

SWX2210P series

Technical Data

Rev.1.03.14



Contents

Important Notice	1
Login Security	1
Function Overview	1
Applicable Models and Revisions	1
Precautions When Updating Firmware	2
Related Documentation	3
Maintenance and Operation Functions	4
User Account Management	4
Function Overview	4
Definition of Terms Used	4
Function Details	4
User account function settings	4
User authentication	5
Related Commands	8
Examples of Command Execution	8
Setting the administrator password	8
Adding a user	8
Points of Caution	8
Related Documentation	9
LED Indicator Control	10
Function Overview	10
Definition of Terms Used	10
Function Details	10
LED indicator illumination specifications	10
About LED modes	11
Other LED indications	12
Related Commands	12
Examples of Command Execution	12
Checking LAN port status	12
Checking LAN port loop detection status	13
Set default LED mode	13
Points of Caution	13
Related Documentation	14
Boot Information Management	15
Function Overview	15
Related Commands	15
Examples of Command Execution	15
Show boot information	15
Clear boot information	16
Points of Caution	16
Related Documentation	16
Show Chassis Information	17
Function Overview	17
Use commands to show chassis information	17
Obtain technical support information remotely	17
Related Commands	17

Examples of Command Execution	17
Show inventory information	17
Show operating information	18
Show technical support information	19
Points of Caution	19
Related Documentation	19
Cable Diagnostics Function	20
Function Overview	20
Definition of Terms Used	20
Function Details	20
How to diagnose cables	20
Related Commands	20
Setting Examples	21
Perform the cable diagnostics	21
Checking previous diagnostic results	21
Points of Caution	21
Related Documentation	21
Config Management	22
Function Overview	22
Definition of Terms Used	22
Function Details	22
Running config	22
Startup config	22
Default config	22
Deciding the config file at startup	23
Controlling the config file via TFTP	23
Related Commands	23
Examples of Command Execution	23
Save running config	23
Erase startup config	24
Points of Caution	24
Related Documentation	24
Remote Access Control	25
Function Overview	25
Definition of Terms Used	25
Function Details	25
Related Commands	26
Examples of Command Execution	26
TELNET server access control	26
HTTP server access restrictions	27
TFTP server access restrictions	27
SNMP server access restrictions	27
Points of Caution	28
Related Documentation	28
Time Management	29
Function Overview	29
Definition of Terms Used	29
Function Details	29

Manually setting the date and time	29
Automatically setting the date and time	29
Time zone setting	30
Related Commands	30
Examples of Command Execution	30
Set clock manually	30
Automatically setting the time	30
Points of Caution	31
Related Documentation	31
SNMP	32
Function Overview	32
Definition of Terms Used	32
Function Details	32
SNMPv1	32
SNMPv2c	33
SNMPv3	33
Restricting SNMP server access	34
Private MIBs	34
Related Commands	34
Examples of Command Execution	34
SNMPv1 setting example	34
SNMPv2c setting example	35
SNMPv3 setting example	35
Points of Caution	35
Related Documentation	36
SYSLOG	37
Function Overview	37
Definition of Terms Used	37
Function Details	37
List of Related Commands	38
Examples of Command Settings	38
Points of Caution	39
Related Documentation	39
Firmware Update	40
Function Overview	40
Definition of Terms Used	40
Function Details	40
Update by transmitting the firmware update	40
Using an HTTP client to update the firmware	41
Reboot after writing	43
Related Commands	43
Examples of Command Execution	44
Using an HTTP client to update the firmware	44
Points of Caution	45
Related Documentation	45
L2MS (Layer2 Management Service)	46
Function Overview	46
Definition of Terms Used	46

Function Details	47
Compatible models	47
L2MS protocol	47
Monitoring agents	47
Agent ownership	47
Agent operations	47
Information notifications from agents	48
L2MS filter/non-L2MS filter	48
Enabling/disabling L2MS	48
Default IP address	48
Related Commands	48
Examples of Command Execution	49
L2MS filter setting	49
L2MS setting	49
Points of Caution	49
Use in conjunction with other functionality	49
SYSLOG Message List	50
Related Documentation	50
LLDP	51
Function Overview	51
Definition of Terms Used	51
Function Details	51
Operating specifications	51
TLV list	52
Related Commands	55
Examples of Command Execution	55
Set LLDP frame transmission/reception	55
Show LLDP interface status	56
Show LLDP connected device information	56
Points of Caution	57
Related Documentation	57
LLDP Automatic Settings	58
Function Overview	58
Definition of Terms Used	58
Function Details	58
Basic specifications	58
Dante Optimization Settings	59
Power shutoff advance notification by the schedule function	59
Related Commands	60
Setting Examples	60
Points of Caution	60
Related Documentation	60
Schedule Function	62
Function Overview	62
Definition of Terms Used	62
Function Details	62
Time Trigger	62
Action	64

Related Commands	64
Setting Examples	65
To supply PoE power to wireless LAN access points only during the specified period (only for PoE-supported models)	65
To shut down a port during the specified period	65
Executable Commands	66
SYSLOG	66
Points of Caution	66
Related Documentation	67
Dante Optimization Settings	68
Function Overview	68
Definition of Terms Used	68
Function Details	68
Automatic optimization settings using LLDP	71
Manual optimization settings via the Web GUI	71
Related Commands	71
Examples of Command Execution	72
Automatic optimization settings using LLDP	72
Points of Caution	73
Related Documentation	73
ProAV Settings	74
Function Overview	74
Definition of Terms Used	74
Details on ProAV Profiles	74
Dante profiles	74
NDI profiles	78
Settings for using multiple profiles	80
Kitting and Troubleshooting	83
[Kitting] Initial setup without having to think about IP addresses	83
[Kitting] Applying the same settings to multiple Yamaha switches at once	86
[Troubleshooting] Checking the network status	89
[Troubleshooting] Checking the Dante device status	91
Points of Caution	92
Related Documentation	92
Trademarks and Trade Names	92
List of Default Settings	93
Interface Control Functions	96
Basic Interface Functions	96
Function Overview	96
Definition of Terms Used	96
Function Details	96
Interface types	96
Interface control	96
LAN port defaults	97
Port mirroring	98
Frame counter	98
Related Commands	99
Examples of Command Execution	100

Basic LAN port settings	100
Mirroring settings	101
Show LAN port information	101
Points of Caution	102
Related Documentation	102
Link Aggregation	103
Function Overview	103
Definition of Terms Used	103
Function Details	103
Static link aggregation specifications	103
Related Commands	104
Examples of Command Execution	105
Set the static logical interface	105
Points of Caution	108
Related Documentation	108
PoE Control	109
Function Overview	109
Definition of Terms Used	109
Function Details	109
PoE power supply function enable/disable control	109
Power supply class and maximum number of ports that can be powered simultaneously	109
Guard band	110
PoE power priority	110
PoE power supply actions	110
Power supply setting by LLDP	111
Related Commands	111
Examples of Command Execution	111
PoE Port Power Supply Settings	111
Points of Caution	112
Related Documentation	112
Layer 2 Functions	113
Forwarding Database	113
Function Overview	113
Definition of Terms Used	113
Function Details	113
FDB entry	113
Automatic MAC address acquisition	114
MAC address manual setting	115
Related Commands	115
Examples of Command Execution	116
Referring to the FDB	116
Delete dynamic entries	116
Changing the dynamic entry ageing time	116
Register static entries	116
Delete static entries	117
Points of Caution	117
Related Documentation	117
VLAN	118

Function Overview	118
Definition of Terms Used	118
Function Details	118
Defining a VLAN ID	118
VLAN settings for the LAN ports	118
Default VLAN	119
Native VLAN	119
Related Commands	119
List of related commands	119
Examples of Command Execution	120
Port-based VLAN settings	120
Tagged VLAN settings	121
Points of Caution	123
Related Documentation	123
Multiple VLAN	124
Function Overview	124
Definition of Terms Used	124
Function Details	124
Basic operating specifications	124
Examples of traffic between multiple VLAN groups	125
Related Commands	125
List of related commands	125
Examples of Command Execution	125
Multiple VLAN settings	126
Points of Caution	127
Related Documentation	127
Proprietary Loop Detection	128
Function Overview	128
Definition of Terms Used	128
Function Details	128
Loop detection operating specifications	128
Loop detection examples	129
Related Commands	130
Examples of Command Execution	131
Points of Caution	132
Related Documentation	132
Pass Through	133
Function Overview	133
Definition of Terms Used	133
Function Details	133
Operating specifications for BPDU pass through	133
Operating specifications for EAP pass through	133
Related Commands	134
Examples of Command Execution	134
Points of Caution	134
Related Documentation	134
Layer 3 Functions	135
IPv4/IPv6 Common Settings	135

Function Overview	135
Definition of Terms Used	135
Function Details	135
DNS client settings	135
Related Commands	136
Examples of Command Execution	136
DNS client settings	136
Points of Caution	137
Related Documentation	137
Basic IPv4 Settings	138
Function Overview	138
Definition of Terms Used	138
Function Details	138
IPv4 address settings	138
Auto IP function	138
Route information settings	139
ARP table settings	139
Related Commands	140
Examples of Command Execution	140
IPv4 network environment settings (DHCP)	140
Points of Caution	141
Related Documentation	141
Basic IPv6 Settings	142
Function Overview	142
Definition of Terms Used	142
Function Details	142
IPv6 address settings	142
Route information settings	143
Neighbor cache table settings	143
Related Commands	144
Examples of Command Execution	144
Setting up an IPv6 network environment (fixed settings)	144
Setting up an IPv6 network environment (automatic settings using RA)	145
Points of Caution	145
Related Documentation	145
IP Multicast Functions	146
IGMP Snooping	146
Function Overview	146
Definition of Terms Used	147
Function Details	148
Related Commands	150
Examples of Command Execution	150
IGMP snooping settings (with multicast router)	150
IGMP snooping settings (without multicast router)	152
IGMP snooping settings (If distributing data in both directions)	154
Points of Caution	157
Related Documentation	157
MLD Snooping	158

Function Overview	158
Definition of Terms Used	158
Function Details	159
Related Commands	160
Examples of Command Execution	161
MLD snooping settings (with multicast router)	161
MLD snooping settings (without multicast router)	162
Points of Caution	164
Related Documentation	165
Traffic Control Functions	166
ACL	166
Function Overview	166
Definition of Terms Used	166
Function Details	166
Generate access list	166
Applying to the interface	166
LAN port settings	167
Related Commands	167
Examples of Command Execution	168
IPv4 access list settings	168
IPv6 access list settings	169
MAC access list settings	170
Points of Caution	172
Related Documentation	172
QoS	173
Function Overview	173
Definition of Terms Used	173
Function Details	174
Enabling or disabling QoS control	174
QoS processing flow	174
Transmission queue assignments	174
Remark	175
Storing in the transmission queue	176
Scheduling	176
Optimizing web conference application settings	177
Separate table 1: Standard PHB (RFC recommended value)	178
Related Commands	179
Examples of Command Execution	180
Priority control (SP) using DSCP values	180
Priority control (WRR) using CoS values	180
Priority control based on DSCP value assigned to each reception port	181
Priority control using port priority trust mode	182
Points of Caution	183
Related Documentation	184
Trademarks and Trade Names	184
Flow Control	185
Function Overview	185
Definition of Terms Used	185

Function Details	185
IEEE 802.3x flow control	185
Back pressure	186
Related Commands	187
Examples of Command Execution	187
Points of Caution	187
Related Documentation	187
Storm Control	188
Function Overview	188
Definition of Terms Used	188
Function Details	188
Related Commands	188
Examples of Command Execution	189
Points of Caution	189
Related Documentation	189
Other Information	190
SNMP MIB Reference	190
Command Reference	191
About Licenses of Open Source Software Used in This Product	192
List of Open Source Software	192
List of License Terms	193
GPLv2	193
OpenSSL	199
Wide-DHCPv6	201
crypt-md5.c	202
ExplorerCanvas	202
jqCanvas	202
jqPlot	203
jQuery	204
jQuery DatePicker plugin	204
jQuery File Upload Plugin / jQuery Iframe Transport Plugin / jQuery XDomainRequest Transport Plugin	204
jQuery Migrate	205
jQuery UI	206
jQuery UI Touch Punch	206
jQuery UI Ympicker	207
PowerTip	207

Important Notice

Login Security

Function Overview

BASIC

This product includes the following user account management improvements as countermeasures for ensuring cyber security.

To eliminate the risk of malicious cyber-attacks and ensure the product is used safely, be sure to read this document carefully and specify an appropriate user password before use.

For more information, refer to [User Account Management](#).

- **Mandatory administrator registration**

- At least one administrator account must be registered for this product.
Therefore, a default administrative user (username: admin and password: admin) has been specified for logging in to the product the first time.
- When first logging into the switch, specify **admin** as the username and password.
- After logging in using the default administrative user account, the user is prompted to change the password setting.

- **Stricter limits on guest user operations**

- If the privileged password is not changed from the default setting, use of the privileged password will be restricted to the following operation.
 - Users without administrator rights cannot transition to the privileged EXEC mode.
 - Factory settings cannot be restored using CLI/ GUI operations.
 - Cannot accept connections as a TFTP server.
- Change the privileged password before performing the above operations.

- **Countermeasure for Brute-Force Attacks**

- As a countermeasure against brute-force attacks, login restrictions are applied after a login fails.
- If an incorrect password is entered three successive times when logging into the switch via the console, web GUI, or other means, login is disabled for **one minute** thereafter, even if the correct password is entered.
- If the password is entered incorrectly, wait at least one minute before trying to login again.

Applicable Models and Revisions

User account management has been improved in the following models and revisions.

Models	Revisions
SWX3220-16MT SWX3220-16TMs	Rev.4.02.10 or later
SWX3200-52GT SWX3200-28GT	Rev.4.00.25 or later
SWX3100-18GT SWX3100-10G	Rev.4.01.29 or later
SWX2322P-16MT	Rev.2.06.10 or later

Models	Revisions
SWX2320-16MT	Rev.2.05.10 or later
SWX2310-52GT SWX2310-28GT SWX2310-18GT SWX2310-10G	Rev.2.04.11 or later
SWR2310-28GT SWR2310-18GT SWR2310-10G	Rev.2.04.12 or later
SWX2310P-28GT SWX2310P-18G SWX2310P-10G	Rev.2.02.24 or later
SWR2311P-10G	Rev.2.02.25 or later
SWP2-10SMF SWP2-10MMF	Rev.2.03.16 or later
SWX2220P-26NT SWX2220P-18NT	Rev.1.05.06 or later
SWX2221P-10NT	Rev.1.05.03 or later
SWX2220-26NT SWX2220-18NT	Rev.1.04.06 or later
SWX2220-10NT	Rev.1.04.03 or later
SWX2210P-28G SWX2210P-18G	Rev.1.03.14 or later
SWX2210P-10G	Rev.1.03.13 or later
SWX2210-24G SWX2210-16G SWX2210-8G	Rev.1.02.14 or later

Precautions When Updating Firmware

If the firmware is updated with stronger user account management functionality, be sure to register an administrator account according to the following procedure before using the switch.

1. Register the administrator account with the previous firmware running, which has not been updated with stronger user account management functionality.
 - If an administrator account already exists, then no account registration is necessary.
 - However, if a password was not specified for the administrator account, be sure to specify a password.
 - It is not a problem if the user name for the administrator account is the default "admin".

```
Yamaha>enable
Yamaha#configure terminal
Yamaha(config)#username (username) privilege on password (password)
```

2. Create a guest user

If necessary, create a guest user.

- If using the username command, create it with the privilege option disabled (off).

```
Yamaha(config)#username (username) privilege off password (password)
```

3. Change the privileged password

- The default privileged password setting is "admin".
- To change the privileged password using a command, use the enable password command.

```
Yamaha(config)#enable password (special privileged access password)
```

4. Update the firmware to the version with a countermeasure taken

- Update the firmware to the version with a countermeasure taken in accordance with [Firmware Update](#).

Related Documentation

- [User account management](#)
- [Remote Access Control](#)
- [Firmware Update](#)

Maintenance and Operation Functions

User Account Management

Function Overview

This product provides the functions shown below for managing user accounts.

- Functions for setting user information
- Functions for user authentication by user name and password

Definition of Terms Used

Default Administrative User

Users with administrator rights specified in default factory settings.
Username: admin and password: admin

Administrative User

Users with administrator rights.
Administrative users are users with the privilege option switched on using the username command.

General User

Users without administrator rights and that require entering the privileged password in order to access the privileged EXEC mode.
General users are users with the privilege option switched off using the username command.

Privileged Password

The password used to assign administrator rights and specified using the enable password command.

Unnamed User

Users with a blank username setting.
Rev. 1.03.12 or earlier firmware versions permitted using unnamed user accounts under factory default settings, but unnamed user accounts were eliminated for newer firmware versions with stronger user account management functionality.

Function Details

User account function settings

User information settings

Use the **username** command to specify the following user information.

- User name
- Password
- Assignment of administrator rights

With factory default settings, the administrative username and password are both "admin".

Setting the privileged password

The privileged password is set using the **enable password** command.
The privileged password is used for the following applications.

- To initialize devices
- To transition users without administrator rights to the privileged EXEC mode by using the console
- To use a TFTP client to send a config file or firmware to the switch

“**admin**” is the privileged password specified in default factory settings, but the operations described above cannot be performed if the privileged password is the default setting. To perform any of those operations, change the privileged password in advance.

Administrator rights

User login operations can be restricted depending on whether or not the user has administrator rights.

- Administrative users (users with administrator rights) can change device settings or update firmware.
- General users (users without administrator rights) can only view device information without changing any settings.

Specifically, the following differences apply depending on whether or not the user has administrator rights.

	CLI		Web GUI	
	Administrative user (with rights)	General user (without rights)	Administrative user (with rights)	General user (without rights)
Show device information	Yes	Yes	Yes	Yes
View settings	Yes	No	Yes	Limited (*1)
Change settings	Yes	No	Yes	No
Restart or initialize devices	Yes	No	Yes	No
Update firmware	Yes	No	Yes	No

*1: Cannot view passwords or other security-related settings.

Once the **enable** command is executed and the privileged password is entered, the privileged EXEC mode can be accessed to perform operations equivalent to an administrative user, even if logged in as a general user. For information about the rights required to execute each command, refer to the command reference.

Encrypt password

Specified passwords can be encrypted using the **password-encryption** command.

To encrypt a password, specify the **password-encryption enable** setting.

Once a password has been encrypted, it cannot be restored to an unencrypted character string state, even by specifying the **password-encryption disable** setting.

Encryption applies to the passwords specified by the following commands.

- **enable password** command
- **username** command

User authentication

When logging in to the console

When the following login prompt appears after connecting to the console, log in by entering the specified username and password.

Username:
Password:

For factory default settings, log in by entering “admin” as the default administrative username (and “admin” as the password).

After using “admin” to log in, the password must be changed to specify a new password.

```
Username: admin
Password: ①

SWX2210P-10G Rev.1.03.14 (Fri Feb  7 14:37:29 2025)
  Copyright (c) 2018-2025 Yamaha Corporation. All Rights Reserved.

Please change the default password for admin.
New Password: ②
New Password(Confirm): ③
Saving ...
Succeeded to write configuration
```

- ① Enter “admin”
- ② Enter the new password.
- ③ Enter the same password again.

If an incorrect password is entered three successive times, login by that same user is restricted for one minute.

```
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 login restriction occurs, the following message is output in the INFO level SYSLOG.

Connection method	Output message
Serial console	Login access from serial console as \{username} was restricted
TELNET	Login access from TELNET as \{username} was restricted: \{IP address}
Web GUI	Login access from HTTP as \{username} was restricted: \{IP address}

Note that if a user with a login restriction enters an incorrect password again, the remaining time until the restriction is cancelled is reset to one minute again.

When logging in to the web GUI

When the following login form appears after accessing the web GUI, log in by entering the specified username

and password.



The image shows a login screen for the SWX2210P-10G device. At the top, there is a black header with the text "SWX2210P-10G" in white. Below the header, the text "SWX2210P" is displayed. The main content area contains two input fields: one for the username and one for the password. The username field is preceded by the text "ユーザー名を入力してください" and "Please enter your username." The password field is preceded by the text "パスワードを入力してください" and "Please enter your password." Below the password field is a "Login" button. At the bottom of the screen, the text "Yamaha Corporation" is displayed.

SWX2210P-10G

SWX2210P

ユーザー名を入力してください
Please enter your username.

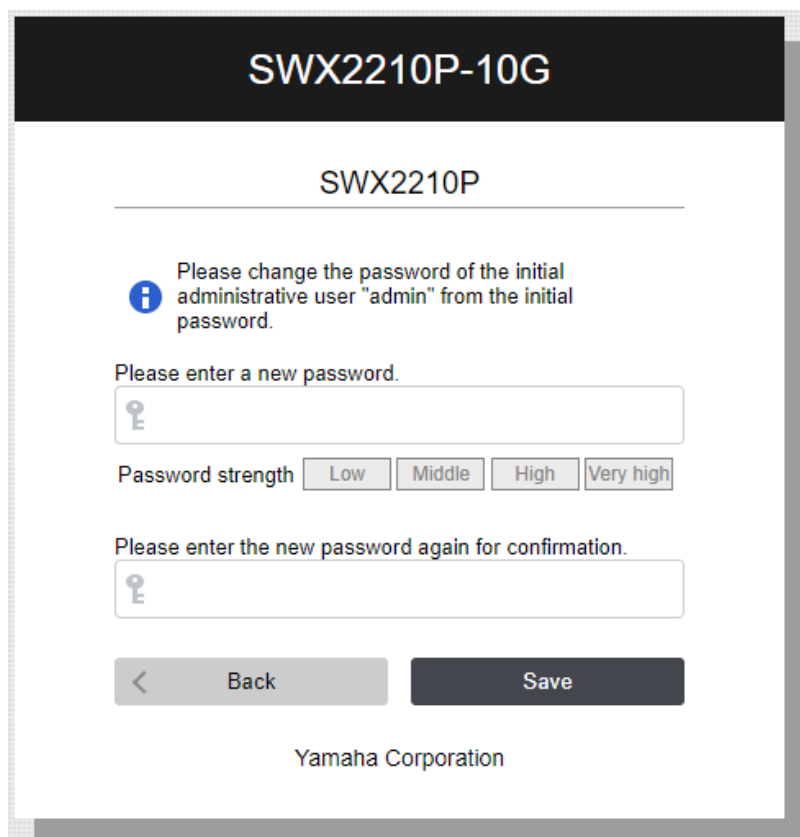
パスワードを入力してください
Please enter your password.

Login

Yamaha Corporation

For factory default settings, log in by entering "admin" as the default administrative username (and "admin" as the password).

Then specify a new password because the login password must be changed after logging in with factory settings.



The image shows a password change screen for the SWX2210P-10G device. At the top, there is a black header with the text "SWX2210P-10G" in white. Below the header, the text "SWX2210P" is displayed. The main content area contains an information icon (i) followed by the text "Please change the password of the initial administrative user 'admin' from the initial password." Below this is a text input field for the new password, preceded by the text "Please enter a new password." To the right of the input field is a "Password strength" section with four buttons: "Low", "Middle", "High", and "Very high". Below the input field is another text input field for confirmation, preceded by the text "Please enter the new password again for confirmation." At the bottom of the screen, there are two buttons: "Back" and "Save". The text "Yamaha Corporation" is displayed at the very bottom.

SWX2210P-10G

SWX2210P

Please change the password of the initial administrative user "admin" from the initial password.

Please enter a new password.

Password strength: Low Middle High Very high

Please enter the new password again for confirmation.

Back Save

Yamaha Corporation

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Setting the privileged password	enable password
Encrypt password	password-encryption
Set user	username
Show user information	show users

Examples of Command Execution

Setting the administrator password

Specify **yamaha_admin** as the administrator password.

```
Yamaha>enable
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#enable password yamaha_admin
```

Adding a user

Grant **privilege options** to the user **yamaha**, and assign the password **yamaha_pass**.

```
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#username yamaha privilege on password yamaha_pass
Yamaha(config)#exit
Yamaha#exit

Username: yamaha
Password:

SWX2210P-10G Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
Copyright (c) 2018-2025 Yamaha Corporation. All Rights Reserved.

Yamaha>enable
Yamaha#
```

Points of Caution

- If no administrative user (user with administrator rights) exists in startup-config when the product is booted, then a default administrative user (with username “admin” and password “admin”) will be added automatically.
For example, that would occur in the following case.
 - Product is booted with factory default settings configured
 - Firmware is updated to a newer version than Rev. 1.03.12 after the product was operated using Rev. 1.03.12 or older firmware and only unnamed users.

- If a user with no password is specified in startup-config when the product is booted, then a password with the same character string as the username will be added automatically.
For example, that would occur in the following case.
 - Firmware is updated to a newer version than Rev. 1.03.12 after Rev. 1.03.12 or older firmware was used to specify users with no password.

Setting with Rev. 1.03.12 or earlier firmware version

```
username yamaha1  
username yamaha2 privilege on
```

Setting after updating firmware to a newer version than Rev. 1.03.12

```
username yamaha1 password yamaha1  
username yamaha2 privilege on password yamaha2
```

- If the password (admin) for the default administrative user admin is left unchanged, then the following restrictions are applied.
 - This product cannot be accessed by TELNET, HTTP, or HTTPS from a network segment other than a VLAN where an IPv4 or IPv6 address is set.
 - Login by users other than the default administrative user is not permitted.

```
Username: yamaha  
Password:  
% Please login as user "admin".
```

Related Documentation

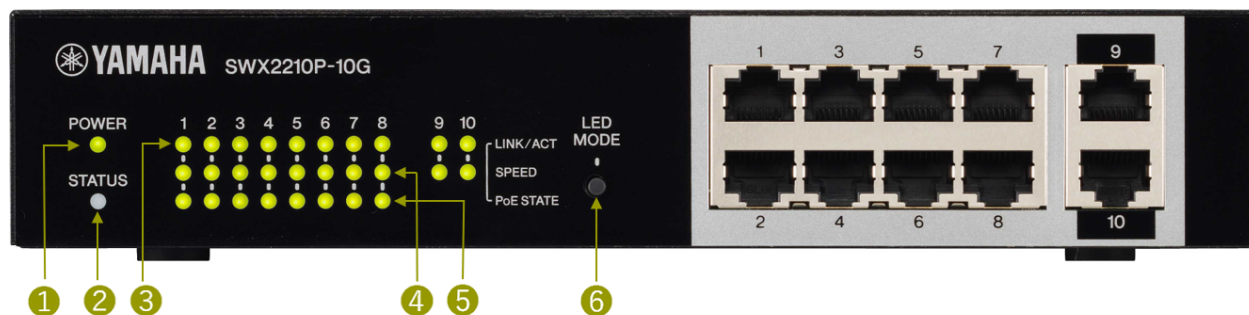
- [Remote Access Control](#)

LED Indicator Control

Function Overview

This product is equipped with five types of LED indicators: **[POWER]**, **[STATUS]**, **[LINK/ACT]**, **[SPEED]**, and **[PoE STATE]**, as well as an **LED MODE button** to be used for switching the LED MODE.

- SWX2210P LED indicators



1. POWER LED
2. STATUS LED
3. LINK/ACT LED
4. SPEED LED
5. PoE STATE LED
6. LED MODE Button

Definition of Terms Used

None

Function Details

LED indicator illumination specifications

The LED indicator illumination specifications for this product are shown below.

- SWX2210P LED indicators

Indicator	Illumination status	Description
POWER	Unlit	Power off
	Steady green	Power on
STATUS LED	Unlit	Normal
	Steady orange	Any of the following conditions: <ul style="list-style-type: none">- Power supply is stopped due to exceeding of the total supply capacity- Power supply is suppressed by a guard band- Power supply is stopped due to an overcurrent- A loop is detected and communication is blocked
	Flashing orange	A system error is detected (fan error/temperature error/power supply error)

Indicator	Illumination status	Description
LINK/ACT	Unlit	Any of the following conditions: - Link is down - The indicator mode is in OFF mode
	Steady green	Link is up
	Flashing green	While forwarding data
	Flashing orange	A loop is detected and communication is blocked
SPEED	Unlit	Any of the following conditions: - Link is down - Connecting via 10BASE-T - The indicator mode is in OFF mode
	Steady orange	Connecting via 100BASE-TX
	Steady green	Connecting via 1000BASE-T
PoE STATE	Unlit	Any of the following conditions: - Power is not supplied - The indicator mode is in OFF mode
	Steady green	Power is being normally supplied
	Steady orange	Any of the following conditions: - Power supply is stopped due to exceeding of the total supply capacity - Power supply is suppressed by a guard band
	Flashing orange	Power supply is stopped due to an overcurrent

About LED modes

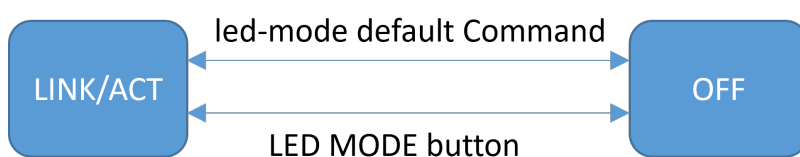
Indicator modes and switching between them

This product offers the following two indicator modes.

Mode name	Function Overview
LINK/ACT mode	The LINK/ACT LED indicates the link status, the SPEED LED indicates the connection speed, and the PoE STATE LED indicates the power supply status.
OFF mode	The LINK/ACT LED, SPEED LED, and PoE STATE LED turn off to reduce power consumption.

The indicator mode can be switched using the LED MODE button.
The flowchart below shows how to switch the indicator mode.

- Switching the indicator mode (when the default LED mode is the LINK/ACT mode)



LED indication for OFF mode

When the LED mode is in the OFF mode, all the LINK/ACT LED, SPEED LED, and PoE STATE LED turn off regardless of the link status, loop detection status, and PoE power supply status.

Changing the LED mode after system startup

This product enables the LED mode after system startup (the default LED mode) to be changed. The initial default LED mode is set to **LINK/ACT** mode, but it can be changed using the **led-mode default** command.

You can check the default LED mode and the currently displayed LED mode using the **show led-mode** command.

Other LED indications

When you turn on the power while holding down the LED MODE button and keep that state for approximately 10 seconds, all port LEDs turn orange regardless of the LED mode status and return to the factory default settings.

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Show LAN port status	show interface
Show loop detection setting status	show loop-detect
Show PoE power supply information	show power-inline
Set default LED mode	led-mode default
Show LED mode	show led-mode

Examples of Command Execution

Checking LAN port status

Use the **show interface** command to check the LAN port status.

```
Yamaha#show interface
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: ac44.f230.02c9
  MRU 1522
  BPDU pass-through: Enabled
  EAP pass-through: Enabled
  Description:
  ifIndex 5001
  Speed-Duplex: auto(configured), 10-half(current)
  Auto MDI/MDIX: on
  Vlan info:
    Switchport mode      : access
    Ingress filter       : enable
    Acceptable frame types : all
    Default Vlan         : 1
```

```

Configured Vlan          :    1
Interface counter:
  input  packets          : 46290
         bytes            : 6834572
         drops            : 0
         broadcast-and-multicast-packets: 31605
  output packets          : 37816
         bytes            : 16869972
         drops            : 0
         broadcast-and-multicast-packets: 19050
:
(Shows information for all LAN ports)

```

Checking LAN port loop detection status

Check the LAN port loop detection status.

```

Yamaha#show loop-detect
loop-detect: Enable

```

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

Set default LED mode

Set the default LED mode to the OFF mode.

```

Yamaha#configure terminal
Yamaha(config)#led-mode default off ①
Yamaha(config)#exit
Yamaha#show led-mode ②
default mode : off
current mode : off

```

① Set default LED mode

② Show LED mode

Points of Caution

None

Related Documentation

None

Boot Information Management

Function Overview

As system boot information, this product manages the information shown in the table below.

Management item	Description
System startup time	Time that the system booted up
Running firmware information	Firmware version currently running, and date generated
Firmware information for previous startup	Version and generated date of the firmware for the previous startup
Reason for boot	Reason why the system booted up. The following reasons for boot are recorded: * Boot due to power on * Reboot due to "reload" command * Reboot due to "cold start" command * Reboot due to firmware update * Reboot due to kernel panic * Reboot due to unidentified reason

This product stores the current boot information and information on the previous four boots, for a total of five boot records.

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Show boot information	show boot
Clear boot information	clear boot list

Examples of Command Execution

Show boot information

- This shows the current boot information.

```
Yamaha>show boot 0
Running EXEC: SWX2210P Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
Previous EXEC: SWX2210P Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
Restart by reload command
```

- This shows a list of the boot history.

```
Yamaha>show boot list
No. Date      Time      Info
-----
```

```
0 2025/02/12 15:38:15 Restart by reload command
1 2025/02/12 11:19:11 Power-on boot
-----
```

Clear boot information

- This clears the boot information.

```
Yamaha#clear boot list
```

Points of Caution

None.

Related Documentation

None.

Show Chassis Information

Function Overview

Use commands to show chassis information

This product provides the display functions shown in the table below.

Display item	Explanation	Commands
Inventory information	Shows information for this product, such as inventory name, model number, and product ID.	show inventory
Operating information	Shows the operating information for this product's programs, such as running software information, CPU usage, memory usage, boot time.	show environment
Technical support information	Outputs all data relevant to the operating state that might be necessary as analytic information for technical support.	show tech-support

Obtain technical support information remotely

A **TFTP client** installed on a PC or other remote terminal can be used to obtain the **technical support information (the output results of "show tech-support")** from this product.

In order to operate this product's TFTP server, use the steps shown below to set up a network environment that allows remote access.

1. Set the IPv4/IPv6 address on a desired VLAN.
2. Use the "tftp-server enable" command to start the TFTP server function of this product.
3. If necessary, hosts able to access the TFTP server can be specified using the "tftp-server access" command.

If using a TFTP client, specify **techinfo** in the remote path for obtaining technical support information.

Related Commands

Related commands are indicated below.

For details, refer to the Command Reference.

Operations	Operating commands
Show inventory information	show inventory
Show operating information	show environment
Show technical support information	show tech-support

Examples of Command Execution

Show inventory information

Check the inventory information of the main unit.

- Name (NAME)
- Description (DESCR)
- Vendor Name (Vendor)

-
- Product ID (PID)
 - Version ID (VID)
 - Serial number (SN)

```
Yamaha>show inventory
NAME: L2 PoE switch
DESCR: SWX2210P-10G
Vendor: Yamaha
PID: SWX2210P-10G
VID: 0000
SN: 1234567890
```

Show operating information

This checks the system operating information (as shown below).

- Boot version
- PoE version
- Firmware revision
- Serial number
- MAC address
- CPU usage ratio
- Memory usage ratio
- Fan operating status
- Fan RPM
- RTC version
- Startup time
- Current time
- Elapsed time from boot
- Unit temperature status
- Unit temperature

```
Yamaha>show environment
SWX2210P-10G BootROM Ver.1.05
SWX2210P-10G PoEROM Ver.1.2.0.15
SWX2210P-10G Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
main=SWX2210P-10G ver=00 serial=1234567890 MAC-Address=ac44.f200.0000
CPU: 42%(5sec) 43%(1min) 43%(5min) Memory: 51% used
Fan status: Normal
Fan speed: FAN1=2689RPM FAN2=2561RPM
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 00:27:27
Temperature status: Normal
Temperature: 49 degree C
Yamaha>
```

Show technical support information

The following commands show information that is 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

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

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

...

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

Points of Caution

None

Related Documentation

None

Cable Diagnostics Function

Function Overview

The cable diagnostic function can be used to easily check whether or not the LAN cable connected to the LAN port has a faulty connection/circuit.
It can be used to troubleshoot network problems or as an easy way to check cables when setting up networks.

Definition of Terms Used

TDR (Time Domain Reflector)

The TDR is used to measure the length of LAN cables or the location of damage based on the reflected signals from a pulse signal sent through the LAN cables.

Function Details

How to diagnose cables

The cable diagnostic function can easily diagnose LAN cables using the time domain reflection (TDR) method. Cable diagnostics is started by executing the **test cable-diagnostics tdr interface** command.

Item	Description
Cable status	The following cable states can be detected. - OK: The cable is electrically connected. - Open: Either no device is connected on the opposite end or the cable is faulty. - Short: A short circuit occurred. Results are displayed for each pair.
Distance to the cable failure point	If the cable status is "Open" or "Short", then the distance to the fault is displayed. Results are displayed for each pair.
Estimated cable length	If the cable status is OK for all pairs, the estimated cable length is displayed. Measurement is possible only when the link is up.

Results from executing cable diagnostics the previous time can be checked using the **show test cable-diagnostics tdr** command.

Only the immediately previous diagnostic results are retained and then overwritten the next time the cable diagnostics command is executed again.

The immediately previous results can be deleted using the **clear test cable-diagnostics tdr** command.

Related Commands

Related commands are indicated below.

For command details, refer to the command reference.

Operations	Operating commands
Perform the cable diagnostics	test cable-diagnostics tdr interface
Display cable diagnostics	show test cable-diagnostics tdr
Clear cable diagnostic results	clear test cable-diagnostics tdr

Setting Examples

Perform the cable diagnostics

Diagnose of the LAN cable connected to port 1.1 as follows.

```
Yamaha# 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 +/- 15 m
	2	OK	-	
	3	OK	-	
	4	OK	-	

Checking previous diagnostic results

Display the previous diagnostic results as follows.

```
Yamaha# 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 +/- 3 m	
	4	Open	5 +/- 3 m	

Points of Caution

- This function performs simplified diagnostics. Note that it cannot be used for precision diagnosis of more specialized equipment.
- When the **shutdown** command is set for the port to be diagnosed, cable diagnosis cannot be performed.
- Be aware that communication is temporarily stopped during cable diagnostics.
- The estimated cable length cannot be measured when the opposing port is linked up with a link speed of less than 1 Gbps or is shut down.

Related Documentation

- None

Config Management

Function Overview

This product uses the following config information to maintain the value of settings.

Config type	Description	User operations possible
Running config (running-config)	The currently-running setting values. Managed in RAM.	View / Save to startup config
Startup config (startup-config)	Saved setting values. Managed in ROM.	View / Delete
Default config (default-config)	The default setting values. Managed in ROM.	No operations possible

Definition of Terms Used

None

Function Details

Running config

running-config is the settings that are currently operating; since it is maintained in RAM, it is destroyed at reboot. On this product, commands executed in configuration mode are immediately applied to running-config, and the unit operates according to these settings.

The contents of running-config can be viewed by using the **show running-config** command.

Startup config

startup-config is settings that are saved in flash ROM, and the contents are preserved through reboot. When this product is started, the settings of startup-config are applied as the initial settings of running-config.

If you attempt to start up in a state where startup-config does not exist, such as after executing the **cold start** command, the default-config is automatically applied.

The running-config settings can be saved in startup-config by the **copy running-config startup-config** command or the **write** command.

This product can only store one startup config on the flash ROM.

If a startup config exists and you save a new startup config, the old startup config will be overwritten.

The contents of startup-config can be erased by the **erase startup-config** command and viewed by the **show startup-config** command.

Default config

default-config contains settings saved in internal flash ROM that are needed for this product to operate minimally as a switch. Like startup-config, the contents are preserved even after a restart.

The factory settings are maintained as default-config.

If startup-config does not exist when the system starts, default-config is copied to startup-config, and applied to running-config.

The contents of default-config cannot be viewed.

Deciding the config file at startup

The following describes the flow for deciding the config file used when this product starts up.

1. If the startup-config exists, the corresponding data is applied as running-config in RAM.
2. If startup-config does not exist in ROM, default-config is applied as running-config in RAM.

Controlling the config file via TFTP

If this product's TFTP server function is enabled, a TFTP client installed on a PC or other remote terminal can be used to perform the following.

1. Acquire the currently running running-config and startup-config
2. Apply previously prepared settings files as running-config and startup-config

In order for the TFTP server to function correctly, an IP address accessible to this product must be specified. The settings files can be acquired/set from a remote terminal in binary mode. Specify the following as the remote path of the acquisition source/transmission destination of the settings files.

Settings file to be acquired/set	Remote path of the acquisition source/transmission destination
running-config	config
startup-config # 0	config0
startup-config # 0 (config only)	reconfig (destination only)

- The startup-config settings are applied as running-config after the system is restarted.
- If you specify "reconfig" as the destination remote path, this product will automatically restart after receiving the settings file.

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Save running config	copy running-config startup-config
Save running config	write
Erase startup config	erase startup-config
Show startup config	show startup-config

Examples of Command Execution

Save running config

Save running-config.

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

Erase startup config

Erase startup-config.

```
Yamaha#erase startup-config ①
erasing...[OK]
Yamaha#
```

① Erase startup-config

Points of Caution

None

Related Documentation

None

Remote Access Control

Function Overview

This product lets you restrict access to the following applications that implement network services.

- TELNET server
- HTTP server / secure HTTP server
- TFTP server
- SNMP server

Definition of Terms Used

None

Function Details

The following three functions are provided to limit access to network services.

- Control whether to leave the service in question running in the background on the system (start/stop control)
- Change reception port number
- Limit the source IP addresses that can access services currently running

The following functions that correspond to each network service are shown in the table below.

- Network service access control

Network service	Start/stop control	Change reception port number	Access source restriction
TELNET server	Yes	Yes	Yes
HTTP server	× (Always booted)	Yes	Yes
Secure HTTP server	Yes	Yes	Yes
TFTP server	Yes	Yes	Yes
SNMP server	× (Always booted)	× (Always 161)	Yes

1. Multiple instances of a network service cannot be started.
If the start control is applied to the same service that is currently running, the service will restart.
Consequently, any connected sessions will be **disconnected**.
2. When restricting access to network services, you can specify the **source IP address (*1)** and whether to **allow or deny access (*2)**.
(*1)...SNMP servers also allow you to specify the community name or user name of the access destination
(*2)...SNMP servers only allow you to specify the access permission conditions.
3. The default settings for the network services are shown in the table below.

Network service	Start/stop status	Reception port number	Access source restriction
TELNET server	run	23	Allow all

Network service	Start/stop status	Reception port number	Access source restriction
HTTP server	run	80	Allow all
Secure HTTP server	run	443	
TFTP server	stop	69	Allow all
SNMP server	run	161	Allow all

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Network service	Operations	Operating commands
TELNET server	Start/stop and change reception port number	telnet-server enable (use argument to specify port number)
	IP address access control	telnet-server access
	Show settings	show telnet-server
HTTP server	Change HTTP server's reception port number	http-server enable (use argument to specify port number)
	Start/stop secure HTTP server and change reception port number	http-server secure enable (use argument to specify port number)
	IP address access control	http-server access
	Show settings	show http-server
TFTP server	Start/stop and change reception port number	tftp-server enable (use argument to specify port number)
	IP address access control	tftp-server access
SNMP server	Access control by IP address and community name or user name	snmp-server access

Examples of Command Execution

TELNET server access control

This example restricts access to the TELNET server.

Change the TELNET server's reception port to 1024.

Connection to the TELNET server is allowed only by clients from 192.168.100.1.

If you specify telnet-server access, access from IP addresses that do not meet the conditions is denied.

```

Yamaha(config)#telnet-server enable 1024 ①
Yamaha(config)#telnet-server access permit 192.168.100.1 ②
Yamaha(config)#end
Yamaha#show telnet-server ③
Service:Enable
Port:1024
Access:

```

```
permit 192.168.100.1
```

- ① Change the reception port to 1024 and reboot the TELNET server
- ② Allow access only from 192.168.100.1
- ③ Check the settings

HTTP server access restrictions

This example restricts access to the HTTP server.

Change the HTTP server's reception port to 8000 and the secure HTTP server's reception port to 9000.

Connection to the HTTP server is allowed only by clients from 192.168.100.1.

If you specify http-server access, access from IP addresses that do not meet the conditions is denied.

```
Yamaha(config)#http-server enable 8000 ①
Yamaha(config)#http-server secure enable 9000 ②
Yamaha(config)#http-server access permit 192.168.100.1 ③
Yamaha(config)#end
Yamaha#show http-server ④
HTTP :Enable(8000)
HTTPS:Enable(9000)
Access:
    permit 192.168.100.1
```

- ① Change the reception port to 8000 and reboot the HTTP server
- ② Change the reception port to 9000 and reboot the secure HTTP server
- ③ Allow access only from 192.168.100.1
- ④ Check the settings

TFTP server access restrictions

This example restricts access to the TFTP server.

Change the TFTP server's reception port to 2048.

Connection to the TFTP server is allowed only by clients from 192.168.100.1.

```
Yamaha(config)#tftp-server enable 2048 ①
Yamaha(config)#tftp-server access permit 192.168.100.1 ②
```

- ① Change the reception port to 2048 and reboot the TFTP server
- ② Allow access only from 192.168.100.1

SNMP server access restrictions

This restricts access to the SNMP server.

Access to "public" communities is restricted to clients from 192.168.100.0/24.

In addition, access to "private" communities is restricted to clients from 192.168.100.1.

```
Yamaha(config)#snmp-server access permit 192.168.100.0/24 community public ①
Yamaha(config)#snmp-server access permit 192.168.100.1 community private ②
```

- ① The community name "public" allows access only from 192.168.100.0/24

② The community name “private” allows access only from 192.168.100.1

Access to the SNMP server is restricted to clients with username “user1” from 192.168.100.0/24.

