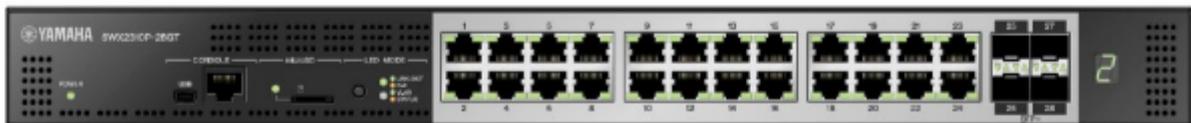
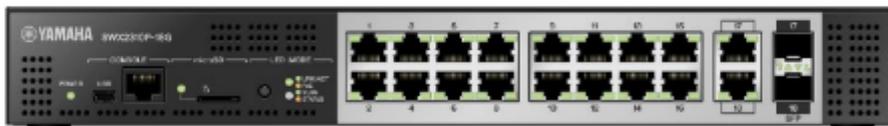


# SWX2310P series

## Technical Data



# Contents

General .....	1
Introduction .....	1
What you can do using the Web GUI .....	1
Operating environment .....	1
Recommended web browser .....	1
JavaScript settings .....	2
Cookie settings .....	2
User access rights .....	2
Note when using together with command input .....	2
Language .....	2
Login/Logout .....	3
Login page .....	3
Login method .....	3
Logout method .....	4
About sessions .....	4
Change password of initial administrative user "admin" .....	4
Select display language .....	4
About each screen .....	5
Dashboard .....	5
LAN MAP .....	5
Detailed settings .....	5
Management .....	6
CONSOLE .....	7
CONFIG .....	7
SYSLOG .....	8
TECHINFO .....	8
Dashboard .....	10
Summary .....	10
Using the dashboard .....	10
Summary .....	10
About the buttons .....	10
Using the gadgets .....	11
Available gadgets .....	11
Gadget details .....	12
About the gadgets .....	14
Interface information .....	14
System information .....	16
Resource information .....	17
SYSLOG .....	18
Terminal monitoring .....	18
Traffic information .....	18
Resource information(Graph) .....	20
Stack information .....	21
Power consumption information .....	22
PoE power supply .....	23
LAN MAP .....	24

About the LAN map . . . . .	24
Summary . . . . .	24
Using the LAN map . . . . .	24
About the buttons. . . . .	24
Using the LAN map . . . . .	25
Change pages . . . . .	25
Use the snapshot function . . . . .	25
Differences in what administrative users and general users can do . . . . .	25
Detail . . . . .	26
Map . . . . .	26
Tag VLAN . . . . .	41
Multiple VLAN. . . . .	45
Device list . . . . .	49
Whole map . . . . .	55
ProAV settings . . . . .	58
ProAV profile . . . . .	58
Summary . . . . .	58
How to use this page. . . . .	58
Introduction. . . . .	58
Set Dante profile. . . . .	58
Set NDI profile. . . . .	61
Set multiple ProAV profiles . . . . .	61
Return to defaults. . . . .	61
Trademark attributions . . . . .	61
Multicast . . . . .	62
Summary . . . . .	62
What's IGMP snooping . . . . .	62
How to use this page. . . . .	63
Introduction. . . . .	63
Warning message. . . . .	63
Change IGMP snooping settings . . . . .	64
Check IGMP snooping operating status . . . . .	64
Detailed settings . . . . .	66
Interface settings . . . . .	67
Physical interface. . . . .	67
Port mirroring settings. . . . .	70
Link aggregation. . . . .	71
Port authentication . . . . .	74
VLAN . . . . .	88
Create VLAN . . . . .	88
Tag VLAN . . . . .	92
Multiple VLAN. . . . .	94
Layer 2 functions . . . . .	95
MAC address table. . . . .	95
Spanning tree . . . . .	97
Loop detection . . . . .	99
Pass through . . . . .	101
DHCP snooping . . . . .	102

---

Layer 3 functions	106
DNS client	106
Routing	108
Multicast	110
Multicast basic settings	110
IGMP snooping	113
MLD snooping	116
Traffic control	118
Access list	118
Application layer	130
RADIUS server	130
Maintenance	141
Unit settings	141
Summary	141
Top page	141
Unit name setting page	141
LED mode setting page	142
Time zone setting page	142
Current date and time setting page	143
Date and time synchronization page	144
Date and time synchronization setting page	144
User settings	146
Summary	147
Top page	148
Password settings	148
User account settings	148
Password settings page	149
Password settings	149
User account settings page	150
User account settings	150
External devices	158
Schedule execution	159
SNMP	164
RMON	174
sFlow	181
LLDP	184
Mail notification	189
Terminal monitoring	192
Dante optimization	196
Y-UNOS (Yamaha Unified Network Operation Service)	198
Maintenance	200
Find this switch	218

---

# General

## Introduction

### What you can do using the Web GUI

#### GUI

The web GUI lets you perform basic settings and management of the Yamaha switch (this unit). The web GUI contains the following screens for you to make settings and perform management.

- Dashboard
- LAN MAP
- Detailed settings
- Management
- CONSOLE
- CONFIG
- SYSLOG
- TECHINFO

### Operating environment

Here we explain the environment that is required in order to use the web GUI.

#### Recommended web browser

We recommend the following web browser for use with the web GUI.

- Windows
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox
- Mac
  - Apple Safari
- iPadOS
  - Apple Safari

The latest version of each browser is recommended.

Microsoft Internet Explorer is not supported.

#### <NOTE>

- Do not use the "Back" or "Forward" buttons of the web browser.
- In some cases, the display layout of a page may become disordered. If this occurs, please access that page once again.

#### <Memo>

- The web GUI uses UTF-8 character encoding.

---

## JavaScript settings

The web GUI uses JavaScript. If your web browser is set to disable JavaScript, you might be unable to use the web GUI. If JavaScript is disabled, please enable JavaScript in your web browser before use.

## Cookie settings

The web GUI uses cookies. If your web browser is set to disable cookies, you might be unable to use the web GUI. Please allow cookies in your web browser before use.

## User access rights

Users who log in to the web GUI are divided into two types: general users and administrative users. These are referred to as "access levels." The differences between the access levels are described below.

- For general users  
Can view the settings of the unit, operate the Web console, and obtain SYSLOG. Cannot change the settings.
- For administrative users  
Can view and change the settings of the unit. Can obtain CONFIG and TECHINFO in addition to operating the Web console and obtaining SYSLOG.

## Note when using together with command input

Settings for this unit can be made not only via the web GUI but also from the command console screen by directly entering commands. Command input allows a broader range of settings than when using the web GUI, and also lets you make settings for functions that are not supported in the web GUI. If you use both command input and the web GUI to make settings, be aware that the commands that you input may be overwritten, or the settings may be cleared.

### <Memo>

- The command console screen contains the following items.
  - Management → "Maintenance" → "Command execution"
- For details on commands, refer to "Command reference."

## Language

The Web GUI allows you to switch the display language. To switch the display language, press the "Language Switch" button  on the top menu, and select a language you want.

The supported languages are as follows.

- Japanese
- English

---

# Login/Logout

## Login page

Start your web browser, and access "http://(the IP address you assigned to this unit)/" to display the login page. The following items are shown on the login page.

- Model name ( Ex. : SWX3220-16MT )
- hostname ( Name configured using the hostname command )
- Input box for user name
- Input box for password
- Login button

If login fails, the following error messages are displayed.

- Incorrect user name or password  
Incorrect username or password, or login as XXXX is restricted.
- Incorrect password three times in a row  
Blocked upon 3 failed login attempts for XXXX. Please try again later.
- Maximum number of sessions have been reached  
Login failed. The maximum number of sessions has been reached.  
Note: Refer to "[About sessions](#)" for details on sessions.

## Login method

Here we explain how to log in to the web GUI of this unit.

1. Start your web browser, and access the login page.
2. Enter the user name and password set by the username command, then press the "Login" button.

### <About users>

- To access this unit in the factory-set state, log in with the user name "admin" and the password "admin".
- When logging in as a user without administrative privileges, you will be logged in as a general user.
- When logging in as a user with administrative privileges, you will be logged in as an administrative user.

### <About general users and administrative users>

- General User  
If you log in as a general user, you will be able to view this unit's settings and operating status. You will not be able to make settings for this unit.
- Administrative User  
If you log in as an administrative user, you will be able to perform all web GUI operations. You can view the unit's settings and operating status, and configure the settings for this unit.

### <About passwords>

- You must enter the password as single-byte characters. Double-byte characters may not be used. Uppercase and lowercase characters are distinguished.
- Take care not to forget the password that you assigned. If you have forgotten the password, ask the administrator who set up this unit for the correct password.

### <NOTE>

- 
- You will not be able to properly login if the browser is configured to block cookies.
  - In this case, refer to the "Introduction 2. Operating environment" section to set up your cookies.

## Logout method

- In the upper right of the screen, press the "Log out" button to display the "Log out" dialog box.
- Press the "Login screen" button in the dialog box to go to the login page.

## About sessions

- If you can successfully login to the Web GUI, a session will be established between the browser in use and this unit.
- Each time you login from a different browser or device, a new session is established.
- The session will be maintained until you log out or the session times out.
- Sessions that have been established will time out after five minutes have elapsed from the last data communication.
- Up to four sessions can be established at one time.
- Information for a session can be checked using the "show users" command.

## Change password of initial administrative user "admin"

- If you log in as the initial administrative user "admin" and the password is "admin", a screen to change the password will appear.
- Enter the password and set it, then the setting is saved.

## Select display language

- A screen for selecting a language appears right after you log in, only if you log in to the Web GUI as an administrative user in the factory-set state.
- Once you select a language, the Web GUI displays in the language.

---

## About each screen

### Dashboard

It shows the various system information of this device in visual form. You can check and monitor the following status.

- Interface information
- System information
- Resource information ( CPU Utilization / MemoryUtilization )
- SYSLOG
- Terminal monitoring
- Traffic information ( Transmit / Reception )
- Resource information ( Graph )
- Stack information
- PoE power supply

### LAN MAP

In this page you can view, manage, and make settings for the Yamahanetwork devices managed by the LAN interface, and any equipment underits management.

The LAN map is shown only if this unit is operating as a manager.

### Detailed settings

In this page you can make detailed network-related settings for this unit. The following items are provided.

- Interface settings
  - Physical interface
  - Port mirroring
  - Link aggregation
  - Port authentication
    - Port authentication settings
    - Server settings
    - Authentication management
    - Web authentication screen
  - PoE
  - L2MS filter
  - Tx queue usage monitoring
- VLAN
  - Create VLAN
  - Tag VLAN
  - Multiple VLAN
- Layer 2 functions
  - MAC address table
  - Spanning tree

- 
- Loop detection
  - Pass through
  - DHCP snooping
  - Layer 3 functions
    - DNS client
    - Routing
  - Multicast
    - Multicast basic settings
    - IGMP snooping
    - MLD snooping
  - Traffic control
    - Access list
      - Create Access list
      - Apply Access list
    - QoS
    - Flow control
    - Storm control
  - Application layer
    - RADIUS server
      - Server settings
      - User management
      - Managing certificates

## Management

In this page you can make settings for this unit, and perform maintenance. The following items are provided.

- Unit settings
- Access management
  - User settings
  - Various server settings
- External devices
  - microSD
- Schedule execution
- SNMP
  - MIB
  - Community
  - SNMPv3 User
  - SNMP trap
- RMON
  - RMON settings
  - Event group

- 
- Alarm group
  - sFlow
  - LLDP
  - Mail notification
  - Terminal monitoring
  - Dante optimization
  - Y-UNOS
  - Maintenance
    - Command execution
    - System self-diagnostics
    - Cable diagnostics
    - Update firmware
    - CONFIG management
    - Summary data management
    - SYSLOG management
    - Backup / Restoration
    - Restart and initialization
  - Find this switch

## CONSOLE

You can access the console screen from the "CONSOLE" menu. A new browser window opens, and a login prompt appears. Enter your username and password to log in.

- Constraints
  - The Key input does not work correctly in Safari for macOS. Please use a browser (Chrome, Edge, Firefox) other than Safari.
  - Launching multiple web consoles is not supported. If you open a new web console, the current session is disconnected.
  - There are the following restrictions when accessing an L2MS agent's web console from the LAN map via an HTTP proxy.
    - If the L2MS manager is a router, it is not supported.
    - If the L2MS manager is a switch, make sure that the firmware supports the web console.
    - Do not launch multiple web consoles. You may temporarily lose access to the Web GUI of the L2MS manager.
- About copy and paste
  - You can copy text to the clipboard by pressing "Ctrl+C" after selecting the text.
  - "Copy" and "Paste" functions in the right-click menu are available only on the Web Console screen.
  - You can paste text from the clipboard by selecting "Paste from browser" from the right-click menu.

## CONFIG

The results of running the "show running-config" command (a setting of this unit) can be viewed in a web browser or acquired as a text file.

- Viewing CONFIG

- In the "CONFIG" menu, press the "Show in browser" button. The execution result of the "show running-config" command is shown in a sub-window.
- To close, press the web browser's close button.
- Obtaining CONFIG as a text file
  - In the "CONFIG" menu, press the "Obtain as text file" button to start the download automatically.
  - The name of the acquired file is "running-config\_YYYYMMDDhhmmss.txt".

YYYY	A.D. ( 4 Digit )
MM	Month ( 2 Digit )
DD	Day ( 2 Digit )
hh	Hours ( 2 Digit )
mm	Minutes ( 2 Digit )
ss	Seconds ( 2 Digit )

## SYSLOG

This feature outputs the log of this unit's operation status in the order of the oldest occurrence time. In the "SYSLOG" menu, the result of running the show logging command can be viewed in a web browser or acquired as a text file.

- Viewing SYSLOG
  - In the "SYSLOG" menu, press the "Show in browser" button. The execution result of the "show logging" command is shown in a sub-window.
  - To close, press the web browser's close button.
- Obtaining SYSLOG as a text file
  - In the "SYSLOG" menu, press the "Obtain as text file" button to start the download automatically.
  - The name of the acquired file is "running-config\_YYYYMMDDhhmmss.txt".

YYYY	A.D. ( 4 Digit )
MM	Month ( 2 Digit )
DD	Day ( 2 Digit )
hh	Hours ( 2 Digit )
mm	Minutes ( 2 Digit )
ss	Seconds ( 2 Digit )

- Constraints
  - If the stack function is enabled, only the SYSLOG of the main switch can be displayed.

## TECHINFO

The "show tech-support" command lets you view status information for all of this unit's functions. In the "TECHINFO" menu, the results of running the "show tech-support" command can be viewed in a web browser or acquired as a text file.

- Viewing TECHNIFO

- 
- In the "TECHINFO" menu, press the "Show in browser" button. The execution result of the "show tech-support" command is shown.
  - To close, press the web browser's close button.
  - Obtaining TECHNIFO as a text file
    - In the "TECHINFO" menu, press the "Obtain as text file" button to start the download automatically.
    - The name of the acquired file is "technifo\_YYYYMMDDhhmmss.txt".

YYYY	A.D. ( 4 Digit )
MM	Month ( 2 Digit )
DD	Day ( 2 Digit )
hh	Hours ( 2 Digit )
mm	Minutes ( 2 Digit )
ss	Seconds ( 2 Digit )

- Notes

- It may take some time to obtain TECHNIFO.
- This unit may undergo loading while the information is being acquired.

---

# Dashboard

## Summary

### Using the dashboard

#### Summary

- **What is the dashboard?**
  - The page that provides visualization and monitoring of various system information and status information is called the "dashboard."
  - When a parameter being monitored exceeds the threshold value, it is shown in a warning field, helping you to determine the cause of a problem or to perform troubleshooting.
- **What is a gadget?**
  - Each window shown in the dashboard is called a "gadget."
  - A gadget that you want to monitor can be placed anywhere you like.
  - Information for each gadget is automatically updated at regular intervals.

#### About the buttons

The dashboard shows the following buttons.

- **About the "Stack switch" button**
  - If the stack configuration is enabled, the stack switch button will be displayed at upper left.
  - Select a stack ID to display the stack information selected on the following gadgets.
    - System information
    - Resource information
    - Interface information
    - Resource information ( Graph )
    - Power consumption information
    - PoE power supply
  - This can only be selected for stacks with active status.
  - The main switch will be selected on the initial screen.
  - Information for selected stacks for separated gadgets will be shown per gadget at the next update timing.
-  **About the "Gadget" button**
  - From the "gadget" buttons () in the upper right, select the gadgets that you want to be displayed.
-  **About the "Warning" button**
  - A maximum of **32 warnings** are shown, from newest to oldest.
  - Each of the displayed gadgets monitors the situation, and when an abnormal situation or a high load is detected, the "Warning" button () flashes and a list of warnings appears under the "Warning" button.
  - The list of warnings shows the contents of the currently detected warnings in order of recentness.
    - Date and time that the abnormality was detected

- Gadget that detected the abnormality
- Detected content
- The bar of the gadget that is the object of the warning is also shown with a flashing "Warning" button.
- When the following conditions are satisfied, the warning will stop being displayed (the conditions differ depending on the detected content).
  - Recovered from an abnormal state (for example, the usage ratio or the throughput fell below the threshold)
  - The state was cleared (for example, the settings were changed or the port linked down)
  - The "Clear" button () of the warning list was pressed (\*)

(\*) **Note that even if you press the "Clear" button so that the warning is not shown in the warning list, it is not the case that the abnormal state has been resolved.**

- If all warning indications disappear, the "Warning" button stops flashing, and the warning list disappears.
- You can press the "Warning" button to open or close the warning list.
- You cannot open the warning list and the warning history list at the same time.

### About the "History" button

- The warning history is shown in order of newness, for a maximum of **64 items**.
- The warning history is shown in **bold**, but warnings that were cleared by the "Clear" button in the warning list are shown in thin characters.
- If there are unconfirmed warning history items that have not been cleared, the lower right of the "History" button () shows the number of those items (in other words the number of warning history items shown in bold) ().  
**If this number is displayed, check the contents of the warnings that have occurred in the warning history list.**
- When you press the "OK" button () of each item in the warning history list, it changes to thin characters as a confirmed history item, and the "OK" button disappears.
- In the warning history list, pressing the "All confirmed" button () changes all history entries to a confirmed state.
- In the warning history list, pressing the "All deleted" button () deletes all history.
- You can press the "History" button to open or close the warning history list.
- You cannot open the warning list and the warning history list at the same time.

## Using the gadgets

### Available gadgets

The following gadgets can be used.

- System information
- Resource information
- Interface information
- SYSLOG
- Terminal monitoring

- 
- Traffic information ( Transmit / Reception )
  - Resource information ( Graph )
  - Stack information
  - Power consumption information
  - PoE power supply

## Gadget details

Each gadget has the following functions.

### • Add gadget:

- Press the "Gadget" button () in the upper right, select the gadget that you want to use from the gadget list, and then press the "Apply" button.
- Gadgets are always added to the far upper left of the dashboard.

### • Delete gadget:

- Press the "Gadget" button () in the upper right, clear a selection from the gadget list, and then press the "Apply" button.
- You can also delete a gadget by pressing the "Close" button () in the upper right of each gadget.

### • Move gadget:

- When you place the mouse over each gadget, the mouse pointer changes to a move symbol, allowing you to drag the gadget to a desired position.
- Candidates for the gadget's movement destination are shown in gray.
- The interface information gadget cannot be moved.

### • Separate the gadget screen:

- A "Separate" button () is shown in the upper right of each gadget.
- If you press the "Separate" button, that gadget alone is shown in a different window.
- At this time, the corresponding gadget in the dashboard is indicated as "In separate window."
- If a gadget is separated, the following occurs.
  - The "Separate" button is no longer shown for the separated gadget.
  - When you update the dashboard display, all separated gadgets return to the dashboard and are shown.
  - When you close the dashboard, all separated gadgets are also closed.
- Separated gadgets can also be displayed by specifying a URL directly in the browser.

When a URL has been directly specified, the main switch will be displayed.

Example) System information gadget: <http://192.168.100.1/dashboard/system.html>

### • Minimize gadget:

- When you press the minimize icon () in the upper left of each gadget, the icon turns sideways () and the gadget display is minimized.
- When you press it again, the icon returns to its original downward orientation () and the gadget returns to its original size.

### • Save gadget position information:

- When you add, delete, or move a gadget, or when you minimize and restore it, the position data of the gadget is saved.

- This information is also saved when the power is turned off and on again.
- This data is initialized if you return the device to its factory-set state.
- If a general user logs in, the gadget position information is not saved.

• **Auto-update gadget:**

- All gadgets are automatically updated at regular intervals.
- The update interval differs depending on the gadget.

• **Warning display:**

- When an abnormal condition or a high load is detected by a gadget, a flashing "Warning" button () is displayed beside the minimize icon of that gadget.
- The following states will initiate this warning.

Gadget	Trigger
System information	When reboot because of startup is detected
	When the CPU temperature exceeds <b>95°C</b> .
	When the PHY temperature exceeds <b>112°C</b> .
	When the SFP temperature exceeds <b>76°C</b> .
	When the temperature sensor exceeds <b>50°C</b> .
	When the PSE temperature exceeds <b>135°C</b> .
	The fan stops.
	The fan speed increases.
Resource information	When CPU usage exceeds <b>80 %</b>
	When memory usage exceeds <b>80 %</b>
Interface information	An loop occurs.
	The SFP optical Rx level exceeds the upper limit.
	The SFP optical Rx level falls below the lower limit.
	The PoE power supply stops abnormally.
	An error occurs in the PoE power supply control.
Traffic information	The throughput exceeds the link speed of <b>60 %</b> .
Stack information	The stack port changed state to down.
	The heartbeat error was detected.
	This unit was selected as the main switch.
SYSLOG	When multiple L2MS managers are detected.

# About the gadgets

## Interface information

Displays the link status of the ports and the PoE power supply status.



- The "Port" icon display lets you check the link status of the ports, the PoE power supply status, and the bandwidth usage rate.
- When you move the mouse cursor over the "Port" icon, detailed port information is shown.
- Press the "LINK/ACT" button to display the link status. Press the "Power supply status" button to display the PoE power supply status. Press the "Bandwidth usage" button to display the bandwidth usage rate.
- The "Port" icon will display as follows, according to the link status, the PoE power supply status, and the bandwidth usage rate.

Link status: For a LAN port

Icon	Description
	Link up (port speed 1000BASE-T)
	Link up (port speed 100BASE-TX)
	Link up (port speed 10BASE-T)
	Link down
	Error occurrence (Loop detection, Shutdown by BPDU guard, Shutdown by port-security, The throughput has exceeded link speed 60.)
	The STP state of the port is discarding. (CIST only) It means that the STP is blocking frames even though the link is up.  * This icon is overlaid on the link-up icon.

Link status: For an SFP port

Icon	Description
	Link up (port speed 10GbE)
	Link up (port speed 1GbE)
	Link down
	Error occurrence (Loop detection, Shutdown by BPDU guard, Shutdown by port-security, Optical RX power error, The throughput has exceeded link speed 60.)

Icon	Description
	The STP state of the port is discarding. (CIST only) It means that the STP is blocking frames even though the link is up.  * This icon is overlaid on the link-up icon.

Link status:Stack port

Icon	Description
	Link up
	Link down

PoE supply:For a LAN port

Icon	Description
	Does not support power supply
	PoE is being supplied (supply Class0–3)
	PoE is being supplied (supply Class4)
	Power supply stopped
	Error occurrence (Power delivery capacity exceeded, Error on the Powered Device, Power supply abnormality)

PoE supply:For an SFP port

Icon	Description
	Does not support power supply

Bandwidth usage:For a LAN port

Icon	Explanation
	Link up ( Bandwidth usage rate $x$ : $95\% \leq x \leq 100\%$ )
	Link up ( Bandwidth usage rate $x$ : $85\% \leq x < 95\%$ )
	Link up ( Bandwidth usage rate $x$ : $75\% \leq x < 85\%$ )
	Link up ( Bandwidth usage rate $x$ : $65\% \leq x < 75\%$ )
	Link up ( Bandwidth usage rate $x$ : $55\% \leq x < 65\%$ )
	Link up ( Bandwidth usage rate $x$ : $45\% \leq x < 55\%$ )
	Link up ( Bandwidth usage rate $x$ : $35\% \leq x < 45\%$ )
	Link up ( Bandwidth usage rate $x$ : $25\% \leq x < 35\%$ )

Icon	Explanation
	Link up ( Bandwidth usage rate $x$ : $15\% \leq x < 25\%$ )
	Link up ( Bandwidth usage rate $x$ : $7.5\% \leq x < 15\%$ )
	Link up ( Bandwidth usage rate $x$ : $0\% \leq x < 7.5\%$ )
	Link down

Bandwidth usage:For an SFP port

Icon	Description
	Link up ( Bandwidth usage rate $x$ : $95\% \leq x \leq 100\%$ )
	Link up ( Bandwidth usage rate $x$ : $85\% \leq x < 95\%$ )
	Link up ( Bandwidth usage rate $x$ : $75\% \leq x < 85\%$ )
	Link up ( Bandwidth usage rate $x$ : $65\% \leq x < 75\%$ )
	Link up ( Bandwidth usage rate $x$ : $55\% \leq x < 65\%$ )
	Link up ( Bandwidth usage rate $x$ : $45\% \leq x < 55\%$ )
	Link up ( Bandwidth usage rate $x$ : $35\% \leq x < 45\%$ )
	Link up ( Bandwidth usage rate $x$ : $25\% \leq x < 35\%$ )
	Link up ( Bandwidth usage rate $x$ : $15\% \leq x < 25\%$ )
	Link up ( Bandwidth usage rate $x$ : $7.5\% \leq x < 15\%$ )
	Link up ( Bandwidth usage rate $x$ : $0\% \leq x < 7.5\%$ )
	Link down

## System information

The following information is displayed.

- **Device name:**
  - Display the device name of the switch.
- **Firmware revision:**
  - Firmware revision
- **Serial number:**
  - Serial number of the device
  - This is also shown by a label on the rear of the chassis.
- **MAC address:**
  - MAC address of the device
  - This is also shown by a label on the rear of the chassis.
- **Currently-running firmware:**
  - The currently started firmware is shown..
  - When it starts from firmware stored in an external memory, shown like "exec(SD)".

---

- **Currently-running settings file:**

- The currently used CONFIG file is shown.
- Select config0 - config4 using the **startup-config select** command.

- **Serial baud rate**

- Displays the baud rate of the console port.

- **System time:**

- Current device date and time
- If the date and time are incorrect, set the date and time either in the Web GUI's "Management" → "Device settings" page, or by using the **clock set** command or the **ntpdate** command.

- **Startup time:**

- System startup date and time

- **Startup reason:**

- Reason for startup
- Start from power-off state, **reload** command, revision up, etc.
- If reboot is detected as the startup reason, the background turns red, and a warning indication (❗) occurs.
  - Check with the network administrator.
  - In the warning list, press the "Clear" button (🗑️) to clear the warning indication.

- **Fan speed :**

- Displays the speed of each fan.

- **Internal chassis temperature :**

- Displays the temperature inside the chassis.

- **SFP optical RX level :**

- Displays the SFP optical Rx level state and the connection module.

- **PoE supply :**

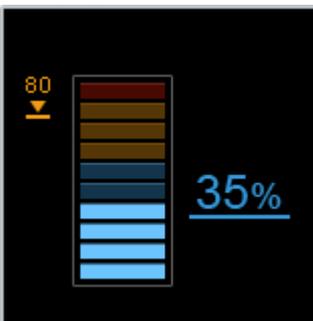
- The display will show whether the PoE power supply is enabled.

- **PoE supply power :**

- The current supply voltage and the maximum supplied voltage will be displayed.

## Resource information

This page shows the CPU usage and memory usage.



- The current values and peak values of CPU usage and memory usage are shown.
- The number at the right of the meter is the current usage, and the number at the left is the peak value.
- You can clear the previous peak value from "Clear peak values,".

- 
- Peak values are also cleared when you restart the device.
  - When you move the mouse cursor to each meter, the peak value and the date and time at which the peak value was recorded are shown.
  - If the CPU usage exceeds **80 %**, a warning display (🚫) is shown.
    - Note the date and time at which the peak value was recorded, and from other gadgets, note the traffic and the log that were occurring during that time.
  - If the memory usage exceeds **80 %**, a warning display (🚫) is shown.
    - Note the date and time at which the peak value was recorded, and from other gadgets, note the traffic and the log that were occurring during that time.

## SYSLOG

This shows the most recent SYSLOG.

- The most recent log is at the top.
- In the select menu you can change the number of lines that are displayed (default: 10 lines).

## Terminal monitoring

Displays a list of monitored devices and the status of each.

- Devices that are determined to be up, down, not started yet ("Idle") and all monitored devices ("All") are counted respectively.
- Displays the monitored target, device name, monitoring type and status for each monitored device.
- Point the mouse cursor above a status column to show the status for that monitored device.
- Press the "Up", "Down", "Idle" and "All" buttons to show only the monitored devices for those statuses.
- When not even one monitored device is registered, "The monitoring devices have not been registered" will be displayed.

## Traffic information

The physical interface traffic is displayed on a graph.

There are different gadgets for the transmission traffic and for the reception traffic.

- Use the "**Live**", "**Day**", "**Month**" and "**Year**" buttons to change the graph rendered.
  - **Live**
    - Traffic can be viewed for the previous two minutes.
    - The graph will be automatically refreshed each second.
  - **Day**
    - Displays traffic per hour for the specified date.
    - The day can be set using the day specification box at the top right of the gadget.
    - Press the date specification box to display the calendar, and select the day to show the graph for the day specified.
    - A date within one year to the past can be set using the calendar.
  - **Month**
    - Displays traffic per day for the specified month.
    - The month can be set using the month specification box at the top right of the gadget.
    - Press the month specification box to display the calendar, and select the month to show the graph for the day specified.

- A past month within one year can be set using the calendar.
- **Year**
  - Displays traffic per month for the specified year.
  - The year can be set using the year specification box at the top right of the gadget.
  - Press the year specification box to display the calendar, and select the year to show the graph for the year specified.
  - The year specification box can be used to specify either the current year or the previous year.
- Press the "Interface selection" button (  ) to display the "Interface selection" dialog box.
- Select the interface to display on the graph, from the "Interface selection" dialog box.
- The average traffic per hour for the interface is rendered on the graph.
- Press the "Export as a CSV file" button (  ) to display the "Traffic information Export summary data" dialog.
- You can export the specified period's traffic summary data as a CSV file in the "Traffic information Export summary data" dialog.
- Press the "Clear summary data" button (  ) to display the "Traffic information Clear summary data" dialog.
- You can delete all the traffic summary data in the "Traffic information Clear summary data" dialog.
- **Up to 8 lines** can be displayed on the graph using the colors blue, salmon pink, yellow, green, gray, sky blue, pink and purple for a total of 8 colors.
  - These colors are allocated in the order that they are rendered on the graph, from the newest interface numbers onwards.
- The Y-axis upper limit grows with the traffic, from a minimum of 10 [kbps] to a maximum of 10 [Gbps].
- The information shown below is shown on the graph for the specified period that is rendered.
  - **Live** : Current time - time 120 sec. ago (hh:mm:ss format)
  - **Day** : 0 o'clock - 23 o'clock
  - **Month** : 1st - 28th, 29th, 30th, 31st
  - **Year** : Jan - Dec
- Point the mouse cursor above a line on the graph to show the interface information, date and traffic amount.
- A legend for the currently displayed graph is shown at the lowermost part of the gadget.
- Using the legend
  - Only the lines on the graph that are enabled using the check boxes in the legend will be displayed.
  - Deselecting the check boxes will hide the corresponding lines from the graph.
  - This is useful when multiple lines are overlapping or when you wish to temporarily monitor a specific interface only.
  - If the interface you are currently monitoring does not exist, the message "The currently monitored interface is not selected" will display.
- Refresh the screen to restore the rendered time period and the selections on the legend to their defaults, as shown below.
  - Rendered period : **Live**
  - Legend check boxes : All applied
- If the traffic exceeds **60%**, a warning (  ) will be displayed.

- 
- If the traffic falls below **50%**, the warning will be cancelled.
  - When displaying a gadget in a separate window using the "Separate" button (
    - The settings prior to being separated will be reflected in the settings for the interface currently being monitored.
    - The rendered time period and the selections on the legend return to their defaults.
    - The settings for the interface selected in a separated window will be reflected in the dashboard gadget when the separated screen is closed.
  - When directly inputting the URL for a separated window and displaying a gadget
    - The rendered time period and the selections on the legend return to their defaults.

## Resource information(Graph)

This shows the CPU usage and memory usage in graph format.

- Use the "**Live**", "**Day**", "**Month**" and "**Year**" buttons to change the graph rendered.
  - **Live**
    - Usage ratio can be viewed for the previous two minutes.
    - The graph will be automatically refreshed each second.
  - **Day**
    - Displays usage ratio per hour for the specified date.
    - The day can be set using the day specification box at the top right of the gadget.
    - Press the date specification box to display the calendar, and select the day to show the graph for the day specified.
    - A date within one year to the past can be set using the calendar.
  - **Month**
    - Displays usage ratio per day for the specified month.
    - The month can be set using the month specification box at the top right of the gadget.
    - Press the month specification box to display the calendar, and select the month to show the graph for the day specified.
    - A past month within one year can be set using the calendar.
  - **Year**
    - Displays usage ratio per month for the specified year.
    - The year can be set using the year specification box at the top right of the gadget.
    - Press the year specification box to display the calendar, and select the year to show the graph for the year specified.
    - The year specification box can be used to specify either the current year or the previous year.
- Press the "Export as a CSV file" button () to display the "Resource information Export summary data" dialog.
- You can export the specified period's resource summary data as a CSV file in the "Resource information Export summary data" dialog.
- Press the "Clear summary data" button () to display the "Resource information Clear summary data" dialog.
- You can delete all the resource summary data in the "Resource information Clear summary data" dialog.

- The average usage ratio is rendered per hour for the monitored period.
- The CPU usage is shown on the graph using blue lines, and the memory usage is shown using salmon pink lines.
- The upper limit for the graph's Y axis is 100 [%].
- The information shown below is shown on the graph for the specified period that is rendered.
  - **Live** : Current time - time 120 sec. ago (hh:mm:ss format)
  - **Day** : 0 o'clock - 23 o'clock
  - **Month** : 1st - 28th, 29th, 30th, 31st
  - **Year** : Jan - Dec
- Point the mouse cursor above a line on the graph to show the monitored period, date and time and usage ratio.
- A legend for the currently displayed graph is shown at the lowermost part of the gadget.
- Using the legend
  - Only the lines on the graph that are enabled using the check boxes in the legend will be displayed.
  - Deselecting the check boxes will hide the corresponding lines from the graph.
- Refresh the screen to restore the rendered time period and the selections on the legend to their defaults, as shown below.
  - Rendered period : **Live**
  - Legend check boxes : All applied
- If the CPU usage exceeds **80%**, a warning (🚨) will be displayed.
- If the CPU usage falls below **80%**, the warning will be cancelled.
- If the memory usage exceeds **80%**, a warning (🚨) will be displayed.
- If the memory usage falls below **80%**, the warning will be cancelled.
- When displaying a gadget in a separate window using the "Separate" button (🗑️)
  - The rendered time period and the selections on the legend return to their defaults.
- When directly inputting the URL for a separated window and displaying a gadget
  - The rendered time period and the selections on the legend return to their defaults.

