group membership information

[Syntax]

show mld snooping groups [detail]
show mld snooping groups *X:X::X:X* [detail]
show 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.

```
SWP1#show mld snooping groups
MLD Connected Group Membership
Group Address                           Interface            Uptime   Expires  Last
Reporter
ff15::1                                 ge3                  00:00:44 00:01:07
fe80::a00:27ff:fe8b:87e3
```

Show detailed MLD group membership information.

```
SWP1#show mld snooping groups detail
MLD Connected Group Membership Details for ge3
```

```
Interface:      ge3
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
```

12.3.9 Show an interface's MLD-related information

[Syntax]

show 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.

```
SWP1#show mld snooping interface vlan0.1
Interface vlan0.1 (Index 5001)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::2a0:deff:feae:b879
 MLD interface has 1 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 30 seconds
 MLD querier timeout is 65 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 70 seconds
 MLD Snooping is globally enabled
 MLD Snooping is enabled on this interface
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is enabled
 MLD Snooping report suppression is enabled
```

12.3.10 Clear MLD group membership entries

[Syntax]

clear mld snooping
clear mld snooping group *X:X::X:X*
clear 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.

```
SWP1#clear mld snooping interface vlan0.1
```

Chapter 13

Traffic control

13.1 ACL

13.1.1 Generate standard IPv4 access list

[Syntax]

access-list *std-ip-acl-id action src-info*
no access-list *std-ip-acl-id* [*action src-info*]

[Parameter]

std-ip-acl-id : <1-99>, <1300-1999>

ID of standard IPv4 access list

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 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)
any	Accept every IPv4 address
host A.B.C.D	Specifies a single IPv4 address (A.B.C.D)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates a standard IPv4 access list.

Multiple conditions (maximum 39) can be specified for the generated access list.

To apply the generated access list, use the "ip access-group" command in interface mode.

The "no access-list std-ip-acl-id action src-info" syntax deletes the standard IPv4 access list that matches all conditions.

The "no access-list std-ip-acl-id" syntax deletes the standard IPv4 access list that matches "std-ip-acl-id."

[Note]

An access list that is applied to an 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 standard IPv4 access list #2 which will permit frames from 192.168.1.0/24.

```
SWP1(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

Delete standard IPv4 access list #2.

```
SWP1(config)#no access-list 2
```

13.1.2 Add comment to standard IPv4 access list

[Syntax]

access-list *std-ip-acl-id* **remark** *line*
no access-list *std-ip-acl-id* **remark**

[Parameter]

std-ip-acl-id : <1-99>, <1300-1999>
ID of standard IPv4 access list to which comment is added

line : Comment to add. Up to 32 ASCII characters can be specified.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a comment (remark) to the already-generated standard IPv4 access list.

If this command is executed with the "no" syntax, the comment is deleted from the standard IPv4 access list.

[Note]

You can use this command to add a comment even after the access list has been applied to the LAN/SFP port. (The last-written comment overwrites the previous one.)

[Example]

Create standard IPv4 access list #2 which permits frames from 192.168.1.0/24, and add the comment "Test."

```
SWP1(config)#access-list 2 permit 192.168.1.0 0.0.0.255
SWP1(config)#access-list 2 remark Test
```

13.1.3 Apply standard IPv4 access list

[Syntax]

ip access-group *std-ip-acl-id direction*
no ip access-group *std-ip-acl-id direction*

[Parameter]

std-ip-acl-id : <1-99>, <1300-1999>
ID of standard 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 a standard IPv4 access list to the LAN/SFP port.

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 the LAN/SFP port.

[Note]

The restrictions of the access list apply only to frames that are subject to being relayed. Frames that are transmitted autonomously are excluded from these restrictions.

It is not possible to register multiple access lists for a single interface.

Access lists can be applied only to LAN/SFP ports. (Logical interfaces are not supported.)

[Example]

Apply standard IPv4 access list #1 to received frames of LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#ip access-group 1 in
```

13.1.4 Generate extended IPv4 access list

[Syntax]

access-list *ext-ip-acl-id action protocol src-info* [*src-port*] *dst-info* [*dst-port*]
no access-list *ext-ip-acl-id* [*action protocol src-info* [*src-port*] *dst-info* [*dst-port*]]

[Parameter]

ext-ip-acl-id : <100-199>, <2000-2699>

ID of extended IPv4 access list

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/X	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Xbit)
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/X	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Xbit)
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 extended IPv4 access list.

This is useful when you want to filter with more detail (specific protocols + destination information) than the standard IPv4 access list.

Multiple conditions (maximum 39) can be specified for the generated access list.

To apply the generated access list, use the "ip access-group" command of interface mode.

The "no access-list ext-ip-acl-id action protocol src-info [src-port] dst-info [dst-port]" syntax deletes the extended IPv4 address list that matches all conditions.

The "no access-list ext-ip-acl-id" syntax deletes the extended IPv4 access list that matches ext-ip-acl-id.

[Note]

An access list that is applied to a LAN/SFP port cannot be deleted using the "no" syntax. You must first cancel the application, and then delete the access list.

The extended IPv4 access list IDs are shared with the MAC access list IDs. This means that if the specified ID is being used by a MAC access list, it is handled as a command error.

For both src-port and dst-port, you can use "range" to specify a range; however for the entire system, only one extended IPv4 access list that specifies a range in this way can be applied to the interface by using the "ip access-group" command.