```
Yamaha(config)#snmp-server access permit 192.168.100.0/24 user user1 ①
```

① Allow access only from 192.168.100.0/24 and the username “user1”

Points of Caution

If you change the IPv4/IPv6 address settings, all settings related to restrictions on access source IP address will be reset.

Use particular caution when changing the IPv4/IPv6 address settings.

Related Documentation

- [User account management](#)

Time Management

Function Overview

This product provides the functions shown below for managing the date and time.

- Manual (user-configured) date/time information setting function
- Automatic date/time setting information function via network
- Time zone setting function

Note that a function to set summertime (DST: Daylight Saving Time) is not provided.

Definition of Terms Used

UTC (Coordinated Universal Time)

This is an official time used when recording worldwide times.

UTC is used as a basis to determine standard time in all countries around the world.

For instance, Japan (JST, or Japan standard time) is nine hours ahead of Coordinated Universal Time, and is thus shown as "+0900 (JST)".

SNTP (Simple Network Time Protocol)

This is a simple protocol to correct clocks by using SNTP packets.

This protocol is defined in RFC4330.

Function Details

Manually setting the date and time

Use the **clock set** command to directly enter clock setting values.

Automatically setting the date and time

Date and time information is collected from a specified time server, and set in this product.

Defined in RFC4330, SNTP (Simple Network Time Protocol) is used as a communication protocol.

Up to two time servers can be specified using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN).

Port number 123 is used for the SNTP client. (This setting cannot be changed by the user.)

The **ntpdate** command can be used to select one of two methods for automatically setting date and time settings.

- One-shot update (a function to update when a command is inputted)
- Interval update (a function to update in a 1–24-hour cycle from command input)

If clock settings are synchronized with two time servers specified, queries are processed in the order they are displayed by the **show ntpdate** command, which is NTP server 1 and then NTP server 2.

Queries to NTP server 2 are only processed if synchronization with NTP server 1 fails.

By default, interval updates are not performed.

If a time server is specified and interval update is enabled, but the default time cannot be set, the time server will be queried one minute after the port is linked up, regardless of the interval cycle time.

Synchronization is blocked during command execution, and an error message is outputted if a timeout occurs.

Time zone setting

In order to manage the time for the region considered as the “base of daily life”, the “clock timezone” command is used to manage the time zone of the users, and reflect this into the time.

The time zone can be set in ± 1 hour increments for Coordinated Universal Time (UTC), from -12 hours to +13 hours.

The default time zone value for this product is **+9.0**.

Related Commands

Related commands are indicated below.

For details, refer to the Command Reference.

Operations	Operating commands
Set clock manually	clock set
Set time zone	clock timezone
Show current time	show clock
Set NTP server	ntpdate server
Synchronize time from NTP server (one-shot update)	ntpdate oneshot
Synchronize time from NTP server (update interval)	ntpdate interval
Show NTP server time synchronization settings	show ntpdate

Examples of Command Execution

Set clock manually

In this example, the time zone is set to **JST** and the current time is set to **2018.11.01 15:50:59**.

```
Yamaha#configure terminal
Yamaha(config)#clock timezone JST ①
Yamaha(config)#exit
Yamaha#clock set 15:50:59 Nov 1 2018 ②
Yamaha#show clock ③
15:50:59 JST Thu Jan 1 2018
```

- ① Time zone setting
- ② Time settings
- ③ Show current time

Automatically setting the time

In this example, the time zone is set to **+9.00** and the local address **192.168.1.1** and **ntp.nict.jp** are specified as the NTP servers.

Also, the NTP server update cycle is changed to **once every 24 hours**.

```
Yamaha#configure terminal
Yamaha(config)#clock timezone +9:00 ①
Yamaha(config)#ntpdate server ipv4 192.168.1.1 ②
Yamaha(config)#ntpdate server name ntp.nict.jp ③
```

```
Yamaha(config)#ntpdate interval 24 ④
Yamaha(config)#exit
Yamaha#show clock ⑤
10:03:20 GMT+9:00 Wed Oct 10 2018
Yamaha#show ntpdate ⑥
NTP server 1 : 192.168.1.1
NTP server 2 : ntp.nict.jp
adjust time : Wed Oct 10 11:46:30 2018 + interval 24 hour
sync server : 192.168.1.1
```

- ① Time zone setting
- ② Set NTP server
- ③ Set NTP server
- ④ Set NTP server update cycle to 24 hours
- ⑤ Show current time
- ⑥ Show NTP time synchronization settings

Points of Caution

None

Related Documentation

- [RFC 4330: Simple Network Time Protocol \(SNTP\) Version 4 for IPv4, IPv6 and OSI](#)

SNMP

Function Overview

Setting SNMP (Simple Network Management Protocol) makes it possible to monitor and change network management information for SNMP management software. In this instance, this product will operate as an SNMP agent.

This product supports communication using SNMPv1, SNMPv2c, and SNMPv3. In terms of management information bases (MIB), it supports RFC1213 (MIB-II) and private MIBs (Yamaha switches).

SNMPv1 and SNMPv2c notify the recipient of the group name (called a “community”), and communicate only with hosts that belong to that community. In this instance, different community names can be given for the two access modes, read-only and read-write.

In this sense, community names function as a kind of password; but since community names are sent over a network using plain text, they carry inherent security risks. The use of SNMPv3 is recommended when more secure communications are required.

SNMPv3 offers communication content authentication and encryption. SNMPv3 does away with the concept of community and instead uses security models called “USM” (User-based Security Model) and “VACM” (View-based Access Control Model). These models provide a higher level of security. This product does not use VACM for access control.

SNMP messages that notify the status of this product are called “traps.” This product transmits standard SNMP traps. In SNMPv1, trap requests that do not ask for an answer with the confirmation of receipt from the recipient are specified as the notification message format. However, with SNMPv2c and SNMPv3, either an “inform” request asking for an answer from the recipient, or a trap request can be selected.

Since this product does not specifically determine a default value for the read-only and community trap names used in SNMPv1 and SNMPv2c, you can specify a community name as appropriate. However, community names are sent over the network in plain text, so be careful to never use a login password or administrator password as the community name.

By default, no access is possible in each SNMP version. The transmission host for the trap is not set, so traps will not be sent anywhere.

This product can restrict access to the SNMP server. Specifying access restrictions can restrict access from unintended hosts.

Definition of Terms Used

None

Function Details

The main characteristics of each SNMP version and the SNMP setting policies are explained below. For specific examples of settings, see [“Examples of Command Execution”](#) below.

SNMPv1

This is authentication between the SNMP manager and agent by using community names. The controlling device (this product) is divided and managed by zones called “communities”.

- Accessing the MIB objects

Community names specified using the **snmp-server community** command are used to permit access. Access is possible from a VLAN interface whose IP address has been specified.

- SNMP traps

The status of switches can be sent to hosts specified using the **snmp-server host** command.

The **snmp-server enable trap** command is used to specify the kind of trap to send.

SNMPv2c

As with SNMPv1, community names are used for authentication between the SNMP manager and agents. The **snmp-server community** command is used to specify the community names used to access switches by SNMPv2c.

The “GetBulk” and “Inform” requests are also now supported from this version.

These requests are used to efficiently retrieve multiple MIB objects, and to confirm replies to notification packets sent from this product.

- Accessing the MIB objects

Community names specified using the **snmp-server community** command are used to permit access. Access is possible from a VLAN interface whose IP address has been specified.

- SNMP traps

The status of switches can be sent to hosts specified using the **snmp-server host** command.

Also, the settings of this command can be used to select whether the transmitted message format is a trap or inform request.

Inform requests are used to request confirmation of reply to the recipient.

SNMPv3

In addition to all of the functions offered in SNMPv2, SNMPv3 offers more robust security functions. SNMPv3 can authenticate and encrypt SNMP packets sent across the network to protect packets from eavesdropping, spoofing, falsification, replay attacks, and other risks and achieve security levels not possible with SNMPv1 or SNMPv2c functionality, such as community names or SNMP manager IP addresses.

- Security

SNMPv3 offers the following security functions.

1. USM (User-based Security Model)

USM is a model for maintaining security at the message level. It offers authentication and encryption based on shared key cryptography and prevents falsification of message streams.

- Security level

This product supports the following security levels. Communications are always authenticated and encrypted.

- AuthPriv : authentication and encryption

- User authentication

For authentication, HMAC is used in the procedure to authenticate the integrity (whether data has been falsified or not) and the source.

A hash is used in the authentication key to confirm whether the message has been falsified, and whether the sender is the user themselves.

HMAC-SHA-96 is supported as the hash algorithm.

- Encryption

With SNMPv3, SNMP messages are encrypted for the purpose of preventing leakage of managed information.

The AES128-CFB encryption scheme is supported.

The **snmp-server user** command can be used to specify usernames, access privileges, and passwords.

This product allows you to set up one ReadOnly user and one ReadWrite user.

2. VACM (View-based Access Control Model)

VACM is a model for controlling access to SNMP messages.

- This product does not use VACM for access control, so all MIB views are accessible.

- **SNMP traps**

The status of switches can be sent to hosts specified using the **snmp-server host** command.

In order to transmit a trap, the **snmp-server user** command must first be used to configure the user.

Also, the settings of this command can be used to select whether the transmitted message format is a trap or inform request.

Inform requests are used to request confirmation of reply to the recipient.

Restricting SNMP server access

Hosts able to access the product's SNMP server can be specified using the **snmp-server access** command.

Access from unintended hosts can be restricted by only allowing access from the intended SNMP manager.

Default settings accept access from all hosts. Specify access restrictions based on the operating environment.

For more information about access restrictions, refer to [Remote Access Control](#).

Private MIBs

This product supports yamahaSW, which is a proprietary private MIB for switch management.

This private MIB allows the obtaining of information for Yamaha's proprietary functions, and for more detailed information about the switch.

For information about supported private MIBs and how to obtain private MIBs, refer to the "SNMP MIB Reference" chapter in the HTML version of this document.

Related Commands

Related commands are indicated below.

For details on the commands, refer to the Command Reference.

Operations	Operating commands
Set host that receives SNMP notifications	snmp-server host
Set notification type to transmit	snmp-server enable trap
Set system contact	snmp-server contact
Set system location	snmp-server location
Set SNMP community	snmp-server community
Set SNMP user	snmp-server user
Specify SNMP server access settings	snmp-server access
Show SNMP community information	show snmp community
Show SNMP user information	show snmp user

Examples of Command Execution

SNMPv1 setting example

This example makes SNMPv1-based network monitoring possible under the following conditions.

1. Set the read-only community name to "public".
2. Set the trap destination as "192.168.100.11", and set "snmptrapname" as the trap community name.
3. Hosts that can access communities named "public" are restricted to only 192.168.100.0/24.

```
Yamaha(config)# snmp-server community public ro ... 1
Yamaha(config)# snmp-server host 192.168.100.11 traps version 1 snmptrapname ... 2
Yamaha(config)# snmp-server access 192.168.100.0/24 community public ... 3
```

SNMPv2c setting example

This example makes SNMPv2c-based network monitoring possible under the following conditions.

1. Set the readable/writable community name as "private".
2. Specify the notification message destination as "192.168.100.12", the notification type as "inform" request format, and the notification destination community name as "snmpinformsname".
3. Hosts that can access communities named "private" are restricted to only 192.168.100.12.

```
Yamaha(config)# snmp-server community private rw ...1
Yamaha(config)# snmp-server host 192.168.100.12 informs version 2c snmpinformsname ...2
Yamaha(config)# snmp-server access 192.168.100.12 community private ...3
```

SNMPv3 setting example

This example makes SNMPv3-based network monitoring possible under the following conditions.

1. Create a user "admin1" with the ReadWrite privilege.
The authentication algorithm is fixed to "HMAC-SHA-96". Set the password "passwd1234".
The encryption algorithm is fixed to "AES128-CFB". Set the encryption password "passwd1234".
2. Create a user "user1" with the ReadOnly privilege.
The authentication algorithm is fixed to "HMAC-SHA-96". Set the password "passwd5678".
The encryption algorithm is fixed to "AES128-CFB". Set the encryption password "passwd5678".
3. Send notifications in trap format (without response confirmation) to 192.168.10.3.
4. Send notifications in inform request format to 192.168.20.3.

```
Yamaha(config)# snmp-server user admin1 admin auth sha passwd1234 priv aes passwd1234
... 1
Yamaha(config)# snmp-server user user1 guest auth sha passwd5678 priv aes passwd5678
... 2
Yamaha(config)# snmp-server host 192.168.10.13 traps version 3 priv admin1
... 3
Yamaha(config)# snmp-server host 192.168.20.13 informs version 3 priv admin1
... 4
```

Points of Caution

- Check the SNMP version that can be used with the SNMP manager beforehand. It is necessary to configure this product in accordance with the SNMP version that will be used.
- The specifications of character strings for community name are as follows.
 - When enclosed in "", the character string in "" is used.
 - The case where there is a character string outside the "" is not supported.
 - The use of \ is not supported.
 - The use of only double quotation marks is not supported.

Related Documentation

- [Yamaha RTpro SNMP](#)
- [Yamaha RTpro Private MIB](#)
- [SNMP MIB Reference](#)
- [Remote Access Control](#)

SYSLOG

Function Overview

This product provides the SYSLOG functions shown below as a means to ascertain the operating state.

1. Functions to collect, reference, and delete the log that is accumulated inside this product
2. Functions for output to the TELNET console simultaneously with logging
3. Functions for transmitting to a previously-registered notification destination (SYSLOG server) simultaneously with logging

Logging, output to the TELNET console, and notifications to the SYSLOG server are performed according to the output level specified by the user. Processing occurs only for the permitted messages.

Logging occurs in RAM, and is automatically backed up to flash ROM or can be backed up manually.

Notifications to the SYSLOG server are done simultaneously with logging, but only if a SYSLOG server has been registered.

Definition of Terms Used

None

Function Details

The SYSLOG function is described below.

1. Logging occurs in RAM, and can accumulate up to 1500 items.
The following three methods for backing up to a flash ROM are available.
 - Automatic backup performed every hour since system boot
 - Manual backup performed by the **save logging** command
 - Automatic backup for system restart that occurs due to reload command or firmware update
2. The logs accumulated in RAM can be viewed by the **show logging** command.
The RAM and flash ROM logs can be deleted using the **clear logging** command.
The log information in RAM will not be deleted by execution of a backup.
In addition, the logs backed up in the flash ROM are expanded into RAM when the system is started.
Therefore, even if the system is restarted using the reload command or firmware update, new logs will be accumulated as continuation of the logs at the previous startup.
3. Log transmission occurs only if the notification destination (SYSLOG server) has been registered.
You can use the **logging host** command to register up to two notification destinations.
Specify the notification destination either by IP address or FQDN.
As the port number of the notification destination, the default port number 514 is used. (This setting cannot be freely set by the user.)
The **logging format** command can be used to change the format of log notifications to not include the header portion (time stamp and host name). The following are log examples.
 - Without the format specified (no logging format)

```
<134>Jan  1 00:00:00 Yamaha [    IMI]:inf: Configuration file is saved in  
"config0"
```

- With the format specified (logging format legacy)

```
<134>[ IMI]:inf: Configuration file is saved in "config0"
```

- The level of log that is transmitted (SYSLOG priority) can be set using the **logging trap** command.
This product allows you to enable or disable output for each level of log.
With the factory settings, the output level enables only Information and Error.

List of Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Function name	Command name
Set log output level	logging trap
Set log output destined to TELNET console	logging stdout
Set log notification destination (SYSLOG server)	logging host
Change the log notification format	logging format
Back up log	save logging
Clear log	clear logging
Show log	show logging

Examples of Command Settings

- Enable debug-level log output, and start log output to the SYSLOG server (192.168.1.100).
Also output informational-level log to the TELNET console.

```
Yamaha(config)# logging trap debug ①  
Yamaha(config)# logging host 192.168.1.100 ②  
Yamaha(config)# logging stdout info ③
```

- ① Enable the debug-level log output
- ② Register a SYSLOG server
- ③ Output an informational-level log to the TELNET console

- Stop notifications to the SYSLOG server.

```
Yamaha(config)# no logging host
```

- Save and show the accumulated log information.

```
Yamaha# save logging ①  
Yamaha# show logging ②  
2018/10/05 15:58:47:[ L2MS]:inf: Start L2MS(Agent)  
2018/10/05 15:58:47:[ VLAN]:inf: Interface vlan1 changed state to up  
2018/10/05 15:58:47:[ IF]:inf: Interface port1.4 changed state to up (10-half)  
2018/10/05 15:58:49:[ L2MS]:inf: Start management by manager(00a0.dec9.d6d2)  
2018/10/05 15:59:32:[ DHCP]:inf: DHCP gets IP address: 192.168.1.9
```

```
2018/10/05 15:59:46:[ SESSION]:inf: Login succeeded as (noname) for TELNET: 192.168.1.6
:
```

- ① Save the log in RAM to ROM
- ② Show the accumulated logs

4. Clear the accumulated log information.

```
Yamaha# clear logging ①
Yamaha# show logging ②
③
```

- ① Clear all accumulated logs
- ② Show the logs
- ③ Nothing is shown because they have been erased

Points of Caution

None

Related Documentation

None

Firmware Update

Function Overview

This product offers the following two firmware update functions, in order to correct problems in the program and to add new functionality.

1. Firmware updates can be transmitted and applied to this product from a remote terminal such as a computer.
2. This product's built-in HTTP client can access an HTTP server, to download and apply the latest firmware.

These update functions can be used to upgrade or downgrade the version of firmware used on this product.

Note that a firmware version downgrade from Rev.1.03.13 or later version to Rev.1.03.12 or earlier version is not possible due to compatibility with new parts.

When successfully finished writing the updated firmware, the **system is automatically rebooted in order to apply the new firmware.**

Definition of Terms Used

None

Function Details

Update by transmitting the firmware update

This function transmits firmware updates to this product from a remote terminal, such as a computer, and applies it as boot firmware.

The update process is executed using a **TFTP client** or the **Web GUI**.

Using a TFTP client to update the firmware

Firmware can be updated by using a **TFTP client** installed on a computer or other remote terminal to transmit the updated firmware to this device.

In order to operate this product's TFTP server, use the steps shown below to set up a network environment that allows remote access.

1. Set the IPv4/IPv6 address on a desired VLAN.
2. Enable the TFTP server. Enable the server using the **tftp-server enable** command.
3. If necessary, hosts able to access the TFTP server can be specified using the **tftp-server access** command.

Follow the rules below when sending the firmware update using the TFTP client.

- Set the transmission mode to "**binary mode**".
- As shown in the table below, specify the remote path to which the firmware update is sent.
- If an administrative password has been specified for this product, use the form **"/PASSWORD"** to specify the administrative password following the remote path.

When updating firmware that uses TFTP clients, the following two types of updates are possible.

- Updated firmware

Type	Remote path
Internal firmware	exec

Type	Remote path
Boot loader	boot

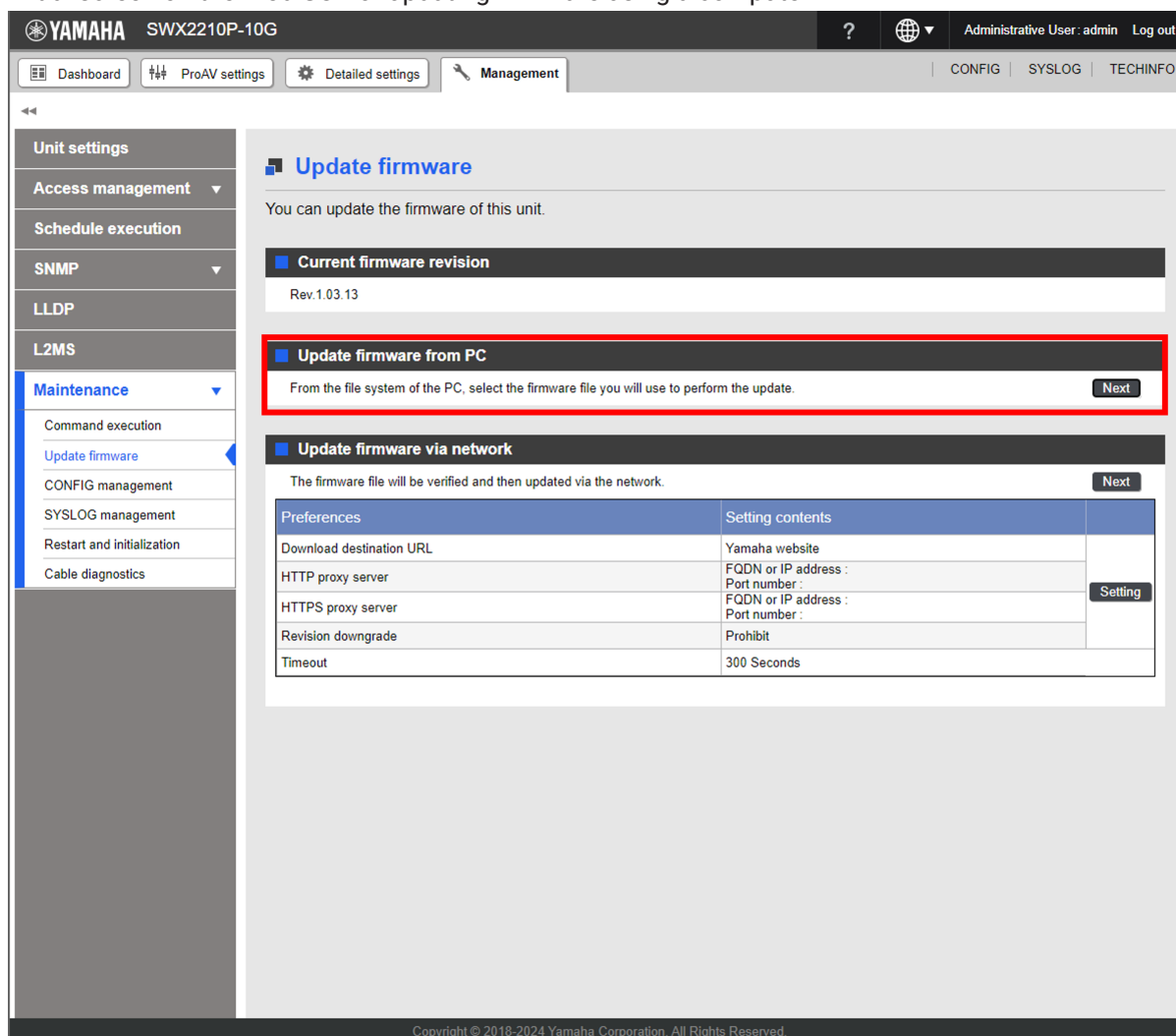
If there is no problem with the firmware update that was sent, the firmware update will be saved.

Updating the firmware by specifying a local file in the Web GUI

Specify the firmware update located on the terminal accessing the Web GUI, and apply it to this product. This function does not do a version comparison with the existing firmware, and will overwrite the specified firmware regardless of version.

To update firmware by specifying a local file, click **[Maintenance] - [Firmware update]** in the Web GUI on the computer. (Refer to the part shown in a red frame on the screenshot below.) Refer to the help contents within the GUI for the specific operation method.

- Initial screen on the Web GUI for updating firmware using a computer



Using an HTTP client to update the firmware

This method of firmware update uses an HTTP client to obtain the firmware update from a specified URL, and then apply it to this product.

This function assumes that the firmware version will be upgraded. Downgrading to a previous version will only be permitted only if the downward revision permission is given.

The firmware cannot be rewritten with the same version of firmware.

An HTTP client can be used to update the firmware using the methods below.

- Use the **firmware-update** command in the CLI (command-line interface).
- Execute **update firmware via network** in the Web GUI.

Updating the firmware with an HTTP client is done by using the settings value shown in the table below.

Setting parameter	Explanation
Download source URL	<p>Sets the source URL from which the firmware is downloaded. A URL of up to 255 characters in length can be set.</p> <p>The initial value is set as follows for each model.</p> <p>SWX2210P-10G: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin</p> <p>SWX2210P-18G: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-18g.bin</p> <p>SWX2210P-28G: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-28g.bin</p>
HTTP proxy server	<p>Specifies the proxy server to use for updating firmware.</p> <p>Specify it either as an IPv4/IPv6 address or FQDN. FQDNs can be up to 255 characters long.</p> <p>No proxy server is specified in default settings.</p>
HTTPS proxy server	
Permit downward revision	<p>Sets whether the current version of firmware can be downgraded to a previous version.</p> <p>The default value is “Don’t allow”.</p> <p>Overwriting the firmware with the same version of firmware is not permitted.</p>
Timeout	<p>Specifies the timer for monitoring the completion of the processes shown below.</p> <p>* Version check of old and new firmware</p> <p>* The download monitoring timer from the specified URL can be specified from 100 seconds to 86,400 seconds, and the initial setting is set to 300 seconds.</p>

For instructions on using the **firmware-update** command, refer to “[Examples of Command Execution](#)” or the “[Command Reference](#)”.

To **update firmware over the network** using the Web GUI, execute **[Maintenance] - [Firmware update]** on the Web GUI. (Refer to the part shown in a red frame on the screenshot below.)

Refer to the help contents within the GUI for the specific operation method.

- Initial Web GUI Screen for Updating Firmware via the Network

SWX2210P-10G

?

Administrative User: admin
Log out

Dashboard
ProAV settings
Detailed settings
Management
CONFIG
SYSLOG
TECHINFO

Unit settings
Access management
Schedule execution
SNMP
LLDP
L2MS
Maintenance
Command execution
Update firmware
CONFIG management
SYSLOG management
Restart and initialization
Cable diagnostics

Update firmware

You can update the firmware of this unit.

Current firmware revision

Rev.1.03.13

Update firmware from PC

From the file system of the PC, select the firmware file you will use to perform the update.

Next

Update firmware via network

The firmware file will be verified and then updated via the network.

Next

Preferences	Setting contents	
Download destination URL	Yamaha website	
HTTP proxy server	FQDN or IP address : Port number :	
HTTPS proxy server	FQDN or IP address : Port number :	
Revision downgrade	Prohibit	
Timeout	300 Seconds	

Setting

Copyright © 2018-2024 Yamaha Corporation. All Rights Reserved.

Reboot after writing

When successfully finished writing the firmware update, the system is automatically rebooted.

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Set firmware update site	firmware-update url
Specify HTTP proxy server to use for updating firmware	firmware-update http-proxy
Specify HTTPS proxy server to use for updating firmware	firmware-update https-proxy
Execute firmware update	firmware-update execute
Set firmware download timeout duration	firmware-update timeout
Permit downward revision	firmware-update revision-down
Show firmware update function settings	show firmware-update

Examples of Command Execution

Using an HTTP client to update the firmware

In this example, the firmware update is stored on the local HTTP server, and this product is set to manage the firmware in order to perform the update.

- Change the download URL to **http://192.168.100.1/swx2210p-10g.bin**.
 - The downward revision setting is left **disabled**.
 - The timeout value is left at **300 sec**.
1. The download URL is changed, and the firmware update settings are confirmed.

```
Yamaha(config)#firmware-update url http://192.168.100.1/swx2210p-10g.bin ①
Yamaha(config)#exit
Yamaha#show firmware-update ②
url:http://192.168.100.1/swx2210p-10g.bin
timeout:300 (seconds)
revision-down:disable
```

- ① Set download source URL
- ② Show firmware update function settings

2. The firmware update is executed.

```
Yamaha#firmware-update execute ①
Found the new revision firmware
Current Revision: Rev.1.03.01
New Revision:     Rev.1.03.02
Update to this firmware? (Y/N)y ②
Download...
%% Completed the firmware download
%% Updating...

③
```

- ① Execute firmware update
- ② Enter y
- ③ The system automatically reboots

3. Pressing "CTRL+C" during the firmware update process will interrupt the update.

```
Yamaha#firmware-update execute
Found the new revision firmware
Current Revision: Rev.1.03.01
New Revision:     Rev.1.03.02
Update to this firmware? (Y/N)y
Download... ①
%% Canceled the firmware download
```

- ① Press the Ctrl and C keys

Points of Caution

Note that a firmware version downgrade from Rev.1.03.13 or later version to Rev.1.03.12 or earlier version is not possible due to compatibility with new parts.

Related Documentation

- [LED Indicator Control](#)

L2MS (Layer2 Management Service)

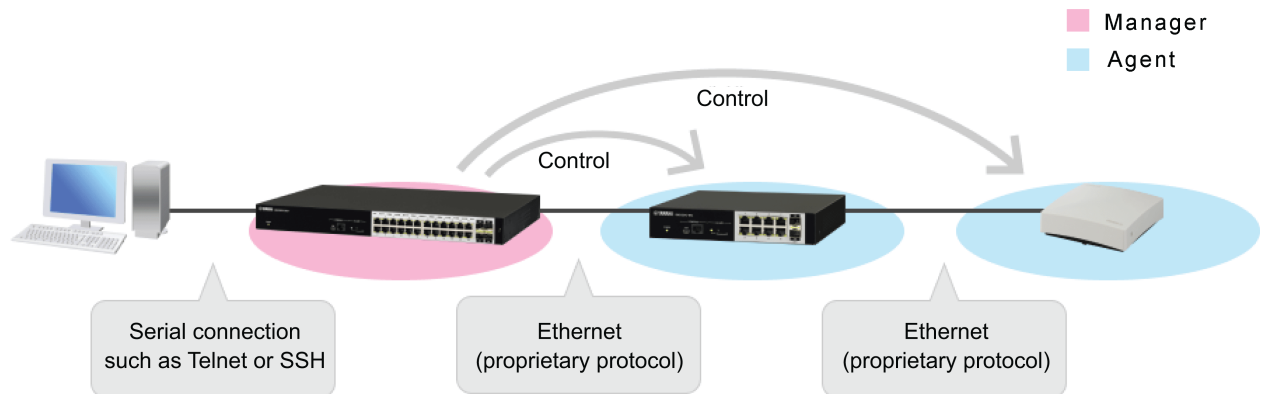
Function Overview

L2MS (Layer2 Management Service) is functionality for managing Yamaha network devices at the layer 2 level. L2MS consists of one manager that performs centralized control and multiple agents that are controlled by the manager.

The SWX2210P functions as an L2MS agent.

The following illustrates how to connect the computer, manager, and agents.

- L2MS connection method



The L2MS manager includes commands for managing the agents and a web GUI for specifying the settings or checking the status of agents. These can be used to operate the agents.

The manager is connected to agents via Ethernet cables and uses a proprietary protocol for communication.

This functionality has the following characteristics.

- Initial settings are not required
Although IP addresses must be specified if using Telnet or SSH, default settings do not need to be specified for agents, because the functionality uses a proprietary protocol for communication. When Ethernet cables are connected, the manager automatically recognizes subordinate agents.
- Multiple supported terminals can be controlled simultaneously
The manager can recognize and control multiple agents simultaneously.

For details on the managers that can manage the SWX2210P, refer to the technical information on each L2MS manager.

- [Technical Reference: LAN Map/Switch Control GUI/Yamaha LAN Monitor: Function Comparison Table](#)

Definition of Terms Used

Manager

A manager is a device that manages Yamaha network devices functioning as an agent based on L2MS and switch control functionality.

It manages Yamaha network switches and Yamaha wireless access points within the network.

Agent

A Yamaha network switch or Yamaha wireless access point that is managed by a manager based on L2MS and switch control functionality.

Settings can be checked or changed from the manager.

Function Details

Compatible models

For manages that can manage the SWX2210P as an agent, see the link below.

- [Technical Reference: LAN Map/Switch Control GUI/Yamaha LAN Monitor: Function Comparison Table](#)

L2MS protocol

L2MS control is performed using the proprietary protocol L2 frames indicated below.

- Content of L2MS Protocol L2 Frames

Item	Value
Destination MAC	01:a0:de:00:e8:12 to 01:a0:de:00:e8:15
Ethertype	0xe812

If a firewall is specified between the manager and agents, the firewall settings must allow these L2 frames to pass through.

Also, when using Yamaha LAN Monitor to update the SWX2210P series firmware with L2MS, use the following unicast L2MS.

- Content of Unicast L2MS Protocol L2 Frames

Item	Value
Destination MAC	Unicast destination MAC address
Ethertype	0xe813

Monitoring agents

Managers monitor subordinate agents by sending query frames at regular intervals.

Agents respond to query frames by sending a response frame to notify the manager that they exist.

For the settings for query frames to be sent by the manager, refer to the technical information on the manager.

Agent ownership

No agent may be simultaneously controlled by multiple managers.

Therefore, only specify one manager per network.

If an agent receives a query frame after rebooting, that agent will be managed by the manager that sent the query frame.

That relationship is canceled if any of the following occur.

- The agent has not received a query frame for 30 seconds
- The manager is restarted, or the management status of the L2MS is reset

Agent operations

If a manager sets a setting for an L2MS-compliant agent or checks its operating status, such actions are referred to as “operating the agent”.

Each manager is provided with commands and a web GUI for operating the agents.

For detailed operating instructions, refer to the technical information on each manager.

Information notifications from agents

If an agent managed by a manager detects a change or error in its own status, it sends information to notify the manager.

Information sent from the agent is output in the manager SYSLOG or web GUI.
For details, refer to the technical information on each manager.

The following information is included in notifications from the SWX2210P.

- Port link up/down status
- Loop detection
- Fan stopped due to error
- Per-port power supply function status
- Per-device power supply function error

L2MS filter/non-L2MS filter

By using the L2MS filter function, you can prohibit the transmission and reception of L2MS control frames used for L2MS control.

By using the non-L2MS filter function, you can also restrict the transmission and reception of frames other than L2MS control frames.

The L2MS filter and non-L2MS filter can be set on a per-port basis. When setting them, use the **l2ms filter** command and **non-l2ms filter** command, respectively.

Enabling/disabling L2MS

You can enable/disable L2MS using the **l2ms enable** and **l2ms disable** commands.

If L2MS is disabled, L2MS control frames are forwarded in the same way as frames other than L2MS control frames, and they can no longer be managed by the L2MS manager.

L2MS is enabled by default.

Default IP address

In the factory default settings or the status immediately after execution of the **cold start** command, a fixed IP address is set. (L2MS functions as an agent.)

At this time, if the agent is managed by the manager, **the DHCP client setting will automatically be configured.**

This is to avoid duplicate IP addresses if multiple agents exist.

Since IP addresses are assigned by the DHCP server within the network, agent web GUIs can be accessed via the HTTP proxy server.

If a DHCP server does not exist in the network, then IP addresses cannot be obtained and agent IP addresses must be specified on the manager LAN map.

Once the IP setting is specified and the startup config has been saved, it will not be automatically specified in the DHCP client thereafter.

Related Commands

Related commands are indicated below.

For details, refer to the Command Reference.

- Basic interface functions: list of related commands

Operations	Operating commands
Switch to L2MS mode	l2ms configuration
Enable L2MS function	l2ms enable
Enable sending/receiving L2MS control frames	l2ms filter
Enable sending/receiving frames other than L2MS control frames	non-l2ms filter
Show L2MS information	show l2ms

Examples of Command Execution

L2MS filter setting

- Disable sending or receiving L2MS control frames at LAN port #1 (port1.1).

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#l2ms filter enable
```

L2MS setting

- Disable L2MS so that it cannot be managed by the L2MS manager.

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#l2ms disable
```

Points of Caution

For precautions on using L2MS, refer to the technical information on each manager.

Use in conjunction with other functionality

Use in conjunction with loop detection functionality

L2MS communication is not possible on ports blocked by loop detection functionality.

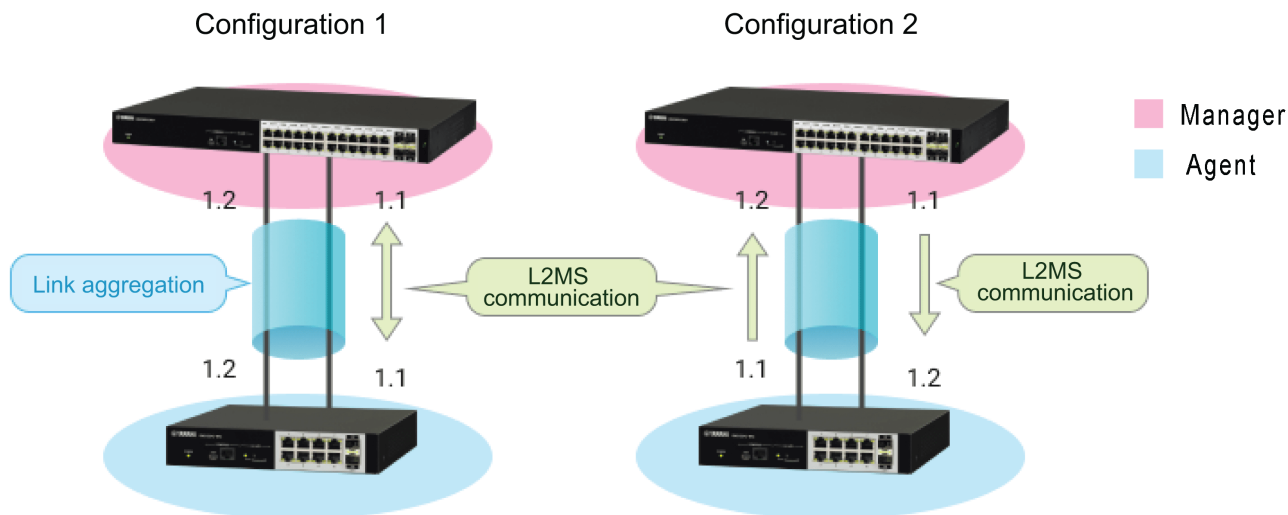
Use in conjunction with link aggregation

If link aggregation is used, L2MS communication is considered to be occurring on “the lowest-numbered linked-up LAN port associated with the logical interface”.

If link aggregation is used in conjunction with the monitoring function for connected terminals and a terminal is discovered at the end of a logical interface connection, then the terminal is considered to be connected to “the lowest-numbered linked-up LAN port associated with the logical interface” and the corresponding port number is shown.

In Configuration 1, L2MS communication is assumed to be occurring between respective ports 1.1.

In Configuration 2, L2MS communication is assumed to be occurring between manager port 1.1 and agent port 1.1.



Using switch control commands of router L2MS managers

The switch control commands of router L2MS managers are commands for the SWX2200 series. These commands do not support use on the SWX2210P series.

However, power supply control using the **switch control function execute start-poe-supply** command and the **switch control function execute stop-poe-supply** command is supported.

SYSLOG Message List

L2MS outputs the following SYSLOG messages.
Output messages appended with the "[L2MS]" prefix.

Output Level	Message	Meaning
Informational	Start L2MS (agent)	The L2MS unit is started as an agent.
	Start management by manager (<Manager_MAC_Address>)	Agent is placed under the control of the manager.
	Release from manager (<Manager_MAC_Address>)	Agent is no longer managed by the manager.
	Received config from manager (<Manager_MAC_Address>)	CONFIG is received from the manager.
	Restart for update settings.	CONFIG received from the manager is reflected and the system is restarted.
	Send config to manager (<Manager_MAC_Address>)	CONFIG is sent to the manager.

Related Documentation

- [Switch control functions of Yamaha routers](#)

LLDP

Function Overview

LLDP is a protocol for passing device management information between a device and its neighboring devices.

Definition of Terms Used

LLDP

Link Layer Discovery Protocol.
This is defined in IEEE 802.1AB.

LLDP-MED

LLDP for Media Endpoint Devices.
This is defined in ANSI/TIA-1057.

Function Details

Operating specifications

Basic specifications

This product supports the following operations.

- LLDP frames are transmitted from any LAN port to convey information about the device itself.
- LLDP frames are received at any LAN port to obtain information about neighboring devices.

LLDP sends and receives information using Type, Length, and Value (TLV) attributes.
For details on the TLV information sent by this product, refer to [TLV list](#).

The following settings are required in order to use the LLDP function.

- Enable LLDP functionality for the overall system using the **lldp run** command.
- Create LLDP agents at applicable interfaces using the **lldp-agent** command.
- Specify the LLDP frame transmit/receive mode using the **set lldp** command.

The LLDP function is **enabled** in default settings for this product.

LLDP frames are always transmitted without tags, regardless of the VLAN settings of the transmitting switch port.

They are also transmitted without tags from a trunk port without a native VLAN.

Transmitted information settings

In this product, only the type of management address to be sent in the basic management TLVs can be set using the **set management-address-tlv** command. Any other transmitted information cannot be changed.

The LLDP frames to be sent from the device itself always contain the following TLVs. For details, refer to **3.2 TLV list**.

- Required TLVs
- Basic management TLVs
- IEEE 802.1 TLV

-
- IEEE 802.3 TLV
 - LLDP-MED TLV (only when an LLDP frame containing an LLDP-MED TLV is received from a neighboring device)

Transmission timer setting

LLDP frame transmission interval is specified by the **set timer msg-tx-interval** command.

The multiplier for calculating the hold time (TTL) for device information is set by the **set msg-tx-hold** command. The TTL for LLDP transmission is the result of the following calculation. The default is **121** seconds.

- **TTL = (value set by the “set timer msg-tx-interval” command) × (value set by the “set msg-tx-hold” command) + 1 (second)**

Maximum connected devices setting

The maximum number of connected devices that can be managed by the corresponding port is set by the **set too-many-neighbors limit** command.

The default value for the maximum number of connected devices is **5 devices**.

Checking LLDP information

LLDP interface settings and received information about neighbor devices can be checked by using the **show lldp interface** command or the **show lldp neighbors** command.

To clear the LLDP frame counter, use the **clear lldp counters** command.

TLV list

The TLVs supported by this product are listed below.

- Required TLVs
- Basic management TLVs
- IEEE 802.1 TLV
- IEEE 802.3 TLV
- LLDP-MED TLV

For detailed specifications of each TLV, refer to IEEE 802.1AB (LLDP) and ANSI/TIA-1057 (LLDP-MED). The TLVs that are transmitted by this product are explained below.

Required TLVs

These are TLVs that LLDP-compliant devices always transmitted.

Three TLVs are transmitted: chassis ID, port ID, and TTL.

The required TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
Chassis ID	Chassis ID	6 bytes	MAC address of the device
Port ID	Port ID	7 to 8 bytes	Port name (port1.X)
Time To Live (TTL)	Hold time of device information (sec)	2 bytes	

Basic management TLVs

These TLVs contain system-related management information such as name, system capabilities, and address.

The basic management TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
Port Description	Port description string	7 to 8 bytes	
System Name	System name string	10 to 10 bytes	
System Description	System description string	28 bytes	SWX2210P-XXG Rev.1.03.XX
System Capabilities	Capabilities supported by the system	2 bytes	0x0004 (bridge)
	Enabled system capabilities	2 bytes	0x0004 (bridge)
Management Address	Management address IP address (4 bytes) or MAC address (6 bytes)	4 or 6 bytes	
	Interface sub-type	1 byte	0x02 (ifIndex)
	Interface number	1 to 2 bytes	ifIndex value

IEEE 802.1 TLV

These TLVs contain information such as the VLAN and link aggregation for the corresponding port.
The IEEE 802.1 TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
Port VLAN ID	Port VLAN number	2 bytes	
Port and Protocol VLAN ID	Protocol VLAN support and enable/disable	1 byte	0x00 (no support)
	Protocol VLAN number	2 bytes	0x0000
Protocol Identity	Byte string that identifies the protocol	0 to 255 bytes	
Link Aggregation	Aggregation capability and status	2 bytes	
	ifIndex number of aggregation logical interface	1 to 2 bytes	
VLAN Name	Name of the VLAN to which the port belongs	0 to 32 bytes	

IEEE 802.3 TLV

These TLVs are used for transmitting information such as the auto negotiation support information and maximum frame size information for the corresponding port.
The IEEE 802.3 TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
MAC/PHY Configuration/Status	Auto negotiation support, and whether enabled or disabled	1 byte	
	Supported communication method for auto negotiation	2 bytes	LAN port: 0x6C01 (10/100/1000M)
	Operational MAU Type Data signaling rate and duplex mode (IETF RFC 4836)	2 bytes	
Power Via MDI	MDI power support status	1 byte	
	PSE power pair Selection of wiring to be used for power supply	1 byte	0x01 (signal line)
	Power class Class0 to Class4	1 byte	
	Power type PSE Device/PD Device	2 bit	0b00 (PSE Device)
	Power source Primary/Secondary	2 bit	0b01 (Primary)
	Priority	2 bit	
	Power required from PD device (in units of 0.1 watts)	2 bytes	
	Power supply of PSE device (in units of 0.1 watts)	2 bytes	
Maximum Frame Size	Maximum frame size	2 bytes	

LLDP-MED TLV

If an LLDP frame containing an LLDP-MED TLV is received from a neighboring device, this TLV will also be contained in the LLDP frame sent from this product.
The LLDP-MED TLVs are listed below.

Type	Description	Length	Value (only fixed values are listed)
LLDP-MED Capabilities	Transmittable LLDP-MED TLVs	2 bytes	0x0009 (LLDP-MED Capabilities, Extended Power-via-MDI TLV)
	Device type	1 byte	0x04 (Network Connectivity)

Type	Description	Length	Value (only fixed values are listed)
Extended Power-via-MDI	Power type PSE Device/PD Device	2 bit	0b00 (PSE Device)
	Power source Primary/Secondary	2 bit	0b01 (Primary)
	Power priority	4 bit	
	Power required from PD (in units of 0.1 watts)	2 bytes	

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Enable LLDP function	lldp run
Create LLDP agent	lldp-agent
Set LLDP transmission/reception mode	set lldp
Set the type of management address	set management-address-tlv
Set the LLDP frame transmission interval	set timer msg-tx-interval
Set the multiplier for calculating the hold time (TTL) for device information	set msg-tx-hold
Set the maximum number of connected devices that can be managed by each port	set too-many-neighbors limit
Show interface status	show lldp interface
Show connected device information for all interfaces	show lldp neighbors
Clear LLDP frame counters	clear lldp counters

Examples of Command Execution

Set LLDP frame transmission/reception

For port1.1, enable LLDP frame transmission/reception.
Set the LLDP frame transmission interval to 60 seconds. Set the LLDP frame TTL to 181 seconds.
Specify 10 as the maximum number of connected devices managed by the port.

