SWX2210P series

Technical Data

Rev.1.03.14

EN

Contents

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
- ProAV settings
- Detailed settings
- Management
- 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.

<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 not be able to use the web GUI itself. 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 not be able to use the web GUI itself.
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 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 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. : SWX2210P-10G)
- 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
  Login failed. The user name or password is incorrect.
- 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, configure the cookie settings Introduction　2. Operating environment.

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 a certain period of time have elapsed from the last data communication.
- Session timeout interval can be set either in the Web GUI’s "Management" → "Access management" → "Various server settings" → "Web GUI access" page, or by using the **http-server login-timeout** command.
- Up to four sessions can be established at one time.
- Information for a session can be checked using the “show users” command.

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

ProAV settings

In this page you can make ProAV settings for this unit. The following items are provided.

- ProAV profile
- Multicast

Detailed settings

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

- Basic settings
- Interface settings
    - Physical interface
    - Port mirroring
    - Link aggregation
    - PoE control
- VLAN
    - Create VLAN
    - Tag VLAN
    - Multiple VLAN
- Layer 2 functions
    - MAC address table
    - Loop detected
    - Pass through
- Layer 3 functions
    - DNS client
- Multicast
    - Multicast basic settings
    - IGMP snooping

- MLD snooping
- Traffic control
  - Access list
    - Create Access list
    - Apply Access list
  - QoS
  - Flow control
  - Storm control

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
- Schedule execution
- SNMP
  - MIB
  - Community
  - SNMPv3 User
  - SNMP trap
- LLDP
- L2MS
- Maintenance
  - Command execution
  - Update firmware
  - CONFIG management
  - SYSLOG management
  - Restart and initialization
  - Cable diagnostics

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)

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

About the dashboard

Using the dashboard

- **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.

The dashboard shows the following buttons.

- **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 "Confirm all" button ( ) changes all history entries to a confirmed state.
- In the warning history list, pressing the "Delete all" 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

The following gadgets can be used.

- System information
- Resource information
- Interface information
- SYSLOG
- Traffic information (Transmit / Reception)
- Resource information (Graph)
- Power consumption information
- PoE power supply

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.

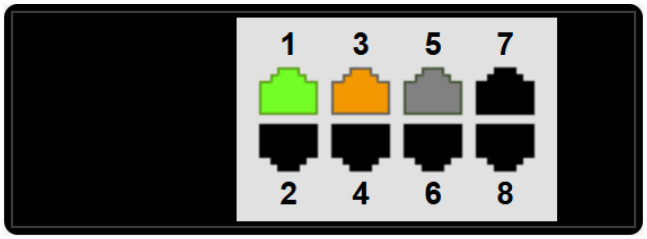
- **Separate the gadget screen:**
  - A "Separate" button () is shown in the upper right of each gadget.
  - If you press the "Separate" button, that gadget alone is shown in a different window.
  - At this time, the corresponding gadget in the dashboard is indicated as "In separate window."
  - If a 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.
    Example) System information gadget: http://192.168.100.240/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
	Thr temperature increases.
	The fan stops.
Resource information	When CPU usage exceeds **80 %**
	When memory usage exceeds **80 %**
Interface information	An loop occurs.
	The PoE power supply stops abnormally.
	An error occurs in the PoE power supply control.
Traffic information	The throughput exceeds the link speed of **60 %**.

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

Icon	Explanation
	Link up (port speed 1000BASE-T)
	Link up (port speed 100BASE-TX)
	Link up (port speed 10BASE-T)
	Link down
	Error occurrence(Loop detection)

PoE supply

Icon	Explanation
	Does not supply power supply
	PoE is being supplied (supply Class0—3)
	PoE is being supplied (supply Class4)
	Power supply stopped
	Error occurrence (PoE power supply stops abnormally)

Bandwidth usage:For a LAN port

Icon	Explanation

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

System information

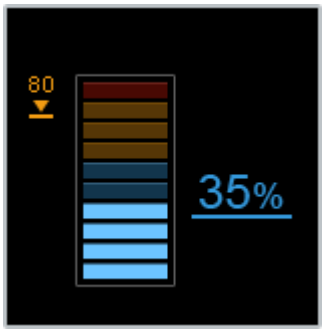
The following information is displayed.

- **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..
- **Currently-running settings file:**
  - The currently used CONFIG file is shown.
- **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.
- **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.
- When you press "Clear peak values," the previous peak values will be cleared.
  - 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).

Traffic information

The physical interface traffic is displayed on a graph.
There are different gadgets for the transmission traffic and for the reception traffic.

- 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.
- **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 [Mbps] to a maximum of 1000 [Mbps].
- Time, from the current time to 120 seconds ago (in the form hh:mm:ss), is shown on the horizontal axis.
- 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 selections on the legend to their defaults, as shown below.
    - 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 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 selections on the legend return to their defaults.

Resource information(Graph)

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

- 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 [%].
- Time, from the current time to 120 seconds ago (in the form hh:mm:ss), is shown on the horizontal axis.

- 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 selections on the legend to their defaults, as shown below.
    - 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 selections on the legend return to their defaults.
- When directly inputting the URL for a separated window and displaying a gadget
    - The selections on the legend return to their defaults.

Power consumption information

A graph of the power consumption by the unit is displayed.

- Shows power consumption every second for the last 2 minutes.
- The graph will be automatically refreshed each second.
- Time, from the current time to 120 seconds ago (in the form hh:mm:ss), is shown on the horizontal axis.
- Moving the cursor over the graph shows the power consumption value for the given date and time.
- The following methods are recommended to suppress power consumption.
    - Slow down the link speed of ports with low bandwidth usage.
    - Use the scheduling functionality to shutdown unused ports or shut off PoE power supply to them at night or on closed days.