## Stack information

The following information is displayed.

- **Stack function**
  - Displays whether the stack function is enabled.
- **Members**
  - Displays the member switch types and roles.
- **Status**
  - Displays the member switch status.
  - Only displayed when the stack function is enabled.
- **Subnet on stack port**
  - Displays a range of IP addresses to use for stacked ports.
- **Virtual MAC-Address**
  - Displays the MAC address used in the stack configuration.

---

## Power consumption information

Displays the power consumption of the device on a graph.

- Use the "**Live**", "**Day**", "**Month**" and "**Year**" buttons to change the graph rendered.
  - **Live**
    - Displays the power consumption [W] per second for the last 2 minutes.
    - The graph will be automatically refreshed each second.
  - **Day**
    - Displays the total hourly power consumption [Wh] for the specified day.
    - The day can be set using the day specification box at the top right of the gadget.
    - Press the date specification box to display the calendar, and select the day to show the graph for the day specified.
    - A date within one year to the past can be set using the calendar.
  - **Month**
    - Displays the total daily power consumption [Wh] for the specified month.
    - The month can be set using the month specification box at the top right of the gadget.
    - Press the month specification box to display the calendar, and select the month to show the graph for the day specified.
    - A past month within one year can be set using the calendar.
  - **Year**
    - Displays the total monthly power consumption [Wh] for the specified year.
    - The year can be set using the year specification box at the top right of the gadget.
    - Press the year specification box to display the calendar, and select the year to show the graph for the year specified.
    - The year specification box can be used to specify either the current year or the previous year.
- Press the "Export as a CSV file" button () to display the "Power consumption information Export summary data" dialog.
- You can export the specified period's power consumption summary data as a CSV file in the "Power consumption information Export summary data" dialog.
- Press the "Clear summary data" button () to display the "Power consumption information Clear summary data" dialog.
- You can delete all the power consumption summary data in the "Power consumption information Clear summary data" dialog.
- The information shown below is shown on the graph for the specified period that is rendered.
  - **Live** : Current time - time 120 sec. ago (hh:mm:ss format)
  - **Day** : 0 o'clock - 23 o'clock
  - **Month** : 1st - 28th, 29th, 30th, 31st
  - **Year** : Jan - Dec
- Point the mouse cursor above a line on the graph to show the date and power consumption.
- Refresh the screen to restore the rendered time period to its default state **Live**.
- The rendered time period returns to its default in the following cases.
  - When displaying a gadget in a separate window using the "Separate" button ()

- 
- When directly inputting the URL for a separated window and displaying a gadget
  - The following recommended methods reduce power consumption.
    - Decrease the link speed of ports with low bandwidth usage.
    - Use the Schedule execution function to shut down unused ports and PoE power supply at midnight and on holidays.

## PoE power supply

Display the PoE power supply.



- The current/maximum power supply, the remaining available powersupply, and the guard band setting values are displayed at the top of the meter.
- The current utilization rate is shown on the right side of the meter, with peak utilization at the top.
- The arrow at the bottom of the meter indicates the guard band threshold value. If the current power supply exceeds the guard band threshold value, no additional power can be supplied.
- When you move the mouse cursor to the meter, the peak value and the date and time at which the peak value was recorded are shown.
- You can clear the previous peak value from "Clear peak values".
  - Peak values are also cleared when you restart the device.

---

# LAN MAP

## About the LAN map

### Summary

The LAN map shows terminal information for the agent devices (Yamaha switches, Yamaha wireless AP) that are connected to the network, providing a visualization of the entire network. You can use the GUI to view the agent status and make VLAN settings. You can also detect network problems to gather information when troubleshooting a problem.

- The switch that controls the LAN map (this unit) is called the "manager," and the Yamaha switches and Yamaha wireless AP units that are controlled by the manager are called "agents."

### Using the LAN map

Here we explain how to use the LAN map.

#### About the buttons

-  **Snapshot button**

You can save the current agent and terminal connection status as a snapshot. You can also export, import, or delete snapshots.

\*In order to use the snapshot function, you must enable the snapshot function from  "Settings".

\*Depending on the network structure, it may take several minutes for saving to be completed. During this time, other processing can still be executed.

- When exporting a snapshot, please allow pop-ups in your browser settings.

-  **Notice button**

Messages for the current network are displayed. This notifies you of agent problems such as a stopped fan or a loop that has occurred.

-  **History button**

This displays the history of notification messages. The history can save up to 1000 items.

 If you press the "Delete all" button, all history is deleted.

-  **Device list button**

The "Device list page" is shown in a separate window. In the device list page you can view a list of the terminals and agents managed in the LAN map, and manage terminal information.

-  **"Whole map" button**

The "Whole map page" is shown in a separate window. On the whole map page, the devices connected to the LAN are displayed on the same map.

-  **Settings button**

---

Here you can make settings for the LAN map function.

### Using the LAN map

To use the LAN map, open the "LAN map settings" dialog box from the "Settings" button, and select the "Manager" check box in the basic settings under "L2MS operation mode".

If "L2MS operation mode" is set to "Agent" or "Do not use", you cannot use the LAN map for this unit. If this unit is operating as agent, use the LAN map on the manager that is controlling this unit.

### Change pages

The LAN map consists mainly of map, tag VLAN, and multiple VLAN pages.

To switch the page that is displayed, use the **page selection toggle switch** located in the upper part of the screen.

### Use the snapshot function

The snapshot function compares the current network connection state to the previously saved network connection state (snapshot), and if a change is detected, displays a warning message. To use the snapshot function, perform the following operations.

1. Use the  **"Settings" button** to open the "LAN map settings" dialog box, and in the snapshot function settings section, select "Use the snapshot function". If you want terminals to also be included in the comparison, select either "Include all terminals in comparison" or "Include only wired terminals in comparison" depending on the terminals that you want to compare.
2. Use the  **"Snapshot" button** to save the snapshot. If you want to apply an exported snapshot to a manager, import that snapshot.

## Differences in what administrative users and general users can do

Basically, a general user can only view information, and cannot perform operations that modify settings, manage snapshots, edit or operate the terminal DB and so on. An administrative user can perform all operations. The following operations cannot be performed by a general user.

- Agent management
-  Using the **"Settings" button** to change LAN map settings
-  Using the **"Acquire" button** to acquire device information.
-  Using the **"Snapshot" button** to manage snapshots
- Editing, deleting, newly registering, importing, and exporting a terminal DB
- Procedure for saving a terminal list and agent list in CSV format

# Detail

## Map

### Summary

This visualizes the network status. You can check the connection status of the devices, and change the settings of a Yamaha switch or Yamaha wireless AP.

### Structure of the map page

The map page provides a "Tree view," "Device detail and settings view," and "Connected devices view" to show the state of the network.

### Tree view

The agent topology starting at the manager is shown in the lower left of the screen. Network devices of other manufacturers are not shown. In the "Tree view," press the **"Devices" icon** to see device information in the "Device details and settings view" and "Connected devices view."

### Device details and settings view

Detailed information and device detail images for the manager or agent selected in the "Tree view" are shown in the upper part of the screen.

### Connected devices view

Devices that are connected to the manager or agent selected in the "Tree view" are shown in the lower right of the screen. If "Device management" is not enabled in "LAN map settings," equipment information (e.g., PC or mobile devices) is not shown.

- **Acquisition date and time**

This is the time at which information was last obtained for equipment that is connected to the manager or agent selected in the "Tree view." This is not shown if "Device management" is not enabled in "LAN map settings."

-  **Acquire button**

This obtains information for terminal that is connected to the manager or agent selected in the "Tree view." This is not shown if "Device management" is not enabled in "LAN map settings."

- **Select page**

Page numbers are shown for the list of currently-displayed terminal. Press ◀ or ▶ or enter a numeric value to move between pages.

-  **Show all button**

All items of device information are shown in the list. While all are displayed, press this again to return to the previous display.

- **List**

Information is listed for equipment that is connected to the manager or agent selected in the "Tree view."

You can press each item's  **Sort switch** to sort the list. The initial screen is sorted in order of port.

The VLAN ID item shows (A) for an access VLAN or (T) for a trunk VLAN.

If the port is being used as a port for a private VLAN, the VLAN ID is not shown, and (P) is shown.

If the port is being used as a port for a voice VLAN, the VLAN ID is not shown, and (V) is shown.

### Checking the status of devices

In "Device details and settings view" you can view detailed device information such as device name and MAC address, and also check the port link status, power supply status, and wireless communication status.

- Device name
- MAC address
- Port link status
- Power supply status
- Wireless communication status

For devices in a stack configuration, you will be able to switch stack ID with the toggle button.

### Checking the link status of ports

In "Device details and settings view," you can use the **"Port" icon** display to check the link status of the port.

If a agent is selected in the "Tree view," you can press the **"Port" icon** in the "Device details and settings view" to see detailed port information. If a **"Port" icon** shows an ↑, this indicates that the port is an uplink port.

The **"Port" icon** is shown as follows depending on the link status.

For a LAN port

Icon	Description
	Link up (port speed 10GBASE-T)
	Link up (port speed 5GBASE-T)
	Link up (port speed 2.5GBASE-T)
	Link up (port speed 1000BASE-T)
	Link up (port speed 100BASE-TX)
	Link up (port speed 10BASE-T)
	Error occurrence
	Link down

For an SFP port

Icon	Description
	Link up (port speed 10GbE)
	Link up (port speed 1GbE)
	Error occurrence

Icon	Description
	Link down

For an Stack port

Icon	Description
	Link up
	Link down

### Checking the power supply status of a switch that supports PoE

In the "Tree view," press the **"Device" icon** of a switch that supports PoE, and in "Device details and settings view," press the **"Power supply status" button** to check the PoE power supply status.

The **"Port" icon** is shown as follows depending on the power supply status.

**For the SWX2322P Series ,SWX2310P Series, SWR2311P Series, SWX2221P-10NT, SWX2220P Series, SWX2210P Series, SWX2200-8PoE,SWX2110P-8G**

Icon	Description
	PoE is being supplied (supply Class0–3)
	PoE is being supplied (supply Class4–8)
	PoE is not being supplied
	Power supply stopped (error occurred)
	Power supply stopped

Note: On the SWX2200-8PoE the power supply class is not displayed in the icon.

**For the SWX2100-10PoE and SWX2100-5PoE**

Icon	Description
	PoE is being supplied (supply Class0–4)
	PoE is not being supplied
	Power supply stopped (error occurred)
	Power supply stopped

### Checking the wireless communication status of a wireless AP

In the "Tree view," press the **"Device" icon** of a Yamaha wireless AP, and in "Device details and settings view," press the  **"Wireless" icon** to check the wireless communication status.

The **"Wireless" icon** is displayed when wireless communication is possible in that frequency band.

## Monitoring network errors

The LAN map monitors the network and notifies you of errors. If an error is detected on the network, a message is displayed below.

- **Notification area**

Press the  **"Notice" button** to see the messages regarding the current network status. The notification area is also shown automatically when a new message is added. If there is a device for which an error was detected, a  is shown beside the **"Device" icon** of the Tree view, and the device information of "Connected device view" is highlighted in  red.

- **History area**

 When you press the **"History" button**, the history of the notification messages is shown.

## Monitoring the operating status and errors of a switch

In the LAN map, when the following operations or error are detected, a message is displayed in the "Notification area" or "History area." Some messages are displayed in both the "Notification area" and the "History area," and some are displayed in only one.

Troubleshooting items	Notification area	History area
The fan of a Yamaha switch is stopped	○	○
The fan of a Yamaha switch has recovered	×	○
The fan speed of the Yamaha switch has increased	○	○
The fan speed of the Yamaha switch has decreased	×	○
The power supply voltage of the Yamaha switch has exceeded the upper threshold	○	○
A line surge has occurred in the power supply of the Yamaha switch	○	○
The temperature ( CPU, PHY, SFP module, Unit, MAC, PSE ) of the Yamaha switch has exceeded the upper threshold	○	○
The temperature of the Yamaha switch has returned to normal	×	○
A loop is occurring at ports of a Yamaha switch	○	○
Optical Rx level of the SFP port of the Yamaha switch has reached an abnormal level	○	○
Optical Rx level of the SFP port of the Yamaha switch has returned to normal level	×	○
Transmission queue usage ratio for the port on the Yamaha switch is high	○	○
Transmission queue usage ratio for the port on the Yamaha switch has returned to normal	×	○
The power being supplied from the Yamaha switch has entered the guard band range	×	○
Power is no longer supplied from a port of a Yamaha switch	×	○
Power has begun being supplied from the port of a Yamaha switch (for each Supply Class).	×	○

Troubleshooting items	Notification area	History area
Power supplied from a port of a Yamaha switch has halted abnormally	○	○
The power being supplied from a Yamaha switch has exceeded the maximum power supply capacity	○	○
An error occurred in the power supply of a Yamaha switch	○	○
The monitoring device is DOWN	○	○
The monitoring device is UP	×	○
The stack port has linked down	○	○
The stack port has linked up	×	○
Duplication of L2MS managers has been detected	○	○
Duplication of L2MS managers has been resolved	×	○

Enable the event monitor function on "LAN map settings" to periodically acquire the current status of the monitoring target event(event information) for the agent.

The monitoring target events and compatible agentes are as follows.

Monitoring target event	Compatible models
Changes in optical Rx level of the SFP port	SWX2300 Series, SWX2310P Series, SWX2310 Series, SWR2311P-10G, SWR2310 Series, SWX3100 Series, SWX3200 Series, SWX2320 Series, SWX2322P Series, SWX3220 Series
Changes in usage ratio for the port transmission queue	
Status notification for device monitoring	
Changes in temperature and FAN speed	SWX2310P Series, SWR2311P-10G, SWX2310-52GT, SWX3200 Series, SWX2320 Series, SWX2322P Series, SWX3220 Series
Changes in power voltage	SWX3200-28GT/52GT

Normally, since a notification is sent to the manager whenever an event occurs on a agent, the agent event that occurs will be detected even if the event monitoring function is disabled. However, we recommend that the event monitoring function be enabled, in case the manager cannot receive the notification for some reason.

### Monitoring the network connection status

In order to monitor the network connection status, enable the snapshot function using the procedure described "About the LANmap"-2-4. Using the snapshot function" in this help.

The snapshot function compares the current network status with the snapshot, and if there is a difference, determines that a network error has been detected. When you press the  "Snapshot" button, the snapshot management dialog box appears, allowing you to save, export, import, or delete snapshots.

- **Save**

Save a snapshot. If "Update network connection status before saving" is enabled, the network connection status information is updated before saving.

- **Export**

The agent snapshot and terminal snapshot are downloaded.

- **Import**

A snapshot saved on the PC is applied to the manager. Use the **"Select a file" button** to select a agent snapshot and a terminal snapshot. If you don't select a terminal snapshot, the existing snapshot is deleted, and an empty terminal snapshot is created.

\*If you use an edited snapshot, it might not work correctly.

- **Delete**

Delete a snapshot.

If the snapshot function is enabled, the agent is always the object of warnings, but the terminal is the object of warnings if all of the following conditions are fulfilled.

- The snapshot function's "Include terminals in comparison" is enabled
- The snapshot function is set to "Include in monitoring" on the terminal DB

If you want all terminals on the network to be excluded from warnings, disable the snapshot function's "Include terminals in comparison". If you want only a specific terminal to be excluded from warnings, enable the snapshot function's "Include terminals in comparison," and edit the terminal DB settings so that the snapshot function of the terminal to be excluded from warnings is set to "Don't include in monitoring". In the case of a terminal that is excluded from warnings, it will not be determined that a network error has been detected even if there is a difference between the connection status and the snapshot.

The snapshot function allows you to check the following operating status and errors. Some messages are displayed in both the "Notification area" and the "History area," and some are displayed in only one.

Troubleshooting items	Notification area	History area
An unregistered agent and terminal are connected	○	○
There is a agent and terminal whose connection ports differ	○	○
There is a agent and terminal that cannot be found	○	○
There is a discrepancy between the states of the agent and terminal	×	○
A snapshot has not been created	○	×
Creation of a snapshot has started	×	○
Creation of a snapshot has finished	×	○
A snapshot is being created	○	×
Creation of a snapshot was interrupted	×	○
Creation of a snapshot failed	×	○

### Searching for a device

To search for a device, input the keywords in the search box and press the  **"Search"** button. All devices whose information matches the keywords will be shown in "Connected devices view". The **"Device" icon** for connected devices matching the keywords inputted in the tree view will be highlighted in  blue-gray.

To cancel the search, press the **"X" button**.

Devices are searched by comparing the keywords with the following device information.

- Route
- SSID
- VLAN ID
- Manufacturer
- Device name
- Comment
- MAC address
- IP address
- Model name
- OS
- Frequency

Pressing the **"Device"** icon highlighted  blue-gray in the tree view will highlight the devices found in the search performed in "Connected devices view" in blue-gray. When the search results overlap with the  red highlights due to error detection,  blue-gray-colored results will be given priority. Lowercase and capital letters are treated the same for keywords.

You can use regular expressions in keywords. Below is an example of regular expressions you can use in the LAN map.

Syntax	Explanation
A	The character "A"
ABC	The characters "ABC"
[ABC]	One character, either "A", "B" or "C"
[A-C]	One character between "A" and "C"
[^ABC]	An arbitrary character that is neither "A", "B" or "C"
.	An arbitrary character
A+	At least one "A" character
A*	At least zero "A" characters
A?	Zero or one "A" character
^A	A string that begins with "A"
A\$	A string that ends with "A"
ABC DEF GHI	"ABC", "DEF" or "GHI"
A{2}	Two "A" characters (AA)
A{2,}	Two or more "A" characters (AA, AAA, AAAA...)
A{2,3}	Two to three "A" characters (AA, AAA)
\b	Word breaks, such as spaces
\B	Any character besides \b

Syntax	Explanation
\d	An arbitrary number (same as [0-9])
\D	Any character besides numbers (same as [^0-9])
\s	Single breaking character
\S	Any single character besides \s
\w	Alphanumeric characters including underlines (same as [A-Za-z0-9_])
\W	Any character besides \w

### Setting and managing agentes

You can set and manage agentes using the buttons that are shown in "Device details and settings view." The buttons shown in "Device details and settings view" will differ depending on the device that is selected in "Tree view."

### Managing agentes

If in "Tree view" you press the manager's "**Device**" icon, and in "Device details and settings view" press the "**Agent management**" button, the agent management settings dialog box appears, allowing you to view information for each device and set the IP address.

The items that can be set and managed for each device are the following.

Note: The following settings can be made on the SWX2110 Series, SWX2110P Series, SWX2210 Series, SWX2210P Series, SWX222x Series, the SWX2300 Series, the SWX2310 Series, the SWX2310P Series, the SWR2310 Series, the SWR2311P Series, the SWX3100 Series, the SWX3200 Series, SWX2320 Series, SWX2322P Series, SWX3220 Series, the WLX202, the WLX212, the WLX222, the WLX302, the WLX313, the WLX322, the WLX323, the WLX402 and the WLX413.

- **IP Address Settings**

This configures the IP address.

The IP address displayed are agentes at the time that the screen is displayed.

The IP address prior to making the settings may be shown, depending on the timing.

- **CONFIG Save/Restore/Delete**

Saves, restores or deletes the CONFIG.

This can be used for bulk operations on multiple agentes as well.

- **Specification method**

This sets the method of specifying the switch.

This can be configured on the SWX2200 Series as well.

### Setting and maintaining switches

In the "Tree view," press the "**Device**" icon of the Yamahaswitch, and in the "Device details and settings view," press the button(the name depends on the switch) to see a dialog box or setting screen.

Here you can make settings for the various functions of theswitch, and perform maintenance such as updating the firmware orrestarting. The items that can be set or viewed, and the maintenancelfunctions that can be executed, will differ depending on the model.

---

**【 For the SWX2300, SWX2310, SWX2310P, SWR2310, SWR2311P, SWX3100, SWX3200, SWX2320, SWX2322P and SWX3220 Series 】**

When you press the "**Open the GUI**" button, the web setting screen of the switch opens in another window.

**【 For the SWX222x Series, SWX2210 Series, SWX2210P Series 】**

Press the "**Switch settings and maintenance**" button to open the dialog box.

**• Device name**

Specify the device name of the switch.

- When "Default device name" is selected, the defaultnames that are predetermined for each device will be set. Normally, this is text that shows the model name and serial number.
- When "Manual settings" is selected, the devicename that was inputted in the input box right afterwards will be set. Input a device name of up to 32 single-byte characters. You can only use single-byte alphanumeric characters and symbols.

**• LED mode**

This lets you configure the LED mode settings.

**• Port mirroring**

This lets you configure the sniffer ports, monitor ports and monitoring direction.

**• QoS function**

This lets you specify whether QoS is used.

**• Maintenance**

The following can be executed for a switch.

- Reset the frame counter
- Restart

When you press the "**Open the GUI**" button, the web setting screen of the switch opens in another window.

**【 For the SWX2200 Series 】**

Press the "**Switch settings and maintenance**" button to open the dialog box.

**• Device name**

Specify the device name of the switch.

Input a device name of up to 32 single-byte characters. You can only use single-byte alphanumeric characters, hyphens (-) and underline characters (\_).

**• Power conservation**

The following settings can be made for the power-conservation function.

- Operation mode

**• Loop detection**

The following settings can be made for the loop detection function.

- MAC address movement number threshold
- Action when a loop is detected

- **Port mirroring**

The following settings can be made for the port mirroring function.

- Operation mode
- Sniffer port and monitoring direction

- **Maintenance**

The following can be executed for a switch.

- Reset the frame counter
- Resume supplying power (for a model that provides PoE)
- Update firmware
- Restart
- Initialize

### **[ For the SWX2110 Series, SWX2110P Series ]**

Press the "**Switch settings and maintenance**" button to open the dialog box.

- **Device name**

Specify the device name of the switch.

Input a device name of up to 32 single-byte characters. You can only use single-byte alphanumeric characters, hyphens (-) and underline characters (\_).

- **LED mode**

This lets you configure the LED mode settings.

- **Flow control**

This lets you specify whether the flow control function is used.

- **Loop detection**

This lets you specify whether the loop detection function is used.

- **EEE**

This lets you specify whether the EEE function is used.

- **Port mirroring**

This lets you configure the sniffer ports, monitor ports and monitoring direction.

- **QoS**

This lets you specify whether QoS is used.

- **IGMP snooping**

This lets you specify whether the IGMP snooping function is used.

- **Maintenance**

The following can be executed for a switch.

- Reset the frame counter
- Update firmware
- Restart
- Initialize

**【 For the SWX2100 Series 】**

Press the "**Switch settings and maintenance**" button to open the dialog box.

- **Device name**

Display the device name of the switch.

- **Port common settings**

Display common settings for the ports.

- **Link aggregation settings**

Displays the link aggregation type and load balance rules.

This item is shown only for the SWX2100-24G.

- **Maintenance**

The following can be executed for a switch.

- Reset the frame counter
- Update firmware
- Restart

### **Making port settings for a switch**

In the tree view, press the "**Device**" icon corresponding to the Yamaha switch; and on the detailed image of the device in "Device details and settings view," select a port and press the "**Port settings**" button to display the port settings dialog box. If a port is not selected in the detailed image of the device in "Device details and settings view," you will not be able to configure the port settings. The port settings can be changed on the Smart L2 switch, SWX2110 series, and SWX2110P series.

**【 For the SWX222x Series, SWX2210 Series, SWX2210P Series 】**

The port settings dialog box appears.

- **Basic**

The following settings can be made for basic functions.

- Port operation
- Automatic cross/straight detection
- Speed
- Flow control
- EEE

- Loop detection

- **QoS**

The following settings can be made for QoS.

- Trust mode
- Remarking of received packets
- Remarking value

- **Tag VLAN**

The following settings can be made for tag VLAN.

- Operation mode
- Access VLAN ID or native VLAN ID
- Trunk VLAN ID

For ports joined to a logical interface, configure the settings from the link aggregation settings.

- **Multiple VLAN**

The following settings can be made for multiple VLAN.

- Joined group

For ports joined to a logical interface, configure the settings from the link aggregation settings.

### **【 For the SWX2200 Series 】**

The port settings dialog box appears.

- **Basic**

The following settings can be made for basic functions.

- Port operation
- Automatic cross/straight detection
- Speed
- Link speed downshift
- Flow control
- Loop detection

- **QoS**

The following settings can be made for QoS.

- DSCP remarking
- Transmit shaping
- Receive policing
- Port priority

- **Tag VLAN**

The following settings can be made for tag VLAN.

- Operation mode

- Access VLAN ID
- Trunk VLAN ID

- **Multiple VLAN**

The following settings can be made for multiple VLAN.

- Joined group

- **Frame counter**

The following settings can be made for the frame counter.

- Transmitted frame
- Received frame

- **Power supply function (for a model that provides PoE)**

The following settings can be made for the power supply function.

- PoE supply class settings

### **【 For the SWX2110 Series, SWX2110P Series 】**

The port settings dialog box appears.

- **Basic**

The following settings can be made for basic functions.

- Port operation
- Automatic cross/straight detection
- Speed
- L2MS filter

- **Tag VLAN**

The following settings can be made for tag VLAN.

- Operation mode
- Access VLAN ID or native VLAN ID
- Trunk VLAN ID

### **Performing power supply operations for the switch port**

In the tree view, press the "**Device**" icon corresponding to the Yamaha switch; and on the detailed image of the device in "Device details and settings view," select a port and press the "**Port power supply operation**" button to display the port power supply settings dialog box. If a port is not selected in the detailed image of the device in "Device details and settings view," and the selected port does not support power supply, you will not be able to perform power supply operations with this port. Power supply settings can be configured for each port from the port power supply operation dialog.

This can be set only on the SWX2100-10PoE, the SWX2100-5PoE, the SWX2110P-8G, the SWX2210P Series, the SWX2221P-10NT, the SWX2220P Series, the SWX2310P Series, the SWR2311P Series, and the SWX2322P Series.

### **Configuring the link aggregation settings**

In the tree view, press the "**Device**" icon corresponding to the Yamaha switch; and press the "**Link aggregation settings**" button in "Device details and settings view" to display the link aggregation settings dialog box. This lets

you configure settings regarding linkaggregation, add a logical interface or configure the VLAN settings and so on.

**This can be set only on the SWX222x Series, and the SWX2210 Series, SWX2210P Series.**

- **Link aggregation and load balancing rules**

This lets you configure the load balancing rule settings.

- **Interface settings**

The following settings can be made for the logical interface.

- **Link aggregation**

The following basic settings can be made.

- Logical interface name
- Joined port
- Interface action

- **Tag VLAN**

The following settings can be made for tag VLAN.

- Operation mode
- Access VLAN ID or native VLAN ID
- Trunk VLAN ID

- **Multiple VLAN**

The following settings can be made for multiple VLAN.

- Joined group

## Wireless AP settings

In the "Tree view," press the **"Device" icon** of a Yamaha wireless AP, and in "Device details and settings view," press the **"Open the GUI" button** to view the web settings screen of the Yamaha wireless AP in a separate window. Settings for the Yamaha wireless AP can be made from the websettings window.

## Find this switch

The "Find this switch" function uses LED and buzzer to notify the user of the device's location in an easy-to-understand way.

Press the "Device" icon of a Yamaha switch in the "Tree view" and then press the "Find this switch" button in "Device details and settings view" to display the dialog.

Note that this function is available only for the SWX222x series.

- The dialog shows the current operating status.  
There is a Start/Stop button on the right side that allows you to start or stop the notification.
- Notification start dialog  
You can start notification by selecting the notification method and the notification period.  
Select one or more notification methods.
  - Blink the LED
  - Sound the buzzer

- Notification stop dialog  
You can stop any notification method.

---

## Tag VLAN

### Summary

You can create VLANs to organize Yamaha switches or Yamaha wireless APs into groups.

### Tagged VLANs can be set for the following agents.

- Yamaha network switch
  - SWX2110-5G, SWX2110-8G, SWX2110-16G, SWX2110P-8G
  - SWX2200-8G, SWX2200-24G, SWX2200-8PoE
  - SWX2210P-10G, SWX2210P-18G, SWX2210P-28G
  - SWX2210-8G, SWX2210-16G, SWX2210-24G
  - SWX2220-10NT, SWX2220-18NT, SWX2220-26NT
  - SWX2221P-10NT, SWX2220P-18NT, SWX2220P-26NT
  - SWX2300-8G, SWX2300-16G, SWX2300-24G
  - SWX2310P-10G, SWX2310P-18G, SWX2310P-28GT
  - SWX2310-10G, SWX2310-18GT, SWX2310-28GT, SWX2310-52GT
  - SWR2311P-10G
  - SWR2310-10G, SWR2310-18GT, SWR2310-28GT
  - SWX3100-10G, SWX3100-18GT
  - SWX3200-28GT, SWX3200-52GT
  - SWX2320-16MT, SWX2322P-16MT, SWX3220-16MT, SWX3220-16TMs
- Yamaha wireless access point
  - WLX202
  - WLX212
  - WLX222
  - WLX302
  - WLX313
  - WLX322
  - WLX323
  - WLX402
  - WLX413

### Notes

- If a switch of a different manufacturer is connected below a manager, the manager will be unable to recognize the corresponding device, and the topology will therefore not be displayed. If communication from the terminal becomes impossible even though the tag VLAN settings are correct, it might be that a switch made by another manufacturer which is blocking VLAN tagged frames is connected below the manager.
- If a Yamaha switch of a model that cannot be determined is connected below the manager, it might be that the VLAN tagged frames cannot pass through that device, depending on the settings of that device.
- Configurations that include MST instances in the spanning tree are not supported.

## Tag VLAN page structure

### Button

-  **New button**

Create a new VLAN group.

In order to join a port to a VLAN group, the VLAN group must first be created.

-  **Refresh display button**

Obtain topology information and VLAN settings information, and redraw the tag VLAN group list and the topology.

Depending on the number of agent units, it may take several seconds to several tens of seconds for the agent VLAN settings information to be reflected.

### Tag VLAN group list

Display the list of VLAN groups that are registered to the manager, and the list of VLAN groups that the agent ports have joined.

However, the list does not show private VLANs or VLAN groups for which frame forwarding is disabled. The port color is assigned to each VLAN group.

### Topology

The topology starting at the manager is shown in the lower part of the screen.

By noting the color of the port, you can determine the VLAN group to which it is joined.

### Make tag VLAN group settings

#### Create new

To create a new VLAN group, press the  **"New" button**. The following settings can be made.

Item name	Description
VLAN-ID	Set the ID of the VLAN.
Name	You can assign a name to the VLAN ID.

After input, press the **"OK" button** to register the VLAN group.

#### 4-2. Change settings

If you want to change the VLAN group settings, press the **"Settings" button** located in the column at the right of the **"Tag VLAN group list"**.

You can edit the name setting.

#### 4-3. Register

If a agent port is joined to a VLAN group that is not registered to a manager, it is shown as an "Unknown" VLAN group in **"Tag VLAN group list"**.

By pressing the **"Register" button** located in the column at the right of **"Tag VLAN group list"**, you can register a VLAN group to a manager.

## Delete

If you want to delete a VLAN group, press the **"Delete" button** located in the column at the right of the **"Tag VLAN group list"**.

Then press the **"OK" button** to delete the settings of the specified VLAN group and also delete the settings of the VLAN group that is applied to the agent.

## Join a tag VLAN group

To select a agent port within the topology, press the **"Select joined port" button** in the right column of **"Tag VLAN group list"**.

The color of the port indicates the setting status of the VLAN group.

The following is a depiction of when the port color is set to

for a VLAN group when selecting the joined ports.

LAN	SFP	Description
		This is an access port that is joined to the specified VLAN group.
		This is an access port that is joined to the default VLAN group.
		This is an access port that is joined to the specified VLAN group. To determine the joined VLAN group, note the color of the port that is assigned in "Tag VLAN group list".
		This is a trunk port or hybrid port. This is joined to the specified VLAN group.
		This is a trunk port or hybrid port. This is not joined to the specified VLAN group.

When you select a port, the color of the port changes, allowing you to join it to the specified VLAN group.

By re-selecting a port, you can un-join it.

When operating the VLAN join status of the port that belongs to the logical interface, the same settings will be applied to all ports belonging to the same logical interface.

After selecting a port, press the **"OK" button** to apply the setting.

- If a Yamaha switch of a model that cannot be determined is disconnected, it might be that the VLAN tagged frames cannot pass through that device, depending on the settings of that device.
- **Automatically joining uplink ports and downlink ports**

If you join a port to a VLAN group, the port that connects from the manager to the corresponding agent (uplink/downlink) will automatically be either a trunk port or a hybrid port.

- **Constraints when joining a VLAN group**

The following constraints apply when making SWX2300 Series, SWX2310 Series, SWX2310P Series, SWR2310 Series, SWR2311P Series, SWX3100 Series, SWX3200 Series, SWX2320 Series, SWX2322P Series, SWX3220 Series settings.

- If the specified VLAN group is used as a private VLAN by agent, a port of the corresponding agent cannot be joined to the specified VLAN group.
- If a port is specified as a private VLAN's promiscuous port, or as a host port, settings for that port cannot be made.
- If a port is used by the link aggregation function, settings for that port cannot be made. (only SWX2300 Series)

Also, you cannot change the stack port settings for devices in a stack configuration.

### Show tag VLAN group settings

In "Tag VLAN group list", colors are assigned to the ports for each VLAN group. By noting the color of a agent port in the topology, you can see the VLAN group to which it is joined.

Examples are shown below.

LAN	SFP	Description
		This is an access port that is joined to a VLAN group other than the default VLAN. To determine the joined VLAN group, note the color of the port that is assigned in "Tag VLAN group list".
		This is a trunk port or hybrid port.
		This is an access port that is joined to the default VLAN group.

You can also check the tag VLAN group settings from the tool tip that appears when you mouse-over. The items shown in the tool tip are as follows.

- Port number
  - For logical interfaces, the logical interface name and thenumbers of all ports belonging to the logical interface will be shown.
  - **saX** is the name of the logical interface for a static link aggregation.
  - **poX** is the name of the LACP virtual interface.
- Port type ( Access, Trunk, Hybrid )
- VLAN group joined

Supplementary information related to SWX2300 Series, SWX2310 Series,SWX2310P Series, SWR2310 Series, SWR2311P Series, SWX3100 Series,SWX3200 Series, SWX2320 Series, SWX2322P Series, SWX3220 Series settings is shown below.