```

Yamaha#configure terminal
Yamaha(config)#interface port1.1
Yamaha(config-if)#lldp-agent ①
Yamaha(lldp-agent)#set timer msg-tx-interval 60 ②
Yamaha(lldp-agent)#set msg-tx-hold 3 ③
Yamaha(lldp-agent)#set too-many-neighbors limit 10 ④
Yamaha(lldp-agent)#set lldp enable txrx ⑤
Yamaha(lldp-agent)#exit

```

```
Yamaha(config-if)#exit
Yamaha(config)#lldp run ⑥
Yamaha(config)#exit
```

- ① Create LLDP agent, mode transition
- ② Set transmission interval
- ③ Set multiplier for TTL calculation: $TTL = 60 \times 3 + 1 = 181$ seconds
- ④ Maximum connected devices setting
- ⑤ Set LLDP transmission/reception mode
- ⑥ Enable LLDP function

Show LLDP interface status

Show the port1.1 LLDP interface information.

```
Yamaha#show lldp interface port1.1 ①
Agent Mode                : Nearest bridge
Enable (tx/rx)            : Y/Y
Message fast transmit time : 1
Message transmission interval : 60
Reinitialisation delay    : 2
MED Enabled               : Y
Device Type               : NETWORK_CONNECTIVITY
LLDP Agent traffic statistics
  Total frames transmitted : 1
  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
```

- ① Show interface information

Show LLDP connected device information

Show LLDP connected device information.

```
Yamaha#show lldp neighbors ①
Interface Name           : port1.1
System Name              : SWX2210P
System Description       : SWX2210P-28G Rev.1.03.13
Port Description         : port1.1
System Capabilities      : L2 Switching
Interface Numbering      : 2
Interface Number         : 5001
OID Number               :
Management IP Address    : 192.168.100.241
Mandatory TLVs
  CHASSIS ID TYPE
    Chassis MAC ADDRESS   : ac44.f284.ef22
  PORT ID TYPE
    INTERFACE NAME       : port1.1
```

```

TTL (Time To Live)           : 121
8021 ORIGIN SPECIFIC TLVs
  Port Vlan id                : 1
  PP Vlan id                  : 0
  Remote VLANs Configured
    VLAN ID                   : 1
    VLAN Name                  : default
  Remote Protocols Advertised:
    IPv4
  Remote VID Usage Digest     : 0
  Remote Management Vlan      : 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         : 0x2
    PSE power pair            : 0x1
    Power class                : 0x0
    Type/source/priority      : 0x0/0x1/0x3
    PD requested power value   : 0.0 W
    PSE allocated power value  : 0.0 W
  Link Aggregation Status     : Disabled
  Link Aggregation Port ID    : 0
  Max Frame Size              : 1522

```

① Show connected device information

Points of Caution

None

Related Documentation

None

LLDP Automatic Settings

Function Overview

The LLDP automatic setting specifies sending/receiving proprietary LLDP frames to automatically perform specific processes, such as specifying settings based on information in LLDP notifications or saving log data.

The following are automatically specified or executed by using the LLDP automatic setting.

- Dante Optimization Settings
 - When the components of the Yamaha ADECIA teleconferencing system are connected, the optimal settings for using Dante are automatically reflected.
- Power shutoff advance notification by the schedule function
 - When the PoE power shutoff is scheduled for the port to which the Yamaha wireless access point is connected, you will be notified of the power shutoff timing in advance, and the Yamaha wireless access point will save a log just before the power shutoff.

To determine Yamaha network switch and wireless access point models that support LLDP automatic setting function, refer to [LLDP automatic setting examples](#).

To determine ADECIA components, refer to [ADECIA product information](#).

Definition of Terms Used

LLDP

Link Layer Discovery Protocol.
This is defined in IEEE 802.1AB.

ADECIA

ADECIA is Yamaha's teleconferencing system. It connects processors, microphones, and speakers used for teleconferencing via a LAN (Dante).

ADECIA Component

Devices (teleconferencing processors, microphones, and speakers) included in ADECIA systems.

Function Details

Basic specifications

If the LLDP automatic setting function is enabled, proprietary LLDP frames will be sent and received.

The LLDP automatic setting as a whole can be enabled and disabled using the **lldp auto-setting** command. The default setting for this product is **enabled**.

Functions enabled with the LLDP automatic setting can be selected using the **lldp auto-setting function** command.

The default setting for this product is to **use all functions**.

In order to use this function, reception of LLDP frames must be enabled.
For this reason, check in advance that the following settings have been made.

- Enable LLDP functionality for the overall system using the **lldp run** command.
- Create LLDP agents at applicable interfaces using the **lldp-agent** command.

- Specify the LLDP frame transmit/receive mode using the **set lldp** command.

LLDP frame transmission and reception are **enabled** in product default settings.

Dante Optimization Settings

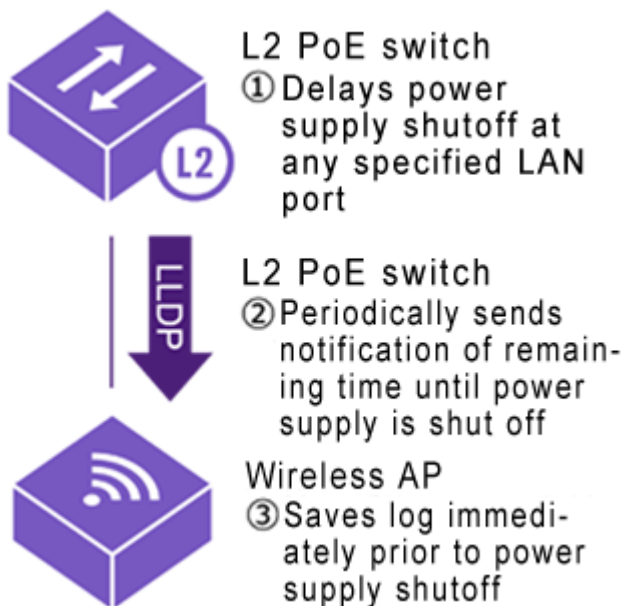
This function automatically applies settings optimized for Dante by receiving LLDP frames created independently by ADECIA components.

For more information, refer to [Dante Optimization Settings](#).

Power shutoff advance notification by the schedule function

When a PoE power shutoff is scheduled for a specific port on a Yamaha network switch, this function periodically notifies of the remaining time from 10 minutes before the power shutoff until the schedule execution via LLDP.

When a wireless access point is notified of the remaining time until the power shutoff via LLDP, it can prevent the log from being lost due to the power shutoff by saving the log just before the power supply is shut off.



If the following criteria are satisfied at a specific port whose LLDP transmission interval is set to a value greater than 30 seconds, the LLDP transmission interval will be overridden and changed to 30 seconds.

- LLDP is used and the LLDP automatic setting function is enabled.
- The PoE power shutoff is scheduled for a specific port.
- Less than 10 minutes remain until the schedule execution.

If the schedule is executed, the schedule setting is deleted, or the setting is changed to a time more than 10 minutes later, the LLDP transmission interval will return to the original setting value.

If the LLDP transmission interval is overridden and changed to 30 seconds by this function, then an asterisk is appended to the LLDP transmission interval value shown by the **show lldp interface** command.

- Example of LLDP transmission interval shown by the **show lldp interface** command

```
SWX#show lldp interface port1.2
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

```

* - Assigned by LLDP.

If the above functionality is used, note the following precautions.

- **Precautions**
 - Advance notification of a power shutoff is provided only if the power shutoff is scheduled for a specific port. Note that the notification will not be provided if the power shutoff is scheduled for the entire system.

Related Commands

Related commands are indicated below.

For details, refer to the Command Reference.

Operations	Operating commands
Enable LLDP automatic settings	lldp auto-setting
Set functions to be enabled with the LLDP automatic setting	lldp auto-setting function
Enable LLDP function	lldp run
Create LLDP agent	lldp-agent
Set LLDP transmission/reception mode	set lldp
Show interface status	show lldp interface

Setting Examples

For instructions on how to configure respective Yamaha network switch and wireless access point settings, refer to the following.

- [Technical reference: LLDP automatic setting examples](#)

Points of Caution

None.

Related Documentation

- [LLDP](#)
- [Dante Optimization Settings](#)
- [Schedule Function](#)
- [Technical reference: LLDP automatic setting examples](#)

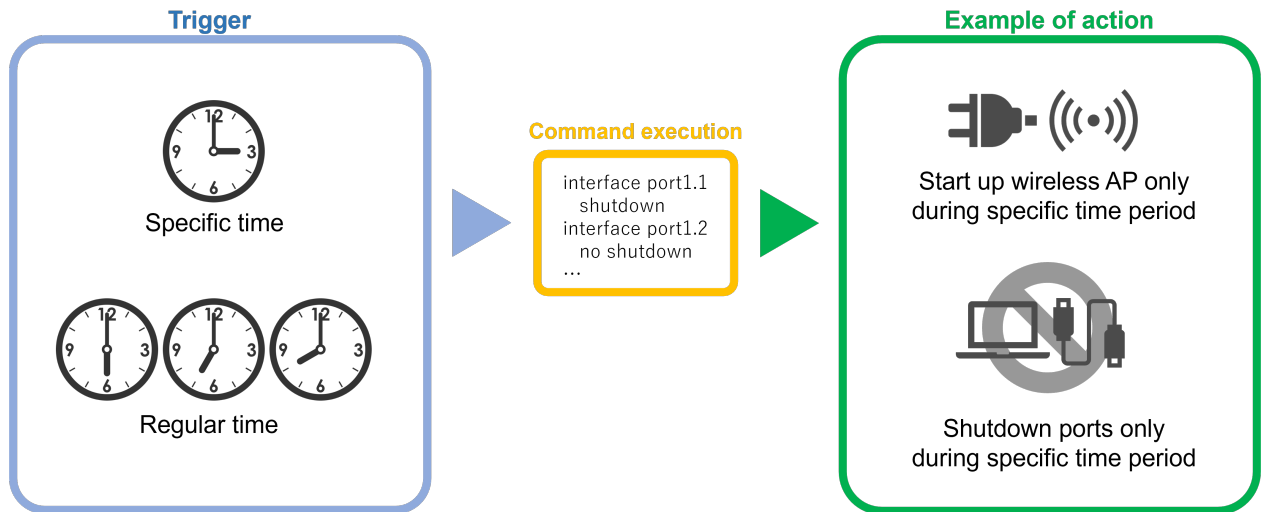
-
- [ADECIA product information](#)

Schedule Function

Function Overview

Scheduling functionality is used to execute specific processes when any particular time or event occurs. This functionality enables the following types of actions using a Yamaha network switch.

- Supplies PoE power to wireless LAN access points only during the specified period.
- Shuts down a port during the specified period.



For information on the functions that can be executed by this product, refer to [Function Details](#) and [Executable Commands](#).

Definition of Terms Used

Trigger

General term for conditions/criteria, such as that the internal clock time matches a specified time or that a specific event occurs.

Time Trigger

Condition that the internal clock time matches a specified time.

Action

Action executed when a trigger is activated.

Function Details

Scheduling functionality involves specifying “triggers” and actions, which are the two parameter settings for executing specific process “actions” when a particular specified time or event trigger occurs. This product only supports **time trigger**.

Time Trigger

Time triggers can be specified in terms of year, month, day, hour, minute, and second.

Time triggers are specified using the **schedule** command.

Available setting parameters are indicated below.

Type		Specification method	Setting value example
Date	Month 1-12	One specific month (such as only December)	12
		Multiple specific months (such as only January and February)	1,2
		Range from specific month to December (such as February to December)	2-
		Range from specific month to specific month (such as February to July)	2-7
		Range from January to specific month (such as January to July)	-7
		Every month	*
	Day 1-31	One specific day (such as day 1 only)	1
		Multiple specific days (such as days 1 and 2 only)	1,2
		Range from specific day to last day (such as day 2 to month-end)	2-
		Range from specific day to specific day (such as days 2 to 7)	2-7
		Range from day 1 to specific day (such as days 1 to 7)	-7
		Every day	*
		Specific day-of-week only (such as Monday only)	mon
		Multiple specific days of the week only (such as Saturday and Sundays only)	sat,sun
		Range from specific day-of-week to specific day-of-week (such as Monday to Friday)	mon-fri
		Range from Sunday to specific day-of-the-week (such as Sunday to Friday)	-fri

Type		Specification method	Setting value example
Hours, minutes, seconds	Hours 0-23	Specific hour only (such as 23:00 only)	23
		Multiple specific hours only (such as 01:00 and 22:00 only)	1,22
		Range from specific hour to 23:00 (such as 02:00 to 23:00)	2-
		Range from specific hour to specific hour (such as 02:00 to 21:00)	2-21
		Range from hour 00:00 to specific hour (such as 00:00 to 21:00)	-21
		Each hour	*
	Minutes 0-59	One specific minute only (such as minute 59 only)	59
		Multiple specific minutes only (such as minutes 1 and 50 only)	1,50
		Range from specific minute to minute 59 (such as minutes 2 to 59)	2-
		Range from specific minute to specific minute (such as minutes 2 to 50)	2-50
		Range from minute 0 to specific minute (such as minutes 0 to 50)	-50
		Each minute	*
	Seconds 0-59	One specific second only (such as second 59 only) This setting may be omitted.	59

Action

Processes executed when a time trigger is activated are called actions.

To specify actions, use the **schedule template** command to switch to the schedule template mode and then specify the action using the **cli-command** command.

This product supports the following actions.

Action	Command for settings	Description
Executes specified command	cli-command command	Executes the specified commands in ascending order of ID numbers.

Related Commands

Related commands are indicated below.

For command details, refer to the command reference.

Operating mode	Commands	Description
Global configuration mode	schedule	Specifies a schedule template ID that specifies the trigger and defines the action.
	schedule template	Specifies the schedule template ID and switches to the schedule template mode.

Operating mode	Commands	Description
Schedule template mode	description	Specifies description of the schedule template.
	action	Enables/disables the schedule template. Use disable to temporarily disable schedule function.
	cli-command	Defines command executed when trigger is activated.

Setting Examples

To supply PoE power to wireless LAN access points only during the specified period (only for PoE-supported models)

Supply PoE power to wireless LAN access points connected to port1.1 and port1.2 on weekdays only between 8:00 and 17:00.

```
Yamaha#
Yamaha# configure terminal
Yamaha(config)# schedule 1 time */mon-fri 8:00:00 1
Yamaha(config)# schedule template 1
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.1
Yamaha(config-schedule)# cli-command 3 power-inline enable
Yamaha(config-schedule)# cli-command 4 interface port1.2
Yamaha(config-schedule)# cli-command 5 power-inline enable
Yamaha(config-schedule)# exit
Yamaha(config)#
Yamaha(config)# schedule 2 time */mon-fri 17:00:00 2
Yamaha(config)# schedule template 2
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.1
Yamaha(config-schedule)# cli-command 3 power-inline disable
Yamaha(config-schedule)# cli-command 4 interface port1.2
Yamaha(config-schedule)# cli-command 5 power-inline disable
Yamaha(config-schedule)# end
Yamaha#
```

To shut down a port during the specified period

Shut down port1.3 and port1.4 from 17:00 on Friday to 8:00 on the following Monday.

```
Yamaha#
Yamaha# configure terminal
Yamaha(config)# schedule 1 time */fri 17:00:00 1
Yamaha(config)# schedule template 1
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.3
Yamaha(config-schedule)# cli-command 3 shutdown
Yamaha(config-schedule)# cli-command 4 interface port1.4
Yamaha(config-schedule)# cli-command 5 shutdown
Yamaha(config-schedule)# exit
Yamaha(config)#
Yamaha(config)# schedule 2 time */mon 8:00:00 2
Yamaha(config)# schedule template 2
```



```
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.3
Yamaha(config-schedule)# cli-command 3 no shutdown
Yamaha(config-schedule)# cli-command 4 interface port1.4
Yamaha(config-schedule)# cli-command 5 no shutdown
Yamaha(config-schedule)# end
Yamaha#
```

Executable Commands

Only the following commands can be executed for the schedule function.

- configure terminal
- interface
- shutdown
- no shutdown
- power-inline disable (PoE-supported models only)
- power-inline enable (PoE-supported models only)
- write
- end
- exit (This command cannot be executed in the privileged EXEC mode)

SYSLOG

The schedule function outputs the following SYSLOG messages.

Level	Output	Description
Info	[SCHEDULE]:inf: ID:X command is done	The schedule template ID:X command was executed when the trigger was activated.
Error	[SCHEDULE]:err: Execution failed at schedule template ID: X, cli-command ID: Y.	Execution of cli-command ID: Y failed in the schedule template ID: X.

Points of Caution

- When actions are executed, the cli-command executes actions in ascending ID number order.
- When actions are executed, even if a command specified by the cli-command results in an execution error, the remaining commands are executed.
- If multiple triggers are activated simultaneously, then actions are executed in ascending order of schedule template ID number.
- If the trigger activation time elapses due to the time setting being set manually by the clock set command or being changed by NTP, then any existing triggers scheduled to be activated within 59 seconds of when the current time setting was changed will be activated.
- If the trigger activation time was changed backward manually by the clock set command or by NTP, then the time triggers are checked again starting from the time to which it was set back.
- This function can be used to periodically save the configuration, but periodic rewriting will consume ROM capacity more quickly. ROM failures due to frequent rewriting are not warranted for free repairs, even if they occur during the warranty period.

Related Documentation

- None

Dante Optimization Settings

Function Overview

The Dante setting optimization function makes it easy to build the optimal environment for Dante digital audio networks.

The function allows users to easily configure all Dante settings at the same time without having to think about individual Dante settings (such as QoS, IGMP snooping, disable flow control, and disable EEE settings).

Definition of Terms Used

Dante

Dante is a digital audio network specification developed by the Audinate Corporation.

ADECIA

ADECIA is Yamaha's teleconferencing system. It connects processors, microphones, and speakers used for teleconferencing via a LAN (Dante).

ADECIA Components

Devices (teleconferencing processors, microphones, and speakers) included in ADECIA systems.

LLDP

Protocol for passing device information to neighboring devices.

Function Details

Dante settings can be optimized by the following two methods.

- Automatic optimization settings using LLDP
 - Automatically applies optimized settings by receiving LLDP frames independently from ADECIA components.
- Manual optimization settings via the Web GUI
 - Apply a Dante profile from the ProAV settings page in the web GUI of this product.

The settings that can be collectively specified at the same time using the Dante setting optimization function are listed below. For automatic setting optimization using LLDP, the applicable settings will differ depending on the ADECIA component firmware version.

Object of setting	Function	Commands	Applicability		
			LLDP (ADECIA V2.5 or earlier)	LLDP (ADECIA V2.8 or later)	Web GUI
Entire system	Disable flow control	flowcontrol disable			Yes
	Enable QoS	qos enable	Yes	Yes	Yes
	Optimize transmission queue by DSCP value	qos dscp-queue 8 2	Yes	Yes	Yes
		qos dscp-queue 26 3		Yes	Yes
		qos dscp-queue 34 4		Yes	Yes
		qos dscp-queue 46 5	Yes	Yes	Yes
		qos dscp-queue 48 5		Yes	Yes
		qos dscp-queue 56 7	Yes	Yes	Yes
		qos dscp-queue [not indicated above] 0	Yes	Yes	Yes
	Set scheduling method	qos scheduling sp	Yes	Yes	Yes
	Always forward linked local multicasts	l2-unknown-mcast forward link-local		Yes	Yes
	Sets MRU	mru 1522			Yes
	Enable LLDP	lldp run		Yes	Yes
VLAN interface	Set profile type	proav profile-type dante-primary/dante-secondary			Yes
	Flood unknown multicasts	l2-unknown-mcast flood		Yes	Yes
	Enable IGMP snooping	ip igmp snooping enable	Yes	Yes	Yes
	Set IGMP snooping version	ip igmp snooping version 3	Yes	Yes	Yes
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment		Yes	Yes

Object of setting	Function	Commands	Applicability		
			LLDP (ADECIA V2.5 or earlier)	LLDP (ADECIA V2.8 or later)	Web GUI
VLAN interface	Enable IGMP query transmission function	ip igmp snooping querier	Yes	Yes	Yes
	Set IGMP query transmission interval	ip igmp snooping query-interval 30	Yes	Yes	Yes
	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable	Yes	Yes	Yes
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable		Yes	Yes
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable		Yes	Yes
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable		Yes	Yes
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable		Yes	Yes
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable		Yes	Yes
	Set always forwarding PTP packets	I2-mcast flood 224.0.1.129		Yes	Yes
		I2-mcast flood 224.0.1.130		Yes	Yes
		I2-mcast flood 224.0.1.131		Yes	Yes
		I2-mcast flood 224.0.1.132		Yes	Yes
		I2-mcast flood 239.254.3.3		Yes	Yes

LAN/SFP port	Set QoS trust mode to DSCP	qos trust dscp	Yes	Yes	Yes
	Disable flow control	flowcontrol disable	Yes	Yes	Yes
	DisableEEE	eee disable	Yes	Yes	Yes
	Enable LLDP transmission and reception	lldp-agent / set lldp enable tx rx		Yes	Yes

Use the Dante optimization setting function after you have made all of the basic switch settings (such as VLAN and IP).

If you make new changes to the settings, the Dante optimization settings will not follow.

Automatic optimization settings using LLDP

Settings optimized for Dante can be applied automatically by receiving LLDP frames created independently by ADECIA components.

Automatic optimization settings via LLDP are set by the **lldp auto-setting** command.

By default, this product is set to **enable** automatic optimization settings via LLDP.

If this function is enabled and an LLDP frame is received from an ADECIA component, then the settings are automatically applied to the running-config settings for the overall system, for the VLAN interface that received the frame, and for the LAN/SFP port where the LLDP frame was received.

In ADECIA V2.8 or the later version, the function is disabled if even one of the automatically specified settings differs from factory settings.

If you save using the **copy running-config startup-config** command or the **write** command, the settings are also applied to the startup-config that is used for the next and subsequent startups.

Even if the port to which the device is connected experiences a link-down state after automatic optimization settings, the automatically added settings are maintained.

This function can be used only for a physical interface (LAN/SFP port). It cannot be used with a link aggregated logical interface.

In addition, LAN/SFP port modes can only be used at access ports. They cannot be used at trunk ports.

In order to use this function, reception of LLDP frames must be enabled.

For this reason, check in advance that the following settings have been made.

- Enable LLDP functionality for the overall system using the **lldp run** command.
- Create LLDP agents at applicable interfaces using the **lldp-agent** command.
- Specify the LLDP frame transmit/receive mode using the **set lldp** command.

LLDP frame transmission and reception are **enabled** in product default settings.

Manual optimization settings via the Web GUI

Apply a Dante profile from the **[ProAV settings] - [ProAV profile]** pages in the web GUI of this product.

For details, refer to [ProAV Settings](#).

Related Commands

Related commands are indicated below.

For details on the commands, refer to the Command Reference.

Operations	Operating commands
Set Dante automatic optimization settings function using LLDP	lldp auto-setting
Enable LLDP function	lldp run
Create LLDP agent	lldp-agent
Set LLDP transmission/reception mode	set lldp
Set flow control (system)	flowcontrol
Set flow control (interface)	flowcontrol
Enable QoS	qos
Set DSCP - transmission queue ID conversion table	qos dscp-queue
Set QoS trust mode	qos trust
Set scheduling method	qos scheduling
Set EEE	eee
Set MRU	mru
Set forwarding linked local multicasts	l2-unknown-mcast forward link-local
Set forwarding unknown multicasts	l2-unknown-mcast
Set forwarding multicast frames	l2-mcast flood
Enable/disable IGMP snooping	ip igmp snooping
Set IGMP snooping version	ip igmp snooping version
Set IGMP snooping fast-leave	ip igmp snooping fast-leave
Set IGMP query transmission function	ip igmp snooping querier
Set IGMP query transmission interval	ip igmp snooping query-interval
Set IGMP packet TTL value checking function	ip igmp snooping check ttl
Set IGMP packet RA checking function	ip igmp snooping check ra
Set IGMP packet ToS checking function	ip igmp snooping check tos
Set IGMP report suppression function	ip igmp snooping report-suppression
Set IGMP report forwarding function	ip igmp snooping report-forward enable
Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable
Set profile type	proav profile-type

Examples of Command Execution

Automatic optimization settings using LLDP

Enable automatic optimization settings using LLDP.

Enable LLDP transmission and reception on port1.1.