PoE power supply

Display the PoE power supply.

- The current/maximum power supply, the remaining available power supply, 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.

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 Network device technical information page .

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 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 primaly dedecated line

Dante primary (VLAN 1)

Select this network structure when the switch is used as a Dante dedicated primary line and there is no need to partition the network with VLANs.

Assign all ports to the same network as VLAN1 and apply the Dante primary profile.
Note that the only differences from selecting "Use as Dante Secondary Dedicated Line "are the profile name and color settings. All other settings are the same.

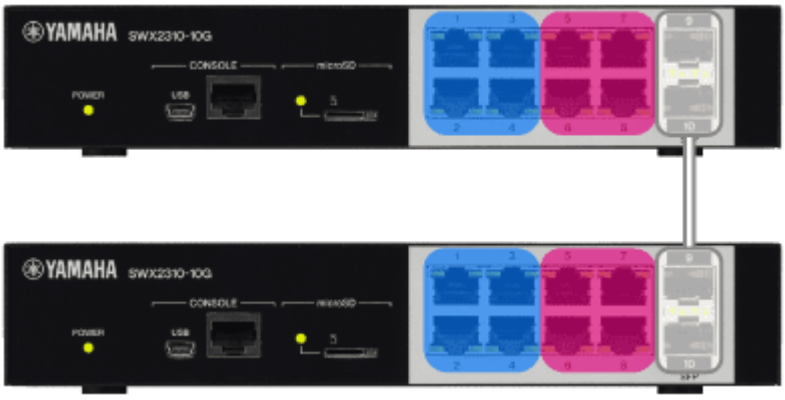
Use as Dante secondary dedecated line

Dante secondary (VLAN 1)

Select this network structure when the switch is used as a Dante dedicated secondary line and there is no need to partition the network with VLANs.

Assign all ports to the same network as VLAN1 and apply the Dante secondary profile.
Note that the only differences from selecting "Use as Dante Primary Dedicated Line "are the profile name and color settings. All other settings are the same.

Bundle Dante primary/secondary lines



Dante primary (VLAN 1)

Dante secondary (VLAN 2)

Trunk (ALL)

Select this network structure when the primary and secondary lines are bundled together for connecting a single LAN cable between switches.
Assign the primary line to VLAN1 and the secondary line to VLAN2, and apply a Dante profile to both VLANs.
The settings applied are the same for the primary (VLAN1) and secondary (VLAN2) 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.
The primary line (VLAN1) is set as the native VLAN (untagged) and the secondary line (VLAN2) is 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 both switches.

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.

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

Redundant Dante primary/secondary lines

Dante primary (VLAN 1)

Dante secondary (VLAN 2)

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

Assign the primary line to VLAN1 and the secondary line to VLAN2, and apply a Dante profile to both VLANs. The settings applied are the same for the primary (VLAN1) and secondary (VLAN2) lines, but in this network configuration, an L2MS filter is applied to ports on the secondary line (VLAN2) 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.

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

Set NDI profile

The NDI optimization settings is applied.
Assign all ports to the same network as VLAN1 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 both switches.

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 to VLAN1.
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.

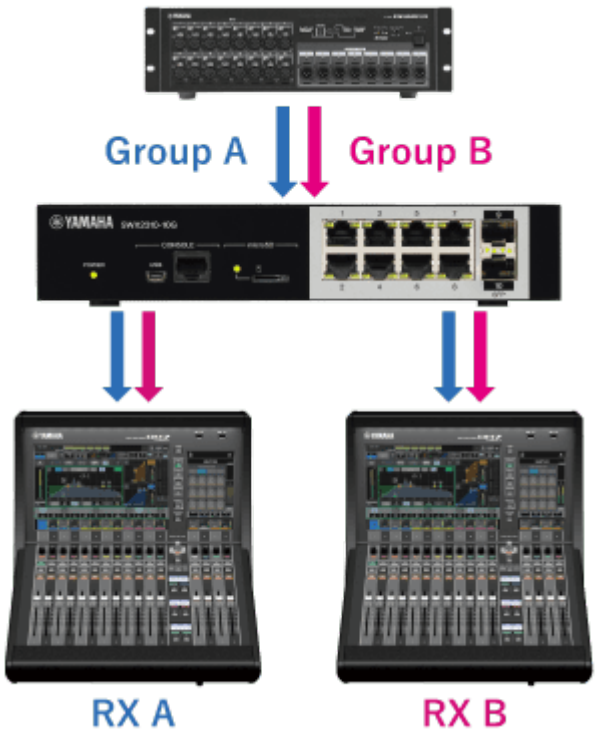
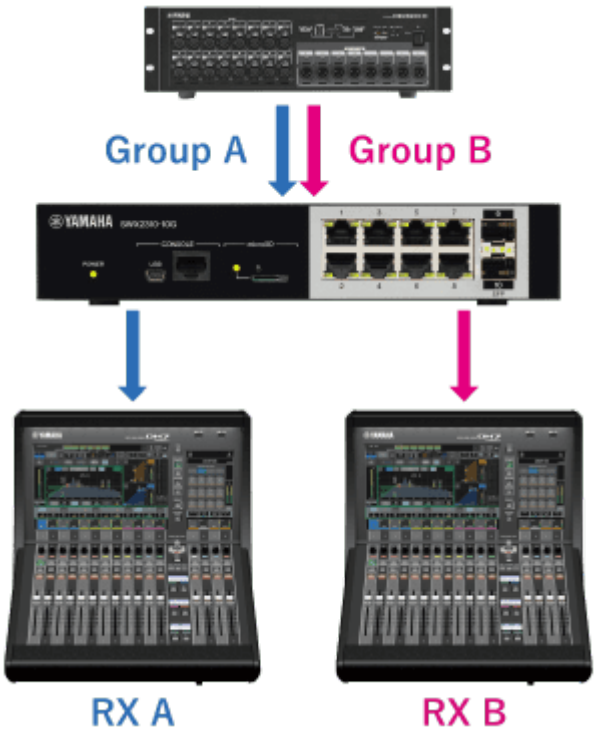
Multicast

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.

