Yamaha L2 Switch

Smart L2 SWX2210P Series

Command Reference

Rev.1.03.13

Contents

Preface

Introduction

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

Chapter 1

How to read the command reference

1.1 Applicable firmware revision

This command reference applies to firmware Yamaha Smart L2 PoE Switch SWX2210P of Rev.1.03.13.
For the latest firmware released after printing of this command reference, manuals, and items that differ, access the following URL and see the information in the WWW server.
https://www.yamaha.com/proaudio/

1.2 How to read the command reference

This command reference describes the commands that you enter from the console of the Yamaha Smart L2 PoE Switch SWX2210P.

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]	Shows the setting value when then command is not shown in the configuration file.
[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 SWX2210P.

Interface type	Prefix	Description	Examples
LAN port	port	Used to specify a physical port. Specify "1" + "." + "port number" after the port number.	When specifying LAN port #1: port1.1
VLAN interface	vlan	Used to specify a VLAN. Specify vlan followed by the "VLAN ID".	To specify VLAN #1: vlan1

Interface type	Prefix	Description	Examples
static logical interface	sa	Used to specify link aggregation that combines multiple LAN port. Specify sa followed by "logical interface ID".	To specify static logical interface #1: sa1

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 SWX2210P lets you perform command operations in the following two ways.

Type of operation	Method of operation	Description
Operation via console	• 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 SWX2210P, in a single operation.

This chapter explains how to use each method.

2.1 Operation via console

2.1.1 Access from a TELNET client

You can use a TELNET client on a computer to connect to the TELNET server of the SWX2210P 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 SWX2210P are as follows.

- The default IPv4 address setting is 192.168.100.240/24 for VLAN #1.
- To change the IPv4 address, use the **ip address** command.

The TELNET server settings of the SWX2210P 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 all hosts.
- To change the reception port number, use the **telnet-server** command.
- Access to the TELNET server can be controlled for each host, and can be specified by the **telnet-server access** command. Specify an IPv4/IPv6 address for hosts to which access is permitted.

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 SWX2210P. The VTY ports of the SWX2210P are as follows.

- With the default VTY port settings, four VTY ports (ID: 0--3) can be used.
- To change the number of VTY ports, use the **line vty** command. (maximum 4 (ID: 0--3))

To make VTY port settings, use the **line vty** command to specify the target VTY port, and then move to line mode. The VTY port settings are common to all VTY ports.

2.1.2 VTY settings

The SWX2210P lets you make the following settings for VTY.

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

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

Setting item	Content of setting
Number of lines shown in one page of the terminal screen	Specifies the number of lines shown on one page of the terminal screen. This can be set as 0--512 lines/page, and the default setting is 24 lines/page. When displaying in this state, 24 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 SWX2210P 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 SWX2210P 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 SWX2210P are as follows.

- The default IPv4 address setting is 192.168.100.240/24 for VLAN #1.
- To change the IPv4 address, use the **ip address** command or the **ip address dhcp** command.

The TFTP server settings of the SWX2210P are as follows.

- The default setting for the TFTP server function is "disabled".
- Specify the **tftp-server** command when using the TFTP server function. The default port is UDP port #69.
- Access to the TFTP server can be controlled in units of hosts, and can be specified by the **tftp-server access** command. Specify an IPv4/IPv6 address for the permitted host.

2.2.2 Reading/writing a configuration file

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

The following configuration files are read or written.

- configuration file

Applicable configuration file	Description	Notes
running-config	Setting values for current operation	
startup-config #0	Saved setting values #0	

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

- IP addresses of the SWX2210P
- 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 configuration file	Load (GET)	Save (PUT)	Remarks
config	running-config	✓	✓	
config0	startup-config #0	✓	✓	
reconfig	startup-config #0	-	✓	Automatically reboots after config PUT (write).
techinfo	tech-support	✓	-	

- You must specify the administrator password after the remote path in the format "/PASSWORD". When the admin password is in the default state, you cannot read/write configuration files. The admin password must be changed first.
- If you PUT (write) with "config" specified as the remote path, the changes are added or overwritten to the current operating settings. Settings that you do not add or change will remain as the current operating settings. Since the setting values are not saved, you must use the **write** command etc. if you want to save them.
- If you want to start operation with a completely new configuration 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 (**enable password 8** command format) is not applied to the settings even if it is PUT to running-config via TFTP. And, users are not actually registered when making settings for users that include encrypted passwords (**username** command).
- If "techinfo" is specified as the remote path, you can obtain a text file with the same contents as when you execute **show tech-support**.

2.3 Login

The login screen is shown when you access SWX2210P via TELNET.

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

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

- Login screen

```
Username: admin
Password: *****
```

- Console screen following login

```
SWX2210P-10G Rev.1.03.13 (Wed Sep  4 08:33:10 2024)
  Copyright (c) 2018-2024 Yamaha Corporation. All Rights Reserved.

SWX2210P>
```

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

- Password change screen

```
Username: admin
Password: *****

SWX2210P-10G Rev.1.03.13 (Wed Sep  4 08:33:10 2024)
  Copyright (c) 2018-2024 Yamaha Corporation. All Rights Reserved.

Please change the default password for admin.
New Password: *****
New Password(Confirm): *****
Building configuration...
[OK]
```

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

- Login restriction screen

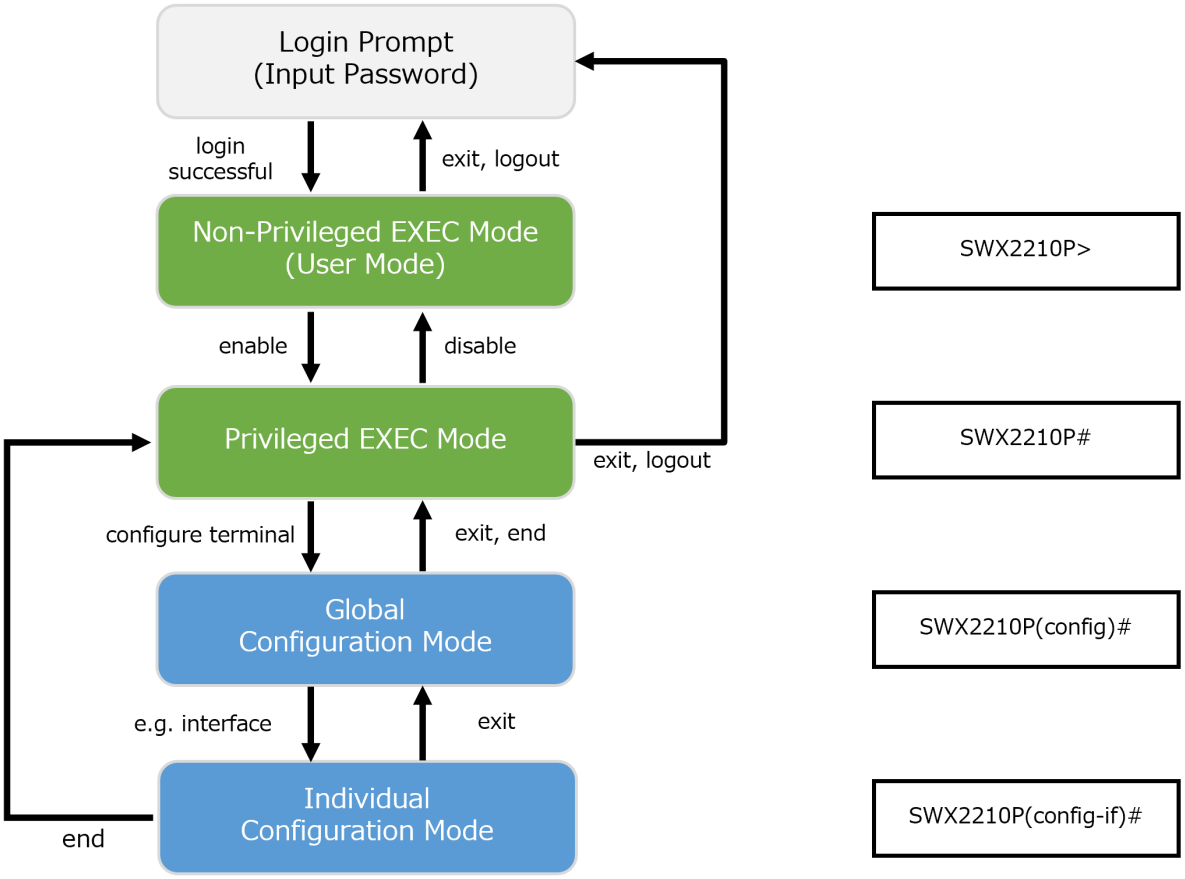
```
Username: user
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or blocked upon 3 failed login attempts for user.
% Please try again later.
```

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

2.4 Command input mode

2.4.1 Command input mode basics

In order to change the settings of the SWX2210P or to reference the status, you must move to the appropriate command input mode and then execute the command. Command input mode is divided into hierarchical levels as shown below, and the commands that can be entered in each mode are different. By noting the prompt, the user can see which mode they are currently in.



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

- **exit** command
- **logout** command
- **enable** command
- **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 port and VLAN interface. To enter individual configuration mode, issue the command for transitioning to the respective mode from global configuration mode.

On SWX2210P, individual configuration mode contains the following modes. Some of the modes within individual configuration mode have a hierarchy.

individual configuration mode	Transition command	Prompt
interface mode	**interface** command	SWX2210P(config-if)#
line mode	**line vty** command	SWX2210P(config-line)#
VLAN mode	**vlan database** command	SWX2210P(config-vlan)#

individual configuration mode	Transition command	Prompt
LLDP agent mode	**lldp-agent** command	SWX2210P(lldp-agent)#
L2MS mode	**l2ms configuration** command	SWX2210P(config-l2ms)#
Schedule template mode	**schedule template** command	SWX2210P(config-schedule)#

2.4.3 Command prompt prefix

he command prompt prefix indicates the host name. In the default state, the host name is the model name "SWX2210P". This indication can be changed by using the **hostname** command to specify the host name. In cases where multiple SWX2210P units are used, management will be easier if separate names are assigned to each switch.

Changing the host name

```
SWX2210P(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 SWX2210P 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 privileged 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 privileged 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

  ```
  SWX2210P(config)#do show vlan brief
  ```
- Entry in abbreviated form

  ```
  SWX2210P(config)#do sh vl br
  ```

2.5 Keyboard operations when using the console

2.5.1 Basic operations for console input

The SWX2210P allows the following operations in the command line.

- Moving the cursor

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

- Deleting an input character

Keyboard operation	Description and notes
Backspace	Delete the character at the left of the cursor
Ctrl + H	
Ctrl + D	Delete the character at the cursor. If this operation is performed when the command line is empty, the result is the same as the **exit** command.

Keyboard operation	Description and notes
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	Discard the command being entered and move to the next line, or abort the currently executed command process. (ex: **ping** command)
Ctrl + Z	Move from individual configuration mode and global configuration mode to privileged 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.

```
SWX2210P#show vlan ?
 <1-4094>      VLAN ID
 brief     VLAN information for all VLANs

SWX2210P#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

```
SWX2210P#con "press the <Tab>key"
       ↓
SWX2210P#configure
```

- Keyword candidate list display

```
SWX2210P(config)#mac-address-table "<Tab> key"
ageing-time learning    static
SWX2210P(config)#mac-address-table
```

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)

```
SWX2210P# 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 SWX2210P provides the following three modifiers for the **show** command.

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

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

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

```
SWX2210P#show running-config | grep vlan1
interface vlan1
```

- (Example) Show the login history with **show logging**.

```
SWX2210P# show logging | include Login
2018/09/20 09:51:53:[ SESSION]:inf: Login failed as (noname) for HTTP: 192.168.1.9
2018/09/20 09:52:03:[ SESSION]:inf: Login succeeded as (noname) for HTTP:
192.168.1.9
2018/09/20 09:57:15:[ SESSION]:inf: Login succeeded as (HttpProxyAdmin) for HTTP:
192.168.1.2
```

Chapter 3

Configuration

3.1 Manage setting values

The SWX2210P 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
Startup configuration (startup-config)	These are the saved setting values. Managed in ROM.	Note / Delete / Copy
Default configuration (default-config)	Default setting values. Managed in ROM.	No operations possible

The start-up flow for the SWX2210P system is as follows.

1. config#0 is selected for the startup config.
2. If the startup config exists, the data in question is deployed to RAM as a running configuration.
   If the startup config does not exist in ROM, the default configuration is deployed to RAM.

If commands etc. are used to modify the settings while the SWX2210P is running, the modified settings are immediately reflected in the running configuration. After modifying the running configuration, executing the **write** or **copy** command will update the startup 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 value

The default setting values for the SWX2210P are shown in the table below.

- Default setting values for the entire system

Category	Setting item	Default value
Terminal settings	Console timeout	600 sec
	Number of lines displayed	24 lines
User account	Default administrator	User name: admin, Password: admin
	Administrator password	admin
	Password encryption	not encrypted
Time management	Time zone	JST (UTC + 9.0H)
	NTP server	none
	NTP update cycle	none

Category	Setting item	Default value
Firmware update	Download URL	http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin (for the SWX2210P-10G) http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-18g.bin (for the SWX2210P-18G) http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-28g.bin (for the SWX2210P-28G)
	Allow revision-down	don't allow
	Timeout	300 sec
LLDP	Behavior	enabled
	Automatically set	enabled
SYSLOG	Debug level log output	OFF
	Information level log output	ON
	Error level log output	ON
	SYSLOG server	none
VLAN setting	LAN port	Associated with default VLAN (vlan1)
	IPv4 address	Grant 192.168.100.240/24 to default VLAN (vlan1)
	IPv6	disabled
	IGMP Snooping	disabled
	MLD Snooping	disabled
Access control	Telnet server status	run (port 23)
	Telnet server access	Permit access from all hosts
	TFTP server status	do not run
	HTTP server status	run (port 80)
	Secure HTTP server status	run (port 443)
	HTTP/HTTPS server access	Permit access from all hosts
	SNMP server status	run (port 161)
	SNMP server access	Permit access from all hosts
L2 switching	Automatic MAC address learning	enabled
	Automatic MAC address learning aging time	300 sec
	Proprietary loop detection	enabled
Interface control	MRU	1,522 Byte
	BPDU pass through	enabled
	EAP pass through	enabled
DNS cliant	Behavior	enabled
Traffic control	QoS	disabled
	Flow control (IEEE 802.3x)	disabled

- Default settings per LAN port

Category	**Setting item**	**Default value**
Common setting	Speed/duplex mode setting	auto
	Cross/straight automatic detection	enabled
	Port description	none
	EEE	disabled
	Port Mode	Access
	Associated VLAN ID	1 (default VLAN)
L2MS	L2MS	enabled
	L2MS filter	disabled
	non-L2MS filter	disabled
L2 switching	Proprietary loop detection	enabled
Traffic control	QoS trust mode	CoS
	Flow control (IEEE 802.3x)	disabled
	Storm control	disabled
PoE power supply	Power supply operation	enabled
LLDP agent	Transmit/Receive mode	transmit and receive

Chapter 4

Maintenance and operation functions

4.1 Passwords

4.1.1 Set administrator password

[Syntax]

enable password *password*

[Parameter]

password : Administrator password

Single-byte alphanumeric characters, " (quotation marks), ' (apostrophes), | (vertical bar), ? (question mark), > (greater than symbol) and single-byte symbols other than space characters (up to 32 characters)

[Initial value]

enable password admin

[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 **password-encryption** command, it is shown in the configuration in the form "**enable password** 8 *password*".

The user cannot enter the password in this format 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.

```
SWX2210P(config)#enable password admin1234
```

4.1.2 Encrypt password

[Syntax]

password-encryption *switch*
no password-encryption

[Parameter]

switch : Set password encryption

Setting value	Description
enable	encrypt
disable	don't encrypt

[Initial value]

password-encryption disable

[Input mode]

global configuration mode

[Description]

Enables password encryption.

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

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

[Note]

If password encryption is changed from disabled to enabled, previously-entered passwords are converted from plain text to an encrypted form. If password encryption is changed from enabled to disabled, previously-encrypted passwords in a configuration file do not return to plain text.

[Example]

Enables password encryption.

```
SWX2210P(config)#password-encryption enable
```

Disabled password encryption.

```
SWX2210P(config)#no password-encryption
```

4.2 User account maintenance

4.2.1 User settings

[Syntax]

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

[Keyword]

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

[Parameter]

username : User name

Up to 32 half-width alphanumeric characters

privilege : Whether or not privileges are granted

Setting value	Description
on	Users will not be prompted to enter a password when switching to privileged EXEC mode Access to web GUI is allowed with administrator privileges
off	Users will be prompted to enter a password when switching to privileged EXEC mode Web GUI can be accessed with guest permissions

password : User's login password

Single-byte alphanumeric characters, " (quotation marks), ' (apostrophes), | (vertical bar), ? (question mark), > (greater than symbol) and single-byte symbols other than space characters (up to 32 characters)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets user information.

A maximum of 33 items of user information can be registered. Note that "privilege off" users are limited to a maximum of 32 items, and "privilege on" users must have at least one item.

The following words cannot be registered as user names.

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

The default password ("admin") cannot be used as a password.

[Note]

If the **password-encryption** command is set, the password is encrypted and shown in the configuration in the format "**username** *username* 8 password *password*".

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

If there are no "privilege on" users set on startup, the default administrator password ("admin") is added.

Users who do not have a password set on startup will automatically be assigned a password that is the same length as the user name.

[Example]

Set the user "**user1234**".

```
SWX2210P(config)#username user1234 password user_pass
```

Set "**user1234**" as a privileged user.

```
SWX2210P(config)#username user1234 privilege on password user_pass
```

4.2.2 Show login user information

[Syntax]

show users

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information on the current logged-in users.

The following items are shown.

Item	Description
Type	Shows the login method. **vty N** is a VTY port **http N** is WebGUI
Own	An * is shown on the line of one's own connection port.
User	Shows the currently logged-in user names.
Status	Shows the login status. If the user is in use, **Login** is indicated.
Login time	Shows the login time.

[Example]

Show login information for the users.

```
SWX2210P>show users
Type    Own  User                                Status  Login time
-----------------------------------------------------------------
vty  0  *    operator_s1                         Login   00:12:59
vty  1       abcdefghijklmnopqrstuvwxyzabcdef    Login   00:00:50
vty  2       -                                   Login   00:00:21
vty  3       -                                   -       -
http 0       user_1234                           Login   01:12:25
http 1       guest_g1                            Login   00:43:21
```

```
http 2       -                                    Login   00:18:04
http 3       -                                    -       -

SWX2210P>
```

4.3 Configuration management

4.3.1 Save running configuration

[Syntax]

copy running-config startup-config

[Input mode]

privileged EXEC mode

[Description]

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

[Note]

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

[Example]

Save the running configuration.

```
SWX2210P#copy running-config startup-config
Building configuration...
[OK]
SWX2210P#
```

4.3.2 Save running configuration

[Syntax]

write

[Input mode]

privileged EXEC mode、global configuration mode、individual configuration mode

[Description]

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

[Note]

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

[Example]

Save the running configuration.

```
SWX2210P#write
Building configuration...
[OK]
SWX2210P#
```

4.3.3 Show running configuration

[Syntax]

show running-config [*section*]

[Parameter]

section : Section to be shown

Setting value	Description
interface	Interface related
switch vlan	VLAN related

[Input mode]

privileged EXEC mode、global configuration 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.

```
SWX2210P#show running-config
!
dns-client enable
!
loop-detect enable
...
!
http-server enable
http-server secure enable
!
telnet-server enable
!
end

SWX2210P#
```

4.3.4 Show startup configuration

[Syntax]

show startup-config

[Input mode]

privileged EXEC mode

[Description]

Shows the settings used at startup (startup configuration).

[Example]

Shows the startup configuration on the next startup.

