



Router RTX1300

User guide

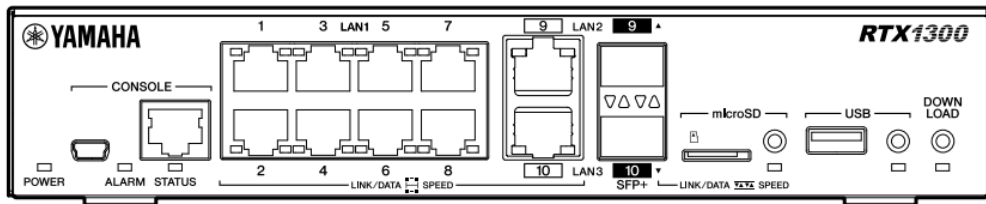


Table of Contents

| | |
|---|----|
| 1. Introduction | 4 |
| 1.1. Accessory | 4 |
| 1.2. Sold separately | 4 |
| 1.3. Notation in this Guide | 5 |
| 1.4. Manual Guide | 6 |
| 1.5. Important Notice | 7 |
| 2. Product Overview | 9 |
| 2.1. Main Feature | 9 |
| 2.2. Main Features..... | 11 |
| 2.3. Names and functions of each part | 14 |
| 3. Steps for use | 22 |
| 4. Install this product | 23 |
| 4.1. Installing the unit horizontally..... | 23 |
| 4.2. Wall Mounting | 24 |
| 4.3. Installed in a 19-inch rack..... | 27 |
| 5. Connecting peripheral devices to this product | 29 |
| 5.1. Connect the power cord | 29 |
| 5.2. Connecting network devices and computers | 30 |
| 5.3. Connecting a USB-connected data communication terminal | 31 |
| 5.4. Connecting the Console Terminal | 31 |
| 5.5. Installing SFP+/SFP Modules | 32 |
| 5.6. Remove the SFP+/SFP module..... | 33 |
| 5.7. Attaching the Direct Attach Cable | 34 |
| 5.8. Remove the direct attach cable | 35 |
| 6. Starting and Stopping the Product..... | 36 |
| 6.1. Startup Step | 36 |
| 6.2. Stop Step | 41 |
| 7. Using the Web GUI..... | 42 |
| 7.1. Login Step | 42 |
| 8. Using the Console | 45 |
| 8.1. How to Log In | 45 |
| 8.2. Login Step | 48 |
| 8.3. Selecting the character set to display | 51 |
| 8.4. Access Level | 51 |
| 8.5. How to use the console | 52 |
| 8.6. Command input assistance function | 53 |
| 8.7. List of commands that can be entered | 54 |
| 9. Setting up the product | 55 |
| 9.1. Setting up user accounts..... | 55 |
| 9.2. Setting the Admin Password..... | 58 |
| 9.3. Setting operation flow | 59 |
| 9.4. Specific Settings | 65 |
| 9.5. Checking Connectivity..... | 66 |
| 9.6. Restoring settings to factory defaults | 67 |
| 10. Manage this product..... | 69 |
| 10.1. System Management Tasks | 69 |
| 10.2. Managing configuration files | 70 |
| 10.3. Firmware revision up | 72 |

| | |
|--|----|
| 10.4. Console Security Settings | 77 |
| 10.5. Settings for management via SNMP | 80 |
| 10.6. Status display | 81 |
| 10.7. Using external memory | 82 |
| 10.8. 85 Operations to Remember..... | 85 |
| 10.9. When the ALARM indicator lights up | 87 |
| 10.10. Checking the communication status with the STATUS indicator | 89 |
| 10.11. Using the EEE Function | 89 |
| 11. Appendix | 90 |
| 11.1. Customer Support (Support Policy) | 90 |
| 11.2. Introduction to Open Source Software | 90 |

1. Introduction

This chapter describes the necessary information for using this product. It also explains what you need to know to read this guide.

1.1. Accessories

This product includes the following accessories:

- Please read first (including warranty card): 1 sheet
- AC100-240V power cord: 1
- Power cord pull-out prevention bracket: 1 piece.
- Rubber feet: 4 pieces
- Dust covers (factory installed on SFP+ slots): 2

NOTICE

The following cables are not included: Please check the respective standards and prepare them separately.

- This cable connects to the RJ-45 CONSOLE port. Please use our optional YRC-RJ45C or an RJ-45/DB-9 console cable of the same standard as the YRC-RJ45C.
- USB cable
This cable connects to the mini-USB CONSOLE port. Use a cable with a USB Type-A connector and a mini-USB Type B (5-pin) connector.

1.2. Sold Separately.

The following items are available separately (optional).

- RJ-45/DB-9 console cable: YRC-RJ45C
This cable connects to the RJ-45 CONSOLE port. Used to log in to the console of this product.
- SFP+ module: YSFP-10G-SR/YSFP-10G-LR
Used to connect fiber optic cables compatible with 10GBASE-SR/10GBASE-LR. For instructions on installing the SFP+ module into the SFP+ slot, see "5.5, "Installing an SFP+/SFP Module".
Please refer to the SFP+ module's instruction manual and use a compatible fiber optic cable.
- SFP module: YSFP-G-SXA/YSFP-G-LXA
Used to connect optical fiber cables compatible with 1000BASE-SX/1000BASE-LX. For instructions on installing the SFP+ module into the SFP+ slot, see "5.5, "Installing an SFP+/SFP Module".
Please refer to the SFP module's instruction manual and use a compatible fiber optic cable.
- Direct attach cable: YDAC-10G-3M, YDAC-10G-1M
Used when directly connecting SFP+ slots of Yamaha products. Although the distance is limited, it is possible to build a 10 Gigabit Ethernet environment at a low cost. For instructions on installing the cable into the SFP+ slot, see "5.7, "Installing a Direct Attach Cable".
- Rack mount kit: YMO-RACK1U
Used when installing this product in a 19-inch rack (1U size). For installation instructions, see "4.3, "Installing in a 19-inch Rack."
- Wall mount kit: YWK-1200D
This is used when installing this product on a wall. For installation instructions, see "4.2, "Installing on a Wall."

NOTICE

Please visit the following website for the latest information and details on optional items.

<https://network.yamaha.com/products/options/>

1.3. Notation in this Guide

1.3.1. About Abbreviations

In this guide, company names and product names are abbreviated as follows:

- Yamaha Router RTX1300: This product
- Microsoft® Windows®: Windows

1.3.2. Trademarks

- The company names and product names mentioned in this guide are either registered trademarks or trademarks of their respective companies.
- This product is equipped with RSA® BSAFETM software from RSA Security Inc. RC4 and BSAFE are registered trademarks of RSA Security Inc. in the United States and other countries.



1.3.3. Definition of Notation

This guide uses the following notations to ensure safe use of this product.

- **WARNING:** This indicates that there is a possibility of death or severe injury.
- **CAUTION:** This suggests that there is a possibility of injury.
- **ATTENTION:** These are the precautions you must observe to prevent product failure, damage, malfunction, and data loss.
- **IMPORTANT:** This is information you must be aware of to operate the product correctly.
- **NOTICE:** Information related to operation and management. Please read for reference.

1.3.4. About the Description Format in the Text

To facilitate understanding, the following rules will be used in the text:

| Contents | rule | example |
|---|---|----------------------------|
| Notes in the text | Emphasis with underline | Cut off communication |
| Command | Lowercase Bold | show config Command |
| Keyboard keys | Enclose in brackets [] | [Enter] key |
| Pressing multiple keys at the same time | List the keys to be pressed simultaneously and connect them with "+." | [Ctrl] + [X] |

1.3.5. About the Contents of this Guide

- Reproduction of any part or all the contents of this guide without permission is prohibited.
- The contents of this guide and the specifications of the central unit are subject to change without notice for improvement purposes.
- This guide does not provide detailed information about the Internet or networks. For details, please refer to commercially available instruction manuals.
- In this guide, we use the following IP addresses, which are reserved for documentation purposes by RFC6890, when giving examples of global IP addresses.

- IP Address Range: 203.0.113.0/24

This IP address cannot be used for communication. When setting it up, please use the one that suits your environment.

1.4. Manual Information

To ensure that you fully utilize the functions of this product, we have prepared the following manuals. Please read the appropriate manual according to your purpose.

- Initial instruction (Included with this product)
This describes the precautions to take when using this product. Please be sure to read and follow the precautions before use.
- User Guide (this guide, website)
This is a manual for those who manage this product and the network to which it is connected. It explains how to install, configure, and manage this product.
We will explain it comprehensively. Please be sure to read and follow the precautions before use.
- Web GUI Operation Manual (Website)
This section provides detailed instructions on how to use the Web GUI. This manual includes information on how to use this product, including basic settings and operation management.
- Command Reference (Website)
This explains the command format and provides examples of how to configure this product.

NOTICE

The latest versions of the above manuals are posted on the following website. Please use your browser's translation feature to check. (The page is in Japanese.)

<http://www.rtpro.yamaha.co.jp/RT/manual.html>

1.5. Important Notices

1.5.1. Warranty Coverage for this Product

We assume no responsibility for any losses, such as loss of information, resulting from using this product. The warranty is limited to the physical damage of this product. Please note.

1.5.2. Security Measures and the Firewall Function of this Product

The Internet is very convenient as it allows you to gather information from all over the world on websites and exchange messages via email. On the other hand, your computer will be at risk of unauthorized access from anywhere in the world. If you are constantly connected to the Internet or have a public server, you must understand the risk of unauthorized access and take security measures. This product has a firewall function for security purposes; however, new methods of unauthorized access and loopholes (security holes) are being discovered day and night, and there is no perfect way to prevent unauthorized access and security holes. Please understand that there are risks involved in connecting to the Internet, and you should always stay up to date with the latest information and take security measures at your own risk.

1.5.3. Regarding Communication Charges

You may need to disable automatic dialing if you use this product with a pay-per-use line service (such as a mobile phone network).

Please be sure to understand the functions before using them.

When the product is connected to a PC or LAN, it monitors the data sent by PC software (email software, web browser, etc.) and the destinations of data transmitted over the LAN.

If there is a destination other than the LAN, the call will be automatically made to the line according to the pre-set contents.

Therefore, if there is a mistake in the settings or you forget to disconnect the line, the software or device may send packets periodically, which may result in unexpected communication charges or provider connection charges.

Please check your communication records regularly to make sure there are no unintended calls. In addition, please regularly visit the Yamaha network equipment website (<https://network.yamaha.com/>) to obtain the latest information on product settings and revision updates. Please use your browser's translation feature to check. (The page is in Japanese.)

You may be charged unexpected communication fees in the following cases:

- When you first start using this product
- When changing the provider connection settings of this product
- When you install new software on your computer
- When you connect a new computer, network device, or peripheral device to the network
- When the product firmware is updated
- Other cases, such as when you perform an unusual operation or notice a difference in the response of communication.

ATTENTION

- If you cancel or change your provider contract, be sure to delete or reconfigure the connection settings of this product.
If you continue to use the connection settings without deleting them, you may receive unintended messages from your carrier or provider.
You may be charged a fee.
- Depending on the provider's conditions (change of access point, maintenance, failure, etc.)
This may result in unexpected communication charges.
Always pay attention to notifications from your provider.

1.5.4. About Fee Information and Cumulative Connection time

Management

When using this product connected to a pay-as-you-go line service (mobile phone network), you can set outgoing call restrictions based on the accumulated charges based on billing information and/or the accumulated connection time.

These functions are based on the fee information provided through pay-as-you-go line services (mobile phone network) and the cumulative connection time calculated by this product, so they cannot accommodate different fee calculation methods due to service discounts, etc., or provider-specific communication time calculation methods.

In actual operation, outgoing call restriction may not function as intended.

If you want to ensure accuracy, please conduct a trial run for a certain period of time to check for any discrepancies.

2. Product Overview

This chapter describes this product's main features and functions, as well as the names and functions of each part of the central unit.

2.1. Main Features

This product is a 10 Gigabit access VPN router for businesses.

By combining it with 10G optical fiber lines, 10 gigabit/multi-gigabit switches, and Wi-Fi 6 compatible wireless LAN access points, you can create a high-speed network environment on both the WAN and LAN sides.

In addition, depending on your current network environment, replacing your router with this product can improve communication speeds.

In addition to the various functions included in the conventional RTX series, it is equipped with a "Flexible LAN/WAN port" function that allows for more flexible LAN construction.

2.1.1. Supports a Variety of Networks

Mobile communication support

To use the mobile Internet connection, you can connect a data communication device compatible with the mobile phone network to the USB port.

Supports IPsec, L2TP, and PPTP

Supports IPsec, L2TP, and PPTP. Virtual private network over the Internet (VPN) to send and receive data more securely.

Flexible LAN/WAN port function

By freely assigning physical ports to LAN interfaces, the previously fixed physical port configuration of LAN interfaces can be flexibly changed. Ports assigned to the same interface function as a switching hub and the link aggregation function can be used to set up a redundant configuration, allowing for flexible support of various LAN environments.

2.1.2. High Network Performance

Supports 10 gigabit lines

Equipped with two ports that support 10 Gigabit Ethernet. Each port is configured with a combo port of an RJ-45 port and an SFP+ slot, so you can select the optimal port to use according to the LAN interface of the connected device.

High Throughput

High-performance CPU, hardware VPN accelerator, and "Fast Pass" for high-speed packet transfer. The "Scan" function ensures high throughput.

2.1.3. Reduce Management Cost

Easy setup

By using the Web GUI's "Easy Setup," you can configure the basic settings of the router using a web browser on your computer, even if you do not know Yamaha router commands.

For information on how to use the Web GUI, see "7. Using the Web GUI."

External memory support

By connecting a microSDHC card or USB memory to the microSD slot or USB port, respectively, The following operations are available for convenient management tasks.

- Operation using firmware and configuration files stored on external memory
- Backing up configuration files to external memory
- Saving logs etc. to external memory

For information about external memory that can be used with this product, refer to "Read Me First" (included with this product or on the website).

For information on using external memory with this product, see section 10.7, "Using External Memory".

Equipped with a mini-USB console port

In addition to the existing RJ-45 console port, a new mini-USB console port is now installed. Even if your computer does not have an RS-232C terminal (COM port), you can use the console to configure it without having to prepare a separate USB-serial conversion cable.

A wealth of technical information

The Yamaha Network Peripheral Device Technical Information page provides detailed information on how to use this product and troubleshooting.

For more advanced technical information, see the

<http://www.rtpro.yamaha.co.jp/>

Please use your browser's translation feature to check.(The page is in Japanese.)

2.1.4. Environmental Considerations

RoHS Compliance

Lead, mercury, cadmium, hexavalent chromium, PBB (polybrominated biphenyls), PBDE (polybrominated diphenyl ethers)

It complies with the European RoHS Directive, which restricts the use of phthalate (Dibutyl Phthalate), DEHP (Bis(2-ethylhexyl) Phthalate), DBP (Dibutyl Phthalate), BBP (Butyl Benzyl Phthalate), and DIBP (Isobutyl Phthalate).

Supports EEE (Energy Efficient Ethernet)

It supports EEE (Energy Efficient Ethernet), which enables power saving in Ethernet communication. For details about the EEE function, see "10.11, "Using the EEE Function."

2.2. Key Features

It inherits the proven functions of Yamaha routers and further enhances them.

2.2.1. Router Function

routing

Routing of IPv4 and IPv6 packets. The following routing protocols are supported:

| Packet Type | Routing Protocols |
|-------------|-----------------------|
| IPv4 | RIP, RIP2, OSPF, BGP4 |
| IPv6 | RIPng, OSPFv3 |

Filter-based routing

The destination of the packet is determined by the IP address, protocol, and port number. You can connect to multiple providers at the same time.

NAT/IP Masquerading

You can use NAT and IP masquerading to convert addresses.

- NAT:
It converts global addresses and private addresses in one-to-one correspondence.
- IP Masquerading:
Multiple private addresses are associated with one global address and converted.

VPN Connection

You can connect bases together via an Internet VPN. The following protocols are supported:

- IPsec (AES, 3DES, DES)
- L2TP
- PPTP

IPv6 connection function

IPv6 Internet connection via IPv6 PPPoE or IPv6 IPoE, IPv4 Internet connection using IPv6 IPoE (IPv4 over IPv6 MAP-E method/DS-Lite method) is supported.

PPPoE client function

You can use the PPPoE client function, which is necessary when using broadband access lines such as FTTH or ADSL lines.

Line backup function

If a problem occurs when using the Internet VPN, line backup can be achieved in a variety of configurations, such as using the mobile phone network as a backup line.

2.2.2. Security Features

Packet Filter

Static and dynamic filters are available.

- Static filters:
Packets are controlled based on source and destination IP addresses, port numbers, and protocols.
- Dynamic Filters:
It controls the flow of IP packets on a per-session basis.

Filtering by MAC address is also possible.

Illegal access detection (IDS) function

It detects malicious packets intended for intrusion or attack, as well as P2P software. Detected unauthorized packets can be discarded and bandwidth can be restricted.

Device authentication function

Using the DHCP-based device authentication function, you can set the access range for each device on the network. You can prohibit network connections from devices other than those with specific MAC addresses, or limit the networks that a device can connect to.

URL Filters

It is equipped with an internal database reference type URL filter function. Accessible URLs are restricted by referencing the database configured in this product.

2.2.3. QoS (Quality of Service) Function

The following basic QoS functions are included, as well as Yamaha's unique adaptive QoS function.

| QoS type | QoS Features |
|------------------------------|--|
| Basic QoS | Priority control, bandwidth control |
| Yamaha's unique adaptive QoS | Dynamic Traffic Control, Dynamic Class Control, Bandwidth Detection Function, Load Notification Function |

2.2.4. Convenient Functions for Operation and Management

Ability to store multiple firmware and configuration files

- The product's non-volatile memory can store multiple firmware and configuration files.
Start this product
You can select the desired firmware and configuration file when you run the software.
For details, see 6.1.2, "Selecting the Firmware and Configuration File to Use and Starting Up".
- The configuration file history is also saved. This is useful when you want to return to the original settings. For details, see Chapter 10.2, "Managing Configuration Files".
- Start the product using firmware and configuration files stored on a micro SDHC card or USB memory
can. This is useful when you want to temporarily try out a setting.
See section 6.1.3, "Booting from Firmware and Configuration Files on an External Memory" for details.

Dashboard

You can check various information such as CPU and memory usage, traffic volume, and VPN connection status on the dashboard on the Web GUI.