```
Yamaha#configure terminal
Yamaha(config)#interface port1.1
Yamaha(config-if)#lldp-agent ①
Yamaha(lldp-agent)#set lldp enable txrx ②
Yamaha(lldp-agent)#exit
Yamaha(config-if)#exit
Yamaha(config)#lldp run ③
Yamaha(config)#lldp auto-setting enable ④
```

- ① Create LLDP agent, mode transition
- ② Set LLDP transmission/reception mode
- ③ Enable LLDP function
- ④ Enable automatic optimization settings using LLDP

Points of Caution

- It is assumed that you will use the Dante optimization setting function after you have made all of the basic switch settings (such as VLAN and IP).
If you make new changes to the settings (such as adding a VLAN), the Dante optimization settings will not follow.
- Manual optimization settings via the Web GUI
 - Note that if you use this function when settings such as QoS settings, flow control settings, EEE settings, and IGMP snooping have already been made, those settings are overwritten by Dante-optimized settings.
- Using LLDP to specify settings automatically
 - This function can be used only for a physical interface (LAN/SFP port). It cannot be used with a link aggregated logical interface.
 - LAN/SFP port modes can only be used at access ports. They cannot be used at trunk ports.
 - In ADECIA V2.8 or the later version, the function is disabled if even one of the automatically specified settings differs from factory settings.

Related Documentation

- [ProAV Settings](#)
- [LLDP](#)
- [QoS](#)
- [Flow Control](#)
- [IGMP Snooping](#)
- [Basic Interface Functions](#)
- [ADECIA Product Information](#)

ProAV Settings

Function Overview

From the web GUI “ProAV Settings” page, you can perform simple GUI operations to collectively configure optimal settings for AVoIP networks on which to transmit audio and video traffic such as Dante and NDI. The following ProAV profiles can be set on this product.

- Dante
- NDI

This technical reference explains the details on the commands that are set when a ProAV profile is applied, as well as kitting (initial setup) and troubleshooting.

For details on how to use the web GUI “ProAV Settings” page, refer to the GUI technical reference.

Definition of Terms Used

Dante

Dante is a professional audio networking solution developed by Audinate, Inc.

A single LAN cable can be used to carry out bidirectional communication of all the information required for a digital audio system, such as multi-channel audio transmission, clock synchronization signals, and control signals.

NDI

NDI is a new protocol developed by Newtek, Inc. to support live video production workflows over IP.

In a typical Gigabit Ethernet environment, this protocol enables real-time mutual transmission of information such as video, audio, and metadata.

Yamaha LAN Monitor

Yamaha LAN Monitor is a computer application that allows you to monitor and control Yamaha switch information and connected devices on your computer.

Details on ProAV Profiles

Dante profiles

The following commands are collectively applied by Dante profiles.

- List of commands applied by Dante profiles

Object of setting	Function	Commands
Entire system	Disable flow control	flowcontrol disable
	Enable QoS	qos enable
	Optimize transmission queue by DSCP value	qos dscp-queue 8 2
		qos dscp-queue 26 3
		qos dscp-queue 34 4
		qos dscp-queue 46 5
		qos dscp-queue 48 5
		qos dscp-queue 56 7
		qos dscp-queue [not indicated above] 0
	Set scheduling method	qos scheduling sp
	Always forward linked local multicasts	l2-unknown-mcast forward link-local
	Sets MRU	mru 1522
	Enable LLDP	lldp run

Object of setting	Function	Commands
VLAN interface	Set profile type	proav profile-type dante-primary/dante-secondary
	Flood unknown multicasts	I2-unknown-mcast flood
	Enable IGMP snooping	ip igmp snooping enable
	Set IGMP snooping version	ip igmp snooping version 3
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment
	Enable IGMP query transmission function	ip igmp snooping querier
	Set IGMP query transmission interval	ip igmp snooping query-interval 30
	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable
	Always forward PTP packets	I2-mcast flood 224.0.1.129
		I2-mcast flood 224.0.1.130
		I2-mcast flood 224.0.1.131
		I2-mcast flood 224.0.1.132
		I2-mcast flood 239.254.3.3
LAN/SFP port	Set QoS trust mode to DSCP	qos trust dscp
	Disable flow control	flowcontrol disable
	Disable EEE	eee disable
	Enable LLDP transmission and reception	lldp-agent set lldp enable tx rx
	Set L2MS filter	I2ms filter disable / enable (*1)

Details on the settings are as follows:

- **Disable flow control**

- **Disabling flow control** ensures that transmission and reception of Dante traffic continue even when the bandwidth is congested.

- **Enable QoS**

- By **enabling QoS**, the priority is given to Dante traffic forwarding.
- By **optimizing transmission queues by DSCP value**, DSCP values related to Dante traffic are

assigned to high-priority transmission queues.

- By **setting the QoS trust mode to DSCP**, the priority control is performed by referring to the DSCP values.
- By **setting the scheduling method to SP (absolute priority)**, priority is given to transmission from the high priority transmission queue.

- **Enable IGMP snooping**

- By **enabling IGMP snooping**, multicast traffic is forwarded only to ports where multicast receivers exist, and unnecessary traffic is not forwarded.
- **Set the IGMP snooping version to IGMPv3.**
In a network configuration using multiple switches, if the switches have different versions, a warning message will be displayed on the “Multicast page” of the ProAV GUI.
When using a Dante network, set the version to IGMPv3.
- By **enabling the IGMP snooping fast leave function**, multicast traffic forwarding stops immediately when a multicast receiver stops receiving it.
When a multicast receiver switches between audio and video, the multicast traffic before the switching can be prevented from causing noise.
- By **enabling the auto-assignment option of the fast leave function**, fast leave is not performed on ports connecting switches in a network configuration using multiple switches.
This prevents immediate stop of multicast traffic forwarding when receivers who want to receive the multicast traffic still exist on the opposing switch.
- **Enable the IGMP query transmission function (querier function).**
When IGMP snooping is used, a querier must exist on the same network.
If there are multiple queriers on the same network, the querier with the smallest IP address becomes the representative querier, and the other queriers automatically stop transmitting queries.
- By **setting the IGMP query transmission interval to 30 seconds**, the IGMP snooping learning state can converge more quickly.
- By **disabling the IGMP packet TTL value/RA/ToS checking function**, even if an invalid IGMP packet is received, the information is appropriately corrected and the IGMP packet is forwarded.
- By **enabling the data transfer suppression function for multicast router ports**, you can conserve the bandwidth between switches in a network configuration using multiple switches.
Normally, all multicast traffic is forwarded to the multicast router port regardless of existence of a multicast receiver. Therefore, in a bidirectional transmission environment, unnecessary multicast traffic consumes the bandwidth between switches.
By using this function, multicast traffic is forwarded only if a multicast receiver exists on the opposing switch, thereby conserving the bandwidth between switches.
- By **disabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.
- By **enabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.

- **Always forward control-use multicast packets**

- By **always forwarding linked local multicasts**, control packets such as mDNS used by Dante are always forwarded when IGMP snooping is enabled.
- By **always forwarding PTP packets**, control packets for time synchronization used by Dante are always forwarded when IGMP snooping is enabled.
- By **flooding unknown multicasts**, multicast traffic without a receiver is forwarded when IGMP snooping is enabled.

- **Disable jumbo frames**

- By **setting the MRU to 1522 bytes**, jumbo frame forwarding is disabled.

- **Disable EEE**

- **Disabling the power saving function** prevents the function from affecting data transfer performance.

- **Enable LLDP**

- **Enabling LLDP transmission and reception** enables the **IGMP snooping fast leave function** and the **IGMP report forwarding function**.

This is because these two IGMP functions operate by using LLDP to determine whether the opposing device is a switch.

- **Set L2MS filter (*1)**

- Only if the Dante network is configured as a **redundant Dante primary/secondary** configuration, the **L2MS filter is enabled** on the Dante secondary port.

L2MS refers to a Yamaha-original control packet used to monitor and control Yamaha switches with integrated management applications such as Yamaha LAN Monitor.

In the redundant configuration, the switches are connected with two cables, a primary cable and a secondary cable. Therefore, enabling the L2MS filter prevents control packets from looping and causing congestion.

In addition, in network configurations other than the redundant configuration, the **L2MS filter is disabled**.

- **Set profile type**

- This setting is used as an identifier to identify the profile type in the ProAV GUI.

NDI profiles

The following commands are collectively applied by NDI profiles.

- List of commands applied by NDI profiles

Object of setting	Function	Commands
Entire system	Enable flow control	flowcontrol enable
	Disable QoS	qos disable
	Always forward linked local multicasts	l2-unknown-mcast forward link-local
	Sets MRU	mru 1522
	Enable LLDP	lldp run

Object of setting	Function	Commands
VLAN interface	Set profile type	proav profile-type ndi
	Flood unknown multicasts	l2-unknown-mcast flood
	Enable IGMP snooping	ip igmp snooping enable
	Set IGMP snooping version	ip igmp snooping version 2
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment
	Enable IGMP query transmission function	ip igmp snooping querier
	Set IGMP query transmission interval	ip igmp snooping query-interval 125
	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable
LAN/SFP port	Enable flow control	flowcontrol enable
	DisableEEE	eee disable
	Enable LLDP transmission and reception	lldp-agent set lldp enable tx rx

Details on the settings are as follows:

- **Enable flow control**

- By **enabling flow control**, when the bandwidth becomes congested, traffic transmission is temporarily stopped until the congestion clears, preventing packet loss.

- **Disable QoS**

- By **disabling QoS**, packets will be forwarded without priority control.

- **Enable IGMP snooping**

- By **enabling IGMP snooping**, multicast traffic is forwarded only to ports where multicast receivers exist, and unnecessary traffic is not forwarded.
- **Set the IGMP snooping version to IGMPv2.**
In a network configuration using multiple switches, if the switches have different versions, a warning message will be displayed on the “Multicast page” of the ProAV GUI.
When using an NDI network, set the version to IGMPv2.
- By **enabling the IGMP snooping fast leave function**, multicast traffic forwarding stops immediately when a multicast receiver stops receiving it.
When a multicast receiver switches between audio and video, the multicast traffic before the switching can be prevented from causing noise.

-
- By **enabling the auto-assignment option of the fast leave function**, fast leave is not performed on ports connecting switches in a network configuration using multiple switches.
This prevents immediate stop of multicast traffic forwarding when receivers who want to receive the multicast traffic still exist on the opposing switch.
 - **Enable the IGMP query transmission function (querier function).**
When IGMP snooping is used, a querier must exist on the same network.
If there are multiple queriers on the same network, the querier with the smallest IP address becomes the representative querier, and the other queriers automatically stop transmitting queries.
 - **Set the IGMP query interval value to the default of 125 seconds.**
 - By **disabling the IGMP packet TTL value/RA/ToS checking function**, even if an invalid IGMP packet is received, the information is appropriately corrected and the IGMP packet is forwarded.
 - By **enabling the data transfer suppression function for multicast router ports**, you can conserve the bandwidth between switches in a network configuration using multiple switches.
Normally, all multicast traffic is forwarded to the multicast router port regardless of existence of a multicast receiver. Therefore, in a bidirectional transmission environment, unnecessary multicast traffic consumes the bandwidth between switches.
By using this function, multicast traffic is forwarded only if a multicast receiver exists on the opposing switch, thereby conserving the bandwidth between switches.
 - By **disabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.
 - By **enabling the IGMP report suppression function**, IGMP reports are forwarded directly without being proxied in a network configuration using multiple switches.
 - **Always forward control-use multicast packets**
 - By **always forwarding linked local multicasts**, control packets such as mDNS used by NDI are always forwarded when IGMP snooping is enabled.
 - By **flooding unknown multicasts**, multicast traffic without a receiver is forwarded when IGMP snooping is enabled.
 - **Disable jumbo frames**
 - By **setting the MRU to 1522 bytes**, jumbo frame forwarding is disabled.
 - **Disable EEE**
 - **Disabling the power saving function** prevents the function from affecting data transfer performance.
 - **Enable LLDP**
 - **Enabling LLDP transmission and reception** enables the **IGMP snooping fast leave function** and the **IGMP report forwarding function**.
This is because these two IGMP functions operate by using LLDP to determine whether the opposing device is a switch.
 - **Set profile type**
 - This setting is used as an identifier to identify the profile type in the ProAV GUI.

Settings for using multiple profiles

On the “Custom” page of the ProAV profile, you can set any profile for each port.
Depending on the profile combination, conflicts in settings may occur, resulting in differences in settings compared to the case where a single profile is used.

When using both Dante and NDI

- List of commands applied when both Dante and NDI are used

Object of setting	Function	Dante profiles	NDI profiles
Entire system	Enable flow control	flowcontrol enable	
	Enable QoS	qos enable	
	Optimize transmission queue by DSCP value	qos dscp-queue 8 2	
		qos dscp-queue 26 3	
		qos dscp-queue 34 4	
		qos dscp-queue 46 5	
		qos dscp-queue 48 5	
		qos dscp-queue 56 7	
		qos dscp-queue [not indicated above] 0	
	Set scheduling method	qos scheduling sp	
	Always forward linked local multicasts	l2-unknown-mcast forward link-local	
	Sets MRU	mru 1522	
	Enable LLDP	lldp run	

Object of setting	Function	Dante profiles	NDI profiles
VLAN interface	Set profile type	proav profile-type dante-primary/dante-secondary	proav profile-type ndi
	Flood unknown multicasts	l2-unknown-mcast flood	l2-unknown-mcast flood
	Enable IGMP snooping	ip igmp snooping enable	ip igmp snooping enable
	Set IGMP snooping version	ip igmp snooping version 3	ip igmp snooping version 2
	Enable IGMP snooping fast-leave function	ip igmp snooping fast-leave auto-assignment	ip igmp snooping fast-leave auto-assignment
	Enable IGMP query transmission function	ip igmp snooping querier	ip igmp snooping querier
	Set IGMP query transmission interval	ip igmp snooping query-interval 30	ip igmp snooping query-interval 125
	Disable IGMP packet TTL value checking function	ip igmp snooping check ttl disable	ip igmp snooping check ttl disable
	Disable IGMP packet RA checking function	ip igmp snooping check ra disable	ip igmp snooping check ra disable
	Disable IGMP packet ToS checking function	ip igmp snooping check tos disable	ip igmp snooping check tos disable
	Enable data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression enable	ip igmp snooping mrouter-port data-suppression enable
	Disable IGMP report-suppression function	ip igmp snooping report-suppression disable	ip igmp snooping report-suppression disable
	Enable IGMP report forwarding function	ip igmp snooping report-forward enable	ip igmp snooping report-forward enable
	Always forward PTP packets	l2-mcast flood 224.0.1.129	-
		l2-mcast flood 224.0.1.130	
		l2-mcast flood 224.0.1.131	
		l2-mcast flood 224.0.1.132	
		l2-mcast flood 239.254.3.3	
LAN/SFP port	Set QoS trust mode	qos trust dscp	qos trust port-priority qos port-priority-queue 2
	Set flow control	flowcontrol disable	flowcontrol enable
	DisableEEE	eee disable	eee disable
	Enable LLDP transmission and reception	lldp-agent set lldp enable tx rx	lldp-agent set lldp enable tx rx
	Set L2MS filter	l2ms filter disable	l2ms filter disable

Differences between using multiple profiles and using a single profile are as follows:

- **Flow control**

- **Flow control is enabled** for the entire system.
- **Flow control is disabled** on ports with a Dante profile applied.
- **Flow control is enabled** on ports with an NDI profile applied.

- **QoS**

- **QoS is enabled** for the entire system.
- **The transmission queues are optimized based on the DSCP values** across the entire system.
- For ports with a Dante profile applied, by **setting the QoS trust mode to DSCP**, the priority control is performed by referring to the DSCP values.
- For ports with an NDI profile applied, by **setting the QoS trust mode to port priority and fixing the transmission queue to 2 (default)**, the packet forwarding priority control is not performed.

Kitting and Troubleshooting

By utilizing the “Yamaha LAN Monitor”, an integrated management tool for Yamaha network devices, you can easily perform kitting (initial setup) and troubleshooting.

Yamaha LAN Monitor can be downloaded for free. For details on how to install and use Yamaha LAN Monitor, refer to the user guide.

[Kitting] Initial setup without having to think about IP addresses

Normally, when using two or more switches in a network, you must appropriately set the IP address of each switch to avoid IP address duplication.

However, if you have a closed AVoIP network that does not need to be connected to an external network, you can use the **Auto IP function** of the switches to automatically assign link local addresses.

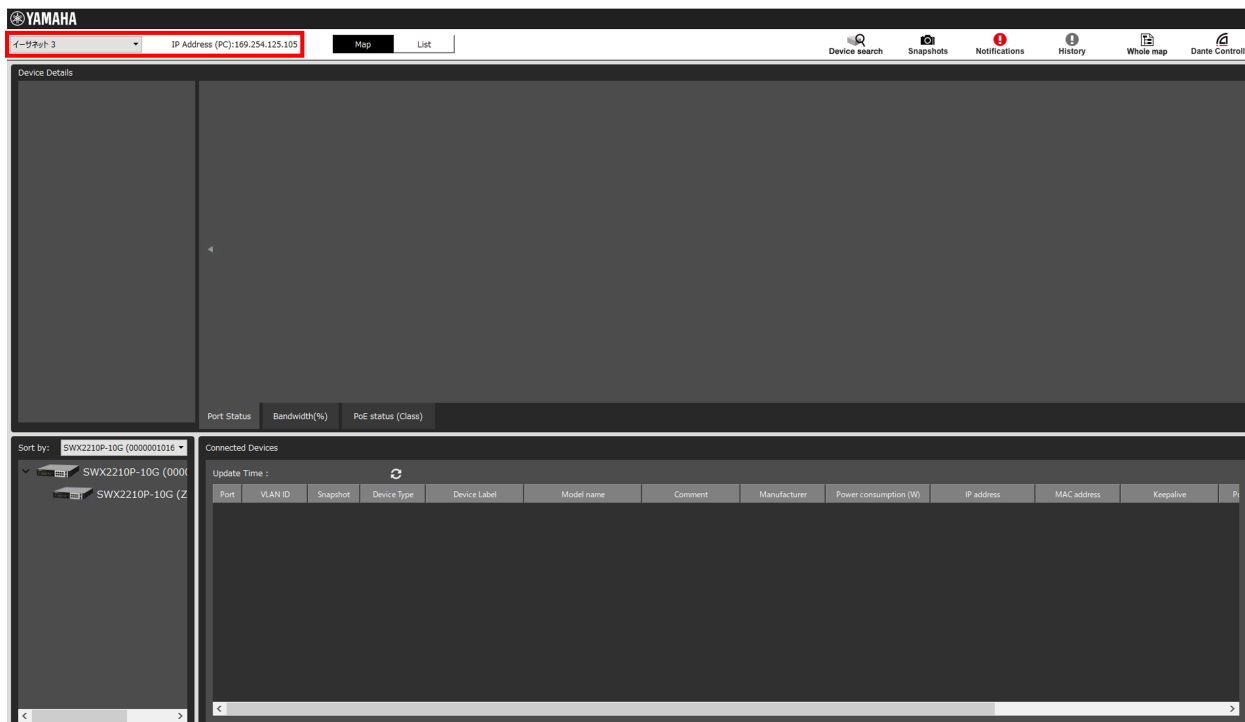
By combining a Yamaha switch in the factory default settings with Yamaha LAN Monitor, you can easily apply the ProAV profile without having to think about setting IP addresses.

1. As a preliminary step, install Yamaha LAN Monitor on your computer and set the IP address of the network adapter used by the computer to “Acquire automatically”.

This procedure allows the computer to operate with a link local address.

(*If a DHCP server exists, the IP address can be acquired via DHCP. However, since a closed AVoIP network is assumed this time, the explanation of DHCP is omitted.)

2. Connect multiple switches in the factory default settings, connect the computer to a port on any switch, and start Yamaha LAN Monitor. When you start it, the following screen will appear.
Make sure that the correct network adapter of the computer is selected in the upper left corner of the screen and that the IP address of the computer is a link local address starting with “169.254.”

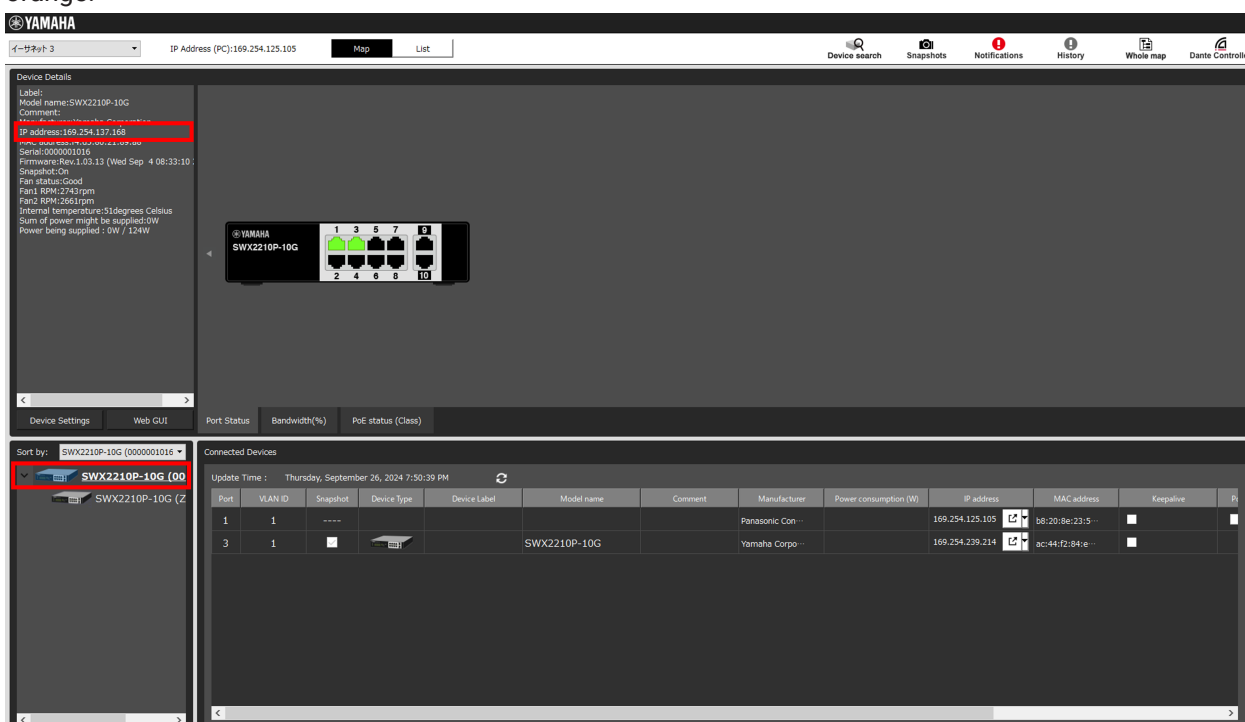


- You can check the IP address by clicking the switch icon on Yamaha LAN Monitor. The default IP address of the Yamaha switch is "192.168.100.240/24". **When the switch is placed under the management of Yamaha LAN Monitor in its factory default settings (state without any changes to its settings), the address will automatically switch to a link local address.**

If the IP address of the switch starts with "169.254.", the switch is operating with a link local address. If the address remains as "192.168.100.240", wait a while until it switches to a link local address, and then refresh the display.

Note that, if the Yamaha switch settings have already been changed from the default settings, the switch will not automatically switch to a link local address. If the address does not switch to the link local address after a while, reset the switch to its default settings.

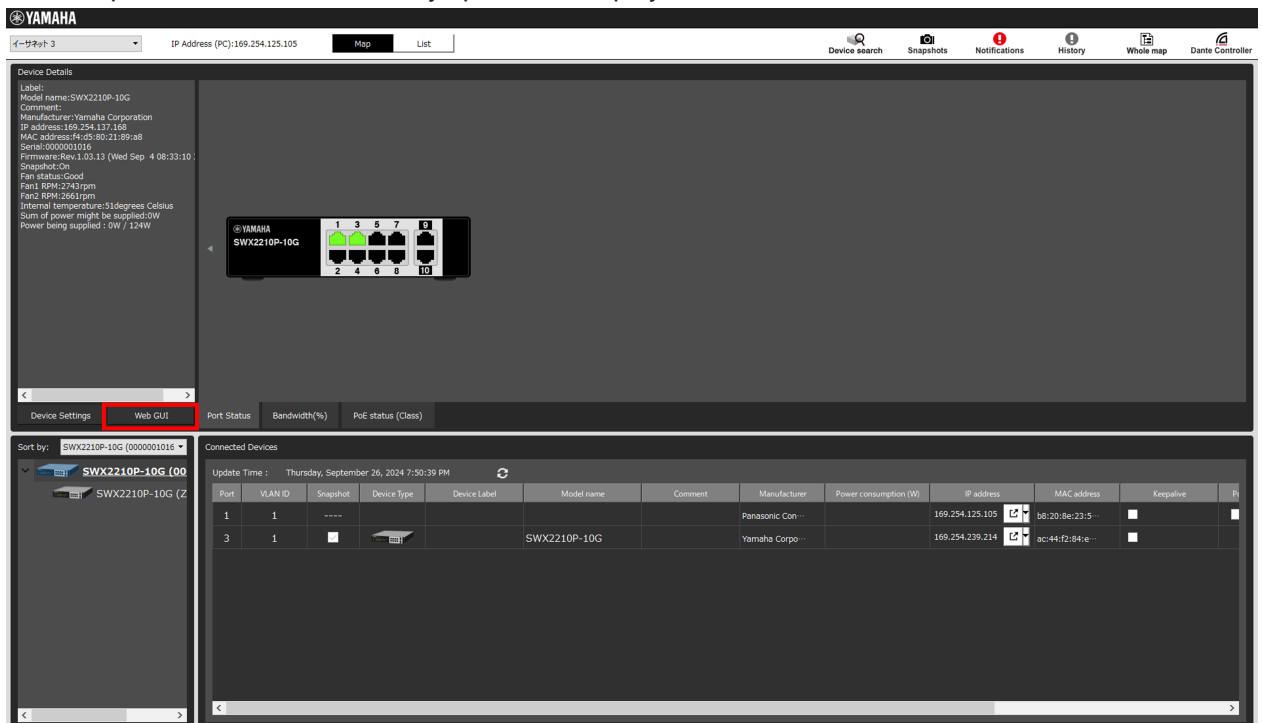
With this product, you can physically initialize the settings by turning on the power while holding down the LED MODE button on the front of the chassis, and then releasing the button when all port LEDs turn orange.



- Once you have confirmed that the IP address of the switch has changed to a link local address, click the

“Web GUI” button.

The computer browser automatically opens and displays the web GUI of the switch.



- On the web GUI login screen, enter the username “admin” and password “admin”. After selecting the language, you will be asked to change your password. Set a password of your choice.

SWX2210P-10G

SWX2210P

ユーザー名を入力してください
Please enter your username.

admin

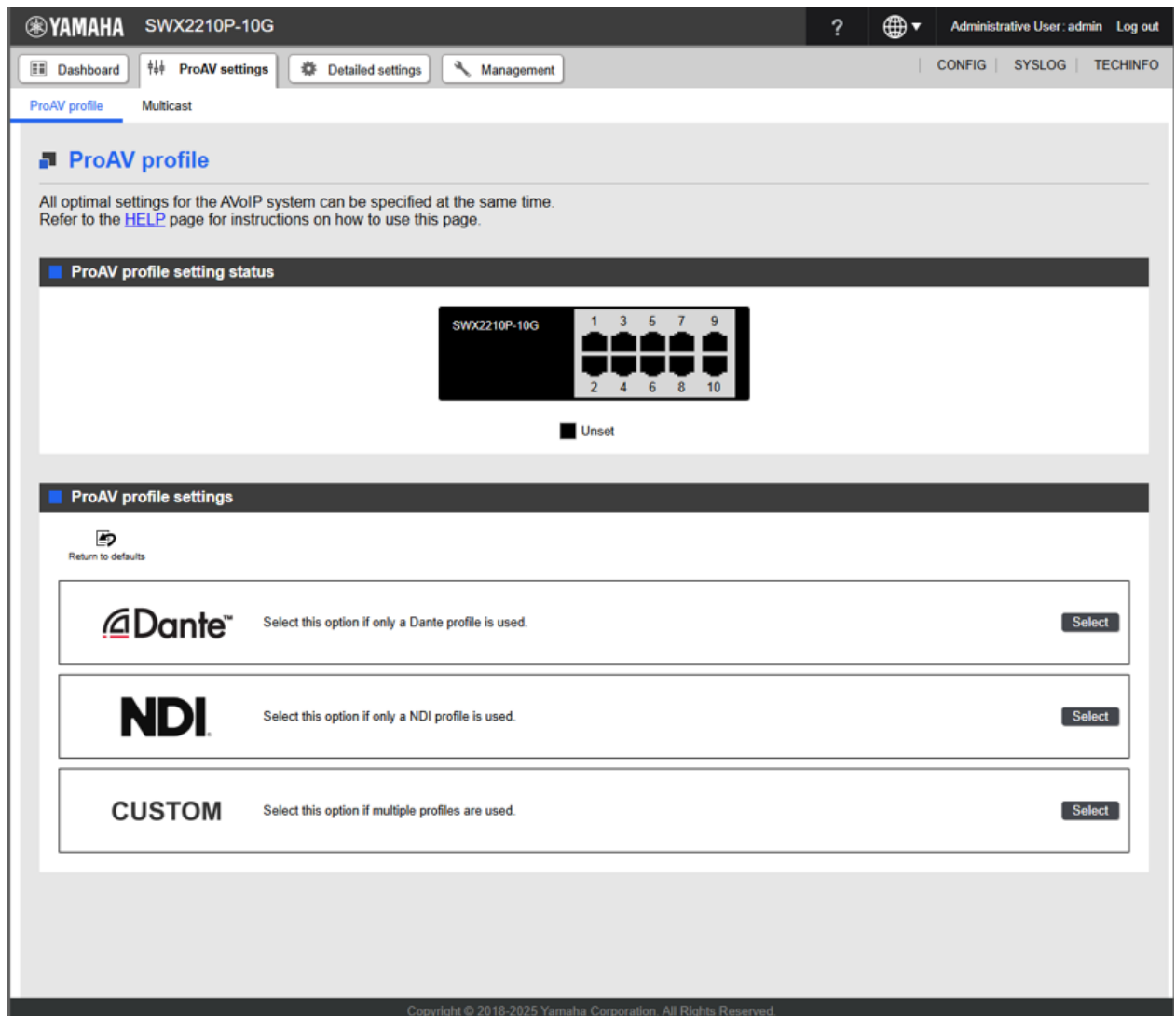
パスワードを入力してください
Please enter your password.

.....

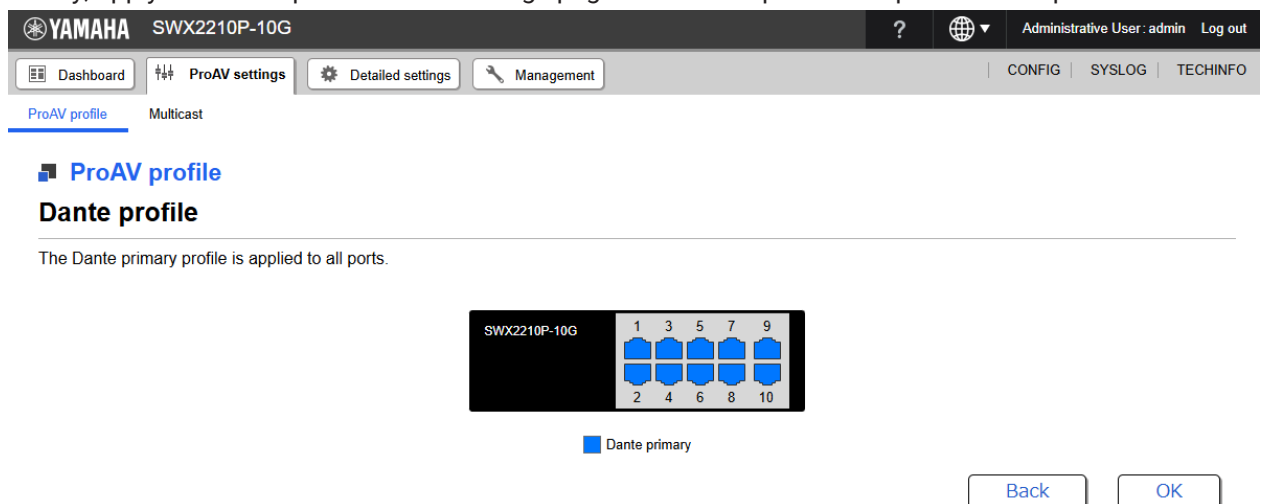
Login

Yamaha Corporation

- Once you have logged in to the web GUI, click the “ProAV Settings” button in the global menu at the top of the screen.
The “ProAV Profile” page will appear as shown below.



- Finally, apply the ProAV profile on the settings page. The ProAV profile setup is now completed.

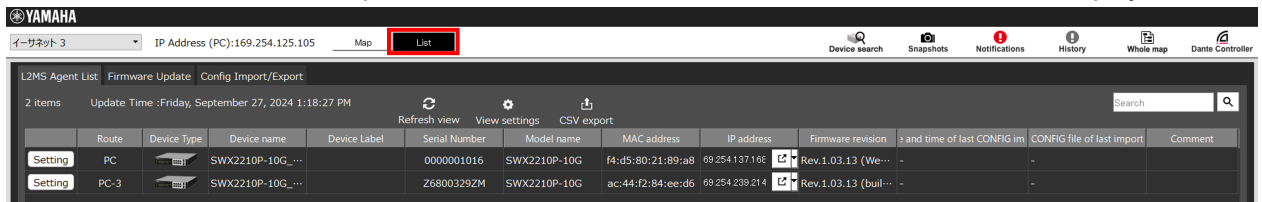


[Kitting] Applying the same settings to multiple Yamaha switches at once

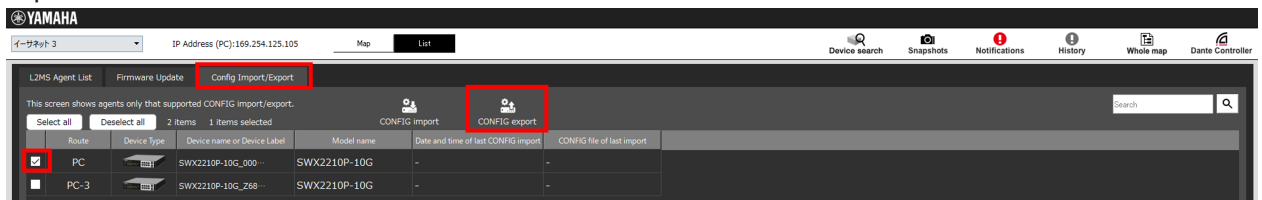
Yamaha LAN Monitor can distribute configuration files (CONFIG files) to multiple Yamaha switches at once. If you are using link local addresses as the IP addresses and want to apply the same settings to all switches, you can efficiently configure the settings for multiple switches.

Note that, if the switch is operated with a fixed IP address, you will need to reconfigure the IP address setting to prevent IP address duplication.

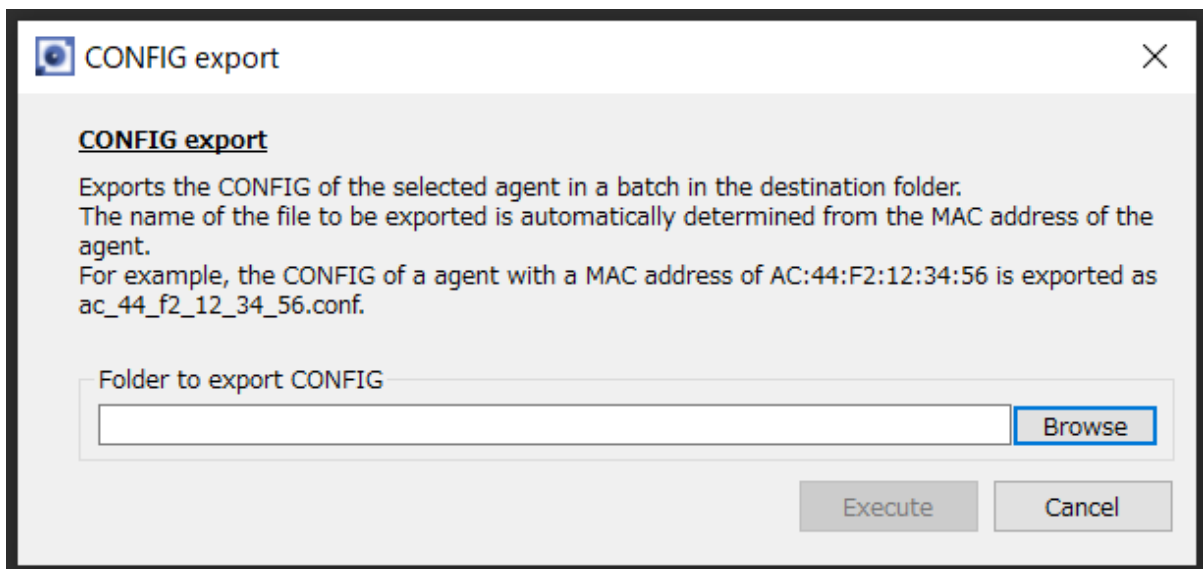
1. Follow the steps in 4.1 to apply the ProAV profile to one switch.
2. Click on the “List” tab at the top of the screen. A list of detected Yamaha switches will be displayed.



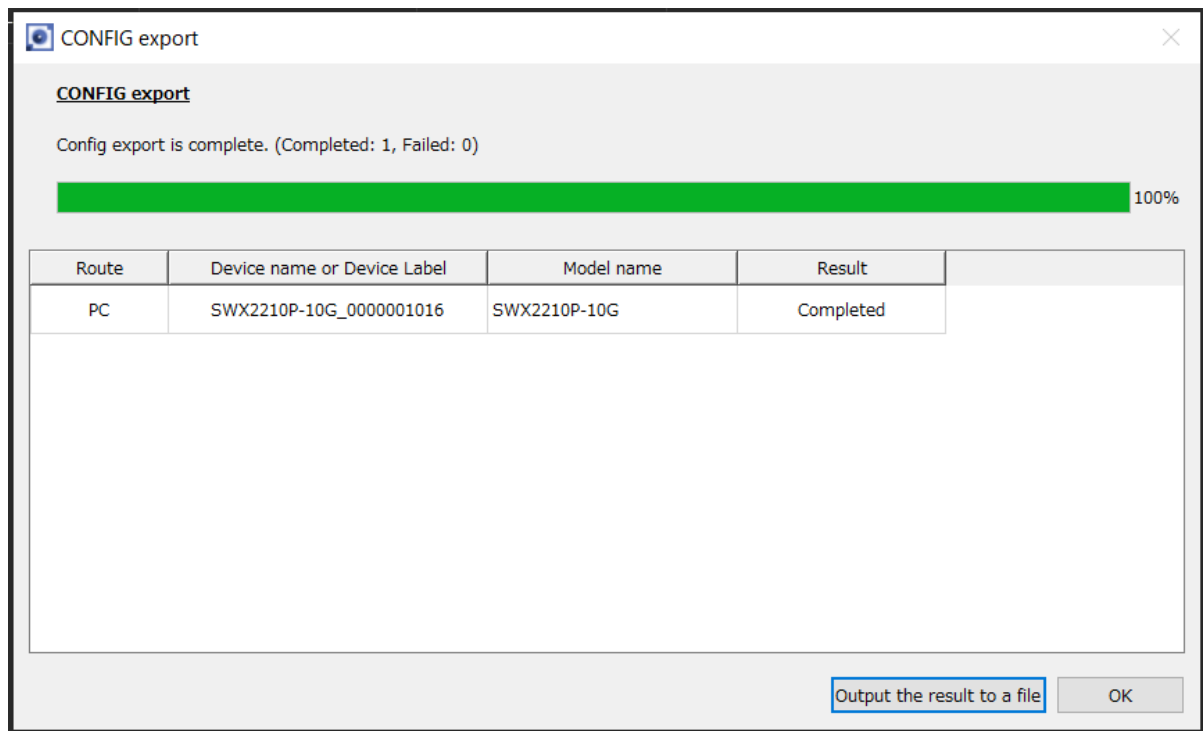
3. Click the “Config Import/Export” tab at the top of the screen. Additionally, check the switch to which the ProAV profile has already been applied, and click the “CONFIG export” button.



4. The “CONFIG export” dialog will appear. Select the directory in which you want to save the CONFIG file and click the “Execute” button.

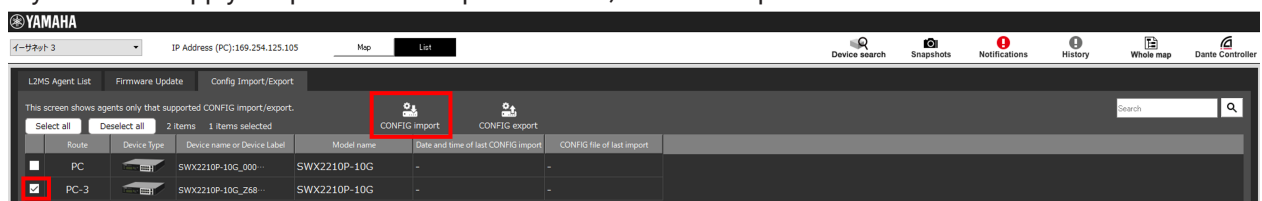


5. The dialog will display the progress and result of the export. Click the “OK” button when the export is completed.



6. Additionally, check the switch to which you want to apply the ProAV profile, and click the “CONFIG import” button.

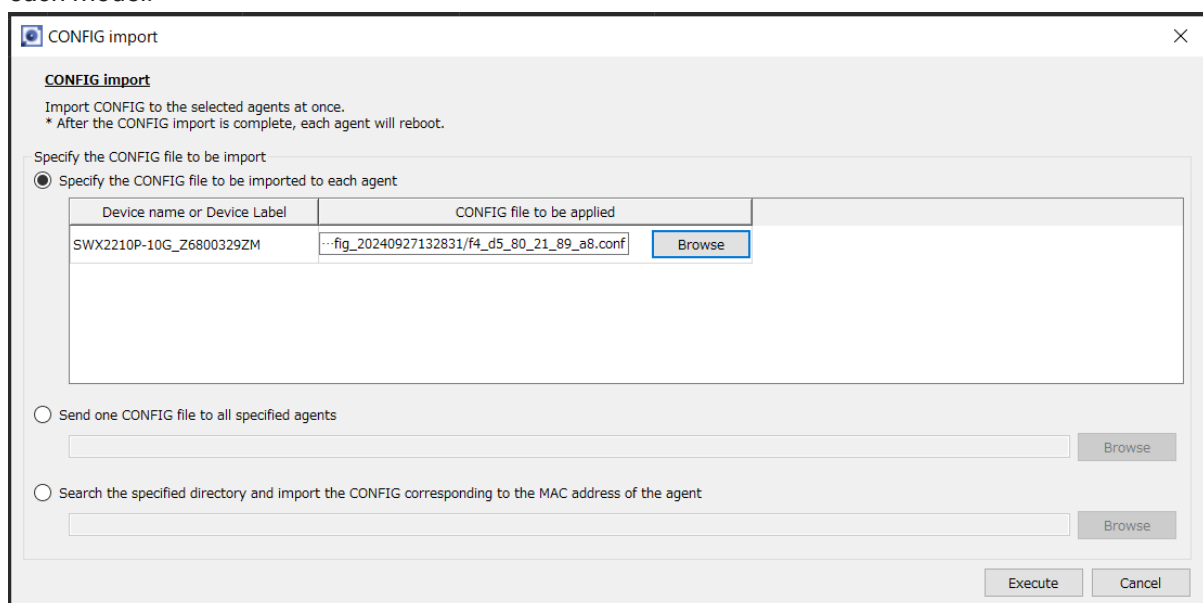
If you want to apply the profile to multiple switches, check multiple check boxes.



7. The “CONFIG import” dialog will appear. Select the CONFIG file saved in the previous step as an import file, and click the “Execute” button.

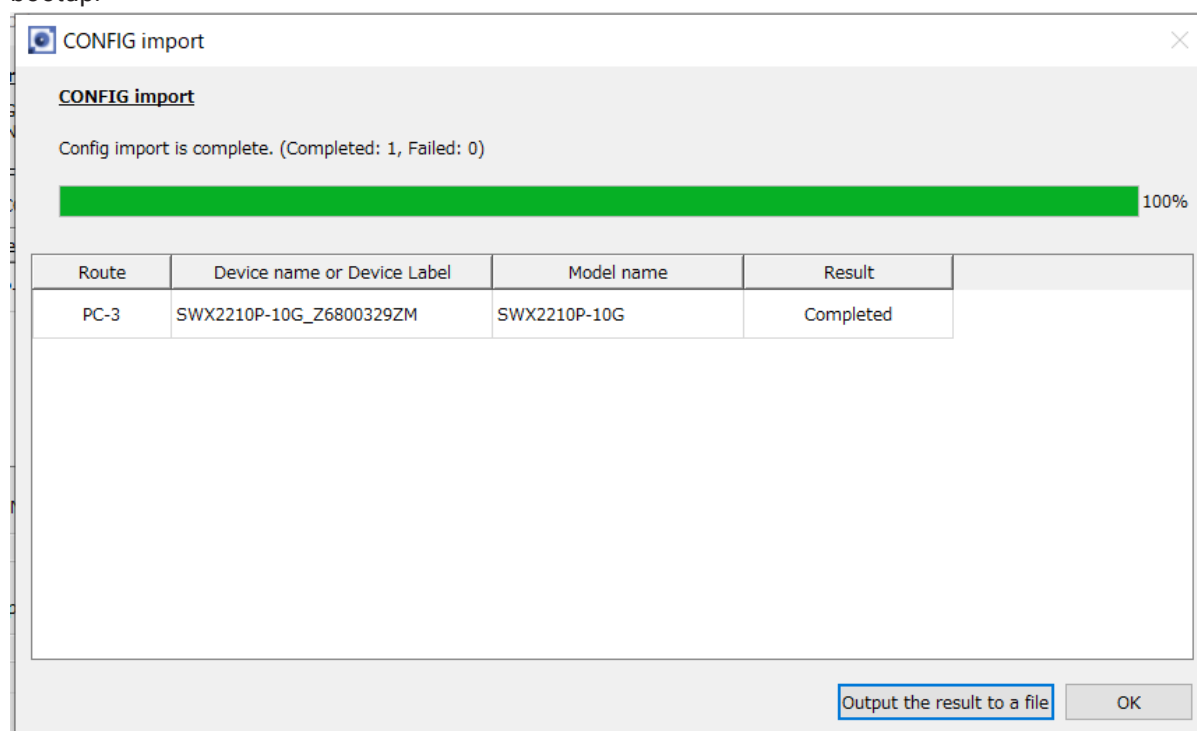
You can specify a CONFIG file for each selected switch, or you can specify the same CONFIG file for all selected switches.

In an environment where different models of switches are used, specify the appropriate CONFIG file for each model.



8. The dialog will display the progress and result of the import. Click the “OK” button when the import is completed.

The switch that receives CONFIG will automatically reboot and the new settings will be applied after the bootup.



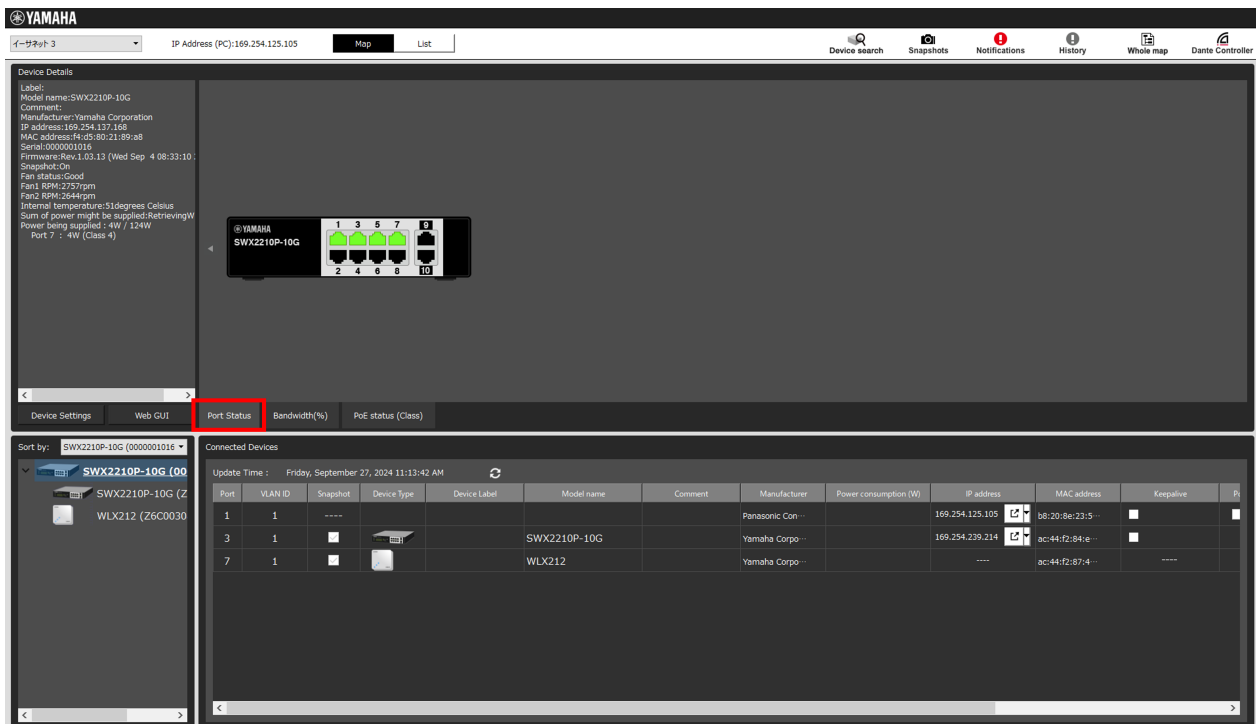
You can also update the firmware on multiple Yamaha switches at once by following the similar procedure using the “Firmware Update” button.

In this way, Yamaha LAN Monitor can be used as a kitting tool for multi-device environments, so please make use of it.

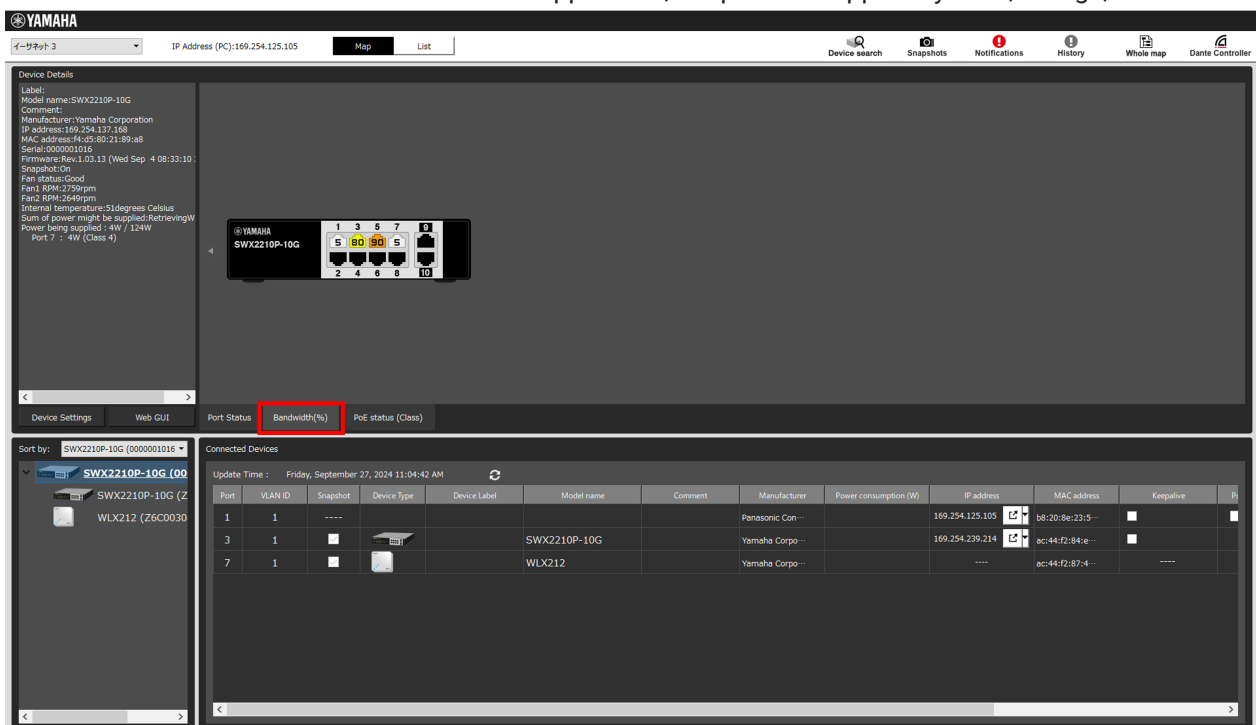
[Troubleshooting] Checking the network status

By using Yamaha LAN Monitor, you can visualize the connection configuration of the entire network, and also check traffic bandwidth usage and PoE power supply status.

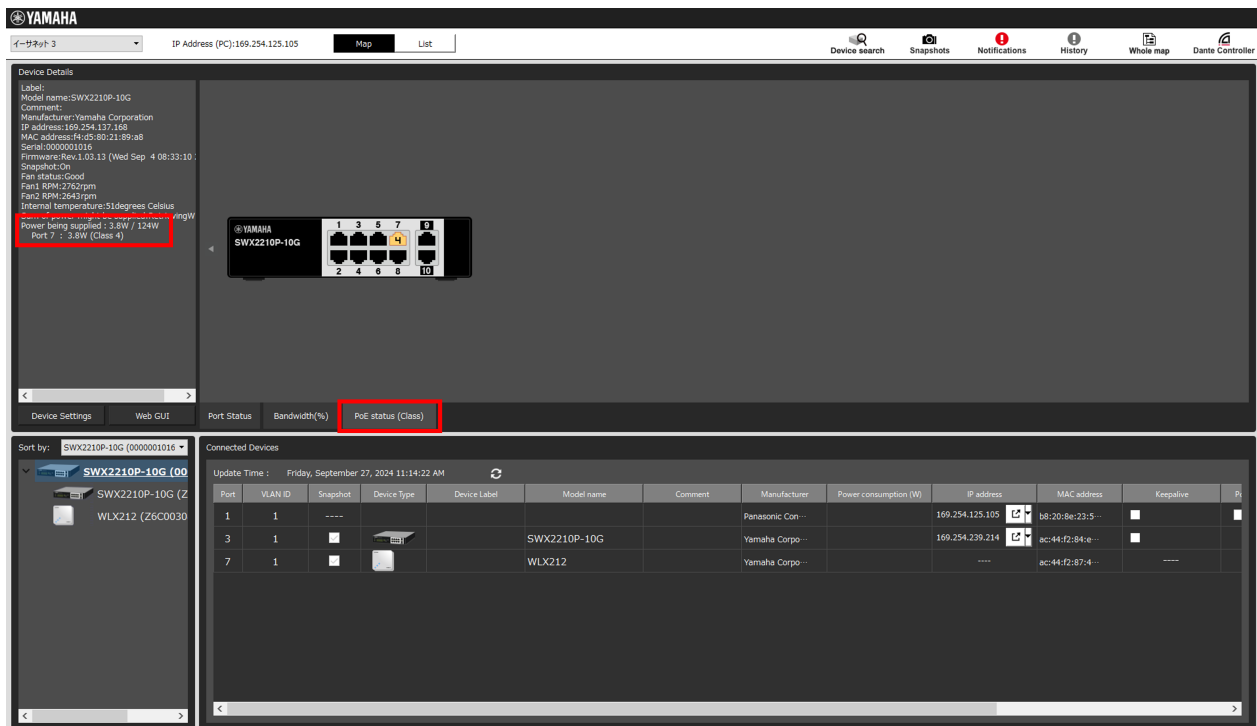
1. Click the switch icon.
“Port Status” is selected by default, which displays real-time link status on the front panel at the top of the screen.
The tree view at the bottom left of the screen allows you to check the current network connection configuration, and the connected device view at the bottom right of the screen allows you to see which devices are connected to which ports.



- To check the traffic bandwidth usage, click the “Bandwidth Usage (%)” button.
The bandwidth utilization of each port is displayed as the percentage against the link speed.
When the bandwidth utilization is close to its upper limit, the port icon appears yellow, orange, or red.



- To check the PoE power supply status, click “PoE Power Supply Status (Class)”.
The power supply class is displayed for ports that are supplying power, and the device details view in the upper left corner of the screen shows the total power supply and the power supply of each port.

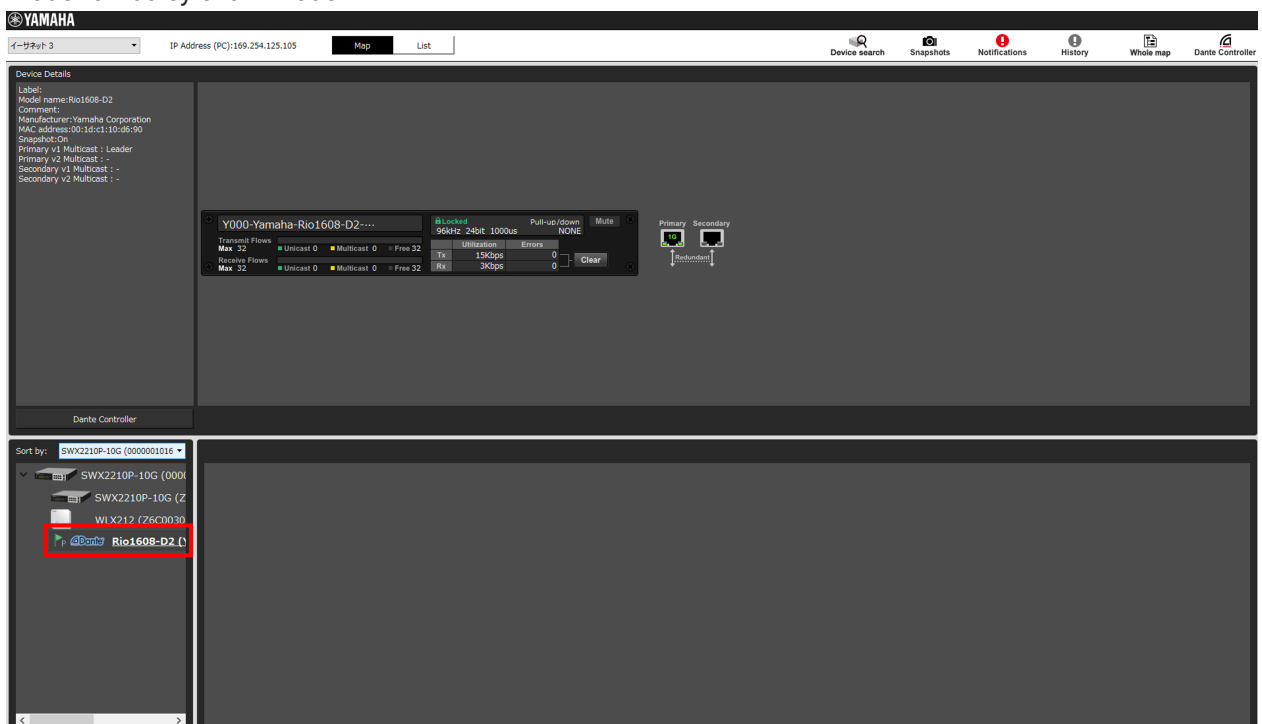


[Troubleshooting] Checking the Dante device status

Yamaha LAN Monitor allows you to check the status of Dante devices and open Dante Controller with one click if it is installed on your computer.

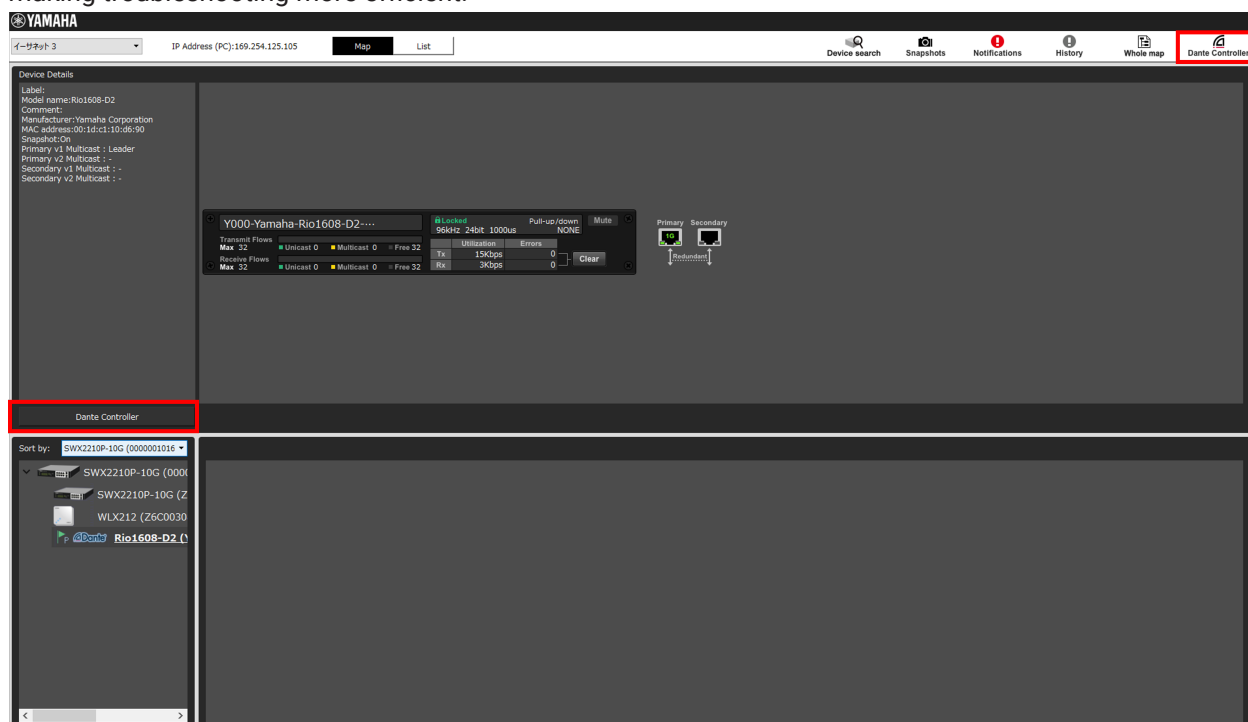
Note that, in order to view Dante devices, Dante Control and Monitoring and Dante Discovery must be installed when Yamaha LAN Monitor is installed.

1. With a Dante device connected to the Yamaha switch, click on the Dante device icon.
 You can monitor the status of the primary and secondary ports, the number of transmission and reception flows, etc.
 You can also check information such as whether the operating mode of the Dante device is “redundant mode” or “daisy chain mode”.



2. Dante Controller can be started by clicking the “Dante Controller” button in the top right or center of the screen. (Dante Controller must be installed beforehand.)

You can seamlessly switch between Yamaha LAN Monitor and Dante Controller on a single computer, making troubleshooting more efficient.



Points of Caution

- The settings configured collectively in ProAV settings are intended for use when this product is used as a switch dedicated to the AVoIP network.
When building a complex network, such as mixing an existing in-house network with an AVoIP network, use the GUI advanced settings pages and commands to appropriately configure the settings.
- When applying the ProAV profile, ports that belong to a logical interface must be detached from the logical interface.
If necessary, first detach the ports from the logical interface, assign the profile, and then re-attach them to the logical interface.
- The ProAV profile assumes an AVoIP network consisting only of Yamaha switches.
Note that, when the IGMP snooping function is used in a multi-vendor environment, determination of the opposing device via LLDP may not work.

Related Documentation

- None.

Trademarks and Trade Names

- Dante™ is a registered trademark of Audinate Pty Ltd.
- NDI® is a registered trademark of Vizrt NDI AB.

List of Default Settings

SWX2210P series default settings are indicated below.

- System-wide default settings

Category	Setting Parameter	Setting value
Console	Telnet console timeout	600 sec
	Number of VTYS	4
	Number of lines displayed	24
Password	Default administrative user	User name: admin Password: admin
	Administrator password	admin
	Encrypt password	Not encrypted
Time Management	Time zone	JST (UTC + 9.0)
	NTP server	None
	NTP update cycle	None
SNMP	Action	Disabled
SYSLOG	debug level log output	OFF
	information level log output	ON
	error level log output	ON
	SYSLOG server	None
Firmware Update	Download URL	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
	Permit downward revision	Prohibit
	Timeout	300 sec
LLDP	Action	Enabled
	Automatic setting function	Enabled
L2MS	Action	Enabled
	Role	Agent

Category	Setting Parameter	Setting value
Access control	Telnet server status	Start (port 23)
	Telnet server access	Allow access from all hosts
	TFTP server status	Do not start
	HTTP server status	Start (port 80)
	Secure HTTP server status	Start (port 443)
	HTTP/HTTPS server access	Allow access from all hosts
	SNMP server status	Start (port 161)
	SNMP server access	Allow access from all hosts
Interface control	MRU	1,522 Byte
	BPDU pass through	Enabled
	EAP pass through	Enabled
	Link Aggregation	None
L2 switching	Automatic MAC address acquisition	Enabled
	Automatic MAC address acquisition aging time	300 sec
	Proprietary Loop Detection	Enabled
	Multiple VLAN	None
IP multicast	IGMP snooping	Disabled
	MLD snooping	Disabled
DNS client	Action	Enabled
Traffic control	QoS	Disabled
	Flow control (IEEE 802.3x)	Disabled
PoE supply	Power supply actions	Enabled
	Guard band	7 W
Web GUI	Language setting	Japanese

- Default settings per LAN port

Category	Setting Parameter	Setting value
Basic settings	Speed/communication mode setting	auto
	Cross/straight automatic detection	Enabled
	Port description	None
	EEE	Disabled
	Port Mode	Access
	Associated VLAN ID	1 (default VLAN)
L2MS	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
LLDP agent	Transmit/receive mode	Enabled
PoE supply	Power supply actions	Enabled
	PoE power priority	Low

- Settings for default VLAN (vlan1)

Setting Parameter		Setting value
IPv4 Address		192.168.100.240/24
IGMP Snooping	Action	Disabled
MLD Snooping	Action	Disabled

Interface Control Functions

Basic Interface Functions

Function Overview

Here we explain the basic interface functions of this product.

Definition of Terms Used

None

Function Details

Interface types

This product can handle the five interface types shown in the table below.

Interface types	Interface ID	Explanation
LAN port	port	This is a physical port of this product. This interface is expressed as port followed by “port number printed on the chassis”. Specifying LAN port #1: port1.1
VLAN interface	vlan	This is a User-defined VLAN. This interface is expressed as vlan followed by “VLAN ID”. Specifying VLAN1: vlan1
Static logical interface	sa	This is the User-defined link aggregation. Multiple LAN ports can be grouped together and used as one interface. This interface is expressed as “ sa ” followed by “logical link ID”. Specifying a static logical interface for logical link ID #1: sa1

Interface control

The interface on this product can be controlled as shown in the table below.

- Interface control items for each port

Control items	Commands	Explanation
Set description	description	Sets the description text for the applicable interface.
Enable/disable	shutdown	Enables/disables the interface.

Control items	Commands	Explanation
Communication speed/communication mode	speed-duplex	Sets the communication speed and communication mode for the interface. (Select from the following values.) - Auto negotiation - 1Gbps / Full duplex - 100Mbps / Full duplex - 100Mbps / Half duplex - 10Mbps / Full duplex - 10Mbps / Half duplex
Cross/straight automatic detection (Auto MDI/MDI-X function)	mdix	Automatically detects the port type (MDI or MDI-X) of the connected port and the cable type (cross or straight). This function gives the ability to interconnect without dependency.
Speed downshift	-	This function automatically reduces the speed and attempts to link when a LAN cable that cannot be used with 1000BASE-T is connected. This function is always enabled for LAN ports. (Cannot be disabled.)
EEE	eee	Sets whether to use the energy saving technology for Ethernet (EEE: Energy Efficient Ethernet). This is standard for IEEE 802.3az.

- System-wide (common to all ports) interface control items

Control items	Commands	Explanation
MRU	mru	Sets the maximum frame size that can be received by the interface, within a range of 1,522–10,240 bytes .
BPDU pass through	pass-through bpdud	Sets whether to enable/disable the transmission of BPDUs (control frames used in the spanning tree).
EAP pass through	pass-through eap	Sets whether to enable or disable the transmission of EAP frames (authentication frames used in IEEE 802.1X authentication).

Command control of each interface is performed as shown on the table below.

- Interface control functionality chart

Interface name	Set description	Enable/disable	Communication speed/communication mode	Cross/straight automatic detection	EEE
LAN port	Yes	Yes	Yes	Yes	Yes
VLAN interface	Yes	No	No	No	No
Static logical interface	Yes	Yes	No	No	No

LAN port defaults

The product LAN ports are in the following state given default settings.

- All LAN ports function as access ports (ports that handle untagged frames), and belong to the default VLAN (VLAN #1).
- An IPv4 address (192.168.100.240/24) is assigned to the default VLAN (VLAN #1) to which all LAN ports belong.

Port mirroring

This product provides a port mirroring function, which copies the data traffic from a selected LAN port to another specified port.

The communication status can be analyzed by collecting the copied packets.

This product allows you to specify four mirror ports, making all other LAN ports allocable as “monitor ports.” However, the following restrictions apply.

- A single monitor port cannot be mirrored to multiple mirror ports.
- A port set as a mirror port cannot be used as a monitor port.
- A LAN port that belongs to a logical interface cannot be used as a mirror port.

The monitoring direction (transmit/receive, transmit only, receive only) can be selected for the monitor ports.

The **mirror** command can be used to set the port mirroring.

The mirror port setting is disabled by default.

Frame counter

This product counts the number of frames transmitted/received for each LAN port. (This is called a “frame counter”.)

To reference the frame counter, use the **show frame counter** command.

The table below shows the display items for the frame counter and their maximum values.

- Received frame counter display items

Display item	Explanation	Maximum value
packets (*1)	Number of received packets	4,294,967,295
octets	Number of octets received	18,446,744,073,709,551,615
total-good-packets (*2)	Number of packets received successfully	4,294,967,295
total-error-packets (*2)	Number of reception error packets (CRC error, alignment error, frame size error)	4,294,967,295
drops (*2)	Number of packets discarded during reception due to a filter function or other reasons	4,294,967,295
broadcast-and-multicast-packets	Broadcast and multicast packets received	4,294,967,295
64octet packets	Number of 64-octet packets received	4,294,967,295
65-127octet packets	Number of 65 to 127-octet packets received	4,294,967,295
128-255octet packets	Number of 128 to 255-octet packets received	4,294,967,295
256-511octet packets	Number of 256 to 511-octet packets received	4,294,967,295
512-1023octet packets	Number of 512 to 1,023-octet packets received	4,294,967,295

Display item	Explanation	Maximum value
1024-MAXoctet packets	Number of 1,024 to maximum-octet packets received (*3)	4,294,967,295

(*1) : The packet value is the total of the (*2) packets.

(*3) : The value will change, depending on the specified **MRU** value.

- Transmitted frame counter display items

Display item	Explanation	Maximum value
packets (*1)	Number of packets transmitted	4,294,967,295
octets	Number of octets transmitted	18,446,744,073,709,551,615
total-good-packets (*2)	Number of packets transmitted successfully	4,294,967,295
total-error-packets (*2)	Number of transmission error packets (Frame size error)	4,294,967,295
drops (*2)	Number of packets discarded during transmission (Since no discarding occurs on the sending side, the counter value is always 0.)	-
broadcast-and-multicast-packets	Broadcast and multicast packets transmitted	4,294,967,295
64octet packets	Number of 64-octet packets transmitted	4,294,967,295
65-127octet packets	Number of 65 to 127-octet packets transmitted	4,294,967,295
128-255octet packets	Number of 128 to 255-octet packets transmitted	4,294,967,295
256-511octet packets	Number of 256 to 511-octet packets transmitted	4,294,967,295
512-1023octet packets	Number of 512 to 1,023-octet packets transmitted	4,294,967,295
1024-MAXoctet packets	Number of 1,024 to maximum-octet (*3) packets transmitted	4,294,967,295

(*1) : The packet value is the total of the (*2) packets.

(*3) : The value will change, depending on the specified **MRU** value.

The frame counter can also be cleared by using the **clear counters** command.

When you execute the **show interface** command to display the LAN port status, the frame counter value to be displayed will be the same frame counter value as the **show frame-counter** command.

Related Commands

Related commands are indicated below.

For command details, refer to the command reference.

- Basic interface functions: list of related commands

Operations	Operating commands
Set description	description
Shutdown	shutdown
Set communication speed and communication mode	speed-duplex
Set cross/straight automatic detection	mdix auto
Set EEE	eee
Show EEE status information	show eee status
Set MRU	mru
Set BPDU pass through	pass-through bpdu
Set EAP pass through	eap-through bpdu
Set port mirroring	mirror
Show mirroring port status	show mirror
Show interface status	show interface
Show simplified interface status	show interface brief
Show frame counter	show frame-counter
Clear frame counters	clear counters

Examples of Command Execution

Basic LAN port settings

Some examples of basic LAN port settings are shown below.
For details on how to make the settings, refer to the Command Reference.

- Set the description text for LAN port #1 (port1.1).

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

- Disable LAN port #1 (port1.1).

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

- Enable LAN port #1 (port1.1).

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#no shutdown
```