```
SWX2210P#show startup-config
!
! Last Modified:  00:00:00 JST Thu Nov 01 2018
!
dns-client enable
!
loop-detect enable
...
!
http-server enable
http-server secure enable
!
telnet-server enable
!
end

SWX2210P#
```

4.3.5 Erase startup configuration

[Syntax]

erase startup-config

[Input mode]

privileged EXEC mode

[Description]

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

[Example]

Erase the startup configuration.

```
SWX2210P#erase startup-config
erasing...[OK]
SWX2210P#
```

4.4 Manage boot information

4.4.1 Show boot information

[Syntax]

show boot [*num*]
show boot all
show boot list

[Keyword]

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

[Parameter]

num	:	<0-4> Shows the boot history entry of the specified number (if this is omitted, boot history number 0 (current) is shown)

[Input mode]

unprivileged EXEC mode、privileged 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.

```
SWX2210P>show boot
 Running EXEC: SWX2210P-10G Rev.1.03.13 (Wed Sep  4 08:33:10 2024)
Previous EXEC: SWX2210P-10G Rev.1.03.13 (Wed Sep  4 08:33:10 2024)
Restart by reload command
```

Shows a list of the boot history.

```
SWX2210P>show boot list
No. Date       Time     Info
--- ---------- -------- ------------------------------------------------
  0 2018/09/15 09:50:29 Restart by reload command
  1 2018/09/14 20:24:40 Power-on boot
--- ---------- -------- ------------------------------------------------
```

4.4.2 Clear boot information

[Syntax]

clear boot list

[Input mode]

privileged EXEC mode

[Description]

Clears the boot information history.

[Example]

Clear the boot information.

```
SWX2210P#clear boot list
```

4.5 Show unit information

4.5.1 Show inventory information

[Syntax]

show inventory

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show the inventory information for this product.

The following items are shown.

Item	Explanation
NAME	Name
DESCR	Summary
Vendor	Vendor name
PID	Product ID
VID	Version ID ("0" if disabled)
SN	Serial number

[Example]

Show inventory information.

```
SWX2210P>show inventory
NAME: L2 PoE switch
DESCR: SWX2210P-10G
Vendor: Yamaha
PID: SWX2210P-10G
VID: 0000
SN: S00000000

SWX2210P>
```

4.5.2 Show operating information

[Syntax]

show environment

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows information about the system's operating environment.

The following items are shown.

- Boot version
- PoE version
- Firmware revision
- Serial number
- MAC address
- CPU usage
- Memory usage
- Fan operating status
- Fan speed
- RTC version
- Boot time
- Current time
- Elapsed time from boot
- Temperature status of this unit

- Temperature of this unit

[Example]

Show operating information.

```
SWX2210P>show environment
SWX2210P-10G BootROM Ver.1.03
SWX2210P-10G PoEROM Ver.1.8.0.3
SWX2210P-10G Rev.1.03.13 (Wed Sep  4 08:33:10 2024)
main=SWX2210P-10G ver=00 serial=S00000000 MAC-Address=aa44.f200.0000
CPU:   26%(5sec)   21%(1min)   21%(5min)    Memory:  40% used
Fan status: Normal
Fan speed: FAN1=2891RPM FAN2=3076RPM
RTC version: 1
Boot time: 2024/09/18 16:47:54 +09:00
Current time: 2024/09/19 17:14:56 +09:00
Elapsed time from boot: 1days 05:06:04
Temperature status: Normal
Temperature: 47 degree C

SWX2210P>
```

4.5.3 Show technical support information

[Syntax]

show tech-support

[Input mode]

privileged EXEC mode

[Description]

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

- show running-config
- show environment
- show inventory
- show boot all
- show logging
- show users
- show interface
- show frame-counter
- show vlan brief
- show loop-detect
- show mac-address-table
- show l2ms
- show qos queue-counters
- show ip igmp snooping groups
- show ip igmp snooping interface
- show ipv6 mld snooping groups
- show ipv6 mld snooping interface
- show power-inline

[Example]

Show technical support information.

```
SWX2210P#show tech-support
#
# Information for Yamaha Technical Support
#

*** show running-config ***
!
dns-client enable
!

...
```

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

SWX2210P#
```

4.6 Time management

4.6.1 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]

privileged EXEC mode

[Description]

Set the system time.

[Example]

Set the time to 0 hours 0 minutes 0 seconds on November 1, 2018.

```
SWX2210P#clock set 00:00:00 Nov 1 2018
```

4.6.2 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.

```
SWX2210P(config)#clock timezone JST
```

Set the time zone to UTC+9 hours.

```
SWX2210P(config)#clock timezone +9:00
```

4.6.3 Show current time

[Syntax]

show clock

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

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

[Example]

Show the current time.

```
SWX2210P>show clock
00:00:00 JST Thu Nov 1 2018
```

4.6.4 Set NTP server

[Syntax]

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

[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 When specifying an IPv6 link local address, the transmitting interface also needs to be specified (in fe80::X%vlanN format).
fqdn	:	Host name of the NTP server

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Registers the address or host name of the NTP server.

Up to two instances of this command can be set.

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

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

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

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

[Example]

Specify 192.168.1.1 as the NTP server.

```
SWX2210P(config)#ntpdate server ipv4 192.168.1.1
```

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

```
SWX2210P(config)#ntpdate server ipv6 fe80::2a0:deff:fe11:2233%vlan1
```

Sets the NTP server to "ntp.example.com".

```
SWX2210P(config)#ntpdate server name ntp.example.com
```

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

[Syntax]

ntpdate oneshot

[Input mode]

privileged 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.

```
SWX2210P#ntpdate oneshot
```

4.6.6 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 0

[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.

```
SWX2210P(config)#ntpdate interval 2
```

Disable periodic time synchronization.

```
SWX2210P(config)#ntpdate interval 0
```

4.6.7 Show NTP server time synchronization settings

[Syntax]

show ntpdate

[Input mode]

unprivileged EXEC mode、privileged 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

```
SWX2210P#show ntpdate
NTP Server 1 : ntp.nict.jp
NTP Server 2 : none
adjust time : Thu Nov 1 09:00:00 2018 + interval 1 hour
sync server : ntp.nict.jp
```

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

```
SWX2210P#show ntpdate
NTP Server 1 : ntp.nict.jp
NTP Server 2 : none
adjust time : Thu Nov 1 09:00:00 2018
sync server : ntp.nict.jp
```

4.7 Terminal settings

4.7.1 Set VTP port and move to line mode (VTY port)

[Syntax]

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

[Parameter]

port1	:	<0-3>
		VTY port number
port2	:	<0-3>
		Last VPY port number when specifying a range

[Initial value]

no line vty 0 3

[Input mode]

global configuration mode

[Description]

After enabling the specified VTY ports, switch to line mode to configure the VTY port settings.

If this command is executed with the "no" syntax, all VTY ports are returned to the default setting.

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.

When this command is executed, the unit switches to line mode and the VTY port settings are overwritten. For instance, when executing **line vty 1**, only the VTY port #1 is enabled, and other VTY ports are disabled.

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.

```
SWX2210P(config)#line vty 0
SWX2210P(config-line)#
```

4.7.2 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 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 timeout time for the VTY port #0 to 5 minutes.

```
SWX2210P(config)#line vty 0
SWX2210P(config-line)#exec-timeout 5 0
SWX2210P(config-line)#
```

4.7.3 Change 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、privileged 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 shown is 24 lines, the default value.

[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.

```
SWX2210P>terminal length 100
SWX2210P>
```

4.7.4 Set 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 default setting of 24 lines is set.

[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.

```
SWX2210P(config)#service terminal-length 100
SWX2210P(config)#
```

4.8 SYSLOG

4.8.1 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

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

[Initial value]

no logging host

[Input mode]

global configuration mode

[Description]

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

The maximum number of entries is 2.

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.

```
SWX2210P(config)#logging host 192.168.100.1
```

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

```
SWX2210P(config)#logging host fe80::2a0:deff:fe11:2233%vlan1
```

4.8.2 Set log notification format

[Syntax]

logging format *type*
no logging format

[Parameter]

type : Log format type

Setting value	Description
legacy	Unique format that does not include header section (timestamp, host name)

[Initial value]

no logging format

[Input mode]

global configuration mode

[Description]

Changes the format of the messages used to notify the SYSLOG server.

If the "no" syntax is executed, the header section (timestamp, host name) is included in the SYSLOG message.

[Example]

Sets the SYSLOG message format to be without a header.

```
SWX2210P(config)#logging format legacy
```

4.8.3 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.

```
SWX2210P(config)#logging trap debug
```

4.8.4 Set log output level (informational)

[Syntax]

logging trap informational
no logging trap informational

[Initial value]

logging trap informational

[Input mode]

global configuration mode

[Description]

Output 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 VTY by executing the **logging stdout info** command.

[Example]

Output the informational level log to SYSLOG.

```
SWX2210P(config)#logging trap informational
```

4.8.5 Set log output level (error)

[Syntax]

logging trap error
no logging trap error

[Initial value]

logging trap error

[Input mode]

global configuration mode

[Description]

Output 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.

```
SWX2210P(config)#logging trap error
```

4.8.6 Set Telnet console output for the log

[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 Telnet console.

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

[Example]

Output the informational level SYSLOG to the Telnet console.

```
SWX2210P(config)#logging stdout info
```

4.8.7 Back up log

[Syntax]

save logging

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Saves all logs accumulated in RAM to flash ROM.

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

[Example]

Back up the log.

```
SWX2210P#save logging
```

4.8.8 Clear log

[Syntax]

clear logging

[Input mode]

privileged EXEC mode

[Description]

Clear the log.

[Example]

Clear the log.

```
SWX2210P#clear logging
```

4.8.9 Show log

[Syntax]

show logging [reverse]

[Keyword]

reverse	:	Shows the log in reverse order

[Input mode]

unprivileged EXEC mode, privileged 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. If you want to save more than this maximum number of log entries, you must use the **logging host** command to send the log to the SYSLOG server and save the data on the host.

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

[Note]

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

The log is maintained when you reboot the system by executing the **reload** command or updating the firmware.

[Example]

Show the log.

```
SWX2210P#show logging
```

4.9 SNMP

4.9.1 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 or IPv6 address for notifications

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

type : Notification message

Setting value	Description
traps	Send notifications as traps (without response confirmation)
informs	Send notifications as inform requests (with response confirmation) Can only 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)

seclevel : Security level requested for authenticating the notification

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

Setting value	Description
priv	Authentication / Encryption (authPriv)

user : User name (maximum 32 characters)

Can be specified only if *version* is '3'

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Set the destination of SNMP notifications.

The maximum number of entries is 8.

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

[Note]

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

[Example]

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

```
SWX2210P(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.

```
SWX2210P(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, and set the user name to admin1.

```
SWX2210P(config)#snmp-server host 192.168.10.13 traps version 3 priv admin1
```

4.9.2 Set notification type to transmit

[Syntax]

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

[Keyword]

all : Enable/disable for all trap types

[Parameter]

trap_type : Type of trap

Setting value	Description
coldstart	During power off/on and firmware update
warmstart	When executing the "reload" command
linkdown	At linkdown
linkup	At linkup
authentication	When authentication fails
temperature	When temperature abnormality is detected or resolved
fan	When fan speed changes, or when fan stops
powerethernet	When a change in PoE status occurs
loopdetect	When a loop is detected/resolved

[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, the specified trap notification type is disabled.

[Example]

Enable coldstart trap.

```
SWX2210P(config)#snmp-server enable trap coldstart
```

Disable all traps.

```
SWX2210P(config)#no snmp-server enable trap all
```

4.9.3 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 swx2210padmin@sample.com.

```
SWX2210P(config)#snmp-server contact swx2210padmin@sample.com
```

4.9.4 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.

```
SWX2210P(config)#snmp-server location MainOffice-1F
```

4.9.5 Set SNMP community

[Syntax]

snmp-server community *community ro_rw*
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

[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.

[Example]

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

```
SWX2210P(config)#snmp-server community public ro
```

Delete the "public" community.

```
SWX2210P(config)#no snmp-server community public
```

4.9.6 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

Single-byte alphanumeric characters, and single-byte symbols other than " (quotation marks), ¥ (yen symbols) and ? (question marks); 32 characters or less

group : Group name

Setting value	Description
admin	A group for which authentication and encryption are always implemented, and for which read/write is allowed for all MIB views
guest	A group for which authentication and encryption are always implemented, and for which read is allowed for all MIB views

auth : Authentication algorithm

Setting value	Description
sha	HMAC-SHA-96

auth_pass : Authentication password

Single-byte alphanumeric characters, and single-byte symbols other than " (quotation marks), ¥ (yen symbols) and ? (question marks), 8–32 characters

priv : Encryption algorithm

Setting value	Description
aes	AES128-CFB

priv_pass : Encryption password

Single-byte alphanumeric characters, and single-byte symbols other than " (quotation marks), ¥ (yen symbols) and ? (question marks), 8–32 characters

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Specifies a user.

Either admin or guest can be specified for the group name of this command, and this specifies the algorithm and password that are used to authenticate and encrypt the communication data.

The communication data is always authenticated and encrypted.

One user each can be set for the user of the admin group with read/write permissions and the user of the guest group with read-only permissions.

The setting as to whether authentication and encryption are used, as well as 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 with read/write permissions. Specify the password (passwd1234) to use for authentication and encryption.

```
SWX2210P(config)#snmp-server user admin1 admin auth sha passwd1234 priv aes
passwd1234
```

Create "user1" as a user with read-only permissions. Specify the password (passwd5678) to use for authentication and encryption.

```
SWX2210P(config)#snmp-server user user1 guest auth sha passwd5678 priv aes passwd5678
```

4.9.7 Restrict access to the SNMP server according to the IP address of the client

[Syntax]

snmp-server access permit *info* [community *community*]
snmp-server access permit *info* [user *user*]
no snmp-server access permit [*info* [community *community*]]
no snmp-server access permit [*info* [user *user*]]

[Keyword]

community : Specifies the community

user : Specifies a user

[Parameter]

info : Specifies the transmission-source IPv4/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 (X:X::X:X) as the IPv6 address
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Specifies all IPv4/IPv6 addresses

community : Community name (maximum 32 characters)

Community to which access conditions are applied

If the community is not specified, the access conditions are applied to all communities.

user : User name (maximum 32 characters)

User to which access conditions are applied

If the user is not specified, the access conditions are applied to all users.

[Initial value]

None

[Input mode]

global configuration mode

[Description]

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

Up to 32 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 the community and user are omitted from the "no" syntax, all settings of the specified *info* are deleted.

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

If the IPv4/IPv6 address has changed, all settings are deleted.

[Example]

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

```
SWX2210P(config)#snmp-server access 192.168.100.0/24
```

Limit the hosts that can be accessed with the community name 'public' to only 192.168.100.0/24, and limit the hosts that can be accessed with the community name 'private' to only 192.168.100.12.

```
SWX2210P(config)#snmp-server access 192.168.100.0/24 community public
SWX2210P(config)#snmp-server access 192.168.100.12 community private
```

Limit the hosts that can be accessed with the community name 'admin1' to only 192.168.100.0/24, and limit the hosts that can be accessed with the community name 'user1' to only 192.168.100.12.

```
SWX2210P(config)#snmp-server access 192.168.100.0/24 user admin1
SWX2210P(config)#snmp-server access 192.168.100.12 user user1
```

4.9.8 Show SNMP community information

[Syntax]

show snmp community

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show SNMP community information.

Shows the community name and access mode.

[Example]

Show SNMP community information.

```
SWX2210P#show snmp community
SNMP Community information
  Community Name: public
  Access: Read-Only
  Community Name: private
  Access: Read-Write
```

4.9.9 Show SNMP user settings

[Syntax]

show snmp user

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the contents of the SNMP user settings.

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

[Example]

Shows the contents of the SNMP user settings.

```
SWX2210P#show snmp user
SNMP User information
  EngineID: 0x8000049e0300a0deaeb90e

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

  User Name: user1
  Group Name: guest
  Auth: sha
  Priv: aes
```

4.10 TELNET server

4.10.1 Start Telnet server and change listening port number

[Syntax]

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

[Keyword]

enable	:	Enable the Telnet server
disable	:	Disable the Telnet server

[Parameter]

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

[Initial value]

telnet-server disable

[Input mode]

global configuration mode

[Description]

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

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

[Example]

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

```
SWX2210P(config)#telnet-server enable 12345
```

4.10.2 Show Telnet server settings

[Syntax]

show telnet-server

[Input mode]

privileged EXEC mode

[Description]

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

- Telnet server function enabled/disabled
- Listening port number
- Filter that controls access to the TELNET server

[Example]

Show the settings of the Telnet server.

```
SWX2210P#show telnet-server
Service:Enable
Port:23
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

4.10.3 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/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 (X:X::X:X) as the IPv6 address
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Specifies all IPv4/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 parameters are omitted with the "no" syntax, all settings are deleted.

If the IPv4/IPv6 address has changed, all settings are deleted.

[Note]

If the "**telnet-server enable**" command is not specified, this command does not work.

[Example]

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

```
SWX2210P(config)#telnet-server access permit 192.168.1.1
SWX2210P(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.

```
SWX2210P(config)#telnet-server access deny 192.168.10.0/24
SWX2210P(config)#telnet-server access permit any
```

4.11 TFTP server

4.11.1 Start TFTP server and change listening port number

[Syntax]

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

[Keyword]

enable	:	Enable the TFTP server
disable	:	Disable the TFTP server

[Parameter]

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

[Initial value]

tftp-server disable

[Input mode]

global configuration mode

[Description]

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

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

[Example]

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

```
SWX2210P(config)#tftp-server enable 12345
```

4.11.2 Show TFTP server settings

[Syntax]

show tftp-server

[Input mode]

privileged EXEC mode

[Description]

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

- TFTP server function enabled/disabled
- Listening port number
- Filter that controls access to the TFTP server

[Example]

Show the settings of the TFTP server.

```
SWX2210P#show tftp-server
Service:Enable
Port:69
Access:
  deny   192.168.100.5
  permit 192.168.100.0/24
```

4.11.3 Restrict access to the TFTP server according to the IP address of the client

[Syntax]

tftp-server access *action info*
no tftp-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/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 (X:X::X:X) as the IPv6 address
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Specifies all IPv4/IPv6 addresses

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Restrict access to the TFTP 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 parameters are omitted with the "no" syntax, all settings are deleted.

If the IPv4/IPv6 address has changed, all settings are deleted.

[Note]

If the "**tftp-server enable**" command is not specified, this command does not work.

[Example]

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

```
SWX2210P(config)#tftp-server access permit 192.168.1.1
SWX2210P(config)#tftp-server access permit 192.168.10.0/24
```

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

```
SWX2210P(config)#tftp-server access deny 192.168.10.0/24
SWX2210P(config)#tftp-server access permit any
```

4.12 HTTP server

4.12.1 Start HTTP server and change listening port number

[Syntax]

http-server enable [*port*]

[Parameter]

port : <1-65535>

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

[Initial value]

http-server enable

[Input mode]

global configuration mode

[Description]

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

This command cannot be deleted, so the HTTP server is always enabled.

[Example]

Set 8080 as the listening port number.

```
SWX2210P(config)#http-server enable 8080
```

4.12.2 Start secure HTTP server and change listening port number

[Syntax]

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

[Keyword]

enable	:	Enables the secure HTTP server
disable	:	Disables the secure HTTP server

[Parameter]

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

[Initial value]

http-server secure disable

[Input mode]

global configuration mode

[Description]

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

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

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

To avoid a high usage rate, it is desirable to avoid access by multiple users to an automatically updating Web page such as the dashboard.

[Example]

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

```
SWX2210P(config)#http-server secure enable 8080
```

4.12.3 Show HTTP server settings

[Syntax]

show http-server

[Input mode]

privileged EXEC mode

[Description]

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

- HTTP server function enabled/disabled
- Number of the listening port of the HTTP server
- Secure HTTP server function enabled/disabled
- Secure HTTP server listening port number
- Filter that limits access to HTTP servers
- Web GUI language
- Login timeout time

[Example]

Show the settings of the HTTP server.

```
SWX2210P#show http-server
HTTP :Enable(80)
HTTPS:Disable
Access:None
Language: Japanese
Login-timeout: 10 (minutes)
```

4.12.4 Restrict access to the HTTP/HTTPS server according to the IP address of the client

[Syntax]

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

[Parameter]

action : Specifies the action for the access condition

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

info : Specifies the transmission-source IPv4/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 (X:X::X:X) as the IPv6 address
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Specifies all IPv4/IPv6 addresses

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Restricts access to the HTTP/HTTPS 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.