- **About native VLAN**

The uplink/downlink ports are the trunk ports, and the defaultVLAN is specified as the native VLAN. If the frame received by the trunk port is untagged, the native VLAN is the VLAN group joined by untaggedframes.

- **About promiscuous ports and host ports of a private VLAN**

If the port is specified as a private VLAN's promiscuous port or a host port, the port type in the tool tip is shown as "Private," and the joined VLAN group is not shown.

## Multiple VLAN

### Summary

You can divide the ports of a single switch into multiple groups, and block communication between groups. In addition to grouping ports into multiple groups, a single port can also be joined to multiple groups. For example, a port that is connected to a terminal that must communicate with all groups, such as a server or router, would be joined to each and every group.

For multiple VLANs, the same IP address is assigned even if the group is different.

The agents for which a multiple VLAN can be set, as well as the maximum number of groups that can be set for each agent on this page are shown below.

Supported agents	Maximum number of groups
SWX2200-24G	24
SWX2200-8G	8
SWX2200-8PoE	8
SWX2210-24G	24
SWX2210-16G	16
SWX2210-8G	8
SWX2210P-28G	28
SWX2210P-18G	18
SWX2210P-10G	10
SWX2220-10NT SWX2221P-10NT	10
SWX2220-18NT SWX2220P-18NT	18
SWX2220-26NT SWX2220P-26NT	26
SWX2310P-28GT SWX2310P-18G SWX2310P-10G	256
SWX2310-52GT SWX2310-28GT SWX2310-18GT SWX2310-10G	256
SWR2311P-10G	256
SWR2310-28GT SWR2310-18GT SWR2310-10G	256
SWX3100-18GT SWX3100-10G	256

SWX3200-52GT SWX3200-28GT	256
SWX2320-16MT SWX2322P-16MT SWX3220-16MT SWX3220-16TMs	256

### Multiple VLAN page structure

The multiple VLAN page consists of three views: tree view, multiple VLAN settings view, and connected devices view.

#### Tree view

These are the same as shown in the map.

The agent topology starting at the manager is shown in the lower left of the screen. Network devices of other manufacturers are not shown. In the "Tree view," press the **"Devices" icon** to see device information in the "Connected devices view". If a agent that supports multiple VLANs is selected, settings are shown in "Multiple VLAN settings view".

#### Multiple VLAN settings view

The multiple VLAN settings of the agent selected in "Tree view" are shown. This is not shown if a manager or agent that does not support multiple VLANs is selected in "Tree view".

- **List of multiple VLAN group settings**

The status of the joined ports for each group of the multiple VLAN are shown in the form of a table. The horizontal direction of the table shows the ports, and the vertical direction shows the groups.

In the table, you can press the  **Port icon** to change the port join status of the corresponding group. A **Port icon** that is in the joined state will change to the color that corresponds to the group (example: ). If you once again press a port icon that is in the joined state, it returns to the non-joined state.

Pressing the **"Port number" button** in the upper edge of the table will select the ports of all groups in the Port column, and pressing the **"Group number" button** in the left edge of the table will select all ports in the Group line. By pressing the **"↘" button** in the upper left of the table, you can select diagonally staggered ports from the upper left.

Ports that are not disabled will not be changed status by any specify method.

All ports that belong to the logical interface will be shown together, as displayed on the right side of the table. The logical interface type and number will be shown as a two-row label above the port numbers.

The logical interface type (sa or po) is shown on the upper row, and the interface number is shown on the bottom row.

Static link aggregation is shown for "sa", and LACP link aggregation is shown for "po".

When operating the group join status of the ports that belong to the logical interface, the same settings will be applied to all ports belonging to the same logical interface.

- **Ports/groups to display**

Move the slider on the bar to change the ports and groups shown on the screen.

The upper bar is for ports, and the lower bar is for groups.

The left-hand slider changes the minimum value, and the right-hand slider changes the maximum value.

- **Minimized view**

Select the check box to display a minimized view of the port and group icons.

When using the minimized view, the arrows for port uplinks and downlinks will not be displayed.

- **"Return all groups to the state prior to the change" button**

Return the ports joined to the multiple VLAN to the state prior to the change.

- **"OK" button**

Apply the settings of the ports joined to the multiple VLAN.

These settings will also apply to ports that are hidden.

The "Multiple VLAN group setting list" can be switched between displayed and hidden by pressing the  button in the upper left.

**The contents of the settings for a previously-specified multiple VLAN group are shown by the switch graphic in the lower part of "MultipleVLAN settings view".**

- **Group select pulldown menu**

Select the multiple VLAN group that is shown by the switch image at the right side.

- **Switch image**

Ports that are joined to the group currently selected in the group select pulldown menu are shown.

### **Connected devices view**

These are the same as shown in the map.

Devices that are connected to the manager or agent selected in the "Tree view" are shown in the lower right of the screen. If "Devicemanagement" is not enabled in "LAN map settings," terminal information (e.g., PC or mobile devices) is not shown.

If a switch is selected as a agent, you can check the type of device that is connected to each port of the switch, and use this as a reference when making multiple VLAN group settings.

- **Acquisition date**

This is the time at which information was last obtained for equipment that is connected to the manager or agent selected in the "Tree view". This is not shown if "Device management" is not enabled in "LAN map settings".

- **Select page**

Page numbers are shown for the list of currently-displayed terminals. Press  or  or enter a numeric value to move between pages.

-  **Acquire button**

This obtains information for terminals that are connected to the manager or agent selected in the "Tree

view". This is not shown if "Device management" is not enabled in "LAN map settings".

- **List**

Information is listed for equipment that is connected to the manager or agent selected in the "Tree view".

You can press each item's  **Sort switch** to sort the list. The initial screen is sorted in order of port.

The VLAN ID item shows (A) for an access VLAN or (T) for a trunk VLAN.

If the port is being used as a port for a private VLAN, the VLAN ID is not shown, and (P) is shown.

If the port is being used as a port for a voice VLAN, the VLAN ID is not shown, and (V) is shown.

### Making settings for multiple VLAN groups

To make multiple VLAN group settings, first select the switch that you want to set from the "Tree view". When you make a selection, the "Multiple VLAN group settings list" appears in the "Multiple VLAN settings view".

When the "Multiple VLAN group settings list" appears, select the ports that you want to join to each group by pressing the corresponding **Port icon**. When making settings, refer to the following tips.

When you finish selecting the ports to join, press the **"OK" button** to apply the settings to the switch and complete the settings.

### Tips when selecting multiple VLAN settings

- You want to select ports efficiently

By using the **"Port number" button** in conjunction with the **"↘" button** you can select ports efficiently. You can use the **"Port number" button** to allow a specific port to communicate with all other ports. For example, the uplink port normally needs to be able to communicate with all other ports, so it is joined to all groups; by pressing the **"Port number" button** in the column of the uplink port, you can avoid the trouble of selecting them individually.

Use the **"↘" button** when you want to join each port to a different group. For example, if you want to block all communication between each downlink port, and allow communication only with the uplink port, press the **"Port number" button** and **"↘" button** in the uplink port column; each group is joined to the uplink port and to one downlink port, allowing you to easily obtain the desired settings. Such settings are often used for a network in an Internet-equipped apartment building.

- When you want to restrict the ports and groups to configure

Adjust the bars for the **"Ports/groups to display"** to show only the ports and groups that you need.

- You want to re-do the settings

By pressing the **"Return all groups to the state prior to change" button** you can return the joined port selection state to the state prior to change.

### Showing settings for multiple VLAN groups

Multiple VLAN groups that have already been specified are indicated by the switch graphic that is shown at the bottom of the "Multiple VLAN settings view". From the pulldown at the left, select the group that you want to check; the ports that are joined to that group change to the color corresponding to the group.

The contents of the settings shown here are the settings that have been actually applied to the switch by pressing the **"OK" button**. The content that is currently being edited in the "Multiple VLAN group settings list" is not reflected in the display.

## Device list

### Summary

In the device list you can view a list of the terminals and agents managed in the LAN map, and use the terminal DB to centrally manage terminal information.

### Terminal list

The terminal list page is explained here.

### Summary

The terminal list page shows a list of the terminals that are managed by the LAN map. You can use the list to check the time that a terminal was detected or the time that it was lost. You can also edit terminal information in the list, or register it to the terminal DB.

### About the buttons

-  **"Delete" button**

Delete information of the selected lost terminal from the terminal list.

-  **"Refresh display" button**

Refresh the terminal list page.

- **"Save as CSV" button**

Save the terminal list as a CSV file.

- **"Edit" button**

Edit terminal information. Edited information is registered in the terminal DB.

### Checking terminal information

In the list you can check the terminal information that is managed by the LAN map. You can press each item's  **Sort switch** to sort the list. The initial screen is sorted in order of route. Lost terminals are shown highlighted in  gray.

The VLAN ID item shows (A) for an access VLAN or (T) for a trunk VLAN.

If the port is being used as a port for a private VLAN, the VLAN ID is not shown, and (P) is shown.

If the port is being used as a port for a voice VLAN, the VLAN ID is not shown, and (V) is shown.

### Editing terminal information and registering it to the terminal DB

You can edit the information for the terminals that are managed by the LAN map. Edited information is registered in the terminal DB. Press the **"Edit" button** of the terminal information that you want to edit, and then edit the information. You can edit the following items.

- Type

Select the type from the selection menu.

\* This is shown as an icon in the map page and multiple VLAN page "Connected device view".

- **Manufacturer**

Enter the manufacturer name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- **Model name**

Enter the model name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- **Device name**

Enter the device name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- **OS**

Enter the OS name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- **Comment**

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- **Snapshot**

Select whether the terminal is or is not included in monitoring for the snapshot function.

\* Terminal information that has been registered can also be edited from the terminal DB page..

Note: When inputting "" or "," for parameters where text is inputted, the maximum number of allowable characters will be less than 128.

### Deleting a lost terminal

You can delete information of a lost terminal from the terminal list. Select the lost terminal information that you want to delete, and press the  **"Delete" button**. The lost terminal information that you selected is deleted.

### Saving a list to a CSV file

You can save the terminal list as a CSV file. Press the **"Save as CSV" button**. The terminal list is saved as a CSV file.

### Terminal DB

The terminal DB page is explained here.

### Summary

The terminal DB page shows a list of the terminals that are registered in the terminal DB. You can newly register, edit, or delete terminal information, and import or export terminal DB settings.

### About the buttons

-  **"Delete" button**

---

Delete the selected terminal information from the terminal DB.

-  **"Register new" button**

Newly register terminal information in the terminal DB.

-  **"Refresh display" button**

Refresh the terminal DB page display.

-  **"Import" button**

Apply the terminal DB saved on the PC to the manager.

-  **"Export" button**

Save the terminal DB as a CSV file.

- **"Edit" button**

You can edit the terminal information that has been registered in the terminal DB.

### Checking terminal information

You can identify the terminal DB in the list. You can press each item's  **Sort switch** to sort the list. The initial screen is sorted in order of MAC address.

### Registering new terminal information

You can newly register terminal information in the terminal DB. Press the  **"Register new" button**, and enter the content to be registered. You can register the following items.

- MAC address

Enter the MAC address of the terminal.

Enter single-byte characters delimited by a ":" (example: 00:a0:de:00:00:00).

- Type

Select the type from the selection menu.

\* This is shown as an icon in the map page and multiple VLAN page "Connected device view".

- Manufacturer

Enter the manufacturer name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- Model name

Enter the model name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- Device name

Enter the device name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- OS

Enter the OS name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- Comment

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- Snapshot

Select whether the terminal is or is not included in monitoring for the snapshot function.

### Editing terminal information

You can edit the terminal information that has been registered in the terminal DB. Press the **"Edit" button** of the terminal information that you want to edit, and then edit the information. You can edit the following items.

- Type

Select the type from the selection menu.

\* This is shown as an icon in the map page and multiple VLAN page "Connected device view".

- Manufacturer

Enter the manufacturer name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- Model name

Enter the model name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- Device name

Enter the device name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- OS

Enter the OS name.

Enter up to 128 single-byte alphanumeric characters or single-byte symbols.

- Comment

- Snapshot

Select whether the terminal is or is not included in monitoring for the snapshot function.

---

## Deleting terminal information

You can delete the selected terminal information from the terminalDB. Select the terminal that you want to delete, and press the  **"Delete" button**. The selected terminal information is deleted.

## Importing a terminal DB

Apply the terminal DB saved on the PC to the manager. Press the  **"Import" button**, and use the **"Select a file" button** to select the terminal DB. The selected terminal DB is applied to the manager.

When directly editing the terminal DB, use no more than 128 single-byte alphanumeric or symbol characters for each item.

A character string that includes multi-byte characters is detected as an empty character string, and a character string that exceeds 128 characters is truncated at 128 characters.

## Exporting a terminal DB

You can save the terminal DB as a CSV file. Press the  **"Export" button**. The terminal DB is saved as a CSV file.

## Agent list

The agent list page is explained here.

## Summary

The agent list page shows a list of the agents that are managed by the LAN map. You can use the list to check the time that an agent was detected or the time that it was lost. You can also change the settings of an agent in the list.

## About the buttons

-  **"Delete" button**

Delete information of the selected lost agent from the agent list.

-  **"Refresh display" button**

Refresh the agent list page display.

- **"Save as CSV" button**

Save the agent list as a CSV file.

- **"Settings" button**

Make agent settings.

## Checking an agent

In the list you can check the agent information that is managed by the LAN map. You can press each item's  **Sort switch** to sort the list. The initial screen is sorted in order of route. Lost agents are shown highlighted in  gray.

---

## Making agent settings

You can edit the settings for the agents that are managed by the LAN map. Settings can be changed on some Yamaha switches. Press the **"Settings" button** of the agent whose settings you want to change, and then change the settings. You can set the following items.

- Device name

Specify the device name of the agent.

- When "Default device name" is selected, the default names that are predetermined for each device will be set. Normally, this is text that shows the model name and serial number.
- When "Manual settings" is selected, the device name that was inputted in the input box right afterwards will be set. Input a device name of up to 32 single-byte characters. The characters that can be input will differ depending on the target agent. See "6-2. Setting and maintaining switches" in "Map" for details.

## Deleting a lost agent

You can delete information of a lost agent from the agent list. Select the lost agent information that you want to delete, and press the  **"Delete" button**. The lost agent information that you selected is deleted.

## Saving a list to a CSV file

You can save the agent list as a CSV file. Press the **"Save as CSV" button**. The agent list is saved as a CSV file.

## Whole map

### Summary

The whole map shows all devices connected to the network, using a single topology. You can switch the topology display range and the device information view, to customize the display and make it easier to view. Use the print function to print the whole map displayed, in order to make use of the map in various network operation management-related situations.

### Notes

- Cookies are used and saved for the whole map view settings. Enable cookies on your browser to save the whole map view settings. See the help content supplied with your browser for instructions on how to enable cookies. If you have made changes to the settings but the changes are not reflected when accessing the whole map once more, cookies may be disabled or have been deleted in your browser.
- You can confirm the link speed between devices (the link speed of the port belonging to higher devices) and link speed, by checking the color and shape of the connector lines between the device icons.
  - See the legend at the top right of the screen for how the colors correspond to link speeds.
  - The link speeds of terminals connected to a Yamaha wireless AP or agents for which the type cannot be determined are shown using gray-colored connector lines.

### About the buttons

-  "Top" button

Used for the focus function. See [Using the focus function](#) for details.

-  "Up" button

Used for the focus function. See [Using the focus function](#) for details.

-  "Refresh display" button

The page will reload.

-  "View settings" button

Here you can configure the information shown on the whole map. For details, see "[Switching the device information view](#)", "[Displaying/hiding a terminal](#)" and "[Switching the port information view](#)."

-  "Print preview" button

This opens the screen for printing. See "[Printing the whole map](#)" for details.

### About the mini whole map

The mini whole map is a reduced version of the whole map. Use this to get a birds'-eye view of the entire map. You can also use the focus function to understand which agent is getting the focus. See [Using the focus function](#) for details.

Note: If the total number of managers, agents and SSIDs on the whole map exceed 200, the mini whole map will not be displayed.

### Switching the device information view

You can switch the device information shown on the right-hand side of the device icons. You can set the items to be displayed for the agents and terminals individually. Use the following operations to configure the settings.

1. Press the  **"View settings" button** at the upper right-hand part of the screen. The view settings screen will display directly below.
2. Select the items to view using the drop-down list boxes to the right of the "agent information" and "terminal information" on the view settings screen. When these items are selected, the device information shown at the right of the device icons on the whole map will switch to the selected item. The settings will automatically be saved at the timing in which they are switched.

Note: The four drop-down list boxes are lined up vertically corresponding to the order in which the device information to the right of the device icons on the whole map is displayed.

#### **Agent information to view can be selected from the following.**

- Device name
- MAC address
- Model name
- IP address
- Hide

#### **Terminal information to view can be selected from the following.**

- IP address
- Manufacturer
- Device name
- MAC address
- Model name
- Comment
- OS
- Hide

Note: Up to 30 single-byte characters are displayed for the device information. If the text length exceeds 30 single-byte characters, the rest of the item will be omitted.

#### **Displaying/hiding a terminal**

You can switch between displaying or hiding terminals shown on the whole map. If you do not need to manage terminals, you can hide the terminals and show only the agents, making the view easier to read. Use the following operations to configure the settings.

1. Press the  **"View settings" button** at the upper right-hand part of the screen. The view settings screen will display directly below.
2. Select the check box to the left of the "Terminal information" text on the view settings screen to display the terminal, and deselect the check box to hide the terminal. The settings will automatically be saved at the timing in which they are switched.

#### **Switching the port information view**

You can switch between displaying or hiding the connecting port and VLAN information shown on the topology of the whole map. Use the following operations to configure the settings.

1. Press the  **"View settings" button** at the upper right-hand part of the screen. The view settings screen will display directly below.
2. Select the check boxes in "Port information" on the view settings screen for the "Port number" and "VLAN-

ID" to view this information, and deselect the check boxes to hide the information. These settings will automatically be saved at the timing in which they are switched.

### Using the focus function

Press the agent icon on the whole map for a focused view of the topology, including the selected agents and the devices that they control.

Focusing on this view will enable the  **"Top" button** and the  **"Up" button** in the top left part of the screen. Press the  **"Top" button** to return to a view of the overall topology, centered on the manager. Press the  **"Up" button** on the top left part of the screen to view the topology, centered on the agents or managers one level above. The agents that are at the center of the topology's focus are shown within a blue border on the mini whole map at the right side of the screen, which helps you to understand their location. You can also view the "Route" in the upper left part of the screen to confirm the location of an agent.

### Printing the whole map

Using the whole map, you can print the currently viewed whole map from the Print preview. Use the following operations to print.

1. Press the  **"Print preview" button** at the upper right part of the screen. The Print preview will display in a separate window.
2. Check the Print preview and press the **"Print this page" button** on the upper part of the screen if everything looks the way you want it. The browser's print preview will be displayed. Set the paper size to A4 or larger when printing.

Note: When changing the focus or device information view after displaying the Print preview, close the Print preview first, make changes to the focus or device information view on the whole map, and then press the  **"Print preview" button** again to open the Print preview. The settings cannot be changed from the Print preview.

Note: When opening an agent configuration series for a topology that is long (in other words, a topology that is too wide to fit) in the Print preview, the width of the topology on the Print preview will be adjusted to horizontally accommodate A4-sized paper.

### Checking the terminals connected to wireless AP

The terminals connected to a wireless AP will be shown for each SSID on the whole map.

Note: Some devices connected to a wireless AP may not display, depending on the firmware version of the wireless AP.

The SSIDs that are set for the wireless AP are shown as icons under the wireless AP icon. Terminals connected by an SSID are displayed under their respective SSID icon. The following information regarding the SSID is displayed to the right of the SSID icon.

- SSID name
- Frequency band

Note: The items displayed cannot be switched.

---

# ProAV settings

## ProAV profile

### Summary

The ProAV Profile page can be used to configure all settings for optimizing the AVoIP network that carries audio and video traffic.

In this unit, following ProAV profiles can be configured.

- Dante
  - Dante is an audio networking solution developed by Audinate for professional audio applications. A single LAN cable is used to bi-directionally communicate information necessary for digital audio systems, such as for transmitting multiple channels of audio signals, clock synchronization signals, and control signals.
- NDI
  - NDI is a new protocol developed by Newtek that supports live video production workflows within IP applications. It enables real-time interactive transmission of video, audio, meta data, and other information within typical Gigabit Ethernet environments.

For details on the commands configured by a ProAV profile, refer to [Yamaha Network Devices Technical Documentation](#).

## How to use this page

### Introduction

This page can be used as a kitting tool for configuring optimal AVoIP network settings. QoS, multicast control, and other settings can all be set to optimal values at the same time by simply selecting a ProAV profile.

The ProAV profile configured on this page assumes the unit will be used as a dedicated switch for an AVoIP network.

If building a complex network, such as by combining an AVoIP network with an existing internal network, specify appropriate settings on the GUI Details settings page or by using commands.

This page assumes that an IP address is assigned to VLAN1.

If VLAN1 is not assigned an IP address, assign an IP address to VLAN1 and access the web GUI from a port associated to VLAN1.

The VLAN1 IP address is already specified in factory default settings, so the setting does not need to be changed before use.

Note that the ports that belong to a logical interface must be removed from the logical interface.

If necessary, remove ports from the logical interface, assign a profile, and then reassign ports to the logical interface.

### Set Dante profile

The Dante optimization settings is applied.

In a Dante network, settings vary depending on the network structure.

### Use as Dante primarily dedecated line



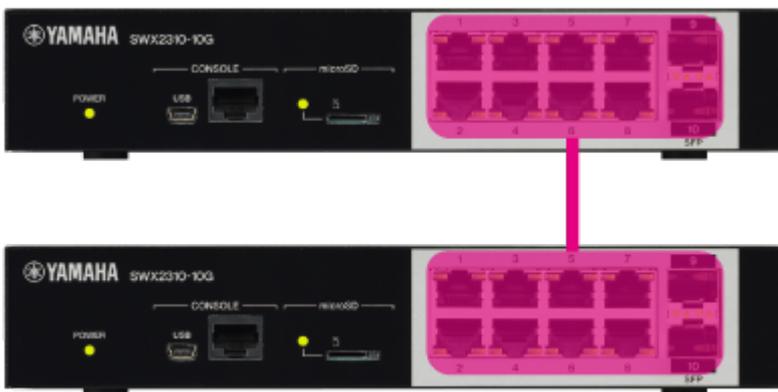
#### Dante primary

Select this network structure when the switch is used as a Dante dedicated primary line.

Assign all ports to the same network and apply the Dante primary profile.

Note that the only differences from selecting "Use as Dante SecondaryDedicated Line" are the profile name and color settings. All othersettings are the same.

### Use as Dante secondary dedecated line



#### Dante secondary

Select this network structure when the switch is used as a Dante dedicated secondary line.

Assign all ports to the same network and apply the Dante secondary profile.

Note that the only differences from selecting "Use as Dante PrimaryDedicated Line" are the profile name and color settings. All othersettings are the same.

### Bundle Dante primary/secondary lines



---

 Dante primary

 Dante secondary

 Trunk

Select this network structure when the primary and secondary lines are bundled together for connecting a single LAN cable between switches.

Separate the network between the primary line and the secondary line, and apply a Dante profile to both networks.

The settings applied are the same for the primary and secondary lines.

The trunk port sends and receives both Dante primary and secondary traffic bundled together.

Designate the ports used to connect to other switches and the corresponding ports on the connected switches as trunk ports.

To change the default primary, secondary, and trunk assignment settings, the Horizontal and Vertical buttons can be used to toggle between vertical and horizontal partition configurations in default settings.

The Horizon button does not appear on models with a single row of ports.

Primary, secondary, and trunk assignments can be changed manually by clicking on the profile selection button and then clicking on the port.

Since the GUI cannot be accessed from the secondary ports, assign the primary profile or trunk status to the port used to connect the computer to the GUI.

#### Redundant Dante primary/secondary lines



 Dante primary

 Dante secondary

Select this network structure when configuring redundant primary and secondary lines and using two LAN cables to connect between switches.

Separate the network between the primary line and the secondary line, and apply a Dante profile to both networks.

The settings applied are the same for the primary and secondary lines, but in this network configuration, an L2MS filter is applied to ports on the secondary line to prevent loops.

Note that L2MS agents connected only to a Dante secondary port will not be detected by the LAN map or Yamaha LAN Monitor.

To change the default primary and secondary assignment settings, the Horizontal and Vertical buttons can be used to toggle between vertical and horizontal partition configurations in default settings.

---

The Horizon button does not appear on models with a single row of ports.

Primary and secondary assignments can be changed manually by clicking on the profile selection button and then clicking on the port.

Since the GUI cannot be accessed from the secondary ports, assign the primary profile to the port used to connect the computer to the GUI.

### **Set NDI profile**

The NDI optimization settings is applied.

Assign all ports to the same network and apply the NDI profile.

### **Set multiple ProAV profiles**

Multiple ProAV profiles can be applied by partitioning the network using VLANs.

With default settings, VLAN1 is assigned to the Dante primary line,VLAN2 to the Dante secondary line, and VLAN3 to the NDI network.

Traffic for all selected profiles is sent/received via the specified trunk port.

Designate the ports used to connect to other switches and the corresponding ports on the connected switches as trunk ports.

The VLAN1 is set as the native VLAN (untagged) and other VLANs are set as the tagged VLAN.

As a precaution, when connecting the switch to another switch on a trunk,be sure to set the same Profile-VLAN assignment settings in bothswitches.

The VLAN assignment for a profile can be changed using the "Change VLAN" button.

Note that VLAN1 must be assigned to one of the profiles.

Profile assignments to ports can be changed manually by clicking on the profile selection button and then clicking on the port.

Since the GUI cannot be accessed from ports not affiliated with VLAN1 (\*),assign the VLAN1 profile or trunk status to the port used to connect the computer to the GUI.

\* This page assumes that an IP address is assigned to VLAN1.

### **Return to defaults**

Press the "Return to defaults" button to initialize the settings of all VLANs for which a profile is set, and all ports will be assigned toVLAN1.

Note that the settings of VLANs for which no profile is set will not be initialized.

### **Trademark attributions**

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

# Multicast

## Summary

The Multicast page can be used to configure IGMP snooping and check the IGMP snooping operating status separately for each ProAV profile.

If multicasting via an AVoIP network, it is generally recommended that IGMP snooping be enabled, but that can lead to trouble if operated with improper settings.

By learning the basic principles of IGMP snooping, this page can be used for simple troubleshooting of IGMP snooping issues.

## What's IGMP snooping

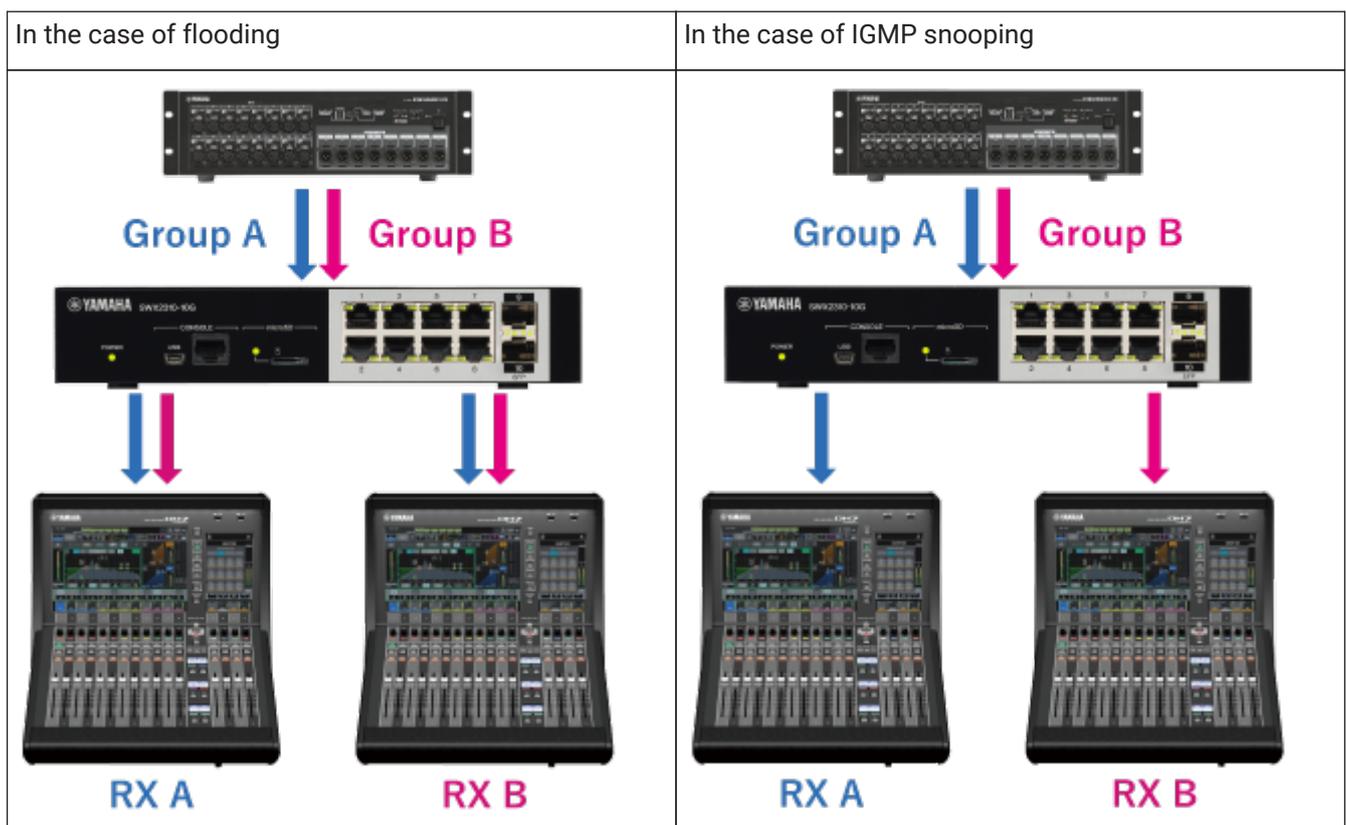
IGMP snooping is a feature that prevents unnecessary multicast traffic from being forwarded.

Normally, multicast traffic is flooded to all affiliated ports in the same network, which wastes bandwidth by forwarding multicast traffic to ports where no multicast receiving terminal exists.

In contrast, if IGMP snooping is enabled, it saves bandwidth by only forwarding the necessary multicast traffic to ports with a receiving terminal connected.

The following example shows the difference between flooding and IGMP snooping, assuming receiving terminal A (RX A) only wants to receive Group A multicast traffic and receiving terminal B (RX B) only wants to receive Group B multicast traffic.

Flooding forwards both Group A and Group B traffic to the port where RX A is connected, but IGMP snooping only forwards Group A traffic to the port where RX A is connected.



Switches with IGMP snooping enabled use "IGMP Query" and "IGMP Report" to learn which multicast group traffic should be sent to which ports.

The following example shows the process flow of processing IGMP queries and IGMP reports.



1. One representative switch in the network periodically sends IGMP queries. The switch that sends the IGMP queries is called the "Querier".
2. When the multicast receiving terminal receives an IGMP query, it sends an IGMP report in response. The IGMP report contains information about the multicast group traffic that the receiving terminal wants to receive.
3. The switch learns which multicast group traffic to send to which port by snooping on the content in IGMP reports.

Since learned multicast group information is automatically deleted after a certain period of time, in order to maintain the correct learning state one querier must always be present in the same network. If multiple queriers exist in the same network, only one querier is retained and the other switches automatically stop sending queries. Note that even if there is no querier, the receiving terminal may spontaneously send an IGMP report, such as when the multicast receiving application is started in the receiving terminal. Note that if multicast group information is learned without a querier present, the corresponding multicast group traffic might not be forwarded to ports where other receiving terminals are connected.

## How to use this page

### Introduction

This page can be used as a troubleshooting tool if a problem related to IGMP snooping occurs. IGMP snooping is **enabled** when profiles are specified on the ProAV profile page.

In this page, IGMP snooping settings can be changed and the IGMP snooping operating status checked separately for each ProAV profile.

First, select a profile from the profile select box in the upper left corner of the page. If a ProAV profile has not been specified, specify the profile on the ProAV Profiles page.

### Warning message

When IGMP snooping is enabled, a warning message appears if the switch detects improper settings. If a warning message appears, review the settings and change them if necessary.

- Warning message

Display message	How to handle warnings
The IGMP version (V2) specified in the profile does not match the version (V3) of the IGMP query received. Set the IGMP version in the profile to the same version as the IGMP query.	Change the IGMP version.
Query transmission is stopped due to the presence of another querier	Enable IGMP query transmission.

---

## Change IGMP snooping settings

The following settings related to IGMP snooping can be changed for each ProAV profile

- IGMP snooping settings
  - Disabled ( Flood IP multicast packets )
    - Disable IGMP snooping  
Multicast packets are always forwarded to all ports in the same VLAN.
  - Enabled ( Control transmission of IP multicast packets )
    - Enable IGMP snooping.  
Multicast packets are forwarded only to the port to which the terminal you want to receive them is connected.  
This function monitors (snoops) IGMP messages exchanged between receiving terminals and a multicast router. It can suppress the flooding of multicast packets and reduce network bandwidth usage.
- Version
  - Select the IGMP version from the following items.
    - IGMPv3
    - IGMPv2
- IGMP query
  - No transmission  
IGMP query transmission function is disabled
  - Transmit periodically  
IGMP query transmission function is enabled. The transmission interval can be specified in the range of 20seconds to 18000 seconds
- Processing method for unknown multicast frames
  - Specify the processing method for unknown multicast frames from below.
    - Flood
    - Discard
  - If IGMP snooping is disabled, "Flood" is automatically selected.

## Check IGMP snooping operating status

IGMP snooping learning status can be checked for each ProAV profile.

If a group is selected in the "Multicast Group" select box, the corresponding IGMP report/query learning status is displayed.

Mouse-over the port with the learning status displayed to show a tooltip with detailed IGMP report/query information.

Note that if both an IGMP report and IGMP query is received at the same port, information about both are displayed in the tooltip.

- IGMP report/query learning status

Display item	Port display	Tooltip information
IGMP report receiving port		Receiving port information Last received report information ( IP address, Version )

Display item	Port display	Tooltip information
IGMP query receiving port		Receiving port information Received query information ( IP address, Version )

Since the learning status for multicast groups changes over time, click the "Update" button to update the display.

When a multicast group has been learned by an IGMP report, the IP address of the multicast group is displayed in the "Multicast Group" select box.

Traffic being sent to learned multicast groups is only forwarded to IGMP report receiving ports.

Unknown multicast groups are not displayed in the "Multicast Group" select box.

If a ProAV profile is specified, unknown multicast group traffic is discarded.

Please change the setting, if you want to flood an unknown multicast group.

If a problem that prevents receiving multicast traffic occurs, check whether the port indicator where the receiving terminal is connected is illuminated orange (which indicates it is an IGMP report receiving port).

