

RTX810

Gigabit VPN Router



Instruction Manual

Thank you for purchasing the Yamaha RTX810.
Please carefully read this manual before use to ensure appropriate installation and configuration.
Please be sure to follow all the warnings and precautions provided in this manual to ensure appropriate and safe use.
Please retain this manual in a safe place for future reference.

Please ensure to read this first.

Thank you very much for purchasing the Yamaha RTX810.

This product is a Gigabit VPN Router that is suitable for use in small- and medium-sized enterprise networks.

Please ensure you have all the following accessories.

- LAN cable (x1)
- Please ensure to read this first.
- CD-ROM (x1)

Main content of this manual

Information regarding preparation for connecting to a network

- Making preparations..... Page 16

Information on connecting to a network

- Connecting to the Internet..... Page 32
- Implementing site-to-site VPN connections Page 57

Information necessary for daily operations management

- Operating and managing the product Page 116

Information on solving issues or problems if any occur

- Troubleshooting..... Page 139

Information on maximizing use of the product

- Enhancing security Page 92
- Maximizing use of the product Page 102

Please also ensure to refer to all the other instruction manuals.

This manual only contains information on using basic functions.

Please refer to the following manuals/Help content according to necessity.

- Command reference manual (CD-ROM): Provides detailed configurations available via console commands.
- Help on the “Basic configuration page”: Provides detailed explanations on the configurable items of each setting screen. Please click “Help” on the “Basic configuration page”.

Table of contents

Please ensure to read this first	2
Particular usage in this manual.....	5
Safety precautions.....	5
Important notice	8
Concerning software license contracts when using the DOWNLOAD button	10

Chapter 1 Introduction

What the product enables you to do.....	12
Name and function of individual parts	13
Front panel/Top panel	13
Rear panel.....	15
Bottom panel	15

Chapter 2 Making preparations

Flow of preparation steps	16
Ensure the following are available before beginning preparations.....	17
Cautions when installing the product.....	17
Preparation 1: Making connections	18
Preparation 2: Opening the “Basic configuration page”	20
Preparation 3: Setting the passwords.....	22
Preparation 4: Setting date and time	27
Preparation 5: Configuring the IP address on the LAN side.....	29
Preparation 6: Changing the IP addresses of PCs in LAN	31

Chapter 3 Connecting to the Internet

Selecting your Internet connection mode	32
Permanently connecting to the Internet through a broadband line (PPPoE/CATV).....	33
Permanently connecting to the Internet using network connection service.....	43
Connecting to the Internet using a USB data communi- cation terminal.....	49

Chapter 4 Implementing site-to-site VPN connections

Creating a Virtual Private Network (VPN) using IPsec (IPsec LAN-to-LAN connection).....	57
Gaining remote access using L2TP/IPsec	61
Gaining remote access using PPTP.....	70
Creating a Virtual Private Network (VPN) using PPTP (PPTP-LAN-to-LAN connection).....	84
Linking LANs together through IPsec tunnels using a closed network.....	88

Chapter 5 Enhancing security

Outline of unauthorized accesses and security measures	92
Configuring the filter settings.....	94
Detecting unauthorized accesses and warning about them	98
Restrict hosts that can change product settings	100

Chapter 6 Maximizing use of the product

Using a service requiring a global IP address within LAN.....	102
Using the netvolante DNS service	104
Publishing a server.....	106
Using mail notification	108
Using in the IPv6 environment	110
Changing the operation settings of UPnP function	112
Controlling Yamaha switches.....	115

Chapter 7 Operating and managing the product

Changing the product settings.....	116
Types of configuration methods available	116
Configuring setting with console commands.....	117
Using the console port.....	121
Using an external memory device.....	123
Operating the product using a configuration file in an external memory device	125
Changing the buzzer settings	126
Checking the communication status with the STATUS lamp.....	127
Using the latest function (Revision up)	128
Checking the configuration information and log of the product	133
Customizing the operation according to your environment (Lua script/Custom GUI).....	137
Lua scripts.....	137
Custom GUI	138

Chapter 8 Troubleshooting

When a problem is suspected.....	139
Q1: Lamps are off.....	140
Q2: Setting failed with the “Basic configuration page”	142
Q3: Internet connection cannot be established.....	144
Q4: VPN communication cannot be established	146
Q5: The DOWNLOAD button does not function	151
Q6: Unable to use USB device	152
Q7: Other problems	154
Communication charges of the USB data communication terminal is abnormal.....	155
Initializing the product settings	159
If you have forgotten the password.....	161

Chapter 9 Annex

Major specifications.....	162
Changing the IP addresses of PCs.....	163
Instructions on transferring/disposing of the product	166
License terms and conditions	167

Particular usage in this manual

Abbreviations

The following company and product names will be abbreviated as below in this manual.

- Yamaha RTX810: The product
- Microsoft® Windows®: Windows
- Microsoft® Windows® 7: Windows 7
- Microsoft® Windows Vista®: Windows Vista
- Microsoft® Windows® XP: Windows XP
- 10BASE-T/100BASE-TX/1000BASE-T cable: LAN cable

Concerning example settings

The examples of setting IP addresses, domain names, URLs and so on that are contained in this manual are provided for explanation. Be sure to use those provided by your ISP (Internet service provider) when setting them.

Concerning detailed technical information

Detailed knowledge of the Internet and networks may be required to fully utilize this product. The attached manual does not describe any such information and hence you will need to refer to a commercially available guidebook or other appropriate materials for more details.

- No part of this document may be copied or used in any form without prior permission from Yamaha.
- The content of this manual, specifications of the product and “Basic configuration page” are subject to change for the sake of improvement without notice (this manual is based on information available as of March 2013).
- Yamaha cannot accept any liability for any loss of or damage to information resulting from any use of the product. Please also note that the warranty only covers physical damage to the product.