Power off log save function

When the POWER switch is set to STANDBY, the log is automatically saved to the non-volatile memory of this product. The log will not disappear even after the power is turned off, so you can check the log before the power was turned off after restarting the product.

Firmware update process/settings file save process fail-safe

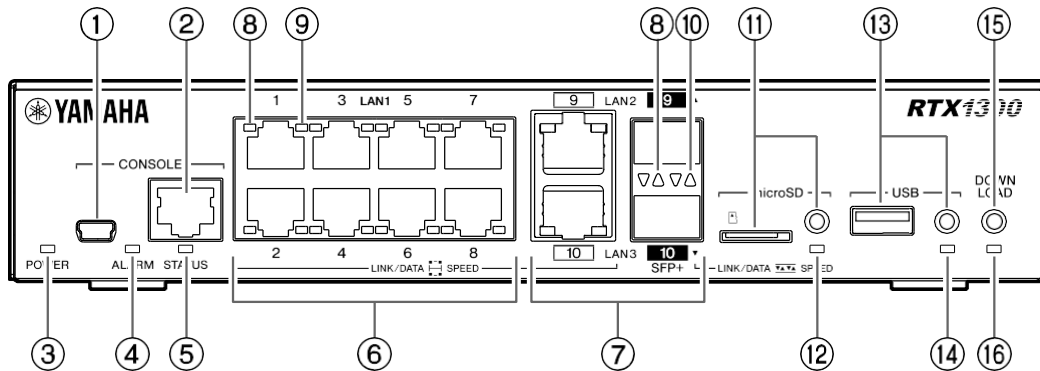
If the power cord is unplugged or a power outage occurs while updating the firmware/settings files in the non-volatile memory of this product and the update process does not end successfully, the firmware/settings files will be reverted to the ones before the update. This prevents situations such as the loss of firmware causing the system to be unable to boot, or the loss of configuration files causing the system to malfunction.

2.3. Names and Functions of each part

This section explains the names and functions of each part of the main unit.

- [2.3.1, "Front"](#)
- [2.3.2, "Rear"](#)
- [2.3.3, "Bottom"](#)
- [2.3.4, "Product Labeling"](#)
- [2.3.5, "Top/Side"](#)

2.3.1. Front



① mini-USB CONSOLE port

Mini-USB port for settings. Connect to the USB port on your computer using a USB cable. Use a USB cable with a USB Type A connector and a mini-USB Type B (5-pin) connector.

② RJ-45 CONSOLE port

RJ-45 port for configuration. Connect to the PC's RS-232C terminal (COM port) using an RJ-45/DB-9 console cable.

③ POWER indicator

Indicates the power status of the product.

| POWER indicator | situation |
|-----------------|--|
| Lights out | The power is off. |
| Green light | It's working. |
| Blinking green | During startup immediately after turning on the POWER switch. Or, the unit is shutting down immediately after the POWER switch is set to STANDBY. |

④ ALARM indicator

This section provides information about faults in this product.

| ALARM indicator | situation |
|-----------------|--|
| Lights out | Operating normally. |
| Red light | One of the following conditions: <ul style="list-style-type: none"> - The hardware protection function was activated due to an increase in the internal temperature of this product. - An abnormal fan stop was detected. - Temperature sensor abnormality detected |

For details, see "10.9, "When the ALARM indicator lights up."

⑤ STATUS indicator

Indicates the backup status of the line.

| STATUS indicator | situation |
|------------------|---|
| Lights out | The main line is ready for communication. |
| Orange light | The main line is not communicating. |

For details, see "10.10, 'Checking the Communication Status with the STATUS Indicator'."

⑥ LAN port

This port supports 10BASE-T, 100BASE-TX, and 1000BASE-T.

In the factory default state, ports 1 to 8 are assigned to the LAN1 interface.

⑦ LAN/SFP+ combo port

You can use either the LAN port or the SFP+ slot.

In the factory default state, port 9 is assigned to the LAN2 interface and port 10 is assigned to the LAN3 interface.

- LAN Port

This port supports 100BASE-TX, 1000BASE-T, 2.5GBASE-T, 5GBASE-T, and 10GBASE-T.

- SFP+ slots

This slot supports 1000BASE-SX, 1000BASE-LX, 10GBASE-SR, and 10GBASE-LR. SFP+/SFP It can be used by attaching a module (sold separately) or direct attach cable (sold separately).

For installation instructions, see Chapter 5.5, "Installing SFP+/SFP Modules" or Chapter 5.7, "Installing Direct Attach Cables".

ATTENTION

The LAN port and SFP+ slot are for exclusive use. LAN ports with the same port number

Do not use both the and SFP+ slots at the same time. It may cause malfunction.

NOTICE

In this guide, the terms "SFP+ slot" and "SFP+ port" are used to mean the following:

- What is "SFP+Slot"?

An interface for connecting SFP+/SFP modules and direct attach cables

- What is "SFP+ port"?

SFP+/SFP module installed, ready to connect optical fiber cable

⑧ LINK/DATA indicator

Indicates the status of the LAN port or SFP+ slot.

| LINK/DATA indicator Tar | situation |
|----------------------------|-------------------------------|
| Lights out | Link is lost (unavailable). |
| Green light | Link established (available). |
| Blinking green | Transferring data. |

ATTENTION

If all LINK/DATA indicators are flashing green and the ALARM indicator is lit red, the hardware protection function may have been activated. For details, see "10.9, "When the ALARM indicator lights up."

⑨ SPEED indicator (LAN port)

Indicates the connection speed of the LAN port.

| SPEED indicator (LAN port) | situation |
|-------------------------------|--|
| Lights out | Not connected. Or it is connected via 10BASE-T or 100BASE-TX. |
| Orange light | Connected via 1000BASE-T. |
| Green light | The connection is via 2.5GBASE-T, 5GBASE-T, or 10GBASE-T. |

ATTENTION

If all SPEED indicators are flashing green and the ALARM indicator is lit red, the hardware protection function may have been activated. More information
For details, see "10.9, "When the ALARM indicator lights up."

⑩ SPEED indicator (SFP+ slot)

Indicates the connection speed of the SFP+ slot.

| SPEED indicator (SFP+ slot) | situation |
|--------------------------------|--|
| Lights out | Not connected. |
| Orange light | The connection is via either 1000BASE-SX or 1000BASE-LX. |
| Green light | The connection is via either 10GBASE-SR or 10GBASE-LR. Or, connect using a direct attach cable. |

ATTENTION

If all SPEED indicators are flashing green and the ALARM indicator is lit red, the hardware protection function may have been activated. More information
For details, see "10.9, "When the ALARM indicator lights up."

⑪ microSD slot and button

This is the slot for inserting a micro SDHC card.

When removing the micro SDHC card, press and hold the microSD button for 2 seconds or more until the microSD indicator

Please turn off the light before removing it.

ATTENTION

Insert the microSDHC card horizontally from the front of the unit. If you insert the microSDHC card at an angle, it may become stuck.

⑫ microSD indicator

Indicates the connection and usage status of the microSDHC card.

| microSD indicator | situation |
|-------------------|---|
| Lights out | No micro SDHC card is inserted in the slot. Or the micro SDHC card can be removed. |
| Green light | A micro SDHC card is plugged in. |
| Blinking green | Accessing the micro SDHC card. |

⑬ USB port and button

This is a port for inserting a USB memory stick or a data communication terminal compatible with mobile phone networks.

When removing the USB device, press and hold the USB button for 2 seconds or more until the USB indicator goes out, then

Please remove it.

⑭ USB indicator

Indicates the connection and usage status of the USB device.

| USB indicator | situation |
|----------------|---|
| Lights out | No USB device is inserted in the port. Or the USB device can be removed. |
| Green light | A USB device is connected. |
| Blinking green | Accessing a USB device. |

⑮ DOWNLOAD button

Press this button for 3 seconds or more to update the firmware.

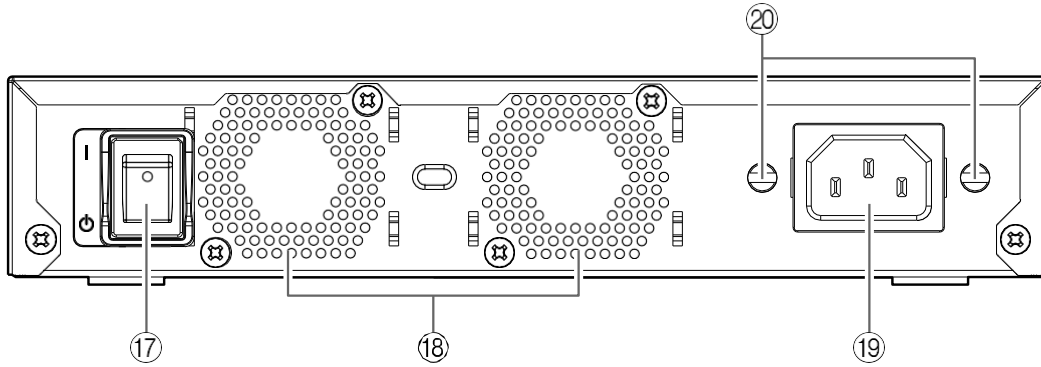
By default, this feature is disabled.

⑯ DOWNLOAD indicator

Indicates the firmware download status.

| DOWNLOAD indicator Tar | situation |
|---------------------------|--|
| Lights out | No firmware download has been performed. |
| Blinking green | Firmware downloading. |

2.3.2. back



17 POWER Switch

Turns the product on/off.

| POWER switch | explanation |
|--------------|--|
| I (ON) | When starting up the product, connect the power cord to the product and then turn the POWER switch ON. |
| ⏻ (STANDBY) | When shutting down the product, set the POWER switch to STANDBY. After the product has performed shutdown procedures such as saving log files, it will automatically turn off. |

For details on how to start and stop this product, please see "6. Starting and Stopping this Product."

NOTICE

If a problem occurs, such as the CONSOLE port not being recognized, The problem may be resolved by turning the power to STANDBY, then turning it ON again to start up the product.

18 Ventilation holes

The heat generated inside is forcibly expelled by a fan.

WARNING

Do not block the ventilation holes or place objects around them. This may cause a fire or malfunction.

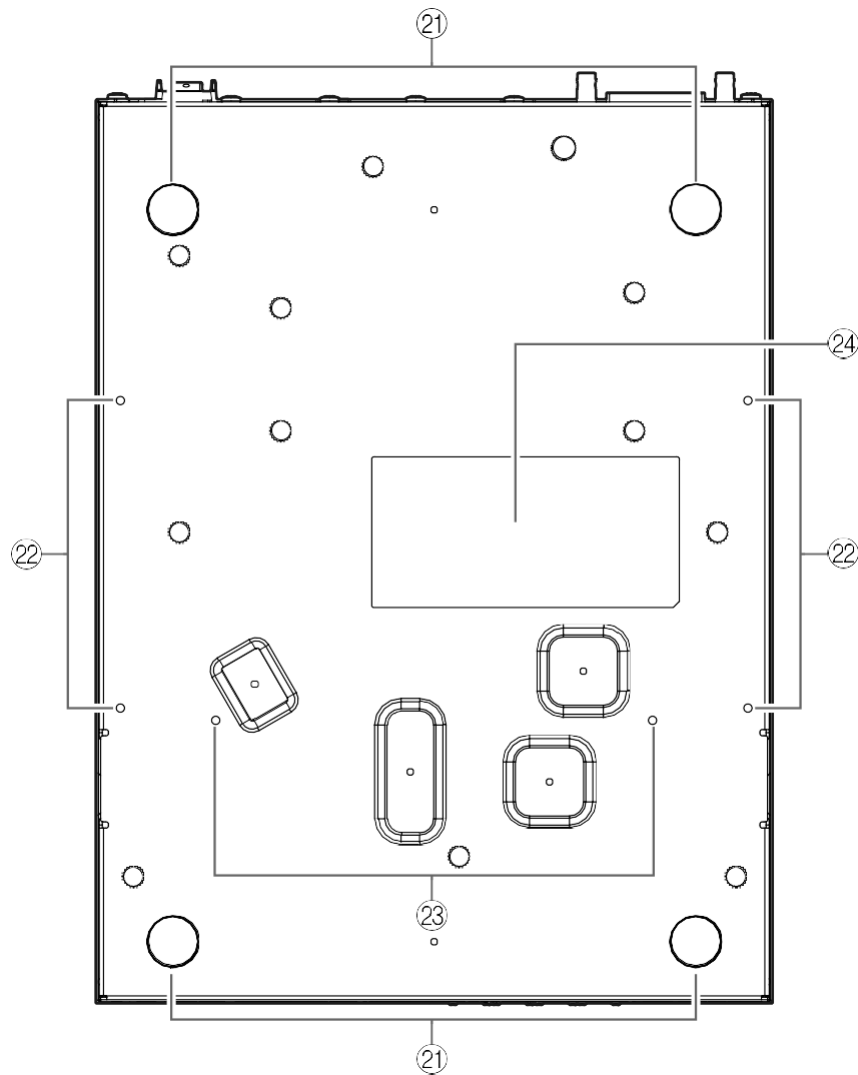
19 Power inlet (3-pole connector, C14 type)

Plug in the included power cord. Connect the power plug to an AC 220 V, 50 Hz power outlet.

20 Power cord prevention bracket mounting hole

Attach the included power cord prevention bracket (U-shaped). For installation instructions, see 5.1, "Connecting the Power Cord."

2.3.3. Bottom



① Rubber foot attachment position

Attach the supplied rubber feet.

ATTENTION

Whether or not the rubber feet are attached depends on how you install this product. For details, please see "Installing this product".

② Wall mount kit mounting holes

Attach the wall mount kit YWK-1200D (option). For installation instructions, see "4.2, Installing on a Wall."

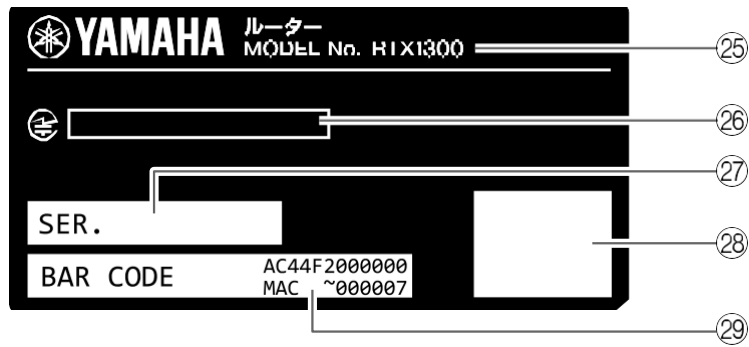
③ Rack mount kit installation holes

Attach the rack mount kit YMO-RACK1U (option). For installation instructions, see "4.3, Installing in a 19-inch Rack."

④ Product label

This contains information such as the product's device name, serial number, MAC address, and the Device ID required when using Yamaha Network Organizer (YNO). For more information, see Chapter 2.3.4, "Product Labels".

2.3.4. Product Label



②⑤ Device name

②⑥ Certification number

②⑦ Serial number

This section contains the serial number used to manage and classify the product.

②⑧ Device ID

This section contains the ID required when using Yamaha Network Organizer (YNO).

②⑨ MAC address

This section lists the range of MAC addresses that this product possesses.

For example, in this diagram, the following MAC addresses are set for each LAN interface.

- MAC address of LAN1 interface: "AC:44:F2:00:00:00"
- MAC address of LAN2 interface: "AC:44:F2:00:00:01"
- MAC address of LAN3 interface: "AC:44:F2:00:00:02"
- MAC address of LAN4 interface: "AC:44:F2:00:00:03"
- :
- MAC address of LAN8 interface: "AC:44:F2:00:00:07"

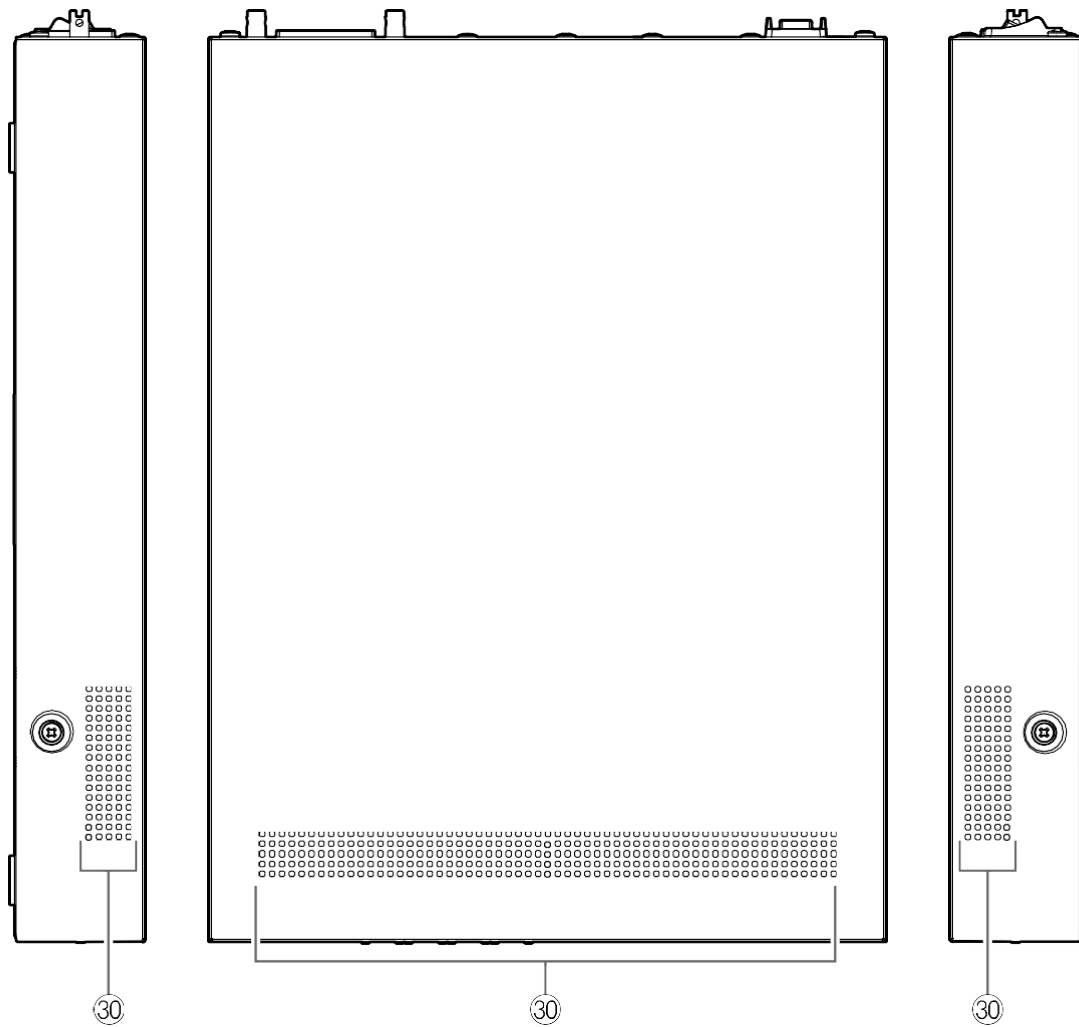
NOTICE

The LAN4 interface to LAN8 interface can be used by configuring the flexible LAN/WAN port function. Please see the following URL for instructions on how to set it up.