[Example]

Create access list #100 that permits communication from the source segment 192.168.1.0/24 to the destination 172.16.1.1.

```
SWP1(config)#access-list 100 permit any 192.168.1.0 0.0.0.255 host 172.16.1.1
```

Delete extended IPv4 access list #100.

```
SWP1(config)#no access-list 100
```

13.1.5 Add comment to extended IPv4 access list

[Syntax]

access-list *ext-ip-acl-id* **remark** *line*
no access-list *ext-ip-acl-id* **remark**

[Parameter]

ext-ip-acl-id : <100-199>, <2000-2699>

ID of extended IPv4 access list to which a comment will be added

line : Comment to add. Up to 32 ASCII characters can be specified.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a comment (remark) to the already-generated extended IPv4 access list.

If this command is executed with the "no" syntax, the comment is deleted from the extended IPv4 access list.

[Note]

You can use this command to add a comment even after the access list has been applied to the LAN/SFP port. (The last-written comment overwrites the previous one.)

[Example]

Create access list #100 that permits communication from source segment 192.168.1.0/24 to destination 172.16.1.1, and add the comment "Test."

```
SWP1(config)#access-list 100 permit any 192.168.1.0 0.0.0.255 host 172.16.1.1
SWP1(config)#access-list 100 remark Test
```

13.1.6 Apply extended IPv4 access list

[Syntax]

ip access-group *ext-ip-acl-id direction*
no ip access-group *ext-ip-acl-id direction*

[Parameter]

ext-ip-acl-id : <100-199>, <2000-2699>

ID of extended 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 extended IPv4 access list to the LAN/SFP port.

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 the LAN/SFP port.

[Note]

The restrictions of the access list apply only to frames that are subject to being relayed. Frames that are transmitted autonomously are excluded from these restrictions.

It is not possible to register multiple access lists for a single interface.

Access lists can be applied only to LAN/SFP ports. (Logical interfaces are not supported.)

As a restriction, an extended IPv4 access list for which the port number range (range X Y) is specified cannot be applied to transmitted frames (out).

[Example]

Apply extended IPv4 access list #100 to received frames of LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#ip access-group 100 in
```

13.1.7 Generate IPv6 access list

[Syntax]

access-list *ipv6-acl-id action src-info*
no access-list *ipv6-acl-id* [*action src-info*]

[Parameter]

ipv6-acl-id : <3000-3699>

ID of IPv6 access list

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 39) can be specified for the generated access list.

To apply the generated access list, use the "ip access-group" command of interface mode.

The "no access-list ipv6-acl-id action src-info" syntax deletes the extended IPv6 address list that matches all conditions.

The "no access-list ipv6-acl-id" syntax deletes the IPv6 access list that matches ipv6-acl-id.

[Note]

An access list that is applied to an 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 standard IPv6 access list #3002 which will permit frames from 3ffe:506::/32.

```
SWP1(config)#access-list 3002 permit 3ffe:506::/32
```

Delete standard IPv6 access list #3002.

```
SWP1(config)#no access-list 3002
```

13.1.8 Add comment to IPv6 access list

[Syntax]

access-list *ipv6-acl-id* **remark** *line*
no access-list *ipv6-acl-id* **remark**

[Parameter]

ipv6-acl-id	:	<1-99>, <1300-1999> ID of IPv6 access list to which comment is added
line	:	Comment to add. Up to 32 ASCII characters can be specified.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a comment (remark) to the already-generated IPv6 access list.

If this command is executed with the "no" syntax, the comment is deleted from the IPv6 access list.

[Note]

You can use this command to add a comment even after the access list has been applied to the LAN/SFP port. (The last-written comment overwrites the previous one.)

[Example]

Create IPv6 access list #3002 which permits frames from 3ffe:506::/32, and add the comment "Test."

```
SWP1(config)#access-list 3002 permit 3ffe:506::/32
SWP1(config)#access-list 3002 remark Test
```

13.1.9 Apply IPv6 access list

[Syntax]

ip access-group *ipv6-acl-id direction*
no ip access-group *ipv6-acl-id direction*

[Parameter]

ipv6-acl-id	:	<3000-3699> 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 the LAN/SFP port.

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 the LAN/SFP port.

[Note]

The restrictions of the access list apply only to frames that are subject to being relayed. Frames that are transmitted autonomously are excluded from these restrictions.

It is not possible to register multiple access lists for a single interface.

Access lists can be applied only to LAN/SFP ports. (Logical interfaces are not supported.)

[Example]

Apply IPv6 access list #3002 to received frames of LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#ip access-group 3002 in
```

13.1.10 Generate MAC access list

[Syntax]

access-list *mac-acl-id action* **mac** *src-info dst-info*
no access-list *mac-acl-id* [*action* **mac** *src-info dst-info*]

[Parameter]

mac-acl-id : <100-199>, <2000-2699>

ID of MAC access list

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 39) can be specified for the generated access list.

To apply the generated access list, execute the "mac access-group" command in interface mode.

The "no access-list mac-acl-id action mac src-info dst-info" syntax deletes the MAC access list that matches all conditions.

The "no access-list mac-acl-id" syntax deletes the MAC access list that matches mac-acl-id.

[Note]

An access list that is applied to a LAN/SFP port cannot be deleted using the "no" syntax. You must first cancel the application, and then delete the access list.

The MAC access list IDs are shared with the extended IPv4 access list IDs. This means that if the specified ID is used by an extended IPv4 access list, it is handled as a command error.

"W" and "H" represent a single character from the range 0-9, a-f, and A-F.

[Example]

Create MAC access list #2000 which discards frames from MAC address 00-A0-DE-12-34-56.

```
SWP1(config)#access-list 2000 deny mac 00A3.DE12.3456 0000.0000.0000 any
```

Delete MAC access list #2000.

```
SWP1(config)#no access-list 2000
```

13.1.11 Add comment to MAC access list

[Syntax]

access-list *mac-acl-id* **remark** *line*
no access-list *mac-acl-id* **remark**

[Parameter]

mac-acl-id : <100-199>, <2000-2699>
ID of extended MAC access list to which a comment will be added

line : Comment to add. Up to 32 ASCII characters can be specified.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a comment (remark) to the already-generated MAC access list.