Safety precautions

Please ensure to carefully read and observe the following precautions in thereby ensuring safe use of the product.

The precautions provided on pages 5 to 9 concern safe and appropriate use of the product and on preventing any risk to you and other people as well as any physical damage. Please ensure to retain it somewhere anyone using the product can access at any time after having first thoroughly read it.

1. This product is intended for use in general offices and was not designed for use in any fields requiring a high degree of reliability in the handling of human lives or valuable assets.
2. Please note that Yamaha cannot accept any liability for any losses or damages resulting from improper use.
3. Please ensure to immediately remove the power cord from the outlet in any of the following cases. Failure to observe this may result in fire or an electric shock. Please ensure to request the dealer concerned to carry out any necessary repairs or inspections.
 - Any abnormal odor or noise occurs;
 - Smoke is emitted;
 - The product is broken; or
 - The product has been exposed to water.
4. Do not handle the product or the power cord with wet hands. Failure to observe this could result in electric shock or damage to the product.
5. Do not insert any metal, paper, or foreign objects into any of the gaps in the panel. Failure to observe this could result in fire, electric shock, or damage to the product.
6. Do not disassemble or alter this product in any way. Failure to observe this could result in fire, electric shock, or damage to the product.
7. Ensure not to damage the cable. Failure to observe this could result in fire, electric shock, or damage to the product.
 - Ensure not to place any heavy objects on the cable.
 - Ensure not to process the cable in any way.
 - Ensure not to use any staples to fix the cable in place.
 - Ensure not to apply excessive force to the cable.
 - Ensure to keep the cable away from anything hot.

Safety precautions (Continued from the previous page)

8. Ensure to only use the specified power supply voltage. Use of any different power supply voltage, for example overseas voltage, could result in damage to the product.
9. Connect the power plug to an outlet that you can see and reach in thereby ensuring that you can easily remove it if the necessity arises.
10. Ensure to fully and securely insert the power plug into the outlet. Being insufficiently inserted could result in an electric shock. It could also lead to dust accumulating on the plug, which could then result in heat or fire.
11. Verify that the current capacity of the outlet or a power strip in thereby ensuring that use of the product does not exceed it. Any overheating or degradation of the power strip could result in fire.
12. Ensure to only use cables that suit the specifications of the port concerned. Connecting any cable other than which fits the originally intended specifications could result in fire or damage to the product.
13. Ensure not to touch any of the ports with your fingers or anything metallic. Failure to observe this could result in electric shock or damage to the product.
14. Ensure the product does not fall or be subjected to strong impact. The internal parts could break, which could then result in electric shock, fire, or damage to the product.
15. Do not install the product anywhere where it will be exposed to dust or humidity, oily smoke or steam, or corrosive gases. Failure to observe this could result in fire, electric shock, or damage to the product.
16. Ensure adequate heat ventilation. Failure to observe this could result in fire or damage to the product.
 - Ensure not to cover the product with a cloth or tablecloth.
 - Ensure the product does not get pushed into a narrow, poorly ventilated place.
 - Ensure the ventilation holes do not get blocked.
17. Ensure not to touch the product or the power cable if you hear thunder. Failure to observe this could result in electric shock.
18. Periodically remove any dirt and dust from the power cable. Failure to observe this could result in fire.
19. Be sure not to install the product in an unstable location or where it will be exposed to vibrations as it could fall over or turn upside down, thus resulting in injury or damage to the product.
20. Be sure not to install the product anywhere where it will be exposed to direct sunlight or extraordinarily high temperatures (near a heater, etc.). Failure to observe this could result in damage to the product.
21. Be sure not to use the product anywhere where it will be exposed to rapid changes in ambient temperature. Any rapid change in ambient temperature could result in condensation on the product, which could then result in damage to the product. Ensure to leave the product for a while until it has dried off with the power turned off if any condensation has occurred.
22. Ensure not to stack the product with other equipment. Failure to observe this could cause heat to build up and damage to the product.
23. Ensure not to connect any cables while the power is turned on. Failure to observe this could result in damage to the product and any connected equipment.
24. Ensure to earth any static electricity from your body or clothing before touching the product. Failure to observe this could result in damage to the product.
25. Connecting a USB data communication terminal to the USB port of the product will enable a wireless WAN connection via the 3G mobile phone network. Even if the data communication terminal contract is a flat-rate system any use of it with an improper configuration could be charged for under the measured-rate system. Please note that Yamaha cannot assume any responsibility for any losses resulting from improper use or configuration of the product.
26. Please note that the USB port and microSD slot of this product will not necessarily support all types of USB memory sticks and microSD cards.
27. Operation of USB memory sticks and microSD cards can be verified from the “Basic configuration page” – “Advanced settings” – “Configure external device” screen – “Test performance of external memory”. Please refer to the following URL for more details on

- the supported USB memory sticks and microSD cards.
<http://www.yamaha.com/products/en/network/>
28. It is recommended that any data on a USB memory stick or microSD card be periodically backed up. Please note that Yamaha cannot assume any responsibility for any damage resulting from the loss or destruction of data during usage of the product.
 29. Please note that Yamaha cannot assume any responsibility for any damage resulting from improper use or configuration of the product.
 30. Ensure not to install the product anywhere it will be exposed to any strong magnetic force.
 31. Do not connect any equipment that generates any noise on the same power line as the product.
 32. Use of the product can result in noise being generated in telephones, radios, and TVs. If any noise does occur then please change the place or direction in which the product is installed.
 33. If you transfer the product you will also need to transfer the instruction manuals.
 34. A lithium battery is used in the product as a power backup for the clock function. Ensure to follow the instructions of your local government when disposing of the battery.
 35. When transferring/disposing of the product please be sure to read the “Instructions on transferring/disposing of the product” (page 166) in this manual and perform the following.
 - (1) Delete the netvolante DNS registration.
 - (2) Initialize all the configurations.
 36. Ensure to follow the instructions of your local government when disposing of the product.
 37. A 1000BASE-T connection will require an Enhanced Category 5 (CAT5e) or better LAN cable.