<http://www.rtpro.yamaha.co.jp/RT/docs/flexible-lan/index.html>

The page is in Japanese. Please use your browser's translation feature to check.

2.3.5. Top/Side



30 Ventilation holes

A fan draws in outside air to cool the interior.

WARNING

Do not block the ventilation holes or place objects around them. This may cause a fire or malfunction.

3. Steps for use

To use this product, please install and configure it according to the following procedure.

| Overview of the process | Link to reference page |
|---|---|
| 1. Place the product in a suitable location. | 4. Install this Product |
| 2. Connect the necessary cables, terminals, etc. | 5. Connect Peripheral Devices to this Product |
| 3. Start the product. | 6. Turn on and Turn off this Product |
| 4. Open the settings screen of this product. | Please see the page that corresponds to the operation method. <ul style="list-style-type: none"> • 7. Use the Web GUI 8. Using the console |
| 5. Configure this product according to your usage conditions. | 9. Set up this Product |
| 6. Manage the Product as needed. | 10. Manage this Product |

NOTICE

- See "2. Product Overview" for an overview of this product's main features and functions.
- For the hardware specifications and warranty provisions of this product, please refer to "Read Me First" (included with this product or on our website).

4. Install this Product

This chapter explains the following three installation methods.

- [4.1, "Installation in a horizontal position"](#)
- [4.2, "Installation on a wall"](#)
- [4.3, "Installing in a 19-inch rack"](#)

WARNING

When installing this product, be sure to follow the "Safety Precautions" in "Read First" (included with this product or on the website).

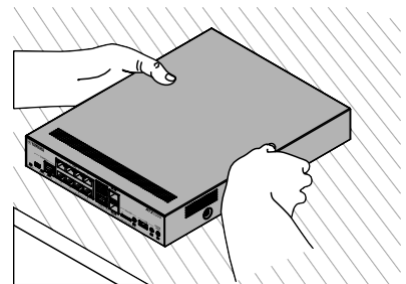
ATTENTION

When selecting a location to install this product, make sure that it meets the following conditions:

- Adequate ventilation, temperature and humidity
- There is enough space for the power cord and LAN cable.
- The location must be such that the product can be easily serviced and maintained.

4.1. Installation the unit Horizontally

With the four rubber feet attached to the bottom of the product, place it on a desk or other level surface.



CAUTION

- **When installing this product horizontally, be sure to attach the rubber feet.**
It may fall and cause injury or damage to the equipment
- **Do not stack this product with other devices.**
This may cause injury or damage to the equipment due to it falling. It can also cause heat to build up and lead to breakdowns.

4.2. Installation on a Wall

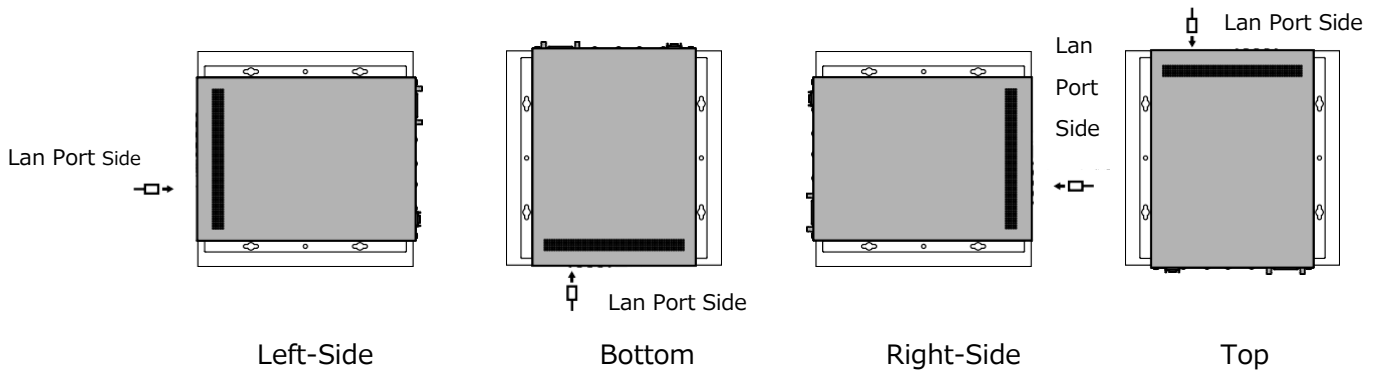
Use the wall mount kit YWK-1200D (sold separately) to install on a wall.

ATTENTION

- Install this product in a location that can adequately withstand its weight.
- Do not install in a location subject to continuous vibration.

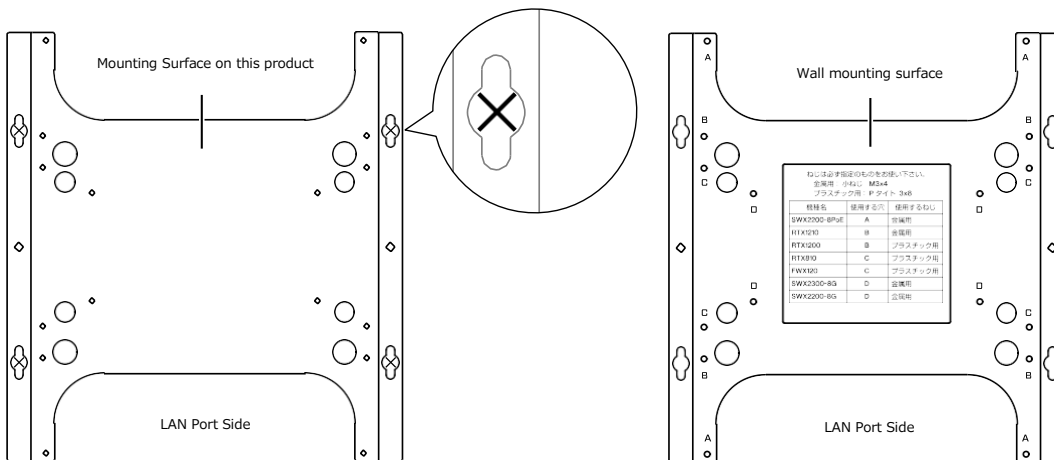
Installation Pattern

When installing this product on a wall, there are four possible installation patterns.

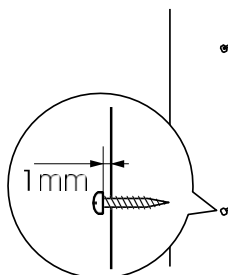


Installation Procedure

1. Place the mounting bracket on the wall and mark the installation position.



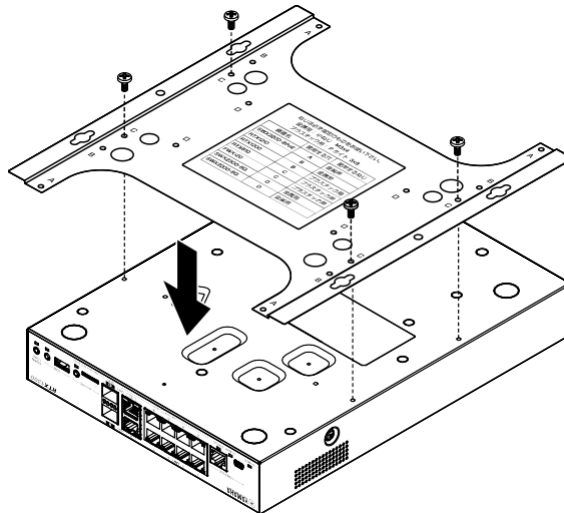
2. Temporarily fasten the four commercially available screws at the positions marked in step 1. Be sure to leave 1 mm of space between the wall and the screw head for the mounting hardware to hook over.



Note

- Always use screws that are compatible with the wall material.
- This may cause injury or damage to the equipment due to it falling.

3. If there are four rubber feet attached to the bottom of the product, remove them.
4. Attach the mounting bracket to this product.
Align the mounting bracket's screw hole "C" with the wall mount kit mounting hole on the bottom of this product.



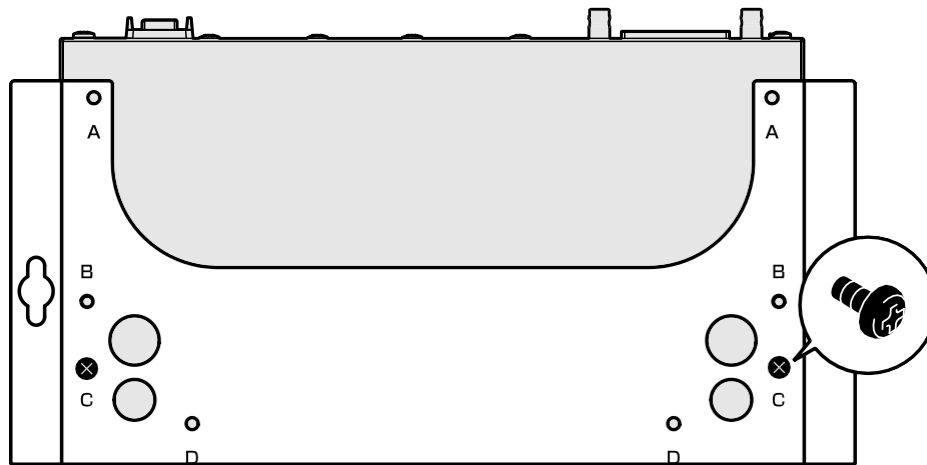
Caveat

- Always unplug the product from the outlet before carrying out this procedure.
- This may cause electric shock or malfunction.

please note

- Attach the mounting bracket with the label facing outwards. It cannot be installed upside down.

5. Attach the mounting bracket to this product using the four screws included in the wall mount kit.
 - Screw hole to be used: "C"
 - Screws to use: For metal housing (black small M3 x 4)



caveat

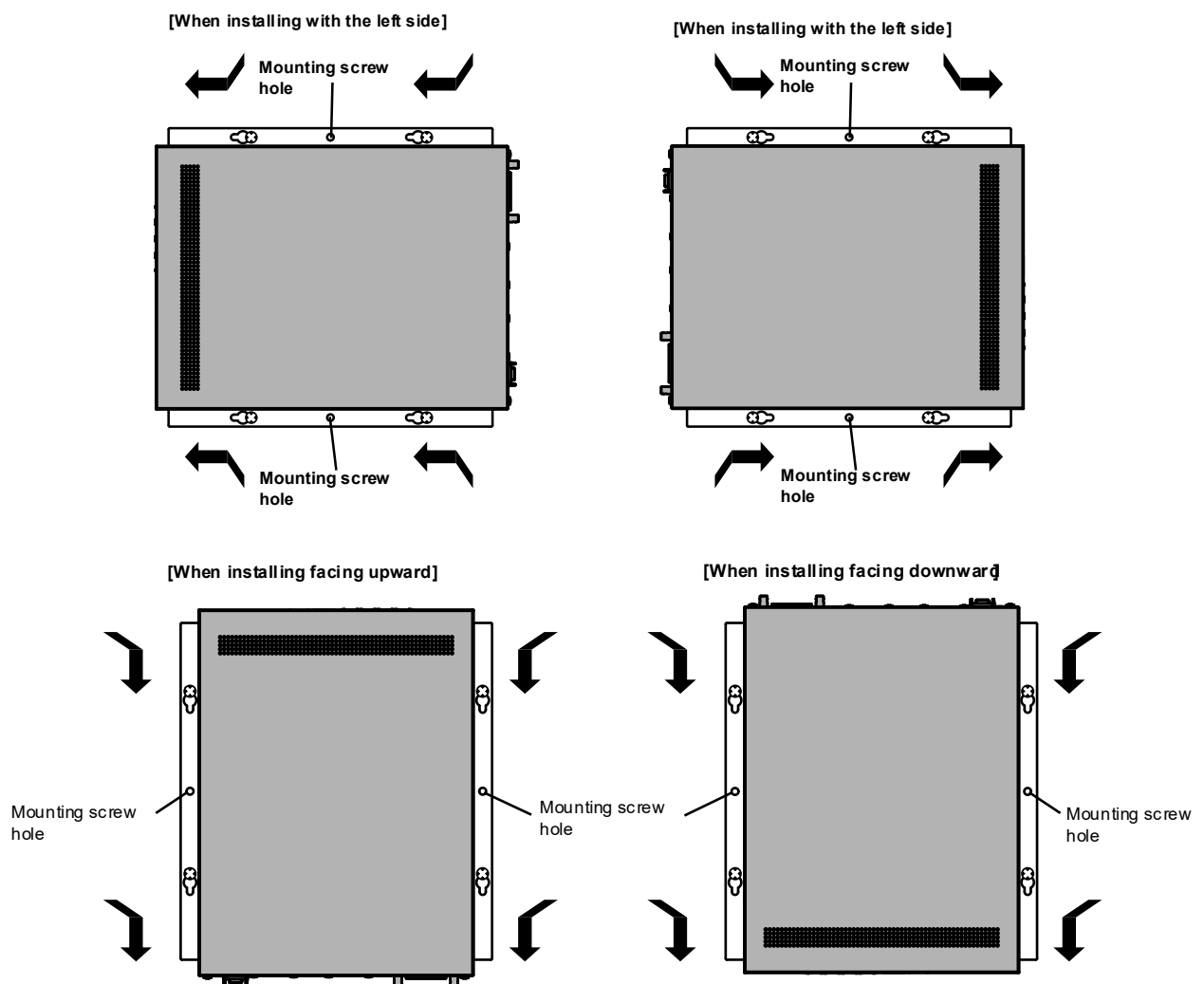
- Always use the specified screws provided with the wall mount kit.

This may cause injury or damage to the equipment due to it falling. It may also cause electric shock or malfunction.

Note

- **Do not drop this product.**
This may cause injury or damage to equipment.
- **Be careful when placing your hands or fingers on the corners of the mounting brackets.**
This can cause injury.

6. Hook the assembled mounting bracket onto the commercially available screws that you temporarily fastened to the wall in step 2 and slide it over.



Note

- **Do not drop this product.**
This may cause injury or damage to equipment.
- **Be careful when placing your hands or fingers on the corners of the mounting brackets.**
This can cause injury.

7. Tighten the commercially available screws that you temporarily fastened to the wall to secure the mounting bracket in place.
8. Attach commercially available screws to the fixing screw holes (2 places) of the mounting bracket.

Note

- Always use screws that are compatible with the wall material.
- This may cause injury or damage to the equipment due to it falling.

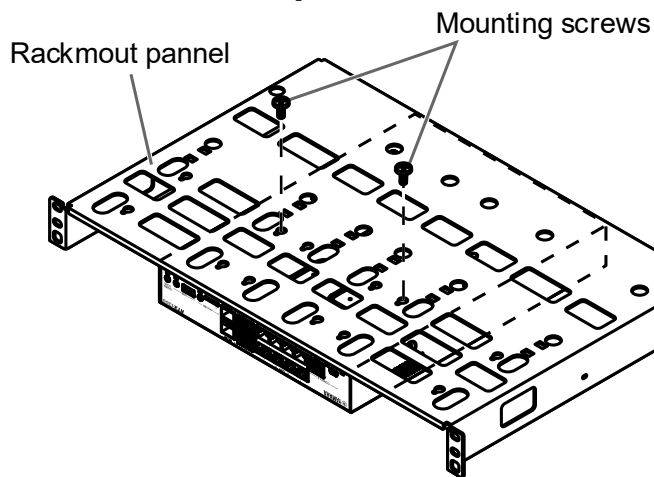
4.3. Installation in a 19-inch rack

Use the rack mount kit YMO-RACK1U (sold separately) to install the unit in an EIA or JIS standard 19-inch rack.

caveat

- Always unplug the product from the outlet before carrying out this procedure.
 - This may cause electric shock or malfunction.
1. If there are four rubber feet attached to the bottom of the product, remove them.
 2. Attach the rack mount panel to this product.
Use the two mounting screws included with the rack mount kit to secure the product to the rack mount kit mounting holes on the bottom of the product.

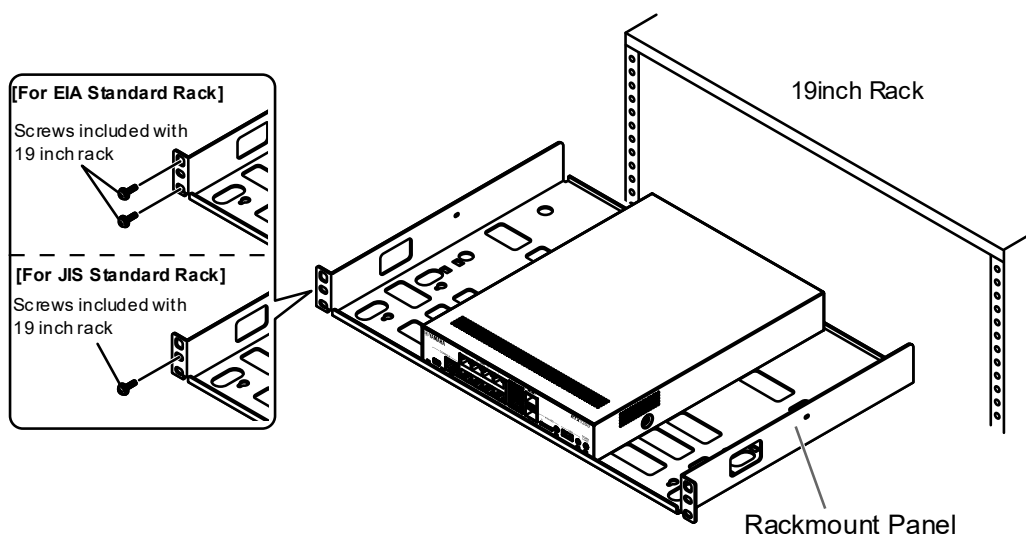
[Viewed from the bottom]



WARNING

- **Be sure to use the specified screws provided with the rack mount kit.**
This may cause injury or damage to the equipment due to it falling. It may also cause electric shock or malfunction.
- **Do not pass cables or cords, such as power cords, through holes in the rack mount panel.**
This may cause fire, electric shock, or malfunction.