If this command is executed with the "no" syntax, the comment is deleted from the MAC access list.

[Note]

You can use this command to add a comment even after the access list has been applied to the LAN/SFP port. (The last-written comment overwrites the previous one.)

[Example]

Create MAC access list #2000 which discards frames from MAC address 00-A0-DE-12-34-56, and add the comment "Test."

```
SWP1(config)#access-list 2000 deny mac 00A0.DE12.3456 0000.0000.0000 any
SWP1(config)#access-list 2000 remark Test
```

13.1.12 Apply MAC access list

[Syntax]

mac access-group *mac-acl-id direction*
no mac access-group *mac-acl-id direction*

[Parameter]

mac-acl-id : <100-199>, <2000-2699>
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 the LAN/SFP port.

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 command is executed with the "no" syntax, the applied access list is deleted from the LAN/SFP port.

[Note]

The restrictions of the access list apply only to frames that are subject to being relayed. Frames that are transmitted autonomously are excluded from these restrictions.

It is not possible to register multiple access lists for a single interface.

Access lists can be applied only to LAN/SFP ports. (Logical interfaces are not supported.)

[Example]

Apply access list #1 to received frames of LAN port #100.

```
SWP1(config)#interface ge1
SWP1(config-if)#mac access-group 100 in
```

13.1.13 Show generated standard IPv4 access list

[Syntax]

show ip access-list [*std-ip-acl-id*]

[Parameter]

std-ip-acl-id : <1-99>, <1300-1999>

ID of standard IPv4 access list

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the registered standard IPv4 access list.

If std-ip-acl-id is omitted, all IPv4 access lists are shown.

[Example]

Show a list.

```
SWP1>show ip access-list
Standard IP access list 3
    deny   10.0.6.0, wildcard bits 0.0.0.255
```

13.1.14 Show generated extended IPv4 access list

[Syntax]

show ip access-list [*ext-ip-acl-id*]

[Parameter]

ext-ip-acl-id : <100-199>, <2000-2699>

ID of extended IPv4 access list

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the registered extended IPv4 access list.

If ext-ip-acl-id is omitted, all IPv4 access lists are shown.

[Example]

Show a list.

```
SWP1>show ip access-list
Extended IP access list 100
    permit any host 10.0.6.195 any
```

13.1.15 Show generated IPv6 access list

[Syntax]

show ip access-list [*ipv6-acl-id*]

[Parameter]

ipv6-acl-id : <3000-3699>

ID of IPv6 access list

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the registered IPv6 access list.

If ipv6-acl-id is omitted, all IPv6 access lists are shown.

[Example]

Show a list.

```
SWP1>show ipv6 access-list
IPv6 access list 3010
    permit fe80:db8:2a0:1::/64
    deny   fe80::/16
```

13.1.16 Show generated MAC access list

[Syntax]

show mac access-list [*mac-acl-id*]

[Parameter]

mac-acl-id : <100-199>, <2000-2699>

ID of MAC access list

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows the registered MAC access list.

If mac-acl-id is omitted, all MAC access lists are shown.

[Example]

how a list.

```
SWP1>show mac access-list
MAC access list 101
    deny   mac 00A0.DE80.0000 0000.0000.FFFF any
    deny   mac host 00A0.DE80.1111 any
MAC access list 110
    deny   mac host 0000.1111.2222 any
```

13.1.17 Show all generated access lists

[Syntax]

show access-list

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Shows all registered access lists

[Example]

Show a list.

```
SWP1>show access-list
Standard IP access list 1
    permit 10.0.6.1 0.0.0.255
    deny   10.0.7.1
    permit 10.0.7.2 0.0.0.255

MAC access list 110
    permit mac any 00A0.DE77.0000 0000.0000.FFFF

Extended IP access list 2101
    permit tcp host 192.168.100.1 any
    permit tcp any 192.168.100.1 0.0.0.255
    deny   tcp any any

IPv6 access list 3010
    permit fe80:db8:2a0:1::/64
    deny   fe80::/16
```

13.1.18 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.

```
SWP1>show access-group
Interface ge7  : MAC access group 110 in
Interface ge15 : IP access group 1 out
Interface ge16 : IP access group 2101 in
Interface ge17 : IPv6 access group 3010 in
```

13.2 QoS (Quality of Service)

13.2.1 Enable/disable QoS

[Syntax]

mls qos enable
no mls qos

[Initial value]

mls qos enable

[Input mode]

global configuration mode

[Description]

Enables QoS.

If this command 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.

```
SWP1(config)#mls qos enable
```

Disable QoS.

```
SWP1(config)#no mls qos
```

13.2.2 Set default CoS

[Syntax]

mls qos cos *value*
no mls qos cos

[Parameter]

value : <0-7>
Default CoS value

[Initial value]

mls qos cos 0

[Input mode]

interface mode

[Description]

Sets the default CoS.

If this command 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 port's trust mode is set to CoS. (Since CoS is not specified for the frame)

[Note]

In order to execute this command, CoS must be enabled.

If this is executed for a port whose trust mode is DSCP, the command results in an execution error.

[Example]

Set the default CoS value to 2.

```
SWP1(config-if)#mls qos cos 2
```

Return the default CoS value to the default value.

```
SWP1(config-if)#no mls qos cos
```

13.2.3 Set trust mode

[Syntax]

mls qos trust *mode*
no mls 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]

mls qos trust cos

[Input mode]

interface mode

[Description]

pecifies the trust mode of the LAN/SFP port.