- Set the communication speed and communication mode for LAN port #1 (port1.1) to **100Mbps/Full**.

```
Yamaha(config)#interface port1.1
```

```
Yamaha(config-if)#speed-duplex 100-full
```

Mirroring settings

In this example, we will set LAN port #1 to monitor the frames transmitted by LAN port #4 and the frames transmitted by LAN port #5.

The roles of the ports are shown below.

- Mirror port: LAN port #1 (port1.1)
 - Monitor port: LAN port #4 (port1.4), LAN port #5 (port1.5)
1. Set the monitor port for mirror port LAN port #1 (port1.1).

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#mirror interface port1.4 direction both ①
Yamaha(config-if)#mirror interface port1.5 direction transmit ②
```

- ① Monitor transmitted and received frames
- ② Monitor transmitted frames

2. Confirm the mirroring settings.

```
Yamaha#show mirror
Monitor Port  Mirror Port  Direction
-----
port1.1      port1.4      both
              port1.5      transmit
```

Show LAN port information

- Confirm the status of LAN port #1 (port1.1).

```
Yamaha#show interface port 1.1
Interface port1.1
Link is UP
Hardware is Ethernet
HW addr: 00a0.deae.b89f
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       : 34753
         bytes         : 7806026
```

```
      drops : 12535
      broadcast-and-multicast-packets: 21176
output packets : 10351
      bytes : 864389
      drops : 0
      broadcast-and-multicast-packets: 7039
```

Points of Caution

None

Related Documentation

None

Link Aggregation

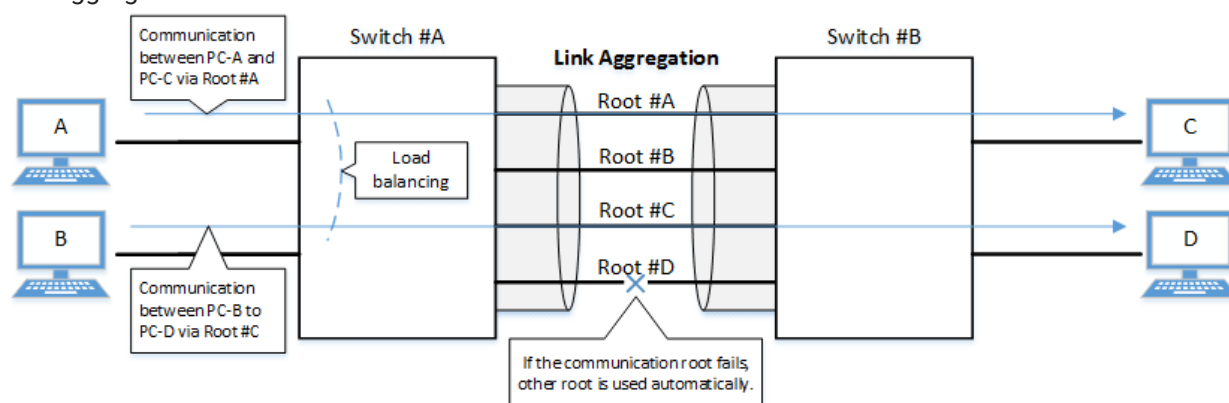
Function Overview

Link aggregation is a function used to combine multiple LAN ports that connect network devices, and handle them as a single logical interface.

Link aggregation is a technology that is useful when multiple communications occur. Communications can be distributed by using a [load balance](#) function within the combined lines.

If one LAN port fails within the lines that were combined using link aggregation, and communications cannot be made, the other ports will continue communicating.

• Link aggregation function overview



The link aggregation functions in this product are shown below.

• Link aggregation functions

Functions provided	Contents
Static link aggregation	Link aggregation for manually setting the LAN ports to combine. This begins to operate as a logical interface when the LAN ports link up.

Definition of Terms Used

Load balance

This is a function to distribute forwarded frames between the LAN ports that are associated with the logical interface.

As a distribution rule, the L2/L3/L4 information within frames is used.

Function Details

Static link aggregation specifications

The specifications for static link aggregation of this product are shown below.

1. The link aggregation of this product can be defined into **eight interfaces**.
An interface number from **1–8** can be assigned.
A single logical interface can be associated with **up to eight LAN ports**.
2. The settings shown below must be the same for each of the LAN ports contained within.
 - Port operation
 - Port mode (access/trunk [including native VLAN settings])

-
- Associated VLAN
 - Associated multiple VLAN group
3. It is recommended that the following settings be consistent across all LAN ports contained within.
- Communication speed/communication mode
 - Flow control
 - Storm control
 - L2MS filter/non-L2MS filter
4. The following operations can be performed for the logical interface.
- Add description text (**description** command)
 - Enable/disable the interface (**shutdown** command)
 - Configure a VLAN and multiple VLAN
5. The **port-channel load-balance** command allows you to select the [load balance](#) rule from the following items.
- The load balance setting is common to all logical interfaces.
The default setting is the **destination/source MAC address**.
- Destination MAC address
 - Source MAC address
 - Destination/source MAC address
 - Destination IP address
 - Source IP address
 - Destination/source IP address
 - Destination port number
 - Source port number
 - Destination/source port numbers
6. Use the **static-channel-group** command to associate a LAN port with a static logical interface.
- When associating a LAN port with an interface number for which there is no static logical interface, a new logical interface will be generated.
 - When the associated LAN port no longer exists as a result of removing LAN ports from a static logical interface, the relevant logical interface will be deleted.
 - One LAN port cannot be associated with multiple logical interfaces.
 - In addition, a LAN port used as a mirror port for port mirroring cannot be associated with a static logical interface.
7. Use the **show static-channel-group** command to show the static logical interface's status.

Related Commands

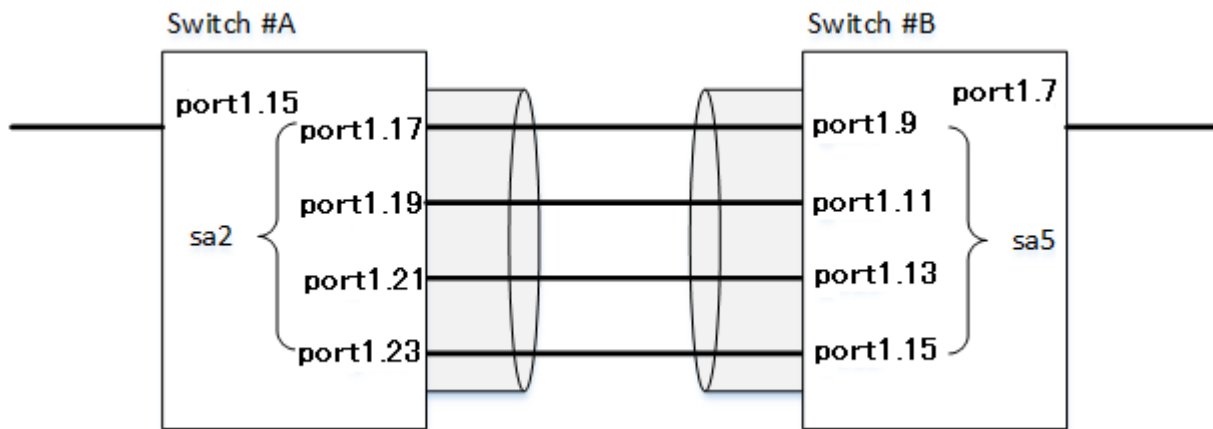
Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Set the static logical interface	static-channel-group
Show the static logical interface status	show static-channel-group
Set load balance function rules	port-channel load-balance

Examples of Command Execution

Set the static logical interface

In this example, we will set link aggregation to use four LAN ports, in order to communicate between L2 switches.



- Static link aggregation is set to static.
The logical interface numbers are as follows: Switch A: #2, switch B: #5.
- The LAN ports associated with the logical interface are all access ports, and are associated with the VLAN #1000.
 1. Define [switch A] VLAN #1000, and associate it with LAN ports (#15, #17, #19, #21, #23).
Together with this, associate LAN ports (#17, #19, #21, #23) with the logical interface #2.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.15 ②
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#interface port1.17 ④
Yamaha(config-if)#switchport access vlan 1000 ⑤
Yamaha(config-if)#static-channel-group 2 ⑥
Yamaha(config-if)#interface port1.19
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.21
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.23
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
```

- ① Define VLAN #1000
- ② Set LAN port #15
- ③ Set the port as access port and associate it with VLAN #1000
- ④ Set LAN port #17
- ⑤ Set the port as access port and associate it with VLAN #1000
- ⑥ Associate it with logical interface #2

2. Confirm the setting status of [switch A] logical interface #2.

```
Yamaha#show static-channel-group
% Static Aggregator: sa2
% Member:
  port1.17
  port1.19
  port1.21
  port1.23
```

3. Define [switch B] VLAN #1000, and associate it with LAN ports (#07, #09, #11, #13, #15). Together with this, associate LAN ports (#09, #11, #13, #15) with logical interface #5.

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.7
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#interface port1.9
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.11
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.13
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.15
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
```

4. Confirm the setting status of [switch B] logical interface #5.

```
Yamaha#show static-channel-group
% Static Aggregator: sa5
% Member:
  port1.9
  port1.11
  port1.13
  port1.15
```

5. Enable [switch A] logical interface.

```
Yamaha(config)#interface sa2 ①
Yamaha(config-if)#no shutdown ②
```

- ① Set logical interface #2
- ② Enable the logical interface

6. Enable [switch B] logical interface.

```
Yamaha(config)#interface sa5 ①
Yamaha(config-if)#no shutdown ②
```

- ① Set logical interface #5
- ② Enable the logical interface

7. Confirm the setting status of [switch A] logical interface.

```
Yamaha#show interface sa2
Interface sa2
  Link is UP
  Hardware is AGGREGATE
  MRU 1522
  BPDU pass-through: Enabled
  EAP pass-through: Enabled
  Description:
  ifIndex 4502
  Vlan info :
    Switchport mode      : access
    Ingress filter       : enable
    Acceptable frame types : all
    Default Vlan        : 1000
    Configured Vlans     : 1000
  Interface counter:
    input  packets      : 2109
           bytes        : 211698
           drops        : 0
           broadcast-and-multicast-packets: 2109
    output packets      : 24
           bytes        : 2952
           drops        : 0
           broadcast-and-multicast-packets: 24
```

8. Confirm the setting status of [switch B] logical interface.

```
Yamaha#show interface sa5
Interface sa5
  Link is UP
  Hardware is AGGREGATE
  MRU 1522
  BPDU pass-through: Enabled
  EAP pass-through: Enabled
  Description:
  ifIndex 4505
  Vlan info :
    Switchport mode      : access
    Ingress filter       : enable
    Acceptable frame types : all
    Default Vlan        : 1000
    Configured Vlans     : 1000
  Interface counter:
    input  packets      : 24
           bytes        : 2952
```

```
      drops : 0
      broadcast-and-multicast-packets: 24
output packets : 2109
      bytes : 211698
      drops : 0
      broadcast-and-multicast-packets: 2109
```

Points of Caution

None.

Related Documentation

- [Basic Interface Functions](#)

PoE Control

Function Overview

PoE (Power over Ethernet) is a technology that supplies power using an Ethernet cable (category 5e or higher). This product complies with **IEEE 802.3at**, which allows the product to supply power to Class 4 powered devices. In IEEE 802.3at, terms called

- Power supply side (device that supplies power) PSE: Power Sourcing Equipment
- Power receiving side (device that receives power): PD: Powered Device

are defined.

This product uses **Alternative A**, which uses the signal lines (1, 2, 3, 6) of cables as the power supply method.

Definition of Terms Used

None

Function Details

PoE power supply function enable/disable control

Ports that support PoE power supply of this product (hereinafter referred to as PoE ports) are as follows.

- SWX2210P-10G: ports 1 to 8
- SWX2210P-18G: ports 1 to 16
- SWX2210P-28G: ports 1 to 24

The power supply function of all the PoE ports of this product is enabled as the factory default.

However, the power supply function can also be disabled on the each port basis.

If the connected device is a normal Ethernet device, the power will not be supplied and the device will operate as a **normal Ethernet port**.

Power supply class and maximum number of ports that can be powered simultaneously

This product is a power supply device that complies with the PoE standards. It can supply **up to 30 W of power per port**.

It automatically detects the connected PD, identifies its power class, and starts the power supply.

The power classes defined in IEEE 802.3at and the maximum number of ports that can be powered simultaneously are shown below.

Class	Power of device that receives power (MAX)	Power of device that supplies power	Maximum number of ports that can be powered simultaneously (Upper limit of PoE power supply)		
			SWX2210P-10G(124W)	SWX2210P-18G(247W)	SWX2210P-28G(370W)
0	13.0 W	15.4 W	8	16	24
1	3.84 W	4.0 W	8	16	24
2	6.49 W	7.0 W	8	16	24
3	13.0 W	15.4 W	8	16	24
4	25.5 W	30.0 W	4 (*)	8 (*)	12 (*)

-
- (*): Depending on the power consumption of the device that receives power, the simultaneous power supply beyond the number of ports listed can be performed.

Guard band

A guard band is a margin set for the maximum power supply to prevent unexpected power outages.

If the available power supply amount reaches or falls below the guard band, power supply to a newly connected PD will be suppressed.

Setting this guard band value appropriately can prevent a newly connected PD from stopping the power supply to other PDs.

This product allows you to specify the guard band value in the range of **0 to 30 W**. The default is **7 W**.

PoE power priority

This product allows you to specify the power supply priority order for each PoE port.

The priority is **critical**, **high**, and **low** in descending order. The default is low for all ports.

Among ports with the same priority setting, the smaller the port number, the higher the priority. The priority goes down in the port number order (1 → 2 → 3...).

When an LLDP frame containing the Power via MDI TLV is received from a PD, the PoE port that received the LLDP frame operates with the power supply priority specified in the LLDP frame regardless of the power supply priority setting.

PoE power supply actions

This product performs the following processes depending on the power consumption.

- When the power consumption of the entire system is about to exceed the upper limit of the PoE power supply.
Power supply from PoE ports is stopped in the order from the lower priority to ensure that power consumption remains within the upper limit of PoE power supply.
At this time, the PoE STATE LED of the port to which power supply has been stopped lights up orange, and the STATUS LED also lights up orange.
In addition, "PortX.X over system power limit" is output to SYSLOG.
- If the available power supply amount reaches or falls below the guard band
Power will continue to be supplied to PDs that are already being powered. However, power will not be supplied to a newly-connected PD regardless of its power supply priority.
At this case, the PoE STATE LED of the port to which power was not supplied lights up orange, and the STATUS LED also lights up orange.
- When the power consumption of a specific PoE port has exceeded the upper limit of the PoE power supply per port
Power supply to the corresponding PoE port will be stopped. Power supply to other PoE ports will continue.
At this time, the PoE STATE LED of the port to which power supply has been stopped flashes orange, and the STATUS LED lights up orange.
In addition, "PortX.X over load" is output to SYSLOG.
- If power consumption is other than the above (within normal range)
Power supply to PDs will continue.
At this time, the PoE STATE LED of the PoE port being powered lights up green.

In addition, the following processing will be performed if the PoE port status or the available power supply amount has changed.

- When power supply is started
"PortX.X power on" is output to SYSLOG.

The PoE STATE LED of the PoE port to which power supply has started lights up green.

- When power supply is stopped
"PortX.X power off" is output to SYSLOG.
The PoE STATE LED of the PoE port to which power supply has been stopped turns off.
- When the remaining available power supply amount reaches or falls below the guard band
"guardband on" is output to SYSLOG.
- When the remaining available power supply amount recovers from a state at or below the guard band
"guardband off" is output to SYSLOG.

Power supply setting by LLDP

When the product receives an LLDP frame containing the Power via MDI TLV from a PD, it automatically changes the power supply action of the PoE port.

This function only works on PoE ports that can receive LLDP frames.

The Power Via MDI TLVs and the corresponding action to be changed are as shown below.

Power Via MDI TLV (IEEE802.3)	Action to be changed
Requested power priority	PoE power priority
PD requested power value	PoE port power allocation

Related Commands

Related commands are indicated below.

For command details, refer to the command reference.

Operations	Operating commands
Set the PoE power supply function for the entire system	power-inline enable
Set the PoE power supply function on an interface basis	power-inline enable
Set the description text for PoE ports	power-inline description
Set the PoE port priority	power-inline priority
Set a guard band	power-inline guardband
Show PoE power supply information	show power-inline

Examples of Command Execution

PoE Port Power Supply Settings

Specify the settings for the power supply function of port1.8.

```
Yamaha(config)#power-inline enable ①
Yamaha(config)#interface port1.8
Yamaha(config-if)#power-inline description AP1 ②
Yamaha(config-if)#power-inline priority critical ③
Yamaha(config-if)#power-inline enable ④
Yamaha(config-if)#exit
Yamaha(config)#exit
```

-
- ① Enable the PoE power supply function for the entire system. * Not required if the default settings are used
 - ② Set AP1 as the PoE port description
 - ③ Set the PoE port priority to the highest
 - ④ Enable the PoE power supply function of the interface. * Not required if the default settings are used

Points of Caution

None

Related Documentation

None

Layer 2 Functions

Forwarding Database

Function Overview

The Forwarding Database (subsequently referred to as the FDB) manages the combination of destination MAC addresses, transmission ports, and VLANs.

This product uses the FDB to determine the forwarding destination port for the received frames.

1. Enable/disable acquisition function
2. Hold Time adjustment for FDB entries acquired
3. Timeout clear for FDB entries acquired
4. Manual registration of FDB entries (static entries)

Definition of Terms Used

FDB

Abbreviation of "Forwarding Data Base."

This database manages the combination of destination MAC address, transmission port, and VLAN.

FDB entry

This is data registered in the FDB, and consists of multiple elements.

Function Details

FDB entry

On this product, the contents listed in the table below are registered as a single entry in the FDB.

Element managed	Description
MAC address	Device MAC addresses can be either unicast or multicast.
VLAN-ID (FID)	The VLAN ID to which the device belongs. This is a value from 1–4094.
Forwarding destination interface ID	The interface on which the device exists*. (*: LAN port or static logical interface)
Action	The processing method for frames addressed to the device. There are two processing methods, "discard" and "forward".
Registration type	The registration type of entries. There are the following types: * dynamic ... Entries registered through automatic acquisition * static ... Entries registered manually via commands

MAC address

This is one of the FDB key items; the VLAN-ID and MAC address are combined to become the record key. Operation differs depending on whether the MAC address is unicast or multicast.

- Unicast
Since the forwarding destination interface ID must be uniquely determined for a given record key,

duplication is not allowed.
(Multiple combinations of the same VLAN-ID and MAC address do not exist.)

- **Multicast**

Multiple forwarding destination interface IDs may exist for a given key record.
In this case, frames are sent to multiple forwarding destination interface IDs.

Up to 8,192 addresses can be registered in this product, including addresses registered via automatic acquisition and manual registration.

The MAC addresses of all received frames can be acquired, and the source MAC address is acquired and registered in the FDB.

(However, if the transmission source MAC address is multicast, this is considered an invalid frame and is discarded without being registered.)

Automatically acquired MAC address information is maintained until the ageing timeout.

VLAN-ID

MAC address acquisition is done per VLAN, and the MAC address and VLAN are managed in the FDB as a pair. For different VLANs, identical MAC addresses are also acquired.

Forwarding destination interface ID

The following IDs are registered.

- LAN port (port)
- Static interface (sa)

Action

This defines the action for a received frame that matches a key record.
If the MAC address is unicast, the actions are as follows.

- forward ... Forward to the forwarding destination interface ID.
- discard ... Discard without forwarding.

If the MAC address is multicast, the actions are as follows.

- forward ... Forward to the forwarding destination interface ID.
- discard ... Cannot be specified.
(The discard setting cannot be made if the MAC address is multicast.)

Registration type

- dynamic ... Registered and deleted automatically. The registration result does not remain in the config file.
- static ... Registered and deleted manually, and therefore remains in the config file.

Automatic MAC address acquisition

Automatic MAC address acquisition refers to the active creation and registration of FDB entries based on the information for the source MAC address of the received frame and the information for the reception port.

Entries registered through automatic acquisition are called “dynamic entries”.

A timer (ageing time) is used to monitor individual entries.

Entries for MAC addresses that have not received frames within a certain amount of time will be deleted from the FDB (see below*).

This prevents invalid device entries from being left over in the FDB due to power shutoff, being moved and so on.

If a frame is received within the specified amount of time, the monitoring timer will be reset.

The control specifications for automatic acquisition are shown below.

1. Automatic MAC address acquisition can be enabled or disabled using the **mac-address-table learning** command.
The setting is enabled by default.
2. If automatic acquisition is changed from enabled to disabled, **all dynamic entries that have been learned will be deleted**.
The acquisition function “disable” setting is useful when you want to flood all ports with all received frames.
3. The aging timer for dynamic entries can be adjusted between **10 and 634 seconds**. The value is specified using **mac-address-table ageing-time** command.
This value is set to 300 seconds by default.
4. Clear the dynamic entries that have been acquired by using the **clear mac-address-table dynamic** command.
The entire contents of the FDB can be cleared at once; or a VLAN number can be specified and all MAC addresses acquired by that VLAN can be cleared from the FDB.
Specifying the port number will clear all MAC addresses from the FDB that were acquired from that port.
5. Use the **show mac-address-table** command to check the automatic acquisition status.
6. There may be a discrepancy between the time set with the **mac-address-table ageing-time** command and the time until the dynamic entry is actually deleted from the MAC address table.

MAC address manual setting

In addition to automatic acquisition using received frames, MAC addresses can be set on this product by using user commands.

Entries that have been registered by using commands are called “static entries”.

The specifications for manual settings are shown below.

1. Use the **mac-address-table static** command to register static entries.
2. The number of static entries that can be manually registered is 256.
3. When registering static entries, dynamic acquisition will not be performed on the corresponding MAC addresses.
Entries that have already been acquired will be deleted from the FDB, and will be registered as static entries.
4. Use the **no mac-address-table static** command to delete static entries.
5. Either “forward” or “discard” can be specified for the destination MAC address of a received frame.
 - When forwarding is specified, either the LAN port forwarding destination or the static logical interface can be specified.
 - When discarding is specified, frames received by the MAC address will not be forwarded to any port, and will be discarded.
6. If registering a multicast MAC address, you cannot specify “discard.”
Also, MAC addresses in the following ranges cannot be registered.
 - 0180.c200.0000–0180.c200.000f
 - 0180.c200.0020–0180.c200.002f

Related Commands

Related commands are indicated below.

For details, refer to the Command Reference.

Operations	Operating commands
Enable/disable the MAC address learning function	mac-address-table learning
Set dynamic entry ageing time	mac-address-table ageing-time
Delete dynamic entries	clear mac-address-table dynamic
Register static entries	mac-address-table static
Delete static entries	no mac-address-table static
View the MAC address table	show mac-address-table

Examples of Command Execution

Referring to the FDB

```
Yamaha#show mac-address-table
VLAN  port    mac          fwd    type    timeout
  1   port1.2  00a0.de11.2233 forward static      0
  1   port1.1  1803.731e.8c2b forward dynamic  300
  1   port1.1  782b.cbc2.218d forward dynamic  300
```

Delete dynamic entries

Deleting an FDB entry registered in the FDB (MAC address 00:a0:de:11:22:33)

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

Changing the dynamic entry ageing time

This example shows how to change the dynamic entry ageing time to 600 seconds.

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

Register static entries

This example shows how frames addressed to a device associated with VLAN #10 (MAC address 00:a0:de:11:22:33) can be forwarded to LAN port 2 (port1.2).

```
Yamaha(config)#mac-address-table static 00a0.de11.2233 forward port1.2 vlan 10
```

This example shows how to discard the frames sent to a device associated with VLAN #10 (MAC address 00:a0:de:11:22:33).

Specifying the interface name ("port1.2" in the example) will have no effect on operations. Since this cannot be omitted, specify the LAN port.

```
Yamaha(config)#mac-address-table static 00a0.de11.2233 discard port1.2 vlan 10
```

Delete static entries

This example shows how to delete the forwarding settings sent to a device associated with VLAN #10 (MAC address 00:a0:de:11:22:33).

```
Yamaha(config)#no mac-address-table static 00a0.de11.2233 forward port1.2 vlan 10
```

Points of Caution

None

Related Documentation

None

VLAN

Function Overview

VLAN (Virtual LAN) is technology that allows a LAN to be constructed virtually, without regard to the physical structure of connections.

This product lets you use VLANs to divide the LAN into [multiple broadcast domains](#).

The VLANs that are supported by this product are shown below.

VLAN types	Summary
Port-based VLAN	Groups that can communicate are configured for each LAN port.
Tagged VLAN	Groups that can communicate are identified, based on the fixed-length tag information appended to the Ethernet frame. Multiple and different VLANs can be made to communicate by means of one LAN port.

Definition of Terms Used

Broadcast domain

This is a range in which broadcast frames can be delivered in a network, such as an Ethernet.

Devices that are connected by relaying a data link layer (MAC layer), such as switching hubs, can belong to the same broadcast domain.

A broadcast domain generally refers to the network in an Ethernet.

Function Details

Defining a VLAN ID

On product, a maximum of 255 VLANs can be defined, with VLAN IDs ranging from 2–4094. (ID #1 is used as the default VLAN ID.)

VLAN IDs are defined using the **vlan** command, after the **vlan database** command is used to enter VLAN mode. For details, refer to the Command Reference.

VLAN settings for the LAN ports

The following settings must be configured after defining the VLANs to use, in order to make use of VLAN on this product.

- LAN port mode settings
- VLAN associations for LAN ports

1. The LAN ports on this product are set to one of the following modes.

- Access port
This is a port that handles untagged frames. It can be associated with one VLAN.
- Trunk port
This is a port that handles both tagged and untagged frames.
It can be associated with multiple VLANs, and is mainly used to connect switches to one another.
This product only supports IEEE 802.1Q. (Cisco ISL is not supported.)

2. Use the **switchport mode** command to set the LAN port mode.
When setting the trunk port, use the input filter (“ingress-filter”) to control whether frames not belonging to the specified VLAN ID will be handled.

-
- Input filter enabled: Only frames set to the specified VLAN ID will be handled.
 - Input filter disabled: Frames with any VLAN ID will be handled.
3. Use the **show interface switchport** command to check the LAN port setting mode.
 4. Use the **switchport access vlan** command to set which VLANs belong to the access port.
 5. Use the **switchport trunk allowed vlan** command to set which VLANs belong to the trunk port.
As the trunk port can be associated with multiple VLANs, use the “all”, “none”, “except”, “add” and “remove” settings as shown below.
 - add
Adds the specified VLAN ID.
VLAN IDs that can be added are limited by the IDs that are defined by the VLAN mode.
 - remove
Deletes the specified VLAN ID.
 - all
Adds all VLAN IDs specified by the VLAN mode.
The VLAN IDs added by the VLAN mode can also be added after this command is executed.
 - none
The trunk port will not be associated with any VLAN.
 - except
Adds all other VLAN IDs except for the ones specified.
The VLAN IDs added by the VLAN mode can also be added after this command is executed.
 6. A VLAN that uses untagged frames (native VLAN) can be specified for the trunk port.
 7. Use the **show vlan** command to check which VLANs belong to a LAN port.

Default VLAN

The default VLAN is VLAN #1 (vlan1), which exists in this switch by default.

As the default VLAN is a special VLAN, it always exists and cannot be deleted.

The following operations can be used to automatically delete the relevant port from the default VLAN.

- Setting any VLAN other than the default as the VLAN for the access port
- Setting any VLAN other than the default as the native VLAN for the trunk port
- Setting the native VLAN for the trunk port to “none”

Native VLAN

A native VLAN is a VLAN that associates untagged frames received by the LAN port that was set as a trunk port.

Defining a LAN port as a trunk port will set the default VLAN (VLAN #1) as the native VLAN.

Use the **switchport trunk native vlan** command when specifying a certain VLAN as the native VLAN.

If you do not want to handle untagged frames on the LAN port, you can set the native VLAN to none. (Specify “none” with the “**switchport trunk native vlan**” command.)

Related Commands

List of related commands

Related commands are indicated below.

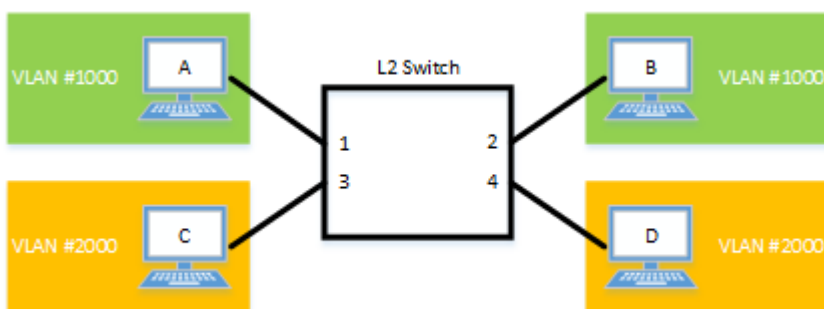
For details, refer to the Command Reference.

Operations	Operating commands
Enter VLAN mode	vlan database
Define VLAN interface, or change a predefined VLAN	vlan
Set access port (untagged port)	switchport mode access
Set associated VLAN of an access port (untagged port)	switchport access vlan
Set trunk port (tagged port)	switchport mode trunk
Set associated VLAN for trunk port (tagged port)	switchport trunk allowed vlan
Set native VLAN for trunk port (tagged port)	switchport trunk native vlan
Show VLAN information	show vlan

Examples of Command Execution

Port-based VLAN settings

In this example, a port-based VLAN is configured for this product in order to allow communication between hosts A–B and hosts C–D.



The LAN port settings for this product are as follows.

- LAN ports #1 and #2: Set as access port, and associated with VLAN #1000
- LAN ports #3 and #4: Set as access port, and associated with VLAN #2000

■ Setting Procedure

1. Switch to VLAN mode using the **vlan database** command, and define two VLANs using the **vlan** command.

```
Yamaha(config)# vlan database ①
Yamaha(config-vlan)# vlan 1000 ②
Yamaha(config-vlan)# vlan 2000 ③
Yamaha(config-if)# exit
```

- ① Switch to VLAN mode
- ② Create VLAN #1000
- ③ Create VLAN #2000

2. Set LAN ports #1–2 as access ports, and associate them with VLAN #1000.

```
Yamaha(config)# interface port1.1 ①
```

```

Yamaha(config-if)# switchport mode access ②
Yamaha(config-if)# switchport access vlan 1000 ③
Yamaha(config-if)# interface port1.2 ④
Yamaha(config-if)# switchport mode access ⑤
Yamaha(config-if)# switchport access vlan 1000 ⑥
Yamaha(config-if)# exit

```

- ① Switch to interface mode
- ② Set the ports as access port
- ③ Define a VLAN ID
- ④ Switch to interface mode
- ⑤ Set the ports as access port
- ⑥ Define a VLAN ID

3. Set LAN ports #3–4 as access ports, and associate them with VLAN #2000.

```

Yamaha(config)# interface port1.3
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 2000
Yamaha(config-if)# interface port1.4
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 2000
Yamaha(config-if)# exit

```

4. Confirm the VLAN settings.

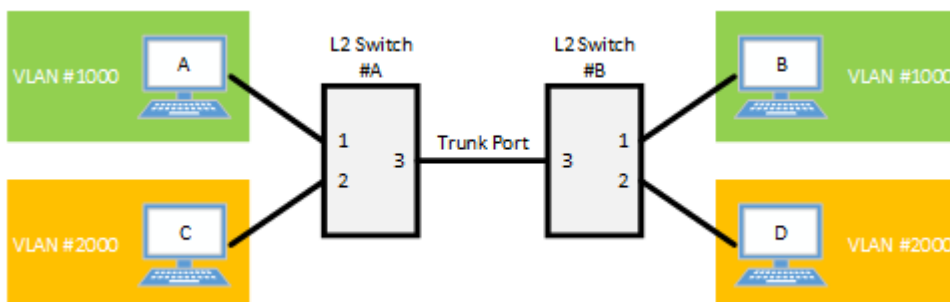
```

Yamaha#show vlan brief
(u)-Untagged, (t)-Tagged
VLAN ID  Name          State  Member ports
=====
1        default      ACTIVE port1.5(u) port1.6(u) port1.7(u)
                port1.8(u) port1.9(u) port1.10(u)
1000     VLAN1000      ACTIVE port1.1(u) port1.2(u)
2000     VLAN2000      ACTIVE port1.3(u) port1.4(u)

```

Tagged VLAN settings

In this example, a tagged VLAN is configured between #A and #B of this product, in order to communicate between hosts A–B and hosts C–D.



The LAN port settings for #A and #B of this product are as follows.

- LAN port #1: Set as access port, and associated with VLAN #1000
- LAN port #2: Set as access port, and associated with VLAN #2000
- LAN port #3: Set as trunk port, and associated with LAN #1000 and VLAN #2000

1. [Switch #A/#B] Define VLAN.

```
Yamaha(config)#vlan database ①  
Yamaha(config-vlan)#vlan 1000 ②  
Yamaha(config-vlan)#vlan 2000 ③
```

- ① Switch to vlan mode
- ② Define VLAN #1000
- ③ Define VLAN #2000

2. [Switch #A/#B] Set LAN port #1 as the access port, and associate it with VLAN #1000.

```
Yamaha(config)#interface port1.1 ①  
Yamaha(config-if)#switchport mode access ②  
Yamaha(config-if)#switchport access vlan 1000 ③  
Yamaha(config-if)#exit
```

- ① Switch to interface mode
- ② Set the ports as access port
- ③ Associate it with VLAN #1000

3. [Switch #A/#B] Set LAN port #2 as an access port, and associate it with VLAN #2000.

```
Yamaha(config)#interface port1.2 ①  
Yamaha(config-if)#switchport mode access ②  
Yamaha(config-if)#switchport access vlan 2000 ③  
Yamaha(config-if)#exit
```

- ① Switch to interface mode
- ② Set the ports as access port
- ③ Associate it with VLAN #2000

4. [Switch #A/#B] Set LAN port #3 as a trunk port, and associate it with VLAN #1000/#2000.

```
Yamaha(config)#interface port1.3 ①  
Yamaha(config-if)#switchport mode trunk ②  
Yamaha(config-if)#switchport trunk allowed vlan add 1000 ③  
Yamaha(config-if)#switchport trunk allowed vlan add 2000 ④  
Yamaha(config-if)#exit
```

- ① Switch to interface mode
- ② Set the port as trunk port
- ③ Add VLAN #1000
- ④ Add VLAN #2000

5. Confirm the VLAN settings.