When "deny" is specified for *action*, "any" cannot be specified for *info*.

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

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

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

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

If the IPv4/IPv6 address has changed, all settings are deleted.

[Note]

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

[Example]

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

```
SWX2210P(config)#http-server access permit 192.168.1.1
SWX2210P(config)#http-server access permit 192.168.10.0/24
```

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

```
SWX2210P(config)#http-server access deny 192.168.10.0/24
SWX2210P(config)#http-server access permit any
```

4.12.5 Set WebGUI display language

[Syntax]

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

[Parameter]

lang : Specify the language

Setting value	Description
japanese	Japanese
english	English

[Initial value]

http-server language japanese

[Input mode]

global configuration mode

[Description]

Sets the WebGUI display language.

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

[Example]

Set the WebGUI display language to English.

```
SWX2210P(config)#http-server language english
```

4.12.6 Set log-in timeout time for HTTP/HTTPS server

[Syntax]

http-server login-timeout *min*
no http-server login-timeout

[Parameter]

min : <1-120>
Timeout time (minutes)

[Initial value]

http-server login-timeout 10

[Input mode]

global configuration mode

[Description]

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

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 timeout time for the HTTP/HTTPS server to 5 minutes.

```
SWX2210P(config)#http-server login-timeout 5
```

4.13 LLDP

4.13.1 Enable LLDP function

[Syntax]

lldp run
no lldp run

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Enable the LLDP function for the entire system.

If this is executed with the "no" syntax, the LLDP function is disabled for the entire system.

[Note]

In order to enable the LLDP function for a port, the following command must be set.

Set the "**set lldp enable**" command's "*type*" (LLDP agent mode) to "txrx", "txonly", or "rxonly" as necessary.

- **lldp run** (global configuration mode)
- **lldp-agent** (interface mode)
- **set lldp enable** *type* (LLDP agent mode)

[Example]

Enable LLDP function transmission and reception for LAN port #1.

```
SWX2210P#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWX2210P(config)#lldp run
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#lldp-agent
SWX2210P(lldp-agent)#set lldp enable txrx
```

4.13.2 Create LLDP agent

[Syntax]

lldp-agent
no lldp-agent

[Initial value]

None

[Input mode]

interface mode

[Description]

Create an LLDP agent, and transition to LLDP agent mode.

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

[Note]

When you delete the LLDP agent, the commands specified in LLDP agent mode are also deleted.

[Example]

Create an LLDP agent on port1.1, and transition to LLDP agent mode.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#lldp-agent
SWX2210P(lldp-agent)#
```

4.13.3 Configure the LLDP auto setting function

[Syntax]

lldp auto-setting *switch*
no lldp auto-setting

[Parameter]

switch : Configure the LLDP auto setting function

Setting value	Description
enable	Enable LLDP automatic setting function
disable	Disable LLDP automatic setting function

[Initial value]

lldp auto-setting disable

[Input mode]

global configuration mode

[Description]

Enables the function by which LLDP frames transmitted by specific Yamaha devices can automatically modify the settings of a switch, or automatically execute specific processes.

The automatic settings and items to automatically execute are shown below.

- If an ADECIA component is connected, this automatically configures the optimal Dante settings.
- Automatically implement active/inactive monitoring via LLDP for the port to which the Yamaha wireless access point is connected.

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

This can be set only for a physical interface.

[Note]

To use this function, you must use the "**set lldp enable**" command to enable reception of LLDP frames.

[Example]

Enable the LLDP automatic setting function.

```
SWX2210P(config)#lldp auto-setting enable
```

4.13.4 Set functions enabled by LLDP auto setting

[Syntax]

lldp auto-setting function *func_type* [*func_type*]
no lldp auto-setting function

[Parameter]

func_type : Function enabled by LLDP auto setting

Setting value	Description
dante-optimization	If an ADECIA component is connected, this automatically configures the optimal Dante settings.
terminal-shutdown-notice	If power supply shutdown is scheduled for a port to which a wireless Yamaha access point is connected, send a notification of the power supply shutdown beforehand.

[Initial value]

lldp auto-setting function dante-optimization terminal-shutdown-noteice

[Input mode]

global configuration mode

[Description]

Sets the functions that are enabled by LLDP auto setting.

If this command is executed with the "no" syntax, all functions are enabled.

To partially disable some functions, overwrite with the command to exclude those parameters.

func type requires at least one parameter to be specified.

This can be set only for a physical interface.

[Note]

When using the default setting to enable all, the CONFIG command is not shown.

For this reason, the command is not shown in the default configuration when using the factory default settings.

[Example]

Only enable notifications beforehand for power supply shutdown to ports to which a Yamaha wireless access point is connected, when using LLDP auto setting.

```
SWX2210P(config)#lldp auto-setting function terminal-shutdown-noteice
```

Enable only the optimal Dante settings if an ADECIA component is connected, when using LLDP auto setting.

```
SWX2210P(config)#lldp auto-setting function dante-optimization
```

Enable automatic setting for all functions with LLDP auto setting.

```
SWX2210P(config)#no lldp auto-setting function
```

4.13.5 Set LLDP transmission/reception mode

[Syntax]

set lldp enable *type*
set lldp disable
no set lldp

[Parameter]

type : Transmission/reception mode

Setting value	Description
rxonly	Set receive-only mode
txonly	Set transmit-only mode
txrx	Set transmit and receive

[Initial value]

set lldp disable

[Input mode]

LLDP agent mode

[Description]

Sets the LLDP frame transmission/reception mode for the applicable interface.

If you specify "**set lldp disable**", LLDP frames are not transmitted or received.

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

[Example]

Set the LLDP transmission/reception mode of LAN port #1 to receive-only.

```
SWX2210P(config)#lldp run
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#lldp-agent
SWX2210P(lldp-agent)#set lldp enable rxonly
```

4.13.6 Set type of management address

[Syntax]

set management-address-tlv *type*
no set management-address-tlv

[Parameter]

type : Type of management address

Setting value	Description
ip-address	Set IP address as the management address
mac-address	Set MAC address as the management address

[Initial value]

set management-address-tlv ip-address

[Input mode]

LLDP agent mode

[Description]

Sets the type of port management address used by LLDP.

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

The specified value is set in "LLDP Management Address TLV".

[Example]

Set the MAC address as the type of management address for LAN port #1.

```
SWX2210P(config)#lldp run
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#lldp-agent
SWX2210P(lldp-agent)#set management-address mac-address
```

4.13.7 Set LLDP frame transmission interval

[Syntax]

set timer msg-tx-interval *tx_interval*
no set timer msg-tx-interval

[Parameter]

tx_interval : <5-3600>

LLDP frame transmission interval (sec)

[Initial value]

set timer msg-tx-interval 30

[Input mode]

LLDP agent mode

[Description]

Sets the LLDP frame transmission interval.

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

[Example]

Set 60 seconds as the LLDP frame transmission interval transmitted by LAN port #1.

```
SWX2210P(config)#lldp run
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#lldp-agent
SWX2210P(lldp-agent)#set timer msg-tx-interval 60
```

4.13.8 Set multiplier for calculating time to live (TTL) of device information

[Syntax]

set msg-tx-hold *value*
no set msg-tx-hold

[Parameter]

value : <1-100>

Multiplier for calculating the time to live (TTL) value of device information

[Initial value]

set msg-tx-hold 4

[Input mode]

LLDP agent mode

[Description]

Sets the multiplier for calculating the time to live (TTL) of device information.

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

This setting is multiplied with the LLDP frame transmission interval (msg-tx-interval), and then increased by +1 to become the TTL value (seconds).

The TTL value is set in the Time To Live TLV.

TTL = msg-tx-interval × msg-tx-hold ＋ 1 (sec)

[Example]

Set 2 as the multiplier used to calculate the time to live (TTL) for device information on LAN port #1.

```
SWX2210P(config)#lldp run
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#lldp-agent
SWX2210P(lldp-agent)#set msg-tx-hold 2
```

4.13.9 Set maximum number of connected devices manageable by a port

[Syntax]

set too-many-neighbors limit *max_value*
no set too-many-neighbors limit

[Parameter]

max_value : <1-100>
Maximum number of connected devices manageable by a port

[Initial value]

set too-many-neighbors limit 5

[Input mode]

LLDP agent mode

[Description]

Sets the maximum number of connected devices that can be managed by a port.

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

If the maximum number of connected device for a port is exceeded, LLDP frames sent from new devices are ignored.

[Example]

Set 10 as the maximum number of connected devices that can be managed by a port on LAN port #1.

```
SWX2210P(config)#lldp run
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#lldp-agent
SWX2210P(lldp-agent)#set too-many-neighbors limit 10
```

4.13.10 Show interface status

[Syntax]

show lldp interface *ifname* [neighbor]

[Keyword]

neighbor : Show information for connected devices.

[Parameter]

ifname : Interface name of the LAN port
Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows LLDP information for the interface specified by "*ifname*".

If "neighbor" is specified, information for the device connected to the interface is shown.

The following items are shown.

For **show lldp interface** *ifname*

- Interface and its stastical information

Agent Mode	Bridge mode (nearest bridge fixed)
Enable (tx/rx)	Transmission mode/reception mode (Y: enabled, N: disabled)
Message fast transmit time	LLDP frame transmission interval (sec) for high-speed transmission interval
Message transmission interval	LLDP frame transmission interval (sec)
Reinitialization delay	Time (sec) for reinitialization after transmission stop
MED Enable	Enable/disable LLDP-MED TLV transmission (fixed at enabled)
Device Type	Device type (fixed at NETWORK_CONNECTIVITY)
Total frames transmitted	No. of LLDP frame transmissions
Total entries aged	No. of devices that have been deleted from the management table, and for which frames have not been received for the no. of TTL sec. or more
Total frames received	No. of LLDP frames received
Total frames received in error	No. of LLDP frame reception errors
Total frames discarded	No. of discarded LLDP frames
Total discarded TLVs	No. of discards TLVs
Total unrecognised TLVs	No. of unrecognized TLVs

For **show lldp interface** *ifname* neighbor

- Basic management information

Interface Name	Name of received interface
System Name	Name of system
System Description	Description of system
Port Description	Description of port
System Capabilities	Capabilities of system
Interface Numbering	Type of interface numbering used
Interface Number	Interface number
OID Number	OID number
Management Address	MAC address or IP address

- Mandatory TLV information

CHASSIS ID TYPE	Type of CHASSIS ID TLV and value
PORT ID TYPE	Type of PORT ID TLV and value
TTL (Time To Live)	How long the device information is retained (sec)

- 8021 ORIGIN SPECIFIC TLV information

Port Vlan id	Port VLAN ID
PP Vlan id	Protocol VLAN ID
VLAN ID	ID of port VLAN
VLAN Name	Name of port VLAN
Remote Protocols Advertised	List of supported protocols
Remote VID Usage Digestt	VID Usage Digestt value
Remote Management Vlan	Name of management VLAN

Link Aggregation Status	Link aggregation enabled/disabled
Link Aggregation Port ID	link aggregation port ID

- 8023 ORIGIN SPECIFIC TLV information

AutoNego Support	Auto negotiation function enabled/disabled
AutoNego Capability	Usable communication methods for auto negotiation
Operational MAU Type	Communication speed and duplex mode
MDI power support	PoE function support availability
PSE power pair	PSE power pair
Power class	PoE power supply class
Type/source/priority	PoE power supply type, source, priority
PD requested power value	Power (in 0.1mW increments) requested by the PD device
PSE allocated power value	Power (in 0.1 mW increments) that the PSE device can supply
Max Frame Size	Maximum frame size

- LLDP-MED TLV information (displayed when LLDP-MED TLV is received)

MED Capabilities	LLDP-MED TLV type list
MED Capabilities Dev Type	LLDP-MED media device type
MED Application Type	Application type
MED Vlan id	VLAN ID
MED Tag/Untag	VLAN tag availability
MED L2 Priority	L2 priority
MED DSCP Val	DSCP value priority
MED Location Data Format	Location data format
Latitude Res	Resolution of latitude (number of valid high-order bits)
Latitude	Latitude (34 bits)
Longitude Res	Longitude resolution (number of valid high-order bits)
Longitude	Longitude (34 bits)
AT	Altitude
	1: Meters
	2: Building floor
Altitude Res	Altitude resolution (number of valid high-order bits)
Altitude	Altitude (30 bits)
Datum	Geodetic datum
	0: World Geodetic System (WGS 84) of the U.S.
	1: North American Datum (NAD 83)
	2: Average lowest tide of the North American Datum (NAD 83)
LCI length	Length of location data

What	Reference location
	0: DHCP server location
	1: Location of the network element considered to be closest to the client
	2: Client position
Country Code	Country code
CA type	CA (Civic Address) type
MED Inventory	Inventory information list

Refer to RFC 3825 for details on location information

[Example]

Show LLDP information for LAN port #1.

```
SWX2210P#show lldp interface port1.1
Agent Mode                    : Nearest bridge
Enable (tx/rx)                : Y/Y
Message fast transmit time    : 1
Message transmission interval : 30
Reinitialization delay        : 2
MED Enabled                   : Y
Device Type                   : NETWORK_CONNECTIVITY
LLDP Agent traffic statistics
  Total frames transmitted       : 0
  Total entries aged             : 0
  Total frames received          : 0
  Total frames received in error : 0
  Total frames discarded         : 0
  Total discarded TLVs           : 0
  Total unrecognised TLVs        : 0
SWX2210P#
```

4.13.11 Show information for connected devices of all interfaces

[Syntax]

show lldp neighbors

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows information for connected devices of all interfaces.

(For the display format, refer to the "**show lldp interface** *ifname* neighbor" command)

[Example]

Show information for connected devices.

```
SWX2210P#show lldp neighbors
Interface Name           : port1.1
System Name              : SWX2210P-10G
System Description       : SWX2210P-10G Rev.1.03.13 (Wed Sep  4 08:33:10 2024)
Port Description         : port1.3
System Capabilities      : L2 Switching
Interface Numbering      : 2
Interface Number         : 3
OID Number               :
Management MAC Address   : ac44.f230.0000
Mandatory TLVs
  CHASSIS ID TYPE
    IP ADDRESS           : 0.0.0.0
  PORT ID TYPE
    INTERFACE NAME       : port1.3
  TTL (Time To Live)     : 41
8021 ORIGIN SPECIFIC TLVs
  Port Vlan id               : 1
  PP Vlan id                 : 0
  Remote VLANs Configured
```

```
    VLAN ID                  : 1
    VLAN Name                : default
  Remote Protocols Advertised :
    Multiple Spanning Tree Protocol
  Remote VID Usage Digestt    : 0
  Remote Management Vlan      : 0
  Link Aggregation Status     : Disabled
  Link Aggregation Port ID    : 0
8023 ORIGIN SPECIFIC TLVs
  AutoNego Support            : Supported Enabled
  AutoNego Capability         : 27649
  Operational MAU Type        : 30
  Power via MDI Capability (raw data)
    MDI power support         : 0x0
    PSE power pair            : 0x0
    Power class               : 0x0
    Type/source/priority      : 0x0
    PD requested power value  : 0x0
    PSE allocated power value : 0x0
  Max Frame Size              : 1522
LLDP-MED TLVs
  MED Capabilities            :
    Capabilities
    Network Policy
  MED Capabilities Dev Type   : End Point Class-3
  MED Application Type        : Reserved
  MED Vlan id                 : 0
  MED Tag/Untag               : Untagged
  MED L2 Priority             : 0
  MED DSCP Val                : 0
  MED Location Data Format    : ECS ELIN
    Latitude Res      : 0
    Latitude          : 0
    Longitude Res     : 0
    Longitude         : 0
    AT                : 0
    Altitude Res      : 0
    Altitude          : 0
    Datum             : 0
    LCI length        : 0
    What              : 0
    Country Code      : 0
    CA type           : 0
  MED Inventory

SWX2210P#
```

4.13.12 Clear LLDP frame counters

[Syntax]

clear lldp counters

[Input mode]

privileged EXEC mode

[Description]

Clear the LLDP frame counter of all ports.

[Example]

Clear the LLDP frame counter.

```
SWX2210P#clear lldp counters
```

4.14 L2MS (Layer 2 management service) settings

4.14.1 Move to L2MS mode

[Syntax]

l2ms configuration

[Input mode]

global configuration mode

[Description]

Moves to L2MS mode in order to make L2MS settings.

[Note]

To return from L2MS mode to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

[Example]

Move to L2MS mode.

```
SWX2210P(config)#l2ms configuration
SWX2210P(config-l2ms)#
```

4.14.2 Set L2MS function

[Syntax]

l2ms enable
l2ms disable
no l2ms

[Keyword]

enable	:	Use the L2MS function
disable	:	Don't use the L2MS function

[Initial value]

l2ms enable

[Input mode]

L2MS mode

[Description]

Sets whether to use the L2MS function.

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

[Example]

Use the L2MS function.

```
SWX2210P(config)#l2ms configuration
SWX2210P(config-l2ms)#l2ms enable
```

4.14.3 Set L2MS control frame transmit/receive

[Syntax]

l2ms filter *switch*
no l2ms filter

[Parameter]

switch : L2MS filter operations

Setting value	Description
enable	Enable the L2MS filter
disable	Disable the L2MS filter

[Initial value]

l2ms filter disable

[Input mode]

interface mode

[Description]

Configures the L2MS filter operation.

With the L2MS filter is enabled, you can prohibit the transmission/reception of L2MS control frames.

If this command is executed with the "no" syntax, the L2MS filter is disabled, and L2MS control frames can be transmitted and received.

[Note]

This command cannot be specified for the following interfaces.

- VLAN interface
- logical interface

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 blocking status due to the loop detection function
- It is inside a logical interface

[Example]

Prevent port1.5 from transmitting or receiving L2MS control frames.

```
SWX2210P(config)#interface port1.5
SWX2210P(config-if)#l2ms filter enable
```

4.14.4 Set frame transmission/reception for frames other than L2MS control frames

[Syntax]

non-l2ms filter *switch*
no non-l2ms filter

[Parameter]

switch : Non-L2MS filter operations

Setting value	Description
enable	Enable non-L2MS filters
disable	Disable non-L2MS filters

[Initial value]

non-l2ms filter disable

[Input mode]

interface mode

[Description]

Configures the non-L2MS filter operations.

With the non-L2MS filter enabled, you can prohibit the transmission/reception of frames other than L2MS control frames.

If this command is executed with the "no" syntax, the non-L2MS filter is disabled, and frames other than L2MS control frames can be transmitted/received.

[Note]

This command cannot be specified for the following interfaces.

- VLAN interface
- logical interface

[Example]

Prevent port1.5 from transmitting or receiving frames other than L2MS control frames.

```
SWX2210P(config)#interface port1.5
SWX2210P(config-if)#non-l2ms filter enable
```

4.14.5 Show L2MS information

[Syntax]

show l2ms

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the following information according to the L2MS operating state.

- Whether managed by the L2MS manager
- MAC address of L2MS manager (if managed)

[Note]

Information is not shown if L2MS is not operating.

[Example]

This shows the L2MS information.

```
SWX2210P>show l2ms
Role : Agent
Status : Managed by Manager (00a0.deaa.aaaa)
```

4.15 Firmware update

4.15.1 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]

For SWX2210P-10G: firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin

For SWX2210P-18G: firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-18g.bin

For SWX2210P-28G: firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-28g.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/swx2210p-10g.bin as the firmware download URL.