In the case of flooding	In the case of IGMP snooping
	

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 20 seconds 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

Basic settings

Summary

This page is for configuring the basic settings.

Top page

This is the top page for the basic settings.

IPv4 settings

- Shows the IPv4 settings.
- The table items are explained below.
    - IPv4 address
        - Displays the IPv4 address setting.
    - IPv4 default gateway
        - Displays the IPv4 default gateway setting.
- Press the “Setting” button to show the page for IPv4 settings.

IPv6 settings

- Shows the IPv6 settings.
- The table items are explained below.
    - IPv6 address
        - Displays the IPv6 address setting.
    - IPv6 default gateway
        - Displays the IPv6 default gateway settings.
- Press the “Setting” button to show the page for IPv6 settings.

IPv4 settings page

This page is for configuring IPv4 settings.
Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

IPv4 settings

- VLAN ID
    - From the list, select the VLAN to assign IPv4 address.
    - However, the VLAN for which frame forwarding is invalid cannot be selected.
- IPv4 address

  Select the IP address from the following items. Only a VLAN for which frame forwarding is valid can be specified for this item.
  Only one VLAN interfaces can be configured for an IPv4 address.

- Obtain automatically using DHCP
    - When auto-acquire does not work, the link local address is automatically configured by the Auto IP function.
- Specify a fixed IP address
    - Enter the IP address and subnet mask.

- IPv4 default gateway
    - Specify an IP address for the IPv4 default gateway.
    - If omitted when DHCP is used, the default gateway obtained by DHCP is used.

IPv6 settings page

This page is for configuring IPv6 settings.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

IPv6 settings

- VLAN ID
    - From the list, select the VLAN to assign IPv6 address.
    - However, the VLAN for which frame forwarding is invalid cannot be selected.
- IPv6 address

  Only one VLAN interfaces can be configured for an IPv6 address.

    - Select whether the IPv6 address will be enabled or disabled from the following items.
        - Disable IPv6
        - Enable IPv6
    - For global addresses, select from the following items.
        - Not set
        - Obtain automatically using RA
        - Specify a fixed IP address
            - Enter the IP address and subnet mask.
    - Set the link local address.
- IPv6 default gateway
    - Specify an IPv6 address for the IPv6 default gateway.
    - If omitted when RA is used, the default gateway obtained by RA is used.

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 settings.

MRU setting

- The MRU settings is shown.
- The table items are explained below.
    - MRU
        - Displays the maximum amount of data that can be received at one time.
- Press the “Setting” button to show the MRU settings page.

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.
    - Speed/communication mode
        - Displays the operating speed and communication mode.
        - For automatic settings, “**(Automatic)**” is displayed at the end of the status indication.
    - EEE function
        - Displays the operating status of the EEE function.
    - Automatic cross/straight detection
        - Displays the operating status of the automatic cross/straight detection.
    - Explanation
        - 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.
    - 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

        - Explanation : Unset
        - Speed/communication mode : Automatic
        - EEE function : Disabled (Don’t use power-conservation Ethernet function)
        - Automatic cross/straight detection : Enabled

MRU settings page

This page is for configuring the MRU settings.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

MRU setting

- MRU
    - Specify the maximum amount of data that can be received at one time.
    - The input range is 1522 - 10240 bytes.

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 setting 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
- Explanation
    - 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
- EEE function
    - Select the operation for the EEE function from the following options.

        - Disabled (Don’t use power-conservation Ethernet function)
        - Enabled (Use power-conservation Ethernet function)
- Automatic cross/straight detection
    - Select the operation for the automatic cross/straight detection from the following options.
        - Enabled
        - Disabled
    - If the automatic cross/straight detection is disabled, MDI is used for the cable connection type.

Port mirroring

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 4 sniffer ports can be configured.
- Monitored ports that are already monitored cannot be monitored from another sniffer port.
- Sniffer ports cannot be monitored from another sniffer port.

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 setting confirmation screen, press the "OK" button.

Port mirroring settings

- Sniffer port
    - When configuring new settings
        - From the list, select the interface for a sniffer port.
        - Other interfaces that are already monitored and sniffer ports are not displayed in the list.
    - When changing settings
        - Displays the interface name of the selected sniffer port.
- 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 the link aggregation.

Load balance rule settings

- Shows the load balance rule settings.
- The table items are explained below.
    - Load balance rule
        - Displays the load balance rule settings.
- Press the “Setting” button to show the page for the load balance rule settings.

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.
    - Explanation
        - 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 8 logical interfaces can be configured.

Load balance rule settings page

This page is for configuring the load balance rule settings.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Load balance rule settings

- Load balance rule

- 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 setting confirmation screen, press the "OK" button.

Logical interface settings

- Logical interface type
  - When configuring new settings
    - Displays the type of logical interface.
  - When changing settings
    - Displays the selected logical interface name.
- Interface number
  - Specifies the interface number.
  - A value from 1 to 8 can be inputted.
  - 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 8 ports can be selected.
- Operation
  - Select from the following logical interface operations.
    - Enable interface
    - Disable interface
- Explanation
  - 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.