```
Yamaha#show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID Name                               State  Member ports
-----
1      default                             ACTIVE port1.3(u) port1.4(u) port1.5(u)
                                           port1.6(u) port1.7(u) port1.8(u)
                                           port1.9(u) port1.10(u)
1000   VLAN1000                             ACTIVE port1.1(u) port1.3(t)
2000   VLAN2000                             ACTIVE port1.2(u) port1.3(t)
```

Points of Caution

None

Related Documentation

None

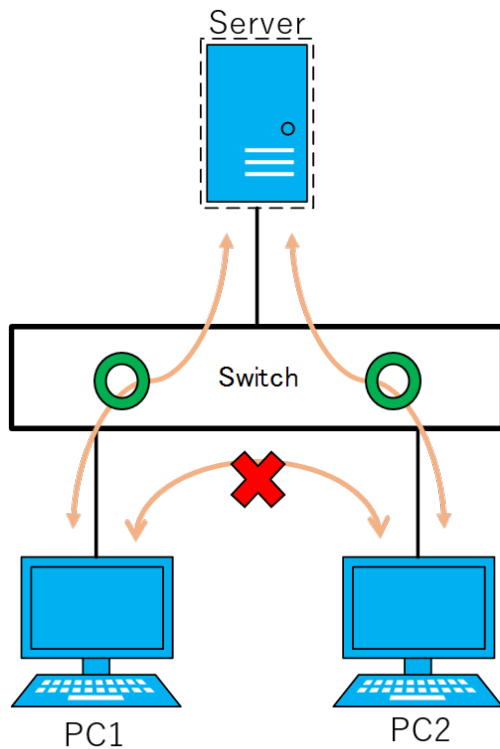
Multiple VLAN

Function Overview

Multiple VLAN allows you to divide ports belonging to the same VLAN into multiple groups and block communication between the groups.

In addition to dividing ports into multiple groups, you can also have one port participate in multiple groups. This function allows users to easily realize the needs such as those shown in the diagram, where communication between terminals needs to be blocked while each terminal can access the server.

- Example of using multiple VLANs



Definition of Terms Used

None

Function Details

Basic operating specifications

Multiple VLAN allows you to create groups within a VLAN.

Use the **switchport multiple-vlan group** command to configure a multiple VLAN group.

Multiple VLANs can be configured on LAN interfaces and link aggregation logical interfaces.

If you wish to configure a multiple VLAN group for a trunk port, this will be applied to all relevant VLANs that belong to the port in question.

The multiple VLAN group settings will also be applied to a multicast frame (*1).

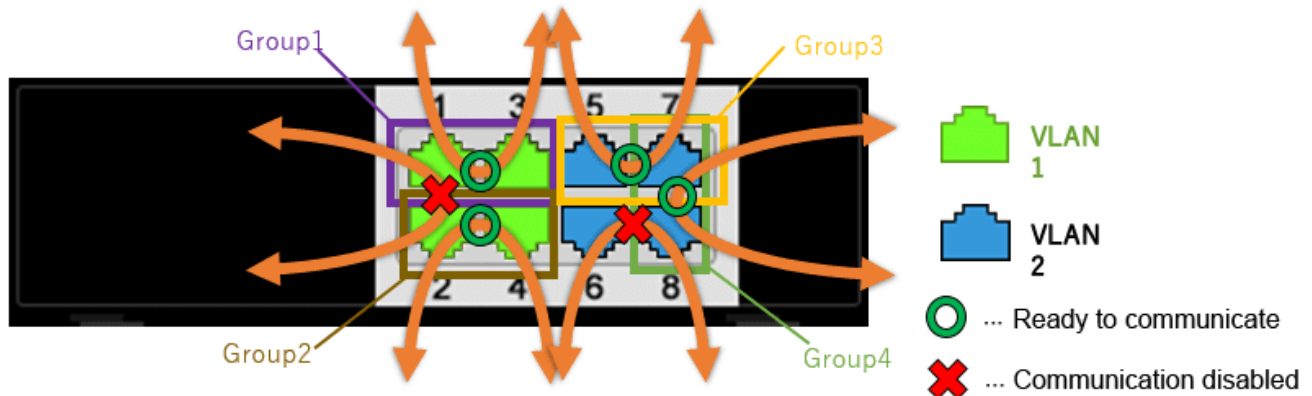
The maximum number of groups is equal to the number of ports on the product.

(*1): The following frames are forwarded to ports with different multiple VLAN groups.

- L2MS control frame

- Control frames used by Yamaha wireless access points
- BPDU frame when BPDU pass through is enabled

Examples of traffic between multiple VLAN groups



When using multiple VLAN group settings (Group #1 through #4) as shown in the diagram above, enabling/disabling traffic between specific ports A/B and the reasons for such as shown in the table below.

Port number A (group)	Port number B (group)	Traffic enable/disable	Reason
port1.1 (Group 1)	port1.2 (Group 2)	Disabled	The multiple VLAN group is different
port1.1 (Group 1)	port1.3 (Group 1)	Enabled	Associated with multiple VLAN group #1
port1.2 (Group 2)	port1.4 (Group 2)	Enabled	Associated with multiple VLAN group #2
port1.5 (Group 3)	port1.7 (Group 3,4)	Enabled	Associated with multiple VLAN group #3
port1.6 (no group)	port1.8 (Group 4)	Disabled	The multiple VLAN group is different
port1.7 (Group 3,4)	port1.8 (Group 4)	Enabled	Associated with multiple VLAN group #4

*In the above example, port1.6 cannot communicate with any port. However, if there are other ports that do not belong to any group, communication is possible between the ports that do not belong to any group.

Related Commands

List of related commands

Related commands are indicated below.
For details, refer to the Command Reference.

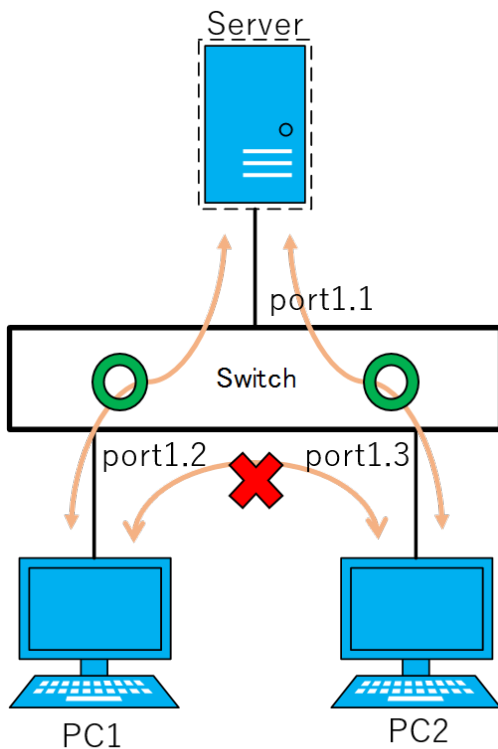
Operations	Operating commands
Multiple VLAN group settings	switchport multiple-vlan group

Examples of Command Execution

Multiple VLAN settings

Within VLAN #1, communication is allowed between PC1 and Server and between PC2 and Server, but communication is blocked between PC1 and PC2.

- Example of multiple VLAN settings



The multiple VLAN group settings are as follows.

- port1.1: Associated with multiple VLAN groups #1 and #2
- port1.2: Associated with multiple VLAN group #1
- port1.3: Associated with multiple VLAN group #2

1. Associate port1.1 with multiple VLAN groups #1 and #2.

```
Yamaha(config)# interface port1.1 ①  
Yamaha(config-if)# switchport multiple-vlan group 1 ②  
Yamaha(config-if)# switchport multiple-vlan group 2 ③  
Yamaha(config-if)# exit
```

- ① Switch to interface mode
- ② Join in multiple VLAN group #1
- ③ Join in multiple VLAN group #2

2. Associate port1.2 with multiple VLAN group #1.

```
Yamaha(config)# interface port1.2 ①  
Yamaha(config-if)# switchport multiple-vlan group 1 ②  
Yamaha(config-if)# exit
```

- ① Switch to interface mode

② Join in multiple VLAN group #1

3. Associate port1.3 with multiple VLAN group #2.

```
Yamaha(config)# interface port1.3 ①  
Yamaha(config-if)# switchport multiple-vlan group 2 ②  
Yamaha(config-if)# exit
```

① Switch to interface mode

② Join in multiple VLAN group #2

Points of Caution

The points of caution regarding this function are as follows.

- The multiple VLAN group to associate with a link aggregation logical interface must be the same.
- A multiple VLAN group is only applicable to forwarding between ports. Voluntary packets will not be affected by the settings of a multiple VLAN group.
- Even if a multiple VLAN is configured, communication may not work correctly due to the following influences.
 - Blocked status of loop detection

Related Documentation

None

Proprietary Loop Detection

Function Overview

This product offers a proprietary system to detect whether there is a loop in the network environment that was configured.

A proprietary loop detection frame is sent from the LAN port, and the unit monitors whether the frame returns or not.

If the transmitted frame returns, the system determines that there is a loop in the port in question.

Definition of Terms Used

LDF (Loop Detection Frame)

This is a Yamaha proprietary Ethernet frame that is used to detect loops.

Function Details

Loop detection operating specifications

The loop detection specifications for this product are shown below.

1. In addition to enabling/disabling the entire system, the loop detection on this product can enable/disable individual ports.
When detecting loops in LAN ports, the system-wide setting must be set to **enable**.
 - Use the **loop-detect** command in global configuration mode for the system-wide setting.
 - Use the **loop-detect** command in the interface mode of the relevant port for the individual LAN port setting.
2. The default settings for the loop detection function are as shown below.
 - System-wide setting: Enabled
 - LAN port setting: Enabled
3. If the loop detection function is enabled for this product, the following operations are performed.
 - Loop detection frames (hereafter “LDF”) are sent **every two seconds** from the linked-up LAN port. **The loop detection function cannot be used** on static logical interfaces, and ports on which mirror settings have been made (mirror ports).
 - When a LAN port receives the loop detection frame that has been sent from the port, a loop occurrence is determined, and the following operations are performed.
 - **Port Blocking**
When the port number of the transmitting LAN port is smaller than the receiving port number, all frames except for LDF are blocked.
The LDF will be transmitted periodically, but LDF will not be forwarded from other devices. For the LAN ports that were blocked, if the LDF that was transmitted does not return within five seconds, it is determined that the loop has been resolved, and normal communications are resumed.
If the blocking duration is specified with the **loop-detect blocking interval** command, a check is made to see if the loop has been resolved when the specified time has elapsed since the loop was detected.
At this time, if the loop is resolved, the blocking status will be cleared, but if the loop is not resolved, the blocking status will continue until the specified time has elapsed again.
 - **Port Detected**
When the port number of the LAN port that was transmitted is larger than the port number during reception, another port is doing the blocking, so communication continues as normal.

- When a loop is detected, the **LINK/ACT LED** indicator on this product will change to **flashing orange**, the **STATUS LED** indicator will change to **illuminating orange**, and the following SYSLOG message will be output.

■ [LOOP]: inf: Detected Loop! : port1.1 ①

① Displayed every 5 seconds from the start of loop detection

- The port lamp display on this product is restored as communications are resumed after the loop is resolved, and the following SYSLOG message is output.

■ [LOOP]: inf: Recovered Loop! : port1.1

4. A force-clear can be performed on the loop detection status (detected, blocking) by using the **loop-detect reset** command.

If a linkdown has occurred on the port where a loop has been detected, the detection status will be cleared.

5. The status of the loop detection function can be checked using the **show loop-detect** command. The following is displayed.

- System Enable/disable status
- Loop detection status (status for each LAN port)

6. When an LDF is received by a LAN port when the loop detection function is disabled, the received frames from all other ports will be forwarded as-is.

However, frames will not be forwarded for static logical interfaces and ports on which mirror settings have been made (mirror ports).

7. In the following kinds of situations, loops in hubs that are connected to this product might not be detected.

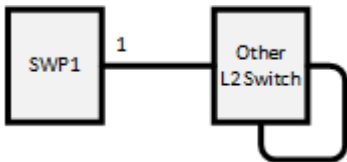
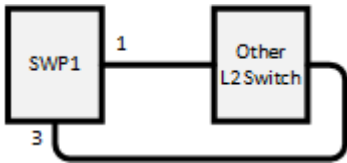
- Loops are being detected in a connected hub
- Loop detection frames are not being forwarded by a connected hub

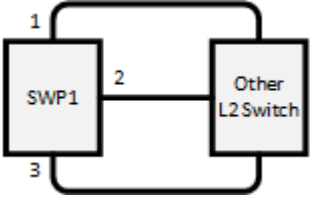
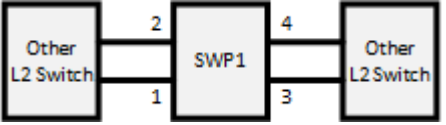
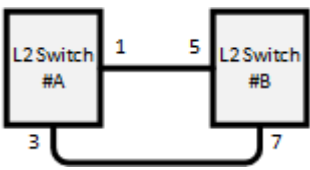
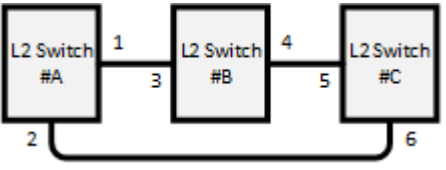
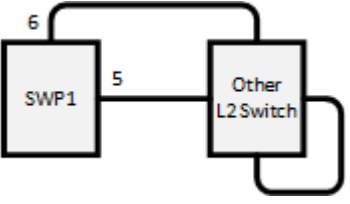
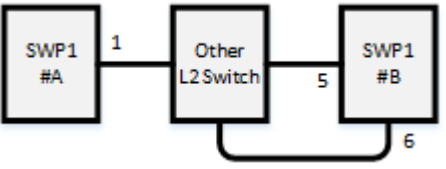
8. If a loop occurs between different port-based VLANs or different multiple VLANs, the following actions are taken.

Condition	Action
A loop occurs between ports that belong to different port-based VLANs	No blocking
A loop occurs between ports that belong to different multiple VLANs	Blocking

Loop detection examples

The following shows examples of loop detection in this product.

Loop detection case	Configuration example	Loop detection status
1		A loop is detected when a port receives the LDF that it has transmitted. port1.1: Blocking
2		When loops are detected in multiple ports on the same terminal, the port with the largest number is blocked. port1.1: Detected port1.3: Blocking

Loop detection case	Configuration example	Loop detection status
3		<p>The loop is avoided by blocking multiple ports. The blocking port is selected using the same rules as case 2.</p> <ul style="list-style-type: none"> port1.1: Detected port1.2: Blocking port1.3: Blocking
4		<p>When loops are detected in multiple groups, the port with the largest number in each group</p> <ul style="list-style-type: none"> port1.1: Detected, port1.2: Blocking port1.3: Detected, port1.4: Blocking
5		<p>When a loop occurs between two switches, one of the switches detects the loop.</p> <ul style="list-style-type: none"> ◦When detected in port1.3 of switch #A <ul style="list-style-type: none"> port1.1: Detected, port1.3: Blocking ◦When detected in port1.7 of switch #B <ul style="list-style-type: none"> port1.5: Detected, port1.7: Blocking
6		<p>Out of the six ports that are connected by cable, the port for which the loop is most quickly detected is the one that is blocked.</p> <ul style="list-style-type: none"> ◦When detected in port1.2 of switch #A <ul style="list-style-type: none"> port1.1: Detected, port1.2: Blocking ◦When detected in port1.4 of switch #B <ul style="list-style-type: none"> port1.3: Detected, port1.4: Blocking ◦When detected in port1.6 of switch #C <ul style="list-style-type: none"> port1.5: Detected, port1.6: Blocking
7		<p>Because the LDF transmitted from each port returns to these ports, port1.5 and port1.6 will both be blocked.</p> <ul style="list-style-type: none"> port1.5: Blocking port1.6: Blocking
8		<p>Port1.6 of switch #B is blocked. Depending on the timing, port1.1 of switch #A will also be blocked; but the loop in port1.1 of switch #A is resolved by blocking port1.6 of switch #B.</p> <ul style="list-style-type: none"> Switch #A port1.1: Blocking Switch #B port1.5: Detected Switch #B port1.6: Blocking

Related Commands

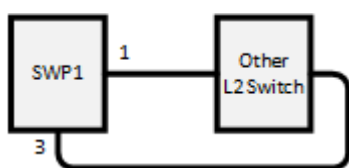
Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Enable/disable loop detection function (system)	loop-detect enable/disable
Enable/disable loop detection function (LAN port)	loop-detect enable/disable
Set the port blocking duration when a loop is detected	loop-detect blocking interval
Reset the loop detection status	loop-detect reset
Refer to the setting status of loop detection	show loop-detect

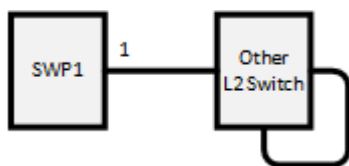
Examples of Command Execution

This example detects any loops occurring on this product using the following configuration, when the loop detection function is enabled.

- [Example 1] Loop occurring within this product



- [Example 2] Loop occurring in a third-party hub connected to this product



This sets LAN ports #1 and #3 to detect loops.

■ Setting Procedure

1. Enable the loop detection function for the entire system.

```
Yamaha(config)#loop-detect enable ①
```

- ① Enable the loop detection function for the entire system

2. Enable the loop detection function for LAN ports #1 and #3.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#loop-detect enable ①
(上記設定をLANポート #3 に対しても行います。)
```

- ① Enable the loop detection function for each LAN port
 - 。 Both the loop detection function for the entire system and that for each LAN port are enabled in default settings.

3. Confirm that the loop detection function has been set.
Confirm whether the loop detection function is enabled(*) for LAN ports #1 and #3.

```
Yamaha>show loop-detect
```

```
loop-detect: Enable
```

port	loop-detect	status
port1.1	enable(*)	Normal
port1.2	enable(*)	Normal
port1.3	enable(*)	Normal
port1.4	enable(*)	Normal
:	:	:

4. If a loop has been detected, the loop detection status can be checked.

。 In the case of example 1:

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

port	loop-detect	status
port1.1	enable(*)	Detected ①
port1.2	enable(*)	Normal
port1.3	enable(*)	Blocking ②
port1.4	enable(*)	Normal
:	:	:

① LAN port #1 enters the detected status

② LAN port #3 enters the blocking status

。 In the case of example 2:

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

port	loop-detect	status
port1.1	enable(*)	Blocking ①
port1.2	enable(*)	Normal
port1.3	enable(*)	Normal
port1.4	enable(*)	Normal
:	:	:

① LAN port #1 enters the blocking status

Points of Caution

None

Related Documentation

None

Pass Through

Function Overview

Pass through is a function that forwards frames addressed to reserved special MAC addresses without discarding them, which would normally be discarded by a normal switch.

This product supports pass-through of BPDU frames used in the spanning tree protocol and EAP frames used in IEEE 802.1X authentication.

When the BPDU pass through is enabled, this product can be installed between switches that use the spanning tree protocol.

When EAP pass through is enabled, this product can be installed between an IEEE 802.1X authenticated switch and a computer.

Definition of Terms Used

BPDU (Bridge Protocol Data Unit)

This is a message used in the spanning tree protocol to avoid loops between compatible devices.

EAP (Extended authentication protocol)

This is an authentication protocol that extends PPP, allowing various authentication methods to be used. This protocol is defined in RFC 3748.

IEEE 802.1X authentication supports the use of this protocol.

Function Details

Operating specifications for BPDU pass through

The specifications for BPDU pass through are indicated below.

1. By enabling BPDU pass through, received BPDU frames can be forwarded without being discarded. If BPDU pass through is disabled, received BPDU frames will be discarded and will not be forwarded.
2. BPDU frames are **forwarded to all ports except the port on which the frames were received, regardless of the settings for tagged VLAN, port-based VLAN, and multiple VLAN.**
3. You can enable or disable BPDU pass through using the **pass-through bpd** command or by navigating to [Detailed settings] - [Pass through] in the web GUI. This function is enabled by default.
4. The BPDU pass through setting is applied on a system-wide basis (common to all ports).

Operating specifications for EAP pass through

The specifications for EAP pass through are indicated below.

1. By enabling EAP pass through, received EAP frames can be forwarded without being discarded. If EAP pass through is disabled, received EAP frames will be discarded and will not be forwarded.
2. EAP frames are **forwarded in the same way as normal multicast frames, according to the settings for tagged VLAN, port-based VLAN, and multiple VLAN.**
3. You can enable or disable EAP pass through using the **pass-through eap** command or by navigating to [Detailed settings] - [Pass through] in the web GUI. This function is enabled by default.
4. The EAP pass through setting is applied on a system-wide basis (common to all ports).

Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Enable/disable BPDU pass through	pass-through bpdu
Enable/disable EAP pass through	pass-through eap

Examples of Command Execution

Enable BPDU pass through for installing this product between switches that use the spanning tree protocol.

- Enable BPDU pass through.

```
Yamaha(config)#pass-through bpdu enable ①
```

- ① Enable BPDU pass through

Enable EAP pass through for installing this product between an IEEE 802.1X authenticated switch and a computer.

- Enable EAP pass through.

```
Yamaha(config)#pass-through eap enable ①
```

- ① Enable EAP pass through

Points of Caution

None

Related Documentation

None

Layer 3 Functions

IPv4/IPv6 Common Settings

Function Overview

This product is compatible with the following **network environment settings that are common to IPv4 and IPv6**, mainly for the purpose of maintenance (configuring the settings of the switch).

1. DNS client settings

Definition of Terms Used

None

Function Details

DNS client settings

This product supports **DNS (Domain Name System) clients**.

If an **FQDN (Fully Qualified Domain Name)** has been set for an NTP server or a syslog server, an inquiry is made to the DNS server to retrieve the IPv4/IPv6 address.

This product provides the following DNS client control functions.

- Set IP address of the DNS server
- Set default domain name
- Set search domain list

Inquiries to the DNS server are **enabled** by default, and the setting can be changed by using the **dns-client enable/disable** command.

Set IP address of the DNS server

Up to three IP addresses can be set for the DNS server, using the methods shown below.

- Manual setting using the **dns-client name-server** command
 - This lets you specify the IPv4/IPv6 address.
- Automatic setting via DHCP

This product **always gives priority to the information that was set via commands**. Check the configured DNS servers by using the **show dns-client** command.

Set default domain name

Only one default domain can be set using the methods shown below. The domain can be specified using up to **256 characters**.

- Manual setting using the **dns-client domain-name** command
- Automatic setting via DHCP

Just as with DNS server IP addresses, this product **prioritizes information specified with commands**.

Check the default domain that was set by using the **show dns-client** command.

The use of a default domain is only allowed if there are no listings in the search domain list.

Set search domain list

This product uses a search domain list to manage the domain names used when inquiring with the DNS. **Up to six** domain names can be set on the search domain list using the method below.

- Manual setting using the **dns-client domain-list** command

The search domain list that has been set can be checked using the **show dns-client** command. The search domain list **must be within 255 characters total for all domain names registered**.

Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

Function types	Operations	Operating commands
DNS client settings	DNS client settings	dns-client enable/disable
	Set DNS server address	dns-client name-server
	Set default domain name	dns-client domain-name
	Set search domain list	dns-client domain-list
	Show DNS client settings	show dns-client

Examples of Command Execution

DNS client settings

Set DNS client settings for this product to prepare an environment for DNS queries.

- Specify 192.168.100.1 and 192.168.100.2 as the IP addresses of the servers for DNS queries.
- Specify example.com as the default domain used for DNS queries.

■ Setting Procedure

1. Enable the DNS query functionality.

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

- Since this is specified as the default value, we do not need to set this specifically.

2. Specify the DNS servers.

```
Yamaha(config)#dns-client name-server 192.168.100.1
Yamaha(config)#dns-client name-server 192.168.100.2
```

3. Set the default domain.

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

4. Check the DNS client information that was set.

```
Yamaha#show dns-client
```

```
DNS client is enabled
```

```
Default domain  : example.com
```

```
Domain list     :
```

```
Name Servers    : 192.168.100.1 192.168.100.2
```

```
* - Values assigned by DHCP Client.
```

Points of Caution

None

Related Documentation

None

Basic IPv4 Settings

Function Overview

This product is compatible with the following **IPv4 network environment settings**, mainly for the purpose of maintenance (configuring the settings of the switch).

1. IPv4 address settings
2. Route information settings
3. ARP table settings

Definition of Terms Used

IPv4 Link Local Address

This is an address that is only valid within the same segment, within the range of **169.254.0.0/16 to 169.254.255.255/16**.

Function Details

IPv4 address settings

This product lets you specify the **IPv4 address and subnet mask** for a **VLAN interface**.
As the setting method, both **fixed settings** and **automatic settings via DHCP** are supported.

- To set the fixed/automatic IPv4 address, use the **ip address** command.
- The IPv4 address setting cannot be left unspecified.
- The following actions occur if addresses are specified automatically by DHCP.
 - The HostName option (option code 12) can be added to the Discover/Request message.
 - The lease time requested to the DHCP server is **fixed at 72 hours**. (The actual lease time will depend on the setting of the DHCP server.)
 - If the **ip address** command is executed with automatic settings and the settings are changed to fixed settings, a release message for the IPv4 address obtained is sent to the DHCP server.
 - The information obtained from the DHCP server can be checked using the **show dhcp lease**.
- An IPv4 address can only be specified for **one VLAN interface**.
If an IPv4 address already specified for a VLAN interface is specified for another VLAN interface, the IPv4 address for the old VLAN interface will be deleted.
The IPv4 address that is allocated to a VLAN interface can be checked using the **show ip interface** command.
- In the initial state, **192.168.100.240/24** is fixed for the **default VLAN (VLAN #1)**.

Auto IP function

As part of the IPv4 address setting functionality, this product provides an auto IP function which automatically generates IPv4 link local addresses based on the MAC address.

The auto IP function only works when an IPv4 address has not been allocated from the DHCP server. (The IPv4 address must be set to "DHCP" as a prerequisite.)

This function confirms whether the automatically-generated IPv4 link local address does not already exist on the network via ARP.

If it has been confirmed that the address does not already exist, the generated address will start to be used.

If the IPv4 address was allocated from the DHCP server after the IPv4 link local address was determined via auto IP, the IPv4 link local address is discarded, and the IP address obtained from the DHCP server is used.

-
- The auto IP function can only be **enabled for VLAN interfaces whose IPv4 address is specified**. In the initial state, the **default VLAN (VLAN #1)** is enabled.

Route information settings

This product refers to a routing table when sending syslog messages and when sending out voluntary IPv4 packets as an IPv4 host for NTP-based time adjustments and so on.

This product uses the following functions to perform the routing table operations.

- Set VLAN interface route information
- Set default gateway
- Show route information

Route information for VLAN interfaces

When setting an IPv4 address on this product for a VLAN interface, the correspondence between the network address and VLAN ID is automatically set as route information.

Set default gateway

The destination for IPv4 packets sent to network addresses that are not set in the routing table can be set as the default gateway on this product.

- To set the default gateway, use the **ip route** command.
- To show the default gateway, use the **show ip route** command.

Show route information

- This product is provided with an FIB (Forwarding Information Base: IP forwarding table) as route information.

FIB is a database that is referenced when deciding how to forward IP packets.

Use the **show ip route** command to check the FIB.

ARP table settings

When sending IPv4 packets, this product uses ARP (Address Resolution Protocol) to obtain the MAC addresses from the IPv4 addresses.

The correspondence between IPv4 address and MAC address is saved in the ARP table with the following specifications.

- The **ARP entries** saved in the ARP table manage the following information.
 - IPv4 address
 - MAC address
 - VLAN interface
- The number of ARP table entries is guaranteed to operate **up to 512 entries**.
- With the default settings, dynamic entries saved in the ARP table are maintained for **300 sec**. The entry timeout value can be changed using the **arp-ageing-timeout** command.
- Dynamic entries saved in the ARP table can be cleared regardless of the timeout value, by using the **clear arp-cache** command.
- Use the **show arp** command to check the ARP table.

Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

Function types	Operations	Operating commands
IPv4 address settings	IPv4 address settings	ip address
	Show IPv4 address	show ip interface
	Set dynamic IPv4 address by DHCP client	ip address dhcp
	Show DHCP client status	show dhcp lease
Route information settings	Set default gateway	ip route
	Show default gateway	show ip route
ARP table settings	Show ARP table	show arp
	Set the dynamic entry hold time	arp-ageing-timeout
	Clear dynamic entries	clear arp-cache

Examples of Command Execution

IPv4 network environment settings (DHCP)

In this example, the IPv4 addresses are set on this product, and an environment is set up for accessing the unit from a remote terminal.

- The IPv4 address is set automatically by **DHCP** for the default VLAN (VLAN #1).
1. Check the IPv4 address that is currently set.
If the default settings are still in effect, the fixed IPv4 address (192.168.100.240/24) is set.

```
Yamaha#show ip interface brief
Interface      IP-Address      Status      Protocol
vlan1          192.168.100.240 up           up
```

2. Specify DHCP for the default VLAN (VLAN #1).
 - Changing the IP address may disable access to this product. Use particular caution when making any changes.

```
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ip address dhcp
Do you really want to change IP address? [y/N]:y
```

3. Use TELNET to access the IP address allocated by the DHCP server and log in.

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

```
SWX2210P-10G Rev.1.03.03 (Thu Jan 16 13:20:45 2020)
Copyright (c) 2018-2020 Yamaha Corporation. All Rights Reserved.
```

```
Yamaha>enable
Password:*****
Yamaha#
```

4. After logging in, check the information provided by the DHCP server.

```
Yamaha#show dhcp lease
Interface    vlan1
-----
IP Address:      192.168.1.9
Expires:         2019/10/13 18:47:32
Renew:           2019/10/12 18:47:32
Rebind:          2019/10/13 12:47:33
Server:
Options:
  subnet-mask    255.255.255.0
  default-gateway 192.168.1.1
  dhcp-lease-time 172800
  domain-name-servers 192.168.1.1
  dhcp-server-identifier 192.168.1.1
  domain-name     domain.test
```

Points of Caution

When the IPv4 address settings are changed, all of the following commands related to remote access control will be deleted.

Use particular caution when changing the IPv4 address.

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

Related Documentation

- [L2 Switching Function: VLAN](#)
- [Remote Access Function: Remote Access Control](#)
- [Yamaha RTpro: What is ARP?](#)

Basic IPv6 Settings

Function Overview

This product is compatible with the following **IPv6 network environment settings**, mainly for the purpose of maintenance (configuring the switch settings).

1. IPv6 address settings
2. Route information settings
3. Neighbor cache table settings

Definition of Terms Used

RA (Router Advertisement)

This is a system that automatically sets address information and network settings on the IPv6 network for devices of the network that is associated with a router.

IPv6 address

The IPv6 address is 128 bits expressed as hexadecimal. The address is divided into eight fields delimited by ":" with 16 bits in each field.

- **2001:02f8:0000:0000:1111:2222:0000:4444**

The expression can be abbreviated according to the following rules.

- If the beginning of a field is a zero, the zero can be omitted.
- A field that consists of four zeros can be abbreviated as a single zero.
- Multiple fields consisting only of consecutive zeros can be abbreviated as "::" **in only one location for the entire address.**

Applying these rules to the above address, we get the following.

- **2001:2f8::1111:2222:0:4444**

IPv6 link-local address

This is an address that is only valid within the same segment, and is in the following range.

- [Start] **FE80:0000:0000:0000:0000:0000:0000:0000**
- [End] **FE80:0000:0000:0000:FFFF:FFFF:FFFF:FFFF**

Function Details

IPv6 address settings

This product lets you specify the **IPv6 address and prefix length** for a **VLAN interface**.

As the setting method, both **fixed settings** and **automatic settings via RA (router advertisement)** are supported.

- In order to specify an IPv6 address, IPv6 functionality must be enabled for the corresponding VLAN interface.
 - To enable IPv6 functionality, use the **ipv6 enable** command.
 - When IPv6 functionality is enabled, an IPv6 link local address is automatically assigned.
- To set a fixed/automatic IPv6 address, use the **ipv6 address** command.

-
- For IPv6 addresses, **one global address and one link local address can be specified only for a single VLAN interface.**

If an IPv6 address already specified for a VLAN interface is specified for another VLAN interface, the IPv6 address for the old VLAN interface will be deleted.

The IPv6 address that can be specified for one VLAN interface can be **either the fixed or automatic setting.**

The IPv6 address that is allocated to a VLAN interface can be checked using the **show ipv6 interface** command.

Route information settings

This product refers to a routing table when sending syslog messages and when sending out voluntary IPv6 packets as an IPv6 host for NTP-based time adjustments and so on.

This product uses the following functions to perform the routing table operations.

- Set VLAN interface route information
- Set default gateway
- Show route information

Route information for VLAN interfaces

When setting an IPv6 address on this product for a VLAN interface, the correspondence between the network address and VLAN ID is automatically set as route information.

When releasing IPv6 addresses set for the VLAN interface, the above settings will be deleted.

Set default gateway

The destination for IPv6 packets sent to network addresses that are not set in the routing table can be set as the default gateway on this product.

- To set the default gateway, use the **ipv6 route** command.
- To show the default gateway, use the **show ipv6 route** command.

Show route information

- This product is provided with an FIB (Forwarding Information Base: IP forwarding table) as route information.

FIB is a database that is referenced when deciding how to forward IP packets.

Use the **show ipv6 route** command to check the FIB.

Neighbor cache table settings

When sending IPv6 packets, this product uses Neighbor Discovery Protocol to obtain the MAC addresses from the IPv6 addresses.

The correspondence between IPv6 address and MAC address is saved in the neighbor cache table with the following specifications.

- The **neighbor cache entries** saved in the neighbor cache table manage the following information.
 - IPv6 address
 - MAC address
 - VLAN interface
- **Up to 10 entries** are saved in the neighbor cache table.

If the maximum number of entries is reached and a new neighbor is found, the oldest neighbor is deleted and the new neighbor is registered.

- Dynamic entries saved in the neighbor cache table can be cleared by using the **clear ipv6 neighbors** command.
- Use the **show ipv6 neighbor** command to check the neighbor cache table.

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Function types	Operations	Operating commands
IPv6 address settings	Enable/disable IPv6 addresses	ipv6 enable/disable
	IPv6 address settings	ipv6 address
	Show IPv6 address	show ipv6 interface
	Set RA setting for IPv6 address	ipv6 address autoconfig
Route information settings	Set default gateway	ipv6 route
	Show default gateway	show ipv6 route
	Show route information	show ipv6 route
Neighbor cache settings	Show neighbor cache table	show ipv6 neighbors
	Clear neighbor cache table	clear ipv6 neighbors

Examples of Command Execution

Setting up an IPv6 network environment (fixed settings)

In this example, the IPv6 addresses are manually set on this product, and an environment is set up for accessing the unit from a remote terminal.

- The IPv6 address is set manually for the default VLAN (VLAN #1).

1. This sets 2001:db8:1::2/64 for the default VLAN (VLAN #1).

```
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ipv6 enable ①
Yamaha(config-if)#ipv6 address 2001:db8:1::2/64 ②
```

- ① Enable IPv6
- ② Specify an IPv6 address

2. Check the IPv6 address that was set.

```
Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
Interface      IP-Address      Status
Protocol
vlan1          2001:db8:1::2/64  up              up
```

```
fe80::2a0:deff:fe:2/64
```

Setting up an IPv6 network environment (automatic settings using RA)

In this example, the IPv6 addresses are automatically set on this product, and an environment is set up for accessing the unit from a remote terminal.

- The IPv6 address is set automatically by **RA** for the default VLAN (VLAN #1).

1. Specify RA for the default VLAN (VLAN #1).

```
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ipv6 enable ①
Yamaha(config-if)#ipv6 address autoconfig ②
```

① Enable IPv6

② Set up RA

2. Check the IPv6 address that was obtained from RA.

```
Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
```

Interface	IP-Address	Status
Protocol		
vlan1	2001:db8::2a0:deff:fe:2/64	up
	fe80::2a0:deff:fe:2/64	up

Points of Caution

When the IPv6 address settings are changed, all of the following commands related to remote access control will be deleted.

Use particular caution when changing the IPv6 address.

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

Related Documentation

- [L2 Switching Function: VLAN](#)
- [Remote Access Function: Remote Access Control](#)

IP Multicast Functions

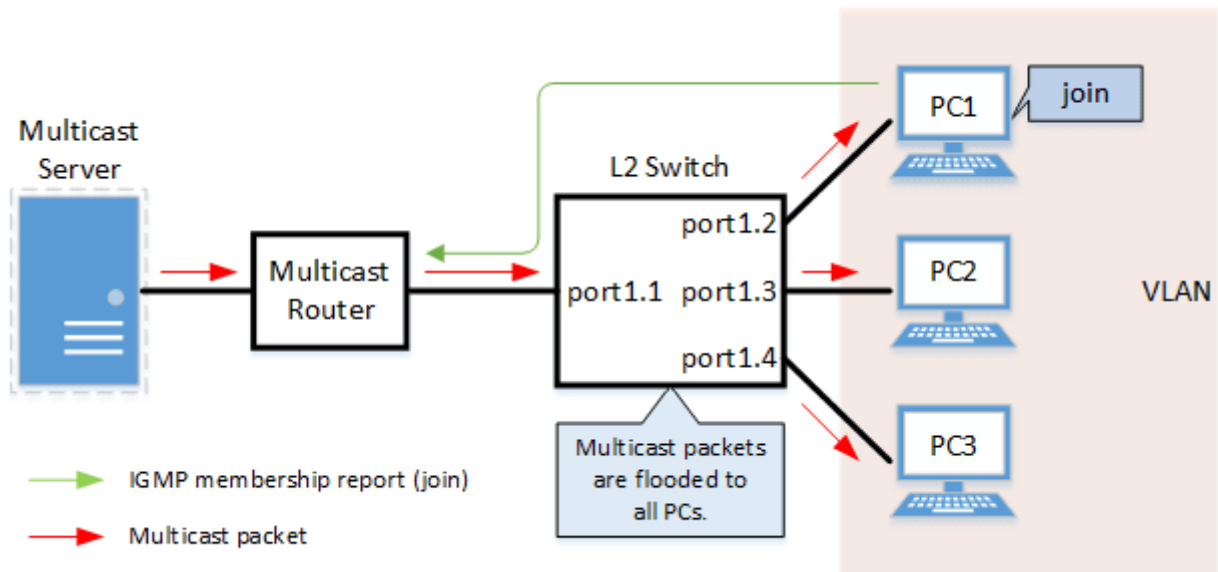
IGMP Snooping

Function Overview

IGMP snooping is a function to suppress consumption of network bandwidth in a VLAN environment, by controlling any surplus multicast flooding.

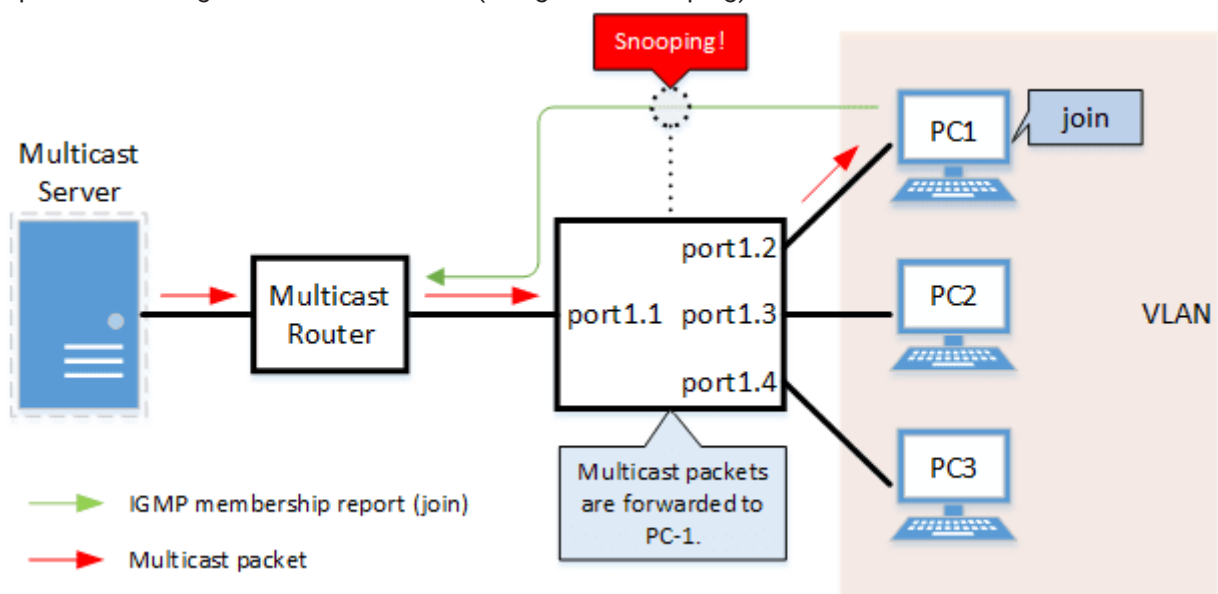
On an L2 switch, since multicast packets are distributed per VLAN, if there is even one device in the VLAN that wants to receive the multicast packet, the packet will be distributed to all ports within the same VLAN.

- Operations during multicast distribution (no IGMP snooping)



When using the IGMP snooping function, the IGMP messages exchanged between the receiving device and the multicast router are monitored (snooped), the packet from the relevant group will only be distributed to the port, to which the device that wants to receive the multicast packet is connected.

- Operations during multicast distribution (using IGMP snooping)



Definition of Terms Used

IGMP (Internet Group Management Protocol)

This is a protocol to control multicast groups.

The multicast router can determine which hosts on the LAN are members of the multicast group, and the hosts can communicate which multicast group they belong to.

There are three protocol versions, respectively defined by **IGMPv1 (RFC1112)**, **IGMPv2 (RFC2236)** and **IGMPv3 (RFC3376)**.

Multicast Router Port

This is the LAN/SFP port to which the multicast router is connected.

The LAN/SFP port that receives the IGMP general query is automatically acquired as the multicast router port.

IGMP Report Suppression Function

This is a function where the switch controls the data transmission load between the multicast router and the hosts.

The messages gathered by this product to perform control are shown below.

- IGMP reports replied to IGMP general queries by hosts, sent from the multicast router
- IGMP leave messages notified by the host

The report suppression function works with IGMPv1/v2/v3.

Fast Leave Function

If a LAN/SFP port receives an IGMPv2/v3 leave message, this function immediately disconnects the port from ports receiving multicast traffic (deletes the FDB entry necessary for transmission).

Normally, when processing IGMPv2/v3 messages, if a leave message is received, a group-specific query is transmitted to that port to confirm that the receiver exists, but if the fast leave function is **enabled**, that action is not performed.

For this reason, the fast leave function is **effective only when there is a single receiver under the control of the LAN/SFP port**.

The fast leave function operates only when an IGMPv2/v3 leave message is received.

If the fast leave function is **enabled** and the **auto-assignment** option is specified, the port to which the switch is connected under the control of the LAN/SFP port will confirm that a receiver exists when a leave message is received.

The **auto-assignment** option allows you to use the fast leave function in a cascaded switch configuration.

IGMP Query Transmission Function (IGMP Querier)

This is a function to send IGMP general and specific queries.

It is used to enable the IGMP snooping function in an environment without a multicast router.

Data Transfer Suppression Function for Multicast Router Ports

This function controls multicast data being forwarded to the multicast router port.

Normally, all multicast group data already acquired by the product is forwarded to the multicast router port, but if this function is **enabled**, then only multicast group data acquired by receiving an IGMP report via the multicast router port is forwarded.

If unnecessary multicast data flow between switches is restricting bandwidth, the problem can be mitigated by **enabling** this function in combination with the **l2-unknown-mcast discard** command.

IGMP Report Forwarding Function

This function forwards IGMP Join/Leave messages to ports to which a switch is connected under the control of the LAN/SFP port.

By enabling this function, IGMP Join/Leave messages will be forwarded to non-querier switches in a cascaded switch configuration.

When using the **data transfer suppression function for multicast router ports** in an environment where multiple multicast data flow, we recommend that this function be **enabled**.

Function Details

The operating specifications for IGMP snooping are shown below.

1. This product offers snooping functions compatible with **IGMP v1/v2/v3**.
You can use the **ip igmp snooping version** command to make later versions operate on this product.
Version settings are made for the **VLAN interface**, and initial settings are for **v3**.
The difference in operations between the configured version and received frame versions are shown in the table below.
 - If an IGMP query whose version is higher than the settings is received, the version will be lowered to the version that was configured, and the query will be forwarded.
 - If an IGMP report whose version is higher than the configured version is received, the relevant report will be discarded without being forwarded.
 - If an IGMP query and report of a lower version than the specified version is received, it is forwarded unmodified as the received version.
2. The settings to **enable/disable** IGMP snooping are made for the **VLAN interface**.
The default value is **disabled**.
3. The IGMP snooping function can handle the following six operations.
 - Multicast router port setting
 - IGMP report suppression
 - Fast leave
 - IGMP query transmission
 - Suppression of data forwarding to multicast router port
 - IGMP report forwarding
4. Although the **multicast router port** is **automatically acquired** on VLAN interfaces where IGMP snooping is set to “**enable**”, the **ip igmp snooping mrouter interface** command can also be used to make static settings.
The **show ip igmp snooping mrouter** command is used to check multicast router ports that are set for the VLAN interface.
5. The **IGMP report suppression function** is specified for VLAN interfaces using the **ip igmp snooping report-suppression** command.
The default value is **enabled**.
When transmitting an IGMP report or IGMP leave message using the report suppression function, the IPv4 address allocated to the VLAN interface will be used for the source IPv4 address.
(The address will be set and transmitted as “0.0.0.0” if it has not been allocated.)
6. The **fast leave function** is set for the VLAN interface using the **ip igmp snooping fast-leave** command.
The default value is **disabled**.
If the fast leave function is **enabled** and the **auto-assignment** option is specified, and a switch is connected under the control of the LAN/SFP port, the fast leave function is automatically **disabled** on that port.
To determine whether or not a switch is connected under the control of the LAN/SFP port, the basic management TLV “System Capabilities” of the LLDP frame received on that port is checked to see if “Bridge” is contained in the TLV.

Therefore, when using the **auto-assignment** option, enable LLDP transmission and reception on both this product and the counterpart switch. If LLDP is enabled on this product, the basic management TLV will always be sent.

7. The **IGMP query transmission function** is supported in order to allow use of IGMP snooping in environments that do not have a multicast router.

The IGMP query transmission function is controlled with the following two parameters.

- IGMP query transmission function Enable/disable
 - The **ip igmp snooping querier** command is used for VLAN interfaces.
 - The default value is **disabled**.
- IGMP query transmission interval
 - This is executed using the **ip igmp snooping query-interval** command.
 - The transmission interval can be set from 20–18,000 sec., and the default value is **125 sec.**

8. When multiple devices transmit queries within a VLAN, the query is sent by the device with the lowest IPv4 address within the VLAN.

When this product receives a query from a device whose IPv4 address is lower than its own, the query transmission function will be halted.

The source IPv4 address that is set when a query is transmitted uses the IPv4 address allocated to the VLAN interface. If an IPv4 address has not been allocated, an IPv4 address allocated to a different VLAN interface is used instead.

9. This product features a function that forces the TTL value of a received IGMP packet to change to “1” if the TTL value is invalid (a value other than “1”), instead of discarding the packet.

This is defined as the “**TTL check function**”, and it can be configured for a VLAN interface by using the **ip igmp snooping check ttl** command.

The default setting value for the **TTL check function** is **enabled (packets with invalid TTL values are discarded)**.

10. This product features a function that adds the RA (Router Alert) option to an IP header of a received IGMPv2/IGMPv3 packet that does not contain the RA option and forwards it instead of discarding.

This is defined as the “**RA check function**”, and it can be configured for a VLAN interface by using the **ip igmp snooping check ra** command.

The default value of the **RA check function** is set to **Disabled (forward packets that do not contain the RA option)**.

11. This product features a function that forces the ToS (Type of field) value of a received IGMPv3 packet to change to “0xc0” if the ToS value is invalid (a value other than “0xc0”), instead of discarding the packet.

This is defined as the “**ToS check function**”, and it can be configured for a VLAN interface by using the **ip igmp snooping check tos** command.

The default value of **ToS check function** is set to **Disabled (forward packets with invalid ToS values)**.

12. The **data transfer suppression function for multicast router ports** is specified for VLAN interfaces using the **ip igmp snooping mrouter-port data-suppression** command.