```
SWX2210P(config)#firmware-update url http://192.168.100.1/swx2210p-10g.bin
SWX2210P(config)#
```

4.15.2 HTTP proxy server settings used for firmware updates

[Syntax]

firmware-update http-proxy *server port*
no firmware-update http-proxy

[Parameter]

server : A.B.C.D

IPv4 address of the HTTP proxy server

: X:X::X:X

IPv6 address of the HTTP proxy server

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

: Single-byte alphanumeric characters and single-byte symbols (255 characters or less)

FQDN of the HTTP proxy server

port : <1-65535>

HTTP proxy server's listening port number

[Initial value]

no firmware-update http-proxy

[Input mode]

global configuration mode

[Description]

Specify the HTTP proxy server used when updating the firmware from a firmware file located on a Web server.

If an HTTP proxy server has not been set, the firmware update is carried out without going through the HTTP proxy server.

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

[Example]

Set the HTTP proxy server to 192.168.100.1 (port number 8080).

```
SWX2210P(config)#firmware-update http-proxy 192.168.100.1 8080
SWX2210P(config)#
```

4.15.3 HTTPS proxy server settings used for firmware updates

[Syntax]

firmware-update https-proxy *server port*
no firmware-update https-proxy

[Parameter]

server : A.B.C.D

IPv4 address of the HTTPS proxy server

: X:X::X:X

IPv6 address of the HTTPS proxy server

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

: Single-byte alphanumeric characters and single-byte symbols (255 characters or less)

FQDN of the HTTPS proxy server

port : <1-65535>

HTTPS proxy server's listening port number

[Initial value]

no firmware-update https-proxy

[Input mode]

global configuration mode

[Description]

Specify the HTTPS proxy server used when updating the firmware from a firmware file located on a Web server.

If an HTTPS proxy server has not been set, the firmware update is carried out without going through the HTTPS proxy server.

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

[Example]

Set the HTTPS proxy server to 192.168.100.1 (port number 8080).

```
SWX2210P(config)#firmware-update https-proxy 192.168.100.1 8080
SWX2210P(config)#
```

4.15.4 Execute firmware update

[Syntax]

firmware-update execute [no-confirm]

[Keyword]

no-confirm	:	Don't confirm the firmware update

[Input mode]

privileged 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.

```
SWX2210P#firmware-update execute
Found the new revision firmware
Current Revision: Rev.1.03.01
New Revision:     Rev.1.03.03
Update to this firmware? (Y/N)y
Download...
%% Completed the firmware download
%% Updating...
SWX2210P#
```

4.15.5 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.

```
SWX2210P(config)#firmware-update timeout 120
SWX2210P(config)#
```

4.15.6 Allow revision-down

[Syntax]

firmware-update revision-down *switch*
no firmware-update revision-down

[Parameter]

switch : Set revision-down permission

Setting value	Description
enable	Permit revision-down
disable	Do not permit revision-down

[Initial value]

firmware-update revision-down disable

[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.

```
SWX2210P(config)#firmware-update revision-down enable
SWX2210P(config)#
```

4.15.7 Show firmware update function settings

[Syntax]

show firmware-update

[Input mode]

privileged EXEC mode

[Description]

Shows the current settings of the firmware update function.

The following items are shown.

- Download source URL
- HTTP proxy server
- HTTPS proxy server
- Download timeout duration
- Allow revision-down

[Example]

Show the current settings of the firmware update function.

```
SWX2210P#show firmware-update
url:http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin
http-proxy:192.168.100.1:8080
https-proxy:192.168.100.1:8080
timeout:300 (seconds)
revision-down:disable
SWX2210P#
```

4.16 Schedule

4.16.1 Schedule settings

[Syntax]

schedule *id* **time** *date time template_id*
no schedule *id*

[Parameter]

id : <1-10>

Schedule number

date : <1-12> or * / <1-12> or sun, mon, ... , sat or *

Month/day

Month setting examples	Setting contents
1	January
1,2	January and February
2-	From February to December
2-7	From February to July
-7	From January to July
*	Monthly

Day setting examples	Setting contents
1	One day
1,2	The 1st and the 2nd
2-	From the 2nd to the 12th
2-7	From the 2nd to the 7th
-7	From the 1st to the 7th
mon	Monday
sat,sun	Saturday and Sunday
mon-fri	From Monday to Friday
-fri	From Sunday to Friday
*	Monthly

time : <0-23> or * : <0-59> or * : <0-59>

h:m:s (the seconds can be omitted)

Hour setting examples	Setting contents
12	12:00
12,13	12:00 and 13:00
12-	From 12:00 to 23:00
10-20	From 10:00 to 20:00
-20	From 0:00 to 20:00
*	Hourly

Minute setting examples	Setting contents
30	30 minutes
15,45	15 minutes and 45 minutes
30-	From 30 minutes to 59 minutes
15-45	From 15 minutes to 45 minutes
-45	From 0 minutes to 45 minutes
*	Each minute

template_id : <1-10>

Schedule template number

[Initial value]

None

[Input mode]

global configuration mode

[Description]

When the specified time is reached, the actions described in the specified schedule template are executed.

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

[Note]

Commands such as **power-inline** can only be executed on models that support PoE power supply.

When multiple schedules are executed at the same time, they are executed beginning with the schedule with the smallest ID.

When specifying the day, you cannot specify using a mix of numbers and weekdays.

If the seconds are omitted, the settings will be the same as when specifying "00" seconds.

For the month and days settings, you can specify ranges using "-" and "," characters, and you can specify all dates using the "*" character. Note that for the seconds setting, you cannot specify ranges using "-" and "," characters, nor can you specify all dates using the "*" character.

[Example]

Configures schedule #1 to execute schedule template #1 every Monday at exactly 22:00, from Monday through Friday.

```
SWX2210P(config)#schedule 1 time */mon-fri 22:00 1
```

4.16.2 Schedule template description text settings

[Syntax]

description *line*
no description

[Parameter]

line : Single-byte alphanumeric characters and single-byte symbols (64 characters or less)

Schedule template description text

[Initial value]

no description

[Input mode]

Schedule template mode

[Description]

Sets the schedule template description text.

If this command is executed with the "no" syntax, the description text in the specified schedule template is deleted.

[Example]

This sets the description text for schedule template #1.

```
SWX2210P(config)#schedule template 1
SWX2210P(config-schedule)#description Switch port1.1 to disable
```

4.16.3 Settings to enable/disable schedule template

[Syntax]

action *switch*
no action

[Parameter]

switch : Schedule template settings

Setting value	Description
enable	Enable schedule template
disable	Disable schedule template

[Initial value]

action enable

[Input mode]

Schedule template mode

[Description]

This enables or disables the schedule template.

Specifying "disable" with this command makes it possible to stop execution of actions due to trigger startup.

If this command is executed with the "no" syntax, the schedule template is enabled.

[Example]

Disables schedule template #1.

```
SWX2210P(config)#schedule template 1
SWX2210P(config-schedule)#action disable
```

4.16.4 Schedule template settings

[Syntax]

schedule template *template_id*
no schedule template

[Parameter]

template_id : <1-10>

Schedule template number

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Switches to the mode for setting the schedule template.

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

[Example]

This switches to the mode for setting schedule template #1.

```
SWX2210P(config)#schedule template 1
SWX2210P(config-schedule)#
```

4.16.5 Schedule template command execution settings

[Syntax]

cli-command *id command*
no cli-command *id*

[Parameter]

id	:	<1-100>
		Command no.
command	:	Command

[Initial value]

None

[Input mode]

Schedule template mode

[Description]

This sets the commands to be executed when the trigger for a schedule function starts.

If this command is executed with the "no" syntax, commands with the specified numbers are deleted.

[Note]

If multiple commands are specified, the commands are executed beginning with the command with the smallest command number.

If multiple commands are specified, the remaining commands will still be executed even if the command results in an execution error while running.

As commands are executed in privileged EXEC mode when the trigger starts, some commands may need to be configured along with commands that switch to an appropriate mode.

The last "write" command must be executed to save the settings.

Commands cannot be specified in abbreviated form. For instance, you must write "interface port1.1" and not "int port1.1" when entering the input mode for Port1.1 of the interface.

For *command*, you can only specify the commands shown below.

configure terminal, interface, shutdown, no shutdown, power-inline disable, power-inline enable, write, end, exit

[Example]

Specify the "configure terminal" command for the schedule template #1 command number #1, the "interface" command for #2, and the "power-inline disable" command for #3.

```
SWX2210P(config)#schedule template 1
SWX2210P(config-schedule)#cli-command 1 configure terminal
SWX2210P(config-schedule)#cli-command 2 interface port1.1
SWX2210P(config-schedule)#cli-command 3 power-inline disable
```

4.17 Cable diagnostics

4.17.1 Execute cable diagnostics

[Syntax]

test cable-diagnostics tdr interface *ifname*

[Parameter]

ifname	:	LAN port interface name
		Applicable interface

[Input mode]

privileged EXEC mode

[Description]

Executes cable diagnostics.

The previous diagnostics result can be checked using the **show test cable-diagnostics tdr** command.

[Note]

Only the most recent diagnostics results can be retained. The results are overwritten if the cable diagnostics are executed again.

[Example]

Executes cable diagnostics for the LAN cable connected to port 1.1.

```
SWX2210P#test cable-diagnostics tdr interface port1.1
The port will be temporarily down during test. Continue? (y/N): y
Cable-diagnostic is running...

Port     Pair  Status  Fault distance  Length
-------------------------------------------------
port1.1  1     OK      -               50 +/- 10 m
         2     OK      -
         3     OK      -
         4     OK      -
SWX2210P#
```

4.17.2 Show cable diagnostics results

[Syntax]

show test cable-diagnostics tdr

[Input mode]

privileged EXEC mode

[Description]

Shows the results of executing the previous **test cable-diagnostics tdr interface** command.

[Example]

Show the results of executing the previous cable diagnostics.

```
SWX2210P#show test cable-diagnostics tdr
Last run on Fri Feb 26 10:30:00 2021

Port     Pair  Status  Fault distance  Length
-------------------------------------------------
port1.3  1     OK      -               -
         2     OK      -
         3     Open    5 +/- 10 m
         4     Open    5 +/- 10 m
SWX2210P#
```

4.17.3 Clear cable diagnostics results

[Syntax]

clear test cable-diagnostics tdr

[Input mode]

privileged EXEC mode

[Description]

Clears the results of executing the previous **test cable-diagnostics tdr interface** command.

[Example]

Clear the results of executing the previous cable diagnostics.

```
SWX2210P#clear test cable-diagnostics tdr
SWX2210P#
```

4.18 General maintenance and operation functions

4.18.1 Set host name

[Syntax]

hostname *hostname*
no hostname [*hostname*]

[Parameter]

hostname	:	Single-byte alphanumeric characters, and single-byte symbols other ? (question marks) (63 characters or less) Host name

[Initial value]

hostname SWX2210P

[Input mode]

global configuration mode

[Description]

Specifies the host name.

The host name specified by this command is used as the command prompt.

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

[Example]

Set the host name as "yamaha."

```
SWX2210P(config)#hostname yamaha
yamaha(config)#
```

4.18.2 Reload system

[Syntax]

reload

[Input mode]

privileged EXEC mode

[Description]

Reboot 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.

```
SWX2210P#reload
reboot system? (y/n): y
```

4.18.3 Initialize settings

[Syntax]

cold start

[Input mode]

privileged 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. To do this, you must first change the administrator password.

[Example]

Initialize the settings.

```
SWX2210P#cold start
Password:
```

4.18.4 Default LED mode setting

[Syntax]

led-mode default *mode*
no led-mode default

[Parameter]

mode : Default LED mode

Setting value	Description
link-act	LINK/ACT mode
off	OFF mode

[Initial value]

led-mode default link-act

[Input mode]

global configuration mode

[Description]

Set the default LED mode.

When link-act is specified, the LED lights up according to the port status.

When off is specified, the LED goes dark.

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

[Example]

Set the default LED mode to OFF mode.

```
SWX2210P(config)#led-mode default off
```

4.18.5 Show LED mode

[Syntax]

show led-mode

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show 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.

```
SWX2210P>show led-mode
default mode : off
current mode : link-act
```

4.18.6 Set ProAV profile type

[Syntax]

proav profile-type *type*

[Parameter]

type : ProAV profile type

Setting value	Description
dante-primary	Dante primary
dante-secondary	Dante secondary
ndi	NDI

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the ProAV profile type.

This command is used with the ProAV settings page in the Web GUI, to select the compatible ProAV profile type for the VLAN.

[Note]

This command is automatically set when setting a ProAV profile from the Web GUI. The command cannot be directly executed.

Chapter 5

Interface control

5.1 Interface basic settings

5.1.1 Set description

[Syntax]

description *line*
no description

[Parameter]

line : Single-byte alphanumeric characters and single-byte symbols (80characters or less)
Description of the applicable interface

[Initial value]

no description

[Input mode]

interface mode

[Description]

Specifies a description of the applicable interface. If this command is executed with the "no" syntax, the description is deleted.

[Example]

Specify a description for LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#description Connected to rtx1210-router
```

5.1.2 Shutdown

[Syntax]

shutdown
no shutdown

[Initial value]

no shutdown

[Input mode]

interface mode

[Description]

Shut down the applicable interface so that it is not used.

An interface for which this command is specified will not link-up even if it is connected.

If this command is executed with the "no" syntax, the applicable interface can be used.

[Note]

This command can be specified only for LAN port and logical interface.

If this command is applied to logical interface, the settings of all LAN port units belonging to that interface are changed.

[Example]

Shut down LAN port #1 so that it is not used.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#shutdown
```

5.1.3 Set speed and duplex mode

[Syntax]

speed-duplex *type*

no speed-duplex

[Parameter]

type : Speed and duplex mode types

Speed and duplex mode types	Description
auto	Auto negotiation
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 port.

[Example]

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

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#speed-duplex 100-full
```

5.1.4 Set MRU

[Syntax]

mru *mru*
no mru

[Parameter]

mru : <1522-10240>

Maximum frame size that can be received

[Initial value]

mru 1522

[Input mode]

global configuration 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.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#mru 9000
```

5.1.5 Set cross/straight automatic detection

[Syntax]

mdix auto *switch*
no mdix auto

[Parameter]

switch : Cross/straight automatic detection operations

Setting value	Description
enable	Enable cross/straight automatic detection
disable	Disable cross/straight automatic detection

[Initial value]

mdix auto enable

[Input mode]

interface mode

[Description]

Enables cross/straight automatic detection. If this is enabled, the necessary cable connection type (straight or cross) is automatically detected, and the connection is specified appropriately.

If this is executed with the "no" syntax, automatic detection is disabled, and MDI is used.

[Note]

This command can be specified only for LAN port.

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

[Example]

Disable cross/straight automatic detection for LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#mdix auto disable
```

5.1.6 Set EEE

[Syntax]

eee *switch*
no eee

[Parameter]

switch : Behavior of the EEE

Setting value	Description
enable	Enable EEE
disable	Disable EEE

[Initial value]

eee disable

[Input mode]

interface mode

[Description]

Enables Energy Efficient Ethernet (EEE).

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

[Note]

This command can be specified only for LAN port.

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

[Example]

Enable EEE for LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#eee enable
```

5.1.7 Show EEE status

[Syntax]

show eee status interface *ifname*

[Parameter]

ifname : LAN port interface name

Interface to show

[Input mode]

unprivileged EXEC mode, privileged 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

[Example]

Show EEE status of LAN port #1.

```
[If EEE is disabled]
  SWX2210P#show eee status interface port1.1
  interface:port1.1
    EEE(efficient-ethernet):  Disabled

[If EEE is enabled]
  SWX2210P#show eee status interface port1.1
  interface:port1.1
    EEE(efficient-ethernet):  Enabled
```

5.1.8 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 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 sniffer port and *ifname* as the monitored port.

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

[Note]

This command can be specified only for LAN port.

Up to four interfaces can be specified as the sniffer port. You cannot monitor multiple sniffer ports with a single monitoring port.

You cannot use an interface configured as a sniffer port to be a monitoring port.

You cannot use LAN ports that belong to a logical interface as sniffer ports.

[Example]

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

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#mirror interface port1.4 direction both
SWX2210P(config-if)#mirror interface port1.5 direction transmit
```

5.1.9 Show port mirroring status

[Syntax]

show mirror [interface *ifname*]

[Keyword]

interface	:	Specify the sniffer port to show

[Parameter]

ifname	:	Interface name of the LAN port sniffer port to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the port mirroring setting. If interface is omitted, the settings for all sniffer ports are shown.

The following items are shown for each sniffer port.

Item	Description
Sniffer Port	Interface name of the sniffer port
Monitored Port	Interface name of the monitored port
Monitoring direction	Direction of traffic that is mirrored

[Example]

Show the sniffer port settings.

```
SWX2210P#show mirror
Sniffer Port Monitored Port Direction
============ ============== ==========
port1.1      port1.4        both
             port1.5        transmit
port1.7      port1.6        both
```

5.1.10 Show interface status

[Syntax]

show interface [*ifname*]

[Parameter]

ifname	:	Interface name

[Input mode]

unprivileged EXEC mode, privileged 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
MRU	Maximum Receive Unit *2
BPDU pass-through	Enable/disable BPDU pass-through *2
EAP pass-through	Enable/disable EAP pass-through *2
Description	Description of interface
ifIndex	Interface index number *2
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)
Switchport mode	Mode of the switchport *2 • access : untagged • trunk : tagged
Ingress filter	Status of ingress filtering *2 • enable : enabled • disable : disabled
Acceptable frame types	Frame types that can be received *2 • 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 *2 • For an untagged port: VLAN specified by the **switchport access vlan** command • For a tagged port: Native VLAN • For a tagged port and set to receive only tagged packets: None • If unspecified: vlan1
Configured Vlans		List of the VLAN IDs that belong to the corresponding interface *2
input	packets	Number of received packets *2
	bytes	Number of received bytes *2
	drops	Number of packets discarded upon receipt *2
	broadcast-and-multicast-packets	Number of broadcast and multicast packets received *2
output	packets	Number of transmitted packets *2
	bytes	Number of transmitted bytes *2
	drops	Number of packets discarded upon transmission *2
	broadcast-and-multicast-packets	Number of transmitted broadcast and multicast packets *2

*1 Shown only for physical interface
*2 Shown only for physical interface and logical interface
*3 Shown only for VLAN interface

[Example]

Show the status of LAN port #1.

```
SWX2210P# show interface port1.1
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: ac44.f200.0000
    MRU 1522
    BPDU pass-through: Enabled
  EAP pass-through: Enabled
  Description: Connected to router
  ifIndex 5001
  Speed-Duplex: auto(configured), 1000-full(current)
  Auto MDI/MDIX: on
  Vlan info:
    Switchport mode         : access
    Ingress filter          : enable
    Acceptable frame types  : all
    Default Vlan            :    1
    Configured Vlans        :    1
  Interface counter:
    input  packets                        : 320
           bytes                          : 25875
       drops                          : 0
           broadcast-and-multicast-packets: 301
    output packets                        : 628
           bytes                          : 129895
       drops                          : 0
           broadcast-and-multicast-packets: 628
```

Show the status of VLAN #1.

```
SWX2210P#show interface vlan1
Interface vlan1
  Hardware is VLAN
  Description: Connected to router(VLAN)
  ARP ageing timeout 1200
  IPv4 address 192.168.100.240/24 broadcast 192.168.100.255
                                          (u)-Untagged, (t)-Tagged
VLAN ID Name                            State   Member ports
======= ================================ ======= ====================================
1       default                         ACTIVE  port1.1(u) port1.2(u) port1.3(u)
                                                port1.4(u) port1.5(u) port1.6(u)
                                                port1.7(u) port1.8(u) port1.9(u)
                                            port1.10(u)
```

5.1.11 Show frame counter

[Syntax]

show frame-counter [*ifname*]

[Parameter]

ifname : Interface name of the LAN port

Interface to show

[Input mode]

unprivileged EXEC mode, privileged 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
total-good-packets	Number of packets normally transmitted/received
total-error-packets	Number of packets transmitted/received with errors (CRC errors, alignment errors, frame size errors, etc.)
drops	Number of packets discarded upon receipt (the counter on the transmitting side is always 0)
broadcast-and-multicast-packets	Number of broadcast and multicast packets transmitted/ received
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 setting value.