If the connection port indicator is not orange, the receiving terminal might be connected to a port with a different profile. Check the profile setting for the port where it is connected.

If that does not solve the problem, try disabling IGMP snooping, but determine whether the bandwidth is sufficient before disabling IGMP snooping.

---

# Detailed settings

---

# Interface settings

## Physical interface

### Summary

This page is for changing the physical interface settings.

### Top page

This is the top page for the physical interface.

### Interface list

- The current operating status and settings for the physical interface are shown for each interface.
- The table items are explained below.
  - Check box
    - Select the check box for bulk settings or to initialize the settings.
  - Port
    - Displays the interface name.
  - Link
    - Displays the link status for the interface.
    - Displays the port type in parentheses for other ports besides the LAN.
  - Speed settings
    - Displays the speed and communication mode settings.
  - EEE
    - Displays the operating status of the EEE function.
  - Description
    - Displays the description text that is set for the interface.
- Press the "Setting" button to display the page where you can change the settings of the selected interface.
- If you press the "Specify all" button, the settings can be changed for all interfaces whose check box is selected.
  - Bulk settings cannot be made by selecting ports of different types.
  - The default settings will be applied to the settings on the physical interface settings page.
- If you press the "Return to defaults" button, the settings will be initialized on all interfaces whose check boxes are selected.
  - Each of the default settings are shown below.
    - Operation : Enable interface
    - Description : Unset
    - Speed/communication mode : Automatic
    - MRU : 1522 Byte
    - EEE function : Disabled (Don't use power-conservation Ethernet function)
    - Automatic cross/straight detection : Enable

**Physical interface settings page**

This page is for changing physical interface-related settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

**Physical interface settings**

- Port
  - Displays the name of the interface for which settings will be made.
- Operation
  - Select from the following interface operations.
    - Enable interface
    - Disable interface
- Description
  - Sets the interface description text.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 80 characters can be inputted.
- Speed/communication mode
  - Select the interface speed and communication method from the following options.
    - For a LAN port
      - Automatic
      - 1Gbps / Full duplex
      - 100Mbps / Full duplex
      - 100Mbps / Half duplex
      - 10Mbps / Full duplex
      - 10Mbps / Half duplex
    - For an SFP port or combo port
      - Automatic
      - 1Gbps / Full duplex
    - For an SFP+ port
      - Automatic
      - 10Gbps / Full duplex
- MRU
  - Specify the maximum amount of data that can be received at one time.
  - The input range is 64 - 10240 bytes.
- EEE function
  - EEE functions can only be set for the LAN port and combo port.
  - Select the operation for the EEE function from the following options.
    - Disable (Don't use power-conservation Ethernet function)
    - Enable (Use power-conservation Ethernet function)
- Automatic cross/straight detection

- Select the operation for the automatic cross/straight detection from the following options.
  - Enable
  - Disable
- If the automatic cross/straight detection is disabled, MDI is used for the cable connection type.

## Port mirroring settings

### Summary

This page is for changing the port mirroring settings.

### Top page

This is the top page for the port mirroring settings.

### Port mirroring settings

- The current settings for the port mirroring are shown.
- The table items are explained below.
  - Check box
    - Select the check box to delete the sniffer port setting.
  - Sniffer port
    - Displays the interface name of a sniffer port.
  - Monitored port
    - Displays the interface name of monitored ports.
  - Monitoring direction
    - Displays the monitoring direction for a monitored port.
- Press the "New" button to display a page where you can create new settings for a sniffer port.
- Press the "Setting" button to display the page where you can change the settings of a sniffer port.
- If you press the "Delete" button, all sniffer ports whose check boxes are selected will be deleted.
- Up to 1 sniffer port can be configured.

### Port mirroring settings page

This page is for changing the port mirroring settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Port mirroring settings

- Sniffer port
  - When configuring new settings
    - This page is for changing the port mirroring settings.
    - Select the interface to operate as a sniffer port.
    - Press the "Select" button to display the "Sniffer port selection" dialog.
  - When changing settings
    - You can select a sniffer port by checking the port check box and clicking the "OK" button in the "Sniffer port selection" dialog.
- Monitored port
  - Select the ports that will be monitored from a selected sniffer port.
  - Press the "Select" button to display the "Monitored port selection" dialog.
  - Monitored ports can be selected in the "Monitored port selection" dialog by placing a checkmark in the corresponding checkbox, selecting the monitoring direction, and pressing the "OK" button.

---

## Link aggregation

### Summary

This page is for configuring the link aggregation settings.

### Top page

This is the top page for link aggregation.

### System settings

- Shows the system settings related to link aggregation.
- The table items are explained below.
  - LACP system priority
    - Displays the LACP priority set in this system.
  - Mixed-speed mode
    - Displays whether the LACP mixed-speed mode is enabled or not.
  - Load balance rules
    - Displays the load balance settings.
- Press the "Settings" button to show the page for system settings related to link aggregation.

### Interface list

- The operating status and settings are shown for the logical interface and the physical interface.
- The table items are explained below.
  - Check box
    - Select the check box to delete the logical interface.
  - Port
    - Displays the interface name.
  - Link
    - Displays the link status for the interface.
  - LACP status
    - One of the following statuses are displayed for the LACP status of the interface.
      - Waiting
      - Negotiating
      - Communication OK
      - -
  - LACP priority
    - During actual operation, the priority will be displayed.
    - Displays a value from 1 to 12 for the priority, calculated based on the LACP priority setting.
  - Description
    - Displays the description text that is set for the interface.
- Press the "New" button to display a page where you can create new settings for a logical interface.
- Press the "Setting" button to display the page where you can change the settings of the selected logical interface.

- If you press the "Delete" button, all logical interfaces whose check boxes are selected will be deleted.
  - When deleting a logical interface, you can specify the physical interface operations after deletion as follows.
    - Enable
    - Disable
- Up to 127 logical interfaces can be configured.
- Up to 96 static logical interfaces can be configured.

### System settings page

This page is for configuring link aggregation-related system settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- LACP system priority
  - Specify the LACP system priority.
- LACP mixed-speed mode
  - Select whether to enable the LACP mixed-speed mode from the following.
    - Disable
      - When this function is disabled, physical interfaces with different communication speeds belonging to the LACP logical interface cannot communicate at the same time.
    - Enable
      - When this function is enabled, physical interfaces with different communication speeds belonging to the LACP logical interface can communicate at the same time.
      - Enable this function when you want to aggregate physical interfaces with different communication speeds into an LACP logical interface.
- Load balance rules
  - The following load balance rules can be selected.
    - 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

### Logical interface settings page

This page is for changing the logical interface settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

---

## Logical interface settings

- Logical interface
  - When configuring new settings
    - The logical interface type can be selected from the following types.
      - Static logical interface
      - LACP logical interface
  - When changing settings
    - Displays the selected logical interface name.
- Interface number
  - Specifies the interface number.
  - A value from 1 to 96 can be inputted for a static logical interface.
  - A value from 1 to 127 can be inputted for an LACP logical interface.
  - This item will be displayed only when configuring new settings.
- Associated port
  - Select the port that will be associated with the logical interface.
  - Press the "Select" button to display the "Physical interface list" dialog box.
  - Select the port check box in the "Physical interface list" dialog box and press the "OK" button to select the associated port.
  - Up to eight ports can be selected for a static logical interface, and up to 12 ports can be selected for an LACP logical interface.
  - When displaying the dialog box for the "Logical interface" item with the LACP logical interface selected, the following settings can be made for each associated port.
    - Operation mode
      - Active
      - Passive
    - LACP priority
      - 1 - 12
    - LACP timeout
      - 3 Seconds
      - 90 Seconds
- Operation
  - Select from the following logical interface operations.
    - Enable interface
    - Disable interface
- Description
  - Sets the interface description text.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 80 characters can be inputted.

## Port authentication

### Port authentication settings

#### Summary

This page is for configuring the port authentication.

To use port authentication, you need to configure the system settings and the interface settings. You also need to configure the authentication server in **Interface settings > Port authentication > Server settings**.

#### Top page

This is the top page for the port authentication settings.

#### System settings

- Displays the port authentication settings for the system.
- The table items are explained below.
  - 802.1X authentication
    - Displays whether 802.1X authentication is enabled or not for the entire system.
  - MAC authentication
    - Displays whether MAC authentication is enabled or not for the entire system.
  - Web authentication
    - Displays whether web authentication is enabled or not for the entire system.
- Press the "Setting" button to display the page for configuring the system settings.

#### Interface settings

- Displays the port authentication settings for the interface.
- The table items are explained below.
  - I/F
    - Displays the interface name.
  - Enabled authentication functions
    - Displays the enabled authentication functions for the interface.
  - Host mode
    - Displays the authentication operation mode setting.
- Press the "Setting" button to display the page for changing the settings of the selected interface.
- Press the "Specify all" button to configure all interfaces with the check box selected.
- If you press the "Return to defaults" button, the settings will be initialized on all interfaces whose check boxes are selected.

#### System settings page

This page is for configuring the port authentication for the system.

You can also change the detailed settings by pressing the "Advanced settings" button.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

---

## System settings

- Authentication functions to be enabled
  - Select the authentication functions to be enabled for the entire system from the following.
    - 802.1X authentication
    - MAC authentication
    - Web authentication
- MAC address format for MAC authentication
  - Select the MAC address format for MAC authentication from the following.
    - Delimiter (-), Lowercase
    - Delimiter (:), Lowercase
    - No delimiter, Lowercase
    - Delimiter (-), Uppercase
    - Delimiter (:), Uppercase
    - No delimiter, Uppercase
- Redirect URL after successful web authentication
  - Specify the destination URL for redirecting the authenticated device after successful web authentication.
  - Enter up to 256 characters using single-byte alphanumeric characters and symbols, excluding ? symbol.
- Clearing authentication status
  - Specify whether or not to clear the authentication status of the device periodically.
  - The input range of the time to clear is from 0 to 23 o'clock.
  - If **Clearing authentication status** is set in the interface settings, the setting in the interface settings takes precedence.

## Interface settings page

This page is for configuring the port authentication for the interface.

You can also change the detailed settings by pressing the "Advanced settings" button.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## Interface settings

- Applicable interface
  - Displays the name of the interface whose settings are to be changed.
- Authentication functions to be enabled
  - Select authentication functions to be enabled for the interface from the following.
    - 802.1X authentication
    - MAC authentication
    - Web authentication
- Host mode
  - Select the authentication operation mode for the authentication function from the following.
    - Single host mode

- If the device connected to the interface has successfully authenticated, only the device can access.  
If another device has already authenticated, this device cannot authenticate or access.
- Multi host mode
  - If any device connected to the interface has successfully authenticated, all devices connected to the interface can access.
- Multi supplicant mode ( Recommended )
  - All devices connected to the interface can individually authenticate, and only the devices successfully authenticated can access.
- Authentication order
  - Select which authentication to use first if both 802.1X authentication and MAC authentication are enabled.
    - 802.1X authentication first
    - MAC authentication first
  - Web authentication authenticates when ID and Password are entered regardless of this setting.
- MAC address registration type after MAC authentication
  - Select a registration type for authenticated MAC addresses to the MAC address table.
    - Register as dynamic entry
    - Register as static entry
  - The aging timer automatically deletes MAC addresses registered as dynamic entries from the MAC address table.
  - The "clear auth state" or the "authclear-state time" command can delete MAC addresses registered as static entries from the MAC address table.
- Guest VLAN
  - Specify the guest VLAN.
  - Press the "Select" button, and then select a VLAN ID from the "VLAN list" dialog.
  - When a guest VLAN is configured, devices that have not successfully authenticated can also access the specified VLAN.
  - This cannot be used with web authentication.
- Dynamic VLAN
  - Specify whether or not to use dynamic VLAN.
  - If you set to use dynamic VLAN, VLANs are dynamically assigned to each device that has successfully authenticated.
  - The VLAN to be assigned depends on the authentication server settings.
- Waiting time for a response from device
  - Specify the waiting time for a response from the device during authentication.
  - The input range is from 1 to 65535 seconds.
- Authentication restriction period after authentication failure
  - Specify the period to restrict authentication after the authentication of a device fails.
  - The input range is from 1 to 65535 seconds.
  - While authentication is restricted, all packets received on the target interface are discarded.
- Re-authentication of authenticated device
  - Specify whether or not to periodically re-authenticate the device that has successfully

- 
- authenticated.
  - The input range of the re-authentication interval is from 300 to 86400 seconds.
  - Clearing authentication status
    - Specify whether or not to clear the authentication status of the device periodically.
    - The input range of the time to clear is from 0 to 23 o'clock.
  - 802.1X authentication operation mode
    - Select the operation mode for 802.1X authentication from the following.
      - Operate as authentication interface
      - Set as authenticated interface
      - Set as unauthenticated interface
  - Forwarding control on unauthenticated ports for 802.1X authentication
    - When 802.1X authentication is enabled, specify the communication restriction method for devices that have not successfully authenticated from the following.
      - Discard both sending and receiving
      - Discard only receiving
    - If any of the following conditions are met, this setting is ignored, and the function operates as **Discard only receiving**.
      - Host mode is set to multi-suppliant mode.
      - MAC authentication is enabled.
    - If the guest VLAN is configured, this setting does not affect the communication restrictions.
  - Number of times to send EAPOL packets
    - Specify the maximum number of times to send EAPOL packets.
    - The input range is from 1 to 10 times.

## Server settings

### Summary

This page is for configuring the authentication server.

Configure the authentication server for port authentication.

To use the built-in RADIUS server as an authentication server, you need to configure the built-in RADIUS server in **Application layer > RADIUS server > Server settings**.

The authentication server can be configured manually as a fixed setting or automatically using the auto-configure via LLDP function.

To enable automatic settings, enable the "auto-configure via LLDP function" in **Management > LLDP**. Then the RADIUS server notified by LLDP has configured automatically.

### Top page

This is the top page for the Server settings.

### Authentication RADIUS server settings

- Displays the authentication RADIUS server settings.
- The table items are explained below.
  - Address
    - Displays the authentication server address.
  - Port number
    - Displays the authentication server port number.
- Press the "New" button to display the page for configuring a new authentication server.
- Press the "Setting" button to display the page for changing the selected authentication server's settings.
- Press the "Delete" button to delete all authentication servers with the check box selected.
- Press the "Register" button to configure the auto-configured RADIUS server as a fixed setting.
- Up to eight authentication server settings can be created, including fixed and automatic settings.
- If both fixed settings and automatic settings are configured, the fixed settings are used first.
- If you create a new fixed setting under the number of authentication server settings reached the maximum, the setting with the largest LLDP receiving port number is deleted from the settings configured automatically via LLDP.

### Common detailed settings

- Displays the common detailed settings.
- The table items are explained below.
  - Waiting time for a response per server
    - Displays the waiting time for a response per server.
  - Number of times to resend requests to server
    - Displays the number of times to resend requests to the server.
  - Server usage restriction period
    - Displays the period for server usage restriction.
  - NAS-Identifier attribute to be notified to the server
    - Displays the NAS-Identifier attribute to be notified to the server.
- Press the "Setting" button to display the page for changing the common detailed settings.

---

## Authentication RADIUS server settings page

This page is for configuring the authentication RADIUS server.

You can also change the detailed settings by pressing the "Advanced settings" button.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Authentication RADIUS server settings

- Server type
  - Select the authentication server type from the following.
    - Use built-in RADIUS server
    - Use external RADIUS server
  - If you select **Use built-in RADIUS server**, the following settings are specified with predetermined values.
    - Server address
    - Server port number
    - Shared password with server
  - This item appears only for new settings.
- Server address
  - Specify the address of the authentication server.
  - Enter the address in one of the following formats.
    - IPv4 address : XXX.XXX.XXX.XXX
    - IPv6 global address : XXXX:XXXX::XXXX:XXXX
    - IPv6 link-local address : fe80::X%vlanN
  - To change the setting, you need to start over from a new setting.
- Server port number
  - Specify the port number of the authentication server.
  - The input range is from 0 to 65535.
- Shared password with server
  - Specify the shared password with the authentication server.
  - Enter up to 128 characters using single-byte alphanumeric characters and symbols, excluding ? and **space** symbols.
  - If you omit the input, the shared password set in the common detailed settings is applied.
- Waiting time for a response from server
  - Specify the waiting time for a response from the authentication server.
  - The input range is from 1 to 1000 seconds.
  - If you omit the input, the waiting time for a response per server set in the common detailed settings is applied.
- Number of times to resend requests to server
  - Specify the number of times to resend requests to the server when the authentication server's response times out.
  - The input range is from 0 to 100 times.
  - If you omit the input, the number of times to resend requests to the server set in the common detailed settings is applied.

## Common detailed settings page

This page is for changing the common detailed settings of the authentication server.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Common detailed settings

- Shared password with server
  - Specify the shared password with the authentication server.
  - Enter up to 128 characters using single-byte alphanumeric characters and symbols, excluding ? and **space** symbols.
- Waiting time for a response from server
  - Specify the waiting time for a response from the authentication server.
  - The input range is from 1 to 1000 seconds.
- Number of times to resend requests to server
  - Specify the number of times to resend requests to the server when the authentication server's response times out.
  - The input range is from 0 to 100 times.
- Server usage restriction period
  - Specify the period to restrict the use of the authentication server temporarily for when the server does not reply after resending requests.
  - The input range is from 0 to 1440 minutes.
- NAS-Identifier attribute to be notified to the server
  - Specify the NAS-Identifier attribute to be notified to the authentication server.
  - Enter up to 253 characters using single-byte alphanumeric characters and symbols, excluding ? symbol.

---

## Authentication management

### Summary

This page is for managing authentication.  
You can check and delete the authentication information of the device.

### Top page

This is the top page for the authentication management.

### Authentication information of devices

- Displays the authentication information for each device.
- The table items are explained below.
  - Port
    - Displays the interface to which the device is connected.
  - Name
    - Displays the name of the device.
  - MAC address
    - Displays the MAC address of the device.
  - Authentication method
    - Displays the authentication method used to authenticate the device.
  - State
    - Displays the authentication status of the device.
  - VLAN
    - Displays the VLAN to which the device belongs.
- A maximum of 100 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- You can press the sort switch to sort by each item.
- Press the "Update" button to update the device's authentication information to the latest status.
- Press the "Delete" button to delete all authentication information with the check box selected.

## Web authentication screen

### Summary

This page is for customizing the web authentication screen.

You can customize the authentication screen for web authentication.

For the specific customization method, please refer to **Interface control functions > Port authentication functions > 3.3.2 Customizing the authentication screen** in the technical data for this product in [Yamaha Network Devices Technical Documentation](#).

### Top page

This is the top page for the web authentication screen.

### Customizing the web authentication screen

- Displays whether customization has been applied or not.
- If the customization has been applied, you can disable the customization by pressing the "Disable" button.
- Press the "Next" button to the right of "Download the original files for customization" to download the original files for customization.
- Press the "Next" button to the right of "Apply the customized files" to open the page to apply the customization.

### Applying customization page

This page is for customizing the web authentication screen.

Select the customized file from "Select a file", and press the "Confirm" button. If the information entered in the confirmation screen is correct, press the "OK" button.

### Applying customization

- Logo file (.png)
  - Specify the logo file.
  - The file extension has to be .png.
- Header file (.html)
  - Specify the header file.
  - The file extension has to be .html.
- Footer file (.html)
  - Specify the footer file.
  - The file extension has to be .html.
- CSS file (.css)
  - Specifies the CSS file.
  - The file extension has to be .css.

---

## PoE

### Summary

This page is for configuring PoE control.

### Top page

This is the top page for PoE control.

### System settings

- Displays the system settings for PoE control.  
The table items are explained below.
  - PoE power supply for the entire system
  - Guardband
- Press the "Setting" button to display the page for configuring the system settings for PoE.

### Interface settings

- Displays the PoE power supply function settings for the interface.  
The table items are explained below.
  - Port  
Displays the interface name.
  - PoE supply  
Displays the PoE power supply function settings for the target interface.
  - Priority  
Displays the power supply priority for the target interface.
  - Description  
Displays the description of the PD device connected to the PoE port.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected.
- Press the "Specify all" button to configure the settings for all interfaces with the check box selected.
- Press the "Setting" button to display the page for configuring the selected interface settings.

### System settings page

This page is for configuring PoE control for the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- PoE power supply for the entire system  
Specify whether to enable or disable the PoE power supply function for the entire system.  
Even if the PoE power supply function for the entire system is enabled, if each port's function is disabled, the PoE power supply function for that port is disabled.
- Guardband  
Specify the guardband.  
The guardband is a margin against the upper limit of the available power supply set to prevent unexpected power outages.  
If the available power supply falls below the guardband, power does not supply even if a new PD device is

connected to a PoE port.  
If 0W is specified, the guardband does not work.

### Interface settings page

This page is for configuring PoE control for the interface.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Interface settings

- PoE supply  
Specify whether to enable or disable the PoE power supply function for the target interface.  
The power supply continues even if the port is in a shutdown state. However, if the PoE power supply function for the entire system is disabled, power is not supplied.
- Priority  
Specify the power supply priority for the target interface.  
If the total power supply to all ports exceeds the upper limit of the available power supply, the port's power supply with the lowest priority stops.
- Description  
Specify the description of the PD device connected to the PoE port.

---

## L2MS filter

### Summary

This page is for configuring L2MS filter settings.  
If you enable L2MS filter, you can block L2MS frames.

### Top page

Displays a list of L2MS filter settings for interfaces.

### Interface list

- Displays the current L2MS filter settings for each interface.
- Press the "Setting" button to display the page for configuring the selected interface.
- Press the "Specify all" button to configure the settings for all interfaces with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected. The default setting of L2MS filter is "Disabled".
- Constraints  
If the L2MS operation mode is disabled, L2MS filter does not work.  
L2MS frames are forwarded.

### Interface settings

This page is for configuring L2MS filter for the interface.  
Enter the settings, and then press the "Confirm" button.  
If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Interface settings

- L2MS filter  
Specify whether to enable or disable L2MS filter for the target interface.  
If it is enabled, the filter blocks L2MS frames. If it is disabled, the filter does not block L2MS frames.

## Tx queue usage monitoring

### Summary

This page is for configuring the tx queue usage monitoring function.

If you disable this function, notifications about the tx queue are not sent in SYSLOG and mail notifications.

### Top page

This is the top page for the tx queue usage monitoring.

### System settings

- Displays the configuration of the tx queue usage monitoring function for the entire system.
- Press the "Setting" button to display the page for configuring the system.

### Interface settings

- Displays the configuration of the tx queue usage monitoring function for each port.
- The table items are explained below.
  - Port
    - Displays the port name.
  - Tx queue usage monitoring
    - Displays the configuration of the tx queue usage monitoring function for the target port.
- Press the "Setting" button to display the page for configuring the selected port.
- Press the "Specify all" button to configure the settings for all ports with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all ports with the check box selected.

### System settings page

This page is for configuring the tx queue usage monitoring function for the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- Tx queue usage monitoring for the entire system
  - Specify whether to enable or disable the tx queue usage monitoring function for the entire system.
  - If this setting is disabled, notifications about the tx queue are not sent.
  - Even if the entire system setting is enabled, notifications are not sent about the tx queue of ports whose individual setting is disabled.

### Interface settings page

This page is for configuring the tx queue usage monitoring function for the interface.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Interface settings

- Port
  - Displays the port name to configure the settings.

- Tx queue usage monitoring
  - Specify whether to enable or disable the tx queue usage monitoring function for the target port.
  - If this setting is disabled, notifications about the tx queue of the target port are not sent.
  - Even if the individual port setting is enabled, notifications are not sent about the tx queue if the entire system setting is disabled.

---

# VLAN

## Create VLAN

### Summary

In this page you can create or delete VLANs, and change the IP address.

### Top page

This is the top page for creating a VLAN.

### VLAN list

- Information for the defined VLANs is displayed
  - IPv4 primary address is displayed in bold.
- A maximum of 20 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- You can press the sort switch to sort by each item.
- Press the "New" button to access a page where you can create a new VLAN
- Press the "Setting" button to access a page where you can change the settings of the selected VLAN
- If you press the "Delete" button, all VLANs whose check box has a check mark will be deleted
  - The following VLAN cannot be deleted
    - Default VLAN ( VLAN ID = 1 )
    - Private VLAN
- Up to 256 VLANs can be created including the default VLAN (VLAN ID == 1).

### VLAN settings page

In this page you can create a new VLAN or edit the settings of an already-defined VLAN.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### VLAN settings

- VLAN ID
  - To create a new VLAN, enter the desired VLAN ID within the valid range (2–4094)
    - The smallest ID of the unregistered VLAN IDs is entered as the default value
    - If an already-registered VLAN ID is entered, it is handled as a change in settings
  - When changing the settings, it is not possible to change the VLAN ID
- Name
  - Specify the name of the VLAN using up to 32 single-byte alphanumeric characters and symbols.
    - The default VLAN (VLAN ID == 1) cannot be renamed
    - A space and "?" cannot be used in the name of the VLAN.
- Frame transmission

Select frame forwarding from the following items.

  - Enable frame transmission

- Disable frame transmission
  - Frame forwarding cannot be disabled for the default VLAN (VLAN ID == 1)
- IPv4 address
  - For IPv4 addresses, you can specify one primary address and up to 4 secondary addresses for each VLAN.
  - You can set up to 8 of these addresses on the entire system.
  - You can set this item only for VLANs with frame forwarding enabled.
  - Set each address as follows.
    - Primary address
      - Select the IP address setting from the following.
        - Not set
        - Obtain automatically using DHCP
          - Selecting the check box for "**Setting the link local address when auto-acquire does not work**" will enable the Auto IP function.
            - The Auto IP function can be enabled for only one VLAN.
            - You cannot select this item if the stack port is set to use Auto IP.
            - You can specify a host name to notify the DHCP server.
          - Specify a fixed IP address
            - Enter the IP address and subnet mask
            - You can set description or note about the IP address as a label.
        - If you select **Obtain automatically using DHCP** or **Specify a fixed IP address**, the various server configurations are changed for the VLAN that you configure as follows.
          - You can access the HTTP server and the TELNET server from the VLAN interface. (To enable access to the SSH server and the TFTP server, you need additional configurations.)
          - No changes are made to the configuration of a server that already has 8 VLAN interfaces registered.
      - Secondary address
        - Enter the following settings in the table.
          - Address
            - Enter the IP address and subnet mask
          - Label
            - You can set description or note about the IP address as a label.
        - Press the  icon to add a configuration form.
        - Press the "Delete" button to delete a configuration form.
- IPv6 address
  - For IPv6 addresses, you can specify up to 5 global addresses and one link-local address for each VLAN.
  - You can set up to 8 of these addresses on the entire system.
  - The IPv6 address cannot be configured when the stack function is enabled.
  - Select whether the IPv6 address will be enabled or disabled from the following items.
    - Disable IPv6

- Enable IPv6
- If you select **Enable IPv6**, the various server configurations are changed for the VLAN that you configure as follows.
  - You can access the HTTP server and the TELNET server from the VLAN interface. (To enable access to the SSHserver and the TFTP server, you need additional configurations.)
  - No changes are made to the configuration of a server that already has 8 VLAN interfaces registered.
- Set each address as follows.
  - Global address
    - Enter the following settings in the table.
      - Address
        - Select from the following items.
          - Obtain automatically using RA
          - Specify the address
          - Specify the address (DHCPv6-PD)
          - Obtain automatically using DHCPv6
        - If you select **Obtain automatically using RA**, you can select whether to operate by DHCPv6 stateless.
        - If you select **Specify the address**, enter the following items.
          - Address
            - Enter the IP address and subnet mask
          - If you select **Specify the address (DHCPv6-PD)**, enter the following items.
            - Prefix name
              - You can select from the prefix names set in DHCPv6-PD client function.
            - Low address
              - Set the lower part (rest) for the prefix obtained by DHCPv6-PD client.
              - You need to specify "0" for the prefix part obtained by DHCPv6-PD client.
          - Enter the IP address and subnet mask
        - Configuration notes
          - You cannot specify "Obtain automatically using RA" and "Obtain automatically using DHCPv6" in global address at the same time.
        - Press the  icon to add a configuration form.
        - Press the "Delete" button to delete a configuration form.
      - Link local address
        - Enter an IP address.
  - DHCPv6-PD client function
    - You can enable DHCPv6-PD client function and configure it to request prefix assignment.
    - You can enable up to 8 interfaces for the entire device.
    - Enter a prefix name if you enable this function.

- 
- Prefix name is the name you attach to the prefix assigned by DHCPv6 client.
  - You can use single-byte alphanumeric characters, dot (.), hyphen (-), and underline (\_).
  - You can set up to 32 characters.
  - Configuration notes
    - You cannot configure settings when IPv6 is disabled.
    - You cannot configure DHCPv6-PD client function when the stack function is enabled.
    - DHCPv6-PD client function cannot be enabled when "Obtain automatically using RA (Enabled DHCPv6 stateless)" or "Obtain automatically using DHCPv6" setting is included in global address.
  - MTU
    - Specify the maximum packet length (MTU value) that the VLAN interface can send.
    - You can specify up to 7 different values other than the default value for the entire device.
    - The input range of MTU is as follows.
      - 68 - 9216 when IPv6 is disabled
      - 1280 - 9216 when IPv6 is enabled
    - When changing the MTU, adjust the MRU as well. If the received frame exceeds the MRU size, the frame is discarded without being forwarded.

## Tag VLAN

### Summary

In this page you can make settings for tagged VLANs.

### Top page

This is the top page for tagged VLANs.

### Tag VLAN settings

- The various settings for tagged VLANs are shown for each LAN/SFP port and logical interface
  - "Frame types that can be received" is displayed according to the operating mode and the VLAN settings. (This item cannot be set in the settings page.)
- Press the "Setting" button to access a page where you can change the settings for the tagged VLAN of the selected interface
- If you press the "Specify all" button, the settings can be changed for all LAN/SFP ports and logical interfaces whose check box contains a check mark
- If you press the "Return to defaults" button, the settings will be initialized for all LAN/SFP ports and logical interfaces whose check box contains a check mark.
  - Default settings for a tagged VLAN are as follows
    - Operating mode: Access
    - Assigned VLAN: Default VLAN (VLAN ID == 1)
- Settings for the LAN/SFP port assigned to a private VLAN cannot be changed
- Settings for the LAN/SFP port assigned to a voice VLAN cannot be changed
- If the operation mode is "Trunk," both the native VLAN and the trunk VLAN are shown as assigned VLANs.

### Tagged VLAN settings page

In this page you can make various settings related to tagged VLANs.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Tag VLAN settings

- Port
  - The LAN/SFP port or logical interface for which settings are made is shown
- Operation mode
  - Access
    - The corresponding port is specified as the access (untagged) port
  - Trunk
    - The corresponding port is specified as the trunk (tagged) port
- Access VLAN
  - This item is shown only if the operating mode is "Access".
  - From the list, select the access port's assigned VLAN
  - However, the following cannot be selected as access VLAN.
    - Private VLAN
    - Voice VLAN

- 
- VLAN for which frame forwarding is invalid
  - NativeVLAN
    - This item is shown only if the operating mode is "Trunk".
    - From the list, select the assignment-destination VLAN (native VLAN) for untagged frames received from the trunk port.
    - However, the following cannot be selected as native VLAN.
      - VLAN selected as trunk VLAN
      - PrivateVLAN
      - VoiceVLAN
      - VLAN for which frame forwarding is invalid
  - TrunkVLAN
    - This item is shown only if the operating mode is "Trunk".
    - Specify the assignment-destination VLAN (trunk VLAN) for tagged frames received at the trunk port.
    - When you press the "Select" button, a list of the selectable VLAN IDs appears in a separate window
    - However, the following cannot be selected as trunk VLAN.
      - VLAN selected as native VLAN
      - PrivateVLAN
      - VoiceVLAN
      - VLAN for which frame forwarding is invalid
    - Place a check mark in the check box of the VLAN ID that you want to specify, and press the "OK" button
  - Ingress filter

Select the ingress filter from the following items. This item is shown only if the operating mode is "Trunk."

    - Enabled ( Receive only if the VLAN ID of the incoming frame is the same as the associated VLAN )
    - Disabled ( Receive all frames )

## Multiple VLAN

### Summary

In this page you can make multiple VLAN settings.

The Multiple VLAN function is used to divide ports for oneswitch into different groups and prohibit communication between thegroups.

A single port can belong to multiple groups, so that the samenetwork address can be assigned even to different groups.

If both the multiple VLAN and port-based VLAN / tagged VLANare used, communication is not possible between ports that belong todifferent VLANs, even if the ports belong to same multiple-VLAN group.

### Top page

This is the top page for multiple VLANs.

### Tag VLAN settings

- The multiple VLAN group settings are shown for each LAN port and logical interface.
- Press the "Setting" button to access a page where you can change the settings for the multiple VLAN of the selected interface.
- If you press the "Specify all" button, thesettings can be changed for all LAN ports and logical interfaces whosecheck box contains a check mark.
- If you press the "Return to defaults" button,the settings will be initialized for all LAN ports and logicalinterfaces whose check box contains a check mark.
  - In default settings, no interfaces belong to a group.

### Multiple VLAN settings page

In this page you can make the multiple VLAN settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the setting confirmation screen, press the "OK" button.

### Multiple VLAN settings

- Port
  - The LAN port or logical interface for which settings are made is shown
- Group
  - Select the VLAN groups to join.
  - Press the "Select" button to display the "Multiple VLAN group selection" dialog box.
  - Groups to join a VLAN can be selected byselecting the corresponding checkboxes in the "Multiple VLAN groupselection" dialog and press the "OK" button.

---

# Layer 2 functions

## MAC address table

### Summary

In this page you can edit the settings of the MAC address table function.

### Top page

This is the top page for the MAC address table.

### Basic settings for MAC address learning function

- The current settings for the MAC address learning function are shown
- When you press the "Setting" button, a page where you can change the MAC address learning function settings will appear

### Static MAC address table settings

- The static MAC address table is shown as a list
- A maximum of 20 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- You can press the sort switch to sort by each item.
- If you press the "New" button, a page appears in which you can create a new static MAC address entry.
- If you press the "Setting" button, a page appears in which you can edit the settings of the selected static MAC address entry.
- If you press the "Delete" button, all static MAC address entries whose check box has a check mark will be deleted
- Up to 512 static MAC address entries can be created from the Web GUI.

### MAC address learning function basic settings page

In this page you can make settings for the MAC address learning function.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Basic settings for MAC address learning function

- MAC address learning function

Select the MAC address learning function from the following items.

- Use MAC address learning function
- Don't use MAC address learning function
- Aging time for dynamic entries
  - Specify a setting in the range of 10 seconds to 400 seconds. The default value is 300 seconds

### Static MAC address table settings page

In this page you can make static MAC address settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

**Static MAC address settings**

## • Kind

Choose from the following items as the type of MAC address to be registered in the static MAC address table.