The default value is **disabled**.

13. The **IGMP report forwarding function** is specified using the **ip igmp snooping report-forward** command for VLAN interfaces.

The default value is **disabled**.

When this function is **enabled** and a switch is connected under the control of the LAN/SFP port, IGMP Join/Leave messages will be forwarded to that port.

To determine whether or not a switch is connected under the control of the LAN/SFP port, the basic management TLV “System Capabilities” of the LLDP frame received on that port is checked to see if “Bridge” is contained in the TLV.

Therefore, when using this function, enable LLDP transmission and reception on both this product and the counterpart switch. If LLDP is enabled on this product, the basic management TLV will always be sent.

Related Commands

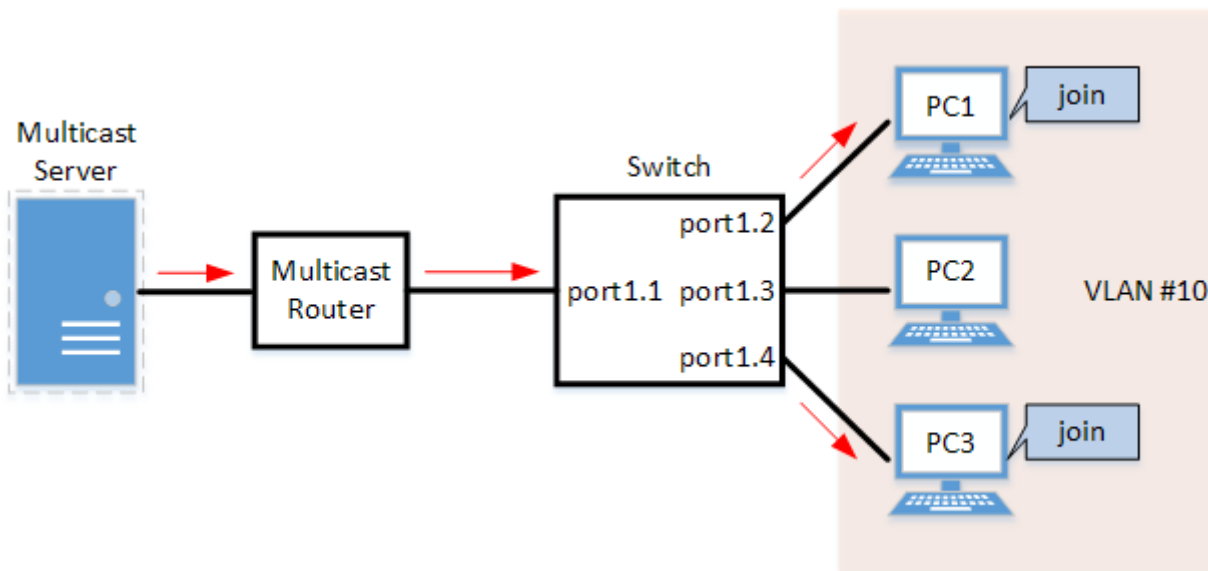
Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Enable/disable IGMP snooping	ip igmp snooping
Set IGMP snooping fast-leave	ip igmp snooping fast-leave
Multicast router port setting	ip igmp snooping mrouter interface
Set the query transmission function	ip igmp snooping querier
Set IGMP query transmission interval	ip igmp snooping query-interval
Set IGMP snooping TTL check	ip igmp snooping check ttl
Set IGMP snooping RA check	ip igmp snooping check ra
Set IGMP snooping ToS check	ip igmp snooping check tos
Set IGMP version	ip igmp snooping version
Set IGMP report suppression function	ip igmp snooping report-suppression
Set the data transfer suppression function for multicast router ports	ip igmp snooping mrouter-port data-suppression
Set IGMP report forwarding function	ip igmp snooping report-forward
Set the processing method for unknown multicast frames in the system	l2-unknown-mcast
Set forwarding of linked local multicasting addresses in the system	l2-unknown-mcast forward link-local
Set the processing method for unknown multicast frames at VLAN interfaces	l2-unknown-mcast
Set forwarding of multicasting frames at VLAN interfaces	l2-mcast flood
Show multicast router port information	show ip igmp snooping mrouter
Show IGMP multicast receiver information	show ip igmp snooping groups
Show IGMP related information for an interface	show ip igmp snooping interface
Clear IGMP group membership entries	clear ip igmp snooping

Examples of Command Execution

IGMP snooping settings (with multicast router)

In an environment with a multicast router, enable the IGMP snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Set LAN ports #1–#4 as **access ports** and **associate them with VLAN #10**.
- Since there is a multicast router, leave the **IGMP query transmission function** as “**disabled**”.
- Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
- **Enable the fast leave function**.

1. Define VLAN #10, and set IGMP snooping.

```

Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping fast-leave ④

```

① Define VLAN #10

② Enable IGMP Snooping for VLAN #10

③ Disable the IGMP query transmission function for VLAN #10

④ Enable the IGMP fast leave function for VLAN #10

- The IGMP query transmission function is disabled in default settings, so there is no need to specify those settings.

2. Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

```

Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①

```

① Configure the settings above for LAN ports #2–#4 as well.

3. Confirm the multicast router port information. (It should be connected to LAN port #1.)

```

Yamaha#show ip igmp snooping mrouter vlan10
VLAN   Interface          IP-address    Expires
-----

```

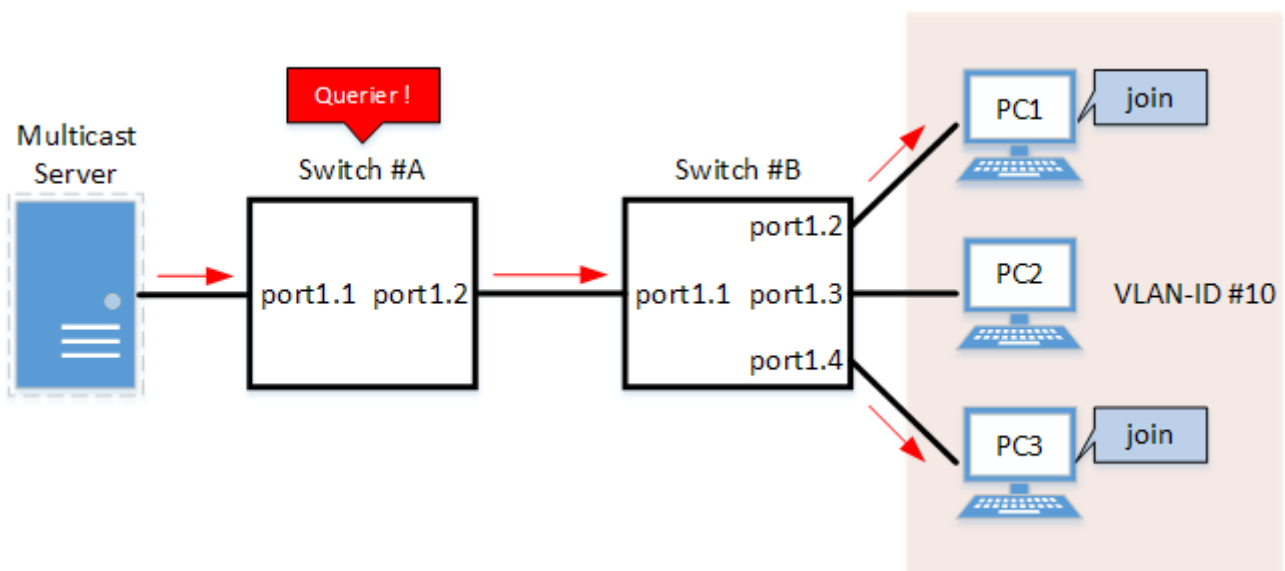
10	port1.1(dynamic)	192.168.100.216	00:00:49
----	------------------	-----------------	----------

4. Confirm the information for the multicast recipient.

```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface  Flags  Uptime    Expires   Last Reporter
Version
10     239.0.0.1                 port1.2    R      00:00:13  00:00:41  192.168.100.2
V3
10     239.0.0.1                 port1.4    R      00:00:02  00:00:48  192.168.100.4
V3
```

IGMP snooping settings (without multicast router)

In an environment without a multicast router, enable the IGMP snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Switch #A
 - Set LAN ports #1–#2 as **access ports and associate them with VLAN #10**.
 - **Enable the IGMP query transmission function.**
Set the IGMP query transmission interval to **20 sec**.
- Switch #B
 - Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
 - Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
 - **Enable the fast leave function.**
 - Since there is a device that sets invalid TTL values in IGMP packets, **disable the TTL check function**.

1. [Switch #A] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
```

```
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
```

- ① Define VLAN #10
- ② Enable IGMP Snooping for VLAN #10
- ③ Enable the IGMP query transmission function for VLAN #10
- ④ Set the IGMP query transmission interval for VLAN #10 to 20 sec.

2. [Switch #A] Set LAN ports #1–#2 as access ports, and associate them with VLAN #10.

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

- ① Configure the settings above for LAN port #2 as well.

3. [Switch #B] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#no ip igmp snooping check ttl ④
Yamaha(config-if)#ip igmp snooping fast-leave ⑤
```

- ① Define VLAN #10
- ② Enable IGMP Snooping for VLAN #10
- ③ Disable the IGMP query transmission function for VLAN #10
- ④ Disable the TTL check function for VLAN #10
- ⑤ Enable the IGMP fast leave function for VLAN #10
 - The IGMP query transmission function is disabled in default settings, so there is no need to specify those settings.

4. [Switch #B] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

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

- ① Configure the settings above for LAN ports #2–#4 as well.

5. [Switch #B] Check the multicast router port information. (It should be connected to LAN port #1.)

```
Yamaha#show ip igmp snooping mrouter vlan10
```

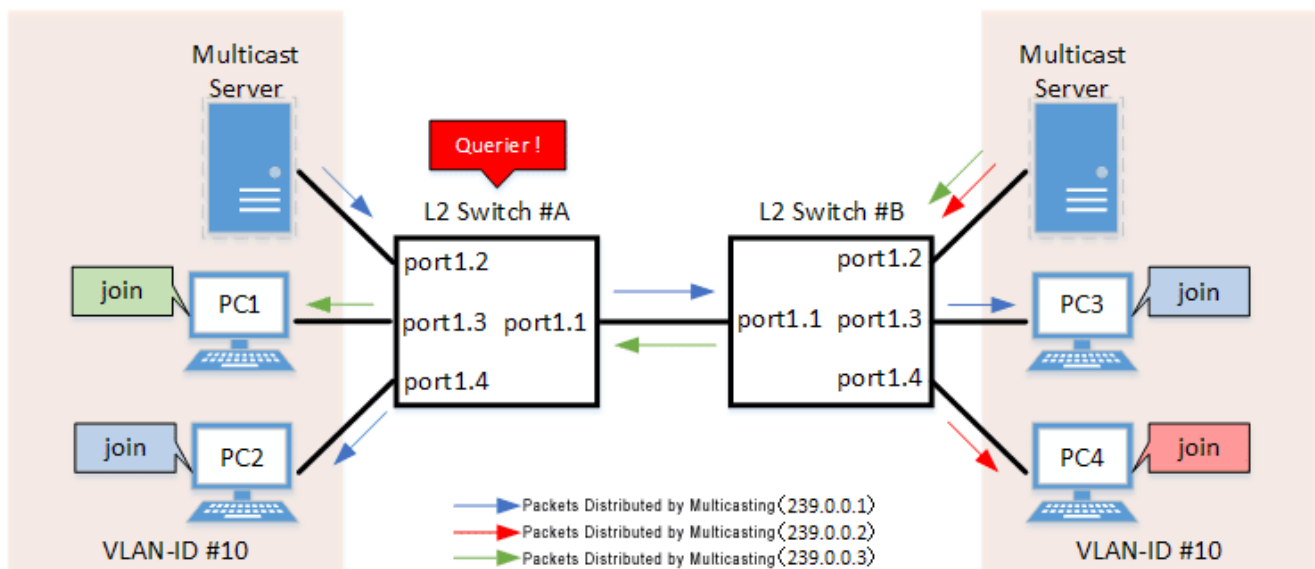

VLAN	Interface	IP-address	Expires
10	port1.1(dynamic)	192.168.100.216	00:00:49

6. [Switch #B] Check the multicast receiver information.

```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface  Flags  Uptime    Expires  Last Reporter
Version
10    239.0.0.1              port1.2    R      00:00:13  00:00:41  192.168.100.2
V3
10    239.0.0.1              port1.4    R      00:00:02  00:00:48  192.168.100.4
V3
```

IGMP snooping settings (If distributing data in both directions)

In a configuration with two switches, both switches are connected to a multicast server and computer. Each computer frequently switches between participating multicast groups to minimize the interruption time.



- Switch #A
 - Set LAN ports #1–#4 as **access ports** and **associate them with VLAN #10**.
 - **Enable the IGMP query transmission function.**
Set the IGMP query transmission interval to **20 sec**.
 - **Enable the fast leave function** and, in order to confirm the existence of multiple multicast receivers connected to the counterpart switch, **enable LLDP transmission and reception and enable the auto-assignment option**.
 - **Disable the IGMP report suppression function.**
 - Increasing the number of multicast servers or data distributions could cause port bandwidth restrictions, so **the data transfer suppression function for multicast router ports is enabled** to only forward the minimum data necessary.
Also, **unknown multicast frames are set to be discarded**.
 - To forward IGMP reports to non-queriers, **enable LLDP transmission and reception and also enable the IGMP report forwarding function**.

- Switch #B

- Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
- Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
- **Enable the fast leave function** and, in order to confirm the existence of multiple multicast receivers connected to the counterpart switch, **enable LLDP transmission and reception and enable the auto-assignment option**.
- **Disable the IGMP report suppression function**.
- Increasing the number of multicast servers or data distributions could cause port bandwidth restrictions, so **the data transfer suppression function for multicast router ports is enabled** to only forward the minimum data necessary.
Also, **unknown multicast frames are set to be discarded**.

1. [Switch #A] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
Yamaha(config-if)#ip igmp snooping fast-leave auto-assignment ⑤
Yamaha(config-if)#ip igmp snooping report-suppression disable ⑥
Yamaha(config-if)#ip igmp snooping mrouter-port data-suppression enable ⑦
Yamaha(config-if)#ip igmp snooping report-forward enable ⑧
```

- ① Define VLAN #10
- ② Enable IGMP Snooping for VLAN #10
- ③ Enable the IGMP query transmission function for VLAN #10
- ④ Set the IGMP query transmission interval for VLAN #10 to 20 sec.
- ⑤ Enable the fast leave function and auto-assignment option for VLAN #10
- ⑥ Disable the report suppression function for VLAN #10
- ⑦ Enable the data transfer suppression function for multicast router ports for VLAN #10
- ⑧ Enable the report forwarding function for VLAN #10

2. [Switch #A] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

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

- ① Configure the settings above for LAN ports #2–#4 as well.

3. [Switch #A] Discard unknown multicast frames.

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

4. [Switch #A] Enable LLDP transmission and reception on LAN port #1.

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

5. [Switch #B] Define VLAN #10, and set IGMP snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping fast-leave ④
Yamaha(config-if)#ip igmp snooping report-suppression disable ⑤
Yamaha(config-if)#ip igmp snooping mrouter-port data-suppression enable ⑥
Yamaha(config-if)#ip igmp snooping report-forward enable ⑦
```

① Define VLAN #10

② Enable IGMP Snooping for VLAN #10

③ Disable the IGMP query transmission function for VLAN #10

④ Enable the fast leave function and auto-assignment option for VLAN #10

⑤ Disable the report suppression function for VLAN #10

⑥ Enable the data transfer suppression function for multicast router ports for VLAN #10

⑦ Enable the report forwarding function for VLAN #10

- The IGMP query transmission function is disabled in default settings, so there is no need to specify those settings.

6. [Switch #B] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

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

① Configure the settings above for LAN ports #2–#4 as well.

7. [Switch #B] Discard unknown multicast frames.

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

8. [Switch #B] Enable LLDP transmission and reception on LAN port #1.

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

9. [Switch #A] Check the multicast receiver information.

```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface  Flags  Uptime    Expires  Last Reporter
Version
10    239.0.0.1              port1.1    R      00:00:02  00:00:48  192.168.100.3
V3
10    239.0.0.2              port1.1    R      00:00:02  00:00:48  192.168.100.4
V3
10    239.0.0.3              port1.3    R      00:00:04  00:00:46  192.168.100.1
V3
10    239.0.0.1              port1.4    R      00:00:03  00:00:47  192.168.100.2
V3
```

10. [Switch #B] Check the multicast router port information. (It should be connected to LAN port #1.)

```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN    Interface          IP-address    Expires
10      port1.1(dynamic)    192.168.100.240  00:00:25
```

11. [Switch #B] Check the multicast receiver information.

```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface  Flags  Uptime    Expires  Last Reporter
Version
10    239.0.0.1              port1.1    R      00:00:03  00:00:47  192.168.100.2
V3
10    239.0.0.3              port1.1    R      00:00:04  00:00:46  192.168.100.1
V3
10    239.0.0.1              port1.3    R      00:00:02  00:00:48  192.168.100.3
V3
10    239.0.0.2              port1.4    R      00:00:02  00:00:48  192.168.100.4
V3
```

Points of Caution

If you want to change the handling of unknown multicast frames, use the **I2-unknown-mcast** command.

Related Documentation

- [VLAN](#)

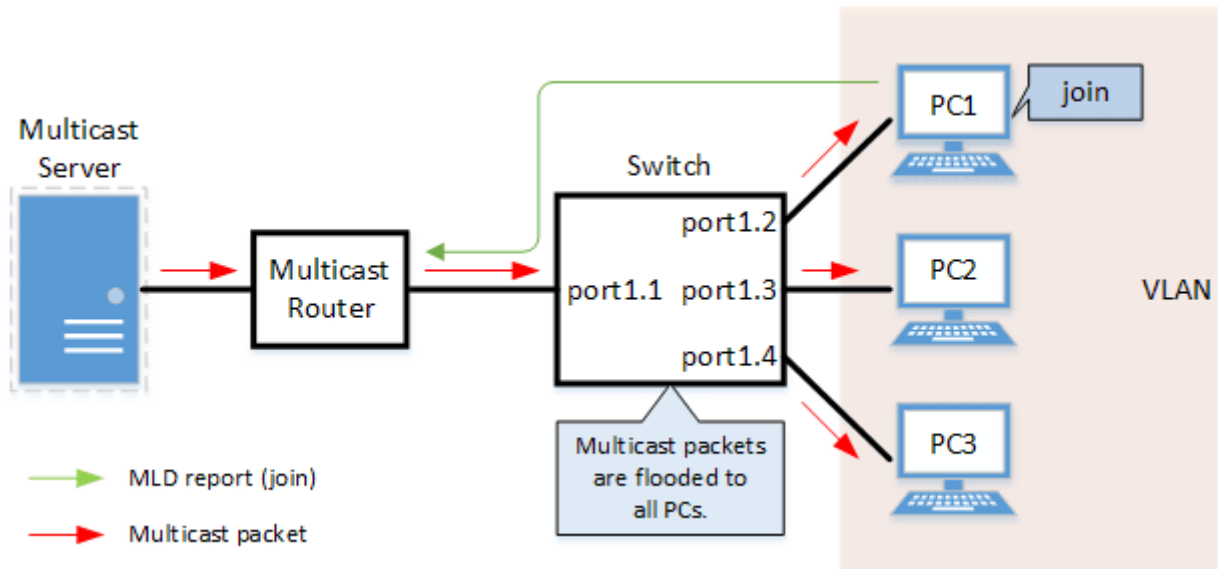
MLD Snooping

Function Overview

MLD snooping is a function to suppress consumption of network bandwidth in an IPv6 VLAN environment, by controlling any surplus multicast flooding.

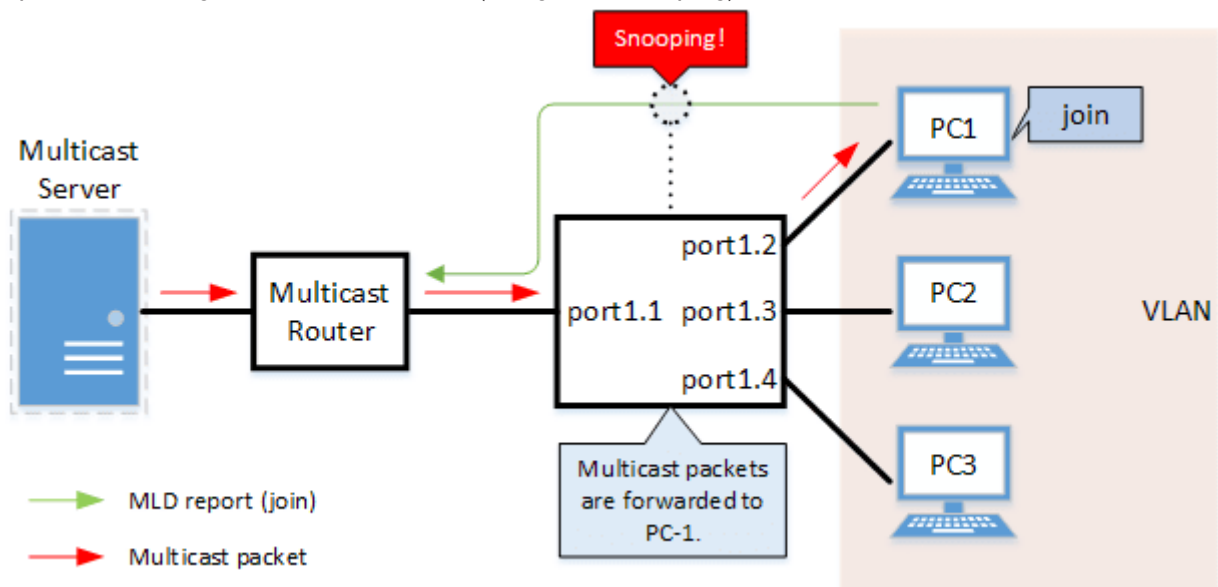
On an L2 switch, since multicast packets are distributed per VLAN, if there is even one device in the VLAN that wants to receive the multicast packet, the packet will be distributed to all ports within the same VLAN.

- Operations during multicast distribution (no MLD snooping)



When using the MLD snooping function, the MLD messages exchanged between the receiving device and the multicast router are monitored (snooped), the packet from the relevant group will only be distributed to the port, to which the device that wants to receive the multicast packet is connected.

- Operations during multicast distribution (using MLD snooping)



Definition of Terms Used

MLD (Multicast Listener Discovery)

This is a protocol to control multicast groups using IPv6 (a sub-protocol of ICMPv6).

The multicast router can determine which hosts on the LAN are members of the multicast group, and the hosts

can communicate which multicast group they belong to.
There are two protocol versions, respectively defined by **MLDv1 (RFC2710)**, and **MLDv2 (RFC3810)**.

Multicast Router Port

This is the LAN/SFP port to which the multicast router is connected.
The LAN/SFP port that receives the MLD general query is automatically acquired as the multicast router port.

MLD Report Suppression Function

This is a function where the L2 switch controls the data transmission load between the multicast router and the hosts.
The messages gathered by this product to perform control are shown below.

- MLD reports replied to MLD general queries by hosts, sent from the multicast router
- MLD Done messages notified by the host and MLD reports (Leave)

The report suppression function works with MLDv1/v2.

MLD Fast Leave Function

This function allows for the LAN/SFP port that received an MLDv1 Done and an MLDv2 report (Leave) to immediately stop receiving multicasts (deleting the necessary FDB entry).
Previously, when an MLDv1 Done message and an MLDv2 report (Leave) was received in the course of MLD leave processing, a group-specific query was sent to check for the existence of a receiver; but if the fast leave function is **enabled**, this operation is not performed.
For this reason, the fast leave function is **effective only when there is a single receiver under the control of the LAN/SFP port**.

MLD Query Transmission Function (MLD Querier)

This is a function to send MLD general and specific queries.
It is used to enable the MLD snooping function in an environment without a multicast router.

Function Details

The operating specifications for MLD snooping are shown below.

1. This product offers snooping functions compatible with **MLD v1/v2**.
You can use the **ipv6 mld snooping version** command to make later versions work on this product.
Version settings are made for the **VLAN interface**, and initial settings are for **v2**.
The difference in operations between the configured version and received frame versions are shown in the table below.
 - If an MLD query whose version is higher than the settings is received, the version will be lowered to the version that was configured, and the query will be forwarded.
 - If an MLD report whose version is higher than the configured version is received, the relevant report will be discarded without being forwarded.
2. The settings to **enable/disable** MLD snooping are made for the **VLAN interface**.
The initial setting for the default VLAN (VLAN #1) and the initial setting after a VLAN is generated are both **disabled**.
3. The MLD snooping function can handle the following four operations.
 - Multicast router port setting
 - MLD report suppression
 - MLD fast leave

- MLD query transmission
4. Although the **multicast router port** is **automatically acquired** on VLAN interfaces where MLD snooping is set to “**enable**”, the **ipv6 mld snooping mrouter interface** command can also be used to make static settings.
The **show ipv6 mld snooping mrouter** command is used to check multicast router ports that are set for the VLAN interface.
 5. The **MLD report suppression function** is specified for VLAN interfaces using the **ipv6 mld snooping report-suppression** command.
The default value is **enabled**.
When transmitting an MLD report or MLD leave message using the report suppression function, the IPv6 link local address allocated to the VLAN interface will be used for the source IPv6 address.
(The address will be set and transmitted as “::” if it has not been allocated.)
 6. The **MLD fast leave function** is set for the VLAN interface using the **ipv6 mld snooping fast-leave** command.
The initial setting for the default VLAN (VLAN #1) and the initial setting after a VLAN is generated are both **disabled**.
 7. The **MLD query transmission function** is supported in order to allow use of MLD snooping in environments that do not have a multicast router.
The MLD query transmission function controls the following two parameters.
 - MLD query transmission function Enable/disable
 - The **ipv6 mld snooping querier** command is used for VLAN interfaces.
 - The initial setting for the default VLAN (VLAN #1) and the initial setting after a VLAN is generated are both **disabled**.
 - MLD query transmission interval
 - This is set using the **ipv6 mld snooping query-interval** command.
 - The transmission interval can be set from 20–18,000 sec., and the default value is **125 sec.**
 8. When multiple devices transmit queries within a VLAN, the query is sent by the device with the lowest IPv6 address within the VLAN.
When this product receives a query from a device whose IPv6 address is lower than its own, the query transmission function will be halted.
The source IPv6 address that is set when a query is transmitted uses the IPv6 link local address allocated to the VLAN interface. If an IPv6 link local address has not been allocated, an IPv6 link local address allocated to a different VLAN interface is used instead.
(If no IPv6 link local addresses have been allocated to any VLAN interfaces, the query is not transmitted.)
 9. In this product, if the Hop Limit of a received MLD packet is invalid (other than 1), the MLD packet will be discarded.
 10. In this product, if a received MLD packet does not contain the Router Alert option, the MLD packet will be discarded.

Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

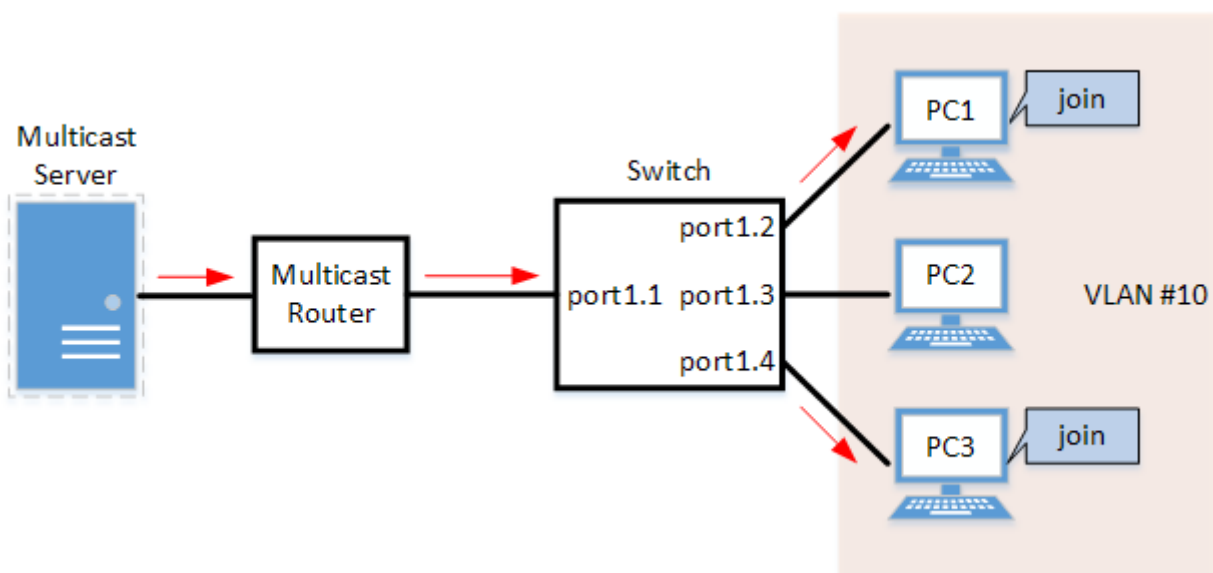
Operations	Operating commands
Enable/disable MLD snooping	ipv6 mld snooping
Set MLD snooping fast-leave	ipv6 mld snooping fast-leave
Multicast router port setting	ipv6 mld snooping mrouter interface

Operations	Operating commands
Set the query transmission function	ipv6 mld snooping querier
Set the MLD query transmission interval	ipv6 mld snooping query-interval
Set the MLD version	ipv6 mld snooping version
Set the MLD report suppression function	ipv6 mld snooping report-suppression
Show multicast router port information	show ipv6 mld snooping mrouter
Show MLD multicast recipient information	show ipv6 mld snooping groups
Show MLD related information for an interface	show ipv6 mld snooping interface
Clear the MLD group membership entries	clear ipv6 mld snooping

Examples of Command Execution

MLD snooping settings (with multicast router)

In an environment with a multicast router, enable the MLD snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Set LAN ports #1–#4 as **access ports** and **associate them with VLAN #10**.
- Since there is a multicast router, leave the **MLD query transmission function** as “disabled”.
- Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
- **Enable the MLD fast leave function**.

■ Setting Procedure

1. Define VLAN #10, and set MLD snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
```



```
Yamaha(config-if)#no ipv6 mld snooping querier ④  
Yamaha(config-if)#ipv6 mld snooping fast-leave ⑤
```

- ① Define VLAN #10
- ② Enable the IPv6 function for VLAN #10
- ③ Enable MLD Snooping for VLAN #10
- ④ Disable the MLD query transmission function for VLAN #10
- ⑤ Enable the MLD fast leave function for VLAN #10

。 The MLD query transmission function is disabled in default settings, so there is no need to specify those settings.

2. Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

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

- ① Configure the settings above for LAN ports #2–#4 as well.

3. Confirm the multicast router port information. (It should be connected to LAN port #1.)

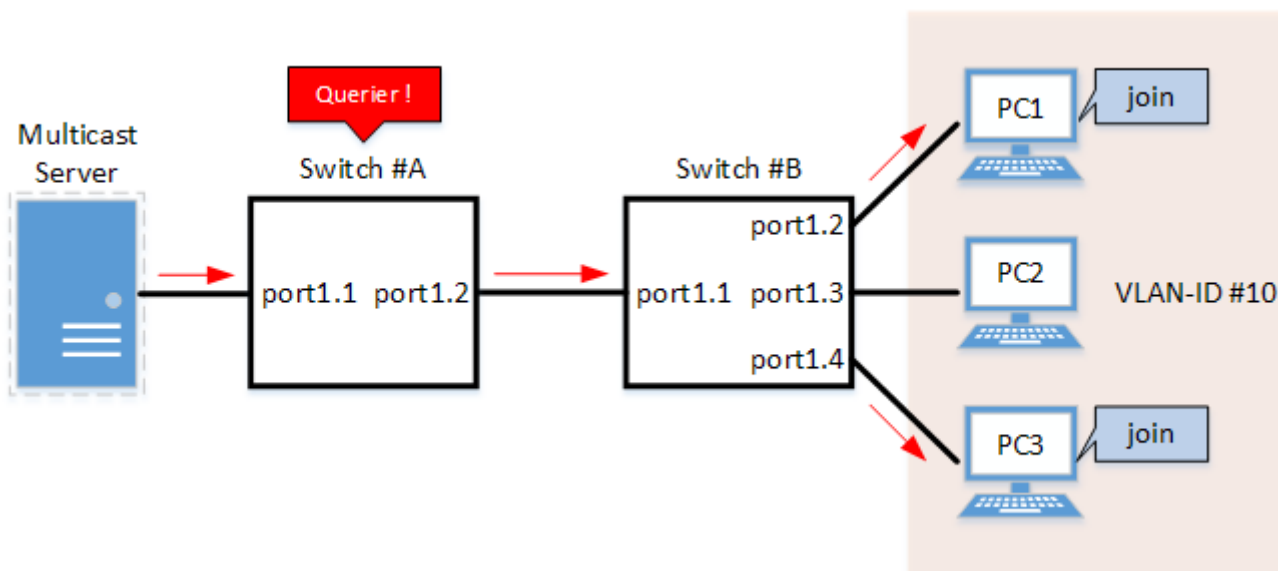
```
Yamaha#show ipv6 mld snooping mrouter vlan10  
VLAN    Interface          IP-address    Expires  
10      port1.1(dynamic)    fe80::2a0:deff:feae:b879    00:00:43
```

4. Confirm the information for the multicast recipient.

```
Yamaha#show ipv6 mld snooping groups  
MLD Connected Group Membership  
Vlan  Group Address          Interface      Uptime  Expires  
Last Reporter  
10    ff15::1                  port1.2       00:00:13 00:00:41  
fe80::a00:27ff:fe8b:87e2  
10    ff15::1                  port1.4       00:00:02 00:00:48  
fe80::a00:27ff:fe8b:87e4
```

MLD snooping settings (without multicast router)

In an environment without a multicast router, enable the MLD snooping function and join a multicast group. Data is distributed only to PC1 and PC3.



- Switch #A
 - Set LAN ports #1–#2 as **access ports and associate them with VLAN #10**.
 - **Enable the MLD query transmission function.**
Set the MLD query transmission interval to * 20 sec*.
- Switch #B
 - Set LAN ports #1–#4 as **access ports and associate them with VLAN #10**.
 - Set **multicast router port** acquisition to **automatic acquisition** only. (A static setting is not used.)
 - **Enable the MLD fast leave function.**

1. [Switch #A] Define VLAN #10, and set MLD snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping query-interval 20 ⑤
```

- ① Define VLAN #10
- ② Enable the IPv6 function for VLAN #10
- ③ Enable MLD Snooping for VLAN #10
- ④ Enable the MLD query transmission function for VLAN #10
- ⑤ Set the MLD query transmission interval for VLAN #10 to 20 sec.

2. [Switch #A] Set LAN ports #1–#2 as access ports, and associate them with VLAN #10.

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

① Configure the settings above for LAN port #2 as well.

3. [Switch #B] Define VLAN #10, and set MLD snooping.

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#no ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping fast-leave ⑤
```

① Define VLAN #10

② Enable the IPv6 function for VLAN #10

③ Enable MLD Snooping for VLAN #10

④ Disable the MLD query transmission function for VLAN #10

⑤ Enable the MLD fast leave function for VLAN #10

。 The MLD query transmission function is disabled in default settings, so there is no need to specify those settings.

4. [Switch #B] Set LAN ports #1–#4 as access ports, and associate them with VLAN #10.

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

① Configure the settings above for LAN ports #2–#4 as well.

5. [Switch #B] Check the multicast router port information. (It should be connected to LAN port #1.)

```
Yamaha#show ipv6 mld snooping mrouter vlan10
VLAN    Interface          IP-address    Expires
10      port1.1(dynamic)   fe80::2a0:deff:feae:b879    00:00:43
```

6. [Switch #B] Check the multicast receiver information.

```
Yamaha#show ipv6 mld snooping groups
MLD Connected Group Membership
Vlan    Group Address          Interface      Uptime    Expires
Last Reporter
10      ff15::1                port1.2       00:00:13  00:00:41
fe80::a00:27ff:fe8b:87e2
10      ff15::1                port1.4       00:00:02  00:00:48
fe80::a00:27ff:fe8b:87e4
```

Points of Caution

If you want to change the handling of unknown multicast frames, use the **l2-unknown-mcast** command.

Related Documentation

- [VLAN](#)
- [Basic IPv6 Settings](#)

Traffic Control Functions

ACL

Function Overview

The access list (ACL) is a conditional statement that determines whether to permit or to deny the frame. If the access list is applied to the interface, the permitted frames and frames not matching the conditions will be transferred, and the denied frames will be discarded.

As this allows for only specified frames to be selected for transfer, this feature is primarily used for security purposes.

This product supports three access list types, as shown in the table below.

- Access list type

Access list type	Deciding criteria	Access list ID	Purpose of use
IPv4 access list	Source IPv4 address	1–2000	Filters access from specific hosts and networks.
IPv6 access list	Source IPv6 address	3001–4000	Filters access from specific hosts and networks.
MAC access list	Source MAC address	2001–3000	Filters access from specific devices.

Definition of Terms Used

ACL

Abbreviation of “**Access Control List**”.

Wildcard mask

Information that specifies which portion of the specified IPv4 address or MAC address is read. This is **used when specifying a range of IPv4 addresses or MAC addresses** as ACL conditions.

- When the wildcard mask bit is “**0**”: check the corresponding bit
- When the wildcard mask bit is “**1**”: do not check the corresponding bit

Examples of settings using wildcard masks are shown below. (The underlined portion is the wildcard mask.)

- To specify conditions for subnet **192.168.1.0/24**: **192.168.1.0 0.0.0.255** (specified in decimal)
- To specify conditions for vendor code **00-A0-DE---**: **00A0.DE00.0000 0000.00FF.FFFF** (specified in hexadecimal)

Function Details

Generate access list

A **maximum of 28** access lists can be created for each of the following types: IPv4 access lists, IPv6 access lists, and MAC access lists.

A **maximum of 128** control conditions can be registered per access list.

If the registered control conditions are not satisfied, forwarding occurs as usual.

Applying to the interface

The following table shows how access lists are applied to the interfaces of this product. Note that only **one** access list can be applied to an interface.

Access list type	LAN port		VLAN interface		Logical interface	
	in	out	in	out	in	out
IPv4 access list	Yes	No	No	No	No	No
IPv6 access list	Yes	No	No	No	No	No
MAC access list	Yes	No	No	No	No	No

The number of access lists that can be applied to the interface depends on the number of control parameters that are registered in the access lists.

The maximum number of control conditions that can be used in the entire system is **896 for IPv4 and MAC combined, and 384 for IPv6**.

Applying an access list to the interface will use resources **“equivalent to the number of control conditions that are registered in the access list”**.

LAN port settings

The steps for applying access lists to LAN ports are shown below.

1. Decide on the filtering parameters, and generate the access list.
 - Add a name if necessary.
2. Check the access list.
3. Apply the access list to the LAN port.
4. Check the applied access list.

A list of operation commands is given below.

- Access list operation commands

Access list type	Generate access list	Check access list	Apply access list	Check applied access list
IPv4 access list	access-list	show access-list	access-group	show access-group
IPv6 access list	access-list	show access-list	access-group	show access-group
MAC access list	access-list	show access-list	access-group	show access-group

Related Commands

Related commands are indicated below.

For details on the commands, refer to the Command Reference.

Operations	Operating commands
Generate IPv4 access list	access-list
Add comment to IPv4 access list	access-list description
Apply IPv4 access list	access-group
Generate IPv6 access list	access-list
Add comment to IPv6 access list	access-list description
Apply IPv6 access list	access-group

Operations	Operating commands
Generate MAC access list	access-list
Add comment to MAC access list	access-list description
Apply MAC access list	access-group
Show generated access list	show access-list
Show access list applied to interface	show access-group

Examples of Command Execution

IPv4 access list settings

■ Specify host

Set **LAN port #1** so that it only allows access from host: **192.168.1.1**.
The access list ID to be used is **#123**, and the access list name **IPV4-ACL-EX** is added.

1. Generate and confirm **access list #123**.

```
Yamaha(config)#access-list 123 permit host 192.168.1.1 ①
Yamaha(config)#access-list 123 deny any
Yamaha(config)#access-list 123 description IPV4-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ③
IPv4 access list 123
  10 permit host 192.168.1.1
  20 deny any
Yamaha#
```

- ① Generate access list
- ② Name access list
- ③ Check access list

2. Apply **access list #123** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv4 access group 123 in
```

- ① Apply access list
- ② Check access list settings

■ Specify network

Set **LAN port #1** so that it only allows access from network: **192.168.1.0/24**.
The access list ID to be used is **#123**, and the access list name **IPV4-ACL-EX** is added.

1. Generate and confirm **access list #123**.

```
Yamaha(config)#access-list 123 permit 192.168.1.0 0.0.0.255 ①
Yamaha(config)#access-list 123 deny any
Yamaha(config)#access-list 123 description IPV4-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show ip access-list ③
IPv4 access list 123
  10 permit 192.168.1.0/24
  20 deny any
Yamaha#
```

- ① Generate access list
- ② Name access list
- ③ Check ACL

2. Apply **access list #123** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv4 access group 123 in
```

- ① Apply access list
- ② Check access list settings

IPv6 access list settings

■ Specify host

Set **LAN port #1** so that it only allows access from host: **2001:db8::1**.
The access list ID to be used is **#3001**, and the access list name is **IPV6-ACL-EX**.

1. Generate and confirm **access list #3001**.

```
Yamaha(config)#access-list 3001 permit 2001:db8::1/128 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#access-list 3001 description IPV6-ACL-EX ②
Yamaha(config)#end

Yamaha# show access-list 3001 ③
IPv6 access list 3001
  10 permit 2001:db8::1/128
  20 deny any
```

- ① Generate access list
- ② Name access list
- ③ Check access list

2. Apply **access list #3001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 3000 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv6 access group 3001 in
```

- ① Apply access list
- ② Check access list settings

■ Specify network

Set **LAN port #1** so that it only allows access from network: **2001:db8::/64**.
The access list ID to be used is **#3001**, and the access list name is **IPV6-ACL-EX**.

1. Generate and confirm **access list #3001**.

```
Yamaha(config)#access-list 3001 permit 2001:db8::/64 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#access-list 3001 description IPV6-ACL-EX ②
Yamaha(config)#end

Yamaha# show access-list 3001 ③
IPv6 access list 3001
  10 permit 2001:db8::/64
  20 deny any
```

- ① Generate access list
- ② Name access list
- ③ Check access list

2. Apply **access list #3001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 3001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv6 access group 3001 in
```

- ① Apply access list
- ② Check access list settings

MAC access list settings

■ Specify host

Set **LAN port #1** so that it only denies access from host: **00-A0-DE-12-34-56** and allows all others.
ID **#2001** and the access list name **MAC-ACL-EX** are added for the access list used.

1. Generate and confirm **access list #2001**.

```
Yamaha(config)#access-list 2001 deny host 00a0.de12.3456 ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 2001 ③
MAC access list 2001
  10 deny host 00A0.DE12.3456
```

- ① Generate access list
- ② Set access list name
- ③ Check access list

2. Apply **access list #2001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 2001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : MAC access group 2001 in
```

- ① Apply access list
- ② Check access list settings

■ **Specify vendor**

Set **LAN port #1** so that it only denies access from vendor code: **00-A0-DE---*** (00-A0-DE-00-00-00 to 00-A0-DE-FF-FF-FF) and allows all others.

ID **#2001** and the access list name **MAC-ACL-EX** are added for the access list used.