3. Attach the rack mount panel to a 19-inch rack.
Install the unit in a 19-inch rack using the included mounting screws (four screws for an EIA standard rack, two screws for a JIS standard rack).



WARNING

- Do not damage cables or cords such as power cords.
- This may cause fire, electric shock, or malfunction.

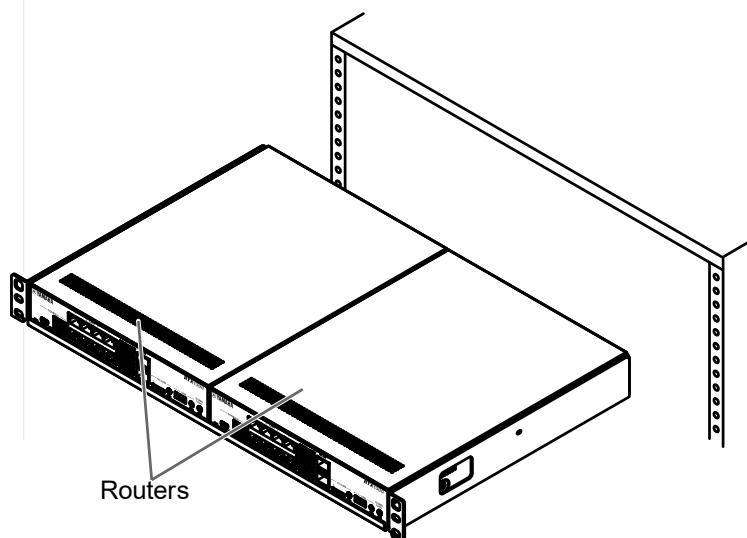
CAUTION

Do not stack this product with other devices.

This may cause injury or damage to the equipment due to it falling. It can also cause heat to build up and lead to breakdowns.

NOTICE

You can also install two of these products side by side.



5. Connecting Peripherals to this Product

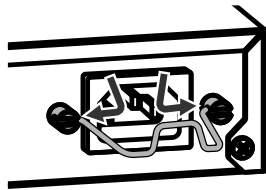
This chapter describes the following connection methods:

- 5.1, "Connect the power cord"
- 5.2, "Connecting network devices and computers"
- 5.3, "Connecting a USB-connectable data communication terminal" (when connecting to a mobile phone network)
- 5.4, "Connecting the Console Terminal"
- 5.5, "Installing SFP+/SFP Modules"
- 5.6, "Removing SFP+/SFP Modules"
- 5.7, "Installing a Direct Attach Cable"
- 5.8, "Removing the Direct Attach Cable"

5.1. Connect the Power Cord

Connect the power inlet of this product to a power outlet using the included power cord.

1. Set the POWER switch of this product to STANDBY.
2. Insert the included power cord prevention bracket into the power cord prevention bracket mounting hole on this product.

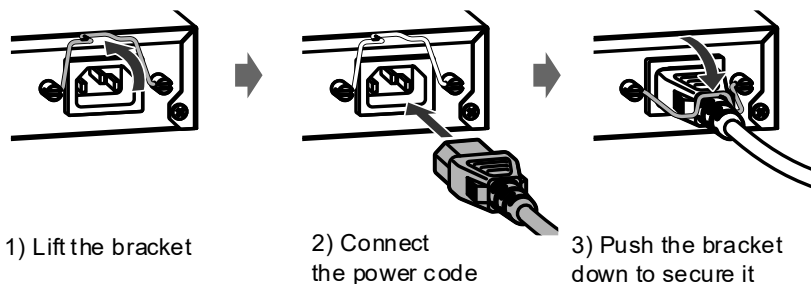


Insert the included bracket into the hole on the main unit from the inside.

CAUTION

The included power cord prevention bracket is designed specifically for use with the included power cord. If you use a power cord other than the one provided, the cord may be damaged or may not be secured properly.

3. Connect the included power cord to this product and secure it in place with the power cord prevention bracket.



4. Connect the earth cord to the earth terminal of the outlet.

ATTENTION

Always connect the earth cord to the earth terminal of the outlet. For gas pipes, etc. Never connect it.

5. Insert the power plug into the outlet.

5.2. Connecting Network Devices and Computers

Connect network devices and computers to the LAN interface of this product.

- [5.2.1, "Connecting to a LAN port"](#)
- [5.2.2, "Connecting to an SFP+ Slot"](#)

ATTENTION

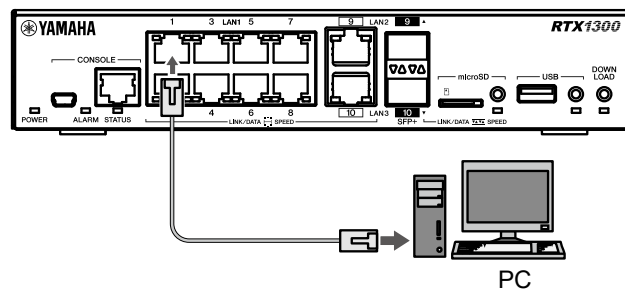
The LAN port and SFP+ slot is for exclusive use. Do not use both the LAN port and the SFP+ slot with the same port number at the same time. It may cause malfunction.

NOTICE

Any of this product's LAN interfaces can also be used to connect to a WAN line.

5.2.1. When Connecting to a LAN Port

Connect the LAN port of the network device or PC to the LAN port of this product with a LAN cable.



ATTENTION

Connecting them incorrectly can result in damage or malfunction of the hardware. Please check carefully before connecting.

Refer to the table below and use a LAN cable that is suitable for the link speed and wiring conditions of each LAN port.

| Link Speed | Maximum Transmission Rate | LAN cable standards | Maximum Transmission Distance |
|------------|---------------------------|-----------------------|-------------------------------|
| 10BASE-T | 10Mbps | Category 3 and above | 100 m |
| 100BASE-TX | 100Mbps | Category 5 or higher | |
| 1000BASE-T | 1 Gbps | Category 5e and above | |
| 2.5GBASE-T | 2.5Gbps | | |
| 5GBASE-T | 5 Gbps | | |
| 10GBASE-T | 10 Gbps | Category 6 | 55 m |
| | | Category 6A | 100 m |

notice

- The maximum transmission distance is a theoretical value, and the actual transmission distance varies depending on the usage environment.
- This product is equipped with an automatic straight/cross LAN port detection function, so you can use either a straight cable or a cross cable.
You can also disable the automatic straight/cross detection function.

5.2.2. When Connecting to an SFP+ slot

Connect in one of the following ways:

- Install an SFP+/SFP module in the SFP+ slot of this product and connect it with a fiber optic cable. For instructions on how to install SFP+/SFP modules, see 5.5, "Installing SFP+/SFP Modules".
- Connect the SFP+ slot of this product directly to the SFP+ slot of the connected device using a direct attach cable.
For instructions on installing a direct attach cable, see 5.7, "Installing a Direct Attach Cable".

5.3. Connecting a USB Data Communication Device

Connect a USB-connected data communications device to the USB port of this product. For information on USB-connectable data communication devices that have been confirmed to work, please visit the following website.

<http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/index.html#cellphones>

The page is in Japanese. Please use your browser's translation feature to check.

CAUTION

Please insert the data communication terminal directly into the USB port of this product. If you connect via a USB extension cable, it may not function properly depending on the type of USB extension cable.
This may not be the case.

5.4. Connecting the Console Terminal

Connect a PC to the CONSOLE port of this product and use it as a console terminal.

This product has two types of CONSOLE ports: Each requires a different cable.

| CONSOLE PORT | cable |
|-----------------------|---|
| mini-USB CONSOLE port | A USB cable with a USB Type A connector and a mini-USB Type B (5-pin) connector |
| RJ-45 CONSOLE PORT | RJ-45/DB-9 console cable |

For details on how to connect and pre-configure your computer, see "8.1.1, "Logging in from a Computer Connected to the CONSOLE Port".

5.5. Installation of SFP+/SFP Modules

Install an SFP+/SFP module (sold separately) into the SFP+ slot of this product.

CAUTION

When installing an SFP+/SFP module, do not look into the light source.

SFP+/SFP modules are Class 1 laser devices. There is a risk of invisible laser radiation being emitted. If the laser light enters the eyes, it may cause visual impairment.

ATTENTION

The LAN port and SFP+ slot are for exclusive use. Do not use both the LAN port and the SFP+ slot with the same port number at the same time. It may cause malfunction.

NOTICE

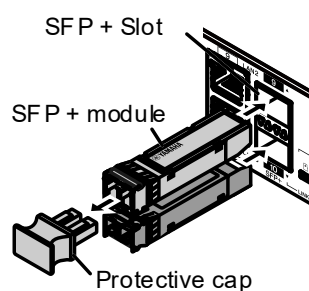
- Please refer to the instruction manual included with each SFP+/SFP module for installation procedures and precautions.
- This product supports hot swapping, so you can install SFP+/SFP modules without turning off the power.

1. Remove the dust cover from the SFP+ slot of the product and insert the SFP+/SFP module.

CAUTION

Be sure to store the removed dust cover in a safe place so as not to lose it.

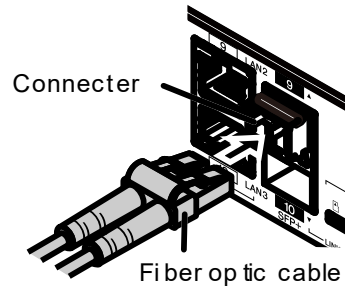
2. Remove the protective cap from the SFP+/SFP module.



CAUTION

Be sure to store the removed protective cap in a safe place so as not to lose it.

3. Connect the optical fiber cable for each module to the SFP+ port (SFP+/SFP module connector)



5.6. Remove the SFP+/SFP module

Remove the SFP+/SFP module installed in the SFP+ slot of the product.

ATTENTION

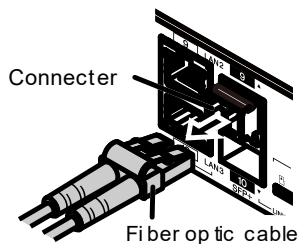
When removing an SFP+/SFP module, do not look into the light source.

SFP+/SFP modules are Class 1 laser devices. There is a risk of invisible laser radiation being emitted. If the laser light enters the eyes, it may cause visual impairment.

NOTICE

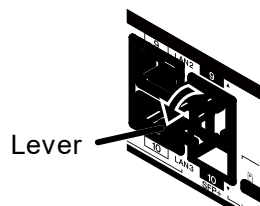
- Please also see:
- This product supports hot swapping, so you can remove the SFP+/SFP module without turning off the power.

1. Remove the fiber optic cable from the SFP+ port (SFP+/SFP module connector).

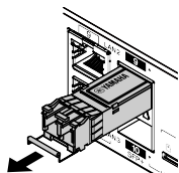


2. If you have connected an SFP+/SFP module to the top SFP+ slot, lower the lever of the SFP+/SFP module.

If you are connecting to a lower SFP+ slot, raise the lever.



3. Hold the lever and pull out the SFP+ /SFP module.



4. Protect your SFP+ slots with dust covers and your SFP+ /SFP modules with protective caps.

CAUTION

If left unprotected, foreign objects may get in and cause a malfunction.

5.7. Attaching the Direct Attach Cable

Attach a direct attach cable (sold separately) to the SFP+ slot of this product.

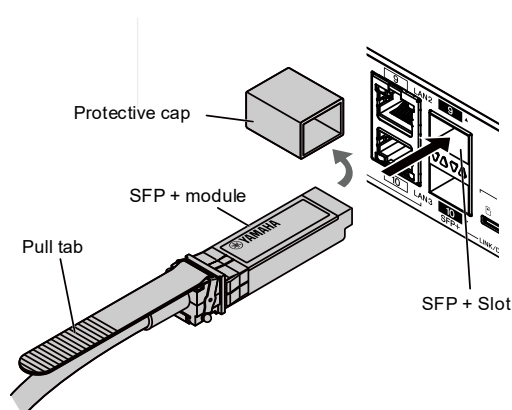
CAUTION

- The LAN port and SFP+ slot are for exclusive use. LAN ports with the same port number
- Do not use both the and SFP+ slots at the same time. It may cause malfunction.

NOTICE

- Please also refer to the instruction manual included with each direct attach cable for installation instructions and precautions.
- This product supports hot swapping, so you can install direct attach cables without having to turn off the power.

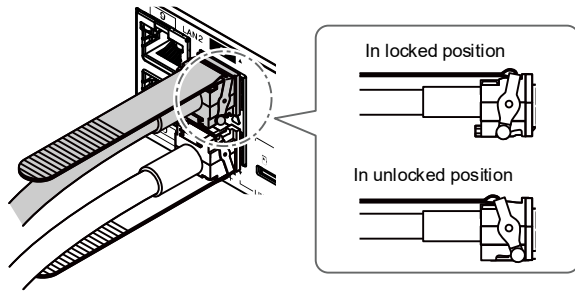
1. Remove the dust cover from the SFP+ slot of the router and the protective cap from the direct attach cable.



CAUTION

Be sure to store the removed dust covers and protective caps in a safe place so as not to lose them.

2. Hold the body of the direct attach cable and insert it firmly into the SFP+ slot on the product.



5.8. Remove the Direct Attach Cable

Remove the direct attach cable from the SFP+ slot of the router

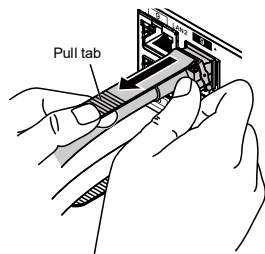
CAUTION

The direct attach cable can be difficult to remove, so refer to the steps below to remove it correctly. Forcing it out may cause damage to the product or the direct attach cable.

NOTICE

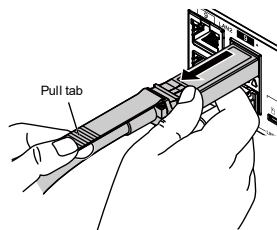
- Please also refer to the instruction manual included with each direct attach cable for removal instructions and precautions.
- This product supports hot swapping, so you can remove the direct attach cable without turning off the power.

1. While holding the part of the direct attach cable equivalent to the SFP+ module towards the back with one hand, use the other hand to pull the pull-out tag towards you to release the lock.



2. Once the lock is released, pull the pull tab and remove the SFP+ module from the direct attach cable.

Slowly pull out the appropriate portion.



3. Protect the SFP+ slots with dust covers and direct attach cables with protective caps.

CAUTION

If left unprotected, foreign objects may get in and cause a malfunction.

6. Turn on and Turn off this Product

This chapter describes how to start and stop this product.

6.1. Startup Procedure

This guide will introduce the following three startup procedures.

- [6.1.1, "Booting with the default firmware and configuration file" \(basic boot procedure\)](#)
- [6.1.2, "Selecting the firmware and configuration file to be used and starting"](#)
- [6.1.3, "Booting with Firmware and Configuration Files from External Memory"](#)

6.1.1. Boot with the Default Firmware and Configuration Files

This is the basic startup procedure. The product boots using the default firmware and configuration files stored in the product's non-volatile memory.

1. Make sure that the POWER switch of this product is set to STANDBY.
2. Verify micro SDHC card or USB memory is not inserted in the microSD slot or USB port of this product.
3. Turn on the POWER switch of this product.
 - The POWER indicator on this product will flash green.
 - After 10 seconds, the product will begin the boot process by loading the default firmware and configuration files.
 - Once the startup process is complete, the POWER indicator will turn green.

6.1.2. Select the Firmware and Configuration Files to be used and Start

If multiple firmware files or multiple configuration files are stored in the non-volatile memory of the product, you can select which firmware and configuration file to use when booting the product. For example, if a problem occurs with this product, you can boot it up with an older revision of the firmware or a configuration file from before the problem occurred. Operation is performed by opening the console screen of this product on a computer connected to the CONSOLE port.

NOTICE

- For the sake of explanation, multiple firmware and configuration files are saved here.
- We will post the console screen when this is done.

1. Make sure that the POWER switch of this product is set to STANDBY.
2. Verify micro SDHC card or USB memory is not inserted in the microSD slot or USB port this product.
3. Connect the computer to the CONSOLE port of this product.
4. Start the console screen of your computer.

5. Turn on the POWER switch of this product.

- The POWER indicator on this product will flash green.
- The product startup message will be displayed on the computer console screen, followed by a 10-second countdown.

```
RTX1300 BootROM Ver. 1.00
  Copyright (c) 2022 Yamaha Corporation. All Rights Reserved.

Press 'Enter' or 'Return' to select a firmware and a configuration.
Default settings: exec0 and config0

Will start automatically in: 10
```

6. Before the 10-second countdown ends, press the Enter key on your computer's console screen.

- A prompt to enter the firmware number will be displayed on the PC console screen.

NOTICE

If 10 seconds pass without pressing the [Enter] key, the product will start up by loading the default firmware and configuration files.

7. Enter the firmware number to be used ("0" or "1").

```
No.  Revision
-----
*0   Rev. 23.00.00
  1   Rev. 23.00.01
-----
Select the firmware [0 or 1]:1
```

8. Press the Enter key.

- A prompt for entering the configuration file number will be displayed on the computer's console screen.

9. Enter the number of the configuration file to be used.

```
No.  Date      Time      Time      No.  Date
-----
* 0   2022/06/17 18:42:36  422 703/703 ospf testing
  0.1 2022/06/17 08:18:06  328 704/704 test
  0.2 2022/06/15 17:17:39  294 705/705
  12022/06/16 11:59:18  292 702/702 BGP+VRRP fix
-----
Select the configuration
[Number in upper list, or '-' (hyphen) to go back] :1
```

- To specify a saved configuration file, enter the configuration file number displayed on the console screen.
(In this example, enter "0", "0.1", "0.2", or "1").

- To create a new configuration file, enter a configuration file number that is not displayed on the console screen (in this example, "2," "3," or "4").

NOTICE

To reselect the firmware, enter "-" (hyphen) and press [Enter]
You can return to step 7 by pressing the

10. Press the Enter key.

- The product will begin the boot process using the selected firmware and configuration files. POWER
The indicator will start flashing green.
- Once the boot process is complete, the POWER indicator will turn solid green.