[Example]

Show the frame counter of LAN port #1.

```
SWX2210P#show frame-counter port1.1
Interface port1.1 Ethernet MAC counters:
Received:
    packets                          :3501
    octets                           :526319
    total-good-packets               :3501
    total-error-packets              :0
    drops                            :0
    broadcast-and-multicast-packets :3501
    64octet       packets            :44
    65-127octet   packets            :1990
    128-255octet  packets            :1465
    256-511octet  packets            :0
    512-1023octet packets            :2
    1024-MAXoctet packets            :0

Transmitted:
    packets                          :3766
    octets                           :295617
    total-good-packets               :3766
    total-error-packets              :0
    drops                            :0
    broadcast-and-multicast-packets :3754
    64octet       packets            :2049
    65-127octet   packets            :1414
    128-255octet  packets            :265
    256-511octet  packets            :34
    512-1023octet packets            :4
    1024-MAXoctet packets            :0
```

5.1.12 Clear frame counters

[Syntax]

clear counters *ifname*
clear counters all

[Keyword]

all	:	Clearing the frame counter information for all interfaces

[Parameter]

ifname	:	Interface name of LAN port or logical interface Applicable interface

[Input mode]

privileged EXEC mode

[Description]

This clears the frame counter for the interface specified by *ifname*.

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

When "all" is specified, clear all frame counters of LAN port.

[Example]

Clear the frame counters of LAN port #1.

```
SWX2210P#clear counters port1.1
```

Clears all the frame counters of LAN port.

```
SWX2210P#clear counters all
```

5.1.13 Enable BPDU pass-through

[Syntax]

pass-through bpdu *switch*
no pass-through bpdu

[Parameter]

switch	:	Behavior BPDU pass-through

Setting value	Description
enable	Enable the BPDU pass-through
disable	Disable the BPDU pass-through

[Initial value]

pass-through bpdu enable

[Input mode]

global configuration mode

[Description]

Enables/disables BPDU pass-through

If this is executed with the "no" syntax, BPDU pass-through is enabled

[Example]

Disables BPDU pass-through

```
SWX2210P(config)#pass-through bpdu disable
```

5.1.14 Enable EAP pass-through

[Syntax]

pass-through eap *switch*
no pass-through eap

[Parameter]

switch : Behavior EAP pass-through

Setting value	Description
enable	Enable the EAP pass-through
disable	Disable the EAP pass-through

[Initial value]

pass-through eap enable

[Input mode]

global configuration mode

[Description]

Enables/disables EAP pass-through

If this is executed with the "no" syntax, EAP pass-through is enabled

[Example]

Disables EAP pass-through

```
SWX2210P(config)#pass-through eap disable
```

5.2 Link aggregation

5.2.1 Set static logical interface

[Syntax]

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

[Parameter]

link-id : <1-8>

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 port.

If a LAN 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 port is no longer present because it was removed from the static logical interface, the static logical interface is deleted.

Up to eight LAN 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 port and the static logical interface. If the settings differ, an error occurs.

- **shutdown** command setting
- VLAN setting

If a static logical interface is newly generated, the above settings of the LAN port are set to the default settings of the static logical interface.

The LAN port used as a sniffer port for port mirroring cannot be associated with static logical interface.

It is not possible to associate a single LAN 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.

```
SWX2210P(config)#interface port1.9
SWX2210P(config-if)#static-channel-group 5
```

5.2.2 Show static logical interface status

[Syntax]

show static-channel-group

[Input mode]

unprivileged EXEC mode, privileged 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 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.

```
SWX2210P#show static-channel-group
% Load balancing: src-dst-mac
% Static Aggregator: sa1
% Member:
        port1.2
        port1.3
% Static Aggregator: sa5
% Member:
        port1.9
        port1.11
        port1.13
        port1.15
```

5.2.3 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 src-dst-mac

[Input mode]

global configuration 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 is a system-wide setting.

In the case of a frame that is not an IPv4/IPv6 packet, the forwarding destination interface is determined according to the forwarding source and destination MAC addresses, regardless of the rules that were specified.

[Example]

With the load balance function, set the system to determine the forwarding destination interface based on the transmission-source and destination IPv4/IPv6 address.

```
SWX2210P(config)#port-channel load-balance src-dst-ip
```

5.3 PoE

5.3.1 Set PoE power supply function (system)

[Syntax]

power-inline *switch*
no power-inline

[Parameter]

switch : System-wide PoE power supply function settings

Setting value	Description
enable	Enables the system-wide PoE power supply function
disable	Disables the system-wide PoE power supply function

[Initial value]

power-inline enable

[Input mode]

global configuration mode

[Description]

Set the system-wide PoE power supply function as enabled or disabled.

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

[Note]

Even if the system-wide PoE power supply function is enabled, power supply will be disabled for each port if the power supply function is disabled for individual ports.

[Example]

Enable the system-wide PoE power supply function.

```
SWX2210P(config)#power-inline enable
```

Disable the system-wide PoE power supply function.

```
SWX2210P(config)#power-inline disable
```

5.3.2 Set PoE power supply function (interface)

[Syntax]

power-inline *switch*
no power-inline

[Parameter]

switch : PoE power supply function settings for the applicable interface

Setting value	Description
enable	Enables the PoE power supply function for the applicable interface
disable	Disables the PoE power supply function for the applicable interface

[Initial value]

power-inline enable

[Input mode]

interface mode

[Description]

Set the applicable interface PoE power supply function as enabled or disabled.

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

[Note]

This will result in a command execution error on all other ports besides PoE port.

Even if the power supply function is enabled with interface mode, power will not be supplied in the following circumstances.

- When the system-wide PoE power supply function is disabled

[Example]

Enable the PoE power supply function for port1.1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#power-inline enable
```

Disables the PoE power supply function for port1.1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#power-inline disable
```

5.3.3 Set description of PoE port

[Syntax]

power-inline description *line*
no power-inline description

[Parameter]

line : Single-byte alphanumeric characters and single-byte symbols (64 characters or less)

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the description text of the PD device to connect to PoE port.

[Note]

The description text that was set is shown with the **show power-inline** command.

[Example]

Set the description of the PD device connected to port1.1 as "AP1".

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#power-inline description AP1
```

5.3.4 Set PoE port power supply priority

[Syntax]

power-inline priority *priority*
no power-inline priority

[Parameter]

priority : Power supply priority

Setting value	Description
critical	Highest
high	High
low	Low

[Initial value]

power-inline priority low

[Input mode]

interface mode

[Description]

Sets the power supply priority for PoE port.

Power supply is prioritized for the newer port numbers between PoE port that have the same priority.

If the amount of power used by the PoE power supply has exceeded the maximum, power supply will stop for the port with the lowest priority.

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

This command is supported only on the SWX2220P-18NT and SWX2220P-26NT.

[Note]

Power supply priority is shown using the **show power-inline** command.

If an LLDP frame that includes power via MDI TLV is received from a PD device, the unit operates according to the power supply priority in the LLDP frame, regardless of the settings of this command.

[Example]

Set the power supply priority for port1.5 to high.

```
SWX2210P(config)#interface port1.5
SWX2210P(config-if)#power-inline priority high
```

5.3.5 Guard band settings

[Syntax]

power-inline guardband *watts*
no power-inline guardband

[Parameter]

watts : <0-30>
Guard band value (W)

[Initial value]

power-inline guardband 7

[Input mode]

global configuration mode

[Description]

Sets the guard band.

The guard band serves as a margin in respect to the overall power supply amount, preventing unintended interruptions in power.

If the amount of usable power is equal to or less than the guard band, power will not be supplied even if a new PD device is connected to PoE port.

The guard band will not operate if "0W" is specified.

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

This command is supported only on the SWX2220P-18NT and SWX2220P-26NT.

[Example]

Sets the guard band to 30W.

```
SWX2210P(config)#power-inline guardband 30
```

Disables the guard band.

```
SWX2210P(config)#power-inline guardband 0
```

Resets the guard band to default values.

```
SWX2210P(config)#no power-inline guardband
```

5.3.6 Show PoE power supply information

[Syntax]

show power-inline
show power-inline interface *ifname*

[Parameter]

ifname : PoE port

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the PoE port power supply information.

Shows detailed information for the specified PoE port if *ifname* is specified.

[Example]

Shows the PoE power supply information.

```
SWX2210P#show power-inline
PoE Status
  Available Power : 124000 mW
  Used Power      :  66400 mW
  Remaining Power :  57600 mW
  Guard Band      :   7000 mW
  Operation Status: Enable

PoE Interface
  Interface Admin    Pri   Oper       Power Class  Max    Description
                                      (mW)         (mW)
================================================================================
  Port1.1   Enable   Cri   Powered    22100     4  30000   n/a
  Port1.2   Enable   Low   Standby        0   n/a  30000   n/a
  Port1.3   Enable   High  Powered    22100     4  30000   n/a
  Port1.4   Enable   Low   Standby        0   n/a  30000   n/a
  Port1.5   Enable   Low   Powered    22200     4  30000   n/a
  Port1.6   Enable   Low   Standby        0   n/a  30000   n/a
  Port1.7   Enable   Low   Standby        0   n/a  30000   n/a
  Port1.8   Enable   Low   Standby        0   n/a  30000   n/a
```

This shows power supply information for port1.1.

```
SWX2210P#show power-inline interface port1.1
PoE Status
  Available Power : 124000 mW
  Used Power      :  66400 mW
  Remaining Power :  57600 mW
  Guard Band      :   7000 mW
  Operation Status: Enable

PoE Interface port1.1
  Powered device type       : n/a
  PoE admin                 : Enable
  Priority                  : Cri
  Detection status          : Powered
  Current power consumption :  22100 mW
  Powered device class      : 4
  Powered allocated         :  30000 mW
  Powered pairs             : Signal (Alternative A)
```

Chapter 6

Layer 2 functions

6.1 FDB (Forwarding Data Base)

6.1.1 Set MAC address learning function

[Syntax]

mac-address-table learning *switch*
no mac-address-table learning

[Parameter]

switch : MAC address learning function operation

Setting value	Description
enable	Enables MAC address learning function
disable	Disables MAC address learning function

[Initial value]

mac-address-table learning enable

[Input mode]

global configuration mode

[Description]

Enables/disables the MAC address learning function.

If this is executed with the "no"syntax, the MAC address learning function is enabled.

[Note]

If the MAC address learning function is disabled, a dynamic entry is not registered in the MAC address table even if a frame is received.

[Example]

Disable the MAC address learning function.

```
SWX2210P(config)#mac-address-table learning disable
```

6.1.2 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.

```
SWX2210P(config)#mac-address-table ageing-time 600
```

6.1.3 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*

[Keyword]

address	:	Specifies the MAC address
vlan	:	Specifies the VLAN ID
interface	:	Specifies the interface

[Parameter]

mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal)
		Applicable MAC address
ifname	:	Name of LAN port or logical interface
		Applicable interface
vlan-id	:	<1-4094>
		Applicable VLAN ID

[Input mode]

privileged 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.

```
SWX2210P#clear mac-address-table dynamic address 00a0.de11.2233
```

6.1.4 Set static entry

[Syntax]

mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]
no mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]

[Keyword]

vlan	:	Specifies the VLAN ID

[Parameter]

mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal)
		Applicable MAC address
action	:	Action applied to frames addressed to mac-addr

Setting value	Description
forward	Forward
discard	Discard

ifname : Name of LAN 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.

```
SWX2210P(config)#mac-address-table static 00a0.de11.2233 forward port1.2
```

6.1.5 Show MAC address table

[Syntax]

show mac-address-table

[Input mode]

unprivileged EXEC mode, privileged 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.

```
SWX2210P>show mac-address-table
VLAN  port      mac             fwd      type     timeout
   1  port1.1   00a0.de11.2233  forward  static         0
```

```
  1   sa1         1803.731e.8c2b  forward  dynamic     300
  1   sa2         782b.cbcb.218d  forward  dynamic     300
```

6.2 VLAN

6.2.1 Move to VLAN mode

[Syntax]

vlan database

[Input mode]

global configuration mode, individual 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 privileged EXEC mode, use the **end** command.

[Example]

Move to VLAN mode.

```
SWX2210P(config)#vlan database
SWX2210P(config-vlan)#
```

6.2.2 Set VLAN interface

[Syntax]

vlan *vlan-id* [name *name*] [state *state*]
no vlan *vlan-id*

[Keyword]

name	:	Specifies the name of the VLAN
state	:	Specifies the state of the VLAN

[Parameter]

vlan-id	:	<2-4094> VLAN ID
name	:	Single-byte alphanumeric characters and single-byte symbols(32characters or less) Name of the VLAN
state	:	Whether frame forwarding is enabled or disabled

Setting value	Description
enable	Frames are forwarded
disable	Frames are not forwarded

[Initial value]

none

[Input mode]

VLAN mode

[Description]

Sets the VLAN interface.

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

If "name" is omitted, the name of the VLAN is specified as "VLANxxxx" (xxxx is the four-digit VLAN ID).

If "state" is omitted, "enable" is specified.

[Note]

If this command is executed with "name" omitted for a VLAN ID for which *name* is already specified, the already-specified *name* is not changed.

Multiple VLAN IDs can be specified for *vlan-id*. However, if multiple VLAN IDs are specified, the name cannot be specified.

To specify multiple items, use "-" or "," as shown below

- To select from VLAN #2 through VLAN #4: 2-4
- To select VLAN #2 and VLAN #4: 2,4

[Example]

Set VLAN #1000 with the name "Sales".

```
SWX2210P(config-vlan)#vlan 1000 name Sales
```

6.2.3 Set access port (untagged port)

[Syntax]

switchport mode access

[Initial value]

switchport mode access

[Input mode]

interface mode

[Description]

Specifies the port type of the applicable interface as an access port.

[Note]

This command can be specified only for LAN port and logical interface.

If this command is applied to a logical interface, the settings of every LAN 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.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#switchport mode access
```

6.2.4 Set associated VLAN of an access port (untagged port)

[Syntax]

switchport access vlan *vlan-id*
no switchport access vlan

[Parameter]

vlan-id	:	<1-4094>
		Associated VLAN ID

[Initial value]

switchport access vlan 1

[Input mode]

interface mode

[Description]

Sets the VLAN ID that is associated as an access port with the applicable interface.

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

[Note]

This command can be set only for a LAN 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 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.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#switchport access vlan 10
```

6.2.5 Set trunk port (tagged port)

[Syntax]

switchport mode trunk [ingress-filter *action*]

[Keyword]

ingress-filter : Specifies the behavior of the ingress filter

[Parameter]

action : Behavior of the ingress filter

Setting value	Description
enable	Enable the ingress filter
disable	Disable the ingress filter

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the port type of the applicable interface as an trunk port.

If "ingress-filter" is omitted, "enable" is specified.

If ingress filtering is enabled, frames are forwarded only if the VLAN ID of the received frame matches the VLAN associated with the interface.

If ingress filtering is disabled, all frames are forwarded.

[Note]

This command can be specified only for LAN port and logical interface.

If this command is applied to a logical interface, the settings of every LAN 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.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#switchport mode trunk
```

6.2.6 Set associated VLAN for trunk port (tagged port)

[Syntax]

switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add *vlan-ids*
switchport trunk allowed vlan except *vlan-ids*
switchport trunk allowed vlan remove *vlan-ids*
no switchport trunk

[Keyword]

all : vlanAssociate to all VLANs that are set by the vlan command

none	:	Dissociate from all VLANs
add	:	Associate to the specified VLAN
except	:	Associate to all VLANs that are set by the vlan command except for the specified
remove	:	Dissociate from the specified VLAN

[Parameter]

vlan-ids	:	<1-4094> VLAN ID set by the **vlan** command To specify multiple items, use "-" or "," as shown below • To select from VLAN #2 through VLAN #4: 2-4 • To select VLAN #2 and VLAN #4: 2,4

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the VLAN ID that is associated as a trunk port with the applicable interface.

If this is executed with the "no" syntax, all associated VLAN IDs are deleted and the port type is changed to access port.

[Note]

This command can be set only for a LAN 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 port associated with that interface are changed.

If the port type is changed to access port, the setting of this command returns to the default setting.

If this is set with "all" or "except" specified, the content of a subsequently changed **vlan** command is always applied.

If this is set with "all" or "except" specified, making the following settings will change the remaining affiliated VLAN IDs to the settings that were specified by "add."

- If you specify "remove" to delete a VLAN ID that is associated
- If you use the **switchport trunk native vlan** command to specify an associated VLAN ID

If you make this setting with "except" specified, and then associate the VLAN ID that had been excluded by specifying "add", the associated VLAN ID is changed to the setting specified by "add".

If you specify "remove" and then specify an unassociated VLAN ID, an error occurs.

For the setting of this command and the **switchport trunk native vlan** command, the last-specified command takes priority.

- If you use the **switchport trunk native vlan** command to specify a VLAN ID that was associated by this command, it is removed from the specified VLAN ID.
- If you specify and associate a VLAN ID that was set by the **switchport trunk native vlan** command, **switchport trunk native vlan none** is set.

[Example]

Set LAN port #1 as the trunk port, and associate it to VLAN #2.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#switchport mode trunk
SWX2210P(config-if)#switchport trunk allowed vlan add 2
```

6.2.7 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 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 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.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#switchport mode trunk
SWX2210P(config-if)#switchport trunk native vlan 2
```

6.2.8 Set multiple VALN

[Syntax]

switchport multiple-vlan group *group*
switchport multiple-vlan *group*
no switchport multiple-vlan_group *group*
no switchport multiple-vlan *group*

[Parameter]

group : 1-N (up to the maximum number of ports)

Group number

[Initial value]

none

[Input mode]

interface mode

[Description]

Specify the group of multiple VLAN associated with the applicable interface.

If a group is specified for the interface, communication can only be made for the interface in question when the VLAN is the same and multiple VLAN groups are between the same interface. Even if the VLAN is the same, communication is not possible if the multiple VLAN group differs.

By default, each interface is not associated with a multiple VLAN group.

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

[Note]

This command can be specified only for LAN port and logical interface.

[Example]

Assign LAN port #1 to multiple VLAN group #10.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#switchport multiple-vlan group 10
```

6.2.9 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, privileged 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
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.

```
SWX2210P>show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID Name                            State   Member ports
======= ================================ ======= ================================
1       default                         ACTIVE  port1.1(u) port1.2(u) port1.3(u)
                                                port1.4(u) port1.5(u) port1.6(u)
                                                port1.7(u) port1.8(u) port1.9(u)
                                                port1.10(u) sa1(u)
```

6.3 Loop detection

6.3.1 Set loop detection function (system)

[Syntax]

loop-detect *switch*
no loop-detect

[Parameter]

switch : Set system-wide loop detection function

Setting value	Description
enable	Enable system-wide loop detection function
disable	Disable system-wide loop detection function

[Initial value]

loop-detect disable

[Input mode]

global configuration mode

[Description]

Enables or disables the system-wide loop detection function.

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

[Note]

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 port that is operating as a sniffer port for the mirroring function
- LAN port that is inside a logical interface

[Example]

Enable the loop detection function for the entire system.

```
SWX2210P(config)#loop-detect enable
```

Disable the loop detection function for the entire system.

```
SWX2210P(config)#loop-detect disable
```

6.3.2 Set loop detection function (interface)

[Syntax]

loop-detect *switch*
no loop-detect

[Parameter]

switch : Set loop detection function for the applicable interface

Setting value	Description
enable	Enable loop detection function for the applicable interface
disable	Disable loop detection function for the applicable interface

[Initial value]

loop-detect enable

[Input mode]

interface mode

[Description]

Enables or disables loop detection function for the applicable interface.

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

[Note]

This command can be specified only for LAN 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 port that is operating as a sniffer port for the mirroring function
- LAN port that is inside a logical interface

[Example]

Enable the loop detection function of LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#loop-detect enable
```

Disable the loop detection function of LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#loop-detect disable
```

6.3.3 Set duration of port blocking via loop detection

[Syntax]

loop-detect blocking interval *interval*
no loop-detect blocking interval

[Parameter]

interval : <300-3600>
Time between loop clearing detection (seconds)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Normally, Blocking is released immediately when the loop is cleared.

When this command is configured, it detects if the loop is cleared at regular intervals.

If the loop is cleared, Blocking is released, but if the loop is not cleared, Blocking continues until that time passes again.

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

[Note]

If a port in the Port Blocking state goes link down, the Port Blocking is removed immediately.

[Example]

Set the Port Blocking loop clearing detection interval to 300 seconds.