Important notice

Concerning the security measures and firewall functionality of the product

The Internet is a convenient tool that can be used to collect information available anywhere in the world on websites and to exchange messages via e-mail. However, it does include the risk of unauthorized access to your PC.

When you maintain a constant connection to the Internet or have a server in place, in particular, you need to understand the risk of unauthorized access and utilize security measures. The product is equipped with a firewall function as a security measure but new unauthorized access methods and loopholes (security holes) are constantly being discovered and thus no completely infallible prevention method exists. We would like you to understand that an Internet connection always includes risk and thus strongly recommend that you constantly obtain the latest information and implement security measures as your own responsibility.

Concerning billing

When the product is used with a measured-rate line service (for example: the 3G mobile phone network) please ensure that you thoroughly understand the auto-outgoing call function prior to use. Whenever the product is connected to the Internet or a LAN it monitors all the data sent by the software on your PC (for example: e-mail software or Web browser) and the addresses of the data being transferred via the LAN. The inclusion of any other address than from the LAN can result in auto-outgoing calls to the line taking place in accordance with the preset configurations.

If an incorrect configuration is set or you forget to disconnect the line the software or equipment may send periodic packets which can then result in unexpected communication charges and/or provider connection fees.

Please ensure to check the communication record and verify whether any unintended communications have taken place. In addition, it is strongly recommended that you periodically check the Yamaha network peripheral equipment website (<http://www.yamaha.com/products/en/network/>) to obtain the latest information on the configurations and revisions of the product.

Unexpected communication charges may occur when you:

- start using the product;
- change any provider connection settings of the product;
- install new software on your PC;
- connect to the network with a new PC, network equipment, or peripheral equipment;
- update the firmware of the product; or
- perform any different operations than usual or sense a difference in the communication response.

Note

- After canceling/changing your provider contract please be sure to delete or reconfigure the connection configuration of the product. Failure to observe this could result in unexpected charges from your telephone carrier or provider.
- Unexpected communication charges could occur according to the status (change in access point, maintenance, error, etc.) of the provider side. Please ensure to pay constant attention to any notifications you receive from your provider.

Control of the cumulative access period of the product

When the product is connected to a measured-rate line service (for example: the 3G mobile phone network) outgoing restrictions can be set that are based on accumulative send/receive data and the cumulative connection period. This function is based on accumulative send/receive data and cumulative connection period calculated by the product and will not necessarily correspond to the different billing calculation methods used due to factors such as service discounts and communication period calculation methods that are unique to the provider concerned.

The outgoing restriction function may not therefore always work as intended in actual use. If greater accuracy is required you will need to conduct tests over a certain period of time to check for any discrepancies.

Concerning trademarks

- All the company and product names used in this manual are registered trademarks or trademarks of the companies concerned.
- This product is equipped with RSA® BSAFE™ software of RSA Security Inc. RC4 and BSAFE are the registered trademarks of RSA Security Inc. in the U.S. and other countries.



Open source software used in the product

- PCRE
- MT19937
- OpenSSL
- Original SSLeay
- Net-SNMP

Please refer to “License terms and conditions” (page 167) for more details on the pertinent license terms and conditions.

Concerning software license contracts when using the DOWNLOAD button

By changing the configuration of the product the DOWNLOAD button can be used to update its internal firmware.

Changing the setting to enable the revision update and performing a revision update by pressing the DOWNLOAD button means that you have thereby agreed with the software license contract (hereinafter referred to as “the contract”). Please ensure that you have read the contract before using it.

Ensure not to change the setting to permit firmware revision update via the DOWNLOAD button if you do not agree with this contract. Yamaha cannot assume any responsibility for any damages resulting from software or any other causes including negligence.

Please ensure to check the “Upgrading the firmware using the DOWNLOAD button” (page 128) for more details on using the DOWNLOAD button.

Please retain this manual in a safe place for future reference.

SOFTWARE LICENSE AGREEMENT

This License Agreement (the “AGREEMENT”) is a legal agreement between you and Yamaha Corporation (“YAMAHA”) under which YAMAHA is providing the firmware of YAMAHA’s router products (the “PRODUCT”) and related software program, documentation and electronic files (collectively, the “SOFTWARE”).

YAMAHA grants you a personal non-exclusive license to use the SOFTWARE only for purposes of running it on the PRODUCT. This AGREEMENT applies to the SOFTWARE which YAMAHA provides you and the installed copy thereof, subject to the provision of 1-1 herein, into the PRODUCT or personal computer owned by you.

1. GRANT OF LICENSE:

- 1-1. YAMAHA grants you a personal non-exclusive license to install the SOFTWARE and use the SOFTWARE on the PRODUCT or other devices, including but not limited to the personal computer, which you own.
- 1-2. You shall not assign, sublicense, sell, rent, lease, loan, convey or otherwise transfer to any third party, upload to a website or a server computer to which specified or unspecified persons may access, or copy, duplicate, translate or convert to another programming language the SOFTWARE except as expressly provided herein. You shall not alter, modify, disassemble, decompile or otherwise reverse engineer the SOFTWARE and you also shall not have any third party to do so.
- 1-3. You shall not modify, remove or delete a copyright notice of YAMAHA contained in the SOFTWARE.
- 1-4. Except as expressly provided herein, no license or right, express or implied, is hereby conveyed or granted by YAMAHA to you for any intellectual property of YAMAHA.