PoE

Summary

This page is for changing the PoE control settings.

Top page

This is the top page for the PoE control settings.

PoE control basic settings

- The current settings of the PoE control for the entire system are show.
- Press the "Setting" button to access a page where you can change the settings.

PoE control settings

- PoE control settings are shown for each interface that supports PoE power supply.
- Press the "Setting" button to access a 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 contains a check mark.
- If you press the "Return to defaults" button, the settings will be initialized for all interfaces whose check box contains a check mark.
    - The default PoE power supply setting is "Enabled" and the default power priority setting is "Low" for all interfaces that support PoE power supply.
- If the PoE control settings is disabled for the entire system, the PoE control settings for each interface cannot be made.

PoE control basic settings page

In this page you can enable/disable PoE power supply for the entire system and set the guard band.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

PoE control basic settings

- PoE power supply for entire system
    - Enabled
        - The PoE power supply will be enabled for the entire system.
    - Disabled
        - The PoE power supply will be disabled for the entire system.
- Guard band
    - The guard band specifies the tolerance for the maximum power supply specified to avoid unintended power supply interruptions.
    - The default guard band setting is "7" W, and the input range is 0 - 30.

PoE control settings page

In this page you can enable/disable PoE power supply and set power priority for the selected interface.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

PoE control settings

- Port
  - The interface for which settings are made is shown.
- PoE power supply
  - Enabled
    - The PoE power supply will be enabled for the selected interface.
  - Disabled
    - The PoE power supply will be disabled for the selected interface.
- Power priority
  - Select power priority from the following items.
    - Low
    - High
    - Critical
  - In descending order, the priority levels are **Critical**, **High**, or **Low**.
  - If interfaces have the same priority setting, the interface with the lower interface number is prioritized.
- Explanation
  - Sets the description text for the interface which supports PoE power supply.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding **?**.
  - Up to 64 characters can be inputted.

VLAN

Create VLAN

Summary

In this page you can create or delete VLANs.

Top page

This is the top page for creating a VLAN.

VLAN list

- Information for the defined VLANs is 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 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)
- 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 setting 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)

- Explanation
  - 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.

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 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 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 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)
- 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 setting confirmation screen, press the "OK" button.

Tag VLAN settings

- Port
    - The LAN 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
- Associated VLAN

  The content of the settings differs depending on the operating mode.

  【 For an access port 】

    - AccessVLAN
        - From the list, select the access port’s assigned VLAN
        - However, the following cannot be selected as access VLAN.
            - VLAN for which frame forwarding is invalid

【 For a trunk port 】

- NativeVLAN
  - 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
    - VLAN for which frame forwarding is invalid
- TrunkVLAN
  - 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 "Select VLAN" dialog box.
  - However, the following cannot be selected as trunk VLAN.
    - VLAN selected as native VLAN
    - 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 one switch into different groups and prohibit communication between the groups.
A single port can belong to multiple groups, so that the same network address can be assigned even to different groups.
If both the multiple VLAN and port-based VLAN / tagged VLAN are used, communication is not possible between ports that belong to different VLANs, even if the ports belong to same multiple-VLAN group.

Top page

This is the top page for multiple VLANs.

Multiple 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, the settings can be changed for all LAN 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 ports and logical interfaces 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 by selecting the corresponding checkboxes in the “Multiple VLAN group selection” dialog and pressing 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

- The current settings for the MAC address learning are shown.
- When you press the "Setting" button, a page where you can change the MAC address learning 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 256 static MAC address entries can be created from the Web GUI.

MAC address learning basic settings page

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

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Basic settings for MAC address learning

- MAC address learning

  Select the MAC address learning from the following items.

  - Use MAC address learning
  - Don’t use MAC address learning
- Aging time for dynamic entries
  - Specify a setting in the range of 10 seconds to 634 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 setting 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 transmission

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

  - Transmit 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, "Transmit" 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.

Loop detection

Summary

In this page you can edit the settings of the 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 loop detection.

Loop detection basic settings

- Displays the system settings of loop detection.
- Resetting the loop detection status
  - You can immediately resolve the loop detection states (e.g., Blocking) by reset feature.
- The table items are explained below.
  - Displays the loop detection settings for the entire system.
  - Displays the blocking interval after a loop is detected.
  - Press the "Setting" button to access a page where you can change the settings.

Loop detection settings

- The loop detection setting and current loop detection status is shown for each LAN port.
- Press the "Setting" button to access a page where you can change the settings of the selected LAN port.
- If you press the "Specify all" button, the settings can be changed for all LAN ports whose check box contains a check mark.
- Pressing the "Update" button will reacquire the current loop detection status for all LAN ports.
- If you press the "Return to defaults" button, the settings will be initialized for all LAN ports whose check box contains a check mark.
  - The default loop detection setting for all ports is "Enabled".
- If the settings do not use the loop detection for the entire system, loop detection settings for each LAN port cannot be made.

Loop detection basic settings page

In this page you can specify whether the loop detection is used for the entire system and the blocking interval.
Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Loop detection basic settings

- Loop detection for the entire system
  - Enable
    - The loop detection will be enabled for the entire system.
  - Disable
    - The loop detection will be disabled for the entire system.
- Blocking interval
  - Auto

        - When a loop is resolved, the loop detection state automatically returns to "Normal".
    - Specify interval
        - Even if the loop has already been resolved, the loop detection status keeps "Blocking" for the specified period from the time when the loop was detected.