NOTICE

After logging in to the product, follow the steps below to install the product with the specified firmware and configuration file.

You can check if it's working.

- Checking via the Web GUI:
Check the display of the "System Information" gadget on the Dashboard Live screen.
For example, if you specify "0" as the firmware number and "1" as the configuration file number, the following will be displayed:
 - Running firmware: exec0
 - Running configuration file: config1
- To check on the console:

Run the show environment command.

For example, if you specify "0" as the firmware number and "1" as the configuration file number, the following will be displayed:

```
> show environment
:
Firmware: exec0 Config. file: config0
:
```

6.1.3. Booting using Firmware and Configuration Files from External Memory

You can start up the product using firmware and configuration files stored on an external memory. This is useful when trying out new firmware or configuration files temporarily.

Preparing the external memory

1. Prepare an external memory (micro SDHC card or USB memory) formatted in FAT or FAT32 format.
2. Save the firmware and configuration files you want to use to the external memory. If this product is in its factory default state, name the firmware file "rtx1300.bin" and the configuration file "config.txt".

NOTICE

- We recommend saving each file directly under the root directory. (When starting this product, multiple files with the same name may exist in the external memory. If present, the file closest to the root directory will be selected.)
- The file names can be changed using the external-memory exec filename command and the external-memory config filename command.

Startup procedure

1. Make sure that the POWER switch of this product is set to STANDBY.
2. Insert the external memory containing the firmware or configuration files you want to use into the microSD slot or USB port of this product.

NOTICE

If no firmware or configuration files are stored in external memory, the product will start up using the firmware and configuration files stored in the product's non-volatile memory.

3. Turn on the POWER switch of this product.
 - The POWER indicator on this product will flash green. After 10 seconds, the product will begin the boot process by loading the default firmware and configuration files.
 - The POWER indicator will change from flashing to lit.
 - When the product recognizes the external memory, the microSD indicator or USB indicator will light up.
 - The product will search for firmware and configuration files on the external memories. The microSD indicator or USB indicator will flash.
 - If firmware or configuration files are found on the external memory, they will be extracted to the product's operating memory. Once the boot process is complete, the three indicators microSD, USB and DOWNLOAD will flash three times.

NOTICE

After logging in to the product, you can check whether the product is operating with the firmware and configuration files loaded from external memory by following the procedure below.

- Checking via the Web GUI:
Check the display of the "System Information" gadget on the Dashboard Live screen.
For example, if you are using firmware and configuration files loaded from a micro SDHC card, you will see something like this:
 - Running firmware: sd1:/rtx1300.bin
 -
- Checking in the console:
Run "**show environment**" command.
For example, if you are using firmware and configuration files loaded from a micro SDHC card, you will see something like this:

```
> show environment
:
Firmware:sd1:/rtx1300.bin
Config. file:sd1:/config.txt
:
```

NOTICE

Use "**external-memory boot permit off**" command to prevent operation with firmware or configuration files in external memory.

6.2. Shutdown Procedure

This section describes how to safely shut down this product.

If the product malfunctions, a communication error occurs, or a security problem occurs, or in other emergency situations, turn off the power immediately.

NOTICE

This section assumes that you understand how to use the console. For more information about using the console, see Chapter 8, Using the Console.

1. Use **“pp disable all”** command to disable all destinations.
2. Use **“disconnect all”** command to disconnect all communications.
3. Save your settings with **“save”** command.

CAUTION

When you change the product settings using the console, the changes are immediately reflected in the product's operation.

However, it is not stored in non-volatile memory. If you turn off the power without saving the settings with the save command, the changed settings will revert to their original state.

For more information, see Finishing Setup.

4. Press and hold the button on the back for 2 seconds or more if a micro SDHC card or USB memory is connected.

Wait until the external memory indicator turns off before removing the external memory.

5. Set the POWER switch to STANDBY.

The POWER indicator will turn off and the unit will enter standby mode.

ATTENTION

Before turning the power of this product back on, wait at least 10 seconds after the POWER indicator goes out.

NOTICE

When you turn off the power with the POWER switch, the product automatically saves the log to the product's non-volatile memory (power-off log save function). The log will not disappear even after the power is turned off, so you can check the log before the power was turned off after restarting the product.

However, if you turn off the power by a method other than the POWER switch, such as by unplugging and plugging in the power cord, the logs before the power was turned off will not be saved.

7. Using the Web GUI

This product is equipped with a Web GUI, which allows you to perform basic settings using a web browser on your PC. It also has a screen that is convenient not only for settings but also for management.

notice

- For details about supported web browsers, please visit the following website.
<http://www.rtpro.yamaha.co.jp/RT/FAQ/gui/browser.html>

7.1. Login Procedure

This section describes how to log in to the Web GUI.

- **7.1.1. First login (in factory default settings)**
Log in to this product using the account of the initial administrative user "admin" (initial password "admin").
To log in to this product, you must change the password of the initial administrative user.
- **7.1.2. Second and subsequent logins (if password has been changed)**

7.1.1. First time login (Factory Default Settings)

To log in to this product, you must change the password for the initial administrative user "admin" (initial password: "admin"). Follow the steps below to log in and change your password.

1. Connect the LAN1 interface (ports 1 to 8) of this product to your computer with a LAN cable.

ATTENTION

Until you change the password for the initial administrative user "admin", you will not be able to log in from a computer connected to the LAN2 or LAN3 interface (ports 9 and 10).

Launch a web browser on your computer.

2. Enter "http://192.168.100.1" in the address bar using alphanumeric characters and press the [Enter] key. A dialog will appear prompting you to enter your username and password.
3. Enter "admin" as the username and "admin" as the password, then click the "Login" button.

The password change screen will be displayed.

The screenshot shows a web browser window with the address bar containing "http://192.168.100.1". Below the address bar, the text "This site is asking you to sign in." is displayed. There are two input fields: "Username" with the text "admin" and "Password" with ten black dots. At the bottom, there are two buttons: "Sign in" (highlighted with a red box) and "Cancel".

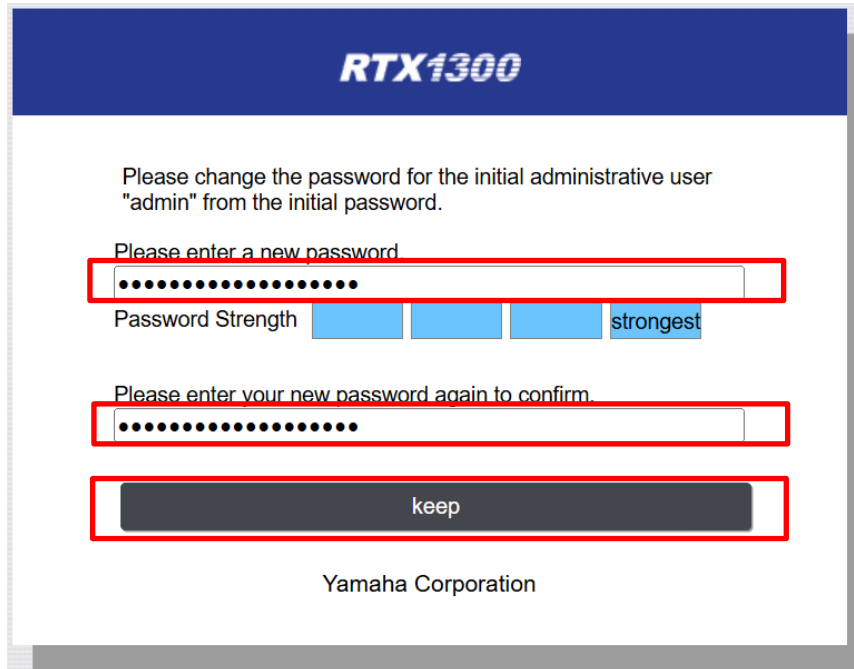
IMPORTANT

You will not be able to log in to the machine until you have set a new password.

NOTICE

If you enter an incorrect username or password three times in a row, an error screen will be displayed. In this case, wait at least one minute and then start over from step 3.

- 4. Enter your new password in both fields and click the "Save" button.



IMPORTANT

- The password must meet the following requirements:
 - Number of characters: 1 to 32
 - Usable characters: Half-width alphanumeric characters, half-width symbols (ASCII characters)
 - Uppercase and lowercase letters are sensitive.
 - The string "admin" cannot be set as a password.
- From a security standpoint, we recommend that you use a password that meets the following criteria:
 - At least 15 characters
 - Includes various character types (uppercase letters, lowercase letters, numbers, symbols)

The Web GUI dashboard will be displayed.

IMPORTANT

From now on, to enhance security, we recommend that you register and use a new user account rather than the initial administrative user "admin". For instructions on registering a user account, please refer to the "Web GUI Operation Manual" (website).

7.1.2. Second and Subsequent Log in (If Password has been Changed)

If you have already changed the password for the initial administrative user "admin", you can log in to this product by following the steps below.

1. Connect the LAN1 interface (ports 1 to 8) of this product to your computer with a LAN cable.
2. Launch a web browser on your computer.
3. Enter "http://(the IP address of this product)/" in the address bar using half-width alphanumeric characters and press the [Enter] key.

A dialog will appear prompting you to enter your username and password.

4. Enter your username and password and click the "Login" button.

Sign in
http://192.168.100.1
Your connection to this site is not private

Username

Password

5.

The Web GUI dashboard will be displayed.

NOTICE

If you enter an incorrect username or password three times in a row, an error screen will be displayed. In this case, wait at least one minute and then start over from step 3.

8. Using the Console

This chapter describes the console of this product.

The console allows you to configure the product and check its status.

8.1. How to Log in

There are three ways to log in to the console:

- [8.1.1, "Logging in from a computer connected to the CONSOLE port"](#)
- [8.1.2, "Logging in via TELNET or SSH from a PC on the LAN"](#)

NOTICE

- Multiple users can be admin users at the same time, configuring from different hosts simultaneously.
- Each user can see the access status of all users currently accessing the site.
- Administrative users can forcefully disconnect other users.

8.1.1. Log in from a Computer Connected to the CONSOLE port

Connect your computer to the CONSOLE port of the product and log in to the product. This product has two types of CONSOLE ports: Use the appropriate cable to connect to either port.

| CONSOLE PORT | cable |
|-----------------------|---|
| mini-USB CONSOLE port | A USB cable with a USB Type A connector and a mini-USB Type B (5-pin) connector |
| RJ-45 CONSOLE PORT | RJ-45/DB-9 console cable |

NOTICE

- If you want to use the mini-USB CONSOLE port, you must first install the USB serial driver.
- If both the mini-USB CONSOLE port and the RJ-45 CONSOLE port are connected to a computer, settings and operations can only be performed using the terminal software that uses the mini-USB CONSOLE port. The output messages from this product are
The output will be sent to the CONSOLE port.

Your PC will need terminal software to control the PC's serial (COM) ports. Please use the terminal software provided by each company for controlling serial devices.

Set the parameters of the terminal software as follows:

| Terminal parameters | Setting Value |
|----------------------|---------------|
| Data Transfer Speed | 9600 bit/s |
| Character Bit Length | 8 |
| Parity Check | none |
| Stop Bits | 1 |
| Flow control | Xon/Xoff |

IMPORTANT

The data transfer speed setting of "9600 bit/s" is the default value for the CONSOLE port of this product. If you change the data transfer rate of the CONSOLE port, you must also change the data transfer rate of the terminal software.

8.1.2. Log in via TELNET or SSH from a Computer on the LAN

You can log in to this product from a computer on the LAN using TELNET or SSH. When this product is shipped from the factory, the IP address of the LAN1 interface is set to "192.168.100.1/24" and the DHCP server is enabled. Therefore, if you connect a computer with DHCP client enabled to the LAN1 interface, it will be automatically assigned an IP address.

IMPORTANT

When you log in for the first time, be sure to connect your computer to the LAN1 interface (one of ports 1 to 8).

Please continue.

You will not be able to log in from computers connected to the LAN2 or LAN3 interface (ports 9 and 10) until you change the password for the initial administrative user "admin."

Logging in via TELNET

You can log in to this product (TELNET server) from a computer on the LAN (TELNET client). Please use the terminal software for TELNET connection provided by each company.

NOTICE

You can also operate it using the Windows command prompt. In that case, Windows Please enable the "Telnet Client" function.

Logging in via SSH

You can log in to this product (SSH server) from a computer on the LAN (SSH client).

To log in to the product using SSH, you must first log in to the product using another method and perform the following settings.

You need to.

- Registering a user to this product
- Enable the SSH server on this product

For more information, see the Command Reference (website).

8.2. Login Procedure

This section describes the procedure for logging in to the console.

- [8.2.1, "First time login \(in factory settings\)"](#)
Log in to this product using the account of the initial administrative user "admin" (initial password "admin").
To log in to this product, you must change the password of the initial administrative user.
- [8.2.2, "Second and subsequent logins \(if password has been changed\)"](#)

8.2.1. First time Log in (Factory Default Settings)

To log in to this product, you must change the password for the initial administrative user "admin" (initial password: "admin"). Follow the steps below to log in and change your password.

1. Connect this product to the PC with a console cable.

IMPORTANT

To log in via TELNET, use the LAN1 interface (any of ports 1 to 8) of this product.

Connect the device (or both) to your computer with a LAN cable. You will not be able to log in from computers connected to the LAN2 or LAN3 interface (ports 9 and 10) until you change the password for the initial administrative user "admin."

2. Start the terminal software on your PC.
3. Press the Enter key.

NOTICE

To log in via TELNET, access the product's IP address "192.168.100.1" using the procedure appropriate for the terminal software launched in step 2.

- A prompt will appear asking for a username.

4. Enter the initial administrative username "admin" and press the Enter key.

```
Username: admin
```

- A prompt will appear waiting for your password.

5. Enter the initial administrative user password "admin" and press the [Enter] key.

```
Password:
```

NOTICE

The password you enter will not be displayed on the console screen. (The same applies to the following steps.)

- A prompt will appear waiting for you to change your password.

IMPORTANT

You will not be able to log in to the machine until you have set a new password.

NOTICE

If you enter the wrong username or password three times in a row, an error message will be displayed on the console screen. In this case, wait at least one minute and then start over from step 3.

6. Enter the new password and press Enter.

```
Initial Admin User admin Please change your password
New_Password:
```

IMPORTANT

- The password must meet the following requirements:
 - Character count: 1 to 32 characters
 - Usable characters: Half-width alphanumeric characters, half-width symbols (ASCII characters)
 - Uppercase and lowercase letters are sensitive.
 - The string "admin" cannot be set as a password.
 - From a security standpoint, we recommend that you use a password that meets the following criteria:
 - At least 15 characters
 - Includes various character types (uppercase letters, lowercase letters, numbers, symbols)
 - You will be prompted to re-enter your password.
7. Enter the same password as in step 6 again and press the Enter key.

```
New_Password(Confirm):
```

- Your game will be saved automatically, and you will be logged in to the game.
- The general user prompt appears.

```
# save
Saving ... CONFIGO Done .
>
```

IMPORTANT

- To configure this product, you must access it as an administrator user. For more details, refer to "8.4 Access Levels" and "Getting Started with Configuration."
- From now on, to enhance security, we recommend that you register and use a new user account instead of the initial administrative user "admin". For instructions on registering a user account, see "9.1.1, "Registering a User Account".

NOTICE

For security reasons, if there is no key input on the console for a certain period of time, you will be automatically logged out. For details, see 10.4.1, "Setting the Login Timer".

8.2.2. Second and Subsequent Log in (If password has been changed)

If you have already changed the password for the initial administrative user "admin", you can log in to this product by following the steps below.

1. Connect this product to the PC with a console cable.

NOTICE

To log in via TELNET or SSH, connect the LAN1 interface (any of ports 1 to 8) of this product to your computer with a LAN cable.

2. Start the terminal software on your PC.
3. Press the Enter key.

NOTICE

When logging in via TELNET, access the IP address of this product using the procedure appropriate for the terminal software launched in step 2.

- A prompt will appear asking for a username.
4. Enter the user name (e.g. "user1") and press the Enter key.

```
Username:user1
```

- A prompt will appear waiting for your password.
5. Enter the password for the user you entered in step 4, and then press the Enter key.

```
Password:
```

NOTICE

The password you enter will not be displayed on the console screen.

- If the password is correct, you will be logged in to the product.

NOTICE

If you enter the wrong username or password three times in a row, an error message will be displayed on the console screen. In this case, wait at least one minute and then start over from step 3.

- The general user prompt appears.

>

important

To configure this product, you will now need to access it as an administrator user. For details, see 8.4, "Access Levels" and Getting Started.

notice

For security reasons, if there is no key input on the console for a certain period of time, you will be automatically logged out. For details, see 10.4.1, "Setting the Login Timer".

8.3. Character Set Selection to Display

To change the character set displayed on the console, use the console character command. You can select one of the following character sets: en.ascii (ASCII), ja.sjis (SJIS), ja.euc (EUC), or ja.utf8 (UTF8). The factory setting is "en.ascii".

Depending on the character set, the language in which error messages, help messages, and the results of executing the show command are displayed will change as follows:

- If the character set is ASCII: Display in English
- If the character set is SJIS, EUC, or UTF8: Display in Japanese

For example, to change the character set displayed on the console to ASCII code, set it as follows:

```
# console character en.ascii
```

8.4. Access Levels

Users who log in to this product are classified into two types: general users and administrative users. This is called the access level.

The different access levels are as follows:

| Access Levels | explanation |
|----------------------|---|
| General user | You can view the settings and communication logs of this product. The settings cannot be changed. When logging in, you will need to enter your user password. |
| Administrative users | In addition to the operations that general users can perform, you can change the settings of this product. Log in as a general user, then use the administrator command to become an administrator user. If an administration password has been set, you will need to enter it. |

The prompt displayed on the console screen will tell you your current access level.

- General user prompt:

>

- Admin user prompt:

```
#
```

You can set a password for each access level.

- For instructions on how to set a user password, see "9.1, "Setting Up User Accounts".

NOTICE

If the password for the initial administrative user "admin" is "admin", you will be requested to change the password the first time you log in. For details, see 8.2, "Login Procedure".

- For instructions on how to set the administrator password, see 9.2, "Setting the Administrator Password".

8.5. How to Use the Console

8.5.1. Command Input Format

The command input format is standard line input. Enter a command on a line after the prompt and press Enter to execute the command.

This product does not normally distinguish between uppercase and lowercase characters when entered from the keyboard. However, it does preserve case for things that are case sensitive, such as usernames and passwords.