- Register a unicast MAC address
- Register a multicast MAC address

## • Destination MAC address

- Enter the MAC address in the format hhhh.hhhh.hhhh.

## • Frame processing

From the following items, select the processing for frames sent to the destination MAC address.

- Forward frames that are being sent to the destination MAC address
- Discard frames that are being sent to the destination MAC address
  - If a multi-cast MAC address is registered, "Forward" is the only frame processing that can be specified

## • Destination VLAN ID

- Select the forwarding-destination VLAN ID from those that are registered in the VLAN database

## • Forwarding destination interface

- If you press the "Select" button, the interfaces assigned to the forwarding-destination VLAN ID are shown as a list  
Place a check mark in the check box of the interface that you want to use as the forwarding-destination interface, and press the "OK" button
- If registering a unicast MAC address, you can specify one interface
- If registering a multicast MAC address, you can specify multiple interfaces

---

## Spanning tree

### Summary

This page is for configuring the spanning tree.

If you want to use the spanning tree function, you need to enable both the system settings and the interface settings.

If the spanning tree is disabled in the system settings, the spanning tree does not work on all interfaces regardless of the interface settings.

### Top page

This is the top page for the spanning tree.

### System settings

- Displays the spanning tree setting for the system.
- Press the "Setting" button to display the page for configuring the system settings.

### Interface settings

- Displays the spanning tree setting for each interface.
- The table items are explained below.
  - I/F
    - Displays the interface name.
  - Spanning tree function
    - Displays whether the spanning tree function is enabled or not on the interface.
- Press the "Setting" button to display the page where you can change the settings of the selected interface.
- If you press the "Specify all" button, the settings can be changed for all interfaces whose check box is selected.
- If you press the "Return to defaults" button, the settings will be initialized on all interfaces whose check boxes are selected.

### System settings page

This page is for configuring the spanning tree for the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- Spanning tree function
  - Select the spanning tree function setting from the following items.
    - Use
    - Don't use

### Interface settings page

This page is for configuring the spanning tree for the interface.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## Interface settings

- Applicable interface
  - Displays the name of the interface whose settings are to be changed.
- Spanning tree function
  - Select the spanning tree function setting from the following items.
    - Use
    - Don't use

---

## Loop detection

### Summary

This page is for configuring the settings for loop detection.

This function monitors whether a loop is occurring by sending its loop detection frame from the port and whether the frame returns to itself or not.

### Top page

This is the top page for the loop detection.

### System settings

- Displays the system settings of loop detection.
- The table items are explained below.
  - Displays the loop detection settings for the entire system.
  - Displays the setting for whether to disable Port Blocking immediately or periodically after the loop is resolved.
  - Displays the setting for automatic recovery from Shutdown (errdisable state).
  - Press the "Setting" button to display the page for configuring the loop detection settings for the entire system.
- Resetting the loop detection status
  - You can immediately resolve the loop detection states (e.g., Shutdown) by reset feature.

### Interface settings

- Displays the settings and operating status of loop detection for each interface.
- The table items are explained below.
  - Check box  
Select the check box for bulk settings or to initialize the settings.
  - Port  
Displays the interface name.
  - Loop detection  
Displays the settings of loop detection for the interface.
  - Port Blocking  
Displays the settings of Port Blocking function.  
If it is enabled, the function blocks frames when a loop is detected.
  - Status  
Displays the operating status of loop detection.
    - Operating  
The loop detection function is operating.
    - Detected  
Loop has been detected. Communication is continued.
    - Blocking  
Blocking the frames. (Restart the communication in 5 seconds after the loop has been resolved)
    - Shutdown  
Shutting down the port. (Restart the communication in 5 minutes after shutting down the

port)

- Stopped

The loop detection function is stopped.

Normally, the state becomes "Stopped" when the loop detection setting is disabled. If it is stopped by other factors, the following factors are indicated in parentheses.

- Mirror port

- If it is a port with mirroring settings (mirror port)

- STP

- You can use the loop detection function with spanning tree. However, the function works only when the spanning tree status of the corresponding port is "Forwarding".

- Press the "Setting" button to display the page for configuring the selected interface settings.
- Press the "Specify all" button to configure the settings for all interfaces with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected.
  - Each of the default settings are shown below.
    - Loop detection: Enabled
    - Port Blocking: Enabled (Block frames when a loop is detected)
- Press the "Update" button to update the table of interface settings.

### System settings page

This page is for configuring the interface settings for loop detection.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- Specify whether to enable or disable the loop detection function for the entire system. Even if set to enable, the loop detection function for an individual port does not work if the port's setting is disabled.
- If this function is used with a spanning tree, the spanning tree takes precedence.

### Interface settings page

This page is for configuring the interface settings for loop detection.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Interface settings

- Loop detection  
Specify whether to enable or disable the loop detection function for the target interface. However, even if set to enable, the loop detection function does not work in the following cases.
  - (1) The loop detection function for the entire system is disabled.
  - (2) The target interface is a port with mirroring settings. (mirror port)
  - (3) Used with spanning tree, and spanning tree status of the target interface is not "Forwarding".
- Port Blocking  
Specify whether to enable or disable the Port Blocking function for the target interface. If set to enable, the function blocks frames when a loop is detected.

---

## Pass through

### Summary

In this page you can edit the settings of the pass through function.  
If you enable the pass through function, you can forward special frames that are usually discarded.

### Top page

This is the top page for pass through.

### EAP pass through setting

- The current setting is shown as to whether the EAP pass through is enabled.
- If the EAP pass through is enabled, the device forwards the received EAPOL frames so that the device can be placed between the IEEE 802.1X authentication switch and PCs.
- Press the "Setting" button to access a page where you can change the settings.

### EAP pass through settings page

In this page you can specify whether the EAP pass through is enabled.  
Enter the settings, and then press the "Confirm" button.  
If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### EAP pass through setting

- EAP pass through
  - Enable
    - Forwards received EAPOL frames.
  - Disable
    - Discards received EAPOL frames.

## DHCP snooping

### Summary

This page is for configuring DHCP snooping.

### Top page

This is the top page of DHCP Snooping.

### Display Binding Database

- Clicking the "Next" button will display a page where you can check the information of DHCP clients registered in the binding database.
- If the system-wide DHCP snooping feature is disabled, the "Next" button cannot be pressed.

### System settings

- Displays the DHCP snooping settings in the system.
- The table items are explained below.
  - DHCP snooping function for the entire system
    - Displays whether or not DHCP snooping is enabled for the entire system.
  - MAC address verification
    - Displays whether or not to enable forwarding DHCP packets with Option 82 information via untrusted ports.
    - MAC address verification process compares the source MAC address for packets received via an untrusted port with the client hardware address and discards corresponding DHCP packets if the addresses do not match.
  - DHCP packets receiving rate limit
    - The setting for the number of DHCP packets that can be received per second is displayed.
  - Option 82 function
    - Shows whether Option 82 information is to be assigned, inspected, or deleted.
  - Forward packets with Option 82
    - Displays whether or not to enable forwarding of DHCP packets with Option 82 information on the Untrusted port.
  - Output to SYSLOG
    - Displays whether the reason for discarding DHCP packets is output to SYSLOG.
- Pressing the "Settings" button will bring up a page where you can configure the system settings.

### VLAN interface settings

- Displays the DHCP snooping function setting for each VLAN interface.
- The table items are explained below.
  - VLAN ID
    - VLAN ID is displayed.
  - DHCP snooping function
    - Displays whether the DHCP snooping function is enabled for the corresponding VLAN ID.
  - Remote ID
    - Displays the string assigned to the Option 82 remote ID.

- Circuit ID
  - Displays information assigned to the Option 82 circuit ID.
- Press the "Setting" button to access a page where you can change the settings of the selected VLAN.
- Press the "Specify all" button to configure the settings for all VLAN interfaces with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all VLAN interfaces with the check box selected.

### Interface settings

- Displays the DHCP snooping function setting for each interface.
- The table items are explained below.
  - Port
    - Displays the name of port for which the settings is to be changed.
  - Port type
    - Displays whether the corresponding port is trusted or untrusted.
  - Subscriber ID
    - Displays the string assigned to the Option 82 subscriber ID.
- Press the "Setting" button to display the page for configuring the selected interface.
- Press the "Specify all" button to configure the settings for all interfaces with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected.

### Display Binding Database page

This page displays information about DHCP clients registered in the binding database.

### Binding database

- Displays information on DHCP clients registered in the binding database.
- Up to 256 items will be displayed.
- You can search neighbor information from the "Search" box.
  - Press  to execute the search.
  - Press  to clear the search.
  - You can use regular expressions shown below in search keywords.
  - Lowercase and capital letters are treated the same for keywords.

Syntax	Explanation
A	The character "A"
ABC	The characters "ABC"
[ABC]	One character, either "A", "B" or "C"
[A-C]	One character between "A" and "C"
[^ABC]	An arbitrary character that is neither "A", "B" or "C"
.	An arbitrary character
A+	At least one "A" character

Syntax	Explanation
A*	At least zero "A" characters
A?	Zero or one "A" character
^A	A string that begins with "A"
A\$	A string that ends with "A"
ABC DEF GHI	"ABC", "DEF" or "GHI"
A{2}	Two "A" characters (AA)
A{2,}	Two or more "A" characters (AA, AAA, AAAA...)
A{2,3}	Two to three "A" characters (AA, AAA)
\b	Word breaks, such as spaces
\B	Any character besides \b
\d	An arbitrary number (same as [0-9])
\D	Any character besides numbers (same as [^0-9])
\s	Single breaking character
\S	Any single character besides \s
\w	Alphanumeric characters including underlines (same as [A-Za-z0-9_])
\W	Any character besides \w

- Press  to update information to the latest information.
- The number of search results to display at one time can be selected by pressing "Display number" on the "Select" menu.
- Press the sort switch to sort by each item.
  - With default settings, results are sorted in ascending order of the VLAN ID.
  - Press the sort switch again to toggle between ascending and descending order.

### System settings page

This page is for configuring DHCP snooping in the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- DHCP snooping function for the entire system
  - Selects whether to enable / disable the DHCP snooping function for the entire system.
- MAC address verification
  - Selects whether to enable / disable the MAC address verification on the Untrusted port.
- DHCP packets receiving rate limit
  - Enters the number of DHCP packets that can be received per second.
- Option 82 function

- Selects whether to enable / disable Option 82 information assignment, inspection, and deletion.
- Forward packets with Option 82
  - Selects whether to enable / disable forwarding packets with Option 82 on the Untrusted port.
- Output to SYSLOG
  - Selects whether to enable / disable output to SYSLOG.

### VLAN Interface settings page

This page is for configuring DHCP snooping on the VLAN interface.

You can also change the detailed settings by pressing the "Advanced settings" button.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### VLAN interface settings

- VLAN ID
  - Displays the VLAN ID for which the setting is to be changed.
- DHCP snooping function
  - Selects whether to enable/disable the DHCP snooping function for the corresponding VLAN ID.
- Remote ID
  - Enters the character string to be assigned to Option 82 remote ID.
  - Enter up to 63 single-byte alphanumeric characters/symbols, excluding the ? symbol.
- Circuit ID
  - Enters the character string to be assigned to Option 82 circuit ID.
  - Enter up to 63 single-byte alphanumeric characters/symbols, excluding the ? symbol.

### Interface settings page

This page is for setting DHCP snooping on the interface.

You can also change the detailed settings by pressing the "Advanced settings" button.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Interface settings

- Port
  - Displays the port name to configure the settings.
- DHCP snooping function
  - Port type
- Subscriber ID
  - Enters the character string to be assigned to Option 82 subscriber ID.
  - Enter up to 50 single-byte alphanumeric characters/symbols, excluding the ? symbol.

# Layer 3 functions

## DNS client

### Summary

This page is for configuring the DNS client settings.

### Top page

This is the top page for the DNS client.

### DNS client settings

- Displays the DNS client settings.
- The table items are explained below.
  - DNS client functions
    - Displays the settings for whether to enable or disable the DNS client function.
  - DNS server address
    - Displays the DNS server address settings used during inquiry for name resolution.
  - Default domain
    - Displays the default domain settings.
  - Search domain
    - Displays the search domain settings.
- Displays **(DHCP)** as a suffix for DNS server address and domain obtained by DHCP client function.
- Displays **(DHCPv6)** as a suffix for DNS server address and domain obtained by DHCPv6 client function.
- Press the "Setting" button to access a page where you can configure the DNS client settings.

### DNS client settings page

This page is for configuring the DNS client settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### DNS client settings

- DNS client functions
  - Select the operation for the DNS client function from the following options.
    - Enable
    - Disable
- DNS server address
  - Specify the DNS server address.
  - For the server address, either an IPv4 address or an IPv6 address can be specified.
  - Up to three server addresses can be specified.
- Default domain
  - Specify the default domain.
  - Up to 256 characters can be inputted.
- Search domain

- Specify the search domain.
- Up to 256 characters can be inputted.
- Up to six search domains can be specified.

## Routing

### Summary

This page is for configuring the routing settings.

### Top page

This is the top page for routing.

### Routing function basic settings

- The current settings for the routing function are shown.
- When you press the "Setting" button, a page where you can change the routing function settings will appear.

### Routing table

- Displays the routing table details.
- The table items are explained below.
  - Check box
    - Select the check box to delete static route information.
  - Enabled route
    - For the route used in actual communications,  Enabled will be displayed.
    - For the routes not used for actual communications,  Disabled will be displayed.
  - Kind
    - Displays one of the following route information types.
      - static
      - connected
  - Destination
    - Displays the destination network address for the route information.
    - If the destination is a default gateway, **default** will be displayed.
  - Gateway
    - Displays the route information gateway.
    - **Null** is displayed for settings to discard packets.
  - Priority
    - Displays the administrative distance for route information.
- Press the "New" button to display a page where you can create new settings for static route information.
- Press the "Setting" button to display a page where you can change the settings for the selected static route information.
- If you press the "Delete" button, all static route information for which the check boxes are selected will be deleted.
- A check box and "Settings" button is displayed for the static route information entry.
- Up to 128 static route information entries can be displayed.
  - When 128 static route information entries are displayed, the "New" button is disabled.

---

### Routing function basic setting page

In this page you can specify whether the routing function is used.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Routing function basic setting page

- Routing function

Select the routing function from the following items.

- Use routing function
- Don't use routing function

### Static route information settings page

This page is for configuring the static route information settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Static route information settings

- Destination network

- When configuring new settings
  - Select a destination network from the following networks.
    - Specifying a network address
      - Input the destination network address.
    - Default gateway

- When changing settings
  - The destination network address is displayed.

- Gateway

- Select from one of the following gateways.
  - Specifying an IP address
    - Input the gateway IP address.
  - Discarding a packet without forwarding

- Priority

- Input the priority.
- The input range is 1 - 255.

---

# Multicast

## Multicast basic settings

### Summary

This page is for basic settings related to multicast.  
Specify processing method for unknown multicast frames.

Unknown multicast frames are frames destined to addresses not registered in IGMP snooping. This product forwards unknown multicast frames to allports as the default setting, which does not matter in low bandwidth environments. However, discarding instead of forwarding in high bandwidth environments may be recommended.

If you want to discard unknown multicast frames and only forward some multicast frames that use link local addresses such as asmDNS, you can exclude them from discarding.

### Top page

This is the top page for multicast basic settings.

### System settings

- Displays the configuration for unknown multicast frames for the entire system.
- The table items are explained below.
  - Processing method for unknown multicast frames
    - Displays the processing method of unknown multicast frames.
  - Excluded frames from discarding (for all VLANs)
    - Displays excluded frames from discarding when configured to discard unknown multicast frames.
- Press the "Setting" button to access a page where you can change the settings.

### VLAN interface settings

- Displays the configuration for unknown multicast frames for each VLAN.
- The table items are explained below.
  - VLAN ID
    - VLAN ID is displayed.
  - Unknown multicast frame
    - Displays the processing method for unknown multicast frames for the target VLAN.
  - Excluded frames from discarding
    - Displays the frames to be excluded from discarding when unknown multicast frames are configured to be discarded in the target VLAN.
- Press the "Setting" button to access a page where you can change the settings of the selected VLAN.
- Press the "Specify all" button to configure the settings for all VLAN interfaces with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all VLAN interfaces with the check box selected.

### System settings page

This page is for configuring unknown multicast frames for the entire system.  
Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## System settings

- Processing method for unknown multicast frames
  - Specify the processing method for unknown multicast frames from below.
    - Flood
    - Discard
- Excluded frames from discarding (for all VLANs)
  - Specify the excluded frames from discarding when configured to discard unknown multicast frames.
  - Specify the following conditions for excluded frames from discarding.
    - Link local address
      - Set all addresses in 224.0.0.0/24 and ff02::/112 as the target.
      - This setting is for all VLANs.
      - This setting is not included in the number of configurable settings for the entire system.

## VLAN Interface settings page

This page is for configuring unknown multicast frames for a VLAN interface.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## VLAN interface settings

- VLAN ID
  - Displays the VLAN ID for which the setting is to be changed.
- Processing method for unknown multicast frames
  - Specify the processing method for unknown multicast frames from below.
    - Follow the system setting
    - Prefer the interface setting
      - Flood
      - Discard
- Excluded frames from discarding
  - Specify the excluded frames from discarding when configured to discard unknown multicast frames.
  - Specify the following conditions for excluded frames from discarding.
    - Destination address
      - Specify the address type from the following.
        - Specify the address
          - Enter the IPv4 multicast address into the text box.
        - mDNS
          - Set 224.0.0.251 as the target.
        - Dante
          - Set 224.0.0.230 - 233 as the target.

- PTP
  - Set 224.0.1.129 - 132 and 239.254.3.3 as the target.
- Press the  icon to add a new row.
- Press the "Delete" button to delete the row.
- You can specify up to 100 addresses to be excluded from the discarding for the entire system.
  - If specifying Dante as the address type, one item is counted as four items.
  - If specifying PTP as the address type, one item is counted as five items.

---

## IGMP snooping

### Summary

In this page you can edit the settings of the IGMP snooping function.

### Top page

This is the top page for IGMP snooping.

### IGMP snooping function settings

- IGMP snooping function settings are shown for each VLAN ID that is defined
- A maximum of 20 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- When you press the "Setting" button, a pagewhere you can change the IGMP snooping function settings for theselected VLAN ID will appear
- If you press the "Specify all" button, the settings can be changed for all VLAN IDs whose check box contains a check mark
- If you press the "Return to defaults" button,the settings will be initialized for all VLAN IDs whose check boxcontains a check mark
  - Default settings for the IGMP snooping function are as follows
    - IGMP snooping function: Disabled
    - IGMP version: IGMPv3
    - IGMP query: No transmission
    - IGMP query transmission interval: 125 seconds
    - TTL check: Enabled
    - RA check : Disabled
    - ToS check : Disabled
    - Multicast router port : None
    - Data transfer suppression function for multicast router ports : Disabled
    - Report suppression function : Enabled
    - Report forwarding function : Disabled
    - Fast leave function : Disabled

### IGMP snooping function settings page

In this page you can make various settings for the IGMP snooping function.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### IGMP snooping function settings

- VLAN ID
  - The VLAN ID for which settings are being made is shown
- IGMP snooping settings
  - Enabled ( Control transmission of IP multicast packets )
    - Enable IGMP snooping.  
Multicast packets are forwarded only to the port to which the terminal you want to receive

them is connected.

This function monitors (snoops) IGMP messages exchanged between receiving terminals and a multicast router. It can suppress the flooding of multicast packets and reduce network bandwidth usage.

- Disabled ( Flood IP multicast packets )
  - Disable IGMP snooping  
Multicast packets are always forwarded to all ports in the same VLAN.
- Version
  - Select the IGMP version from the following items.
    - IGMPv3
    - IGMPv2
- IGMP query
  - No transmission  
IGMP query transmission function is disabled
  - Transmit periodically  
IGMP query transmission function is enabled. The transmission interval can be specified in the range of 20 seconds to 18000 seconds
- TTL check

Select the TTL check from the following items.

  - Enabled ( IGMP packets other than TTL=1 are discarded )
  - Disabled ( IGMP packets other than TTL=1 are corrected to TTL=1 and transmitted )
- RA check

Select the RA check from the following items.

  - Disabled ( RA option is added to IGMP packets and transmitted )
  - Enabled ( IGMP packets without a RA option are discarded )
- ToS check

Select the ToS check from the following items.

  - Disabled ( ToS is corrected to 0xc0 in IGMP packets and transmitted )
  - Enabled ( IGMP packets with invalid ToS are discarded )
- Multicast router port
  - The multicast router port is the interface to which the multicast router is connected. This device automatically learns the interface that receives the IGMP query as the multicast router port. Also, you can statically configure the multicast router port.
  - To statically configure multicast router ports, press the "Select" button. The interfaces that belong to the specified VLAN ID are listed. Then, check the check box of the interface to use as the multicast router port, and press the "Confirm" button.
- Data transfer suppression function for multicast router ports
  - This function suppresses network traffic load by stopping unnecessary multicast frames transfer to the multicast router port.
  - Select from the following items.
    - Disable

- 
- Disabling this function causes multicast frames to be transferred to the multicast router port as well if any port is receiving IGMP report messages.
  - Enable
    - Enabling this function causes multicast frames to be transferred to the multicast router port as well only when the multicast router port receives IGMP report messages.
  - Report suppression function
    - This function suppresses the network traffic load between the multicast router and the host.
    - Select from the following items.
      - Enable
        - Enabling this function transfers received IGMP report and leave messages to the IGMP querier at once.
      - Disable
        - Disabling this function transfers received IGMP report and leave messages to the IGMP querier as is without combining them.
  - Report forwarding function
    - This function transfers IGMP report and leave messages to the port where a switch is connected in the same VLAN.
    - The System Capabilities information included in the LLDP Basic Management TLV is used to judge whether a switch is connected to the port or not.
    - Select from the following items.
      - Enable
        - Enabling this function transfers received IGMP report and leave messages to the multicast router ports and the ports where a switch is connected.
      - Disable
        - Disabling this function transfers received IGMP report and leave messages to the multicast router ports only.
  - Fast leave function
    - Fast leave function is a function not to check the receiver's existence in the IGMP leave process.
    - This function is effective when only one receiver is connected to the LAN/SFP port.
    - Select from the following items.
      - Disable
        - Disable the fast leave function.  
The IGMP leave process sends a group-specific query to check the receivers' existence.
      - Enable
        - Enable the fast leave function.  
The IGMP leave process does not check the receiver's existence.
        - If you check the "Disable on ports where a switch is connected" check box, the fast leave function will not be used on ports where the switch is connected.
-

## MLD snooping

### Summary

In this page you can edit the settings of the MLD snooping.

### Top page

This is the top page for MLD snooping.

### MLD snooping settings

- MLD snooping settings are shown for each VLAN ID that is defined.
- A maximum of 20 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- When you press the "Setting" button, a page where you can change the MLD snooping settings for the selected VLAN ID will appear.
- If you press the "Specify all" button, the settings can be changed for all VLAN IDs whose check box contains a check mark.
- If you press the "Return to defaults" button, the settings will be initialized for all VLAN IDs whose check box contains a check mark.
  - Default settings for the MLD snooping are as follows.
    - MLD snooping : Disabled
    - Version : MLDv2
    - MLD query : No transmission
    - MLD query transmission interval : 125 Seconds
    - Multicast router port : None
    - Report suppression function : Enabled
    - Fast leave function : Disabled
- You cannot configure MLD snooping when the stack function is enabled.

### MLD snooping settings page

In this page you can make various settings for the MLD snooping.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### MLD snooping settings

- VLAN ID
  - The VLAN ID for which settings are being made is shown.
- MLD snooping
  - Enabled ( Control transmission of IPv6 multicast packets )
    - Enable MLD snooping  
Multicast packets are forwarded only to the port to which the terminal you want to receive them is connected.  
This function monitors (snoops) MLD messages exchanged between receiving terminals and a multicast router. It can suppress the flooding of multicast packets and reduce network bandwidth usage.
  - Disabled ( Flood IPv6 multicast packets )

- 
- Disables the MLD snooping  
Multicast packets are always forwarded to all ports in the same VLAN.
  - Version
    - Select the MLD version from the following items.
      - MLDv1
      - MLDv2
  - MLD query
    - No transmission  
MLD query transmission function is disabled.
    - Transmit periodically  
MLD query transmission function is enabled. The transmission interval can be specified in the range of 20 seconds to 18000 seconds.
  - Multicast router port
    - The multicast router port is the interface used to connect multicast routers.  
This device automatically learns the interface that receives the MLD query as the multicast router port. Also, you can statically configure the multicast router port.
    - To statically configure multicast router ports, press the "Select" button. The interfaces that belong to the specified VLAN ID are listed.  
Then, check the check box of the interface to use as the multicast router port, and press the "Confirm" button.
  - Report suppression function
    - This function suppresses the network traffic load between the multicast router and the host.
    - Select from the following items.
      - Enable
        - Enabling this function transfers received MLD report and leave messages to the MLD querier at once.
      - Disable
        - Disabling this function transfers received MLD report and leave messages to the MLD querier as is without combining them.
  - Fast leave function
    - Fast leave function is a function not to check the receiver's existence in the MLD leave process.
    - This function is effective when only one receiver is connected to the LAN/SFP port.
    - Select from the following items.
      - Disable
        - Disable the fast leave function.  
The MLD leave process sends a group-specific query to check the receivers' existence.
      - Enable
        - Enable the fast leave function.  
The MLD leave process does not check the receiver's existence.
-

---

# Traffic control

## Access list

### Create Access list

#### Summary

In this page you can create or delete access lists, and change their settings.

#### Top page

This is the top page for creating an access list.

#### Access lists

- The information for the access list you created will be displayed.
- The table items are explained below.
  - ID
    - The access list ID will be displayed.
  - Type
    - The access list type will be displayed.
  - Description
    - The description text set in this access list will be displayed.
- A maximum of 20 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- You can press the sort switch to sort by each item.
- Press the "New" button to display the page where you can create a new access list.
- Press the "Setting" button to show the page where you can change the settings of the selected access list.
- If you press the "Delete" button, all access lists whose check boxes are selected will be deleted.
  - Access lists that are applied to class maps cannot be deleted.
- On this page, you can reference and configure up to 512 access lists.

#### Access list settings page

This page is for creating new access lists, or for changing the settings of existing access lists.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

#### Access list settings

- Access list
  - Select the access list type from the following items.
    - IPv4 access list
    - IPv6 access list
    - MAC access list
  - When changing the settings, the access list type cannot be changed.
  - The IPv6 access list settings cannot be configured when the stack function is enabled.

- Access list ID
  - Set the configurable access list ID from the following ranges, according to the access list type.
    - IPv4 access lists
      - 1 - 2000
    - IPv6 access lists
      - 3001 - 4000
    - MAC access lists
      - 2001 - 3000
  - When changing the settings, the access list ID cannot be changed.
- Description
  - Specify the description text using up to 32 single-byte alphanumeric characters and symbols.
  - The "?" character cannot be used in the description text.
- Control conditions
  - Specify the control conditions for the access list.
  - Up to 256 control conditions can be configured per access list.
  - Press the "Add" button to display the "Control condition settings" dialog.
  - In the "Control condition settings" dialog, you can specify conditions for which traffic is permitted and denied as per the following items.
    - Operation
      - Select the actions to be taken when the traffic matches the control conditions, shown in the items below.
        - Permit
        - Deny
    - Source address
      - Select the source address to be targeted from the following items.
        - All addresses
        - Specify host address
        - Specifying a network address
          - This cannot be specified for a MAC access list.
        - Specify host address with wildcard bit
          - Specify the address and wildcard mask.
          - This cannot be specified for a IPv6 access list.
      - If the wildcard mask bit is "1," the bit in the same address position will not be checked.
      - When specifying the conditions for subnet 192.168.1.0/24, do so as shown below.
        - Address : 192.168.1.0, Wildcard mask : 0.0.0.255
      - When specifying the conditions for vendor code 00-A0-DE---\*, do so as shown below.
        - Address : 00A0.DE00.0000, Wildcard mask : 0000.00FF.FFFF
    - Destination address
      - The details for the items to be set for the destination address are equivalent to those of the **source address**.
      - This cannot be specified for a IPv6 access list.

- Protocol
  - Select the protocol to be targeted from the following items.
    - All protocols
    - TCP
    - UDP
    - ICMP
    - Specify protocol number
      - Input a protocol number from 0 to 255.
  - When selecting TCP or UDP as a protocol, specifying the source and destination port numbers.
    - You can specify either a single number or a number range for the port number.
    - Input a port number from 0 to 65535.
  - When selecting TCP as a protocol, you can specify the conditions regarding the TCP vendor control flag.
    - If more than one bit is specified, it works under the AND condition. Packets with all the specified bits set to 1 are targets.
    - For example, you can deny only TCP connections from outside to inside by allowing only packets with ACK bit or RST bit of 1 for the interface's direction.
    - In this case, you need to set two control conditions. One is to allow packets with an ACK bit value of 1, and the other is to allow packets with an RST bit value of 1.
  - This cannot be specified for a MAC access list or a IPv6 access list.
- Press the "Delete" button to delete the corresponding control conditions.
- Press the ▲ or ▼ icons to change the order in which the control conditions are applied.
- When evaluating the control conditions, control conditions with earlier numbers will be evaluated first; and if the conditions match, the conditions that follow will not be checked.

---

## Apply Access list

### Summary

Apply the access list for the interface on this page.

### Top page

This is the top page for applying the access list.

### Interface list

- The access list information applied to the interface is displayed.
- The table items are explained below.
  - I/F
    - Displays the interface name.
  - Access list (IN)
    - The information listed below for the access list applied to the input side of the interface is shown here.
      - ID
        - The access list ID will be displayed.
      - Type
        - The access list type will be displayed.
      - Description
        - The description text set in this access list will be displayed.
  - Access list (OUT)
    - Information for the access list applied to the input side of the interface is shown here.
    - Information similar to the access list (IN) will be displayed.
- Press the "Setting" button to display the page where you can change the settings of the selected interface.
- If you press the "Specify all" button, the settings can be changed for all interfaces whose check box is selected.
- If you press the "Return to defaults" button, the settings will be initialized on all interfaces whose check boxes are selected.

### Selection page for access lists to apply

This page is for selecting the access list to apply to the interface.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Select access list to apply

- Applicable interface
  - The interface on which the access list will be applied is displayed.
- Access list to apply (IN)
  - Select the access list to apply to the input side of the interface.
  - Press the "Select" button to display the file "Access list selection" dialog box.
  - On the "Access list selection" dialog, you can select the check box for an access list and press the "OK" button to select the access list to apply.

- Press the "Detail" button in the "Access list selection" dialog box to display the targeted access list.
  - In the IPv4 access list which specifies port numbers by range, only one interface can be applied for the entire system.
  - The number of control conditions that can be applied to an interface are 512 for the entire system.
  - Applying an access list to one interface will decrease a number of applicable control conditions equal to the control conditions included in the access list.
  - For example, when an access list with five specified control conditions is applied to the input side of port 1.1, the number of control conditions that can be applied is decreased by 5.
  - Note that the number of control conditions that can be actually applied is less than 512, because the control conditions are also used in the system and other functions.
- Access list to apply (OUT)
    - Select the access list to apply to the output side of the interface.
    - The setting details for the access list (OUT) to be applied **are equivalent to the access list (IN) to be applied.**
    - IPv4 access lists which specify port numbers by range cannot be applied to the output side.
    - MAC access lists cannot be applied to the output side of an interface.
    - Access lists cannot be applied to the output side of a logical interface.

---

## QoS

### Summary

In this page you can edit the settings of the QoS (Quality of Service) function. You can enable/disable the QoS function, and change the trust mode.

### Top page

This is the top page for QoS.

### Web conference applications optimization

- The "Next" button starts the procedure to configure the optimal QoS settings for the web conference application.

### System settings

- Displays the QoS settings for the entire system.
- The table items are explained below.
  - QoS function
    - Displays whether the QoS function is enabled.
  - CoS - transmit queue mapping table
    - Displays the transmit queue ID settings corresponding to the CoS value.
  - DSCP - transmit queue mapping table
    - Displays the transmit queue ID settings corresponding to the DSCP value.
- Press the "Setting" button to access a page where you can change the settings
- To enable the QoS function, you must disable flow control.

### Interface settings

- The trust mode setting used by the QoS function is shown for each LAN/SFP port
- Press the "Setting" button to access a page where you can change the settings of the selected LAN/SFP port
- If you press the "Specify all" button, the settings can be changed for all LAN/SFP ports whose check box contains a check mark
- If you press the "Return to defaults" button, the settings will be initialized for all LAN/SFP ports whose check box contains a check mark
  - The default trust mode setting for all ports is "CoS"
  - The default CoS value for all ports is "0" by default.
- If the settings do not use the QoS function, QoS function settings cannot be made

### Web conference applications optimization page

This page provides optimal QoS settings for web conference applications.

When you have inputted the settings, press the "Confirm" button.

If there are no mistakes in the input content confirmation screen, press the "OK" button.

The following settings are configured in the Optimal Settings for Web conference application.

- Enables QoS.
- Set trust mode to DSCP for all ports.
- Assigns the DSCP value used by the web conference application to be optimized to the highest priority outgoing

queue.

- Assigns the DSCP value not used by the web conference application to be optimized to the lowest priority outgoing queue.
- Sets scheduling of all transmit queues to Strict Priority.

### Web conference applications optimization

- Target application
  - Select the web conference application to be optimized.

### System settings page

In this page you can specify whether the QoS function is used.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

Be aware that if the settings do not use the QoS function, all QoS-related settings will be cleared.

### System settings

- QoS function
  - Disable
    - The QoS function will be disabled. At this time, all QoS settings will be cleared.
  - Enable
    - The QoS function will be enabled. QoS-related settings and commands can be executed.
- CoS - transmit queue mapping table
  - Configures the transmit queue ID settings corresponding to each CoS value.
  - The input range of the transmit queue ID is 0 to 7, and a larger ID has a higher priority for sending frames.
  - If you press the "Easy input" button, the following settings can be entered together into the CoS - transmit queue mapping table.
    - Initialization
      - Factory default settings.
- DSCP - transmit queue mapping table
  - Configures the transmit queue ID settings corresponding to each DSCP value.
  - The input range of the transmit queue ID is 0 to 7, and a larger ID has a higher priority for sending frames.
  - When "Display only RFC compliance values" is checked, only RFC-compliant DSCP values will be displayed. However, all DSCP values will be displayed on the input confirmation screen.
  - If you press the "Easy input" button, the following settings can be entered together into the DSCP - transmit queue mapping table.
    - Initialization
      - Factory default settings.
    - Dante optimization
      - Assigns DSCP values used by Dante to the highest priority queue and unused DSCP values to the lowest priority queue.
    - Web conference applications optimization
      - Assigns DSCP values used by the web conference application to the highest priority queue and unused DSCP values to the lowest priority queue.