2. OWNERSHIP AND COPYRIGHT:

The SOFTWARE is protected under the copyright laws and owned by YAMAHA. You agree and acknowledge that YAMAHA transfers neither ownership interest nor intellectual property in the SOFTWARE to you under this AGREEMENT or otherwise.

3. EXPORT RESTRICTIONS:

You agree to comply with all applicable export control laws and regulations of the country involved, and not to export or re-export, directly or indirectly, the SOFTWARE in violation of any such laws and regulations.

4. SUPPORT AND UPDATE:

YAMAHA, YAMAHA's subsidiaries and affiliates, their distributors and dealers are not responsible for maintaining or helping you to use the SOFTWARE. No updates, bug-fixes or support will be made available to you for the SOFTWARE.

5. DISCLAIMER OF WARRANTY:

5-1. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5-2. IN NO EVENT SHALL YAMAHA, YAMAHA'S SUBSIDIARIES AND AFFILIATES, THEIR DISTRIBUTORS AND DEALERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS PROFITS, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS INTERRUPTION OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES) ARISING OUT OF THE SOFTWARE, USE THEREOF, OR INABILITY TO USE THEREOF EVEN IF YAMAHA, YAMAHA'S SUBSIDIARIES AND AFFILIATES, THEIR DISTRIBUTORS OR DEALERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

5-3. YAMAHA, YAMAHA'S SUBSIDIARIES AND AFFILIATES, THEIR DISTRIBUTORS AND DEALERS SHALL HAVE NO OBLIGATION TO INDEMNIFY YOU AGAINST ANY CLAIM OR SUIT BROUGHT BY A THIRD PARTY ALLEGING THAT THE SOFTWARE OR USE THEREOF INFRINGES ANY INTELLECTUAL PROPERTY OF SUCH THIRD PARTY.

6. TERM:

6-1. This AGREEMENT becomes effective upon your agreeing the terms and conditions herein and continues in effect unless or until terminated in accordance with the provision of 6-2 or 6-3 herein.

6-2. You may terminate this AGREEMENT by deleting the SOFTWARE installed into the PRODUCT.

6-3. This AGREEMENT will also terminate if you fail to comply with any of the terms and conditions of this AGREEMENT.

6-4. In case this AGREEMENT is terminated in accordance with the provision 6-3, you shall promptly delete the SOFTWARE.

6-5. Notwithstanding anything contains herein, Sections 2 through 6 shall survive any termination or expiration hereof.

7. SEPARABILITY:

In the event that any provision of this AGREEMENT is declared or found to be illegal by any court or tribunal of competent jurisdiction, such provision shall be null and void with respect to the jurisdiction of that court or tribunal and all the remaining provisions of this AGREEMENT shall remain in full force and effect.

8. U.S. GOVERNMENT RESTRICTED RIGHTS NOTICE:

The Software is a "commercial item," as that term is defined at 48 C.F.R. 2.101 (Oct 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users shall acquire the Software with only those rights set forth herein.

9. ACKNOWLEDGMENT:

You agree that this AGREEMENT is the complete and exclusive statement of agreement between you and YAMAHA concerning the subject matter hereof and supersedes all proposals or prior agreements, verbal or written, and any other communications between you and the parties relating to the subject matter hereof. NO amendment to this AGREEMENT shall be effective unless signed by a duly authorized representative of YAMAHA.

10. GOVERNING LAW:

This AGREEMENT shall be governed by and construed in accordance with the laws of Japan without reference to the principles of conflict of laws.

What the product enables you to do

The product is a Gigabit VPN Router that is equipped with a gigabit LAN port. In addition to CATV/ADSL/FTTH connections the product can also be used with various other types of Internet connections that include mobile Internet via a USB data communication terminal and the 3G mobile phone network.

Gigabit Ethernet and 3G mobile communication

The product is equipped with a WAN port that can be connected to FTTH, CATV, or ADSL broadband line modems. In addition, mobile Internet can also be utilized by connecting the USB port to a 3G mobile phone network data communication terminal.

Virtual Private Network with IPsec, L2TP, and PPTP

The product is compatible with IPsec, L2TP and PPTP, and data can thus be transferred more safely via the creation of a Virtual Private Network (VPN) that utilizes the Internet (broadband) connection.

Power OFF/Log Saving function

Rebooting the product can be performed as an emergency recovery operation in the case of any instability. The product shifts to wait status after saving the log in the memory to the internal non-volatile memory when the power is turned off, which can then be checked for the status before the power was turned off.

Easy operation

- The “Basic configuration page” included with this product for use with settings can be used to change the basic configurations of the product using the Web browser of your PC.
- Merely pressing the DOWNLOAD button enables revision updates (upgrade) of the internal firmware. If any new functions have been added after you have purchased the product they can be accessed via a revision update. In addition to directly downloading any firmware updates to the main unit you can also transfer them from a PC, USB memory stick, or microSD.

Compliance with various external memories

The configuration file and log of the product can be saved in commercially available USB memory sticks or microSD cards. In addition, the product can also be booted using firmware or a configuration file saved on a USB memory stick or microSD card.

Setting and management of Yamaha switches supported

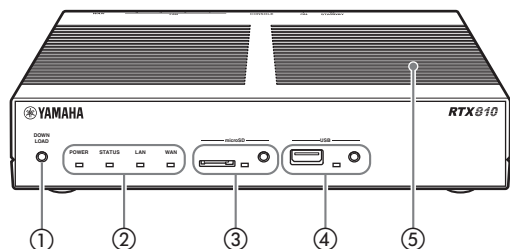
The product, in conjunction with proprietary Yamaha switches, can display the network configuration and port status on its “Basic configuration page”. In addition, individual port configurations of the Yamaha switches and collective VLAN settings both for the product and Yamaha switches are also available.