8.5.2. Screen Display

If the number of lines of information displayed on the screen is too large to fit on one screen, the screen will close after the set number of lines are displayed.

The display of the face will stop. In addition, the following message will be displayed at the bottom of the screen:

```
---more---
```

- Press the space bar to display the remaining lines.

When you press the Enter key, the following line is displayed:

- Once the information has been displayed to the end, you will automatically be returned to command input mode.

If you want to end the display without viewing all the information, press the [Q] key. After this, you can enter commands.

The camera will return to a working state.

The number of lines of information displayed on the screen can be set with the console lines command. To display more information than can fit on one screen without the screen display stopping, set the following:

```
# console lines infinity
```

8.5.3. Editing Keyboard Input

- To correct one character entered using the keyboard, press the [Backspace] or [Delete] key on the keyboard to delete that character.
- If you move the cursor using the [←] or [→] key while entering text, the next character you enter will be inserted at the cursor position.

NOTICE

The arrow keys may not function properly depending on the type of console terminal. In this case, use the key operations in the table below.

- The following key operations are available for editing keyboard input:

| Key operations | meaning |
|----------------|--|
| [Ctrl] + [A] | Move cursor to beginning of line |
| [Ctrl] + [B] | Move cursor one character left |
| [Ctrl] + [C] | Enter a new line without executing the command |
| [Ctrl] + [D] | Delete the character under the cursor |
| [Ctrl] + [E] | Move cursor to end of line |

| Key operations | meaning |
|----------------|--|
| [Ctrl] + [F] | Move cursor one character to the right |
| [Ctrl] + [K] | Delete the character after the cursor |
| [Ctrl] + [U] | Clear the input line |
| [Ctrl] + [W] | Delete the character before the cursor |

notice

You can also use the help command to find out how to operate the console screen.

```
>help
```

8.5.4. Keyboard Input Error Messages

If the command name is inappropriate, if the number of parameters in the command is inappropriate, or if the parameters exceed the specifiable range, an error message will be displayed on the console screen after you press the [Enter] key. For example, if you forget to enter a required parameter, the following error message appears:

```
# console lines
Error: Insufficient or too many parameters
```

NOTICE

In addition to the command operation errors listed above, this product can also display communication error messages. Communication error messages are recorded in the communication log.

8.6. Command Input Assistance Function

The console has a command history function, a command completion candidate display function, and a command name completion function to assist with keyboard input.

8.6.1. Command History Feature

- By pressing the [Up] key or [Ctrl] + [P], you can recall all commands you have entered and executed up to that point on the command line. You can use the [↓] key or [Ctrl] + [N] to call up the next command executed after the currently displayed command to the command line.

NOTICE

The arrow keys may not function properly depending on the type of console

terminal.

In such cases, use Ctrl+P or Ctrl+N.

- You can delete, edit, and move the cursor over the recalled command in the same way as you would with a command you typed in directly.

For instructions on how to do this, see "8.5.3, "Editing Keyboard Input".

8.6.2. Command Auto-Completion Suggestion Feature

- If you press the [?] key before or during command input, a list of commands that can be entered next will be displayed. The new command line will be displayed up to the part before you typed the ? key.

(Example 1) When you enter "cons" into the console and then press the [?] key

Suggested keywords following "cons" will be displayed.

```
#cons?
?console #
cons
```

(Example 2) When you enter "console" into the console and then press the [?] key

Since the keyword "console" has already been completed, suggestions for keywords following "console" will be displayed. Note that there is a space between the keyword and the "?".

```
# console ?
? character columns info lines prompt
# console
```

- After entering the command name, pressing the [?] key will display the command input format and a description.

NOTICE

If you want to include the character "?" in a command parameter, enter "¥" (yen sign, "¥" (backslash) on an English keyboard) immediately before the "?". The "¥" removes the help function of the key and allows you to enter the "?" character.

8.6.3. Command name Auto-Completion Feature

- When you are entering a command name, you can press the Space key or the Tab key to complete any missing parts of the command name or the keywords of the parameters following the command. If there are multiple candidates for completion, the confirmed part will be completed.
- If completion is possible up to the end of a command, pressing the Enter key will execute the command after completion. For example, you can type "sa" and press Enter to execute the save command.

8.7. List of Commands that can be Entered

The "show command" can be used to display a list of command names and brief descriptions.

```
# show command
administrator:      Logs in as an administrator.
administrator password: Assigns a password for administrator.
```

For details on each command, please see the "Command Reference" (website).

9. Configure this Product

This chapter describes the following settings for this product:

- Items to be set first
 - [9.1, "Setting up user accounts"](#)
 - [9.2, "Setting the Admin Password"](#)
- Setup procedure, precautions, etc.
 - [9.3, "Settings Operation Flow"](#)
 - [9.4, "Specific Settings"](#)
 - [9.5, "Checking Connectivity"](#)
- How to reset your settings
 - [9.6, "Restore factory settings"](#)

notice

The IP addresses used as examples in this chapter are for illustrative purposes only. When actually setting it up, please read it according to your environment.

9.1. Setting up User Accounts

This section explains how to configure the following:

- [9.1.1, "Registering a User Account"](#)
- [9.1.2, "Changing a User's Permissions"](#)
- [9.1.3, "Changing a User's Password"](#)

9.1.1. Register a User Account

If someone other than the network administrator accesses this product, for security reasons we recommend that they log in using a user account other than the initial administrative user "admin".

You can register a user account with the login user command. The conditions for setting the username and password are as follows:

| item | Setting conditions |
|----------|--|
| username | <ul style="list-style-type: none"> • Number of characters: 1 to 32 • Usable characters: Half-width alphanumeric characters, hyphens (-), and underscores (_) • The characters are case sensitive. |
| password | <ul style="list-style-type: none"> • Number of characters: 1 to 32 • Usable characters: Half-width alphanumeric characters, half-width symbols (ASCII characters) • The characters are case sensitive. • The string "admin" cannot be set. |

For example, to register a user account with the username "user1" and the password "Password-1234567890", enter the following:

```
# Login user user1 Password-1234567890
Password Strength : Very Strong
# save
```

IMPORTANT

- From a security standpoint, we recommend that you use a password that meets the following criteria:
 - At least 15 characters
 - Includes a variety of characters (uppercase and lowercase letters, numbers, and symbols)
- You can change user permissions according to the purpose of using the registered account. See Chapter 9.1.2, "Changing User Permissions" for details.
- For security reasons, please refer to "9.2, "Administrative Passwords" in addition to registering user accounts.

[We also recommend that you set up the "settings" for your device.](#)

ATTENTION

Even admin users cannot view the password after it has been set. If you forget your password, run the login user command again. You can override the password setting by specifying a registered username and a new password.

9.1.2. Change a User's Permissions

You can change a user's permissions by running **"user attribute"** command with a registered username. If someone other than the network administrator accesses this product, we recommend that you set user permissions according to the purpose of the account.

NOTICE

For instructions on how to register a username, see chapter 9.1.1, "Registering a User Account".

There are three setting patterns for user permissions for this product:

Depending on the setting, the login permissions to this product differ as follows:

| Value | Permissions when using Console | Permission when using the Web GUI | Remarks |
|-------|---|-----------------------------------|--|
| 2 | Can be promoted to administrative user (No need to enter an administrative password) | Log in as an admin user | Equivalent to the initial administrative user "admin" is your authority. |
| 1 | Can be promoted to administrative user (Administrative password must be entered) | Log in as a general user | This permission is automatically set for users immediately after registration. |
| off | Cannot be promoted to admin user | Log in as a general user | |

NOTICE

For instructions on setting the administration password, see Chapter 9.2, "Setting the Administration Password".

For example, if you want to give the user "user1" administrative user privileges even when using the Web GUI, enter the following:

I will.

```
# user attribute user1 administrator=2
# save
```

NOTICE

For more information about **"user attribute"** command, see the Command Reference (website).

9.1.3. Change a User's Password

You can override the password setting by specifying a registered username and a new password with **"login user"** command.

For details on operation methods and password entry conditions, see "9.1.1, "Registering a User Account".

9.2. Setting the Admin Password

The "admin password" is the password that the user added in 9.1.1, "Register a User Accounts", enters when accessing the console of this product as an administrative user.

The administrator password is not set for this product when it is shipped from the factory. For added security, we recommend setting an administration password.

To set the administrative password, use **"administrator password"** command.

Passwords must be a maximum of 32 ASCII characters and are case sensitive.

```
# administrator password
Old_Password:
New_Password:
New_Password(Confirm):
Password Strength: Very Strong
# save
```

NOTICE

The password you enter will not be displayed on the console screen.

IMPORTANT

From a security standpoint, we recommend that you use a password that meets the following criteria:

- 15 characters or more
- Includes various character types (uppercase letters, lowercase letters, numbers, symbols)

ATTENTION

- Even the admin user cannot see the admin password after it has been set.
Password
Be sure not to forget your password.
- By using an external memory, you can change the boot firmware and settings of this product regardless of the administrator password setting. Therefore, the admin password is changed.
- This makes it possible to execute commands that can only be executed by administrative users.
To prevent the use of external memory to change the boot firmware or modify the settings, use the following command:
 - **external-memory boot permit off**
 - **operation external-memory download permit off**
 - **operation execute batch permit off**

9.3. Setup Operation Flow

This product operates according to the configuration file stored in the product's internal memory. This section explains the flow of operations when directly editing configuration files.

- 9.3.1, "Using the Console"
 - Start the setup
 - setting
 - Checking the settings
 - Finishing the setup
- 9.3.2, "Using TFTP"
 - Advance preparation
 - Settings (sending the settings file)
 - Checking the settings (getting the settings file)
 - Finishing the setup

ATTENTION

Administrative users should be fully aware that incorrect configuration of this product could cause serious damage to the entire network when performing configuration work.

9.3.1. Using the Console

Edit the configuration file by entering commands directly into the console screen of this product.

Start the setup

After logging in as a general user, access as an administrative user with the administrator command.

If an administration password has been set, you must enter it.

```
>administrator  
  
Password:  
#
```

NOTICE

If you are logged in as the initial administrative user “admin”, you can access as the administrative user without entering the administrative password.

setting

Enter commands directly into the console screen.

For details on the settings, see 9.4, “Specific Settings”.

IMPORTANT

To change the settings for the destination information for the line connection, follow the steps below.

1. Use “**pp disable**” command to disable the target destination.
2. (If connected to the line) Use “**disconnect**” command to disconnect communication with the target device.
3. Execute various commands to change the destination information settings.
4. Use “**pp enable**” command to set the target destination to a usable state.

Checking the settings

The configuration details can be displayed on the console screen using the show config command. If you have applied new settings to your machine, please check them.

```
# show config  
# RTX1300 Rev.23.00.03 (Tue May 17 19:28:362022)  
# MAC Address: ac:44:f2:00:00:00 -ac:44:f2:00:00:07  
# Memory 1024Mbytes, 8LAN  
#Reporting Date:Jun1909:33:072022  
login user admin *  
User attribute admin administrator=2  
ip lan1 address 192.168.100.1/24  
:  
#
```

Finishing the setup

When you enter a configuration command, it is immediately reflected in the operation of this product, but the configuration is not saved in non-volatile memory. To save the settings, run the save command.

```
#save
Saving... CONFIGO Done
#
```

ATTENTION

If you turn off the power or restart the unit without saving the settings, the changed settings will be reset.

NOTICE

If you are working with a configuration file on the external memory, the settings are saved to the external memory.

When logging out as an administrative user, you can also save the settings changed with the setting commands to the non-volatile memory of this product.

Run the quit command with the save option as follows:

```
# quit save
```

If you execute **“quit”** command without executing **“save”** command, a message appears asking whether you want to save the settings. To save, press the [Y] key. To not save, press the [N] key.

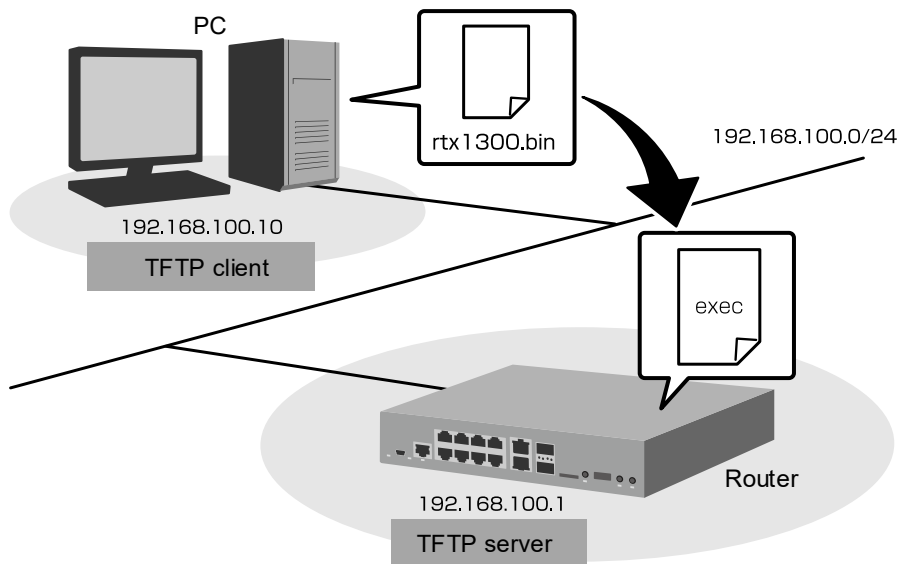
```
# quit
Do you want to save the new settings?? (Y/N)
Save new configuration ? (Y/N)
```

9.3.2. Using TFTP

You can edit the configuration file of this product by transferring the configuration file created on your PC to this product using TFTP.
can.

When configuring using TFTP, this product acts as a TFTP server and the computer acts as a TFTP client.

You can run "**tftp**" command from Command Prompt in Windows, or from the Terminal application in macOS.



This guide explains how to change the settings of this product using TFTP from a Windows computer. If you are using something other than a PC, please replace the operations on the Windows PC as appropriate for your environment.

Advance preparation

- **Setting up this product (TFTP server)**

Execute the tftp host command on the console of this product to transfer the configuration file to the computer.

Set the IP address of the (TFTP client).

For example, if your computer's IP address is "192.168.100.10", enter it as follows:

```
>administrator
Password:
# tftp host 192.168.100.10
# save
```

- **Setting up the PC (TFTP client)**

Enable the TFTP client setting on your computer.

NOTICE

In the case of Windows, TFTP is disabled in the initial state. To use TFTP, display the [Turn Windows Features on or off] screen from the Windows [Control Panel] and enable the TFTP client.

- **Creating a configuration file**

Enter the set of commands to be set on this product into a text file and save it on your computer. For details on the settings, see 9.4, "Specific Settings".

IMPORTANT

In the text file, enter a new line after the last command. Commands without a newline will not be executed.

NOTICE

By entering the clear configuration command at the beginning of the text file, you can completely rewrite the contents of the configuration file (deleting the existing configuration contents of this product)

If you do not enter the clear configuration command, the commands entered in the text file will be added based on the existing configuration of this product.

Settings (Transfer of settings file)

Execute the tftp command from your computer to transfer the configuration file to this product.

NOTICE

- The TFTP execution format depends on the OS.
- Set the transfer mode to "ASCII" or "Character".
- If an administration password is set for this product, specify the administration password after the file name.

Start the Windows command prompt and enter the following:

(example)

IP address of this product:

192.168.100.1 Administration

password for this product: "adM123"

Name of the configuration file to be transferred to this product: "config1.txt"

```
C:\>tftp 192.168.100.1 PUT config1.txt config/adM123
Transfer successful: xxxx bytes in x second, xxxx Bytes/s
```

```
C:¥
```

NOTICE

You can also specify "config0" through "config4" instead of "config". For details about configuration file numbers, see Chapter 10.2, "Managing Configuration Files".

Checking the settings (getting the settings file)

Execute the tftp command from your computer to read the product's settings as a settings file. If you have applied new settings to your machine, please check them.

NOTICE

- The command format you use depends on the host's operating system.
- Set the transfer mode to "ASCII" or "Character".
- If an administration password is set for this product, specify the administration password after the file name.

Start the Windows command prompt and enter the following:

(example)

IP address of this product:

192.168.100.1 Administration

password for this product: "adM123"

Name of the file to save on your computer: "config0.txt"

```
C:\>tftp 192.168.100.1 GET config/adM123 config0.txt
Transfer successful:xxxx bytes in x second, xxxx Bytes/s

C:¥
```

NOTICE

You can also specify "config0" through "config4.2" instead of "config". For more information about the setting file numbers, see 10.2, "Managing Configuration Files".

Finishing the setup

When you transfer the settings file, the settings are immediately reflected in the operation of this product, but the settings are not saved in non-volatile memory. To save the settings, transfer a text file containing the save command to this product as a settings file.

For instructions on how to transfer the configuration file, see "Settings (Transferring the Configuration File)."

ATTENTION

If you turn off the power or restart the unit without saving the settings, the changed settings will be reset.

IMPORTANT

In a text file, enter a newline after the save command. Commands without a line break will not be executed.

NOTICE

If you are working with a configuration file on the external memory, the settings are saved to the external memory.

9.4. Specific Settings

The main configuration items and the commands used to configure them are shown below.

| Setting items | Commands to use | Factory default value |
|---------------------|----------------------------|-----------------------|
| routing | IP routing | on |
| OSPF | ospf use | off |
| RIP | rip use | off |
| BGP | bgp use | off |
| Terminal parameters | console character | ja.sjis |
| | console columns | 80 |
| | console lines | twenty four |
| | set-serial-baudrate | 9600 |
| Login Timeout | Login timer | 300 |
| IP address | ip lan1 address | 192.168.100.1/24 |
| | ip lan2 address | none |
| | ip lan3 address | none |

For details on each command and other commands, see the Command Reference (website).

You can also easily set it up by using the configuration examples or contacting our customer service center.

Using the configuration examples

When setting up, first think of a specific configuration diagram, like in the setting examples.

If the LAN has already been set up, list the network addresses and the protocols being sent and received, and write them directly on the configuration diagram. If network addresses have not been decided, you must allocate network addresses appropriate for the number of hosts connected to the network.

Once the network addresses have been decided, we need to consider how to route each network.

If your network is relatively small, you may be able to use Proxy ARP, or static routing may be sufficient. Dynamic routing is required when several networks are interconnected. It may be uniquely determined depending on the connection partner.

The configuration examples mainly describe configurations for LAN-to-LAN connections via WAN lines. If you have a dial-up connection to a provider or a connection to the Internet, filtering will be necessary to restrict host access, deal with unauthorized access, and protect against DoS attacks.