```
SWX2210P(config)#loop-detect blocking interval 300
```

6.3.4 Reset loop detection status

[Syntax]

loop-detect reset

[Input mode]

privileged 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.

```
SWX2210P#loop-detect reset
```

6.3.5 Show loop detection function status

[Syntax]

show loop-detect

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the settings and status of the loop detection function.

The following content is displayed.

- System-wide loop detection function setting
- Interval time for checking that Port Blocking loops have been resolved ("Auto" or "N seconds")
- Loop detection status for each LAN port
  - Interface name (port)
  - Setting of the loop detection function (loop-detect) for LAN port. If the loop detection function is operating, (*) is added
  - Loop detection status (status)

[Example]

Shows the loop detection status.

```
SWX2210P>show loop-detect
loop-detect: Enable
blocking interval: 300 seconds

port        loop-detect         status
----------------------------------------
port1.1        enable           Normal
port1.2        enable           Normal
port1.3        enable(*)        Normal
port1.4        enable           Normal
port1.5        enable(*)        Detected
port1.6        enable(*)        Normal
port1.7        enable(*)        Blocking
port1.8        enable(*)        Normal
port1.9        enable(*)        Normal
port1.10       enable           Normal
```

Chapter 7

Layer 3 functions

7.1 IPv4 address management

7.1.1 Set IPv4 address

[Syntax]

ip address *ip_address*/*mask* [label *textline*]

[Keyword]

label	:	Set label for IPv4 address

[Parameter]

ip_address	:	A.B.C.D
		IPv4 address
mask	:	<1-31>
		Number of mask bits
textline	:	Label (maximum 64 characters)

[Initial value]

ip address 192.168.100.240/24 *VLAN #1 only

[Input mode]

interface mode

[Description]

Specifies the IPv4 address and net mask for the VLAN interface.

IPv4 addresses can be assigned to a maximum of 1 VLAN interfaces.

If a **ip address** or **ip address dhcp** command has already been specified for different VLAN interface when the **ip address** or **ip address dhcp** has been set for a VLAN interface, the old settings are deleted.

You cannot delete the IPv4 address using the "no" syntax.

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

When executing this command, a confirmation message is shown that confirms whether to change the IPv4 address.

If the IPv4 address is changed, the following commands are deleted.

- **telnet-server access**
- **http-server access**
- **tftp-server access**
- **snmp-server access**

[Example]

Specifies 192.168.1.100 as the IPv4 address for VLAN #1.

```
SWX2210P(config)#interface vlan1
SWX2210P(config-if)#ip address 192.168.1.100/24
Do you really want to change IP address? [y/N]: y
```

7.1.2 Show IPv4 address

[Syntax]

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

[Parameter]

interface	:	VLAN interface name

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the IPv4 address for each interface.

The following content is displayed.

- IPv4 address
  - If an IPv4 address has been specified dynamically by the **ip address dhcp** command, an "*" is shown added before the IPv4 address.
  - If the **ip address** command has not been set, the indication "unassigned" is shown.
- Physical layer status
- Data link layer status

If an interface is specified, information for that interface is shown. If the interface is omitted, information is shown for all interfaces for which an IPv4 address can be specified.

[Note]

An error occurs if the specified interface is one to which an IPv4 address cannot be assigned.

[Example]

Shows the IPv4 address of every VLAN interface.

```
SWX2210P>show ip interface brief
Interface            IP-Address               Admin-Status          Link-Status
vlan1                192.168.1.100/24         up                    up
vlan2                unassigned               up                    down
```

7.1.3 Automatically set dynamic IPv4 address with a DHCP client

[Syntax]

ip address dhcp [hostname *hostname*]

[Keyword]

hostname	:	Set host name of DHCP client

[Parameter]

hostname	:	Text string used for the host name

[Initial value]

None

[Input mode]

interface mode

[Description]

This uses the DHCP client to assign the IPv4 address granted by the DHCP server to the VLAN interface.

If the host name is specified, the HostName option (option code 12) can be added to the Discover/Request message.

If an IPv4 address has been obtained and you execute the **ip address** command, this sends a release message for the obtained IP address to the DHCP server.

IPv4 addresses can be assigned to a maximum of 1 VLAN interfaces.

You cannot delete the DHCP client setting using the "no" syntax.

When executing this command, a confirmation message is shown that confirms whether to change the IPv4 address.

If the IPv4 address is changed, the following commands are deleted.

- **telnet-server access**
- **http-server access**
- **tftp-server access**
- **snmp-server access**

[Note]

The lease time requested from the DHCP server is fixed at 72 hours. However, the actual lease time will depend on the setting of the DHCP server.

Even if this command is used to obtain the default gateway, DNS server, and default domain name from the DHCP server, the settings of the **ip route, dns-client name-server and dns-client domain-name**commands take priority.

If an IPv4 address cannot be obtained from the DHCP server even by using this command, then an IPv4 link local address (169.254.xxx.xxx/16) is automatically assigned using the Auto IP function.

If an IPv4 address could be obtained from the DHCP server after the IPv4 link local address was generated, the IPv4 address obtained from the DHCP server is used.

[Example]

Use the DHCP client to assign an IPv4 address to VLAN #100.

```
SWX2210P(config)#interface vlan100
SWX2210P(config-if)#ip address dhcp
Do you really want to change IP address? [y/N]: y
```

7.1.4 Show DHCP client status

[Syntax]

show dhcp lease

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the DHCP client status. The following items are shown.

- Interface operating as a DHCP client
- Assigned IPv4 address
- Lease expiration time
- Lease renewal request time
- Lease rebinding time
- DHCP server name
- Information obtained as DHCP option
  - Net mask
  - Default gateway
  - Lease time
  - DNS server
  - DHCP server ID
  - Domain name

[Example]

Shows the DHCP client status.

```
SWX2210P>show dhcp lease
Interface vlan1
------------------------------------------------------------------------------
IP Address:                    192.168.100.2
Expires:                       2018/01/01 00:00:00
Renew:                         2018/01/01 00:00:00
Rebind:                        2018/01/01 00:00:00
Server:
Options:
  subnet-mask                  255.255.255.0
  default-gateway              192.168.100.1
  dhcp-lease-time              259200
  domain-name-servers          192.168.100.1
  dhcp-server-identifier       192.168.100.1
  domain-name                  example.com
```

7.2 IPv4 route control

7.2.1 Set IPv4 static route

[Syntax]

ip route 0.0.0.0/0 *gateway*
ip route 0.0.0.0 0.0.0.0 *gateway*
no ip route 0.0.0.0/0 [*gateway*]

no ip route 0.0.0.0 0.0.0.0 [*gateway*]

[Parameter]

gateway	:	A.B.C.D IPv4 address of gateway

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Adds a static route for IPv4.

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

[Example]

Set the default gateway to 192.168.1.1.

```
SWX2210P(config)#ip route 0.0.0.0/0 192.168.1.1
```

7.2.2 Show IPv4 forwarding table (route)

[Syntax]

show ip route

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the IPv4 forwarding table (FIB: Forwarding Information Base).

[Example]

Show the IPv4 forwarding table.

```
SWX2210P>show ip route
Codes: C - connected, S - static
       * - candidate default

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.1.1, vlan1
C       192.168.1.0 is directly connected, vlan1
```

7.3 ARP

7.3.1 Show ARP table

[Syntax]

show arp

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show the ARP cache.

Shows in ascending order of IP address.

[Example]

Show the ARP cache.

```
SWX2210P>show arp
 IP Address      MAC Address      Interface  Type
192.168.100.10  00a0.de00.0000    vlan1      Dynamic
192.168.100.100 00a0.de00.0001    vlan1      Dynamic
```

7.3.2 Clear ARP table

[Syntax]

clear arp-cache

[Input mode]

privileged EXEC mode

[Description]

Clear the ARP cache.

[Example]

Clear the ARP cache.

```
SWX2210P#clear arp-cache
```

7.3.3 Set ARP timeout

[Syntax]

arp-ageing-timeout *time*
no arp-ageing-timeout [*time*]

[Parameter]

time	:	<1-3000>
		ARP entry 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.

```
SWX2210P(config)#interface vlan1
SWX2210P(config-if)#arp-aging-timeout 300
```

7.4 IPv4 ping

7.4.1 IPv4 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]

privileged 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.

```
SWX2210P#ping 192.168.100.254 repeat 3 size 120
PING 192.168.100.254 (192.168.100.254): 120 data bytes
120 bytes from :192.168.100.254, seq=0 ttl=64 time= 8 ms
120 bytes from :192.168.100.254, seq=1 ttl=64 time= 9 ms
120 bytes from :192.168.100.254, seq=2 ttl=64 time=10 ms


--- 192.168.100.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 8/9.00/10 ms
```

7.5 IPv6 address management

7.5.1 Set IPv6

[Syntax]

ipv6 *switch*

no ipv6

[Parameter]

switch : IPv6 operation

Setting value	Description
enable	Enables IPv6
disable	Disables IPv6

[Initial value]

ipv6 disable

[Input mode]

interface mode

[Description]

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

IPv6 can be enabled with a maximum of 1 VLAN interface.

If an **ipv6 address** command has already been specified for a different VLAN interface when the **ipv6 enable** command has been set for a VLAN interface, the old settings are deleted.

If IPv6 is disabled, the related settings are also simultaneously deleted.

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

[Note]

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

[Example]

Enable IPv6 for VLAN #1.

```
SWX2210P(config)#interface vlan1
SWX2210P(config-if)#ipv6 enable
```

7.5.2 Set IPv6 address

[Syntax]

ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address [*ipv6_address*/*prefix_len*]

[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.

An IPv6 address can be set for a VLAN interface for which the **ipv6 enable** command has been set.

One global address and one link local address can be set for one VLAN interface.

If the **ipv6 address autoconfig** command was specified, the setting of the "ipv6 address autoconfig" command is automatically deleted.

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

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

If the IPv6 address is changed, the following commands are deleted.

- **telnet-server access**
- **http-server access**
- **tftp-server access**
- **snmp-server access**

[Example]

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

```
SWX2210P(config)#interface vlan1
SWX2210P(config-if)#ipv6 address 2001:db8:1::2/64
```

7.5.3 Set RA for IPv6 address

[Syntax]

ipv6 address autoconfig
no ipv6 address

[Initial value]

None

[Input mode]

interface mode

[Description]

Uses RA to specify the IPv6 address for the VLAN interface.

RA can be set for a VLAN interface for which the **ipv6 enable** command has been set.

If the **ipv6 address ipv6_address/prefix_len** command is specified when this command is set, 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.

If the IPv6 address is changed, the following commands are deleted.

- **telnet-server access**
- **http-server access**
- **tftp-server access**
- **snmp-server access**

[Example]

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

```
SWX2210P(config)#interface vlan1
SWX2210P(config-if)#ipv6 address autoconfig
```

7.5.4 Show IPv6 address

[Syntax]

show ipv6 interface [*interface*] **brief**

[Parameter]

interface : VLAN interface name

Interface to show

[Input mode]

unprivileged EXEC mode、privileged 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.

[Example]

Shows the IPv6 address of every VLAN interface.

```
SWX2210P>show ipv6 interface brief
Interface        IPv6-Address                              Admin-Status
Link-Status
vlan1            2001:db8:1::2/64
                 fe80::2a0:deff:fe:2/64                    up                    up
vlan2            unassigned                                up
down
```

7.6 IPv6 route control

7.6.1 Set IPv6 static route

[Syntax]

ipv6 route ::/**0** *gateway*
ipv6 route 0:**0**:**0**:**0**:**0**:**0**:**0**:**0**/**0** *gateway*
no ipv6 route ::/**0** [*gateway*]
no ipv6 route 0:**0**:**0**:**0**:**0**:**0**:**0**:**0**/**0** [*gateway*]

[Parameter]

gateway : X:X::X:X

IPv6 address of gateway

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

[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]

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

```
SWX2210P(config)#ipv6 route ::/0 fe80::2a0:deff:fe:1%vlan1
```

7.6.2 Show IPv6 forwarding table (route)

[Syntax]

show ipv6 route

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the IPv6 forwarding table (FIB: Forwarding Information Base).

[Example]

Show the IPv6 forwarding table.

```
SWX2210P>show ipv6 route
Codes: C - connected, S - static
Timers: Uptime

S     ::/0 via 2002:db8:1::1, vlan1, 00:00:03
C     ::/0 via fe80::2a0:deff:fe67:dd1d, vlan1, 00:21:17
C     2001::/64 via ::, vlan1, 00:21:17
C     fe80::/64 via ::, vlan1, 00:23:28
```

7.7 Neighbor cache

7.7.1 Show neighbor cache table

[Syntax]

show ipv6 neighbors

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the neighbor cache table.

[Example]

Show the neighbor cache table.

```
SWX2210P>show ipv6 neighbors
 IPv6 Address                              MAC Address     Interface  Type
2001:db8:1:0:3538:5dc7:6bc4:1a23          0011.2233.4455   vlan1      dynamic
2001:db8:cafe::1                          00a0.de80.cafe   vlan1      dynamic
fe80::0211:22ff:fe33:4455                 0011.2233.4455   vlan1      dynamic
fe80::6477:88ff:fe99:aabb                 6677.8899.aabb   vlan1      dynamic
```

7.7.2 Clear neighbor cache table

[Syntax]

clear ipv6 neighbors

[Input mode]

privileged EXEC mode

[Description]

Clears the neighbor cache.

[Example]

Clear the neighbor cache.

```
SWX2210P#clear ipv6 neighbors
```

7.8 IPv6 ping

7.8.1 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 (in bytes)
timeout	:	Specifies the time to wait for a reply after transmitting the specified number of Echo requests

[Parameter]

host : Host name or IPv6 address (X:X::X:X)

Destination to which ICMPv6 Echo is sent

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

count : Number of times to execute (if omitted: 5)

Setting value	Description
<1-2147483647>	Execute the specified number of times
continuous	Execute repeatedly until Ctrl+C is entered

datalen : <36-18024>

Length of 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]

privileged 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.

```
SWX2210P#ping6 fe80::2a0:deff:fe11:2233%vlan1
PING fe80::2a0:deff:fe11:2233%vlan1 (fe80::2a0:deff:fe11:2233): 56 data bytes
56 bytes from fe80::2a0:deff:fe11:2233: seq=0 ttl=64 time=2 ms
56 bytes from fe80::2a0:deff:fe11:2233: seq=1 ttl=64 time=4 ms
56 bytes from fe80::2a0:deff:fe11:2233: seq=2 ttl=64 time=10 ms
56 bytes from fe80::2a0:deff:fe11:2233: seq=3 ttl=64 time=10 ms
56 bytes from fe80::2a0:deff:fe11:2233: seq=4 ttl=64 time=10 ms

--- fe80::2a0:deff:fe11:2233%vlan1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2/7.20/10 ms
```

7.9 DNS client

7.9.1 Set DNS lookup function

[Syntax]

dns-client *switch*
no dns-client

[Parameter]

switch : DNS client operations

Setting value	Description
enable	Enable the DNS client
disable	Disable the DNS client

[Initial value]

dns-client disable

[Input mode]

global configuration mode

[Description]

Enables or disables the DNS query function.

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

[Note]

When the **dns-client** command is specified, only settings via the **dns-client domain-name**, **dns-client domain-list** and **dns-client name-server** commands are disabled. Domain names or DNS server IP addresses obtained from a DHCP server with the "ip address dhcp" command are not disabled.

[Example]

Enable the DNS lookup function.

```
SWX2210P(config)#dns-client enable
```

7.9.2 Set DNS server list

[Syntax]

dns-client name-server *server*
no dns-client 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

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

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Adds a server to the DNS server list.

Up to three servers can be specified.

If this command is executed with the "no" syntax, the specified server is deleted from the DNS server list.

[Note]

If the **ip address dhcp** 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.

```
SWX2210P(config)#dns-client name-server 192.168.100.1
SWX2210P(config)#dns-client name-server 2001:db8::1234
SWX2210P(config)#dns-client name-server fe80::2a0:deff:fe11:2233%vlan1
```

7.9.3 Set default domain name

[Syntax]

dns-client domain-name *name*
no dns-client domain-name *name*

[Parameter]

name : Domain name (maximum 255 characters)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Specifies the default domain name used for DNS queries.

If this command is executed with the "no" syntax, the default domain name is deleted.

[Note]

The setting of this command takes priority if the default domain name (option code 15) was obtained from the DHCP server by the "**ip address dhcp**" command.

If a query domain list is specified by the "**dns-client domain-list**" command, the default domain name specified by this command and the default domain name automatically specified by the "**ip address dhcp**" command are not used.

[Example]

Set the default domain name to example.com.

```
SWX2210P(config)#dns-client domain-name example.com
```

7.9.4 Set query domain list

[Syntax]

dns-client domain-list *name*
no dns-client domain-list *name*

[Parameter]

name : Domain name (maximum 255 characters)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Adds a domain name to the list of domain names used for DNS queries.

Up to six domains can be registered in the query domain list.

If this command is executed with the "no" syntax, the specified domain name is deleted from the query domain list.

[Note]

If a query domain list is specified by this command, the default domain name specified by the "**dns-client domain-name**" command and the default domain name automatically specified by the "**ip address dhcp**" command are not used.

[Example]

Add the domain names example1.com and example2.com to the query domain list.

```
SWX2210P(config)#dns-client domain-list example1.com
SWX2210P(config)#dns-client domain-list example2.com
```

7.9.5 Show DNS client information

[Syntax]

show dns-client

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the DNS client information.

The following content is displayed.

Item	Description
DNS Client is enabled	DNS client is enabled
DNS Client is disabled	DNS client is disabled
Default domain	Default domain name
Domain list	Query domain list
Name Servers	DNS server list (IP address)

[Example]

Shows the DNS client information.

```
SWX2210P>show dns-client

DNS client is enabled
 Default domain  : example.com
 Domain list     : example1.com example2.com
 Name Servers    : 192.168.100.1 2001:db8::1234 fe80::2a0:deff:fe11:2233%vlan1

 * - Values assigned by DHCP Client.
```

Chapter 8

IP multicast control

8.1 IP multicast basic settings

8.1.1 Set processing method for unknown multicast frames

[Syntax]

l2-unknown-mcast *mode*

[Parameter]

mode : Sets the processing method for multicast frames

Setting value	Description
discard	Discard
flood	Flood

[Initial value]

l2-unknown-mcast flood

[Input mode]

global configuration mode

[Description]

Specifies the processing method for multicast frames that are not registered in the MAC address table.

[Example]

Discard unknown multicast.

```
SWX2210P(config)#l2-unknown-mcast discard
```

8.1.2 Setting the processing method for unknown multicast frames (interface)

[Syntax]

l2-unknown-mcast *mode*
no l2-unknown-mcast

[Parameter]

mode : Sets the processing method for multicast frames

Setting value	Description
discard	Discard
flood	Flood

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the processing method for multicast frames received by the VLAN interface, which are not registered in the MAC address table.

If this command is executed with the "no" syntax, the setting returns to its default value, the system-wide processing method for unknown multicast frames is used.

[Note]

This command can be specified only for VLAN interfaces.

This command is prioritized over the settings for the system-wide processing method for unknown multicast frames.

[Example]

This discards the multicast frames received by VLAN #1 that are not registered in the MAC address table.