If this command 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 port 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	**mls qos cos-queue**
DSCP	DSCP - egress queue ID conversion table	**mls qos dscp-queue**
Port Priority	Priority specified for each receiving port	**mls 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 the LAN/SFP port, the trust mode cannot be changed.

Some QoS functions have limitations on execution depending on the trust mode, or may show different results.

[Example]

Set the trust mode of the LAN/SFP port to DSCP

```
SWP1(config-if)#mls qos trust dscp
```

Set the trust mode of the LAN/SFP port to the default setting (CoS).

```
SWP1(config-if)#no mls qos trust

or

SWP1(config-if)#mls qos trust cos
```

13.2.4 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 the LAN/SFP port 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 command 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 a LAN/SFP port, 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP1(config-pmap-c)#remark-map yellow ip-dscp 10
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.5 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.

If this command is executed with the "no" syntax, the policy map is deleted from the LAN/SFP port.

[Note]

In order to execute this command, QoS must be enabled.

If a policy map has already been applied to the LAN/SFP port, 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. 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

Trust mode	Command	Restrictions
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.

[Example]

Apply policy map "policy1" to LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

Remove policy map "policy1" from LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#no service-policy input policy1
```

13.2.6 Show status of QoS function setting

[Syntax]

show mls 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.

```
SWP1#show mls qos
  Enable
```

13.2.7 Show QoS information for LAN/SFP port

[Syntax]

show mls qos interface [*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 QoS settings for the specified LAN/SFP port. The following content is shown.

Item	Description
Port Trust Mode	Trust mode of LAN/SFP port (CoS/DSCP/Port-Priority)
Input Policy-Map Name	Name of policy map already applied to the LAN/SFP port and 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)

Item	Description
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)

```
SWP1#show mls qos interface ge1

  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)

```
SWP1#show mls qos interface ge1

  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
```

13.2.8 Show egress queue usage ratio

[Syntax]

show mls 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.

```
SWP1#show mls qos queue-counters ge1
QoS: Enable
Interface ge1 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 %
```

13.2.9 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.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show information for policy map "policy1."

```
SWP1#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)
```

13.2.10 Show map status

[Syntax]

show mls qos map-status *type* [*name*]

[Parameter]

type : Type of map to show

Setting value	Description
policy	Show policy map status information
class	Show policy class status information

name : The name of the policy map (or class map) to show. If this is omitted, all policy maps (or class maps) are shown.

[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 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 to which the policy map is applied ポ
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 association	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."

```
SWP1#show mls qos map-status policy policy1
policy1 status
  input port            : ge3

  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."

```
SWP1#show mls 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
```

13.2.11 Set CoS - egress queue ID conversion table

[Syntax]

mls qos cos-queue *cos-value queue-id*
no mls qos cos-queue

[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 command 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, CoS 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."

```
SWP1(config)#mls qos cos-queue 0 4
```

Return the egress queue ID of CoS value "0" to the default value.

```
SWP1(config)#no mls qos cos-queue 0
```

13.2.12 Set DSCP - egress queue ID conversion tabl

[Syntax]

mls qos dscp-queue *dscp-value queue-id*
no mls 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 command 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."

```
SWP1(config)#mls qos dscp-queue 0 4
```

Return the egress queue ID of DSCP value "23" to the default value.

```
SWP1(config)#no mls qos dscp-queue 23
```

13.2.13 Set port priority order

[Syntax]

mls qos port-priority-queue *queue-id*
no mls qos port-priority-queue

[Parameter]

queue-id : <0-7>

Egress queue ID assigned to LAN/SFP port

[Initial value]

mls qos port-priority-queue 2

[Input mode]

interface mode

[Description]

Specifies the priority (egress queue ID) for the receiving port.

nIf this command is executed with the "no" syntax, the egress queue ID for the specified port 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 a port whose trust mode is not "port priority," the command results in an execution error.

[Example]

Assign egress queue ID #4 as the port priority for LAN port #1.

```
SWP1#interface ge1
SWP1(config-if)#mls qos port-priority-queue 4
```

13.2.14 Specify egress queue of frames transmitted from the switch itself

[Syntax]

mls qos queue sent-from-cpu *queue-id*
no mls qos queue sent-from-cpu

[Parameter]

queue-id : <0-7>
Egress queue ID

[Initial value]

mls 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 command 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.

```
SWP1(config)#mls qos queue sent-from-cpu 5
```

13.2.15 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.

- 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 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 the LAN/SFP port, then the class map that is associated with the policy map cannot be edited or deleted.

[Example]

Create class map "class1."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#
```

13.2.16 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 a LAN/SFP port 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP1(config-pmap-c)#remark-map yellow ip-dscp 10
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.17 Set traffic classification conditions (access-group)

[Syntax]

match access-group *acl-id*
match access-group *name*
no match access-group *acl-id*
no match access-group *name*

[Parameter]

acl-id	:	<1 - 99>
		Standard IPv4 access list ID
	:	<100 - 199>
		Extended IPv4 access list ID
	:	<1300 - 1999>
		Standard IPv4 access list ID
	:	<2000 - 2699>
		Extended IPv4 access list ID or MAC access list ID
	:	<3000 - 3699>
		IPv6 access list ID
name	:	Access list name

[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 command 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.