The Yamaha network equipment website also provides several examples of configuration. Please refer to.

<https://network.yamaha.com/setting/>

Please use your browser's translation feature to check.(The page is in Japanese.)

Contact the Customer Service Center

If you are unsure of the desired configuration (config) or have any questions, you can contact our Customer Service Center. In this case, the time it takes to resolve the problem can be shortened if you prepare a configuration diagram and configuration files in advance, and if there are any operational problems, a DEBUG-level SYSLOG as well. For information on obtaining the

configuration file, see "Checking the Configuration". For information on how to take SYSLOG, see "10.8.4, "Checking SYSLOG".

For contact information, see 11.1.2, "Contact Information".

9.5. Verify Connectivity

Once the setup is complete, check that connections to the other network, FTP servers on the Internet, etc. are made correctly and as intended.

There are two commands to check the connection with the other party: ping and traceroute.

- **ping Command**

In a relatively simple network, it is run to check packet reachability to each network connection point or host.

- **traceroute Command**

This is run to check whether packets pass as intended over a route that passes through multiple networks.

NOTICE

Windows will not respond to pings if the firewall is enabled.

9.6. Restoring Settings to Factory Defaults

There are three ways to reset the settings of this product to the factory default settings:

- [9.6.1, "Restore to factory settings using the microSD, USB, and DOWNLOAD buttons"](#)
- [9.6.2, "Restoring to factory settings with the cold start command"](#)
- [9.6.3, "Restoring the Product to the Factory Defaults Using the Web GUI"](#)

IMPORTANT

- All communications will be cut off immediately after the operation is performed.
- The IP address of this product will be reset to "192.168.100.1/24" (factory default).
- When you reset the product to its factory settings, all setting files and SYSLOG data stored in non-volatile memory will be erased (and cannot be restored).
If necessary, please back up any information to a computer or other device in advance. For information on how to read data, please refer to the "Web GUI Operation Manual" (website) or "Command Reference" (website).
- Even if you reset the product to its factory settings, the firmware recorded in the non-volatile memory will remain intact.

9.6.1. Reset to Factory Settings with the microSD, USB, and DOWNLOAD Buttons

You can reset the product to its factory settings by simultaneously pressing and holding the microSD, USB, and DOWNLOAD buttons on the front of the product while turning it on.

1. Set the POWER switch of this product to STANDBY.
2. While pressing and holding the microSD, USB, and DOWNLOAD buttons simultaneously,

turn the POWER switch ON. The product will start up and return to the factory settings.

9.6.2. Use the Cold Start Command to Reset to Factory Settings

You can reset this product to its factory settings by executing the cold start command on the console screen. When you run the cold start command, you will be prompted to enter the admin password. After you enter the administration password, the product will reboot and return to its factory settings.

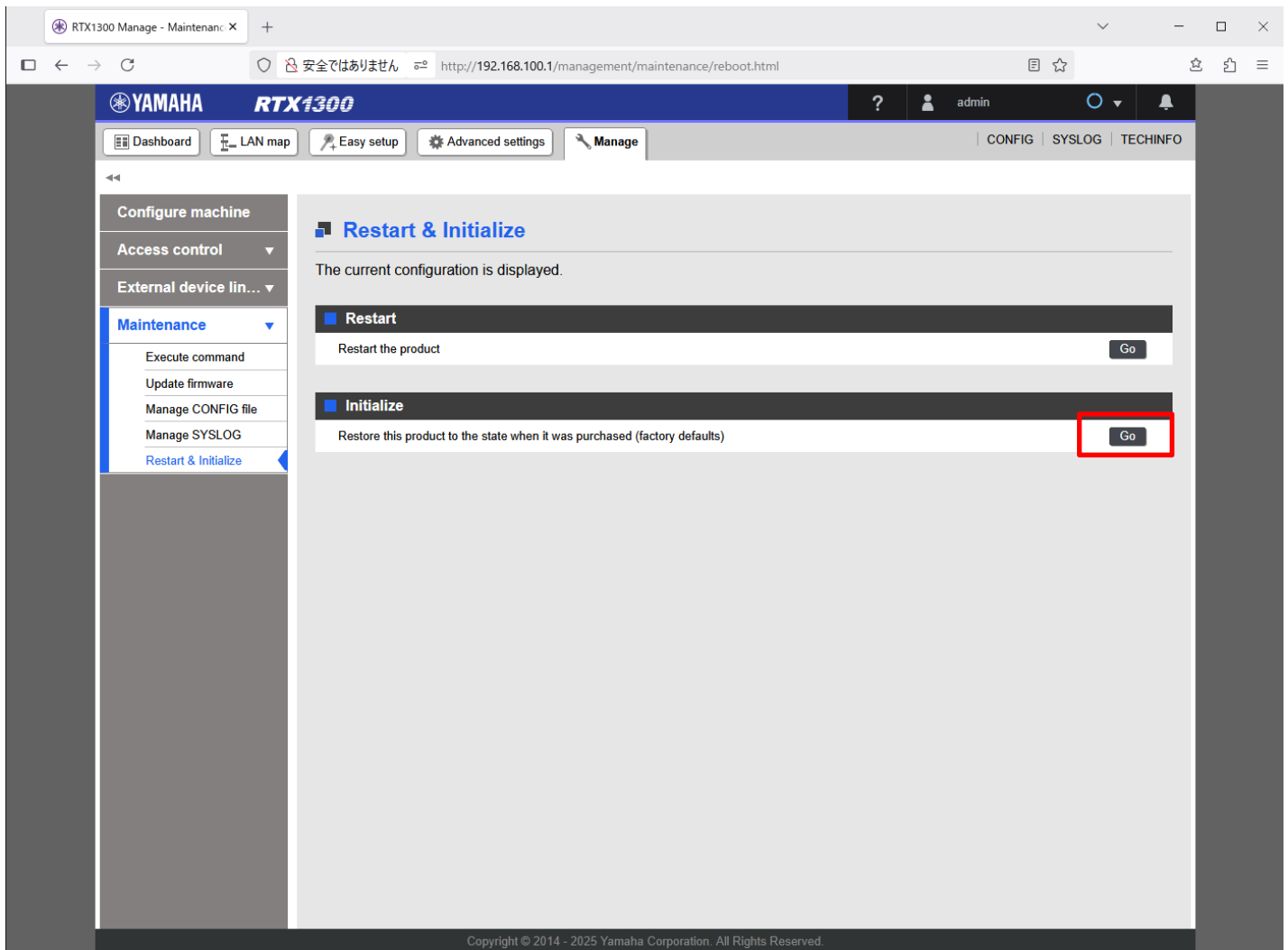
```
>administrator  
Password:  
# cold start  
Password:
```

NOTICE

If you are logged in via TELNET, etc., that communication will be disconnected.

9.6.3. Restoring this Product to its Factory Settings using the Web GUI

You can restore this product to its factory settings from the "Administration" tab - "Maintenance" - "Restart and Reset" screen of the Web GUI.



For details, please refer to the "Web GUI Operation Manual" (website).

10. Managing this product

This chapter describes the daily management tasks and provides specific configuration and diagnostic methods.

NOTICE

The IP addresses used as examples in this chapter are for illustrative purposes only. When actually setting it up, please read it according to your environment.

10.1. System Management Tasks

In the following situations, the administrator should take appropriate action:

- When adding new recipient information
- When deleting unnecessary recipient information
- When there is a change in the recipient information
- When the connection method with your Internet service provider is changed
- When the network configuration on the LAN side is changed
- When managing system and network security
- When updating the firmware of this product
- When a malfunction or network failure occurs

Please regularly manage the following items:

- Changing user and administrative passwords
- Change the authentication password used for various communications
- Check the communication log
- Check and clear accounts

10.2. Managing Configuration Files

This product can store five configuration files (config0 to config4) in the built-in non-volatile memory. In addition, each of these configuration files can have two backup files. The names of the backup files will be "configX.1" and "configX.2".

A backup file is automatically generated each time the save command is executed. For example, if you run the save command while running "config1", the non-volatile memory records: It changes.

- The contents of "config1" in non-volatile memory will become the backup file "config1.1", and the current settings will become "config1".
- If "config1.1" already exists, the backup file will be named "config1.2".
- If "config1.2" already exists, its contents will be discarded.

NOTICE

If you are working with a configuration file on external memory, executing the save command will save the configuration to the external memory. In this case, no backup file is generated.

Before executing the save command, be sure you are familiar with the sequence of the currently running configuration file.

- **You can check the currently running configuration file number by executing the show environment command.**

```
> show environment
:
Firmware: exec0Running configuration file:config0
Default Firmware: exec0Default configuration file:config1.1
:
```

- **You can check the list of configuration files and backup files by running the show config list command.**

```
> show config list
No.   Date       Time       Size   Sects   Comment
-----
* 0   2022/06/17 18:42:36   422 703/703 ospf testing
  0.1 2022/06/17 08:18:06   328 704/704 test
  0.2 2022/06/15 17:17:39   294 705/705
  12022/06/16 11:59:18   292 702/702 BGP+VRRP fix
-----
```

If you perform a save operation at this time, a backup file will be generated, just as if you had executed the save command, and the existing file will be overwritten.

ATTENTION

If you start the program by specifying a backup file, and then run the save command after startup, the contents of the operating memory (the backup file

specified at startup) will be overwritten with the configuration file.

Setting the default configuration file

The default configuration file is the one that is automatically selected during the startup process if you do not specify a configuration file.

When accessing via TELNET or remote setup, you cannot select the executable file and configuration file during the startup process, and the default configuration file is automatically selected.

To set the default configuration file, use the set-default-config command.

The results of running the set-default-config command are not saved to a configuration file, so there is no need to save your changes with the save command.

For example, to set the default configuration file to "config1.1", set it as follows:

```
# set-default-config 1.1
```

Copy the configuration file or the backup file

To save a configuration file or a backup file to a configuration file with a different number sequence, use the copy config command.

Both a configuration file and a backup file can be specified as the source, but only a configuration file can be specified as the destination.

The following is an example of copying the backup file "config1.2" to "config3".

```
# copy config 1.2 3
```

Delete the configuration file or the backup file

To delete configuration files or backup files, use the delete config command. When you delete a configuration file, all backup files with the same number sequence are deleted at the same time. Also, if backup file 1 is deleted, backup file 2 will be deleted at the same time.

10.3. Firmware Revision up

Overview and instructions for transferring firmware obtained from the Yamaha Network Peripheral Device Technical Information page to this product.

Let me explain the procedure.

NOTICE

You can update firmware revisions from older to newer, and vice versa.
You can also revert from one to the other.

There are five ways to update the firmware:

- Use the DOWNLOAD button
(→ 10.3.1, "Revision Up Using the DOWNLOAD Button")
- Use the tftp command on your PC
(→ 10.3.2, "Revision Up Using TFTP")
- Using external memory
(→ 10.3.3, "Revision Up Using External Memory")
- Use SFTP from your PC's SSH client
- Use the SCP function of this product

NOTICE

- To use SFTP, you need to install SSH client software on your computer.
- For information on how to update using SFTP or SCP, please see the Yamaha Network Peripheral Devices Technical Information page.
<http://www.rtpro.yamaha.co.jp/RT/docs/sftpd/>
<http://www.rtpro.yamaha.co.jp/RT/docs/scp/>

Preparation before updating the firmware

Before updating the firmware, you should verify that the firmware you have downloaded is correct.

To verify if the firmware was downloaded correctly, use the MD5SUM Utility to verify the MD5 checksum.

NOTICE

- The MD5SUM utility can be obtained from the Yamaha network peripherals technical information page below.
<http://www.rtpro.yamaha.co.jp/RT/utility/md5sum/>
- The MD5 checksum file "rtx1300.md5" should be downloaded together with the firmware.

To check the MD5 checksum, enter the following at the Windows command prompt:

```
C:\>md5sum -v -c rtx1300.md5
rtx1300.bin OK
```

If you don't see "OK," the file may be corrupted. Pay attention to the transfer mode.
Please download the firmware again.

10.3.1. Revision up using the DOWNLOAD Button

If this product is connected to a network, you can press the DOWNLOAD button to automatically update the firmware to that on the web server. (http revision up)

To enable this feature, use the operation http revision-up permit command.

To specify the web server from which to download the firmware, use the http revision-up url command. When shipped from the factory, the unit is configured to download firmware from Yamaha's web server.

Press and hold the DOWNLOAD button for 3 seconds or more to check whether a new firmware revision is available.

If a new firmware revision is available, it will be automatically downloaded and the firmware will be updated.

If the revision upgrade is successful, the product will restart.

ATTENTION

Do not turn off the power to this product until it has restarted.

NOTICE

You can also allow overwriting with older revision firmware by using the http revision-down permit command.

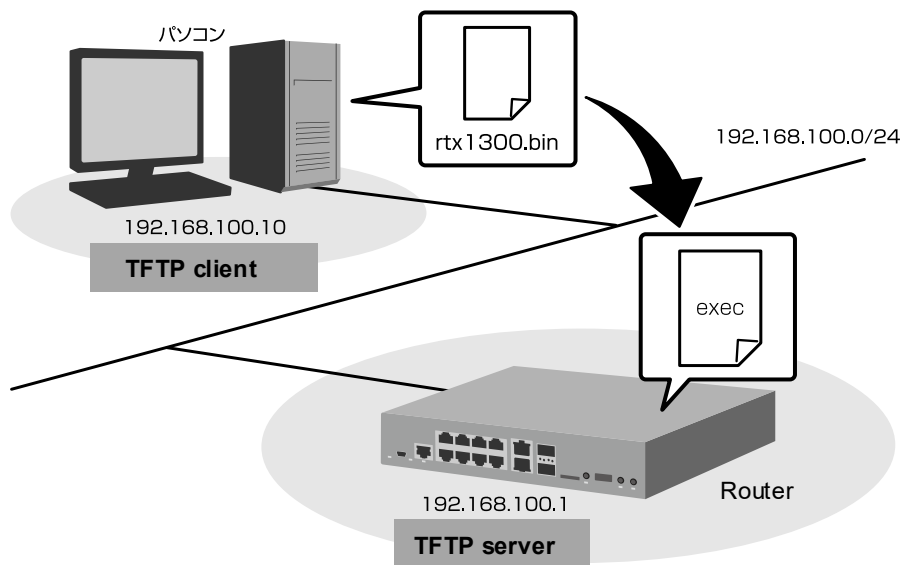
10.3.2. Revision upgrade using TFTP

When updating the revision using TFTP, this product acts as a TFTP server and the PC acts as a TFTP client.

You can run **"tftp"** command from Command Prompt in Windows, or from the Terminal application in macOS.

The TFTP execution format depends on each OS. Please take note of the following points when running this command.

- The transfer mode should be binary. (expressed as binary or bin)
- The file name on this product side is "exec".
- The source file name is "rtx1300.bin".



NOTICE

- In the case of Windows, TFTP is disabled in the initial state. To use TFTP, display the [Turn Windows Features on or off] screen from the Windows [Control Panel] and enable the TFTP client.
- Updating the firmware will not change the settings of this product.

This section explains how to update the firmware of this product using TFTP from a Windows computer. If you are using a computer other than a Windows computer, please replace the operations on the Windows computer as appropriate for your environment.

1. Set the IP address of the computer (TFTP client) to which the firmware will be transferred to this product (TFTP server).
 - On the console of this product, enter the following:
Here, set the computer's IP address as "192.168.100.10".

```
# tftp host 192.168.100.10
```

2. To avoid unstable conditions while modifying the program, communication on the PP side will be disconnected.

- On the console of this product, enter the following:

```
# pp disable all
```

IMPORTANT

In this example, the save command is not executed, so after restarting this product, does not result in the state in which communication on the PP side is disconnected (the state in which the PP disables all commands is executed).

3. Transfer the firmware from your computer to this product.

- Start the Windows command prompt and enter the following:

```
C:¥>tftp -i 192.168.100.1 PUT rtx1300.binexec
Transfer successful: xxxx bytes in x second, xxxx Bytes/s

C:¥
```

NOTICE

In this product, instead of exec, exec0 or can specify exec1. You can also specify "no-reboot" (do not restart this product) or "reboot" (restart this product) as an option for the tftp command.

While the firmware transferred to this product is being written to the non-volatile memory, the STATUS, LAN, microSD, The USB and DOWNLOAD indicators will light up in sequence. Once the firmware has been written to non-volatile memory, the product will automatically restart.

ATTENTION

Do not turn off the power to this product until it has restarted. Because it takes a long time to write to non-volatile memory, the TFTP client may time out, but the revision update can be completed successfully.

NOTICE

If the unit is running on firmware in an external memory, the firmware in the external memory will be updated.

4. Execute "**show environment**" command on the product console to verify that the firmware has been updated correctly.

10.3.3. Revision up Using External Memory

You can update the firmware by loading it from an external memory device into this product. This is useful when you want to update the firmware for multiple units of this product.

This method also allows you to load a configuration file at the same time.

To update the revision using an external memory, follow the steps below.

1. Save the firmware obtained from the Yamaha Network Peripheral Device Technical Information page to external memory. The file name should be "rtx1300.bin".
If you want to load a configuration file at the same time, save the text file containing the commands to external memory as well. Name the file "config.txt".

NOTICE

- We recommend saving each file directly under the root directory.
(When starting this product, multiple files with the same name may exist in the external memory.
If present, the file closest to the root directory will be selected.)
- The file names can be changed using the external-memory exec filename command and the external-memory config filename command.

2. Connect the external memory to the product while it is running.
 - When the external memory is recognized, a buzzer will sound and the microSD indicator or USB indicator on the product will light up.
3. While pressing the microSD button or USB button, press and hold the DOWNLOAD button for more than 3 seconds.
 - The buzzer will sound and the microSD indicator or USB indicator will flash while the firmware is being loaded into the product. Next, the STATUS, LAN, microSD, USB, and DOWNLOAD indicators will light up in sequence while the firmware is copied to the product's non-volatile memory.
Once the firmware has been written to non-volatile memory, the product will automatically reboot.

ATTENTION

Do not turn off the power to this product until it has restarted.

NOTICE

After rebooting, the product will operate with the firmware and configuration files in the external memory.
If this is not necessary, remove the external memory device while the product is restarting and the POWER indicator is flashing.

4. Execute the show environment command on the product console to verify that the firmware has been updated correctly.

NOTICE

To prohibit revision upgrades using external memory, use **“operation external-memory download permit off”** command.