- Please select at least one web conference application.

## Interface settings page

Set the "Trust mode" setting which means whether the transmission queue is determined based on the packet's CoS value or the DSCP value or the Port priority.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## Interface settings

- Port
  - The LAN/SFP port for which settings are made is shown
- Trust mode
  - Use CoS value to determine transmission queue
    - The packet's CoS value and the "CoS - Transmission queue ID conversion table" are used to determine the transmission queue
    - If the received packet is an untagged packet, the default CoS value is applied
    - A default CoS value within the 0 - 7 range can be specified.
  - Use DSCP value to determine transmission queue
    - The packet's DSCP value and the "DSCP - Transmission queue ID conversion table" are used to determine the transmission queue
  - Use the priority specified for the port to determine the transmission queue
    - The transmission queue is determined according to the "Port priority order"
    - Select the transmission queue to be assigned as the port priority order in the range of 0 - 7. Higher numbers indicate a higher priority order; with the default settings, 2 is selected
    - The setting can be changed only if the trust mode is set to "Port priority"
  - If a policy map is applied to the LAN/SFP port, you cannot change the trust mode setting.

## Flow control

### Summary

This page is for configuring flow control (the IEEE 802.3x PAUSE frame transmission and reception).

### Top page

This is the top page for flow control.

### System settings

- Displays the current setting whether to use flow control (the IEEE 802.3x PAUSE frame transmission and reception) for the entire system.
- Press the "Setting" button to display the page for configuring the settings.
- To enable flow control for the entire system, you need to disable the QoS function.

### Interface settings

- Displays flow control settings for each LAN/SFP port.
- Press the "Setting" button to display the page for configuring the selected interface.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected.
- Press the "Specify all" button to configure the settings for all interfaces with the check box selected.

### System settings page

This page is for configuring flow control (the IEEE 802.3x PAUSE frame transmission and reception) for the entire system.

Once you have entered the settings, press the "Confirm" button.

If the input information on the confirm page is correct, press the "OK" button.

### System settings

- Flow control for entire system  
You can specify whether to enable or disable flow control for the entire system.  
Even if flow control for the entire system is enabled, flow control does not work for a port whose individual port setting is disabled.
- Constraints  
If flow control is enabled, the tail drop function is disabled. However, this excludes the case where the stack function is enabled.

### Interface settings page

This page is for configuring flow control (the IEEE 802.3x PAUSE frame transmission and reception) for the interface.

Once you have entered the settings, press the "Confirm" button.

If the input information on the confirm page is correct, press the "OK" button.

### Interface settings

- Flow control  
Specify whether to enable or disable flow control for LAN/SFP ports.  
If it is enabled, Pause frames are sent and received regardless of whether the target device supports flow control.

- Auto negotiation

Use auto negotiation to verify that the target device supports flow control.

If the target device does not support flow control, Pause frames are not sent or received.

- Constraints

- In the following cases, only receiving Pause frames is supported.

If the stack function is enabled

- In the following cases, auto negotiation does not work even if it is enabled.

When an SFP+ module is used

## Storm control

### Summary

This page is for changing the storm control settings.

If the storm control is enabled, the load on the unit can be reduced by discarding specific frames received that exceed bandwidth threshold values.

### Top page

This is the top page for the storm control settings.

### Storm control settings

- The current settings for the storm control are shown for each interface.
- The table items are explained below.
  - Check box
    - Select the check box for bulk settings or to initialize the settings.
  - Port
    - Displays the interface name.
  - Target frame
    - Displays the target frames for storm control.
  - Upper limit for bandwidth percent
    - Displays the upper limit for the bandwidth percentage.
    - Frames received that exceed the upper limit value are discarded.
- Press the "Setting" button to display the page where you can change the settings of the selected interface.
- If you press the "Specify all" button, the settings can be changed for all interfaces whose check box is selected.
  - The default settings will be applied to the settings on the storm control settings page.
- If you press the "Return to defaults" button, the settings will be initialized on all interfaces whose check boxes are selected.
  - The storm control is disabled for all ports by default.

### Storm control settings page

This page is for storm control settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Interface settings

- Port
  - Displays the name of the interface for which settings will be made.
- Storm control
  - Select the operation for the storm control from the following options.
    - Disable
    - Enable
- Target frame
  - Broadcast frame

- Enables broadcast storm control.
- Multicast frame
  - Enables multicast storm control.
- Unicast frame
  - Enables control for unicast frames sent from an unknown address.
- Upper limit for bandwidth percent
  - Specifies the upper limit value for the bandwidth percentage.
  - Upper limit values can be specified to two decimal places.
  - Frames received that exceed the upper limit value are discarded.
  - The same upper limit value is applied to all applicable frames.

# Application layer

## RADIUS server

### Server settings

#### Summary

This page is for performing operations related to the certificate authority and RADIUS server.

#### Top page

This is the top page for the RADIUS server.

#### Certificate authority management

- Press the “Next” button to the right of “Create certificate authority” to begin the process of creating a certificate authority.
- Press the “Next” button to the right of “Delete certificate authority” to begin the process of deleting the certificate authority.
- Press the “Next” button to the right of “Backup/restoration files and settings related to certificate authority” to begin the process of backing up or restoring.

#### RADIUS server settings

- Displays the settings for the RADIUS server.
- The table items are explained below.
  - RADIUS server usage
    - Displays whether a RADIUS server is to be used or not.
    - If a RADIUS server is to be used, the port number will be displayed.
  - Interfaces that can access the RADIUS server
    - Displays the interfaces that can access the RADIUS server.
  - Reauthentication interval configured for authenticator
    - Displays the settings for the reauthentication interval configured on the authenticator by the RADIUS server.
  - Authentication method
    - Displays the authentication method settings used by the RADIUS server.

#### RADIUS client list

- Displays the RADIUS client settings.
- The table items are explained below.
  - Check box
    - Select the check box to delete the RADIUS client settings.
  - IP address
    - Displays the RADIUS client address.
- A maximum of 20 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- You can press the sort switch to sort by each item.

- Press the "New" button to access a page where you can configure the settings for a new RADIUS client.
- Press the "Setting" button to access a page where you can change the selected RADIUS client settings.
- Press the "Delete" button to delete all RADIUS clients whose check boxes are selected.
- On this page, you can configure up to 100 RADIUS clients.

### Certificate authority creation page

This is the certificate authority creation page.

Enter the certificate authority name, and then press the "Confirm" button.

If there are no mistakes in the input content confirmation screen, press the "OK" button.

If a certificate authority already exists, you will not be able to create a certificate authority.

### Create a certificate authority

- Name
  - Specifies the certificate authority name.
  - Enter from 3 to 32 single-byte alphanumeric characters/symbols, with the following exceptions:  
**\\/?space**
  - You cannot set the name as **DEFAULT**.
  - If this is omitted, the name **swx-radius** will be automatically set.

### Certificate authority deletion page

This is the certificate authority deletion page.

Press the "OK" button to delete the certificate authority.

Deleting the certificate authority will delete all RADIUS-related settings, certificates and so on.

### Backup / Restoration page

This page is for backup/restoration of settings related to certificate authorities.

Enter the contents, and then press the "Confirm" button.

If there are no mistakes in the input content confirmation screen, press the "OK" button.

The following files and settings will be backed up and restored.

- Certificate authority
- Various certificates
- RADIUS client settings
- RADIUS user settings

### Backup / Restoration

- Content to execute
  - Select below whether a content to execute.
    - Back up
    - Restore
    - Import the backup file of a Yamaha wireless AP
- File to restore
  - Press the "Select a file" button to specify the file to restore.
  - When "Import the backup file of a Yamaha wireless AP" is selected, specify the file backed up on WLX402 or WLX313.

- zip file password
  - Enter up to 32 single-byte alphanumeric characters/symbols, with the following exceptions:  
**#&^\;|' }**
  - When backing up, enter the password set for the backup file.
  - When restoring or importing the backupfile of a Yamaha wireless AP, enter the password set for the backup file when it was backed up.
    - When using a file without a password, restore or import successfully with or without input of password.

## RADIUS server settings page

In this page you can configure the settings for a RADIUS server.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## RADIUS server settings

- RADIUS server usage
  - Select below whether a RADIUS server will be used.
    - Use
    - Don't use
  - When **Use** is selected, specify the port number.
  - Input a port number from 1024 to 65535.
  - When **Use** is selected, a certificate authority is created when the settings are made, if one does not already exist.
- Interfaces that can access the RADIUS server
  - Press the "Select" button to display the "VLAN interface list" dialog box.
  - You can select the port check box in the "VLAN interface list" dialog box and press the "OK" button to select the associated interface.
  - Up to 7 VLAN interfaces can be selected.
- Reauthentication interval configured for authenticator
  - Select the reauthentication interval configured on the authenticator from the options below.
    - 3600 Seconds
    - 43200 Seconds
    - 86400 Seconds
    - 604800 Seconds
- Authentication method
  - Select the authentication method used by the RADIUS server from the methods below.
    - PAP
    - PEAP
    - EAP-MD5
    - EAP-TLS
    - EAP-TTLS

---

## RADIUS client settings page

This page is for configuring the RADIUS client settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### RADIUS client settings

- IP address
  - Specifies the RADIUS client address.
  - Enter IPv4 addresses using the XXX.XXX.XXX.XXX format.
  - Enter IPv6 addresses using the XXXX:XXXX::XXXX.XXXX format.
  - When the settings are changed, the IP address of the selected RADIUS client will be displayed as text.
- Secret text string
  - Specifies the secret text string of the RADIUS client.
  - Enter up to 128 single-byte alphanumeric characters/symbols, with the following exceptions:  
**\\|\"?space**

## User management

### Summary

This page is for configuring the RADIUS user settings.

### Top page

This is the top page for RADIUS users.

### User settings

- Displays the settings for the RADIUS user.
- The table items are explained below.
  - Check box
    - Select the check box to delete the RADIUS user settings.
  - User ID
    - Displays the user ID for the RADIUS user.
  - Name
    - Displays the name of the RADIUS user.
  - Authentication method
    - Displays the authentication method for the RADIUS user.
  - VLAN
    - Displays the VLAN that can be accessed by the RADIUS user.
- Input the text string in the text box at the top of the table, and press the  icon to search for user information.
- The drop-down list box to the left of the text box lets you select one of the following items to filter the search parameters even further.
  - None
  - User ID
  - Name
  - Authentication method
  - VLAN
- A maximum of 100 items can be displayed for one page. Press  or  or enter a numeric value to switch between pages.
- You can press the sort switch to sort by each item.
- Press the “New” button to display a page where you can create new settings for the RADIUS user.
- Press the “Setting” button to access a page where you can change the settings of the selected RADIUS user.
- Press the “Delete” button to delete the settings for all RADIUS users whose check boxes are selected.
- Press the “Import” button to display a page where you can import settings for the RADIUS user.
- Press the “Export” button to export the settings for RADIUS users as a CSV file.
- On this page, you can configure up to 2000 RADIUS users.

## User settings page

This page is for configuring the RADIUS user settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### User settings

- Select an authentication function
  - Select the authentication method used by the RADIUS user from the methods below.
    - 802.1X
    - MAC
    - Web
    - None
  - When the authentication method is selected, the items that must be entered and the items that do not need to be entered for the selected authentication function will become clear.
    - When using a Yamaha device as the authenticator, we recommend that you select an authentication function.
  - When **Not specified** is selected, all items will become selectable.
    - When using a non-Yamaha device as the authenticator, we recommend that you select **Not specified**.
  - When changing the settings, it is not possible to select anything besides **Not specified**.
- User ID
  - Specifies the user ID for the RADIUS user.
  - Specify a text string from 3 to 32 characters.
  - The characters that can be inputted depends on the type of authentication method.
    - For PAP, EAP-MD5, EAP-TTLS, and PEAP:
      - Single-byte alphanumeric characters/symbols, with the following exceptions: `\|'?"space`
    - For EAP-TLS:
      - Single-byte alphanumeric characters/symbols, with the following exceptions: `\|/:<>|"?"space*`
  - You cannot set the name as **DEFAULT**.
  - When using MAC authentication, input the MAC address for the user's terminal.
    - For the MAC address, use one of the following input formats according to the authenticator settings.
      - XX:XX:XX:XX:XX:XX
      - XX-XX-XX-XX-XX-XX
      - XXXXXXXXXXXXX
    - When **MAC authentication** is selected for "Select an authentication function," the MAC address that was entered will be automatically reflected in the "Password" and "Password (confirm)" fields.
- Password
  - Specifies the password for the RADIUS user.
  - Enter up to 32 single-byte alphanumeric characters/symbols, with the following exceptions: `\|'?"`
  - When using MAC authentication, input the MAC address for the user's terminal.

- Password ( Confirm )
  - To confirm, enter the password once again that you entered in the "Password" field.
- Authentication method
  - Select the authentication method used to authenticate the RADIUS user from the methods below.
    - PAP
    - PEAP, EAP-MD5, EAP-TTLS
    - EAP-TLS
- Name
  - Specifies the name of the RADIUS user.
  - Enter up to 32 single-byte alphanumeric characters/symbols, with the following exception: ?
- Terminal MAC address
  - Input this address when you wish to control access by using a supplicant MAC address in addition to authentication via user ID and password.
  - Enter the address using the XXXX.XXXX.XXXX format.
- VLAN
  - Specifies the VLAN to assign to the user via dynamic VLAN.
  - Input a VLAN from 1 to 4094.
- SSID of connected device
  - For users that are authenticated via a wireless AP, this specifies the SSID that can be used to connect.
  - Enter up to 32 single-byte alphanumeric characters/symbols, with the following exceptions: \
- Recipient e-mail address for certificates
  - Specify the e-mail recipient addresses used when sending client certificates.
  - Input up to 256 single-byte alphanumeric characters and single-byte symbols.
  - You cannot use symbols other than \_-, and @.
- Period of certificate validity
  - Specifies the period of validity that is set when creating a client certificate.
  - Enter the date in YYYY/MM/DD format.
  - Dates from the current system date to 2037/12/31 can be entered for the period of validity.

### User settings import page

This page is for importing the RADIUS user settings.

Enter the contents, and then press the "Confirm" button.

If there are no mistakes in the input content confirmation screen, press the "OK" button.

The client certificates for users that were deleted during import will automatically be revoked.

### Import user settings

- File to import
  - Select the CSV file to import.
- Issue a certificate
  - Select below whether to issue a client certificate after the import is completed.
    - Issue a certificate for users whose settings have been changed, and send e-mail

- Issue a certificate for users whose settings have been changed
- Do not issue a certificate

## Managing certificates

### Summary

This page is for performing certificate-related operations.

### Top page

This is the top page for certificate operations.

### Mail notification settings

- Displays e-mail notification-related settings for certificates.
- The table items are explained below.
  - Mail template ID for sending certificates
    - Displays the mail template ID to be used when attaching and sending a client certificate via e-mail.
  - Mail template ID for certificate period of validity notifications
    - Displays the mail template ID to be used when attaching and sending a client certificate period of validity notification via e-mail.
  - Timing of period of certificate validity notifications
    - Displays the settings for the timing used to send the period of validity notifications for client certificates.

### User list

- Displays the certificate information for the RADIUS user.
- The table items are explained below.
  - Check box
    - Select the check box to issue, revoke or download a certificate.
  - User ID
    - Displays the user ID for the RADIUS user.
  - Name
    - Displays the name of the RADIUS user.
  - Mail address
    - The RADIUS user e-mail addresses will be displayed.
  - Period of validity (Settings)
    - Displays the certificate's period of validity for the RADIUS user.
  - Period of validity (certificate)
    - Displays the period of validity of the client certificate associated with a RADIUS user.
    - If there are multiple client certificates, the certificate with the most recent period of validity will be shown.
- Input the text string in the text box at the top of the table, and press the  icon to search for user information.
- The drop-down list box to the left of the text box lets you select one of the following items to filter the search parameters even further.
  - None
  - User ID

- Name
- Mail address
- Certificates not issued
- Expired certificates
- Certificates soon to expire
  - Displays users whose certificates will expire within one month.
- Certificates revoked
- You cannot specify a search text string when selecting either **Certificates not issued**, **Expired certificates**, **Certificates soon to expire** or **Certificates revoked**.
- A maximum of 100 items can be displayed for one page. Press ◀ or ▶ or enter a numeric value to switch between pages.
- You can press the sort switch to sort by each item.
- Press the “Issue” button in the “Specified users” box to issue certificates for all RADIUS users whose check boxes are selected.
  - You can select the check box for **Attach certificates issued and send via e-mail** that is displayed in the dialog box and press the “OK” button to attach and send the issued certificates via e-mail.
  - The e-mail recipients are the e-mail addresses of each RADIUS user.
- Press the “Revoke” button in the “Specified users” box to revoke certificates for all RADIUS users whose check boxes are selected.
  - Select the certificate which will be revoked from the list below.
    - Old certificates
    - New certificates
    - Both
  - For users with only one certificate, the certificate is revoked regardless of which of the above is selected.
- Press the “Download” button in the “Specified users” box to download the certificates for all RADIUS users whose check boxes are selected.
- Press the “Send” button in the “Specified users” box to attach and send the certificates for all RADIUS users whose check boxes are selected.
- Press the “Download” button in the “All users” box to download the certificates for all RADIUS users.
- Press the “Send” button in the “All users” box to attach and send the certificates for all RADIUS users via e-mail.
- Some operations will be restricted for the statuses shown below.
  - The certificate authority does not exist
  - Certificate is being issued
- If a user exists whose certificate has not been issued, a notification will be shown in the blue information box.
  - Press the “Bulk issue” button to issue client certificates in bulk, for users corresponding to the following.
    - Users who have never issued certificate
    - Users who was changed password or expire after issued certificate
- The progress will be shown in the blue information box while the certificates are being issued.

## Mail notification settings page

This page is for settings related to certificate e-mail notifications.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Mail notification settings

- Mail template ID for sending certificates
  - Select the mail template ID.
- Mail template ID for certificate period of validity notifications
  - Select the mail template ID.
- Timing of period of certificate validity notifications
  - Specify the timing of the period of certificate validity notifications.
  - Input a value from 1 to 90.
  - Up to three can be specified.

## Certificate operations page

This page is for performing certificate-related operations.

Enter the contents, and then press the "Confirm" button.

If there are no mistakes in the input content confirmation screen, press the "OK" button.

### Certificate operations

- Certificate to operate
  - Information for the target certificate for the operation will be displayed.
  - Select the check box of the certificate for which the operation is performed.
- Content to execute
  - Select the certificate operation from the list below.
    - Download certificate
    - Attach certificates and send via e-mail
    - Set certificate to revoke

---

# Maintenance

## Unit settings

### Summary

Various settings can be specified for the unit.

### Top page

This is the top page for unit settings. A description of each setting is shown.

### Unit name setting

Displays the unit name that is set.

- Press the "Setting" button to access a page where you can change the settings.

### LED mode setting

Displays the LED mode that is set.

- Press the "Setting" button to access a page where you can change the settings.

### Time zone setting

Displays the time zone setting.

- Press the "Setting" button to access a page where you can change the settings.

### Current date and time setting

The current date and time specified for this unit are shown.

- Press the "Setting" button to access a page where you can change the settings.

### Date and time synchronization setting

The NTP server that is queried at the specified time and date synchronization interval is shown.

- Press the "Next" button to access a page where you can synchronize the time.
- Press the "Setting" button to access a page where you can change the settings.

### Unit name setting page

In this page you can set the unit name.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

### Unit name setting

- Device name
  - Enter an arbitrary character string for use as the hostname.
  - Enter up to 63 single-byte alphanumeric characters/symbols, with the following exceptions: ?

---

## LED mode setting page

In this page you can set the LED mode.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

### LED mode setting

- LED mode
  - Select the LED mode from the following.
    - LINK/ACT mode
      - LED indicator lights will illuminate, flash, or switch OFF depending on the LAN port status.
    - PoE mode
      - LED indicator lights will illuminate or switch OFF depending on the PoE supply status.
      - Cannot be selected when the stack function is enabled
    - VLAN mode
      - LED indicator lights will illuminate or switch OFF depending on the VLAN belonging status.
      - Cannot be selected when the stack function is enabled
    - STATUS mode
      - LED indicator lights will illuminate, flash, or switch OFF depending on the error status of the following functions.
        - Loop detection
        - SFP optical reception level monitoring
        - PoE supply
      - Cannot be selected when the stack function is enabled
    - OFF mode
      - LED always stays off.

## Time zone setting page

This page is for configuring the settings related to time zone.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

### Time zone setting

- Time zone
  - Select the time zone from the following.
    - UTC
    - JST
    - Difference from GMT ( -12:00 to +13:00 )
- Daylight saving time
  - Select the daylight saving time operation from the following.
    - Disable

- 
- Enable
  - Time zone during daylight saving time
    - During daylight saving time, the time zone name specified in this item is displayed as the time zone abbreviation.
    - Enter up to 7 single-byte alphanumeric characters.
  - Daylight saving time period
    - Specify the date and time that daylight saving time starts and ends.
    - If you want to execute the specified period only once, select **By date** and enter the following.
      - Date
        - Enter in the format YYYY/MM/DD.
      - Time
        - Enter in the format hh:mm.
    - If you want to execute the specified period annually, select **Recurring** and enter the following.
      - Month
        - The input range is from January to December.
      - Week
        - Select from the following.
          - First
          - Second
          - Third
          - Fourth
          - Last
      - Day of week
        - Select from the following.
          - Sunday
          - Monday
          - Tuesday
          - Wednesday
          - Thursday
          - Friday
          - Saturday
      - Time
        - Enter in the format hh:mm.
  - Daylight saving time offset
    - Specify the time to advance at the start of daylight saving time.
    - The input range is from 1 to 1440 minutes.

### Current date and time setting page

In this page you can set the current date and time.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

---

## Current date and time setting

- Current time
  - In the "Year/Month/Day" box, enter the date in **YYYY/MM/DD** format.
    - When you move the focus to the box, a calendar is displayed. You can select a date to enter that date in the box.
    - You can also enter this manually.
  - In the "hours:minutes:seconds" box, enter the time in **hh:mm:ss** format.
    - When you move the focus to the box, a calendar is displayed. You can select a date to enter that date in the box.
    - You can also enter this manually.

## Date and time synchronization page

In this page you can synchronize the time with an NTP server.

When you press the "OK" button, the time is synchronized with the NTP server that is specified as the query destination.

## Date and time synchronization setting page

In this page you can make settings for synchronization with an NTP server.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

## Date and time synchronization setting

- Date and time synchronization interval
  - Specifies the interval at which time is synchronized with the NTP server.
  - You can choose from the following as the synchronization interval.
    - Unused
    - 1 hour – 24 hours
  - The default value is 1 hour
- NTP server to query
  - Enter the host name or IP address of the NTP server that will perform synchronization.
  - Up to two NTP servers can be configured.

---

>= Access management  
:leveloffset: 5

---

# User settings

---

# Summary

This page is for configuring the user settings.

## Top page

This is the top page for the user settings.

### Password settings

- Password-related settings are displayed.
- The table items are explained below.
  - Privileged password
    - Displays whether the privileged password has been set.
  - Encryption
    - The display will show whether password encryption is enabled.
- Press the "Setting" button to access the page where you can change the password-related settings.

### User account settings

- Displays a list of user account settings.
- The table items are explained below.
  - Check box
    - Select the check box to delete user account settings.
  - User name
    - Displays the user name.
  - Administrative privileges
    - Displays whether the user account has been given administrative privileges.
- Press the "New" button to display the page where you can set up a new user account.
- Press the "Setting" button to access a page where you can change the settings of the selected user account.
- If you press the "Delete" button, all user accounts whose check boxes are selected will be deleted.
- Settings can be made for up to 33 user accounts.
- There must be at least one user configuration that has administrative privileges.

---

# Password settings page

This page is for making password-related settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## Password settings

- Privileged password
  - Enter the privileged password that you want to set.
  - You can use up to 32 single-byte alphanumeric characters and symbols. (excluding "|>?space)
  - If the password is not changed, select the **Privileged password not changed** check box.
  - If a password has already been set, the **Privileged password not changed** check box will be selected by default.
  - Refer to the password strength when deciding on your password, which is displayed as you type.
  - The strength of the password is indicated in four levels from "weakest" to "strongest" based on the following conditions.
    - Number of characters
    - Types of characters
      - Uppercase alphanumeric characters included
      - Lowercase alphanumeric characters included
      - Numerals included
      - Symbols included
- Privileged password ( Confirm )
  - To confirm the password that you entered in the "Privileged password" field, enter the password once again.
- Encrypt password
  - Select the password encryption settings from the settings shown below.
    - Encrypt
    - Don't encrypt
  - You cannot restore a password that has been encrypted.
  - The settings for this field will affect the following passwords.
    - Privileged password
    - User account passwords

# User account settings page

This page is for configuring the user account settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## User account settings

- User name
  - When configuring new settings
    - Specifies the user name to set.
    - Single-byte alphanumeric characters can be inputted.
    - Up to 32 characters can be inputted.
    - The following text strings cannot be set.
      - lp
      - adm
      - bin
      - ftp
      - gdm
      - man
      - rpc
      - sys
      - xfs
      - halt
      - mail
      - news
      - nscd
      - sync
      - uucp
      - root
      - sshd
      - games
      - daemon
      - gopher
      - nobody
      - ftpuser
      - mtsuser
      - rpcuser
      - mailnull
      - operator
      - shutdown
  - When changing settings

- 
- Shows the selected user account name.
  - New password
    - Enter the new password that you want to set.
    - You can use up to 32 single-byte alphanumeric characters and symbols. (excluding "|>?space)
    - The operation for password strength is the same as the "Privileged password" item in the **Password settings** page.
  - New password ( Confirm )
    - To confirm the password that you entered in the "New password" item, enter the password once again.
  - Administrative privileges
    - Select from one of the following administrative privileges.
      - Do not set
      - Set
    - User accounts that have been given administrative privileges can log in as an administrative user when logging into the Web GUI.

## Various server settings

### Summary

In this page you can make settings for each type of server.

### Top page

This is the top page for making settings for each type of server.

The current settings are shown for the servers listed below.

- HTTP server
- Telnet server
- SSH server
- TFTP server
- SNMP server

### Web GUI access

- Displays the settings for the HTTP server.
- The table items are explained below.
  - Use HTTP server
    - Displays whether an HTTP server is to be used or not.
    - If an HTTP server is to be used, the port number will be displayed.
  - Use secure HTTP server
    - Displays whether a secure HTTP server is to be used or not.
    - If a secure HTTP server is to be used, the port number will be displayed.
  - Interfaces that can access the HTTP server
    - Displays the interfaces that can access the HTTP server.
    - You can access a management VLAN without server settings.
  - Clients that can access the HTTP server
    - Displays the clients that can access the HTTP server.
  - Time until auto logout
    - Displays the time for automatic logout.
  - Use HTTP proxy
    - Displays whether an HTTP proxy server is to be used or not.
    - If an HTTP proxy server is to be used, the timeout interval is displayed.

### Access via Telnet

- Displays the settings for the Telnet server.
- The table items are explained below.
  - Use Telnet server
    - Displays whether a Telnet server is to be used or not.
    - If a Telnet server is to be used, the port number will be displayed.
  - Interfaces that can access the Telnet server
    - Displays the interfaces that can access the Telnet server.

- You can access a management VLAN without server settings.
- Clients that can access the Telnet server
  - Displays the clients that can access the Telnet server.

### Access via SSH

- Displays the settings for the SSH server.
- The table items are explained below.
  - Use SSH server
    - Displays whether an SSH server is to be used or not.
    - If an SSH server is to be used, the port number will be displayed.
  - Interfaces that can access the SSH server
    - Displays the interfaces that can access the SSH server.
    - You can access a management VLAN without server settings.
  - Clients that can access the SSH server
    - Displays the clients that can access the SSH server.
  - Client existence check from SSH server
    - Displays whether the SSH server checks for existing clients.
    - If the SSH server is set to check for existing clients, this displays the check interval and the number of times checked before disconnecting.

### Access via TFTP

- Displays the settings for the TFTP server.
- The table items are explained below.
  - Use TFTP server
    - Displays whether a TFTP server is to be used or not.
    - If a TFTP server is to be used, the port number will be displayed.
  - Interfaces that can access the TFTP server
    - Displays the interfaces that can access the TFTP server.
    - You can access a management VLAN without server settings.

### Access via SNMP

- Displays the settings for the SNMP server.
- The table items are explained below.
  - Clients that can access the SNMP server
    - Displays the clients that can access the SNMP server.

### Web GUI access page

In this page you can configure the settings for an HTTP server.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

---

**Web GUI access**

- Use HTTP server
  - Select below whether an HTTP server will be used or not.
    - Use
    - Don't use
  - When "**Use**" is selected, specify the port number.
  - Input a port number from 1 to 65535.
- Use secure HTTP server
  - Select below whether an secure HTTP server will be used or not.
    - Use
    - Don't use
  - When "**Use**" is selected, specify the port number.
  - Input a port number from 1 to 65535.
- Interfaces that can access the HTTP server
  - Press the "Select" button to display the "VLAN interface list" dialog box.
  - You can select the port check box in the "VLAN interface list" dialog box and press the "OK" button to select the associated interface.
  - Up to 8 VLAN interfaces can be selected.
- Clients that can access the HTTP server
  - Select the client access restriction methods from the following options.
    - Permit all
    - Specify conditions
  - When "Specify conditions" is selected, up to 8 conditions can be specified.
  - The conditions are specified as shown below.
    - Operation
      - To restrict client access, select from the following operations.
        - Permit
        - Deny
    - Conditional
      - Select from the following targets for client access restriction.
        - All addresses
        - Specified IP address
    - IP address
      - When "**Specified IP address**" is selected, specify the IP address.
      - The following IP addresses shown below can be specified.
        - IPv4 address
          - Example: 192.168.100.1
        - IPv4 network address
          - Example: 192.168.100.0/24
        - IPv6 address
          - Example: fe80::1234:5678

- IPv6 network address
      - Example: 2001:1234:5678:90ab::0/64
    - Press the  icon to add a configuration form.
    - Press the "Delete" button to delete a configuration form.
- Time until auto logout
  - Specify the time for automatic logout.
  - The user is automatically logged out when the time specified in this item elapses since the last access to the Web GUI.
  - Input a time from 1 minute to 49 days 17 hours 2 minutes 23 seconds.
- Use HTTP proxy
  - Select below whether an HTTP proxy server will be used or not.
    - Use
    - Don't use
  - When "**Use**" is selected, specify the timeout interval.
  - Input a timeout interval from 1 to 180.

### Access via Telnet page

In this page you can configure the settings for a Telnet server.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Access via Telnet

- Use Telnet server
  - Select below whether a Telnet server will be used or not.
    - Use
    - Don't use
  - When "**Use**" is selected, specify the port number.
  - Input a port number from 1 to 65535.
- Interfaces that can access the Telnet server
  - The setting method for this item is the same as for the "Interfaces that can access the HTTP server" item on the Web GUI access page.
- Clients that can access the Telnet server
  - The setting method for this item is the same as for the "Clients that can access the HTTP server" item on the Web GUI access page.

### Access via SSH page

In this page you can configure the settings for an SSH server.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

If a host key has not been generated for the SSH server, the host key will be automatically generated when you modify the settings for using the SSH server.

### Access via SSH

- Use SSH server
  - Select below whether an SSH server will be used or not.
    - Use
    - Don't use
  - When "**Use**" is selected, specify the port number.
  - Input a port number from 1 to 65535.
- Interfaces that can access the SSH server
  - The setting method for this item is the same as for the "Interfaces that can access the HTTP server" item on the Web GUI access page.
- Clients that can access the SSH server
  - The setting method for this item is the same as for the "Clients that can access the HTTP server" item on the Web GUI access page.
- Client existence check from SSH server
  - Select below whether the SSH server checks for existing clients.
    - Check
    - Do not check
  - When "**Check**" is selected, specify the check interval and the number of times checked before disconnecting.
  - Input a check interval from 1 to 2147483647.
  - Input the number of times checked from 1 to 2147483647.

### Access via TFTP page

In this page you can configure the settings for a TFTP server.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Access via TFTP

- Use TFTP server
  - Select below whether a TFTP server will be used or not.
    - Use
    - Don't use
  - When "**Use**" is selected, specify the port number.
  - Input a port number from 1 to 65535.
- Interfaces that can access the TFTP server
  - The setting method for this item is the same as for the "Interfaces that can access the HTTP server" item on the Web GUI access page.

### Access via SNMP page

In this page you can configure the settings for a SNMP server.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

---

## Access via SNMP

- Clients that can access the SNMP server
  - Configure clients that can access the SNMP server.
  - Only predefined communities can be selected for the client community.
  - Specify the client IP address by IPv4 or IPv6 address.
  - Press the  icon to add a client.
  - Press the "Delete" button to delete the client.
  - You can configure up to 32 clients.

# External devices

## microSD

### Summary

On this page you can perform operations with the microSD card.

The microSD card will automatically be mounted when it is inserted into this unit.

When removing the microSD card from this unit while the unit is powered on, be sure to unmount the microSD card first.

If the stack function is enabled, you can perform operations with the microSD card that is inserted to the main switch.

### Top page

This is the microSD top page.

Displays the mounting status of the microSD card. You can also begin the steps here for switching the mounting status of the microSD card.

### Mounting switch for microSD card

- Displays the mounting status of the microSD card.
- Press the "Next" button to begin the steps for switching the mounting status of the microSD card.

### microSD card mounting switch page

This page is for switching the microSD card mounting status.

Press the "OK" button to switch the mounting status of the microSD card.

If the microSD card is already mounted, it will be unmounted; and if the microSD card is already unmounted, it will be mounted.

---

## Schedule execution

### Summary

In this page you can make settings for schedule execution.

The schedule execution function of this product has two setting items, schedule template and schedule.

Schedule template settings allow you to create a template of detailed settings for processes involved in executing scheduled functions and operations, such as the specific functions to be executed, the applicable item involved, and the execution sequence.

In schedule settings, you can select when to execute schedules and which templates to execute.

### Top page

This is the top page for making settings for schedule execution.

### List of schedule template

- Information for the currently registered schedule template are shown.
- The table items are explained below.
  - Template ID
    - Registered schedule template ID are shown.
  - Status
    - The status of the schedule template are shown.
  - Template description
    - Description of the schedule template are shown.
- If you press the "New" button, a page appears in which you can create a new schedule template.
- If you press the "Setting" button, a page appears in which you can edit the settings of the selected schedule template.
- If you press the "Delete" button, all schedule templates whose check box has a check mark will be deleted.
- Up to 10 schedule templates can be registered.

### List of schedule

- Information for the currently registered schedule are shown.
- The table items are explained below.
  - Schedule ID
    - Registered schedule ID are shown.
  - Execution timing
    - The execution timing of the schedule are shown.
  - Template to be executed
    - The information about the template to be executed when the schedule executed are shown.
- If you press the "New" button, a page appears in which you can create a new schedule.
- If you press the "Setting" button, a page appears in which you can edit the settings of the selected schedule.
- If you press the "Delete" button, all schedules whose check box has a check mark will be deleted.
- Up to 10 schedules can be registered.