[Example]

Specify access list #1 as the classification conditions for class map "class1."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
```

13.2.18 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 command 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."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#match cos 1 2
```

13.2.19 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 command 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."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#match ip-precedence 3 4
```

13.2.20 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 command 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."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#match ip-dscp 48 56
```

13.2.21 Set traffic classification conditions (Ethernet Type)

[Syntax]

match ethertype *type*
no match ethertype

[Parameter]

type : 0xXXXX

Specifies the type value of the Ethernet frame in hexadecimal.

[Input mode]

class map mode

[Description]

Uses the Ethernet frame's type value as the condition to classify the traffic class.

If this command is executed with the "no" syntax, the condition setting using the Ethernet frame's type value is deleted.

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.

[Example]

Set Ethernet frame type value "0x0800" as the classification condition for class map "class1."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#match ethertype 0x0800
```

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 command 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."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#match vlan 20
```

13.2.23 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."

```
SWP1(config)#class-map class1
SWP1(config-cmap)#match vlan-range 20 to 30
```

13.2.24 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)	QoS-Access-List Name	Access list name
	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

Section	Item		Description
Pre-marking setting, egress queue setting (set)	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		Change egress queue (DSCP)
Metering/policing/remarking setting (police/remark-map)	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		ction for bandwidth class Red (drop/ remark)

- Of the various items in the "match" section and the "set" section, only the single item that has been specified for each section is shown.
- Regardless of the section, the section is 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 class map "class1."

```
SWP1#show class-map class1

    Class-Map Name: class1
      Match vlan 10
      Set CoS: 4
      Police: Mode: SrTCM
              average rate (48 Kbits/sec)
              burst size (12 KBytes)
              excess burst size (12 KBytes)
              yellow-action (Remark [CoS:2])
              red-action (Drop)
```

13.2.25 Generate standard IPv4 access list

[Syntax]

ip-access-list *list-id action src-info*
ip-access-list standard *name action src-info*
no ip-access-list *list-id action src-info*
no ip-access-list standard *name action src-info*

[Parameter]

list-id : <1 - 99>|<1300 - 1999>

Standard IPv4 access list ID

name : Name of access list (Maximum 32 characters; uppercase and lowercase are distinguished. You cannot specify a text string consisting only of numerals.)

action : Action for the access condition

Setting value	Description
deny	Specifies "deny" as the action for the access condition
permit	Specifies "permit" as the action for the access condition

src-info : Transmission-source IPv4 address that is the condition

Setting value	Description
A.B.C.D E.F.G.H	Specifies the condition as an IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)
any	Don't specify the transmission-source IPv4 address (accept all IPv4 address)

[Input mode]

global configuration mode

[Description]

Generates a standard IPv4 access list.

When generating a list, you can either specify a defined ID or assign a desired name.

If you want to apply this to traffic classification conditions, execute the **match access-group** command in class map mode.

For a single ID, you can repeat this to make up to 30 registrations.

[Note]

In order to execute this command, QoS must be enabled.

An error occurs if the maximum number of registrations is exceeded, or if you specify content that is already registered.

[Example]

Create a standard IPv4 access list #2 which permits packets from 192.168.1.0/24 through 192.168.2.0/24

```
SWP1(config)#ip-access-list 2 permit 192.168.1.0 0.0.0.255
SWP1(config)#ip-access-list 2 permit 192.168.2.0 0.0.0.255
```

Create a standard IP access list "TEST" which permits packets from 192.168.1.0/24 through 192.168.2.0/24

```
SWP1(config)#ip-access-list standard TEST permit 192.168.1.0 0.0.0.255
SWP1(config)#ip-access-list standard TEST permit 192.168.2.0 0.0.0.255
```

Delete 192.168.1.0/24 from standard IPv4 access list #2

```
SWP1(config)#no ip-access-list 2 permit 192.168.1.0 0.0.0.255
```

Delete 192.168.1.0/24 from standard IP access list "TEST"

```
SWP1(config)#no ip-access-list standard TEST permit 192.168.1.0 0.0.0.255
```

13.2.26 Generate extended IPv4 access list

[Syntax]

ip-access-list *list-id action protocol src-info dst-info*
ip-access-list extended *name action protocol src-info dst-info*
no ip-access-list *list-id action protocol src-info dst-info*
no ip-access-list extended *name action protocol src-info dst-info*

[Parameter]

list-id : <100 - 199>|<2000 - 2699>

Extended IPv4 access list ID

name : Name of access list (Maximum 32 characters; uppercase and lowercase are distinguished. You cannot specify a text string consisting only of numerals.)

action : Action for the access condition

Setting value	Description
deny	Specifies "deny" as the action for the access condition
permit	Specifies "permit" as the action for the access condition

protocol : 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 : Transmission-source IPv4 address that is the condition

Setting value	Description
A.B.C.D E.F.G.H	Specifies the condition as an IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)
any	Don't specify the transmission-source IPv4 address (accept all IPv4 address)

dst-info : Transmission-destination IPv4 address that will be the condition

The method of specifying this is the same as when specifying the transmission-source IPv4 address (*src-info*)

[Input mode]

global configuration mode

[Description]

Generates an extended IPv4 access list.

An extended IPv4 access list is useful when you want to filter with more detail (specific protocols + destination information) than the standard IPv4 access list.

When generating a list, you can either specify a defined ID or assign a desired name.

If you want to apply this to traffic classification conditions, execute the **match access-group** command in class map mode.

For a single ID, you can repeat this to make up to 30 registrations.

[Note]

In order to execute this command, QoS must be enabled.

An error occurs if the maximum number of registrations is exceeded, or if you specify content that is already registered.

The extended IPv4 access list IDs are shared with the MAC access list IDs. An error occurs if you use an ID that is specified for a MAC access list.