Loop detection settings page

In this page you can specify whether the loop detection is used for the selected interface.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Loop detection settings

- Port
    - The LAN port for which settings are made is shown
- Loop detection
    - Enabled
        - The loop detection will be enabled for the selected interface.
    - Disabled
        - The loop detection will be disabled for the selected interface.

Pass through

Summary

In this page you can edit the settings of the pass through function.
You can enable/disable the pass through function.

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.
- EAP frames are used for IEEE 802.1X authentication.
- If EAP pass through is enabled, the unit can be installed between an IEEE 802.1X authentication switch and a computer.
- Press the "Setting" button to access a page where you can change the settings.

BPDU pass through setting

- The current setting is shown as to whether the BPDU pass through is enabled.
- BPDU frames are used in the spanning tree protocol (STP).
- If BPDU pass through is enabled, the unit can be installed between switches using STP.
- 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 setting confirmation screen, press the "OK" button.

EAP pass through setting

- EAP pass through
    - Enabled
        - Forwards received EAP frames.
    - Disabled
        - Discards received EAP frames.

BPDU pass through settings page

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

BPDU pass through setting

- BPDU pass through
    - Enabled
        - Forwards received BPDU frames.
    - Disabled

- Discards received BPDU frames.

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.
- 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 setting 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 255 characters can be inputted.
- Search domain
    - Specify the search domain.
    - Up to 255 characters can be inputted.

- Up to six search domains can be specified.

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 all ports 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 mDNS, 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 page where you can change the IGMP snooping function 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 IGMP snooping function are as follows
        - IGMP snooping function: Enabled
        - 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.
            - When the "Disable on ports where a switch is connected" is checked, the fast leave function is not used on the port where a 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

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.
    - Comment
        - The comment 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.
- On this page, you can reference and configure up to 28 access list for each access list type of IPv4/IPv6/MAC.

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 setting 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.
- 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.

- Comment
  - Specify the comment using up to 32 single-byte alphanumeric characters and symbols.
  - The "?" character cannot be used in the comment text.
- Control conditions
  - Specify the control conditions for the access list.
  - Up to 128 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
  - 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.
            - Comment
                - The comment set in this access list 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 setting 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 "Select access list" dialog box.
    - On the "Select access list" 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 "Select access list" dialog box to display the targeted access list.

QoS

Summary

In this page you can edit the settings of the QoS (Quality of Service) function.

Top page

This is the top page for QoS.

Setting optimization for web conferencing software

- Clicking the "Next" button starts the process of optimizing QoS settings for the selected web conferencing software.

System settings

- Displays the QoS function settings for the entire system.
- The table items are explained below.
    - QoS function
        - Displays whether the QoS function is enabled or disabled.
    - Scheduling method
        - Displays the scheduling method settings.
    - CoS - Tx Queue ID Conversion Table
        - Displays the Tx queue ID setting corresponding to the CoS value.
    - DSCP - Tx Queue ID Conversion Table
        - Displays the Tx queue ID setting 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 port
- Press the "Setting" button to access a page where you can change the settings of the selected LAN port
- If you press the "Specify all" button, the settings can be changed for all LAN ports whose check box contains a check mark
- If you press the "Return to defaults" button, the settings will be initialized for all LAN 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

Settings optimization page for web conferencing software

This page is for optimizing QoS settings for web conferencing software.
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.

Setting optimization for web conferencing software with change the following settings.
- QoS is enabled.
- The trust mode is set to DSCP for all ports.

- The following DSCP values used by Zoom Meetings are assigned to a high-priority Tx queue.
- The following DSCP values used by Microsoft Teams are assigned to a high-priority Tx queue.
- All other DSCP values are assigned to the lowest-priority Tx queue.

Setting optimization for web conferencing software

- Applicable software
  - Scheduling is set to Strict Priority for all Tx queues.

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.
- Scheduling method
  - Weighted Round Robin
    - Frames are transmitted based on the weight ratio for each queue.
    - Frames can also be transmitted from a lower-priority queue, within a specified percentage.
  - Strict Priority
    - The data with the highest priority in the transmission queue will be transmitted first.
    - When a frame is stored in a high-priority queue, it can never be transmitted from a lower-priority queue.
- CoS - Tx Queue ID Conversion Table
  - Sets the Tx queue ID corresponding to each CoS value.
  - The Tx queue ID setting range is 0 - 7, where the larger the ID setting value, the higher the priority for sending frames.
  - The "Easy Input" button allows the following settings to be entered at the same time in the CoS - Tx Queue ID Conversion Table.
    - Default Settings
      - These are the factory default settings.
- DSCP - Tx Queue ID Conversion Table
  - Sets the Tx queue ID corresponding to each DSCP value.
  - The Tx queue ID setting range is 0 - 7, where the larger the ID setting value, the higher the priority for sending frames.
  - When "Display only RFC compliant values" is checked, only RFC-compliant DSCP values will be displayed. However, all DSCP values will be displayed on the input confirmation screen.
  - The "Easy Input" button allows the following settings to be entered at the same time in the DSCP - Tx Queue ID Conversion Table.

        - Default Settings
            - These are the factory default settings.
        - Setting optimization for web conferencing software
            - This assigns the DSCP values used by the web conferencing software to the highest priority queue and the unused DSCP values to the lowest priority queue.
            - Select at least one web conferencing software.

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 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.
        - If remarking is enabled, the CoS value is remarked by the specified value, and the transmission queue is reassigned.
        - For details on checking and changing the "CoS - Transmission queue ID conversion table," refer to the command reference.
    - 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.
        - If remarking is enabled, the DSCP value is remarked by the specified value, and the transmission queue is reassigned.
        - For details on checking and changing the "DSCP - Transmission queue ID conversion table," refer to the command reference.
    - 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".