---

## Schedule template settings page

In this page you can create a new schedule template or edit the settings of an already-registered schedule template.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Schedule template settings

- Template ID
  - The ID of the schedule template being set is displayed.
  - Newly created templates are automatically assigned the lowest unregistered serial number as the template ID.
- Template description
  - Sets the schedule template description text.
  - Enter up to 64 single-byte alphanumeric characters/symbols, excluding the ? symbol.
- Status
  - Select template status from the following items.
    - Enabled
      - Enables the template
    - Disabled
      - Disables the template
      - The contents of the template are not executed at the time of schedule execution.
- Import source of the schedule execution contents
  - Select the import source of the schedule execution contents from the following items.
    - CONFIG of the device
      - Executes the schedule execution contents saved in CONFIG of the device at the time of schedule execution.
      - The schedule execution contents entered on this page are saved in CONFIG of the device.
    - Script file in SD card
      - Loads the schedule execution contents from the script file in SD card at the time of schedule execution.
      - Please refer to [How to use the script file](#) for specific usage.
- Contents of schedule execution
  - Enter the commands to be executed by the scheduled execution.
  - You can enter multiple commands together by separating them with line-returns.
  - Specify settings that result in 20 or fewer command lines.
  - Schedule execution always starts with the specially-privileged EXEC mode (enable).
  - For prohibited commands and command details, refer to the command reference and the information provided on the [Network device product information page](#) and [Yamaha Network Devices Technical Documentation](#) .
  - If you press the "Easy input" button, you can quickly enter the corresponding commands for the following functions.
    - Shutdown

- Cancel shutdown
- Disable PoE power supply
- Enable PoE power supply
- Save TECHINFO into SD card
- Save settings
- About the linkage function with Yamaha wireless AP
  - When disabling the PoE power supply to a Yamaha wireless AP connected to this unit, you can configure the unit to stop the power supply after the Yamaha wireless AP's shutdown process.
  - To use this linkage function, select the check box of "Stop power supply after notifying the Yamaha wireless AP" when specifying "Disable PoE power supply" in "Easy input".
  - This linkage function works as below.
    - The unit notifies the remaining time to stop the power supply at the schedule executed. The time is notified via LLDP to the powered Yamaha wireless AP by the target port.
    - Once the notification is received, the Yamaha wireless AP executes the shutdown process. The power supply stops 10 minutes later than the schedule execution.
  - This linkage function works when the auto-configure via LLDP function is enabled.
  - The auto-configure via LLDP function is configured in **Detailed Settings > LLDP**.

### Schedule settings page

In this page you can create a new schedule or edit the settings of an already-registered schedule.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Schedule settings

- Schedule ID
  - The ID of the schedule being set is displayed.
  - Newly created templates are automatically assigned the lowest unregistered serial number as the schedule ID.
- Trigger type
  - Select the trigger to execute the schedule execution from the following items.
    - Time
      - When the time specified in the execution timing arrives, the device executes the schedule execution.
    - Event
      - When the event specified in the execution timing occurs, the device executes the schedule execution.
- Execution timing
  - If you select **Time** for **Trigger type**, select the timing to execute the schedule execution.
    - Easy input
      - Select a typical frequency pattern for the schedule execution timing.
    - Period

- Select the periodic pattern of schedule execution from the following items.
      - Every day
      - Every week
      - Every month
      - Every year
    - If "Every week" is selected, mark the checkbox for the day of the week when the schedule is to be executed.
    - If "Every month" is selected, enter the day when the schedule is to be executed in the "Day" box.
    - If "Every year" is selected, enter the month and the day when the schedule is to be executed in the "Month" box and the "Day" box.
    - Enter numeric values in the "Month" and "Day" boxes.
    - Multiple months/days can be specified as comma-delimited values. (Example: Enter "10,20" to specify 10 and 20.)
    - A hyphen can be used to indicate a range of values. (Example: Enter "1-3" to specify 1, 2, and 3.)
    - When you focus on the "Month" and "Day" boxes, the input form that can be operated with a mouse click is displayed.
  - Time
    - In the "Hours:Minutes:Seconds" box, enter the time in **hh:mm:ss** format.
    - When you focus on the "Hours:Minutes:Seconds" box, an input form that can be operated with a mouse click is displayed.
  - Input in command format
    - Enter the "Date" and "Time" in the command format.
    - This allows specifying settings in more detail than the Easy input mode.
    - Enter the "Date" in **MONTH/DATE** format.
    - Enter the "Time" in **hh:mm:ss** format.
    - For details on command format, refer to the command reference and to the information provided on the [Network device product information page](#) and [Yamaha Network Devices Technical Documentation](#) .
- If you select **Event** for **Trigger type**, select the event that triggers to execute the schedule execution.
  - When you start up the device
    - When you start up the device, the device executes the schedule execution.
  - When you attached an SD card
    - When you attached an SD card, the device executes the schedule execution.
- Template to be executed
  - Select the template to be executed in the schedule execution.

### How to use the script file

If you select the script file in SD card as the importsource of the schedule execution contents in the schedule templatesettings, the contents of the script file are executed at the time of schedule execution.

To use the script file, you need to insert an SD card with the script file saved in the specified path `"/(modelname)/schedule/script.txt"` into the device beforehand.

---

You can enter up to 100 lines of commands into the scriptfile. Commands after the 101 line are not executed at the time of schedule execution.

# SNMP

## MIB

### Summary

This page is for configuring MIB settings.

### Top page

This is the top page for MIB.

### Management information settings

- The contents of the Management information settings are shown.
- Press the "Setting" button to access a page where you can change the settings.

### Management information setting page

This page is for configuring Management information settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Management information settings

- Administrator information (sysContact)
  - Sets the string of Administrator information (sysContact).
  - The character string entered here is stored in the MIB variable sysContact.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 255 characters can be inputted.
- Installation site information (sysLocation)
  - Sets the string of Physical location information (sysLocation).
  - The character string entered here is stored in the MIB variable sysLocation.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 255 characters can be inputted.

---

## Community

### Summary

This page is for configuring SNMP community settings.

### Top page

This is the top page for Community.

### List of communities

- Information for the currently registered community are shown.
- The table items are explained below.
  - Community name
    - Registered communities name are shown.
  - Access mode
    - Access mode set to community are shown.
- If you press the "New" button, a page appears in which you can create a new community.
- If you press the "Setting" button, a page appears in which you can edit the settings of the selected community.
- If you press the "Delete" button, all communities whose check box has a check mark will be deleted.
  - If you check the "Delete from related settings as well" check box in the delete dialog, the following settings are changed with the deletion of the community.
    - Deletes the trap destination settings specifying the community to be deleted.
    - Deletes the clients that can access the SNMP server settings specifying the community to be deleted.
- Up to 16 communities can be registered.

### Community setting page

This page is for configuring SNMP community settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Community settings

- Community name
  - Sets the community name.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 32 characters can be inputted.
- Change the settings related to the community accordingly.
  - The following setting is changed accordingly to the change of community settings.
    - Change the community name used in the trap destination settings to the changed name.
    - Change the community name used in the clients that can access the SNMP server settings to the changed name.
  - This item will be displayed only when changing settings.
  - If you check the check box, the "Detail display" button will be displayed on the confirmation page.

- Press the "Detail display" button to open the dialog with the following information.
  - Trap destination settings which the community name to be changed.
- Access mode
  - Select the access mode of the community from the list below.
    - ReadOnly
      - Only read to MIB is allowed.
    - ReadWrite
      - Both read and write to MIB are allowed.

---

## SNMPv3 User

### Summary

This page is for configuring the settings related to SNMPv3 User.

### Top page

This is the top page for SNMPv3 User.

### MIB view list

- Displays the list of registered MIB views.
- The table items are explained below.
  - View name
    - Displays the registered MIB view name.
- Press the "New" button to display the page for registering a new MIB view.
- Press the "Setting" button to display the page for changing the selected MIB view settings.
- Press the "Delete" button to delete the MIB views with the check box selected.
  - If you check the "Delete from relatedsettings as well" check box in the delete dialog, the following settings are changed with the deletion of the MIB view.
    - Deletes the MIB view settings from the group settings as well. If there are no more readable and writable MIBviews, deletes the group settings as well.
    - Deletes the user settings belonging to the group to be deleted.
    - Deletes the trap destination settings specifying the user to be deleted.
- You can register up to 16 MIB views.

### Group list

- Displays the list of registered groups.
- The table items are explained below.
  - Group name
    - Displays the registered group name.
  - Readable MIB view
    - Displays the MIB view that is readable by users who belong to this group.
  - Writable MIB view
    - Displays the MIB view that is writable by users who belong to this group.
  - Security level
    - Displays the security level required for users who belong to this group.
- Press the "New" button to display the page for registering a new group.
- Press the "Setting" button to display the page for changing the selected group settings.
- Press the "Delete" button to delete the groups with the check box selected.
  - If you check the "Delete from relatedsettings as well" check box in the delete dialog, the following settings are changed with the deletion of the group.
    - Deletes the user settings belonging to the group to be deleted.
    - Deletes the trap destination settings specifying the user to be deleted.
- You can register up to 16 groups.

## User list

- Displays the list of registered users.
- The table items are explained below.
  - User name
    - Displays the registered user name.
  - Group
    - Displays the name of the group to which this user belongs.
  - Authentication algorithm
    - Displays the authentication algorithm that this user uses for communication.
  - Encryption algorithm
    - Displays the encryption algorithm that this user uses for communication.
- Press the "New" button to display the page for registering a new user.
- Press the "Setting" button to display the page for changing the selected user settings.
- Press the "Delete" button to delete the users with the check box selected.
  - If you check the "Delete from related settings as well" check box in the delete dialog, the following settings are changed with the deletion of the user.
    - Deletes the trap destination settings specifying the user to be deleted.
- You can register up to 16 users.

## MIB view settings page

This page is for configuring settings related to MIB view of SNMP.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## MIB view settings

- View name
  - Set the MIB view name.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 32 characters can be inputted.
- Change the settings related to the view accordingly.
  - The following setting is changed accordingly to the change of MIB view settings.
    - Change the MIB view name used in the group settings to the changed MIB view name.
  - This item will be displayed only when changing settings.
  - If you check the check box, the "Detail display" button will be displayed on the confirmation page.
  - Press the "Detail display" button to open the dialog with the following information.
    - Group settings where MIB view name to be changed.
- Entry
  - Set the MIB objects to be allowed access.
  - MIB object ID
    - Specify the MIB object ID.
    - Single-byte numeric characters and dot (.) can be inputted.

- Up to 64 characters can be inputted.
- Type
  - Select "Include in management(include)" to allow access to the specified MIB object ID or "Excludefrom management (exclude)" to not allow access.
- Press the  icon to add an entry.
- Press the "Delete" button to delete the entry.
- You can specify up to 8 entries.
- You need to specify at least one entry.

## Group settings page

This page is for configuring the settings related to groups of SNMP.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## Group settings

- Group name
  - Set the group name.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 32 characters can be inputted.
- Change the settings related to the group accordingly.
  - The following settings are changed accordingly to the change of group settings.
    - Change the group name used in the user settings to the changed group name.
  - This item will be displayed only when changing settings.
  - If you check the check box, the "Detail display" button will be displayed on the confirmation page.
  - Press the "Detail display" button to open the dialog with the following information.
    - Group settings for which the group name is changed
- Readable MIB view
  - Select a MIB view that is readable by users who belong to this group.
  - Press the "Select" button and select a MIB view from the "Select MIB view" dialog.
- Writable MIB view
  - Select a MIB view that is writable by users who belong to this group.
  - Press the "Select" button and select a MIB view from the "Select MIB view" dialog.
- Security level
  - Configure the security level required for users who belong to this group.
  - You cannot use encryption alone without authentication.
  - User authentication for MIB access fails if the user settings do not meet the security level of the group.

## User settings page

This page is for configuring the settings related to users of SNMP.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## User settings

- User name
  - Set the user name.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 32 characters can be inputted.
- Change the settings related to the user accordingly.
  - The following setting is changed accordingly to the change of user settings.
    - Change the user name used in the trap destination settings to the changed user name.
    - Change the security level used in the trap destination settings according to this user setting.
  - This item will be displayed only when changing settings.
  - If you check the check box, the "Detail display" button will be displayed on the confirmation page.
  - Press the "Detail display" button to open the dialog with the following information.
    - Trap destination settings where user name to be changed
    - Trap destination settings where the security level to be changed
- Group
  - Select a group to which this user belongs.
  - Press the "Select" button and select a group from the "Select group" dialog.
- Authentication algorithm
  - Select an authentication algorithm that this user uses for communication.
- Authentication password
  - Enter from 8 to 32 single-byte alphanumeric characters/symbols, excluding the ? symbol.
  - If the setting of the authentication algorithm is "None", this setting is not available.
- Encryption algorithm
  - Select a encryption algorithm that this user uses for communication.
  - If the setting of the authentication algorithm is "None", this setting is not available.
- Encryption password
  - Enter from 8 to 32 single-byte alphanumeric characters/symbols, excluding the ? symbol.
  - If the setting of the authentication or encryption algorithm is "None", this setting is not available.

---

## SNMP trap

### Summary

This page is for configuring SNMP trap settings.

### Top page

This is the top page for SNMP trap.

### Trap type settings

- The contents of the settings of trap type are shown.
- Press the "Setting" button to access a page where you can change the settings.

### List of traps destinations

- Information for the currently registered traps destinations are shown.
- The table items are explained below.
  - Destination address
    - Registered traps destination address are shown.
  - Version
    - SNMP version that used in trap are shown.
  - Community / User
    - SNMP community name or user name that used in trap are shown.
  - Message type
    - SNMP message type that used in trap are shown.
  - Security level
    - Displays the security level required in the user settings for the device to send traps.
- If you press the "New" button, a page appears in which you can create a new traps destination.
- If you press the "Setting" button, a page appears in which you can edit the settings of the selected traps destination.
- If you press the "Delete" button, all traps destinations whose check box has a check mark will be deleted.
- Up to 8 traps destinations can be registered.

### Trap type setting page

This page is for configuring Trap type settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Trap type settings

- Trap type
  - Select the trap type to send by SNMP agent from the list below.
    - Boot from power OFF state
      - Send traps when the power is turned on/off or when firmware is updated.
    - Restart without power OFF
      - Send traps when restart by reload command.

- Link down of port
  - Send traps when link down of port.
- Link up of port
  - Send traps when link up of port.
- Fail authentication
  - Send traps when SNMP message to non-registered community or user is received.
- Change Temperature status
  - Send traps when Temperature state is changed for example when temperature abnormally detected.
- Change FAN status
  - Send traps when FAN state is changed for example when FAN abnormally detected.
- Detect / lose L2MS agent
  - Send traps when an L2MS agent is detected or lost.
- Detect / cancel ErrDisable
  - Send traps when the ErrDisable is detected or canceled.
- RMON event
  - Send traps when the RMON event is executed.
- Change device monitoring status
  - Send traps when the device monitoring function detects a change in the device status.
- Detect root of spanning tree / change of topology
  - Send traps when a new root bridge is detected or when a topology change is detected.
- Change PoE status
  - Send traps when PoE state is changed.
- Detect / resolve the loop
  - Send traps when a loop is detected or resolved.

### Trap destination setting page

In this page you can create a new trap destination or edit the settings of an already-registered trap destination.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Trap destination settings

- Destination address
  - Sets the destination address of traps.
  - For the destination address, either an IPv4 address or an IPv6 address can be specified.
  - For IPv6 link local addresses, you must also specify the interface to send from. (Format: fe80::X%vlanN)
- Version
  - Select the SNMP version used by traps.
    - SNMPv1
      - Send traps using SNMP version 1.

- 
- SNMPv2c
    - Send traps using SNMP version 2c.
  - SNMPv3
    - Send traps using SNMP version 3.
  - Community / User
    - Select the community or users used by traps.
    - Click the "Select" button to display the "Community selection" dialog or "User selection" dialog.
    - List of already-defined community or user is displayed at "Community selection" dialog or "User selection" dialog.
    - In the "Community selection" dialog or "User selection" dialog, pressing the "Select" button enables selection of communities or users used by traps at the destination where the traps are sent.
  - Message type
    - Select the SNMP message type used by trap.
      - Use Trap
        - Message type that does not require response confirmation to the destination.
      - Use Inform Request
        - Message type that require response confirmation to the destination.
    - If SNMPv1 is selected as the version, then the message type cannot be selected.
    - The Trap message type is always used for version SNMPv1.
  - Security level
    - Set the security level required in the user settings for the device to send traps.
    - You cannot use encryption alone without authentication.
    - Sending traps fails if the user settings do not meet the security level of the trap destination settings.

# RMON

## RMON settings

### Summary

This page is for configuring RMON settings.

You can enable or disable the RMON function for the entire system, and specify Ethernet statistics group and history group for physical interface.

You cannot configure RMON function when the stack function is enabled.

### Top page

This is the top page for the RMON settings.

### System settings

- Displays the RMON function settings for the entire system.
- Press the "Setting" button to display a page for configuring the system settings.

### Interface settings

- Displays the configuration of each port's Ethernet statistics and history groups.
- The table items are explained below.
  - Port
    - Displays the port name.
  - Ethernet statistics group
    - Settings
      - Displays whether the Ethernet statistics group for the port is enabled.
    - Index
      - Displays the index of Ethernet statistics group specified for the port.
  - History group
    - Settings
      - Displays whether the history group for the port is enabled.
    - Index
      - Displays the index of history group specified for the port.
- Press the "Setting" button to display a page for configuring the selected interface settings.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected.

### System settings page

This page is for configuring the RMON function settings for the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## System settings

- RMON function
  - Specify whether to enable or disable the RMON function for the entire system.
  - If this setting is disabled, the following processes are executed.
    - Collecting statistics for the Ethernet statistics group is stopped.
    - Collecting history for the history group is stopped.
    - Sampling the alarm group is stopped.
  - If this setting is enabled, the following processes are executed.
    - Deletes the previously collected Ethernet statistics and restarts the collection.
    - Deletes the previously collected history and restarts the collection.
    - Deletes the previously collected sampling data and restarts sampling.

## Interface settings page

This page is for configuring RMON settings for the interface.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## Interface settings

- Port
  - Displays the port name to configure the settings.
- Ethernet statistics group
  - Specify the Ethernet statistics group.
  - Index
    - Set the index of the Ethernet statistics group.
    - The input range is 1 - 65535.
    - An index that is already in use cannot be specified.
  - Owner name
    - Set the owner name of the Ethernet statistics group.
    - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
    - Up to 127 characters can be inputted.
  - Press the  icon to add an Ethernet statistics group.
  - Press the "Delete" button to delete the Ethernet statistics group.
  - You can specify up to 8 Ethernet statistics groups.
  - If you check the "Delete previously collected statistics" check box, previously collected Ethernet statistics will be deleted for already registered indexes whose settings have not been changed.
- History group
  - Specify the history group.
  - Index
    - Set the index of the history group.

- The input range is 1 - 65535.
- An index that is already in use cannot be specified.
- Number of saved history
  - Set the number of saved history of the history group.
  - The input range is 1 - 65535.
- Save interval
  - Set the history saving interval of the history group.
  - The input range is 1 - 3600.
- Owner name
  - Set the owner name of the history group.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 127 characters can be inputted.
- Press the  icon to add a history group.
- Press the "Delete" button to delete the history group.
- You can specify up to 8 history groups.
- If you check the "Delete previously collected history" check box, previously collected history will be deleted for already registered indexes whose settings have not been changed.

---

## Event group

### Summary

This page is for configuring RMON event group settings.

You cannot configure RMON function when the stack function is enabled.

### Top page

This is the top page for the RMON event group.

### Event group settings

- Displays a list of event group settings.
- The table items are explained below.
  - Index
    - Displays the index of event group.
  - Event execution content
    - Displays the execution content of event group.
  - Trap destination
    - Displays SNMP community or user specified as trap destination if the event execution content includes "Send trap".
- Press the "New" button to display a page where you can create new settings for the event group.
- Press the "Setting" button to display a page where you can change the settings of the selected event group.
- If you press the "Delete" button, all event groups whose check boxes are selected will be deleted.
- Up to 128 event group settings can be displayed.

### Event group settings page

This page is for configuring RMON event group settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Event group settings

- Index
  - To create a new event group, set the index of the event group.
    - The smallest index of unregistered event groups is entered as the initial value.
    - The input range is 1 - 65535.
    - An index that is already in use cannot be specified.
  - This cannot be changed when changing the settings.
- Event execution content
  - Select an execution content when this event is called.
  - You need to specify the trap destination of event group if the event execution content includes "Send trap".
- Trap destination for event group

- Specify the community or user for trap destination of event group.
- Only the community or user specified in the SNMP trap destination settings can be selected.
- Description
  - Enter a description for the event group.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 127 characters can be inputted.
- Owner name
  - Set the owner name of the event group.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 127 characters can be inputted.

---

## Alarm group

### Summary

This page is for configuring RMON alarm group settings.

You cannot configure RMON function when the stack function is enabled.

### Top page

This is the top page for the RMON alarm group.

### Alarm group settings

- Displays a list of alarm group settings.
- The table items are explained below.
  - Index
    - Displays the index of alarm group.
  - Monitoring MIB
    - Displays the MIB specified to be monitored in the alarm group.
  - Monitoring port
    - Displays the port information of the monitoring MIB.
- Press the "New" button to display a page where you can create new settings for the alarm group.
- Press the "Setting" button to display a page where you can change the settings of the selected alarm group.
- If you press the "Delete" button, all alarm groups whose check boxes are selected will be deleted.
- Up to 1024 alarm group settings can be displayed.

### Alarm group settings page

This page is for configuring RMON alarm group settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Alarm group settings

- Index
  - To create a new alarm group, set the index of the alarm group.
    - The smallest index of unregistered alarm groups is entered as the initial value.
    - The input range is 1 - 65535.
    - An index that is already in use cannot be specified.
  - This cannot be changed when changing the settings.
- Monitoring MIB object
  - Select MIB object to be monitored.
  - You can select a MIB from those belonging to the index of Ethernet statistics group you have enabled.
- Sampling interval
  - Specify the sampling interval in seconds for the monitoring MIB values.

- Comparison method between sample value and the threshold
  - Select a comparison method between the value obtained by sampling and the threshold.
- Upper threshold
  - Specify the upper threshold and event to be executed when the value exceeds the upper threshold.
  - The input range is 1 - 2147483647.
  - You can select an event to execute from registered event groups.
- Lower threshold
  - Specify the lower threshold and event to be executed when the value falls below the lower threshold.
  - The input range is 1 - 2147483647.
  - You can select an event to execute from registered event groups.
- Initial event execution timing
  - You can select the upper or lower threshold for initial alarm determination when both the upper and lower thresholds are enabled.
- Owner name
  - Set the owner name of the alarm group.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 127 characters can be inputted.

---

## sFlow

### Summary

This page is for configuring sFlow settings.

This unit operates as a sFlow agent.

You need to prepare a sFlow collector separately.

### Top page

This is the top page for the sFlow.

### System settings

- Displays the sFlow settings for the entire system.
- The table items are explained below.
  - sFlow function
    - Displays whether to enable or disable the sFlow function for the entire system.
  - IP address of agent
    - Displays the IP address of sFlow agent.
  - IP address of collector
    - Displays the IP address of sFlow collector.
  - Port of collector
    - Displays the UDP port number of sFlow collector.
  - Maximum datagram size
    - Displays the maximum datagram size sent from sFlow agent to sFlow collector.
- Press the "Setting" button to display the page for configuring the system.

### Interface settings

- Displays the sFlow settings for the interface.
- The table items are explained below.
  - Port
    - Displays the interface name.
  - Packet flow sampling
    - Displays sampling rate for packet flow sampling at the target interface.
  - Counter sampling
    - Displays polling interval for counter sampling at the target interface.
- Press the "Setting" button to display the page for configuring the selected interface.
- Press the "Specify all" button to configure the settings for all interfaces with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected.

### System settings page

This page is for configuring the sFlow settings for the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## System settings

- sFlow function
  - Specify whether to enable or disable the sFlow function for the entire system.
- IP address of agent
  - Set the IP address of sFlow agent.
  - It is used for sFlow header of sFlow datagram.
  - IPv6 address cannot be specified when the stack function is enabled.
- IP address of collector
  - Set the IP address of sFlow collector.
  - IPv6 address cannot be specified when the stack function is enabled.
  - The following IPv4 addresses cannot be specified.
    - All 0 (0.0.0.0)
    - Loopback (127.0.0.1)
    - Multicast (224.0.0.0 - 239.255.255.255)
    - class E (240.0.0.0 - 255.255.255.255)
  - The following IPv6 addresses cannot be specified.
    - All 0 (:::0)
    - Loopback (:::1)
    - Multicast (FF00::)
- Port of collector
  - Set the UDP port number of sFlow collector.
- Maximum datagram size
  - Set the maximum datagram size sent from sFlow agent to sFlow collector.

## Interface settings page

This page is for configuring the sFlow settings for the interface.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

## Interface settings

- Port
  - Displays the port name to configure the settings.
- Packet flow sampling
  - Select from the following packet flow sampling operations.
    - Disable
    - Enable
  - Sampling rate
    - Specify how many packets you want to take sample statistics for each by packet flow sampling.
    - Set the appropriate value, paying attention to the following.
      - If you set the value too small, CPU load will be high.
      - The more you increase ports with packet flow sampling enabled, the more CPU load

increases.

- High CPU load might affect precision of information because the unprocessed sampling contents will be discarded.
- Maximum header size
  - Specify the maximum header size of Ethernet frames to be sampled by packet flow sampling.
- Counter sampling
  - Select from the following counter sampling operations.
    - Disable
    - Enable
  - Polling interval
    - Specify how many seconds you want to take sample statistics for each by counter sampling.

## LLDP

### Summary

**This page is for changing LLDP settings and viewing neighbor information obtained by LLDP.**

\* LLDP (Link Layer Discovery Protocol) is a protocol to collect neighbor information. In this unit, following operations are supported.

- Unit information is periodically transmitted to neighboring devices.
- Reception of information from neighboring devices.
- Display of received neighbor information.

### Top page

This is the top page for the LLDP.

### Neighbor information list

- Pressing the "Next" button displays a page where acquired neighbor information can be viewed.
- The "Next" button is disabled if the LLDP function is disabled.

### System settings

- Displays the LLDP settings for the system.
- The table items are explained below.
  - LLDP
    - Displays whether LLDP is enabled or disabled for the entire system.
  - Auto-configure via LLDP function
    - The current settings for the auto-configure via LLDP function are displayed.
  - System name
    - Displays the system name to be notified by LLDP.
  - System description
    - Displays the system description to be notified by LLDP.
- Press the "Setting" button to display the page for configuring the system.

### Interface settings

- Displays the LLDP settings for the interface.
- The table items are explained below.
  - Port
    - Displays the interface name.
  - LLDP frame transmission and reception
    - Displays the LLDP frame transmission and reception mode for the target interface.
- Press the "Setting" button to display the page for configuring the selected interface.
- Press the "Specify all" button to configure the settings for all interfaces with the check box selected.
- Press the "Return to defaults" button to initialize the settings for all interfaces with the check box selected.

## Neighbor information list page

This page displays a summary of neighbor information obtained by LLDP.  
Displays ports where neighbor information was received and part of that information.

### Neighbor information list

- Displays a list of neighbor information obtained by LLDP.
- Up to 1000 neighbor information is displayed.
- Pressing the "Detail" button displays a page for viewing details about the selected neighbor information.
- You can search neighbor information from the "Search" box.
  - Press  to execute the search.
  - Press  to clear the search.
  - You can use regular expressions shown below in search keywords.
  - Lowercase and capital letters are treated the same for keywords.

Syntax	Explanation
A	The character "A"
ABC	The characters "ABC"
[ABC]	One character, either "A", "B" or "C"
[A-C]	One character between "A" and "C"
[^ABC]	An arbitrary character that is neither "A", "B" or "C"
.	An arbitrary character
A+	At least one "A" character
A*	At least zero "A" characters
A?	Zero or one "A" character
^A	A string that begins with "A"
A\$	A string that ends with "A"
ABC DEF GHI	"ABC", "DEF" or "GHI"
A{2}	Two "A" characters (AA)
A{2,}	Two or more "A" characters (AA, AAA, AAAA...)
A{2,3}	Two to three "A" characters (AA, AAA)
\b	Word breaks, such as spaces
\B	Any character besides \b
\d	An arbitrary number (same as [0-9])
\D	Any character besides numbers (same as [^0-9])
\s	Single breaking character
\S	Any single character besides \s

Syntax	Explanation
\w	Alphanumeric characters including underlines (same as [A-Za-z0-9_])
\W	Any character besides \w

- Press  to update information to the latest information.
- The number of search results to display at one time can be selected by pressing "Display number" on the "Select" menu.
- If the number of neighbor information results exceeds the "display number" setting, the range of neighbor information results can be changed by pressing  .
- Press the sort switch to sort by each item.
  - With default settings, results are sorted in ascending order of the receiving port.
  - Press the sort switch again to toggle between ascending and descending order.
  - "Receiving ports" are sorted in order of port number.
  - Other items are sorted alphabetically based on the character string.

### Neighbor information detail page

This page displays details for neighbor information selected on the neighbor information page.

### Details of neighbor information

- Each information item in the obtained neighbor information is displayed.
- If obtained neighbor information contains no information for an item, "-" is displayed.
- For details on the information displayed, refer to [Yamaha Network Devices Technical Documentation](#).

### System settings page

This page is for configuring the LLDP settings for the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- LLDP
  - Specify whether to enable or disable LLDP for the entire system.
- Auto-configure via LLDP function
  - Specify whether to enable or disable Auto-configure via LLDP function.
- System name
  - Specify the system name to be notified by LLDP.
  - Enter up to 255 single-byte alphanumeric characters/symbols, excluding the ? symbol.
- System description
  - Specify the system description to be notified by LLDP.
  - Enter up to 255 single-byte alphanumeric characters/symbols, excluding the ? symbol.

---

## Interface settings page

This page is for configuring the LLDP settings for the system.

You can also change the detailed settings by pressing the "Advanced settings" button.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Interface settings

- Port
  - Specify whether to enable or disable LLDP for the entire system.
- LLDP frame transmission and reception
  - Select the operation for LLDP frame transmission and reception from the following options.
    - Enabled
      - Enables LLDP frame transmission and reception.
      - Select direction to enable from the following items.
        - Transmit & Receive
        - Transmit
        - Receive
    - Disabled
      - Disables LLDP frame transmission and reception.
- Option TLV to send
  - Select the information to be sent by LLDP from the following items.
    - Basic management TLV
      - Sends administrative information about the system, such as the system name and the functions it supports.
    - IEEE 802.1 TLV
      - Sends information about the VLAN and link aggregation of the port.
    - IEEE 802.3 TLV
      - Sends information about the auto negotiation and PoE of the port.
    - LLDP-MED TLV
      - Sends information about network policy and extended PoE of the port.
- LLDP frame transmission interval
  - Specifies the transmission interval of LLDP frames in terms of seconds.
  - Input a transmission interval of LLDP frames from 5 to 3600.
- Hold time (TTL) of device information sent by LLDP
  - Specify a hold multiplier to decide a hold time ( TTL ).
  - Input a hold multiplier from 1 to 100.
  - The upper limit of Hold time (TTL) is 65535.
- Fast transmission period setting
  - Specify a transmission interval and a send number of LLDP frames during the fast transmission period.
  - Input a transmission interval from 1 to 3600.
  - Input a send number from 1 to 8.

- Time from stop sending LLDP frames to reinitialization
  - Specify the waiting time from when LLDP is disabled to when LLDP can be re-enabled on the port.
  - Input a time from stop sending LLDP frames to reinitialization from 1 to 8.
- Type of Management address sent by LLDP
  - Select management address type from the following items.
    - IP address
    - MAC address
- Maximum number of managed devices
  - Specifies the maximum number of managed devices.
  - Input a maximum number of managed devices from 1 to 1000.

---

## Mail notification

### Summary

In this page you can make settings related to mail notification. When a mail notification is received, mail is automatically sent to the assigned recipient when the specified conditions are met.

First use the "New" button in "Registered mail server list" to register the mail server of the recipient. After registering this, use the "New" button in "Mail notification settings list" to make mail notification settings.

### Top page

This is the top page for mail notifications.

### List of registered mail servers

- Information for the currently registered mail server (SMTP server) is shown.
- You can use the "New" button at the top of the list to add settings.
- If you want to change the settings, press the "Settings" button located at the right of the table. A page for changing the settings appears, allowing you to change the settings.
- If you want to delete settings, select the setting that you want to delete, and press the "Delete" button located above the list. A confirmation dialog box appears; press the "Delete" button to delete the setting.
- Up to 10 mail servers can be registered.

### List of mail notification settings

- The currently specified mail notification settings are shown.
- You can use the "New" button at the top of the list to add settings.
- If you want to change the settings, press the "Settings" button located at the right of the table. A page for changing the settings appears, allowing you to change the settings.
- If you want to delete settings, select the setting that you want to delete, and press the "Delete" button located above the list. A confirmation dialog box appears; press the "Delete" button to delete the setting.
- If you want to do mail sending test, press the "Next" button located at "Sending test" item. A confirmation dialog box appears; press the "OK" button to do mail sending test.

### Mail server settings page

This page lets you make settings for the recipient's mail server (SMTP server). Check the items that you specified, and then press the "Confirm" button. If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### List of registered mail servers

- ID
  - This is the identifying number of the mail server settings. It is assigned automatically.
- Account identification name
  - Specify the mail server's account identification name. For convenience, specify a name that will be easy to recognize.
  - You can use up to 64 single-byte characters.
  - This can be omitted.
- SMTP server address
  - Enter the IP address or domain name of the SMTP server used when sending mail.

- You can use up to 64 single-byte characters.
- SMTP server port number
  - Enter the SMTP server's port number.
  - If "Submission port (port number 587)" is checked, the submission port, which is port number 587, is specified.
- Encrypting SMTP
  - This setting determines whether to encrypt SMTP with SSL when sending mail.
  - Selecting "Not encrypt" is to use SMTP for sending mail.
  - Selecting "Encrypt with SSL (over SSL)" is to use SMTPS (SMTP over SSL) for sending mail, so that SMTP is encrypted with SSL.
    - It is recommended to set 465 for "SMTP server port number".
  - Selecting "Encrypt with SSL (STARTTLS)" is to use SMTPS (STARTTLS) for sending mail, so that SMTP is encrypted with SSL.
  - For STARTTLS, communication is encrypted only if the SMTP server supports encryption using SSL.
  - Encryption using SSL is not available when setting an IPv6 address as the SMTP server address.
- SMTP authentication
  - Select from the drop-down list box whether to authenticate with the SMTP server.
  - To authenticate, enter the following settings.
    - User name
      - This setting determines the user name used when authenticating to the SMTP server.
      - Up to 64 single-byte characters are allowed.
    - Password
      - This setting determines the password used when authenticating to the SMTP server.
      - Up to 64 single-byte characters are allowed.