[Example]

Create extended IPv4 access list #100 which permits traffic from the transmission-source 192.168.1.0/24 segment and 192.168.2.0/24 segment to 10.1.1.1

```
SWP1(config)#ip-access-list 100 permit any 192.168.1.0 0.0.0.255 host 10.1.1.1
SWP1(config)#ip-access-list 100 permit any 192.168.2.0 0.0.0.255 host 10.1.1.1
```

Create extended IP access list "TEST" which permits traffic from the 192.168.1.0/24 segment and 192.168.2.0/24 segment to 10.1.1.1

```
SWP1(config)#ip-access-list extended TEST permit any 192.168.1.0 0.0.0.255 host
10.1.1.1
SWP1(config)#ip-access-list extended TEST permit any 192.168.2.0 0.0.0.255 host
10.1.1.1
```

Delete the transmission-source 192.168.1.0/24 from extended IPv4 access list #100

```
SWP1(config)#no ip-access-list 100 permit any 192.168.1.0 0.0.0.255 host 10.1.1.1
```

Delete the transmission-source 192.168.1.0/24 from extended IPv4 access list "TEST"

```
SWP1(config)#no ip-access-list extended TEST permit any 192.168.1.0 0.0.0.255 host
10.1.1.1
```

13.2.27 Generate IPv6 access list

[Syntax]

ip-access-list *list-id action src-info*
ip-access-list ipv6 *name action src-info*
no ip-access-list *list-id action src-info*
no ip-access-list ipv6 *name action src-info*

[Parameter]

list-id : <3000 - 3699>

IPv6 access list ID

name : Name of access list (Maximum 32 characters; uppercase and lowercase are distinguished. You cannot specify a text string consisting only of numerals.)

action : Action for the access condition

Setting value	Description
deny	Specifies "deny" as the action for the access condition
permit	Specifies "permit" as the action for the access condition

src-info : 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	Don't specify the transmission-source IPv6 address (accept all IPv6 address)

[Input mode]

global configuration mode

[Description]

Generates an IPv6 access list.

When generating a list, you can either specify a defined ID or assign a desired name.

If you want to apply this to traffic classification conditions, execute the **match access-group** command in class map mode.

For a single ID, you can repeat this to make up to 30 registrations.

[Note]

In order to execute this command, QoS must be enabled.

An error occurs if the maximum number of registrations is exceeded, or if you specify content that is already registered.

[Example]

Create an IPv6 access list #3002 which permits packets from 3ffe:506::/32 through 3ffe:507::/32

```
SWP1(config)#ip-access-list 3002 permit 3ffe:506::/32
SWP1(config)#ip-access-list 3002 permit 3ffe:507::/32
```

Create an IPv6 access list "TEST" which permits packets from 3ffe:506::/32 through 3ffe:507::/32

```
SWP1(config)#ip-access-list ipv6 TEST permit 3ffe:506::/32
SWP1(config)#ip-access-list ipv6 TEST 3ffe:507::/32
```

Delete 3ffe:506::/32 from IPv6 access list #3002

```
SWP1(config)#no ip-access-list 3002 permit 3ffe:506::/32
```

Delete 3ffe:506::/32 from IPv6 access list "TEST"

```
SWP1(config)#no ip-access-list ipv6 TEST permit 3ffe:506::/32
```

13.2.28 Generate MAC access list

[Syntax]

mac-access-list *list-id action src-info dst-info*
no ip-access-list *list-id action src-info dst-info*

[Parameter]

list-id : <2000 - 2699>

MAC access list ID

action : Action for the access condition

Setting value	Description
deny	Specifies "deny" as the action for the access condition
permit	Specifies "permit" as the action for the access condition

src-info : Transmission-source MAC address that is the condition

Setting value	Description
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	Specify as a MAC address (HHHH.HHHH.HHHH) with wildcard bits (WWWW.WWWW.WWWW)
any	Don't specify the transmission-source MAC address (apply to all MAC addresses)

dst-info : Destination MAC address that is the condition

The method of specifying this is the same as when specifying the transmission-source MAC address (*src-info*)

[Input mode]

global configuration mode

[Description]

Generates a MAC access list.

If you want to apply this to traffic classification conditions, execute the **match access-group** command in class map mode.

For a single ID, you can repeat this to make up to 30 registrations.

[Note]

In order to execute this command, QoS must be enabled.

An error occurs if the maximum number of registrations is exceeded, or if you specify content that is already registered.

The MAC access list IDs are shared with the extended IPv4 access list IDs. An error occurs if you use an ID that is specified for the extended IPv4 access list.

[Example]

Create MAC access list #2000 which discards frames from MAC addresses 00-03-28-12-34-56 and 00-03-28-78-9A-BC.

```
SWP1(config)#mac-access-list 2000 deny 0003.2812.3456 0000.0000.0000 any
SWP1(config)#mac-access-list 2000 deny 0003.2878.9abc 0000.0000.0000 any
```

Delete MAC address 00-03-28-12-34-56 from MAC access list #2000.

```
SWP1(config)#no mac-access-list 2000 deny 0003.2812.3456 0000.0000.0000 any
```

13.2.29 Show QoS access list

[Syntax]

show qos-access-list *acl-id*
show qos-access-list *name*

[Parameter]

acl-id	:	<1 - 99>
		Standard IPv4 access list ID
	:	<100 - 199>
		Extended IPv4 access list ID
	:	<1300 - 1999>
		Standard IPv4 access list ID
	:	<2000 - 2699>
		Extended IPv4 access list ID or MAC access list ID
	:	<3000 - 3699>
		IPv6 access list ID
name	:	Access list name

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Show QoS access list information.