```
SWX2210P(config)#interface vlan1
SWX2210P(config-if)#l2-unknown-mcast discard
```

8.1.3 Forwarding setting for link local multicast frames

[Syntax]

l2-unknown-mcast forward link-local
no l2-unknown-mcast forward link-local

[Initial value]

None

[Input mode]

global configuration mode

[Description]

When l2-unknown-mcast discard is set, the frame for the link local multicast address is forwarded without being discarded.

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

[Note]

The link local multicast address for this command falls within the ranges shown below.

- IPv4: 224.0.0.0/24
- IPv6: ff02::/112

[Example]

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

```
SWX2210P(config)#l2-unknown-mcast discard
SWX2210P(config)#l2-unknown-mcast forward link-local
```

8.1.4 Forwarding setting for multicast frames

[Syntax]

l2-mcast flood *ipv4_addr*
no l2-mcast flood *ipv4_addr*

[Parameter]

ipv4_addr	:	A.B.C.D IPv4 multicast address

[Initial value]

None

[Input mode]

interface mode

[Description]

Floods the frames with the IPv4 multicast address specified by the destination in multicast traffic received by the VLAN interface.

Up to 100 instances of this command can be set system-wide.

If this command is executed with the "no" syntax, the specified IPv4 multicast address settings are deleted.

If no IPv4 multicast address is specified, all settings are deleted.

[Note]

This command can be specified only for VLAN interfaces.

The IPv4 multicast address specified by this command is excluded from IGMP snooping.

[Example]

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

```
SWX2210P(config)#interface vlan1
SWX2210P(config-if)#l2-mcast flood 224.0.0.251
```

8.2 IGMP snooping

8.2.1 Set enable/disable IGMP snooping

[Syntax]

ip igmp snooping *switch*
no ip igmp snooping

[Parameter]

switch : IGMP snooping operations

Setting value	Description
enable	Enable IGMP snooping
disable	Disable IGMP snooping

[Initial value]

ip igmp snooping enable

[Input mode]

interface mode

[Description]

Enables the IGMP snooping setting of the interface.

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

[Note]

This command can be specified only for VLAN interface.

[Example]

Enable IGMP snooping for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping enable
```

Disable IGMP snooping for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping disable
```

8.2.2 Set IGMP snooping fast-leave

[Syntax]

ip igmp snooping fast-leave [auto-assignment]
no ip igmp snooping fast-leave

[Keyword]

auto-assignment : If the switch is connected to and controlled by the LAN/SFP port, the fast-leave function is disabled.

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables IGMP snooping fast-leave for the interface.

If this is executed with the "no" syntax, IGMP snooping fast-leave is disabled.

If the switch is connected to and controlled by the LAN/SFP port when the auto-assignment option is specified, the fast-leave function is automatically disabled only for that port.

If it cannot be determined whether there is a switch connected to and controlled by LAN/SFP port, the determination is made based on whether "Bridge" is included in the "System Capabilities" of the basic management TLV for the LLDP frame that's received at the relevant port.

[Note]

This command can be specified only for VLAN interface.

On a VLAN interface for which multiple hosts are connected to the LAN/SFP port, use this command to either enable the auto-assignment option or disable the fast-leave function altogether.

[Example]

Enable IGMP snooping fast-leave for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping fast-leave
```

Disable IGMP snooping fast-leave for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ip igmp snooping fast-leave
```

8.2.3 Set multicast router connection destination

[Syntax]

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

[Parameter]

ifname	:	LAN port interface name Interface to set

[Initial value]

none

[Input mode]

interface mode

[Description]

Statically sets the LAN port to which the multicast router is connected.

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

[Note]

This command can be specified only for VLAN interface.

The multicast router must be connected to the specified LAN port. If an IGMP report is received from the receiver, it is forwarded to the specified LAN port.

[Example]

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping mrouter interface port1.8
```

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ip igmp snooping mrouter interface port1.8
```

8.2.4 Set query transmission function

[Syntax]

ip igmp snooping querier
no ip igmp snooping querier

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the IGMP query transmission function.

If this is executed with the "no" syntax, the IGMP query transmission function is disabled.

[Note]

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

Note that if you change the IP address while leaving this command enabled, queries will no longer be sent with the correct IP address following the change.

[Example]

Enable the transmission function for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping querier
```

Disable the transmission function for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ip igmp snooping querier
```

8.2.5 Set IGMP query transmission interval

[Syntax]

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

[Parameter]

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

[Initial value]

ip igmp snooping query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for IGMP queries.

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

[Note]

This command can be specified only for VLAN interface.

[Example]

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping query-interval 30
```

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ip igmp snooping query-interval
```

8.2.6 Set TTL value verification function for IGMP packets

[Syntax]

ip igmp snooping check ttl *switch*

no ip igmp snooping check ttl

[Parameter]

switch : TTL value verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check ttl enable

[Input mode]

interface mode

[Description]

Sets the TTL value verification function for IGMP packets.

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

When this is enabled, IGMP packets with illegal TTL values in the IP header (besides 1) will be discarded.

When disabled, the relevant packet will be discarded, and the TTL value will be corrected to 1 and forwarded.

[Note]

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

[Example]

Enable the TTL value verification function of IGMP packets for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping check ttl enable
```

Disnable the TTL value verification function of IGMP packets for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping check ttl disable
```

8.2.7 Set RA verification function for IGMP packets

[Syntax]

ip igmp snooping check ra *switch*
no ip igmp snooping check ra

[Parameter]

switch : RA verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check ra disable

[Input mode]

interface mode

[Description]

Sets the RA verification function for IGMPv2/IGMPv3 packets.

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

If this is enabled, IGMPv2/IGMPv3 packets whose IP headers do not include an RA (Router Alert) option are discarded.

When disabled, the relevant packet is not discarded; instead, an RA option is added to the IP header and the packet is forwarded.

[Note]

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

[Example]

Enable the RA verification function of IGMP packets for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping check ra enable
```

Disnable the RA verification function of IGMP packets for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping check ra disable
```

8.2.8 Set ToS verification function for IGMP packets

[Syntax]

ip igmp snooping check tos *switch*
no ip igmp snooping check tos

[Parameter]

switch : ToS verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check tos disable

[Input mode]

interface mode

[Description]

Sets the ToS verification function for IGMP packets.

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

When this is enabled, IGMPv3 packets with illegal ToS in the IP header (besides 0xc0) will be discarded.

When disabled, the relevant packets are not discarded; instead, the ToS will be corrected to 0xc0 and forwarded.

[Note]

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

[Example]

Enable the ToS verification function of IGMP packets for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping check tos enable
```

Disnable the ToS verification function of IGMP packets for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping check tos disable
```

8.2.9 Set IGMP version

[Syntax]

ip igmp snooping version *version*
no ip igmp snooping version

[Parameter]

version : <2-3>

IGMP version

[Initial value]

ip igmp snooping version 3

[Input mode]

interface mode

[Description]

Sets the IGMP version.

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

[Note]

This command can be specified only for VLAN interface. 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.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping version 2
```

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ip igmp snooping version
```

8.2.10 Settings for IGMP Report Suppression

[Syntax]

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

[Parameter]

switch : IGMP report suppression

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping report-suppression enable

[Input mode]

interface mode

[Description]

Configures IGMP report suppression.

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

When enabled, the minimum number of messages will be sent to the multicast router ports based on the information obtained from the received Report messages and Leave messages.

When disabled, the received Report messages and Leave messages will be sequentially transmitted to the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables IGMP report suppression at VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping report-suppression enable
```

Disables IGMP report suppression at VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping report-suppression disable
```

8.2.11 Set the IGMP report forwarding function

[Syntax]

ip igmp snooping report-forward *switch*
no ip igmp snooping report-forward

[Parameter]

switch : IGMP report forwarding function

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping report-forward disable

[Input mode]

interface mode

[Description]

This configures the IGMP report forwarding function.

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

When this is enabled and a switch is connected to and controlled by LAN/SFP port, an IGMP Report message or a Leave message is forwarded to that port, in addition to the multicast router port.

When disabled, the IGMP Report messages and Leave messages will be forwarded only to the multicast router port.

If it cannot be determined whether there is a switch connected to and controlled by LAN/SFP port, the determination is made based on whether "Bridge" is included in the "System Capabilities" of the basic management TLV for the LLDP frame that's received at the relevant port.

[Note]

This command can be specified only for VLAN interface.

[Example]

Enables the IGMP report forwarding function for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping report-forward enable
```

Disables the IGMP report forwarding function for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping report-forward disable
```

8.2.12 Settings for Suppression of Data Transmission to Multicast Router Ports

[Syntax]

ip igmp snooping mrouter-port data-suppression *switch*
no ip igmp snooping mrouter-port data-suppression

[Parameter]

switch : Suppression of data transmission to multicast router ports

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping mrouter-port data-suppression disable

[Input mode]

interface mode

[Description]

Configures suppression of data transmission to multicast router ports.

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

When enabled, the relevant data will be transmitted to the multicast router ports only when Report messages are received by the multicast router ports.

When disabled, the relevant data will be transmitted to the multicast router ports when Report messages are received by any of the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables suppression of data transmission to multicast router ports at VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping mrouter-port data-suppression enable
```

Disables suppression of data transmission to multicast router ports in VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ip igmp snooping mrouter-port data-suppression disable
```

8.2.13 Show multicast router connection port information

[Syntax]

show ip igmp snooping mrouter *ifname*

[Parameter]

ifname : VLAN interface name

Interface to show

[Input mode]

unprivileged EXEC mode, privileged 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.

```
SWX2210P#show ip igmp snooping mrouter vlan2
VLAN    Interface                IP-address            Expires
2       port1.8(dynamic)         192.168.100.216       00:00:49
```

8.2.14 Show IGMP group membership information

[Syntax]

show ip igmp snooping groups
show ip igmp snooping groups *A.B.C.D*
show ip igmp snooping groups *ifname*

[Parameter]

A.B.C.D	:	Multicast group address
ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows IGMP group membership information.

[Example]

Show IGMP group membership information.

```
SWX2210P#show ip igmp snooping groups
IGMP Snooping Group Membership
Vlan  Group Address   Interface  Uptime    Expires   Last Reporter   Version
1     239.255.255.250 port1.5    01:06:02  00:03:45  192.168.100.11  V3
```

8.2.15 Show an interface's IGMP-related information

[Syntax]

show ip igmp snooping interface *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows IGMP-related information for a VLAN interface.

[Example]

Show IGMP-related information for VLAN #1.

```
SWX2210P#show ip igmp snooping interface vlan1

IGMP Snooping information for vlan1
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2/v3 fast-leave is enabled
 IGMPv1/v2 Report suppression enabled
 IGMPv2/v3 fast-leave auto-assignment is enabled
 IGMPv3 Report suppression enabled
 IGMPv1/v2/v3 Report forwarding enabled
 IGMP Snooping check TTL is enabled
 IGMP Snooping check RA is enabled
 IGMP Snooping check ToS is enabled
 IGMP Snooping Mrouter-port Data suppression disabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 1
 Number of v1-reports: 0
 Number of v2-reports: 6
 Number of v2-leaves: 0
 Number of v3-reports: 127
 Number of v1-query-warnings: 0
 Number of v2-query-warnings: 0
 Number of v3-query-warnings: 0
 Active Ports:
  port1.1 (F,R)
  port1.2

  F - Fast-leave auto-assignment is enabled
```

```
R - Report forwarding is enabled
```

8.2.16 Clear IGMP group membership entries

[Syntax]

clear ip igmp snooping
clear ip igmp snooping group *A.B.C.D*
clear ip igmp snooping interface *ifname*

[Keyword]

group	:	Specifies the multicast group address to be cleared
interface	:	Specifies the VLAN interface to be cleared

[Parameter]

A.B.C.D	:	Multicast group address "*" indicates all entries
ifname	:	VLAN interface name Interface to clear

[Input mode]

privileged EXEC mode

[Description]

Clears IGMP group membership entries.

[Example]

Clear IGMP group membership entries for VLAN #1.

```
SWX2210P#clear ip igmp snooping interface vlan1
```

8.3 MLD snooping

8.3.1 Enable/disable MLD snooping

[Syntax]

ipv6 mld snooping *switch*
no ipv6 mld snooping

[Parameter]

switch : MLD snooping operations

Setting value	Description
enable	Enable MLD snooping
disable	Disable MLD snooping

[Initial value]

ipv6 mld snooping enable

[Input mode]

interface mode

[Description]

Configures the operations of the MLD snooping setting of the interface.

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

[Note]

This command can be specified only for VLAN interfaces.

[Example]

Enable MLD snooping for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping enable
```

Disnable MLD snooping for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping disable
```

8.3.2 Set MLD snooping fast-leave

[Syntax]

ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables MLD snooping fast-leave for the interface.

If this is executed with the "no" syntax, MLD snooping fast-leave is disabled.

[Note]

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

Do not enable this command on a VLAN interface for which multiple hosts are connected to the LAN/SFP port.

[Example]

Enable MLD snooping fast-leave for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping fast-leave
```

Disable MLD snooping fast-leave for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ipv6 mld snooping fast-leave
```

8.3.3 Set multicast router connection destination

[Syntax]

ipv6 mld snooping mrouter interface *ifname*
no ipv6 mld snooping mrouter interface *ifname*

[Parameter]

ifname	:	Interface name of LAN port Interface to set

[Initial value]

none

[Input mode]

interface mode

[Description]

Statically sets the LAN 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.

The multicast router must be connected to the specified LAN port. If an MLD report is received from the receiver, it is forwarded to the specified LAN port.

[Example]

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping mrouter interface port1.8
```

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ipv6 mld snooping mrouter interface port1.8
```

8.3.4 Set query transmission function

[Syntax]

ipv6 mld snooping querier
no ipv6 mld snooping querier

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the MLD query transmission function.

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

[Note]

This command can be specified only forVLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

When using this command, you must specify the **ipv6 enable** command for one of the VLAN interfaces. Note that if the **ipv6 enable** command has not been specified, MLD query is not transmitted.

[Example]

Enable the MLD query transmission function for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping querier
```

Disable the MLD query transmission function for VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ipv6 mld snooping querier
```

8.3.5 Set MLD query transmission interval

[Syntax]

ipv6 mld snooping query-interval *interval*
no ipv6 mld snooping query-interval

[Parameter]

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

[Initial value]

ipv6 mld snooping query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for MLD queries.

If this command is executed with the "no" syntax, the MLD query transmission interval is returned to the default setting.

[Note]

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

[Example]

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping query-interval 30
```

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ipv6 mld snooping query-interval
```

8.3.6 Set MLD version

[Syntax]

ipv6 mld snooping version *version*
no ipv6 mld snooping version

[Parameter]

version : <1-2>
MLD version

[Initial value]

ipv6 mld snooping version 2

[Input mode]

interface mode

[Description]

Sets the MLD version.

If this command is executed with the "no" syntax, the MLD version returns to the default setting (V2).

[Note]

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

If an MLD packet of a different version than this setting is received, the following action occurs.

- If V1 is specified
  - If a V2 query is received, it is forwarded as a V1 query
  - If a V2 report is received, it is discarded
- If V2 is specified
  - If a V1 query is received, it is forwarded as a V1 query
  - If a V1 report is received, it is forwarded as a V2 report

[Example]

On VLAN #2, set the MLD version to 1.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping version 1
```

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

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#no ipv6 mld snooping version
```

8.3.7 Settings for MLD Report Suppression

[Syntax]

ipv6 mld snooping report-suppression *switch*
no ipv6 mld snooping report-suppression

[Parameter]

switch : MLD report suppression

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ipv6 mld snooping report-suppression enable

[Input mode]

interface mode

[Description]

Configures MLD report suppression.

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

When enabled, the minimum number of messages will be sent to the multicast router ports based on the information obtained from the received Report messages and Leave messages.

When disabled, the received Report messages and Leave messages will be sequentially transmitted to the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables MLD report suppression at VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping report-suppression enable
```

Disables MLD report suppression at VLAN #2.

```
SWX2210P#configure terminal
SWX2210P(config)#interface vlan2
SWX2210P(config-if)#ipv6 mld snooping report-suppression disable
```

8.3.8 Show multicast router connection port information

[Syntax]

show ipv6 mld snooping mrouter *ifname*

[Parameter]

ifname : VLAN interface name

Interface to show

[Input mode]

unprivileged EXEC mode, privileged 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.

```
SWX2210P#show ipv6 mld snooping mrouter vlan2
VLAN    Interface                   IP-address              Expires
2       port1.8(dynamic)            192.168.100.216         00:00:49
```

8.3.9 Show MLD group membership information

[Syntax]

show ipv6 mld snooping groups
show ipv6 mld snooping groups *X*:*X*::*X*:*X*
show ipv6 mld snooping groups *ifname*

[Parameter]

X:X::X:X	:	Multicast group address
ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows MLD group membership information.

[Example]

Show MLD group membership information.

```
SWX2210P#show ipv6 mld snooping groups
MLD Snooping Group Membership
Vlan Group Address Interface Uptime   Expires  Last Reporter            Version
1    ff15::1       port1.3   00:00:44 00:01:07 fe80::a00:27ff:fe8b:87e3 V2
```

8.3.10 Show an interface's MLD-related information

[Syntax]

show ipv6 mld snooping interface *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show a VLAN interface's MLD-related information.

[Example]

Show MLD-related information for VLAN #1.

```
SWX2210P#show ipv6 mld snooping interface vlan1

MLD Snooping information for vlan1
 MLD Snooping enabled
 Snooping Querier none
 MLD Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 MLDv1/v2 fast-leave is disabled
 MLDv1 Report suppression enabled
 MLDv2 Report suppression enabled
 Router port detection using MLD Queries
 Number of router-ports: 0
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v1-leaves: 0
 Number of v2-reports: 127
 Number of v1-query-warnings: 0
 Number of v2-query-warnings: 0
 Active Ports:
  port1.26
  port1.5
```

8.3.11 Clear MLD group membership entries

[Syntax]

clear ipv6 mld snooping
clear ipv6 mld snooping group *X:X::X:X*
clear ipv6 mld snooping interface *ifname*

[Keyword]

group	:	Specifies the multicast group address to be cleared
interface	:	Specifies the VLAN interface to clear

[Parameter]

X:X::X:X	:	Multicast group address "*" indicates all entries
ifname	:	VLAN interface name Interface to clear

[Input mode]

privileged EXEC mode

[Description]

Clears MLD group membership entries.

[Example]

Clear MLD group membership entries for VLAN #1.

```
SWX2210P#clear ipv6 mld snooping interface vlan1
```

Chapter 9

Traffic control

9.1 ACL

9.1.1 Generate IPv4 access list

[Syntax]

access-list *ipv4-acl-id* [*seq_num*] *action src-info*
no access-list *ipv4-acl-id* [*seq_num*] [*action src-info*]

[Parameter]

ipv4-acl-id : <1-2000>

ID of IPv4 access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

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

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

Setting value	Description
A.B.C.D E.F.G.H	Specifies an IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
host A.B.C.D	Specifies a single IPv4 address (A.B.C.D)
any	Applies to all IPv4 addresses

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Generates a IPv4 access list.

Multiple conditions (MAX:128 items) can be specified for the generated access list.

To apply the generated IPv4 access list, use the **access-group** command in interface mode.

If the "no" syntax is used to specify "action" and following, the IPv4 access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and thereafter, the IPv4 access list of the matching access ID is deleted.

[Note]

An access list that is applied to an LAN port cannot be deleted using the "no" syntax. Before you can delete the access list, you must rescind the application of that list.