Trademark Attributions

- Zoom is a registered trademark or trademark of Zoom Video Communications, Inc. in the U.S.A. and other countries.
- Microsoft Teams is a registered trademark or trademark of Microsoft Corporation in the U.S.A. and other countries.

Flow control

Summary

In this page you can edit the settings of the flow control.

You can enable/disable the flow control.
If the flow control is enabled, frame discarding can be controlled when a network is congested.

Top page

This is the top page for flow control.

Flow control basic settings

- The current setting is shown as to whether the flow control is used.
- Press the "Setting" button to access a page where you can change the settings.

Flow control settings

- The flow control setting is shown for each LAN port.
- Press the "Setting" button to access a page where you can change the settings of the selected LAN port.
- If you press the "Specify all" button, the settings can be changed for all LAN ports whose check box contains a check mark.
- If you press the "Return to defaults" button, the settings will be initialized for all LAN ports whose check box contains a check mark.
    - The default flow control setting for all ports is "Disabled".
- If the settings do not use the flow control for the entire system, flow control settings for each LAN port cannot be made.

Flow control basic settings page

In this page you can specify whether the flow control is used for the entire system.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Flow control basic settings

- Flow control
    - Don’t use flow control
        - The flow control will be disabled for the entire system.
    - Use flow control
        - The flow control will be enabled for the entire system.

Flow control settings page

In this page you can specify whether the flow control is used for the selected interface.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Flow control settings

- Port
    - The LAN port for which settings are made is shown.

- Flow control
    - Disabled
        - The flow control will be disabled for the selected interface.
    - Enabled
        - The flow control will be enabled for the selected interface.

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 setting confirmation screen, press the "OK" button.

Storm control 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.
        - Disabled
        - Enabled
- 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.

Management

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

The time zone setting is shown.

- 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

- Unit name
  - Enter an arbitrary character string for use as the hostname.
  - Enter up to 63 single-byte alphanumeric characters or single-byte symbols.

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.
    - OFF mode
      - LED always stays off.

Time zone setting page

In this page you can set the 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)

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/date" box, enter the date in **YYYY/MM/DD** format.
    - When you move the focus to the box, a calender 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 calender 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
  - Periodic time synchronization is disabled by default.
- 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

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 settings.
- The table items are explained below.
    - Check box
        - Select the check box to delete user settings.
    - User name
        - Displays the user name.
    - Administrative privileges
        - Displays whether the user has been given administrative privileges.
- Press the "New" button to display the page where you can set up a new user.
- Press the "Setting" button to access a page where you can change the settings of the selected user.
- If you press the "Delete" button, all users whose check boxes are selected will be deleted.
- Settings can be made for up to 32 users.

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 setting confirmation screen, press the "OK" button.

Password settings

- Privileged password
    - Enter the administrative password that you want to set.
    - 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 setting confirmation screen, press the "OK" button.

User account settings

- User name
  - When configuring new settings
    - Specifies the user name to set.
    - Characters that can be inputted include single-byte alphanumeric characters.
    - Up to 32 characters can be inputted.
  - When changing settings
    - Shows the selected user name.
- New password
  - Enter the new password that you want to set.
  - 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
- Users 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
- TFTP server
- SNMP server

Web GUI access

- Displays the settings for the HTTP server.
- The table items are explained below.
    - Port number of HTTP server
        - Displays the port number of HTTP server.
    - 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.
    - Clients that can access the HTTP server
        - Displays the clients that can access the HTTP server.
    - Time until auto logout
        - Displays the time until auto logout.

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.
    - Clients that can access the Telnet server
        - Displays the clients that can access the Telnet server.

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.
    - Clients that can access the TFTP server

        - Displays the clients that can access the TFTP server.

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 settings 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 setting confirmation screen, press the "OK" button.

Web GUI access

- Port number of HTTP server
    - Specifies the port number of HTTP server.
    - 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.
- 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
    - Conditions are evaluated in ascending order of numbers.
    - If even one condition is specified, all access from clients that do not meet any condition will be denied.
    - Press the  icon to add a configuration form.
    - Press the "Delete" button to delete a configuration form.
- Time until auto logout
    - In the list box, select the time until auto logout.
    - If the desired time setting is not shown in the list box, select "Specify" and enter the desired time setting in the text box below the list box.
    - Any time setting within the range of 1 - 120 minutes may be entered.

Access via Telnet settings 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 setting 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.
- 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 TFTP settings 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 setting 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.

- Clients that can access the TFTP 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 SNMP settings page

Displays the settings for the SNMP server.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Access via SNMP

- Clients that can access the SNMP server
  - Select the client access restriction methods from the following options.
    - Permit all
    - Specify access conditions
  - When **Specify conditions** is selected, up to 32 conditions can be specified.
- Access condition
  - Specify condition for to restrict access from client.
  - Press the ▲ or ▼ icons to change the order in which the access conditions are applied.
  - Following points about SNMP server access condition differ from other type servers.
    - Access restriction behavior is always "Permit".
    - Community or user that apply condition can be selected.
  - The setting method for other item is the same as for the "Clients that can access the HTTP server" item on the Web GUI access page.