If parameters are omitted, all QoS access lists are shown.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show information for standard IPv4 access list #2.

```
SWP1#show qos-access-list 2
Standard IP QoS access list: 2
    permit 192.168.1.0, wildcard bits 0.0.0.255
    permit 192.168.2.0, wildcard bits 0.0.0.255
```

Show information for all access lists.

```
SWP1#show qos-access-list

  Standard IP QoS access list: 2
    permit 192.168.1.0, wildcard bits 0.0.0.255
    permit 192.168.2.0, wildcard bits 0.0.0.255

  Extended IP QoS access list: 100
    permit any 192.168.1.0 0.0.0.255 host 10.1.1.1
    permit any 192.168.2.0 0.0.0.255 host 10.1.1.1

  MAC QoS access list: 2000
    deny   0003.2812.3456 0000.0000.0000 any
    deny   0003.2878.9ABC 0000.0000.0000 any

  IPv6 QoS access list: 3002
    permit 3ffe:506::/32
    permit 3ffe:507::/32
```

13.2.30 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#set cos 2
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.31 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit
```

```
[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#set ip-precedence 5
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.32 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	12, 14, 18, 20, 22, 26, 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#set ip-dscp 10
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.33 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 SWP1 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP1(config-pmap-c)#remark-map yellow ip-dscp 10
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
```

```
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.34 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 SWP1 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#police twin-rate 48 96 12 12 yellow-action remark red-action drop
SWP1(config-pmap-c)#remark-map yellow ip-dscp 10
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.35 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 command 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 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP1(config-pmap-c)#remark-map yellow ip-dscp 10
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.36 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 the 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 the LAN/SFP port

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"

```
SWP1(config)#aggregate-police AGP-01
SWP1(config-agg-policer)#
```

13.2.37 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 SWP1 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]
SWP1(config)#aggregate-police AGP-01
SWP1(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-action
drop
SWP1(config-agg-policer)#remark-map yellow ip-dscp 10
SWP1(config-agg-policer)#exit
```

13.2.38 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 policer

[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 : peration 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 SWP1 is implemented as a twin-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, CBS:12kbyte, and EBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

```
[Aggregate policer creating]
SWP1(config)#aggregate-police AGP-01
SWP1(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWP1(config-agg-policer)#remark-map yellow ip-dscp 10
SWP1(config-agg-policer)#exit
```

13.2.39 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 command 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 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 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]
SWP1(config)#aggregate-police AGP-01
SWP1(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWP1(config-agg-policer)#remark-map yellow ip-dscp 10
SWP1(config-agg-policer)#exit
```

13.2.40 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."

```
SWP1#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)
```

13.2.41 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]
SWP1(config)#aggregate-police AGP-01
SWP1(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-action
drop
SWP1(config-agg-policer)#remark-map yellow ip-dscp 10
SWP1(config-agg-policer)#exit

[Set policy]
SWP1(config)#policy-map policy1
```

```
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#police-aggregate AGP-01
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#class class2
SWP1(config-pmap-c)#police-aggregate AGP-01
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.42 Show metering counters

[Syntax]

show mls qos metering-counters [*ifname*]

[Parameter]

ifname : LAN/SFP port 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.

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.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the metering totals for LAN port #1.

```
SWP1#show mls qos metering-counters ge1
Interface: ge1(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
```

13.2.43 Clear metering counters

[Syntax]

clear mls qos metering-counters [*ifname*]

[Parameter]

ifname : LAN/SFP port name. If this is omitted, the command applies to all ports.

[Input mode]

unprivileged EXEC mode、priviledged EXEC mode

[Description]

Clears the metering totals for all policers (individual policers / aggregate policers) on the specified LAN/SFP port.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Clear the metering totals for LAN port #1.

```
SWP1#clear mls qos metering-counter ge1
```

13.2.44 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#set cos-queue 3
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.45 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]
SWP1(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP1(config)#class-map class1
SWP1(config-cmap)#match access-group 1
SWP1(config-cmap)#exit

[Policy settings]
SWP1(config)#policy-map policy1
SWP1(config-pmap)#class class1
SWP1(config-pmap-c)#set ip-dscp-queue 24
SWP1(config-pmap-c)#exit
SWP1(config-pmap)#exit
SWP1(config)#interface ge1
SWP1(config-if)#service-policy input policy1
```

13.2.46 Set egress queue scheduling

[Syntax]

mls qos wrr-weight *queue-id weight*
no mls qos wrr-weight *queue-id*

[Parameter]

queue-id	:	<0-7>
		Egress queue ID
weight	:	<1-32>
		Weight of WRR

[Initial value]

no mls qos wrr-weight 0

no mls qos wrr-weight 1

no mls qos wrr-weight 2

no mls qos wrr-weight 3

no mls qos wrr-weight 4

no mls qos wrr-weight 5

no mls qos wrr-weight 6

no mls 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 port ports.

If this command 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).

```
SWP1(config)#no mls qos wrr-weight 7
SWP1(config)#no mls qos wrr-weight 6
SWP1(config)#mls qos wrr-weight 5 5
SWP1(config)#mls qos wrr-weight 4 5
SWP1(config)#mls qos wrr-weight 3 5
SWP1(config)#mls qos wrr-weight 2 2
SWP1(config)#mls qos wrr-weight 1 1
SWP1(config)#mls qos wrr-weight 0 1
```

13.2.47 Set traffic shaping (individual port)

[Syntax]

traffic-shape rate kbps *CIR* **burst** *BC*
no traffic-shape rate

[Parameter]

CIR : <18-1000000>

Traffic rate (kbps). Since rounding occurs, the value actually applied to the input value might be less (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 command is executed with the "no" syntax, the port shaping setting is disabled.

[Note]

In order to execute this command, QoS must be enabled.

Since rounding occurs on the traffic rate, the value actually applied to the input value might be less.

Input value	Traffic rate granularity (kbps)
18 - 23476	17.28
23477 - 1000000	261

[Example]

Reduce transmission from LAN port #1 down to CIR:30016 kbps, Bc:1876000 byte.