[Example]

Create IPv4 access list #1 that denies traffic from source segment 192.168.1.0/24.

```
SWX2210P(config)#access-list 1 deny 192.168.1.0 0.0.0.255
```

Delete IPv4 access list #1.

```
SWX2210P(config)#no access-list 1
```

9.1.2 Add comment to IPv4 access list

[Syntax]

access-list *ipv4-acl-id* **description** *line*
no access-list *ipv4-acl-id* **description**

[Parameter]

ipv4-acl-id : <1-2000>
ID of IPv4 access list to which a comment will be added

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

[Initial value]

None

[Input mode]

global configuration mode

[Description]

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

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

[Note]

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

[Example]

Create IPv4 access list #1 that denies traffic from source segment 192.168.1.0/24, and add the comment "Test".

```
SWX2210P(config)#access-list 1 deny 192.168.1.0 0.0.0.255
SWX2210P(config)#access-list 1 description Test
```

9.1.3 Apply IPv4 access list

[Syntax]

access-group *ipv4-acl-id direction*
no access-group *ipv4-acl-id direction*

[Parameter]

ipv4-acl-id : <1-2000>
ID of IPv4 access list to apply

direction : Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames

[Initial value]

None

[Input mode]

interface mode

[Description]

Apply an IPv4 access list to LAN 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 LAN port.

[Note]

Only one access list can be registered on the same interface.

However, if an access list setting for received frames is specified for an LAN port that is associated with an logical interface, then the setting for the most recent port number of logical interface is applied to other associated ports.

[Example]

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

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#access-group 1 in
```

9.1.4 Generate IPv6 access list

[Syntax]

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

[Parameter]

ipv6-acl-id : <3001-4000>

ID of IPv6 access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

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

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

Setting value	Description
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Accept every IPv6 address

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Generates a IPv6 access list.

Multiple conditions (MAX:128 items) can be specified for the generated access list.

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

If the "no" syntax is used to specify "action" and following, the IPv6 access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and following, the IPv6 access list of the matching access ID is deleted.

[Note]

An access list that is applied to an LAN port cannot be deleted using the "no" syntax. Before you can delete the access list, you must rescind the application of that list.

[Example]

Create an IPv6 access list #3002 which denies packets from 3ffe:506::/32.

```
SWX2210P(config)#access-list 3002 deny 3ffe:506::/32
```

Delete IPv6 access list #3002.

```
SWX2210P(config)#no access-list 3002
```

9.1.5 Add comment to IPv6 access list

[Syntax]

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

[Parameter]

ipv6-acl-id	:	<3001-4000> ID of IPv6 access list to which a comment will be added
line	:	Comment to add. Up to 32 ASCII characters excluding question marks 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 LAN port. (The last-written comment overwrites the previous one.)

[Example]

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

```
SWX2210P(config)#access-list 3002 deny 3ffe:506::/32
SWX2210P(config)#access-list 3002 description Test
```

9.1.6 Apply IPv6 access list

[Syntax]

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

[Parameter]

ipv6-acl-id	:	<3001-4000> ID of IPv6 access list to apply
direction	:	Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames

[Initial value]

None

[Input mode]

interface mode

[Description]

Apply an IPv6 access list to LAN 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 LAN port.

[Note]

Only one access list can be registered on the same interface.

However, if an access list setting for received frames is specified for an LAN port that is associated with an logical interface, then the setting for the most recent port number of logical interface is applied to other associated ports.

[Example]

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

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#access-group 3002 in
```

9.1.7 Generate MAC access list

[Syntax]

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

[Parameter]

mac-acl-id : <2001-3000>

ID of MAC access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

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

src-info : Specifies the transmission-source MAC address information that is the condition

Setting value	Description
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	Specifies the MAC address (HHHH.HHHH.HHHH) with wildcard bits (WWWW.WWWW.WWWW)
host HHHH.HHHH.HHHH	Specifies an individual MAC address (HHHH.HHHH.HHHH)
any	Applies to all MAC addresses

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Generates a MAC access list.

Multiple conditions (MAX:128 items) can be specified for the generated access list.

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

If the "no" syntax is used to specify "action" and thereafter, the MAC access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and thereafter, the MAC access list of the matching access ID is deleted.

[Note]

An access list that is applied to an LAN port cannot be deleted using the "no" syntax. Before you can delete the access list, you must rescind the application of that list.

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

[Example]

Create MAC access list #2001 which denies frames from MAC address 00-A0-DE-12-34-56.

```
SWX2210P(config)#access-list 2001 deny 00A0.DE12.3456 0000.0000.0000
```

Delete MAC access list #2001.

```
SWX2210P(config)#no access-list 2001
```

9.1.8 Add comment to MAC access list

[Syntax]

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

[Parameter]

mac-acl-id	:	<2001-3000> ID of extended MAC access list to which a comment will be added
line	:	Comment to add. Up to 32 ASCII characters excluding question marks 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 LAN port. (The last-written comment overwrites the previous one.)

[Example]

Create MAC access list #2001 which denies frames from MAC address 00-A0-DE-12-34-56, and add the comment "Test".

```
SWX2210P(config)#access-list 2001 deny 00A0.DE12.3456 0000.0000.0000
SWX2210P(config)#access-list 2001 description Test
```

9.1.9 Apply MAC access list

[Syntax]

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

[Parameter]

mac-acl-id	:	<2001-3000> ID of MAC access list to apply
direction	:	Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames

[Initial value]

None

[Input mode]

interface mode

[Description]

Applies the MAC access list to LAN 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 LAN port.

[Note]

Only one access list can be registered on the same interface.

However, if an access list setting for received frames is specified for an LAN port that is associated with an logical interface, then the setting for the most recent port number of logical interface is applied to other associated ports.

[Example]

Apply access list #2001 to received frames of LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#access-group 2001 in
```

9.1.10 Show generated access list

[Syntax]

show access-list [*acl_id*]

[Parameter]

acl-id : <1-2000>, <2001-3000>, <3001-4000>

Access list ID

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the registered access list.

If *acl_id* is omitted, all access lists are shown.

[Example]

Show a list.

```
SWX2210P>show access-list
IPv4 access list 1
    10 deny 192.168.1.0/24
MAC access list 2001
    10 deny host 00A0.DE12.3456
IPv6 access list 3002
    10 deny 3ffe:506::/32
```

9.1.11 Show access list applied to interface

[Syntax]

show access-group

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

For each interface, this shows the ID of all access lists that are applied.

[Example]

Show a list.

```
SWX2210P>show access-group
Interface port1.1 : IPv4 access group 1 in
Interface port1.7 : IPv6 access group 3002 in
Interface port1.8 : MAC access group 2001 in
```

9.2 QoS (Quality of Service)

9.2.1 Enable/disable QoS

[Syntax]

qos *switch*
no qos

[Parameter]

switch : QoS operation

Setting value	Description
enable	Enable QoS
disable	Disable QoS

[Initial value]

qos disable

[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]

The following commands related to QoS cannot be executed when QoS is disabled.

- **qos cos**
- **qos trust**
- **qos port-priority-queue**
- **show qos interface**

[Example]

Enable QoS.

```
SWX2210P(config)#qos enable
```

Disable QoS.

```
SWX2210P(config)#qos disable
```

9.2.2 Set default CoS

[Syntax]

qos cos *value*
no qos cos

[Parameter]

value : <0-7>

Default CoS value

[Initial value]

qos cos 0

[Input mode]

interface mode

[Description]

Sets the default CoS.

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.

[Note]

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

If this is executed for a port whose trust mode is not "CoS", the command results in an execution error.

However, if a QoS setting is applied to an LAN port that is associated with an logical interface, then the setting for the most recent port number of logical interface is applied to other associated ports.

[Example]

Set the default CoS value to 2.

```
SWX2210P(config-if)#qos cos 2
```

Return the default CoS value to the default value.

```
SWX2210P(config-if)#no qos cos
```

9.2.3 Set trust mode

[Syntax]

qos trust *mode*
no qos trust

[Parameter]

mode : Trust mode

Setting value	Description
cos	Determines the egress queue based on the CoS value
dscp	Determines the egress queue based on the DSCP value
port-priority	Applies the specified priority to the receiving port

[Initial value]

qos trust cos

[Input mode]

interface mode

[Description]

Specifies the trust mode of the LAN port.

If this command is executed with the "no" syntax, the default value (CoS trust mode) is specified.

When the trust mode is "cos", the CoS value of received frames is used to determine the transmission queue. When the trust mode is "dscp", the DSCP value of received frames is used to determine the transmission queue. When the trust mode is "port priority", the priority specified for the receiving interface is used to determine the transmission queue.

The transmission queue that is associated with the CoS and DSCP values cannot be changed.

Within the QoS processes, there are two types of timing that determine (change) the transmission queue.

1. When assigning the transmission queue
2. Remarking specified

Item 2 can only be specified when the trust mode is "CoS" or "DSCP". The transmission queue is assigned according to the remarked CoS or DSCP values.

[Note]

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

However, if a QoS setting is applied to an LAN port that is associated with an logical interface, then the setting for the most recent port number of logical interface is applied to other associated ports.

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

[Example]

Specifies DSCP for the trust mode of the LAN port.

```
SWX2210P(config-if)#qos trust dscp
```

Sets the trust mode of the LAN port to the default setting (CoS).

```
SWX2210P(config-if)#qos trust cos
```

9.2.4 Set CoS - egress queue ID conversion table

[Syntax]

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

[Parameter]

cos-value : <0-7>
CoS value of conversion source

queue-id : <0-7>
Egress queue ID corresponding to CoS value

[Initial value]

See [Note]

[Input mode]

global configuration mode

[Description]

Specifies the values of the CoS - egress queue ID conversion table that is used to determine the egress queue.

If this 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, QoS must be enabled.

The following table shows the default settings of the CoS - egress queue ID conversion table.

CoS value	Transmission 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".

```
SWX2210P(config)#qos cos-queue 0 4
```

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

```
SWX2210P(config)#no qos cos-queue 0
```

9.2.5 Set DSCP - egress queue ID conversion table

[Syntax]

qos dscp-queue *dscp-value queue-id*
no qos dscp-queue *dscp-value*

[Parameter]

dscp-value : <0-63>

DSCP value of the conversion source

queue-id : <0-7>

Egress queue ID corresponding to DSCP value

[Initial value]

See [Note]

[Input mode]

global configuration mode

[Description]

Specifies the values of the DSCP - egress queue ID conversion table that is used to determine the egress queue.

If this command is executed with the "no" syntax, the transmission 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-transmission queue ID conversion table.

DSCP value	Transmission 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 transmission queue #4 to DSCP value "0".

```
SWX2210P(config)#qos dscp-queue 0 4
```

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

```
SWX2210P(config)#no qos dscp-queue 23
```

9.2.6 Set port priority order

[Syntax]

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

[Parameter]

queue-id : <0-7>

Transmission queue ID set for LAN port

[Initial value]

qos port-priority-queue 2

[Input mode]

interface mode

[Description]

Sets the priority (transmission queue ID) of the receiving interface for LAN port.

If this command is executed with the "no" syntax, the transmission queue ID for the specified interface is returned to the default setting (2).

The port priority is used to determine the egress queue when the trust mode is set to "port priority".

[Note]

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

If this is executed for a interface whose trust mode is not "port priority", the command results in an execution error.

However, if a QoS setting is applied to an LAN port that is associated with an logical interface, then the setting for the most recent port number of logical interface is applied to other associated ports.

[Example]

Assign transmission queue ID #4 as the port priority forLAN port #1.

```
SWX2210P#interface port1.1
SWX2210P(config-if)#qos port-priority-queue 4
```

9.2.7 Show status of QoS function setting

[Syntax]

show qos

[Input mode]

unprivileged EXEC mode、privileged 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.

```
SWX2210P#show qos
  Enable
```

9.2.8 Show QoS information for LAN port

[Syntax]

show qos interface [*ifname*]

[Parameter]

ifname : LAN port name. If this is omitted, the command applies to all ports.
Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows QoS setting information for the specified LAN port. The following content is displayed.

Parameter	Explanation
Port Trust Mode	LAN port trust mode (CoS/DSCP)
Port Default CoS Priority	Default CoS value (note 1)
Port-Priority-Queue	Port priority (note 3)
Remarking value	Remarking value for CoS or DSCP (note 4)

Parameter	Explanation
Queue Scheduling	Scheduling method and weight of transmission queue. The weight value is fixed. Shows the transmission queue usage ratio.
CoS (Queue)	CoS-transmission queue ID conversion table (note 1)
DSCP (Queue)	DSCP-transmission queue ID conversion table (note 2)

Note 1: Shown only for CoS trust mode.

Note 2: Shown only for DSCP trust mode.

Note 3: Shown only if the trust mode is "port priority".

Note 4: Shown only if the **remark** command is set.

[Note]

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

[Example]

Show the QoS settings of LAN port #1. (trust mode CoS).

```
SWX2210P#show qos interface port1.1

  Port Trust Mode: CoS

  Remarking: 2

  Port Default CoS priority: 0

  Queue Scheduling:
  Queue0 : Weighted   1  ( 5%)
  Queue1 : Weighted   1  ( 5%)
  Queue2 : Weighted   2  (10%)
  Queue3 : Weighted   2  (10%)
  Queue4 : Weighted   3  (15%)
  Queue5 : Weighted   3  (15%)
  Queue6 : Weighted   4  (20%)
  Queue7 : Weighted   4  (20%)

  Cos (Queue): 0(2), 1(0), 2(1), 3(3), 4(4), 5(5), 6(6), 7(7)
```

Show the QoS settings of LAN port #1. (trust mode DSCP).

```
SWX2210P#show qos interface port1.1

  Port Trust Mode: DSCP

  Remarking: 33

  Queue Scheduling:
  Queue0 : Weighted   1  ( 5%)
  Queue1 : Weighted   1  ( 5%)
  Queue2 : Weighted   2  (10%)
  Queue3 : Weighted   2  (10%)
  Queue4 : Weighted   3  (15%)
  Queue5 : Weighted   3  (15%)
  Queue6 : Weighted   4  (20%)
  Queue7 : Weighted   4  (20%)

  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)
```

9.2.9 Show egress queue usage ratio

[Syntax]

show qos queue-counters [*ifname*]

[Parameter]

ifname : LAN port name. If this is omitted, the command applies to all ports.

Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the packet buffer usage ratio for each transmission queue of the specified LAN port.

Since the packet buffer is shared between all ports, the packet buffer usage ratio for each cue varies depending on the packet buffer usage ratio of each port and the system.

[Note]

This command can be used regardless of the QoS status (enabled/disabled).

[Example]

Show the queue usage ratio of LAN port #1.

```
SWX2210P#show qos queue-counters port1.1
QoS: Enable
Interface port1.1 Memory Usage:
  Queue 0          59.4 %
  Queue 1          15.0 %
  Queue 2           0.0 %
  Queue 3           0.0 %
  Queue 4           0.0 %
  Queue 5           3.6 %
  Queue 6           0.0 %
  Queue 7           0.1 %
```

9.2.10 Set remarking

[Syntax]

remark *type value*
no remark

[Parameter]

type : Type of remarking

Setting value	Description
cos	Remarking the CoS value
dscp	DSCP remarking

value : <0-7>

CoS remarking value

: <0-63>

DSCP remarking value

[Initial value]

None

[Input mode]

interface mode

[Description]

Specifies the remarking operation of the LAN port.

For remarking, you can specify either a CoS value or a DSCP value.

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

If a trust mode that differs from the **qos trust** is specified for *type*, the command results in an error.

[Note]

Although QoS must be enabled to make remarking operate, this command can be executed even if QoS is disabled.

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]

Overwrites the frame received by LAN port #1 with DSCP value 10.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#remark dscp 10
```

9.2.11 Set scheduling method

[Syntax]

qos scheduling *type*
no qos scheduling

[Parameter]

type : Scheduling method

Setting value	Description
wrr	WRR (weighted round-robin) method
sp	SP (strict priority) method

[Initial value]

qos scheduling wrr

[Input mode]

global configuration mode

[Description]

Sets the scheduling method.

When executed with the "no" syntax, WRR (weighted round-robin) is used for the scheduling method.

[Example]

Sets the scheduling method to SP (strict priority).

```
SWX2210P(config)#qos scheduling sp
```

9.3 Flow control

9.3.1 Set flow control (IEEE 802.3x PAUSE send/receive) (system)

[Syntax]

flowcontrol *switch*
no flowcontrol

[Parameter]

switch : Flow control operation

Setting value	Description
enable	Enable flow control
disable	Disable flow control

[Initial value]

flowcontrol disable

[Input mode]

global configuration mode

[Description]

Enables flow control for the entire system (IEEE 802.3x PAUSE frame send/receive).

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

[Note]

If flow control is enabled, the tail drop function is automatically disabled.

The threshold for starting to transmit the PAUSE frame changes, depending on the packet buffer usage for the system or for each port.

Flow control for each interface operates only if the flow control settings of the system and of the interface are each enabled.

[Example]

Enable flow control for the system.

```
SWX2210P(config)#flowcontrol enable
```

9.3.2 Set flow control (IEEE 802.3x PAUSE send/receive) (interface)

[Syntax]

flowcontrol *switch*
no flowcontrol

[Parameter]

switch : Flow control operation

Setting value	Description
enable	Enable flow control
disable	Disable flow control

[Initial value]

flowcontrol disable

[Input mode]

interface mode

[Description]

Enables flow control for the LAN port (IEEE 802.3x PAUSE frames send/receive).

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

[Note]

This command can be specified only for LAN 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 PAUSE frame pause time transmitted by this product for a pause time request is 0xFFFF (65535).

The threshold for starting to transmit the PAUSE frame changes, depending on the packet buffer usage for the system or for each port.

[Example]

Enable flow control for LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#flowcontrol enable
```

Disable flow control for LAN port #1.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#no flowcontrol
```

9.3.3 Show flow control operating status

[Syntax]

show flowcontrol [inteface *ifname*]

[Keyword]

interface : Specifies the interface to show

[Parameter]

ifname : LAN port name. If this is omitted, the command applies to all interfaces.

Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows information related to flow control (enabled/disabled, number of PAUSE frames sent/received).

[Note]

The number of PAUSE frames sent and received are shown only if flow control is enabled on the corresponding port.

The number of PAUSE frames sent and received is cleared when you execute the **clear frame-counters** command.

[Example]

Show flow control information for LAN port #1.

```
SWX2210P#show flowcontrol port1.1
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Enable               4337       0
```

Show flow control information for all ports

```
SWX2210P#show flowcontrol
System flow-control: Enable
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Enable               4337       0
port1.2     Disable                 -       -
port1.3     Enable                  0    1732
port1.4     Disable                 -       -
port1.5     Disable                 -       -
port1.6     Disable                 -       -
port1.7     Disable                 -       -
port1.8     Disable                 -       -
port1.9     Disable                 -       -
port1.10    Disable                 -       -
```

9.4 Storm control

9.4.1 Set storm control

[Syntax]

storm-control *type* [*type*..] **level** *level*

no storm-control

[Parameter]

type : Storm control type

Storm control type	Description
broadcast	Enables broadcast storm control
multicast	Enables multicast storm control
unicast	Enables control for unicast frames with unknown address

level : <0.00-100.00>

Specifies the threshold value as a percentage of the bandwidth
The threshold value can be specified to the second decimal place

[Initial value]

no storm-control

[Input mode]

interface mode

[Description]

Applies reception restrictions to a LAN port enabling broadcast storm control, multicast storm control and control of unicast frames with unknown addresses.

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%.

```
SWX2210P(config)#interface port1.1
SWX2210P(config-if)#storm-control broadcast multicast level 30
```

9.4.2 Show storm control reception upper limit

[Syntax]

show storm-control [*ifname*]

[Parameter]

ifname : LAN port interface name

Interface to show

[Initial value]

None

[Input mode]

unprivileged EXEC mode, privileged 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.

```
SWX2210P#show storm-control
Port     BcastLevel    McastLevel    UcastLevel
port1.1    30.00%        30.00%       100.00%
port1.2    20.00%        20.00%        20.00%
port1.3   100.00%       100.00%       100.00%
port1.4   100.00%       100.00%       100.00%
port1.5    50.00%        50.00%       100.00%
port1.6   100.00%       100.00%       100.00%
port1.7   100.00%       100.00%        30.00%
port1.8   100.00%       100.00%        30.00%
port1.9   100.00%       100.00%        30.00%
port1.10  100.00%       100.00%        30.00%
```

Index

P

Q

R

S

T

U

V

W