10.4. Console Security Settings

There are two ways to ensure system security:

- [10.4.1, "Setting the Login Timer"](#)
- [10.4.2, "Setting Security Classes"](#)

10.4.1. Login Timer Settings

If there is no key input on the console for a certain period of time, you will be automatically logged out of the product. With the factory default settings, the time until logout (login timer) is 300 seconds.

There are two ways to change the login timer value:

- **Add the login timer command:**
You can set the login timer all at once for all users who do not have the user attribute command set.
- **Add the login-timer option to the user attribute command:** **You can set the login timer for each user.**

The following explanation uses the example where the following command is set in this product.

```
# show config
:
login user admin *
Loginuseruser1 *
login user user2 *
user attribute admin administrator=2
:
#
```

- **By adding the login timer command, you can change the login timer for users "user1" and "user2" at the same time.**
 - To set the login timer to 120 seconds, enter the following:

```
# login timer 120
# save
```

NOTICE

The login timer for the initial administrative user "admin" will not be changed (because the user attribute command is set at the factory).

- To set the login timer for each user, enter the currently configured user attribute command with the login-timer option added.
 - To set the login timer for the initial administrative user "admin" to 120 seconds, enter the following:
To do.

```
# user attribute admin administrator=2 login-timer=120
# save
```

- To set the login timer for the user "user1" (who does not currently have a user attribute command set) to 120 seconds, enter the following:

```
# user attribute user1 administrator=1 login-timer=120
# save
```

In either case, specifying "clear" instead of "120" as the parameter will disable automatic logout. In this case, you will remain logged in to this product until you execute the quit command.

NOTICE

If you are logged in to this product via TELNET or SSH, from a security standpoint, Even if you specify "clear" for the meter, the login timer is treated as 300 seconds.

10.4.2. Security Class Settings

By setting the security class, you can select the method for logging in to the TeraStation's console, and change whether or not the TELNET client function and SSH client function can be used.

- **Choosing a method to log in to the console**

There are three ways to log in to the console:

- Log in from the CONSOLE port
- Logging in via LAN using TELNET or SSH
- Logging in from a remote router (remote setup)

There are security classes ranging from Level 1 to Level 3.

Depending on the level, you can restrict how you log in to this product as follows.

| level | From the CONSOLE port Log in | Via TELNET or SSH Log in | From a remote router Log in |
|-------|---------------------------------|-----------------------------|--------------------------------|
| 1 | permission | permission | permission |
| 2 | permission | permission | rejection |
| 3 | permission | rejection | rejection |

The factory default security class is "1".

- **Whether or not the TELNET client function can be used**

You can enable or disable the TELNET client function.

| TELNET Parameters | Using the TELNET client function |
|----------------------|-------------------------------------|
| on | permission |
| off | rejection |

The factory default value is "off".

- **Availability of SSH client function**

You can enable or disable the SSH client function.

| SSH parameters | Using the SSH client function |
|----------------|-------------------------------|
| On | permission |
| Off | rejection |

The factory default value is "off".

To set a security class, use the security class command.

For example, to set the security class level to "2" and enable the TELNET client, enter the following:

```
#securityclass2offon #  
save
```

You can check the security class settings using the show environment command.

```
> showenvironment  
:  
Security Class:2. FORGET:OFF, TELNET:ON  
:
```

10.5. Configuring for Management via SNMP

This product supports RFC1157 (SNMP) and RFC1213 (MIB-II).

By configuring the Simple Network Management Protocol (SNMP), you can use an SNMP manager to monitor and change network management information.

The SNMP settings are as follows:

| Command Name | explanation |
|--|--|
| <code>snmp community read-only</code> | Set the community name for the SNMP read-only access mode. |
| <code>snmp community read-write</code> | Set the community name for SNMP read/write access mode. |
| <code>snmp host</code> | Set the hosts that are allowed to access via SNMP. |
| <code>snmp syscontact</code> | Sets the MIB variable "sysContact". |
| <code>snmp syslocation</code> | Set the MIB variable "sysLocation". |
| <code>snmp sysname</code> | Set the MIB variable "sysName". |
| <code>snmp trap community</code> | Set the community name for sending traps. |
| <code>snmp trap host</code> | Sets the trap receiving host. |

ATTENTION

If you change the community name, set a character string that is different from the user password and admin password. The community name is set to "public" as the factory default.

NOTICE

- A group that exchanges information using SNMP is called a community. There are two access modes between communities: read-only and read-write.
- The SNMP message that notifies the status of this product is called a trap.

When shipped from the factory, access to this product via SNMP is not permitted. You can use the `snmp host` command to set the hosts that are allowed access.

For example, to allow access from all hosts and set the IP address of the host that will receive traps to "192.168.112.25", set it as follows:

```
# snmp host any
# snmp trap host 192.168.112.25
# save
```

10.6. Status Display

You can use the **show** command to check the status of this product.

Use this command when you need to check the product's status or resolve a problem during operation.

| Display items | Command Name | explanation |
|--|-------------------------|--|
| Viewing Resource Usage | show environment | Displays the resource usage of this product. |
| Viewing the ARP table | show arp | Displays the ARP table held by this product. |
| Displaying SYSLOG | show log | Displays logs regarding operation status and communication. |
| IP routing information table | show ip route | Displays the IP routing information table. |
| Displaying LAN side status | show status lanN | Displays the LAN side MAC address, MTU, and communication statistics. |
| Displaying the status of a USB-connected data communication terminal | show status wan1 | Information on communication via USB-connected data communication terminals Displays the IP address and MTU. |
| Display the status of each destination | show status pp N | Displays the status of the specified contact, whether it is currently connected or the last time it was connected. |

10.7. Using External Memory

By connecting an external memory to this product, the following functions are available.

- [10.7.1, "Copying the firmware from an external memory device to this product"](#)
- [10.7.2, "Copying Configuration Files Between the Product and External Memory"](#)
- [10.7.3, "Saving the Product's SYSLOG to an External Memory"](#)

NOTICE

External memory used with this product must be formatted in FAT or FAT32 format.

10.7.1. Copying Firmware from External Memory to this Product

Copy the firmware stored in the external memory to the non-volatile memory of this product.

If multiple firmware versions are stored in the non-volatile memory of this product, you can use any firmware version to operate this product.

It can be started. This is useful when you want to try out new firmware temporarily.

1. Connect the external memory to the microSD slot or USB port of this product.
2. **Use the `copy exec` command to copy the firmware stored in the external memory to the non-volatile memory of this product.**
 - To copy the firmware "rt_firmware.bin" stored on external memory to the non-volatile memory of this product, enter the following on the product console.

For micro SDHC cards:

```
# copy exec sdl:rt_firmware.bin0
```

For USB memory:

```
# copy exec usbl:rt_firmware.bin0
```

3. Press the Enter key.

- The firmware stored in the external memory will be copied to the non-volatile memory of this product.

4. Press and hold the microSD button or USB button on the front of the product for more than 2 seconds.

Wait until the indicator for the relevant external memory goes out before removing the external memory.

NOTICE

- To use the copied firmware, restart the product using the power switch or the restart command.
- If multiple firmware files are stored in the non-volatile memory of this product, see "6.1.2, "Selecting the Firmware and Configuration File to Use and Starting Up"" for the startup procedure.
- Instead of steps 2 and 3, you can also copy by pressing and holding the microSD button or USB button and the DOWNLOAD button simultaneously for 3 seconds. Once copying is complete, the product will automatically restart.

10.7.2. Copying Configuration Files between this Product and External Memory

Copies configuration files between this product's non-volatile memory and external memory.

If you save multiple setting files in the non-volatile memory of this product, you can start the product using any setting file. This is useful when a problem occurs with the product settings and you want to start the product with the configuration file before the problem occurred.

1. Connect the external memory to the microSD slot or USB port of this product.
2. Use **"copy config"** command to copy configuration files between external memory and the product's non-volatile memory.
 - To copy the configuration file "rt_config1.txt" saved in external memory to the non-volatile memory of this product as configuration file "0", enter the following in the console.

For microSDHC cards:

```
# copy config sdl:rt_config1.txt0
```

For USB memory:

```
# copy config usb1:rt_config1.txt0
```

- To copy the configuration file "0" stored in the non-volatile memory of this product to the external memory as the configuration file "rt_config1.txt", enter the following in the console.

For microSDHC cards:

```
# copy config 0sdl:rt_config1.txt
```

For USB memory:

```
# copy config 0usb1:rt_config1.txt
```

3. Press the Enter key.

- The configuration file will be copied to the product's non-volatile memory or external memory.

4. Press and hold the microSD button or USB button on the front of the product for more than 2 seconds.

Wait until the indicator for the relevant external memory goes out before removing the external memory.

NOTICE

- To use the copied configuration file, restart the product using the power switch or the restart command.
- If you have saved multiple configuration files in the non-volatile memory of this product, see "6.1.2, "Selecting the Firmware and Configuration File to Use and Starting Up"" for the startup procedure.
- Instead of steps 2 and 3, you can also copy by pressing and holding the microSD button or USB button and the DOWNLOAD button simultaneously for 3 seconds. Once copying is complete, the product will automatically restart.

10.7.3. Save the SYSLOG of this Product to an External Memory

Save the SYSLOG of this product to external memory.

If a problem occurs with this product, loading the SYSLOG saved in the external memory onto a PC can help resolve the problem.

stand.

1. Connect the external memory to the microSD slot or USB port of this product.
2. Use “**external-memory syslog filename**” command to set the file name of the SYSLOG to be saved in the external memory.
 - If you want to name the SYSLOG file "rt_syslog.log", enter the following in the console.

For micro SDHC cards:

```
# external-memory syslog filename sd1:rt_syslog.log
```

For USB memory:

```
# external-memory syslog filename usb1:rt_syslog.log
```

- The SYSLOG of this product will be saved in the external memory as "rt_syslog.log".
- From then on, the SYSLOG of this product will continue to be saved to the external memory until you stop saving the SYSLOG.

NOTICE

- In the factory default state,
- When the size of the SYSLOG file stored in the external memory reaches its upper limit, the SYSLOG file will be rotated (backed up). For more information, see the Command Reference (website).

10.8. Operations to Remember

This section describes operations that can be performed to make managing your machine easier, and operations that are useful if a problem occurs.

- [10.8.1, "Terminating a Communication Without Changing the Destination Information"](#)
- [10.8.2, "Setting the timer for connecting and disconnecting the cellular line"](#)
- [10.8.3, "Monitoring communication costs"](#)
- [10.8.4, "Checking SYSLOG"](#)

10.8.1. Terminating Communication Without Changing the Destination Information

This product automatically connects and disconnects the line based on the destination information. If maintenance is required, you can disable connections to specific destinations without changing the settings. To disable a connection, you can:

Restricting calls to and from specified destinations

By using "**pp disable**" command, you can prohibit calls from and to the specified number. For example, to apply "**pp disable**" command to destination information number 2, set it as follows.

```
# pp disable2
```

10.8.2. Set a Timer for Connecting and Disconnecting your Mobile Phone Line

You can set various timers for connecting and disconnecting mobile phone lines for each contact information.

| Timer Type | Command Name | explanation |
|----------------------------|--------------------------------------|---|
| Disconnection Timer | Mobile disconnect time | If there is no data being sent or received from the PP side, the line will be disconnected after this timer has elapsed. The factory default value is "60 seconds." |
| Input Disconnection Timer | mobile disconnect input time | If no data is received from the PP side, the line will be disconnected when this timer expires. The factory default value is "120 seconds." |
| Output Disconnection Timer | mobile disconnect output time | If no data is being sent to the PP side, the line will be disconnected when this timer expires. The factory default value is "120 seconds." |
| Forced Disconnect Timer | Mobile access limit time | Limits the maximum time you can connect to a peer. When this timer expires, the connection will be forcibly disconnected regardless of the communication status. |

| | | |
|---|-----------------------------------|---|
| Disconnection due to packet communication limit | Mobile access limit length | When the cumulative data length of packets being sent and received reaches the upper limit, the connected line will be forcibly disconnected regardless of the communication status. The factory default value is "50 MB". |
|---|-----------------------------------|---|

For more information, see the Command Reference (website).

10.8.3. Monitor Communication Costs

You can monitor your communications costs using “**show account**” command.
If you want to monitor communication costs over a certain period of time, use “**clear account**” command to clear the accumulated amount when you start monitoring.

10.8.4. Check the SYSLOG

By using the SYSLOG function, you can check information about filtered packets and the operation status of various functions.

There are three types of logs that are output to SYSLOG: You can set whether or not to output each type.

| type | Information gained | Command Name | Factory default value |
|--------|---|----------------------|-----------------------|
| NOTICE | Filtered packet information, etc. | Syslog notice | off |
| INFO | Operation status of various functions, etc. | syslog info | on |
| DEBUG | Debugging information | syslog debug | off |

Check the SYSLOG currently being output

For example, if you want to temporarily check the DEBUG type SYSLOG, follow the steps below.

1. Use “**clear log**” command to clear past SYSLOG.

```
# clear log
```

2. Use “**syslog debug**” command to set the output of DEBUG type SYSLOG.

```
# syslog debug on
```

3. Check the newly output SYSLOG using “**show log**” command.

```
# show log
```

4. Use “**no syslog debug**” command to revert the setting to not output DEBUG type SYSLOG.

```
# no syslog debug
```

Transferring SYSLOG

The SYSLOG of this product can be transferred to a SYSLOG host that has a SYSLOG function.

This is useful when you want to record a large amount of communication logs over a long period of time.

To specify the destination for the SYSLOG, use “**syslog host**” command.

For example, if the IP address of the SYSLOG host is "192.168.112.25", set it as follows:

```
# syslog host 192.168.112.25
# save
```

10.9. When the ALARM Indicator Lights up

If the ALARM indicator on the front of the product lights up red while the product is operating, it may be due to the following reasons.

Please check the status of this product and refer to the link for the relevant item.

| Product status | | Reason why the ALARM indicator is lit |
|---------------------------|---|--|
| The buzzer is ringing | LINK/DATA indicators for all LAN ports and SFP+ slots and the SPEED indicator is flashing green | The internal temperature of this product has risen and the hardware protection function has been activated. (→ 10.9.1, “Hardware Protection Function”) |
| | No LINK/DATA or SPEED indicators are flashing green | An abnormal fan stop was detected. (→ 10.9.2, “Fan Stoppage”) |
| The buzzer is not ringing | | An abnormality was detected in the temperature sensor. (→ 10.9.3, “Temperature sensor error”) |

10.9.1. Hardware Protection

The hardware protection function is a function that promotes internal cooling if the internal temperature of this product becomes extremely high.

This will prevent the product from breaking down or catching fire.

When the hardware protection function is activated, the operation of this product will change as follows:

- Turn the fan speed to maximum
- Shut down all LAN ports and SFP+ slots to cut off communication.
- The hardware protection function will be notified by the following method.
 - The LINK/DATA indicator and SPEED indicator for all LAN ports and SFP+ slots flash green.
 - The ALARM indicator lights up red.
 - The buzzer sounds at regular intervals

ATTENTION

The above operation will continue even if the temperature inside the unit drops after the hardware protection function is activated. If you restart the product or set the POWER switch to STANDBY, the operation that was activated will be canceled.

What to do when the hardware protection function is activated

Restart the product or set the POWER switch to STANDBY.

Also, please review the installation environment of this product to ensure that the internal temperature of the product is appropriate. If the hardware protection function is still activated, immediately stop using the product and be sure to ask the retailer where you purchased it to repair or inspect it.

10.9.2. Abnormal Fan Stop

If an abnormal fan stop is detected, the product will notify you by the following methods:

- The ALARM indicator lights up red.
- The buzzer sounds at regular intervals
- A warning is displayed on the Live screen of the Web GUI dashboard to notify of fan abnormalities.

NOTICE

- Once the fan is running again, all of the above notifications will be cleared.
- You can also check the fan status using **"show environment"** command.

```
> show environment
:
FAN1: OK (low speed)fan2: OK (low speed)
```

What to do when the fan stops working

Check to see if any foreign objects are preventing rotation.

If no foreign objects or other causes can be found, the fan itself may be faulty. Immediately discontinue use

Please stop using the product and be sure to ask the store where you purchased it to repair or inspect it.

10.9.3. Temperature Sensor Abnormality

If a temperature sensor abnormality is detected, the operation of this product will change as follows:

- Turn the fan speed to maximum
- The ALARM indicator lights up red.

What to do when an abnormality occurs in the temperature sensor

The temperature sensor may be faulty. Stop using the product immediately and be sure to have it repaired at the store where you purchased it.

Please request an inspection.

10.10. Checking the Communication Status with the STATUS

Indicator

If various keep-alive functions are enabled and a constant connection is established with the destination device, you can check the communication status with the destination device on the product's STATUS indicator.

If the STATUS indicator is lit orange, communication with the connected device is not possible. Please check for any line failures or malfunctions in the communication devices that make up the network.

When communication with the connected device is restored, the STATUS indicator will turn off.

ATTENTION

The keep-alive function requires a certain amount of time to detect a state in which communication is not possible. Therefore, even if the STATUS indicator is not lit, communication with the connected device may not be possible.

NOTICE

The STATUS indicator will also light up if you use the DOWNLOAD button to update the firmware. For details, see "10.3.1, 'Revision Up Using the DOWNLOAD Button'".

10.11. Using the EEE Function

This product supports EEE (Energy Efficient Ethernet).

- 10BASE-Te
- 100BASE-TX/1000BASE-T/2.5GBASE-T/5GBASE-T/10GBASE-T (LPI)

NOTICE

- The EEE function is disabled in the factory default setting.
- To use the EEE function, devices connected to the LAN port must also support the EEE function.

To enable EEE, set it as follows:

- To set LAN port 1 to 10BASE-Te:

```
# lan port type 1 10-hdx energy-saving=on
# save
```

- To set LAN port 1 to LPI:

```
# lan port type 1 auto energy-saving=on
# save
```

ATTENTION

When the EEE function is enabled, communication may not be possible depending on the connected device. If communication is not possible, disable the EEE function.

11. appendix

11.1. Customer Support (Support Policy)

Yamaha Corporation will provide support to help you use this product comfortably and to get the most out of its performance and functions. For more information, please see our support policy.

<https://network.yamaha.com/support/policy/>

Please use your browser's translation feature to check.(The page is in Japanese.)

11.2. Information on open source software

The firmware for this product contains open source software. You can check the copyright information and terms of use for each open source software using the following command.

```
> show copyright detail
```