Wide range of content available from the Yamaha network peripheral equipment website

The Yamaha network peripheral equipment website (<http://www.yamaha.com/products/en/network/>) has a wide range of advanced usage examples and detailed explanations of Yamaha routers available.

Name and function of individual parts

Front panel/Top panel



① DOWNLOAD button

If the product was set to permit firmware revision updating via the DOWNLOAD button the firmware can be updated merely by pressing and holding down the button for three seconds. Please refer to “Using the latest function (Revision up)” (page 128) for more details.

② Lamps

The lamps indicate the operating status of the product. Please refer to the “Each lamp on the front panel indicates one of the three statuses” (page 14) for the relationship between the lamp light and the status of the product.

- **POWER:** Indicates the current power status of the product
- **STATUS:** Indicates whether communication with any connected equipment is active or not
- **LAN:** Indicates the usage status of the LAN port
- **WAN:** Indicates the usage status of the WAN port

③ microSD lamp/button/slot

Commercially available microSD cards can be used to copy the configuration file (pages 123 and 134), save the log file (page 133), and update the firmware (page 130).

Before ejecting the microSD card, be sure to first cancel the connection by pressing and holding down the microSD button for two seconds.

Note

When reinserting a microSD card please ensure that it has first been completely ejected.

④ USB lamp/button/port

Connecting a commercially available USB memory stick enables the configuration file to be copied (pages 123 and 134), the log to be saved (page 133), and the firmware updated (page 130). In addition, communication can also take place via use of a 3G mobile phone line by connecting a USB connection data communication terminal (page 50).

Before removing any USB devices please be sure to cancel the connection by pressing and holding down the USB button for two seconds.

Note

Do not connect the USB memory slot with any other USB equipment than USB data communication terminals. Failure to observe this could damage the product.

⑤ Ventilator

This is a hole used to release the internal heat.

Name and function of individual parts (Continued from the previous page)

Each lamp on the front panel indicates one of the three statuses (●Lit
⊗Flashing ○Off)

POWER lamp

- The product is powered on.
- ⊗ The product is starting up immediately after the power switch is turned on or shutting down immediately after the power switch is placed in STANDBY position.
- The product is powered off or the power went out.

STATUS lamp

- Communication is disabled.
Refer to “When the STATUS lamp lights up” (page 127).
- Communication is enabled.

LAN lamp

- LAN is enabled.
- ⊗ Data is flowing through the LAN.
- LAN is disabled.

WAN lamp

- WAN is enabled.
- ⊗ Data is flowing through the WAN.
- WAN is disabled.

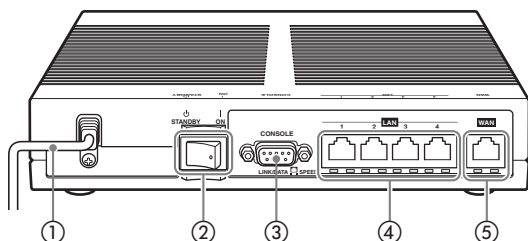
microSD lamp

- A microSD card is inserted into the microSD slot but the product is not accessing it.
- ⊗ The product is accessing the microSD card.
- No microSD card has been inserted into the microSD slot, or the microSD card inserted into the slot can be taken out.

USB lamp

- A USB memory stick is inserted into the USB port but the product is not accessing it.
 - ⊗ The product is accessing the USB memory stick.
 - A USB memory stick is not inserted into the USB port, or the USB memory stick inserted into the port can be taken out.
-

Rear panel



① Power cord

Power cord and plug shape vary depending on the destination.

② Power switch

This switches the power status of the product to ON/STANDBY.

③ Console port

For use in connecting the RS-232C terminals (serial connector) of PCs when it is necessary to perform configurations from the console. For more information, see “Using the console port” (page 121).

④ LAN ports

The LAN port is for use connections with the LAN port or hub port of a PC via a LAN cable.

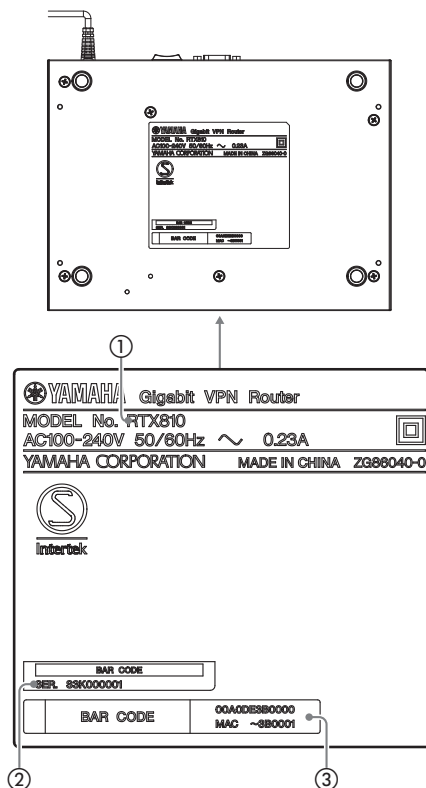
The power part of each LAN port includes a LINK lamp (left) and SPEED lamp (right).

- **Link lamp:** Off (link lost), lit up (link established), or flashing (transferring data) according to the individual status of the link concerned.
- **SPEED lamp:** Off (100BASE-TX/10BASE-T) or lit up (1000BASE-T) according to the speed of the connection.