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 setting 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.
  - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding **?**.
  - Up to 64 characters can be inputted.
- Template status
  - Select template status from the following items.
    - Enabled
      - Enables the template
    - Disabled
      - Disables the template
- Contents of schedule execution
  - Specify the following items as the schedule execution contents.
    - Function to be executed
      - Select the function to be executed by schedule execution from the following items.
        - Shutdown
        - Cancel shutdown
        - Disable PoE power supply
        - Enable PoE power supply
        - Save settings
    - Applicable item
      - Select the applicable item of the function to be executed.
      - The choices available for the applicable item setting vary depending on the settings selected in the "Function to be executed" field.
  - "Execution cost" is the cost required for storing scheduled processes for execution inside the product and corresponds to the number of cli-command lines.
  - This product allows using an execution cost up to 100 for each template.
  - Specify settings so that the total "execution cost" is 100 or less.
  - Click the  icon to add a configuration form.
  - Click the “Delete” button to delete a configuration form.
  - Execution content specified or edited outside the schedule template settings screen is displayed in command format.

- If editing a template displayed in command format, enter the setting in console command format (abbreviated input is not accepted).
- You can enter multiple commands together by separating them with line-returns.
- Specify settings that result in 100 or fewer command lines.
- Schedule execution always starts with the specially-privileged EXEC mode (enable).
- The commands that can be set are as follows.
  - configure terminal
  - interface
  - shutdown
  - no shutdown
  - power-inline disable
  - power-inline enable
  - write
  - end
  - exit (Cannot be executed in "special privilege EXEC mode")
- For details on commands to enter, refer to the command reference and to the information provided on the Network device product information page and Network device technical information page.

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 setting 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.
- Execution timing
  - 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 "Hour:Minute:Second" 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 the 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 Network device technical information page.

- Template to be executed
    - Select the template to be executed in the 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 setting 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.
- 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 setting 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 **?**, **"**, and **¥**.
    - Up to 32 characters can be inputted.
- If there are settings related to the community (traps, access condition to SNMP server), also change those settings.
    - Check the check box and press the "OK" button to change the before change community name used in the following settings to the after change community name.
        - Trap destination settings
        - Access condition to SNMP server
    - This item will be displayed only when changing settings.
    - If you check the check box, the "Show details" button will be displayed on the confirmation page.
    - When the "Show details" button is pressed, a new window is opened and the following items are displayed.
        - Settings to be changed
            - A list of settings to which the change of community name will be applied is displayed.

        - Settings to be deleted
            - A list of settings which will be overwritten and deleted due to change community name is displayed.

- 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 SNMPv3 User settings.
Communication content is constantly authenticated and encrypted using HMAC-SHA-96 for the authentication algorithm and AES128-CFB for the encryption algorithm. These settings cannot be changed.
The authentication/encryption algorithms and password must match the settings specified for the corresponding SNMP manager.

Top page

This is the top page for SNMPv3 User.

User settings

- Information for the currently registered users are shown.
- The table items are explained below.
    - User name
        - Registered user name are shown.
    - Access mode
        - Access mode set to user are shown.
- If you press the "Setting" button, a page appears in which you can edit the settings of the selected user.
- If you press the "Return to defaults" button, the settings will be initialized on all users whose check boxes are selected.
- One ReadWrite user and one ReadOnly user can be registered.

User setting page

In this page you can register new users or change settings for users that are already registered.
Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

User settings

- Access mode
    - Displays the access mode of the user for which settings will be made.
        - ReadOnly
            - Only permitted to read in MIB views.
        - ReadWrite
            - Permitted to either read or write in MIB views.
    - Both ReadOnly users and ReadWrite users can access all MIB views.
- User name
    - Sets the user name.
    - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding **?**, **¥**, **"**.
    - Up to 32 characters can be inputted.
- Authentication password
    - Sets the authentication password.

    - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding **?**, **¥**, ".
    - Within 8 to 32 characters can be inputted.
- Encryption password
    - Sets the encryption password.
    - Characters that can be inputted include single-byte alphanumeric characters and symbols, excluding **?**, **¥**, ".
    - Within 8 to 32 characters can be inputted.

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.
- 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 setting 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 FAN status
            - Send traps when FAN state is changed for example when FAN abnormally detected.
        - Change Temperature status
            - Send traps when Temperature state is changed for example when temperature abnormally detected.
        - Change PoE status
            - Send traps when PoE state is changed.
        - Detect/Resolve loop
            - Send traps when PoE state is changed.

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 setting 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 thte message type cannot be selected.
- The Trap message type is always used for version SNMPv1.

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.
- 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.
- 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.

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
¥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 corresponding  button to sort the list.
  - With default settings, results are sorted in ascending order of the receiving port.
  - Pressing  again switches 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 Network device technical information page.

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 LLDP auto-configuration function.
  - To use LLDP auto-configuration, the connected device must support LLDP auto configuration. To confirm supported models, check the "LLDP Auto-Configuration" page in the unit’s technical documentation.
  - The LLDP auto-configuration function includes the following features.
    - Dante optimization setting
      - When certain Dante-enabled Yamaha device is connected to the unit, optimal settings for using Dante is automatically applied.
    - Notification before power is shut off
      - If the PoE power supply is scheduled to be shut off at a port connected to a Yamaha wireless AP device, notification of the shut-off timing is sent in advance and the Yamaha wireless AP device is prepared to have the power shut off.

Interface settings page

In this page you can make settings for the LLDP.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

Interface settings

- Port
  - Displays the name of the interface for which settings will be made.
- 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
- 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.
- 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 100.

L2MS settings

Summary

This page is for changing the L2MS settings.

L2MS (Layer2 Management Service) is a function for managing Yamaha network devices at the layer 2 level. These settings can be used to enable/disable L2MS units or specify frame input permission settings using L2MS filters.

Top page

This is the top page for the L2MS settings.

L2MS settings

- The current settings of the L2MS are show.
- Press the "Setting" button to access a page where you can change the settings.