1. Generate and confirm **access list #2001**.

```
Yamaha(config)#access-list 2001 deny 00a0.de00.0000 0000.00ff.ffff ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 2001 ③
MAC access list 2001
  10 deny 00A0.DE00.0000 0000.00FF.FFFF
```

- ① Generate access list
- ② Set access list name
- ③ Check access list

2. Apply **access list #2001** to **LAN port #1**.

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 2001 in ①
Yamaha(config-if)#end
Yamaha#
```

```
Yamaha#show access-group ②  
Interface port1.1 : MAC access group 2001 in
```

- ① Apply access list
- ② Check access list settings

Points of Caution

- If access lists are applied to LAN ports belonging to a logical interface, the settings applied to the port with the lowest port number of the logical interface will also be applied to the other ports belonging to that logical interface.

Related Documentation

- [L2 switching functions: VLAN](#)

Function Overview

QoS (Quality of Service) is a technology for reserving a specified bandwidth for communications over a network, guaranteeing a fixed speed of communication. Application data is classified and grouped, and then forwarded by group priority level, referring to the DSCP in the IP header or the CoS in the IEEE802.1Q tag.

Definition of Terms Used

CoS (IEEE 802.1p Class of Service)

This expresses priority as a 3-bit field in the VLAN tag header, with a value from 0–7. Also called 802.1p user priority.

IP Precedence

This expresses priority as a 3-bit field in the TOS field of the IP header, with a value from 0–7. Used to indicate the traffic class of the frame in question, for the device that receives the frame.

DSCP (Diffserv Code Point)

This expresses priority as a 6-bit field in the TOS field of the IP header, with a value from 0–63. Since DSCP uses the same TOS field as IP precedence, it is compatible with IP-Precedence. Used to indicate the traffic class of the frame in question, for the device that receives the frame.

Default CoS

This is the CoS value that is assigned to an untagged frame for the purpose of internal processing.

Transmission queue

This product has eight transmission queues per port. The transmission queues are numbered from ID 0–7, with larger ID numbers being given higher priority.

Trust mode

This indicates what will be the basis for deciding (trusting) the transmission queue ID. This product can use the CoS value or DSCP value of the received frame to allocate the transmission queues. The setting can be configured on a per-LAN/SFP port basis, and the default status (when QoS is enabled) is set to CoS.

Transmission queue ID conversion table

This is a conversion table used when deciding on the transmission queue ID from either the CoS value or the DSCP value. There are two kinds of transmission queue ID conversion tables, the CoS-transmission queue ID conversion table and the DSCP-transmission queue ID conversion table. Each kind is used with its own trust mode. Mapping can be freely changed by the user.

Port priority

This is the priority order assigned for each reception port. If the trust mode is “port priority,” frames received at that port are placed in the transmission queue according to the port’s priority setting.

Function Details

Enabling or disabling QoS control

When shipped from the factory, the QoS control of this product is set to **disable**.

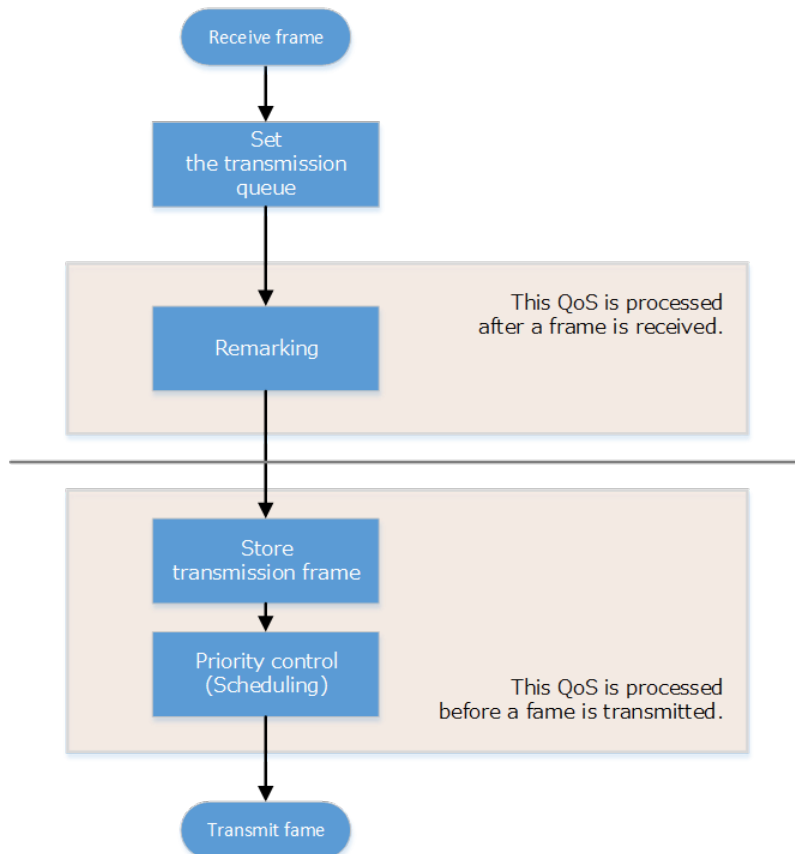
To enable QoS control, use the **qos enable** command. To disable this, use the **no qos** command.

Most QoS control commands cannot be executed if QoS is not enabled.

The QoS function status can be checked using the **show qos** command.

QoS processing flow

The QoS processing flow is shown below.



Transmission queue assignments

When this product receives a frame, it determines the initial value of the transmission queue ID according to the **CoS value or DSCP value** within the frame and the **port priority** of the reception port.

Of the factors such as the frame's CoS value and DSCP value, the port's **trust mode** determines which factor will be the basis for determining the transmission queue.

The **trust mode** can be changed by the **qos trust** command. The default value (when QoS is enabled) is set to **CoS**.

The transmission queue is assigned per **trust mode**, using the following rules.

- When trust mode is "CoS"
 - When the received frame is a frame with a VLAN tag, the CoS value within the tag is used to determine the transmission queue ID.
 - When the received frame is a frame without a VLAN tag, the **default CoS** that is managed by this product is used to determine the transmission queue ID.
The default setting (when QoS is enabled) and the **default CoS** are set to **"0"**. The setting can be

changed using the **qos cos** command.

- Conversion from the CoS value to the transmission queue ID is performed by the CoS-transmission queue ID conversion table.
One such table is maintained by the system, and with the default settings (when QoS is enabled), the settings are as follows. The setting can be changed using the **qos cos-queue** command.

CoS value	Transmission queue ID	Traffic Type
0	2	Best Effort
1	0	Background
2	1	Standard(spare)
3	3	Excellent Effort(Business Critical)
4	4	Controlled Load(Streaming Multimedia)
5	5	Video(Interactive Media) less than 100 msec latency and jitter
6	6	Voice(Interactive Media) less than 10 msec latency and jitter
7	7	Network Control(Reserved Traffic)

- When trust mode is "DSCP"

- The DSCP value in the IP header is used to determine the transmission queue ID.
- Conversion from the DSCP value to the transmission queue ID is performed by the DSCP-transmission queue ID conversion table.
One such table is maintained by the system, and with the default settings (when QoS is enabled), the settings are as follows. The setting can be changed using the **qos dscp-queue** command.

DSCP value	Transmission queue ID	Traffic Type
0 - 7	2	Best Effort
8 - 15	0	Background
16 - 23	1	Standard(spare)
24 - 31	3	Excellent Effort(Business Critical)
32 - 39	4	Controlled Load(Streaming Multimedia)
40 - 47	5	Video(Interactive Media) less than 100 msec latency and jitter
48 - 55	6	Voice(Interactive Media) less than 10 msec latency and jitter
56 - 63	7	Network Control(Reserved Traffic)

- When trust mode is "port priority"

- The transmission queue ID is determined by the **port priority**.
- By default (when QoS is enabled), **port priority** is set to **2**. The setting can be changed using the **qos port-priority-queue** command.

Remark

The CoS value or DSCP value of the received frame is rewritten on a per-port basis.

Use this function to control the priority of frames received on a specific port. Since remarking is performed before the transmission queue is reassigned, the CoS value or DSCP value after remarking is also used for priority control of this product. If the trust mode is "port priority," the transmission queue ID cannot be changed by the remarking.

Storing in the transmission queue

Frames are stored in the transmission queue that is finally determined through a series of QoS processing. In order to resolve transmission queue congestion, this product provides a system to select and discard frames.

- This product uses the **tail drop** method to resolve overflow in the transmission queue. Frames discarded by tail drop are counted by the frame counter.
- It is not possible to change the threshold value for tail drop.
- Each port shares the packet buffer, and the proportion of the packet buffer that can be used by the transmission queue on each port fluctuates depending on the usage status of the packet buffer.
- You can use the **show qos queue-counters** command to check how much packet buffer is used by each transmission queue.
- The usage of the transmission queue can be checked using the **show qos queue-counters** command.
- The number of packets discarded by tail drop can be checked using the **show interface, show frame-counter** command.

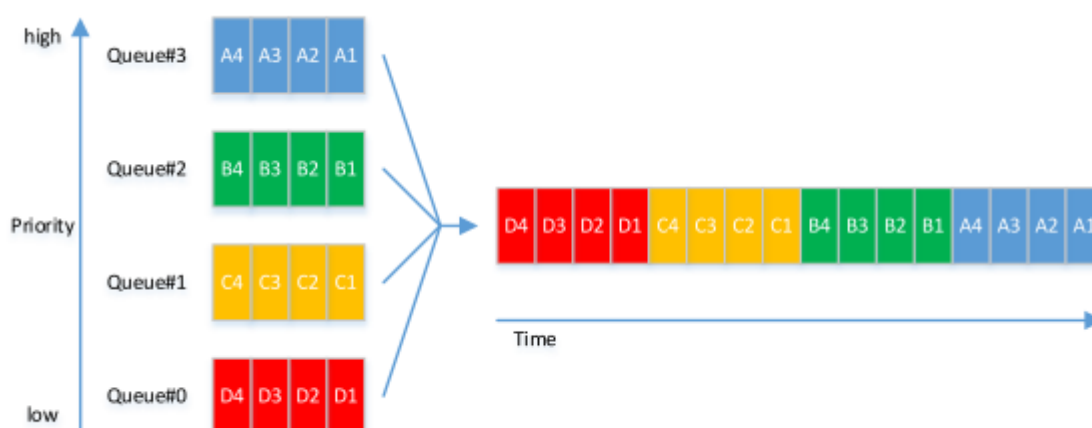
Scheduling

Scheduling is used to determine what rules are used to send out the frames that are stored in the transmission queue.

Appropriate control of the scheduling along with the system to control congestion will help ensure QoS. (Inappropriate scheduling will result in degradation of QoS.)

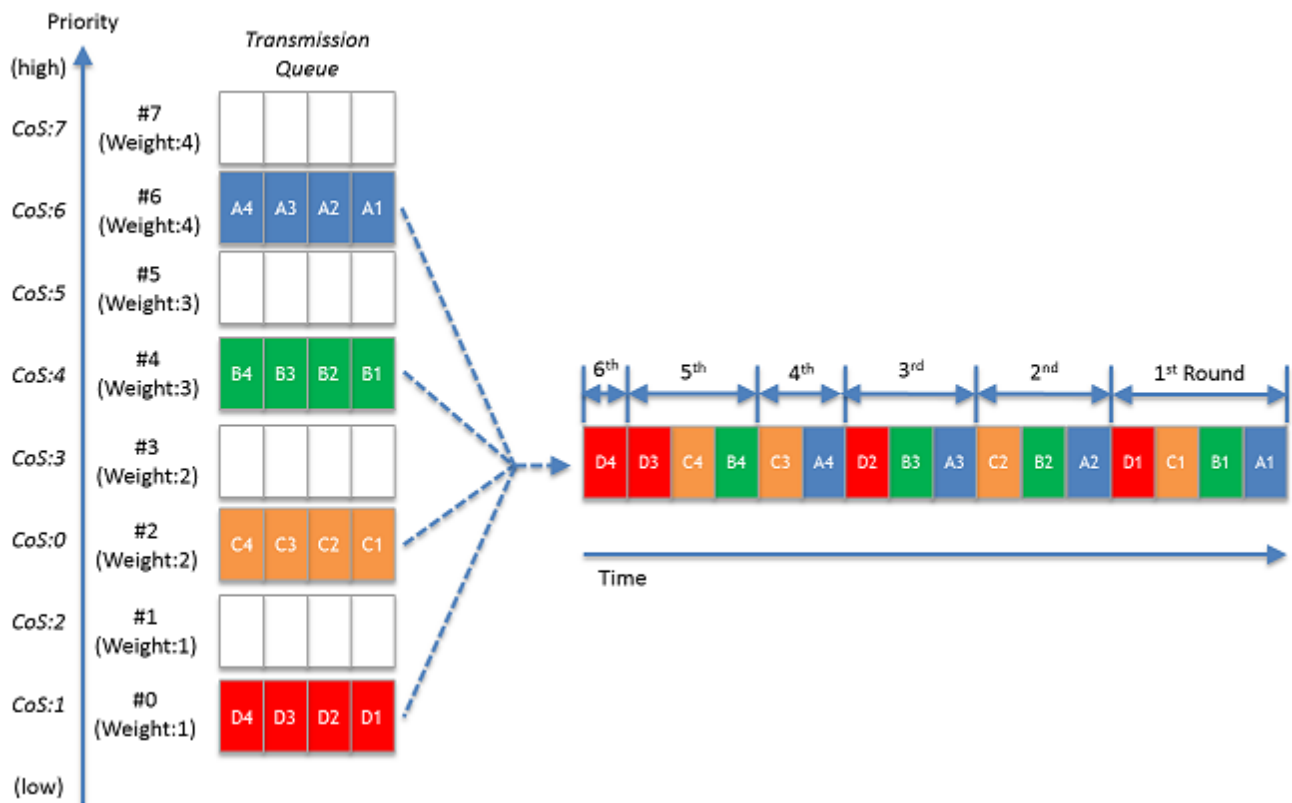
This product supports two types of scheduling for the transmission queue, the **strict priority system (SP)** and the **weighted round-robin (WRR)** system.

- Strict priority system (SP: Strict Priority) The higher the queue priority, the higher the transmission priority. When a frame is stored in a high-priority queue, it can never be transmitted from a lower-priority queue.



- Weighted round-robin system (WRR: Weighted Round Robin)
Each queue is assigned a **weight** and transmits frames accordingly. Frames can also be transmitted from a lower-priority queue, within a specified percentage. **Weights** are determined according to the table below.
- Weight of each transmission queue

Transmission queue ID	Weight	Ratio
7 (highest priority)	4	20%
6	4	20%
5	3	15%
4	3	15%
3	2	10%
2	2	10%
1	1	5%
0 (lowest priority)	1	5%



The transmission queue settings are made for the entire system, not for each interface.

To configure the scheduling setting, use the **qos scheduling** command.

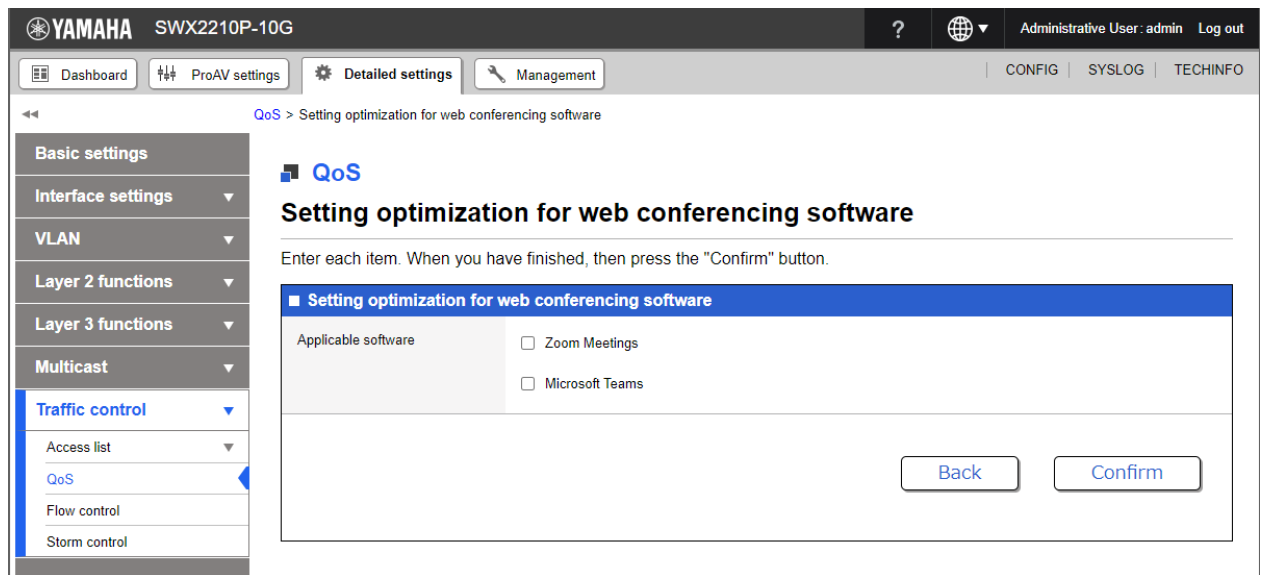
By default (when QoS is enabled), the scheduling setting is "WRR."

Optimizing web conference application settings

QoS settings for web conference application software can be configured easily via the Web GUI.

By merely using simple operations to select the web conference application to use, communication can be prioritized for that web conference application, such as Zoom Meetings or Microsoft Teams.

- * Page for optimizing web conference application settings



Optimizing web conference application settings involves configuring the following settings.

- Enable QoS.
- Set the trust mode for all ports to DSCP.
- Assign the DSCP value for the web conference application to be optimized to a high-priority sending queue. The DSCP values used for web conference applications are indicated below.
To use the web conference application settings to change the DSCP value used by the web conference application to a non-default value, use the **qos dscp-queue** command to change the link between the DSCP value and sending queue.
 - Zoom Meetings
 - 56 (Audio)
 - 40 (Video/Screen sharing)
 - Microsoft Teams
 - 46 (Audio)
 - 34 (Video)
 - 18 (Application/Screen sharing)
- Assign the DSCP value not used by the web conference application being optimized to the lowest-priority sending queue.
- Change the scheduling mode for all sending queues to the absolute priority method.

This web conference application setting optimization function includes functionality for configuring QoS settings for individual switches. To fully maximize the benefits of QoS settings, they must be configured for the entire network, including the router, at the same time.

If the DSCP value for the web conference application was changed to a non-default value, also change the DSCP sending queue assignment settings separately.

Separate table 1: Standard PHB (RFC recommended value)

PHB	DSCP value	RFC
Default	0	RFC2474

PHB		DSCP value	RFC
CS (Class Selector)	CS0	0	RFC2474
	CS1	8	
	CS2	16	
	CS3	24	
	CS4	32	
	CS5	40	
	CS6	48	
	CS7	56	
AF (Assured Forwarding)	AF11	10	RFC2597
	AF12	12	
	AF13	14	
	AF21	18	
	AF22	20	
	AF23	22	
	AF31	26	
	AF32	28	
	AF33	30	
	AF41	34	
	AF42	36	
	AF43	38	
EF (Expedited Forwarding)		46	RFC2598

Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Enabling or disabling QoS control	qos enable
Set default CoS	qos cos
Change trust mode	qos trust
Set CoS-transmission queue ID conversion table	qos cos-queue
Set DSCP-transmission queue ID conversion table	qos dscp-queue
Set port priority order	qos port-priority-queue
Set scheduling method	qos scheduling

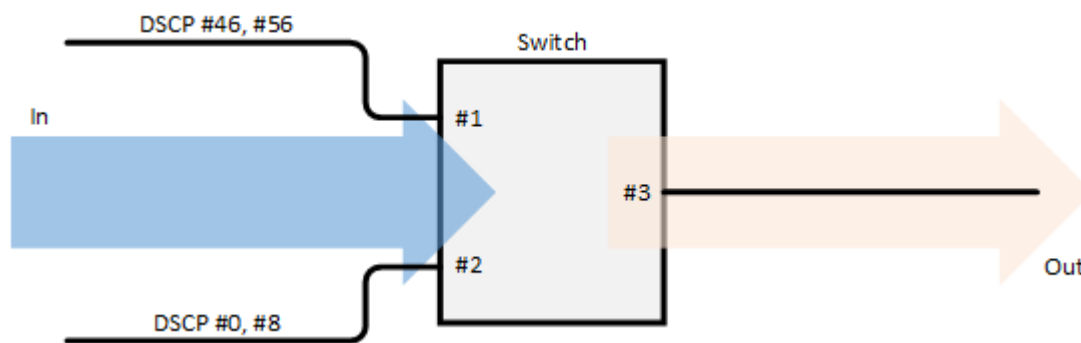
Operations	Operating commands
Show status of QoS function setting	show qos
Show QoS information for LAN/SFP port	show qos interface
Show egress queue usage ratio	show qos queue-counters
Set remarking	remark

Examples of Command Execution

Priority control (SP) using DSCP values

This example allocates the transmission queue based on the DSCP value of the frame, for priority control (SP). The SP priority control gives priority on the processing of frames with large DSCP values from LAN port #3.

* DSCP priority control: setting example



1. Enable QoS and set the trust mode for the reception ports (LAN ports #1 and #2).

```
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust dscp ③
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ④
Yamaha(config-if)#qos trust dscp ⑤
Yamaha(config-if)#exit
```

- ① Enable QoS
- ② Setting for LAN port #1
- ③ Change the trust mode to DSCP
- ④ Setting for LAN port #2
- ⑤ Change the trust mode to DSCP

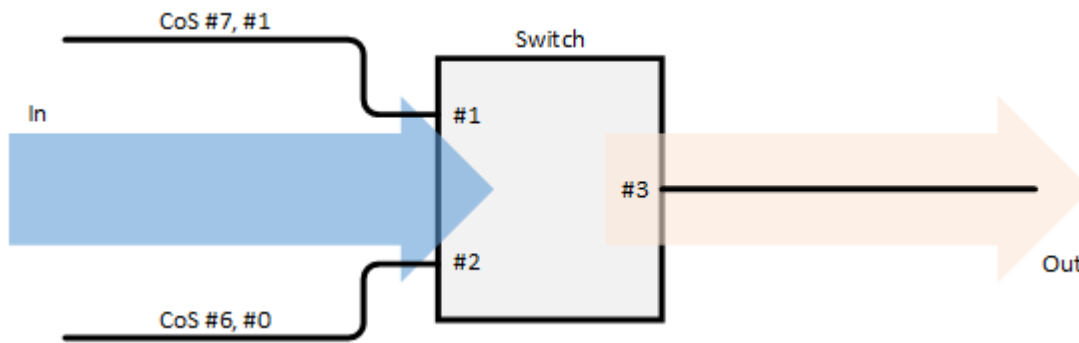
2. Set the scheduling method.

```
Yamaha(config)# qos scheduling sp
```

Priority control (WRR) using CoS values

This example allocates the transmission queue based on the CoS value of the frame, for priority control (WRR).

- Priority control using CoS values: setting example



1. Enable QoS and set the trust mode for the reception ports (LAN ports #1 and #2).

```
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust cos ③
Yamaha(config-if)#qos cos 2 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust cos ⑥
Yamaha(config-if)#qos cos 2 ⑦
Yamaha(config-if)#exit
```

- ① Enable QoS
- ② Setting for LAN port #1
- ③ Change the trust mode to CoS
- ④ Treat untagged frames as if they were received with a CoS value of 2
- ⑤ Setting for LAN port #2
- ⑥ Change the trust mode to CoS
- ⑦ Treat untagged frames as if they were received with a CoS value of 2

2. Set the scheduling method.

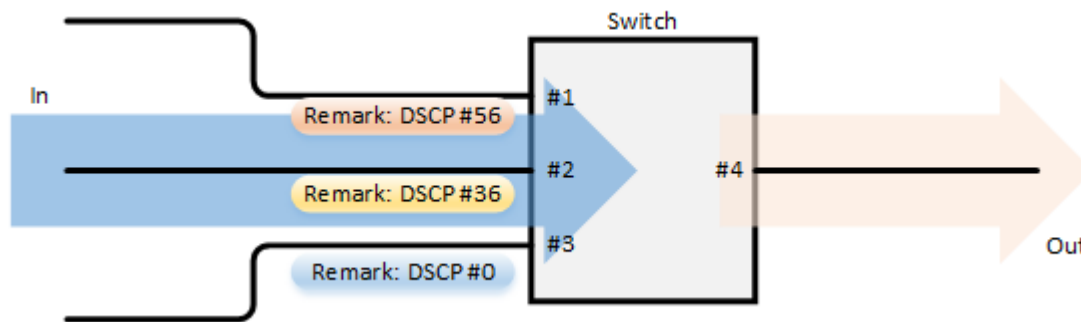
```
Yamaha(config)# qos scheduling wrr
```

Priority control based on DSCP value assigned to each reception port

A DSCP value is assigned to each reception port, and the transmission queues are reassigned based on the DSCP values.

In the following example, frames received on LAN port #1 are stored in the highest-priority transmission queue (ID: 7, weight of 20%), frames received on LAN port #2 are stored in the second highest-priority transmission queue (ID: 5, weight of 15%), and frames received on LAN port #3 are stored in the transmission queue (ID: 2, weight 10%) whose priority is the lowest among the three LAN ports.

- Priority control based on DSCP value assigned to each reception port: setting example



- Remarking settings for individual reception ports
 - Set the DSCP value for frames received on LAN port #1 (port1.1) to **56**.
 - Set the DSCP value for frames received on LAN port #2 (port1.2) to **36**.
 - Set the DSCP value for frames received on LAN port #3 (port1.3) to **0**.
1. Enable QoS and set the trust mode and remarking for the reception ports (LAN ports #1, #2, and #3).

```

Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust dscp ③
Yamaha(config-if)#remark dscp 56 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust dscp ⑥
Yamaha(config-if)#remark dscp 36 ⑦
Yamaha(config-if)#exit
Yamaha(config)#interface port1.3 ... ⑧
Yamaha(config-if)#qos trust dscp ⑨
Yamaha(config-if)#remark dscp 0 ⑩
Yamaha(config-if)#exit

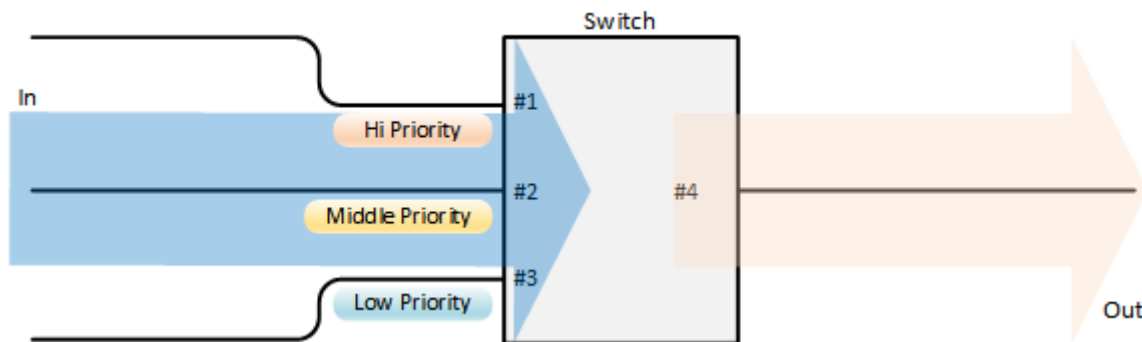
```

- ① Enable QoS
- ② Setting for LAN port #1
- ③ Change the trust mode to "DSCP"
- ④ Set the DSCP value for frames received on LAN port #1 to 56
- ⑤ Setting for LAN port #2
- ⑥ Change the trust mode to "DSCP"
- ⑦ Set the DSCP value for frames received on LAN port #1 to 36
- ⑧ Setting for LAN port #3
- ⑨ Change the trust mode to "DSCP"
- ⑩ Set the DSCP value for frames received on LAN port #1 to 0

Priority control using port priority trust mode

The transmission queue is determined according to the port priority order that is specified for each reception port.

- Priority control using port priority: setting example



- Set priority for each reception port
 - Set LAN port #1 (port1.1) to priority order 6.
 - Set LAN port #2 (port1.2) to priority order 4.
 - Set LAN port #3 (port1.3) to priority order 2.
1. Enable QoS and set the trust mode for the reception ports (LAN ports #1, #2, and #3).

```

Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust port-priority ③
Yamaha(config-if)#qos port-priority-queue 6 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust port-priority ⑥
Yamaha(config-if)#qos port-priority-queue 4 ⑦
Yamaha(config-if)#exit
Yamaha(config)#interface port1.3 ⑧
Yamaha(config-if)#qos trust port-priority ⑨
Yamaha(config-if)#qos port-priority-queue 2 ⑩
Yamaha(config-if)#exit

```

- ① Enable QoS
- ② Setting for LAN port #1
- ③ Change the trust mode to "port priority"
- ④ Set the port priority to 6
- ⑤ Setting for LAN port #2
- ⑥ Change the trust mode to "port priority"
- ⑦ Set the port priority to 4
- ⑧ Setting for LAN port #3
- ⑨ Change the trust mode to "port priority"
- ⑩ Set the port priority to 2

Points of Caution

- If QoS settings are applied to LAN/SFP ports belonging to a logical interface, the settings applied to the port with the lowest port number of the logical interface will also be applied to the other ports belonging to that logical interface.

Related Documentation

None

Trademarks and Trade Names

- Zoom is a trademark or registered trademark of Zoom Video Communications, Inc. in the United States and other countries.
- Microsoft Teams is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.

Flow Control

Function Overview

A switching hub initially stores received frames in memory and then performs relay processing. When many frames are sent at the same time and relay processing cannot keep up (a congested state), exceeding the available memory capacity for storage, the frames to be relayed are discarded. This product includes the following two functions to help mitigate such congestion.

- When ports are operating at full duplex: IEEE 802.3x flow control can be enabled.
- When ports are operating at half duplex: the back pressure function will always be enabled.

Definition of Terms Used

Bit Time

On a 10BASE network, the speed is **10Mbps**, so 1 bit time = 100 nsec.
In the same way, the bit time on 100BASE is 10 nsec, and on 1000BASE is 1 nsec.

Jam Signal

In half-duplex communications, where data cannot be transmitted and received at the same time, there is a possibility of data collision.

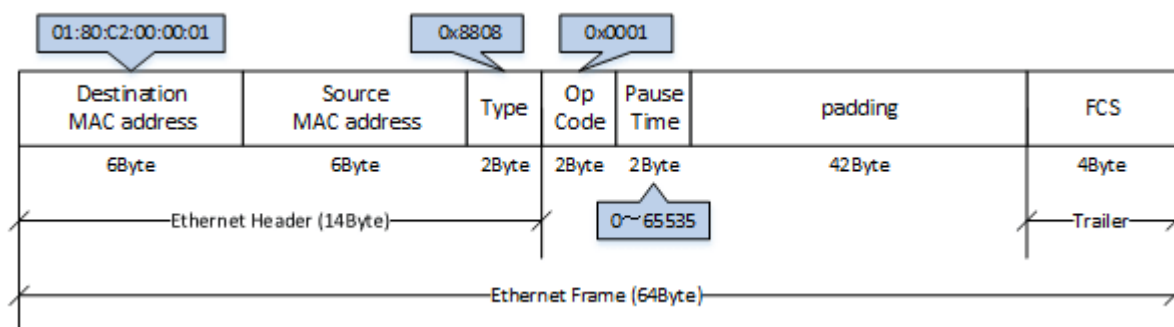
The transmitting device monitors the possibility of data collision during transmission. When possible data collision is detected, the device stops transmitting and sends a jam signal. After the jam signal is sent, the device waits for a random interval before resuming transmission.

Although undefined in IEEE, jam signals that use a 32-digit alternating “1” and “0” bit sequence (such as “10101010101010101010101010101010”) are often used.

Function Details

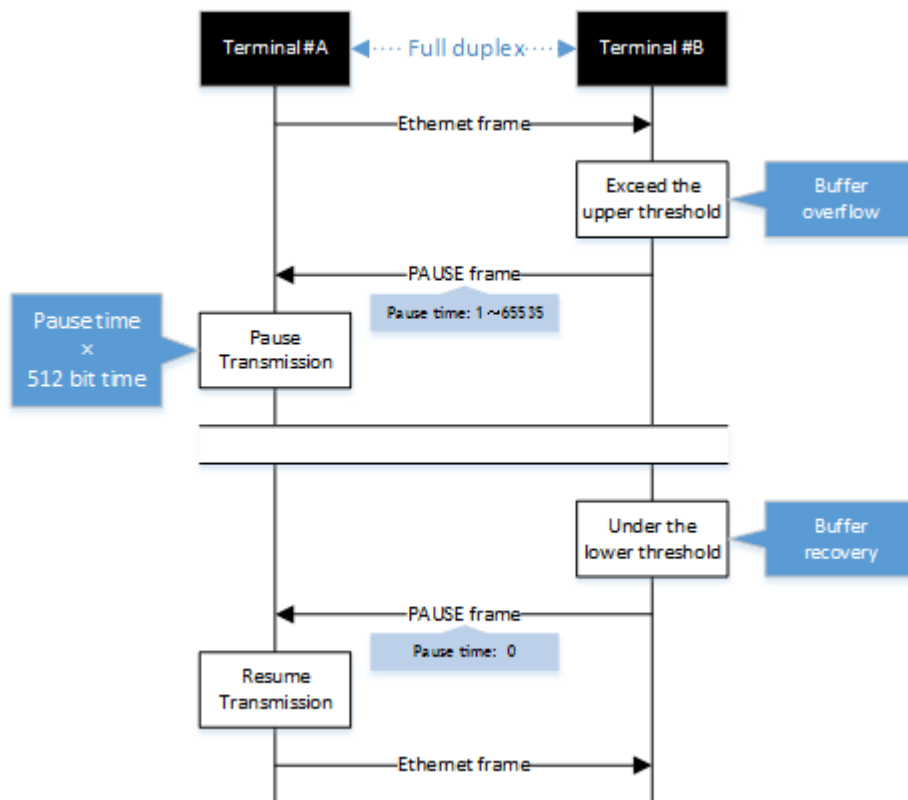
IEEE 802.3x flow control

For full duplex communication, the MAC control protocol with IEEE802.3x option can be used. The **MAC control frame** in the diagram below is used for flow control.



The following flow control operations are performed, based on the restriction start threshold and the restriction cancel threshold.

- Flow control: processing flow



This product can be used for either transmitting or receiving MAC control frames. The operations for each are shown below.

- MAC control frame transmission processing
 - Frames are stored in the packet buffer. When the number of frames exceeds the restriction start threshold, a PAUSE frame with a pause time of 65535 is sent.
 - When the overflow in the packet buffer is resolved, and the number of frames falls below the restriction cancel threshold, a PAUSE frame with a pause time of 0 is sent.
- MAC control frame reception processing
 - When a PAUSE frame with a pause time of 1–65535 is received, the transmission processing will be stopped if the corresponding **bit time** has elapsed, or if the a PAUSE frame with a pause time of 0 has been received.

Use the **flowcontrol** command to enable or disable the flow control (when transmitting/receiving MAC control frames).

This setting can be made for the system and for each transmitting/receiving LAN port, and is set to “disable” by factory default.

In order to enable flow control for an individual port, flow control must be enabled for the system.

The **tail drop function is disabled** when flow control is enabled in the system.

Packet buffers are shared among ports, and the restriction start threshold and the restriction cancel threshold change dynamically according to packet buffer usage. (This behavior cannot be changed.)

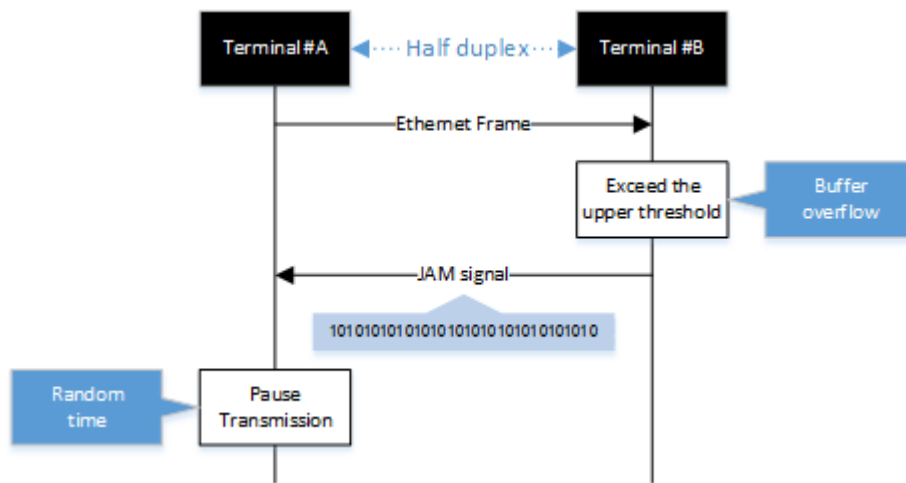
Back pressure

This product sends a **jam signal** whenever the receiving buffer of a LAN port is about to overflow.

With this, the sender waits for a random amount of time as per the CSMA/CD, and then sends the frames.

When the LAN port is operating at **half duplex**, the **back pressure function will always be enabled**.

- Back pressure processing flow



Related Commands

Related commands are indicated below.
For details, refer to the Command Reference.

Operations	Operating commands
Set (system) flow control (IEEE 802.3x PAUSE send/receive)	flowcontrol
Set (interface) flow control (IEEE 802.3x PAUSE send/receive)	flowcontrol
Show flow control operating status	show flowcontrol

Examples of Command Execution

Enable flow control on LAN port #1.
After the function is enabled, check the flow control operating status.

```
Yamaha(config)#flowcontrol enable
Yamaha(config)#interface port1.1
Yamaha(config-if)#flowcontrol both
Yamaha(config-if)#end
Yamaha#show flowcontrol port1.1
Port      FlowControl    RxPause TxPause
-----
port1.1   Both           0       64
```

Points of Caution

None

Related Documentation

None

Storm Control

Function Overview

This product provides a **storm control** function as a countermeasure against L2 loops and DoS attacks. Broadcasts, multicasts, and unicast (dlf) frames that are addressed to an unknown host are monitored for each LAN port, and frames that exceed a preset threshold value are discarded. This prevents such frames from taking up bandwidth on the LAN port.

Definition of Terms Used

Broadcast Storm/Multicast Storm

This means a situation where frames addressed for broadcast or multicast are continuously forwarded. In this situation, the switch floods all ports except for the reception port with the broadcast or multicast. When this is received by another switch, all ports except for the reception port are flooded in the same way. When this continues, it can lead to the following symptoms.

- Bandwidth is taken up by the broadcast frames/multicast frames
- The switch's CPU load increases, making normal operations difficult
- Devices connected to the switch become unable to communicate

Unicast Storm

This means a situation where frames addressed to an unknown unicast destination (dlf: Destination Lookup Failure) are continuously forwarded. When the MAC address of the receiving device has not been registered in the ARP table, all ports on the switch except for the reception port are flooded. This leads to the same symptoms occurring as with a broadcast storm or multicast storm.

Function Details

The operating specifications for storm control are shown below.

1. The storm control function can be enabled for LAN ports.
The setting is **disabled for all ports** by default.
2. Storm control on this product can be specified as a tolerance percentage for the bandwidth of the LAN ports that receive broadcast frames, multicast frames, and frames addressed to an unknown unicast destination.
(Control can be made in two decimal points. Specifying 100% is the same as disabling the storm function.)
The bandwidth tolerance is common for all frames, and the user can select the applicable frames. This setting is made using the **storm-control** command.
3. When frames exceeding the permitted bandwidth are received, the excessive frames are discarded.
4. Use the **show storm-control** command to check the storm control information set for the LAN port.

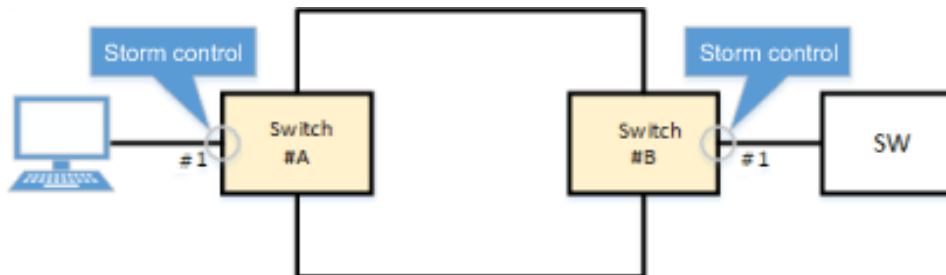
Related Commands

Related commands are indicated below.
For command details, refer to the command reference.

Operations	Operating commands
Set storm control	storm-control
Show storm control reception upper limit	show storm-control

Examples of Command Execution

In this example, the receivable L2 broadcast packets for LAN port 1 are restricted to a port bandwidth of 30%.



```

Yamaha(config)#interface port1.1
Yamaha(config-if)#storm-control broadcast level 30 ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show storm-control
Port      BcastLevel  McastLevel  UcastLevel
port1.1   30.00%      100.00%      100.00%
port1.2   100.00%      100.00%      100.00%
port1.3   100.00%      100.00%      100.00%
port1.4   100.00%      100.00%      100.00%
port1.5   100.00%      100.00%      100.00%
port1.6   100.00%      100.00%      100.00%
port1.7   100.00%      100.00%      100.00%
port1.8   100.00%      100.00%      100.00%
port1.9   100.00%      100.00%      100.00%
port1.10  100.00%      100.00%      100.00%

```

① Limit broadcast to 30% of bandwidth

Points of Caution

None

Related Documentation

- [Layer 2 Function: Proprietary Loop Detection](#)

Other Information

SNMP MIB Reference

For more information, see the “SNMP MIB Reference” chapter in the HTML version of this document.

Command Reference

https://manual.yamaha.com/network/rt/swx2210p/cmdref_swx2210p_en.html

About Licenses of Open Source Software Used in This Product

List of Open Source Software

The open source software used in this product and their licenses are shown in the table below.

- Open source software and licenses

Open source software	License
u-boot	GPLv2
OpenLLDP	GPLv2
OpenSSL	OpenSSL
Wide-DHCPv6	3-clause BSD
crypt-md5.c	2-clause BSD
ExplorerCanvas	Apache 2.0
jqCanvas	MIT
jqPlot	MIT/GPL2
jQuery	MIT
jQuery DatePicker plugin	MIT
jQuery File Upload Plugin	MIT
jQuery Iframe Transport Plugin	MIT
jQuery XDomainRequest Transport Plugin	MIT
jQuery Migrate	MIT
jQuery UI	MIT
jQuery UI Touch Punch	MIT/GPL2
jQuery UI Widget	MIT
jQuery UI Ympicker	MIT/GPL2
PowerTip	MIT

- About GPL/LGPL licensed software

This product includes software licensed under the GNU General Public License (GPL) or GNU Lesser General Public License (LGPL).

Customers may obtain the source code of the software and reproduce, distribute, and modify it in accordance with the GPL or LGPL.

Any portion of the source code of this product that is licensed under the GPL or LGPL may be provided by Yamaha (for a period of five years from the final shipment date).

Yamaha shall not be liable for any damages arising from changes, additions, deletions, or other actions to the software of this product made by a third party other than Yamaha (or a party authorized by Yamaha). Reuse of source codes provided by Yamaha is not guaranteed. Yamaha shall not be liable for the source codes.

- Software other than those licensed under the GPL/LGPL

This product uses open source software in accordance with the license conditions provided by the copyright holders.

Yamaha shall not be liable for the source codes.

List of License Terms

GPLv2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so

that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to

control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING

WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>
```

```
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.
```

```
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public License along
with this program; if not, write to the Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if

necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

OpenSSL

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

OpenSSL License

```
/* =====
 * Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
```

```
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

```
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
```



```

* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the routines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

Wide-DHCPv6

```
$KAME: COPYRIGHT,v 1.2 2004/07/29 19:02:18 jinmei Exp $
```

Copyright (C) 1998-2004 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

crypt-md5.c

```
* Copyright (c) 2003 Poul-Henning Kamp
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
```

ExplorerCanvas

Copyright 2006 Google Inc.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

jqCanvas

The MIT License

Copyright (c) 2008 David Kwast <david *dot* kwast *at* gmail>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jqPlot

Title: jqPlot Charts

Pure JavaScript plotting plugin for jQuery.

About: Version

version: 1.0.4
revision: 1121

About: Copyright & License

Copyright (c) 2009-2012 Chris Leonello
jqPlot is currently available for use in all personal or commercial projects under both the MIT and GPL version 2.0 licenses. This means that you can choose the license that best suits your project and use it accordingly.

See <GPL Version 2> and <MIT License> contained within this distribution for further information.

The author would appreciate an email letting him know of any substantial use of jqPlot. You can reach the author at: chris at jqplot dot com or see <http://www.jqplot.com/info.php>. This is, of course, not required.

If you are feeling kind and generous, consider supporting the project by making a donation at: <http://www.jqplot.com/donate.php>.

sprintf functions contained in jqplot.sprintf.js by Ash Searle:

version 2007.04.27
author Ash Searle
<http://hexmen.com/blog/2007/03/printf-sprintf/>
<http://hexmen.com/js/sprintf.js>

The author (Ash Searle) has placed this code in the public domain:

"This code is unrestricted: you are free to use it however you like."

jQuery

jQuery JavaScript Library v1.9.1
<http://jquery.com/>

Includes Sizzle.js
<http://sizzlejs.com/>

Copyright 2005, 2012 jQuery Foundation, Inc. and other contributors
Released under the MIT license
<http://jquery.org/license>

Date: 2013-2-4

jQuery DateTimePicker plugin

Copyright (c) 2013 <http://xdsoft.net>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jQuery File Upload Plugin / jQuery Iframe Transport Plugin / jQuery XDomainRequest Transport Plugin

MIT License

Copyright © 2010 Sebastian Tschan, <https://blueimp.net>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jQuery Migrate

Copyright jQuery Foundation and other contributors, <https://jquery.org/>

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at <https://github.com/jquery/jquery-migrate>

The following license applies to all parts of this software except as documented below:

====

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

All files located in the `node_modules` and external directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms above.

jQuery UI

Copyright jQuery Foundation and other contributors, <https://jquery.org/>

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at <https://github.com/jquery/jquery-ui>

The following license applies to all parts of this software except as documented below:

====

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Sample code is defined as all source code contained within the demos directory.

CC0: <http://creativecommons.org/publicdomain/zero/1.0/>

====

All files located in the node_modules and external directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms above.

jQuery UI Touch Punch

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero
Dual licensed under the MIT or GPL Version 2 licenses.

Depends:

```
jquery.ui.widget.js  
jquery.ui.mouse.js
```

jQuery UI Ympicker

jQuery UI Ympicker 1.8.21

Copyright 2012, AUTHORS.txt (<http://jqueryui.com/about>)
Dual licensed under the MIT or GPL Version 2 licenses.
<http://jquery.org/license>

<http://docs.jquery.com/UI/Ympicker>

Depends:
 jquery.ui.core.js

PowerTip

Copyright (c) 2018 Steven Benner (<http://stevenbenner.com/>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