⑤ WAN port

The WAN port is for connecting to a cable modem, ADSL modem, or ONU via a LAN cable.

Bottom panel



① Equipment name

Provides the equipment name of the product.

② Serial number

Provides the serial number used to manage/classify the product.

③ MAC address

Provides the individual network ID numbers unique to the equipment on the LAN side and WAN side. In the example of “00A0DE3B0000”, “MAC - 3B0001” provided in the figure above the individual MAC addresses on the LAN side and WAN side are as follows:

- MAC address on the LAN side: 00A0DE3B0000
- MAC address on the WAN side: 00A0DE3B0001

Flow of preparation steps

You must make preparations for using the product in this order:

Make the necessary preparations for configuring network connections.

Preparation 1

Connecting a PC (or PCs) and your broadband line to the product and powering it on

▶ Page **18**

Preparation 2

Opening the “Basic configuration page”

▶ Page **20**

Preparation 3

Setting the password of the product

▶ Page **22**

Preparation 4

Setting date and time

▶ Page **27**

Preparation 5

Configuring the IP address on the LAN side of the product

▶ Page **29**

Preparation 6

Changing the IP addresses of PCs in LAN

▶ Page **31**

Configuring network connections

Steps required for configurations depend on the connection mode. For details, refer to “Selecting your Internet connection mode”.

▶ Page **32**

Ensure the following are available before beginning preparations

LAN cables

Provide LAN cables based on the number of PCs and distance.

HUB

Up to four PCs can be directly connected to the LAN ports of the product. If you desire to connect five or more PCs, use a hub (a switch hub) that supports 10BASE-T, 100BASE-TX, or 1000BASE-T.

Information regarding the network to which the product is attached

Predetermine the IP address to be assigned to the LAN side of the product.

Note

To connect the product to a network that uses a DHCP server, you need to disable the DHCP server function of the product. For details, contact your network administrator.

Cautions when installing the product

Please carefully read and observe the “Safety precautions” on page 5 when installing the product.

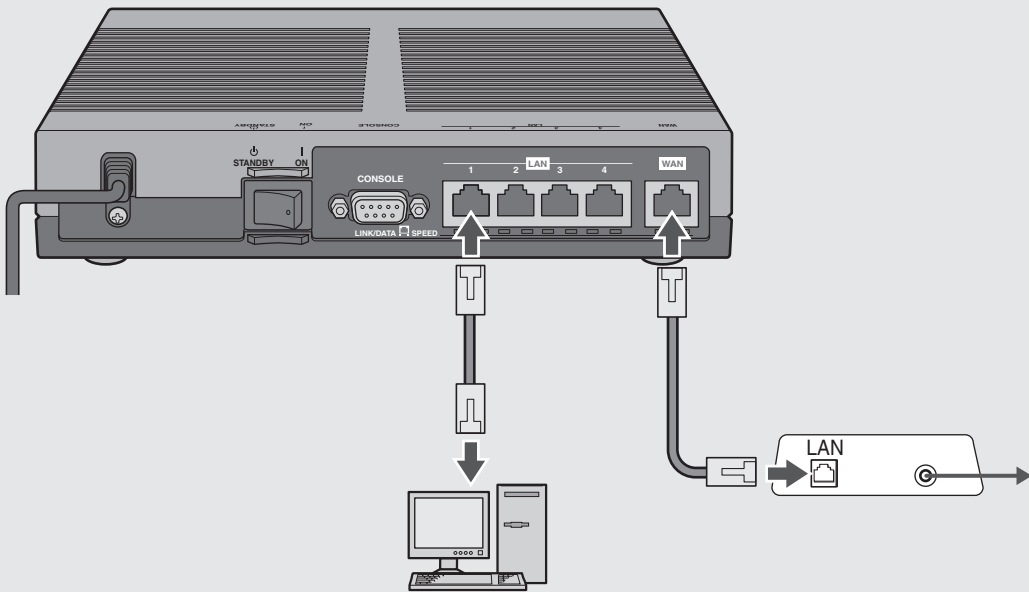
Preparation 1

2

Making connections

Tip

- To connect the product to the Internet through a USB data communication terminal, refer to “Connecting to the Internet using a USB data communication terminal” (page 49).



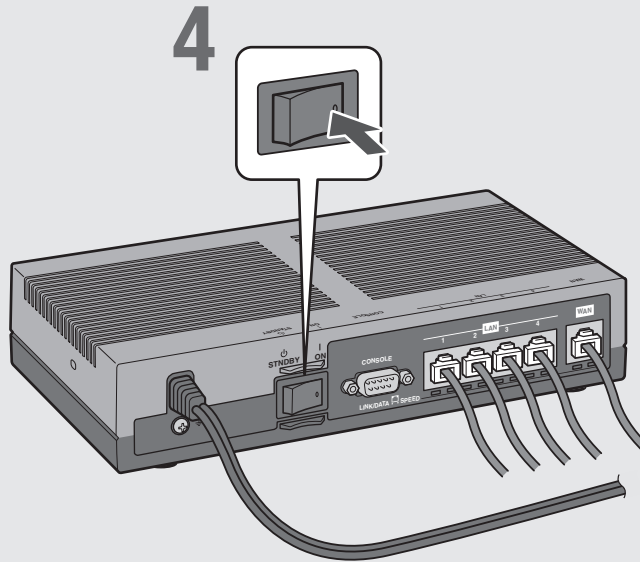
1 Connect the LAN port of your PC to one of the LAN ports of the product with a LAN cable.

2 Connect the LAN port of your cable modem, ADSL modem or ONU to the WAN port of the product with a LAN cable.

Please also refer to the document provided by your provider and instruction manuals for ADSL modem and ONU.