L2MS filter settings

- The current settings for the L2MS filter 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.
    - Rejection of L2MS frame
        - Displays the filter setting for blocking L2MS frames.
    - Rejection of Non-L2MS frame
        - Displays the filter settings for blocking non-L2MS frames.
- 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 L2MS filter 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.
        - Rejection of L2MS frame : Disabled
        - Rejection of Non-L2MS frame : Disabled

L2MS settings page

In this page you can enable/disable L2MS.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

L2MS settings

- L2MS
    - Enabled

        - L2MS will be enabled.
        - This device functions as an L2MS agent and can be controlled by the L2MS manager.
    - Disabled
        - L2MS will be disabled.
        - L2MS frames can be transmitted in the same manner as non-L2MS frames, but cannot be controlled by the L2MS manager.

L2MS filter settings page

This page is for L2MS filter settings.

Enter the settings, and then press the "Confirm" button.
If there are no mistakes in the setting confirmation screen, press the "OK" button.

L2MS filter settings

- Port
    - Displays the name of the interface for which settings will be made.
- Rejection of L2MS frame
    - Select the operation for the filter for blocking L2MS frames from the following options.
        - Disabled
        - Enabled
- Rejection of Non-L2MS frame
    - Select the operation for the filter for blocking non-L2MS frames from the following options.
        - Disabled
        - Enabled
- If both filters are enabled, all frames are rejected at the interface.
- Be aware that it will no longer be possible to access the GUI form a port where the non-L2MS filter is enabled.

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 "Execute" 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.
  - You can enter multiple commands together by separating them with line-returns.
  - You can enter up to 300 lines.
  - 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 Network device technical information page.
  - The following commands cannot be entered.
    - ping
    - ping6
    - do
    - reload
    - cold start
    - firmware-update execute
    - erase startup-config
    - show startup-config
    - show tech-support
    - quit
    - disable
    - logout
    - exit (When in special privilege EXEC mode)
- 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)

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 the network. Various settings for updating the firmware via the network are displayed.

Current firmware revision

- The currently-used firmware revision is shown.

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.

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.

Note that the unit will automatically restart when the firmware has been updated successfully.

Update firmware from PC

- Specify update file
    - Selects the firmware file used for the update

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 webserver.

Note that the unit will automatically restart when the firmware has been updated successfully.

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.

Firmware update basic 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.

Firmware update basic settings

- Download source URL
  - This is the setting of the URL at which the firmware is located.
- HTTP proxy server
  - FQDN or IP address
    - Specify a proxy server FQDN or IP address that is no more than 255 single-byte alphanumeric or symbol characters long.
  - Port number
    - Specifies the port number of the proxy server.
    - Input a port number from 1 to 65535.
- HTTPS proxy server
  - FQDN or IP address
    - Specify a proxy server FQDN or IP address that is no more than 255 single-byte alphanumeric or symbol characters long.
  - Port number
    - Specifies the port number of the proxy server.
    - Input a port number from 1 to 65535.
- 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 files.

This unit operates in accordance with its CONFIG file (settings data). A CONFIG file consists of a combination of multiple commands.

Top page

This is the top page for CONFIG file management.

Here you can start the process of importing a CONFIG file from the PC, or the process of exporting a CONFIG file to the PC.

Import CONFIG file

- Press the "Next" button to begin the process of importing a CONFIG file from the PC.

Export CONFIG file

- Press the "Next" button to begin the process of exporting a CONFIG file to the PC.

Import CONFIG file page

In this page, a CONFIG file from the PC can be copied to internal non-volatile memory, updating the CONFIG file.

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 file is the same as the import-destination CONFIG file, the unit restarts automatically after the import has ended successfully.

Import CONFIG file

- Currently-used CONFIG file
  - The currently used CONFIG file is shown.
- File to import
  - Press the "Select a file" button to display the file selection dialog box.
- Import-destination file
  - Select the import-destination CONFIG file in internal non-volatile memory.

Export CONFIG file page

In this page you can copy a CONFIG file from internal non-volatile memory to the PC.

When you have finished entry, check the entered content and press the "OK" button.

Export CONFIG file

- Currently-used CONFIG file
  - The currently used CONFIG file is shown.
- File to export
  - Select the CONFIG file in internal non-volatile memory that you want to export.

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 type 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.

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
  - DEBUG
    - This setting specifies whether DEBUG type SYSLOG is output.
  - INFO
    - This setting specifies whether INFO type SYSLOG is output.
  - ERROR
    - This setting specifies whether ERROR type SYSLOG is output.
- SYSLOG transmission
  - Header
    - This is the header setting when outputting the SYSLOG to an external host.
    - You can specify whether or not to include the time stamp and device name in the header of the SYSLOG message.
  - 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.

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.

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.

Initialization

- Privileged password
    - To return the unit to its factory-set state, enter the privileged password.

Cable diagnostics

Summary

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

Cable diagnostics page

In this page you can diagnose cables. To diagnose a cable, select the port and press the "Execute" button. Press the "Clear" button to clear the diagnostic results shown.

Cable diagnostics

- Port
  - Port diagnosed is displayed.
- Result
  - The status of the cable connected to the LAN port is displayed.
    - OK : The cable is electrically connected.
    - Open : Either a device is not connected on the opposite end or the cable is faulty.
    - Short : A short-circuit occurred.
- Distance to cable fault
  - If "Open" or "Short" is indicated in results, then the distance from the LAN port to the cable fault is displayed in meters.
- Estimated cable length
  - If "OK" is indicated in results, then the estimated cable length is displayed in meters.
  - Estimated cable length is undetermined when the opposite port is linking up at a link speed of less than 1G or shutdown.

Published 03/2025
YJ-A0