### Mail notification settings page

In this page you can make mail notification settings. You can specify the transmission source and the recipient address of mail notifications. Check the items that you specified, and then press the "Confirm" button. If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Mail notification settings

- ID
  - This is the identifying number of the mail notification settings. It is assigned automatically.
- Source (From)
  - Specify the sender's mail address of the mail that will be sent.  
SMTP server:
    - Select the SMTP server used when sending the mail.  
Mail address:
    - Enter the sender's mail address of the mail that will be sent.
    - You can use up to 256 single-byte characters. However, you cannot use symbols other than underline (\_), hyphen (-), dot (.), and at-sign (@).
- Destination (To)

- 
- Enter the recipient's mail address of the mail that will be sent.
  - You can register up to four items; the mail is sent to all of the registered mail addresses.
  - You can use up to 256 single-byte characters. However, you cannot use symbols other than underline (\_), hyphen (-), dot (.), and at-sign (@).
  - This setting does not affect the mail send function of the RADIUS server.
  - Subject
    - Specify the subject of the mail that will be sent.
    - You can use up to 128 single-byte characters.
    - If you select "Use specified subject," the subject name will be the specified subject.
    - This setting does not affect the mail send function of the RADIUS server.
  - Notification content
    - The contents of the notification are specified as follows.
      - LAN map error detection
        - This notification will be made only if this unit is operating as an L2MS manager.
        - Select the LAN map events to be notified from the following.
          - Device abnormality
          - Loop detection
          - SFP optical Rx level abnormality
          - Transmission queue monitoring
          - PoE supply
          - Snapshot
          - Duplication of L2MS managers
      - Status notification for terminal monitoring
        - The change in status monitored by the device monitoring function will be notified.
      - Stack error detection
        - Failure information of the stack function will be notified.
    - This setting does not affect the mail send function of the RADIUS server.
  - Mail transmission wait time
    - Specify the time by which mail transmission is delayed after the notification event occurs.
    - If other notification events occur during this wait time, those notifications are combined and sent in a single email.
    - This setting does not affect the mail send function of the RADIUS server.
-

---

## Terminal monitoring

### Summary

On this page you can make settings for device monitoring.

The device communication status can be monitored by specifying the monitoring target and method.

You can also specify the action to be executed when the device status changes.

Device monitoring settings can be made only from the Web GUI.

Although the contents of the device monitoring settings are not shown in the CONFIG file, when an operation (such as "erase startup-config") is performed on the CONFIG file, the same operation is performed on the device monitoring settings.

If the auto-configure via LLDP function is enabled, the Yamaha wireless AP connected to this unit is automatically monitored by LLDP.

### Top page

This is the top page for device monitoring.

### List of monitored terminals

- The device monitoring status and settings are shown here.
- The table items are explained below.
  - Check box
    - Select the check box to delete device monitoring settings.
  - Status
    - One of the device monitoring statuses as follows are displayed.
      - IDLE
      - UP
      - DOWN
    - Refer to [Conditions for determining monitored device status](#) for the conditions used to determine the above statuses.
  - Include in monitoring
    - Displays information for the monitoring target(s).
    - If the monitoring type is "Ping", the IP address of the monitored device will be displayed.
    - For monitoring types other than "Ping", the interface number will be displayed.
  - Device name
    - Displays the name of the device being monitored.
  - Monitoring type
    - Displays one of the following monitoring types for the device being monitored.
      - Ping
      - Frame reception volume
      - LLDP
  - PoE supply
    - Displays one of the following PoE power supply statuses for the device being monitored.
      - Power is being supplied (Class 0)
      - Power is being supplied (Class 1)
      - Power is being supplied (Class 2)

- Power is being supplied (Class 3)
  - Power is being supplied (Class 4)
  - Stopped
  - -
- Press the "New" button to display a page where you can create new settings for monitored devices.
  - Press the "Setting" button to access a page where you can change the settings of the selected device.
  - Press the "Update" button to update the table.
  - If you press the "Delete" button, all monitored devices whose check boxes are selected will be deleted.
  - Up to 256 monitored devices can be configured.
    - Of these, up to 64 monitored devices with ping can be configured.

### Monitored device settings page

This page is for configuring the monitored device settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Setting monitored devices

- Device name
  - Specifies the device name.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding ?.
  - Up to 80 characters can be inputted.
- Monitoring type
  - Select from one of the following monitoring methods.
    - Ping-based communication monitoring
    - Frame reception volume monitoring
    - LLDP reception interval monitoring
  - This item cannot be changed when changing the settings.
- Destination IP address for ping
  - Specifies the IP address to which a ping message will be transmitted.
  - This item will only be displayed when **Ping-based communication monitoring** is selected for the "Monitoring type" item.
- Time waiting for reply
  - Specifies the time required to determine whether the ping response has failed.
  - The input range is 1 - 60.
  - This item will only be displayed when **Ping-based communication monitoring** is selected for the "Monitoring type" item.
- Number of failures before detecting unavailable device
  - Specifies the number of times that the ping response must fail before determining that the monitored device is unavailable.
  - The input range is 1 - 100.
  - This item will only be displayed when **Ping-based communication monitoring** is selected for the "Monitoring type" item.

- Port
  - Specifies the port for frame monitoring.
  - The input format is portX.YY.
  - This item will only be displayed when **Frame reception volume monitoring** or **LLDP reception interval monitoring** is selected for the "Monitoring type" item.
- Monitor start band
  - Specifies the bandwidth at which frame reception volume monitoring will start.
  - The input range is 1 - 1000000000.
  - This item will only be displayed when **Frame reception volume monitoring** is selected for the "Monitoring type" item.
- Unavailable device detection band
  - Specifies the band value for determining that the monitored device is unavailable.
  - The input range is 0 - 999999999.
  - The value specified for this item must be less than the value used for "Monitor start band".
  - This item will only be displayed when **Frame reception volume monitoring** is selected for the "Monitoring type" item.
- Operation when detecting change in status
  - Terminal reboot due to temporary stop of PoE power supply
    - The PoE power supply for the target port will be temporarily stopped only when the device is detected to be unavailable.
      - Target port
        - Specifies the port for which the PoE power supply will be stopped.
        - The input format is portX.YY.
        - This item will only be displayed when **Ping-based communication monitoring** is selected for the "Monitoring type" item.
      - Duration of power supply stop
        - Specifies the time for which the PoE power supply will be stopped.
        - The input range is 1 - 60.
  - SNMP trap transmission
    - When a change of status is detected, a trap is notified to the SNMP manager.
  - Mail notification
    - An e-mail is sent when a change of status is detected.
    - The e-mail server, destination and so on must be configured in order to send e-mail.
    - Further, you must select the **Status notification for device monitoring** in the "Mail notification settings" as the "notification content".
    - Configure the e-mail server and e-mail template on the **E-mail notifications** page.

#### Conditions for determining monitored device status

This explains the conditions for when the monitored device status changes.

- Monitoring with ping
  - If a ping packet transmitted by this unit does not return within the set **time waiting for reply**, this is counted as one failure. The status is determined by how many failures occur.
  - The conditions for change in status are shown below.

- 
- IDLE status
    - Initial status determination has not been completed after setting the monitored device.
  - UP status
    - Ping transmission has not failed continuously for the **Number of failures before detecting unavailable device** that was set.
  - DOWN status
    - Ping transmission fails continuously for the **Number of failures before detecting unavailable device** that was set.
- Monitoring according to frame reception volume
    - Measures the frame reception volume for the monitoring target and determines the status.
    - The conditions for change in status are shown below.
      - IDLE status
        - After the monitored device is configured, the frame reception volume for the monitored target port has not once exceeded the **monitor start band** that was set.
      - UP status
        - After the frame reception volume for the monitored target port exceeded the **monitor start band** that was set, it did not fall below the **unavailable device detection band**.
        - The frame reception volume for the monitored target port rose above the **unavailable device detection band** in DOWN status.
      - DOWN status
        - The frame reception volume for the monitored target port fell below the **unavailable device detection band** in UP status.
- Monitoring with LLDP
    - Status is determined by the LLDP frame reception status at the monitored target port.
    - The conditions for change in status are shown below.
      - IDLE status
        - After the monitored device is configured, no LLDP frames have been received at the monitored target port.
      - UP status
        - The next LLDP frame was able to be received at the monitored target port, within the TTL of the previously accepted LLDP frame.
        - An LLDP frame could be received in DOWN status at the monitored target port.
      - DOWN status
        - The next LLDP frame could not be received at the monitored target port, within the TTL of the previously accepted LLDP frame.

## Dante optimization

### Summary

This is the page for operations related to the Dante optimization settings.

The Dante optimization settings can be made manually or by means of auto-configure via LLDP.

### Top page

This is the top page for configuring the Dante optimization.

### Dante optimization

- The current settings for the auto-configure via LLDP function are displayed.
- Press "Next" button to begin the steps for Dante optimization settings.
- Press "Setting" button to display the page where the settings for the auto-configure via LLDP function can be modified.
- This function cannot be used when the stack function is enabled.

### Multicast basic settings (System)

- Displays the configuration for unknown multicast frames for the entire system.
- The table items are explained below.
  - Processing method for unknown multicast frames
    - Displays the processing method of unknown multicast frames.
  - Excluded frames from discarding (for all VLANs)
    - Displays excluded frames from discarding when configured to discard unknown multicast frames.

### Multicast basic settings (VLAN interface)

- Displays the configuration for unknown multicast frames for each VLAN.
- The table items are explained below.
  - VLAN ID
    - VLAN ID is displayed.
  - Unknown multicast frame
    - Displays the processing method for unknown multicast frames for the target VLAN.
  - Excluded frames from discarding
    - Displays the frames to be excluded from discarding when unknown multicast frames are configured to be discarded in the target VLAN.

### QoS settings

- Displays the QoS settings for the entire system.
- The table items are explained below.
  - QoS function
    - Displays whether the QoS function is enabled.
  - CoS - transmit queue mapping table
    - Displays the transmit queue ID settings corresponding to the CoS value.

- 
- DSCP - transmit queue mapping table
    - Displays the transmit queue ID settings corresponding to the DSCP value.

### Manual settings page

This is the page for the Dante optimization settings.

Select VLAN interfaces, and then press the "Confirm" button. If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Manual settings

- VLAN interface
  - Press the "Select" button to display the "VLAN interface list" dialog box.
  - You can select VLAN interfaces in the "VLAN interface list" dialog by checking the check boxes and pressing the "OK" button.

### Auto-configure via LLDP function page

This is the page for setting auto-configure via LLDP function.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### Auto-configure via LLDP function

- Auto-configure via LLDP function
  - Select whether to enable the auto-configure via LLDP function settings, from the options below.
    - Enable
    - Disable

## Y-UNOS (Yamaha Unified Network Operation Service)

### Summary

This is the page for operations related to the Y-UNOS function.

This function is not available when the stack function is enabled.

### Top page

This is the top page for the Y-UNOS.

### System settings

- Displays the current status of the Y-UNOS function.
- Press the "Setting" button to display a page where you can change the settings of the Y-UNOS function.
  - The button is disabled when the stack function is enabled.

### Detected devices list

- Press the "Next" button to display a page where you can check the detected devices' information.
  - The button is disabled when the stack function is enabled.

### System settings page

This page is for configuring the Y-UNOS settings for the system.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

### System settings

- Y-UNOS function
  - Specify whether to enable or disable the Y-UNOS function.

### Detected devices list page

This page displays the information of devices detected by the Y-UNOS function.

### Detected devices list

- Displays the information of devices detected by the Y-UNOS function.
- Up to 128 items will be displayed.
- You can search neighbor information from the "Search" box.
  - Press  to execute the search.
  - Press  to clear the search.
  - You can use regular expressions shown below in search keywords.
  - Lowercase and capital letters are treated the same for keywords.

Syntax	Explanation
A	The character "A"
ABC	The characters "ABC"

Syntax	Explanation
[ABC]	One character, either "A", "B" or "C"
[A-C]	One character between "A" and "C"
[^ABC]	An arbitrary character that is neither "A", "B" or "C"
.	An arbitrary character
A+	At least one "A" character
A*	At least zero "A" characters
A?	Zero or one "A" character
^A	A string that begins with "A"
A\$	A string that ends with "A"
ABC DEF GHI	"ABC", "DEF" or "GHI"
A{2}	Two "A" characters (AA)
A{2,}	Two or more "A" characters (AA, AAA, AAAA...)
A{2,3}	Two to three "A" characters (AA, AAA)
\b	Word breaks, such as spaces
\B	Any character besides \b
\d	An arbitrary number (same as [0-9])
\D	Any character besides numbers (same as [^0-9])
\s	Single breaking character
\S	Any single character besides \s
\w	Alphanumeric characters including underlines (same as [A-Za-z0-9_])
\W	Any character besides \w

- Press  to update information to the latest information.
- The number of search results to display at one time can be selected by pressing "Display number" on the "Select" menu.
- Press the sort switch to sort by each item.
  - With default settings, the list is sorted in ascending order by model name.
  - Press the sort switch again to toggle between ascending and descending order.

---

# Maintenance

## Command execution

### Summary

In this page you can perform operations related to command execution.

### Command execution page

In this page you can execute commands and acquire the results of command execution. After entering the command in the command entry field, press the "OK" button to execute the command. If you press the "Clear" button, the contents of the command entry field are cleared.

### Command execution

- Command input
  - In the command entry field, enter the setting in console command format (abbreviated input is not accepted).
  - You can enter multiple commands together by separating them with line-returns.
  - Execution always starts with the specially-privileged EXEC mode (enable). Enter the mode change command each time.
  - For details on commands to enter, refer to the command reference and to the information provided on the [Network device product information page](#) and [Yamaha Network Devices Technical Documentation](#).
  - The following commands cannot be entered.
    - ping
    - ping6
    - telnet
    - ssh
    - ssh-server host key generate
    - reload
    - restart
    - cold start
    - firmware-update execute
    - firmware-update sd execute
    - startup-config select
    - erase startup-config
    - copy running-config startup-config
    - copy startup-config
    - show config
    - show running-config
    - show startup-config
    - show history
    - show tech-support
    - backup system
    - restore system

- remote-login
  - stack enable
  - stack disable
  - no stack
  - stack subnet
  - no stack subnet
  - boot prioritize sd
  - no boot prioritize sd
  - quit
  - disable
  - logout
  - exit ( When in special privilege EXEC mode )
  - copy radius-server local
  - crypto pki generate ca
  - no crypto pki generate ca
  - system-diagnostics on-demand execute
- Command execution result
    - Displays the command execution result.
      - Success ... Shown if the command executed successfully.
      - Error ... Shown if the command you entered could not be executed.
      - Prohibited ... Shown if a prohibited command was entered.
  - Command execution log
    - The console log is output as the command execution record.
    - The command execution log will not necessarily always show the identical result as when the console setting operation was executed.
    - By pressing the "Obtain as text file" button, you can acquire the contents of the command execution log as a text file.
    - The name of the acquired file is "command\_YYYYMMDDhhmmss.txt".

YYYY	...	A.D. ( 4 Digit )
MM	...	Month ( 2 Digit )
DD	...	Day ( 2 Digit )
hh	...	Hours ( 2 Digit )
mm	...	Minutes ( 2 Digit )
ss	...	Seconds ( 2 Digit )

## System self-diagnostics

### Summary

This page is for finding system failures.

The system self-diagnostics function consists of boot-up, on-demand, and health-monitoring diagnostics.

- Boot-up diagnostics
  - Verifies whether any failures exist in the system boot-up sequence.
  - Performs at system start-up.
- On-demand diagnostics
  - Verifies whether any failures exist in the hardware components (e.g., interface) and memory.
  - The user can perform this at any time.
- Health monitoring diagnostics
  - Verifies whether any failures exist in the hardware components (e.g., fan) and temperatures.
  - Performs all the time in the background while the system is working.

### Top page

This is the top page for system self-diagnostics.

The top page shows each diagnostics result.

Open the accordion to display the details of each diagnostics result.

In a stack configuration, only the diagnostics results of the main switch are shown.

Diagnostics results of units other than the main switch are not shown.

If you want to check the diagnostics results of units other than the main switch using GUI, please refer to [Procedure to check the diagnostics results in a stack configuration](#).

### Boot-up diagnostics

- The boot-up diagnostics performs the following tests.
  - Loading test
    - Verifies the loading status of software modules.
    - Displays "Passed" if all modules are loaded successfully or displays "Failed" otherwise.
    - The information about modules that failed to load is not displayed.  
If you want to specify the module that failed to load, find the following errors in the log.  
"[HAMON]:err: An unexpected error has occurred. (XXXX daemon)"
- XXXX part shows the module name.
  - RTC test
    - Verifies accessing the RTC register.
    - Retrieves the time twice from RTC, then displays "Passed" if the time has changed or displays "Failed" if it is the same.  
It also displays "Failed" if retrieving the time from RTC (reading the register) fails.
  - Packet processor test
    - Verifies accessing the packet processor register.

- Writes to and reads from the packet processor register, then displays "Passed" if the values match or displays "Failed" if the values do not match. It also displays "Failed" if accessing the register fails.

### On-demand diagnostics

- Press the "Perform diagnostics" button to display the page for performing on-demand diagnostics.
- Press the "Discard diagnostics results" button to display the page for discarding the on-demand diagnostics results.
- You cannot perform on-demand diagnostics if the state of the stack is active. If you want to perform on-demand diagnostics when the stack function is enabled, please refer to [Procedure to check the diagnostics results in a stack configuration](#).
- The on-demand diagnostics performs the following tests.
  - PHY test
    - Verifies accessing the PHY register.
    - Writes to and reads from the PHY register, then displays  if the values match or displays  if the values do not match. It also displays  if accessing the register fails.

### Health monitoring diagnostics

- Press  to update the results of health-monitoring diagnostics.
- The health-monitoring diagnostics performs the following tests.
  - Temperature test
    - Monitors the temperatures below.
      - CPU
      - PHY
      - SFP
      - TS
      - PSE
    - Displays "Passed" if the temperature has not exceeded the threshold or displays "Failed" otherwise.
  - Fan test
    - Monitors the fan speed.
    - Displays "Passed" if the fan speed is normal or displays "Failed" if the fan has stopped or the fan speed has increased.
  - Temperature sensor test
    - Monitors the temperature sensors.
    - Displays "Passed" if the temperature sensors are working properly or displays "Failed" if any error has occurred.
  - PoE test
    - Monitors the PoE power supply status.
    - Displays  if the PoE power supply control is normal or displays  if any error has occurred.
  - SFP test

- Monitors the SFP optical Rx level.
- Displays  if the optical RX level is in the normal range or displays  if it is out of the range.

### **On-demand diagnostics performing page**

This page is for performing on-demand diagnostics.

Press the "OK" button to perform the on-demand diagnostics.

All ports are shut down while the diagnostics is performing.

The unit restarts automatically after performing on-demand diagnostics.

### **On-demand diagnostics results discarding page**

This page is for discarding the on-demand diagnostics results.

Press the "OK" button to discard the on-demand diagnostics results.

### **Procedure to check the diagnostics results in a stack configuration**

The diagnostics results show only for the unit currently logged in.

If you want to check the diagnostics results of all units in the stackconfiguration using GUI, perform the following procedures.

- Disconnect the connections between the member switches.
- Access the GUI of the unit that you want to show the diagnostics results.
- (Optional) Perform on-demand diagnostics.

---

## Cable diagnostics

### Summary

This page is for diagnosing whether cable failures have occurred.

The cable diagnostics can check failures of the LAN cables connected to the LAN ports of this unit.

You can use this to troubleshoot network problems or as a simple cable check when setting up a network.

Please note that this diagnostics is a simplified function, so it cannot detect as precisely as a specialized device.

Cables should be longer than 10m for correct diagnostics.

The diagnostics does not work correctly if the port is supplying PoE power.

### Top page

This top page is for cable diagnostics.

### Cable diagnostics

- Press the "OK" button to perform the cable diagnostics.
  - The following ports are not able to perform cable diagnostics.
    - The port interface is disabled
    - The port is shut down by loop detection
    - The port is shut down by spanning tree
    - The port is shut down by port security violation
  - The port under diagnostics will temporarily linke down.
- Press the "Discard diagnostics results" button to delete the last cable diagnostics results.
- The cable diagnostics results show the following items.
  - Port
    - The port performed diagnostics.
  - Result
    - The status of cable connected to LAN port.
      - OK : Electrically connected.
      - Open : A target device is not connected, or the cable is damaged.
      - Short : The cable is shorted.
  - Distance to the cable failure point
    - If the result is "Open" or "Short", displays the distance from the LAN port to the cable failure point in meters.

## Update firmware

### Summary

In this page you can perform operations related to firmware update.

### Top page

This is the top page for firmware update.

You can start the procedure for updating the firmware via thenetwork. Various settings for updating the firmware via the network are displayed.

### Firmware update information

- Displays the firmware revision and basic settings.
- Displays the firmware revision for the next start-up if a restart is pending after a firmware update.
- Press the "Setting" button to access a page where you can change the settings.

### Update firmware from PC

- When you press the "Next" button, the procedure for updating the firmware from the PC will be started.

### Update firmware via network

- When you press the "Next" button, the procedure for updating the firmware via the network will be started.
- Various settings for updating the firmware via the network are displayed.
- Press the "Setting" button to access a page where you can change the settings.

### Firmware update basic settings page

This page is for configuring the basic settings for the firmware update.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

### Firmware update basic settings

- Restart timing after the update
  - Specify the restart timing after the firmware update.
- Restart method after the update
  - If you want the system to restart after the firmware update in a stack configuration automatically, you can specify whether each switch restarts in sequence or simultaneously.
  - This item cannot be configured when the stack function is disabled.

### Update firmware from PC page

In this page you can specify the firmware file placed on the PC from which you are accessing the web GUI, and perform the firmware update.

In "Select file," select the firmware file that you want to use for the update, and press the "Confirm" button. If there are no mistakes in the confirmation screen, press the "OK" button.

### Update firmware from PC

- Specify update file

- Selects the firmware file used for the update
- Restart after the update
  - Specify whether or not to restart after the firmware update automatically.
  - The timing for restarting depends on the **Restart timing after the update** in the **Firmware update basic settings**.

### Update firmware via network page

In this page you can download a firmware file from a web server, and perform the firmware update. This function lets you easily perform the entire process of checking for the latest firmware, downloading it, and updating the firmware.

When you open the page, the revision of the firmware file on the web server is automatically checked.

If the download URL is the Yamaha website and an updateable firmware revision is found. The "OK" button displays a guide to the software license agreement website. Please read the contents on the website and press the "OK" button if you agree to the terms. Press the "OK" button to start downloading the firmware file from the web server.

### Update firmware via network

- Current firmware revision
  - The revision of the currently-used firmware file is shown.
- Firmware revision available for update
  - Updatable revisions of the firmware files on the web server are shown.
- Restart after the update
  - Specify whether or not to restart after the firmware update automatically.
  - The timing for restarting depends on the **Restart timing after the update** in the **Firmware update basic settings**.

### Update via network settings page

In this page you can make various settings for updating the firmware via the network.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

### Update via network settings

- Download source URL
  - This is the setting of the URL at which the firmware is located.
- HTTP proxy server
  - This is the HTTP proxy server setting used to download the firmware via the network.
- Revision downgrade
  - This setting permits or forbids rewriting to an older version of firmware.
- Timeout
  - This setting specifies the timeout time during the process of updating the firmware via the network.

## CONFIG management

### Summary

In this page you can import and export CONFIG.

This unit operates in accordance with its CONFIG file (settingsdata). A CONFIG file consists of a combination of multiple commands.

### Top page

This is the top page for CONFIG management.

You can start the process of importing a CONFIG, or the process of exporting a CONFIG.

### Import

- Press the "Next" button to display a page where you can import a CONFIG.

### Export

- Press the "Next" button to display a page where you can export a CONFIG.

### Import page

In this page, a CONFIG from the PC can be copied to internal non-volatile memory, updating the CONFIG.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

If the currently used CONFIG is the same as the import-destination CONFIG, the unit restarts automatically after the import has ended successfully.

If you want to start up with a CONFIG file that is not currently being used, change the setting using the **startup-config select** command before restarting.

### Import CONFIG

- Import method
  - Select the import method from the following options.
    - Import all settings (.zip)
      - Import information such as a CONFIG file and a L2MS agent CONFIG together.
      - You cannot be used when using YNO manager for access.
    - Import a CONFIG file (.txt)
      - Import a CONFIG file.
    - Import a L2MS agent CONFIG (.bin)
      - Import a L2MS agent CONFIG.
- Settings to import
  - Press the "Select a file" button to display the file selection dialog box.
  - You can use the settings obtained on the export page.
- Import-destination
  - Select the import-destination CONFIG in internal non-volatile memory.
  - Cannot be changed when the stack function is enabled. (The currently used CONFIG is selected.)

---

## Export page

In this page you can copy a CONFIG from internal non-volatile memory to the PC.

When you have finished entry, check the entered content and press the "OK" button.

## Export CONFIG

- Export method
  - Select the export method from the following options.
    - Export all settings (.zip)
      - Export information such as a CONFIG file and a L2MS agent CONFIG together.
      - You cannot be used when using YNO manager for access.
    - Export a CONFIG file (.txt)
      - Export a CONFIG file.
    - Export a L2MS agent CONFIG (.bin)
      - Export a L2MS agent CONFIG.
- Settings to export
  - Select the CONFIG in internal non-volatile memory that you want to export.
  - Cannot be changed when the stack function is enabled. (The currently used CONFIG is selected.)

## Summary data management

### Summary

This page is for performing operations related to the summary data.

### Top page

This is the top page for summary data management.

The settings for whether to back up the summary data or not are displayed.

Here you can start the process of clearing the summary data and exporting summary data to a PC.

### Backup settings for summary data

- The settings for whether to back up the summary data or not are displayed.
- Press the "Setting" button to access a page where you configure the backup settings.

### Clearing summary data

- Press the "Next" button to begin the process of clearing the summary data.

### Export summary data

- Press the "Next" button to begin the process of exporting the summary data to a PC.

### Backup settings page for summary data

This page is for configuring the summary data backup settings.

Enter the settings, and then press the "Confirm" button.

If there are no mistakes in the input content of the confirmation screen, press the "OK" button.

When backup settings are enabled, the summary data will be backed up whenever an SD card has been inserted.

### Backup settings for summary data

- Summary data to be backed up
  - Select the summary data to back up from the list below.
    - Traffic information
    - Resource information
    - Power consumption information

### Page for clearing summary data

This page is for clearing the summary data.

When you have inputted the settings, press the "Confirm" button.

If there are no mistakes in the input content confirmation screen, press the "OK" button.

When the summary data has been cleared, both the data saved in internal volatile memory and the data backed up to SD card will be cleared.

### Clearing summary data

- Summary data to clear
  - Select the summary data to clear from one of the following.
    - Traffic information
    - Resource information

- Power consumption information

### Export page for summary data

This page is for exporting summary data.

When you have finished inputting, check the inputted content and press the "OK" button.

Implementing the summary data export will download a ZIP file.

See [Export file configuration](#) for more information on the configuration of the ZIP file.

### Export summary data

- Summary data to export
  - Select the summary data to export from one of the following.
    - Traffic information(Transmit)
    - Traffic information(Reception)
    - Resource information
    - Power consumption information
- Specifying a timespan
  - Select the month(s) of the data to be exported.
  - Specify the month(s) from the previous year using the drop-down list box.

### Export file configuration

This explains about the folder that will be extracted when decompressing the ZIP file.

The configuration when the **October 2017traffic information (received)** is exported is shown below.

- 20171103150412\_trf\_rx\_csv.zip
  - 20171103150412\_trf\_rx\_csv
    - 20171001\_trf\_rx\_hour.csv
    - :
    - 20171031\_trf\_rx\_hour.csv
    - 201710\_trf\_rx\_day.csv

This explains about the folder and files after extraction.

- 20171103150412\_trf\_rx\_csv
  - The CSV files with the summary data are contained in this folder.
  - The time of export and data type are used in the folder name.
  - One of the following will be used for the data type, according to the type specified.
    - trf\_tx  
For traffic information (transmission)
    - trf\_rx  
For traffic information (reception)
    - resource  
For resource information
- 20171001\_trf\_rx\_hour.csv
  - This is the CSV file with the summary data.

- The date, data type and data unit time will be included in the file name for the target data.
- The naming convention for the data type is the same as for the folders.
- One of the following will be used for the data unit time.
  - hour  
Files that are totaled every hour, containing one days' worth of data
  - day  
Files that are totaled every day, containing one months' worth of data

---

## SYSLOG management

### Summary

In this page you can view and edit the settings of the SYSLOG function.

The operation history of this device is output as the SYSLOG (log data) according to the settings of the SYSLOG function. In addition to recording the SYSLOG inside this device, you can also specify a destination address for output to an external host.

### Top page

This is the top page for SYSLOG management.

The current settings for the SYSLOG function are shown.

### SYSLOG settings

- The output-level of SYSLOG that is output, and the header information and destination address for the SYSLOG transmission are shown.
- Press the "Setting" button to access a page where you can change the settings.
- You can delete the saved log.

### SYSLOG settings page

In this page you can make settings for the SYSLOG function.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

For details on the various SYSLOG types, refer to the command reference.

### SYSLOG settings

- SYSLOG type
  - ERROR
    - This setting specifies whether ERROR type SYSLOG is output.
  - INFO
    - This setting specifies whether INFO type SYSLOG is output.
  - DEBUG
    - This setting specifies whether DEBUG type SYSLOG is output.
- SYSLOG transmission
  - Header
    - You can configure the header for outputting SYSLOG to external hosts.
    - You can specify whether to include or exclude the timestamp and hostname in the SYSLOG message header.  
The hostname is stored as the device name of the unit.
  - SYSLOG transmission destination address
    - This is the transmission destination address setting when outputting the SYSLOG to an external host.
    - You can specify up to two IPv4/IPv6 destination addresses.
    - For IPv6 link local addresses, you must also specify the interface to send from. (Format:

fe80::X%vlanN)

- If no destination address is specified, the SYSLOG is recorded only inside the switch.

◦ Facility

- This is the facility setting when outputting the SYSLOG to an external host.
- Select the facility value from 0 - 23.

---

## Backup / Restoration

### Summary

This page is for the backup and restoration of the configuration of the entire device.

If the device fails, you can restore the backup file to a newly prepared device to restore the settings.

The backup file contains the following information.

- Startup-config and its associated information
- Setting values for the startup-config select command
- Setting values for the boot prioritize sd command

Do not perform any operation (such as the write command or the erase startup-config command) related to the CONFIG while performing the backup or restoration on this page.

In a stack configuration, you need to back up and restore for each switch.

### Top page

This is the top page for the backup/restoration.

### Backup

- Press the "Next" button to display the page for backing up the system.

### Restoration

- Press the "Next" button to display the page for restoring the system.

### Backup page

This page is for downloading the configuration of the entire device as a backup file.

Press the "OK" button to download the backup file for the device that you are currently accessing.

If the stack function is disabled, the execution screen is displayed. Press the "OK" button to download the backup file for the device that you are currently accessing.

If the stack function is enabled, the input screen is displayed. Select the device to back up, and press the "Confirm" button. Then press the "OK" button on the execution screen to download the selected device's backup file.

The following is an explanation of the screen when the stack function is enabled.

### Backup

- Stack ID of the device to back up
  - Select the stack ID of the device to back up.
  - The model name and the serial number of the selected device are displayed.

### Restoration page

This page is for restoring the backup configuration of the entire device to this device.

When you have entered the settings, press the "Confirm" button. If there are no mistakes in the input content confirmation screen, press the "OK" button.

When the restoration is complete, the device automatically restarts.

## Restoration

- Backup file
  - Select the backup file to restore.

## Restoration procedure in a stack configuration

When the stack function is enabled, the configuration for the entire device cannot restore from this page.

If some of the devices that make up the stack fail and need to replace them, follow the procedure below to restore them.

- Update the firmware of the newly prepared device to the same version as the device to be replaced.
- After updating the firmware, access this page and restore the configuration you have backed up before for the entire device.
- After the restoration and restart are complete, turn off the power. Then connect the device to the main switch in operation, and turn on the power.

---

## Restart and initialization

### Summary

In this page you can restart this unit and return it to the factory-set state.

### Top page

This is the top page for restart and initialization.

Here you can start the process of restarting this unit or returning it to the factory-set state.

### Restart

- When you press the "Next" button, the process of restarting this unit will begin.

### Initialization

- When you press the "Next" button, the process of returning this unit to the factory-set state will begin.

### Restart page

In this page you can restart this unit.

When you press the "OK" button, the unit will restart.

If the stack function is disabled, press the "OK" button to restart the unit.

If the stack function is enabled, select the device to restart from the input screen and press the "Confirm" button. Then, press the "OK" button on the execute screen to restart the specified device.

Note that when you execute restart, the settings that were being changed will not be saved. In addition, the GUI cannot be accessed until restart has completed.

### Initialization page

In this page you can return this unit to its factory-set state.

After you have entered the privileged password, press the "Confirm" button. Confirm the content to be executed, and if you want to return this unit to its factory-set state, press the "OK" button.

Note that when the unit is returned to its factory-set state, all settings will return to their default values, including the address for accessing the GUI.

If the stack function is enabled, only the main switch is initialized.

### Initialization

- Privileged password
  - To return the unit to its factory-set state, enter the privileged password.

## Find this switch

### Summary

The "Find this switch" function uses the LED installed in this product to inform you of the installation location of the product in an easy-to-understand manner.

Please use it when you want to check the installation location of the product or when you want to show the operation target to the workers at the site.

While this function is running, the LED will be in the following states, respectively.

- LED : The LEDs on all ports flash orange.

### "Find this switch" execution page

This page is for executing the "Find this switch" function.

### Find this switch

- Displays the execution status of "Find this switch" function.
- You can start the "Find this switch" function by pressing the "Start" button when it is stopped.
- You can stop the "Find this switch" function by pressing the "Stop" button when it is running.
- Press the "Start" button to display the dialog and select the following items to start the notification.
  - Notification method
    - Select the Type of notification from the following.
      - Blink the port LED
        - Blinks the LEDs on all ports in orange while the function is running.
        - It cannot be selected when the Current LED mode is OFF mode.
        - You can configure the LED mode in "Management → Unit settings → LED mode setting".
  - Notification period
    - Select the time to continue the notification from the following.
      - 30 Seconds
      - 1 Minutes
      - 3 Minutes
      - 5 Minutes
      - 10 Minutes
      - 1 Hours
    - After pressing the "OK" button, the notification will be automatically stopped when the Duration of notification expires.