Note

If you switch an environment in which a cable modem, an ADSL modem, or an ONU is directly connected to a PC to a connection with the product, or an installed router is replaced with the product, proper connections may not be made because, for instance, addresses cannot be obtained. In some cases, you may need to configure some settings, to perform a reset, or to wait for a specified period of time (e.g., at least 20 minutes). For more information, follow the instructions in the relevant manuals.



3 Plug the power cord of this product into an electrical outlet.

4 Place the **POWER** switch in the **ON** position.

The **POWER** lamp lights up after flashing several times.

5 Power your **PC** or **hub**.

If the **LAN** and **WAN** lamps on the front panel light up or flash, the product is correctly connected to your **PC** or **hub**.

⚠ If the LAN lamp does not light up or flash:

- Check that the **LAN** cable is correctly connected and your **PC** or **hub** is powered on.
- No **LAN** lamps light or flash when all **PC**s and the **hub** connected the product are powered on.

⚠ If the WAN lamp does not light up or flash:

Check that the **ADSL** modem (or cable modem or **ONU**) is correctly connected to the product or the **ADSL** modem (or cable modem or **ONU**) is powered on.

Now, the connecting procedures are completed.
Proceed with other preparations.

▶ See page **20**

Opening the “Basic configuration page”

To change the configurations of the product, open the “Basic configuration page” using a Web browser on a PC connected to the product.

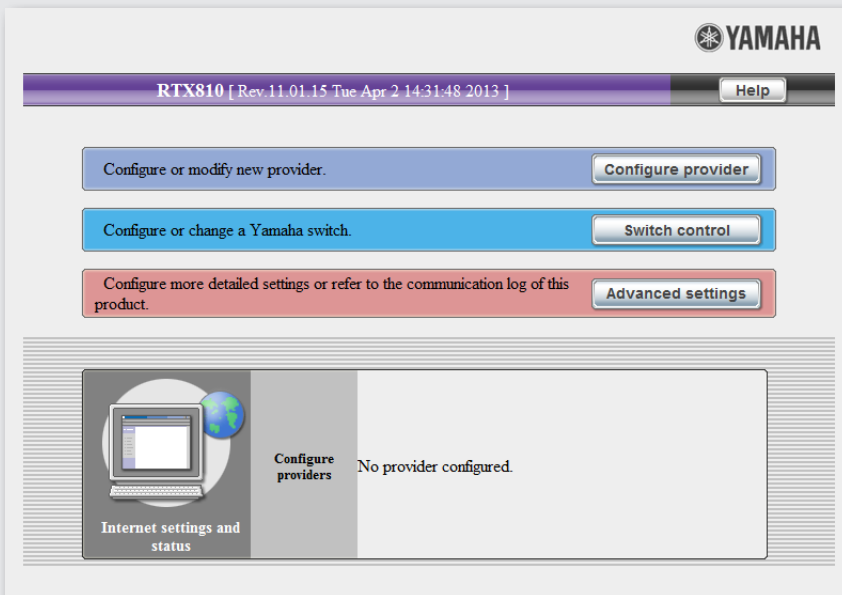
Follow the steps below to open the “Basic configuration page”.

Note

- To use the “Basic configuration page”, you need Windows Internet Explorer 8 or later.
- The descriptions in this manual use Windows 7 and Internet Explorer 9 screens as examples. For other environments, you have slightly different screen displays, though operations stay the same.

Tip

If you enter commands in a console window using Telnet software, you can configure settings in more detail compared to doing them in the “Basic configuration page” (console commands). For details on connecting to the product using Telnet software, please refer to page 118. For information on the commands available to the product, please refer to “Command reference” (included in the attached CD-ROM).



- 1 Check that the product is powered on.
- 2 Launch a web browser on your PC.
- 3 Type “http://192.168.100.1/” in the address bar and then press Enter.

The “Windows Security” screen appears.

- 4 Leave the “User name” and “Password” fields blank, and click “OK”.

The top page of the “Basic configuration page” appears.

Note

Enter user name and password if you have set them.

- ❗ If the top page of the “Basic configuration page” does not appear:

Refer to “Setting failed with the “Basic configuration page”” (page 142).

Understanding the “Basic configuration page”

The screenshot shows the 'Advanced settings' page for 'Configure machine'. The page has a breadcrumb trail: [Top] > [Advanced settings] > [Configure machine]. The main content area is divided into two sections: 'Configure date and time' and 'Configure buzzer'. The 'Configure date and time' section includes a checkbox for 'Change to the following date and time setting', a 'Manual configuration' section with input fields for year (2013), month (04), day (24), hour (01), minute (07), and second (22), a 'Contact NTP server' field, and an 'Auto adjustment via NTP server' section with a dropdown menu set to 'not use' and a time field set to '01 : 57'. The 'Configure buzzer' section includes a checked checkbox for 'Notify following status changes (notification conditions) using buzzer' and a 'Buzzer alert status' section with two checked checkboxes: 'Notify with buzzer the USB device status' and 'Notify with buzzer the micro SD device status'. At the bottom of the page are three buttons: 'Submit', 'Back', and 'Return to top'. Annotations with lines pointing to these elements provide the following descriptions:

- Configure machine**: Indicates the current screen name.
- Help**: Shows Help screen.
- Submit**: Accept your entries and save them in the product.
- Back**: Return to the previous page without saving your entries.
- Return to top**: Return to the top page without saving your entries.
- Advanced settings**: Configure the settings as needed.

Preparation 3

2

Making preparations

Setting the passwords

The factory default passwords are not set for the product. It is recommended that you set passwords to provide security measures. Once a password is set, anyone trying to access the product must enter it which makes it difficult for third parties to modify the configurations of the product.