```
SWP1#interface ge1
SWP1(config-if)#traffic-shape rate kbps 30016 burst 1876
```

13.2.48 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> ID of egress queue
CIR	:	<18-1000000> Traffic rate (kbps). Since rounding occurs, the value actually applied to the input value might be less (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 command is executed with the "no" syntax, the egress queue shaping setting is disabled.

[Note]

In order to execute this command, QoS must be enabled.

Since rounding occurs on the traffic rate, the value actually applied to the input value might be less.

Input value	Traffic rate granularity (kbps).
18 - 23476	17.28
23477 - 1000000	261

[Example]

Reduce transmission from queue #0 of LAN port #1 down to CIR:10 Mbps and Bc:64000 byte.

```
SWP1#interface ge1
SWP1(config-if)#traffic-shape queue 0 rate kbps 10000 burst 64
```

13.3 Flow control

13.3.1 Set flow control (IEEE 802.3x PAUSE send/receive) (system)

[Syntax]

flowcontrol enable
no flowcontrol

[Initial value]

no flowcontrol

[Input mode]

global configuration mode

[Description]

Enables flow control for the entire system (IEEE 802.3x PAUSE frames send/receive).

If this command 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.

Flow control for each interface operates only if the flow control settings of the system and of the interface are each enabled.

If flow control is enabled, the tail drop function is automatically disabled.

[Example]

Enable flow control for system.

```
SWP1(config)#flowcontrol enable
```

13.3.2 Set flow control (IEEE 802.3x PAUSE send/receive) (interface)

[Syntax]

flowcontrol *type*
no flowcontrol

[Parameter]

type : Flow control operation

Setting value	Description
enable	Enable flow control auto negotiation
auto	Enable flow control auto negotiation
both	Enable transmission/reception of Pause frames

[Initial value]

no flowcontrol

[Input mode]

interface mode

[Description]

Enables flow control for the LAN/SFP port (IEEE 802.3x PAUSE frames send/receive).

If this 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 SWP1 transmits a PAUSE frame is 0xFFFF (65535).

[Example]

Enable flow control for LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#flowcontrol enable
```

Disable flow control for LAN port #1.

```
SWP1(config)#interface ge1
SWP1(config-if)#no flowcontrol
```

13.3.3 Set flow control threshold (start/cancel control)

[Syntax]

flowcontrol threshold pause *pause-rate* **cancel** *cancel-rate*
no flowcontrol threshold

[Parameter]

pause-rate : <1-100>

Specifies the threshold value at which control will start, as a percentage (1% - 100%) of the buffer usage. The threshold value for starting control must be higher than the threshold value for canceling control.

cancel-rate : <1-100>

Specifies the threshold value at which control is canceled, as a percentage (1% - 100%) of the buffer usage.

[Initial value]

flow control threshold pause 80 cancel 60

[Input mode]

global configuration mode

[Description]

Flow control threshold values are specified with the system as the unit.

If this command is executed with the "no" syntax, the threshold value for starting control and the threshold value for canceling control are returned to their default settings.

[Note]

These settings apply to every LAN/SFP port for which flow control is enabled.

[Example]

Set the flow control threshold values to pause = 75, cancel = 50.

```
SWP1(config)#flowcontrol threshold pause 75 cancel 50
```

Reset the flow control threshold values to their default values.

```
SWP1(config)#no flowcontrol threshold
```

13.3.4 Show flow control operating status

[Syntax]

show flowcontrol [inteface *ifname*]

[Keyword]

interface : Specifies the interface to show

[Parameter]

ifname : Name of the 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, threshold values for starting and ending control, number of PAUSE frames sent/received).

[Note]

The control start/end threshold values and 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.

```
SWP1#show flowcontrol ge1
Port    FlowControl    Pause Threshold Cancel Threshold    RxPause TxPause
-----   -----------    --------------- ----------------    ------- -------
ge1     Enable                      80               60       4337       0
```

Show flow control information for all ports

```
SWP1#show flowcontrol
System flow-control: Enable
Port    FlowControl    Pause Threshold Cancel Threshold    RxPause TxPause
```

```
-----   -----------    --------------- ----------------    ------- -------
ge1     Enable                    80                60       4337       0
ge2     Disable                    -                 -          -       -
ge3     Enable                    80                60          0    1732
ge4     Disable                    -                 -          -       -
ge5     Disable                    -                 -          -       -
ge6     Disable                    -                 -          -       -
ge7     Disable                    -                 -          -       -
ge8     Disable                    -                 -          -       -
ge9     Disable                    -                 -          -       -
```

13.4 Storm control

13.4.1 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%.

```
SWP1(config)#interface ge1
SWP1(config-if)#storm-control broadcast multicast level 30
```

13.4.2 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.

```
SWP1#show storm-control
Port    BcastLevel    McastLevel    UcastLevel
ge1       30.00%        30.00%       100.00%
ge2       20.00%        20.00%        20.00%
ge3      100.00%       100.00%       100.00%
ge4      100.00%       100.00%       100.00%
ge5       50.00%        50.00%       100.00%
ge6      100.00%       100.00%       100.00%
ge7      100.00%       100.00%        30.00%
ge8      100.00%       100.00%        30.00%
ge9      100.00%       100.00%       100.00%
```

Index

M

N

P

R

S

T

V

W