The product has two passwords: administration password and login password. First, set the administration password and then set the login password.

YAMAHA
RTX810 [Rev.11.01.15 Tue Apr 2 14:31:48 2013] [Help](#)

Configure or modify new provider. [Configure provider](#)

Configure or change a Yamaha switch. [Switch control](#)

Configure more detailed settings or refer to the communication log of this product. [Advanced settings](#) **1 Click**

Configure LAN (IP address, DHCP server)	Configure
Configure machine(Date/Time, buzzer)	Configure
Configure users and access limits(HTTP, TELNET, SSH, SFTP)	Configure 2 Click
Configure external device	Configure

Advanced settings **Configure users and access limits** [Help](#)

[Top] > [Advanced settings] > [Configure users and access limits]

Configure user and password

Number of registered users: 0 [Configure](#)

Nameless user [Configure](#)

If you setup an admin password you will be prompted for it when logging onto Basic configuration.

Administration password: Retype the same again: **4 Fill in**

Encrypt and save the admin password

3 Fill in

SSH and SFTP server function

SSH and SFTP server function: use do not use

Allowable SSH usage hosts: Allow all

IP addressing: _____

Allowable SFTP usage hosts: Deny all

IP addressing: _____

Encryption algorithm:

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-cbc
- aes192-cbc
- aes256-cbc
- 3des-cbc
- blowfish-cbc
- cast128-cbc
- arcfour

Number of simultaneous users: 8

[Submit](#) **5 Click** [Back](#) [Return to top](#)

1 Click “Advanced settings” on the top page of “Basic configuration page”.

The “Advanced settings” screen appears.

2 Click “Configure” to the right of “Configure users and access limits(HTTP, TELNET, SSH, SFTP)”.

The “Configure users and access limits” screen appears.

3 Type the password of the product in “Administration password”.

Each password character entered is represented by a black dot.

4 Retype the password you entered in Step 3.

5 Click “Submit”.

The password you have set takes effect and a confirmation screen appears.

6 Click “Return to top”.

The “Windows Security” screen appears.

7 Type the password you entered in Step 3 in “Password” and then click “OK”.

The top page of the “Basic configuration page” reappears.

Set the login password of the product.



Tip

Leave “User name” blank.

The screenshots show the following steps:

- Click **Advanced settings** (8 Click).
- Click **Configure** for **Configure users and access limits** (9 Click).
- Click **Configure** for **Nameless user** (10 Click).
- Fill in the **login password** (11 Fill in).
- Retype the same password (12 Fill in).
- Click **Submit** (13 Click).

8

Click “Advanced settings” on the top page of “Basic configuration page”.

The “Advanced settings” screen appears.

9

Click “Configure” to the right of “Configure users and access limits(HTTP, TELNET, SSH, SFTP)”.

The “Configure users and access limits” screen appears.

10

Click “Configure” to the right of “Nameless user”.

The “Configure nameless user” screen appears.

11

Type the login password in “login password”.

Each password character entered is represented by a black dot.

12

Retype the login password you entered in Step 11.

13

Click “Submit”.

The password you have set takes effect and a confirmation screen appears.

14

Click “Return to top”.

The top page of the “Basic configuration page” reappears.

Preparation 4

Setting date and time

In the “Configure machine” screen, configure the date and time for the product.

2

Making preparations

The image shows a sequence of three screenshots from a Yamaha web interface, illustrating the steps to configure the date and time. The screenshots are connected by downward-pointing arrows.

Step 1: The first screenshot shows the main menu with three options: "Configure or modify new provider.", "Configure or change a Yamaha switch.", and "Configure more detailed settings or refer to the communication log of this product." The "Advanced settings" button is highlighted with a red box and a callout bubble labeled "1 Click".

Step 2: The second screenshot shows a list of configuration options. The "Configure machine(Date/Time, buzzer)" option is highlighted with a red box and a callout bubble labeled "2 Click".

Step 3: The third screenshot shows the "Advanced settings" page with the "Configure machine" sub-page selected. The "Configure date and time" section is highlighted with a red box and a callout bubble labeled "3 Check". The checkbox "Change to the following date and time setting" is checked.

Step 4: The "Manual configuration" section is highlighted with a red box and a callout bubble labeled "4 Fill in". The date and time fields are filled in: Year: 2013, Month: 04, Day: 24, Hour: 01, Minute: 07.

Step 5: The "Submit" button is highlighted with a red box and a callout bubble labeled "5 Click".

Step 6: The "Return to top" button is highlighted with a red box and a callout bubble labeled "6 Click".

1 Click “Advanced settings” on the top page of “Basic configuration page”.

The “Advanced settings” screen appears.

2 Click “Configure” to the right of “Configure machine(Date/Time, buzzer)”.

The “Configure machine” screen appears.

3 Select “Change to the following date and time setting” under “Configure date and time”.

4 Enter your local date and time.



Tip

To set the exact time, enter a time several minutes ahead and click “Submit” simultaneously with a time signal.

5 Click “Submit”.

A confirmation screen appears.

6 Click “Return to top”.

The top page of the “Basic configuration page” reappears.

To automatically set the time of the product:

Using a NTP (network time protocol) server on the Internet allows you to automatically set the time of the product.

Note

- Depending on the security settings on the product, you might not set a time using an NTP server on the product as well as on a PC within a LAN. To use an external NTP server, change the filter settings (page 96).
- If the firewall security level is set to 4 or 5 (static security filter), a response packet sent from an NTP server is discarded. Because of this, it is not possible to set a time. If this is the case, set the firewall security level to 6 or 7 (dynamic security filter) (page 96).

Preparation 5

2

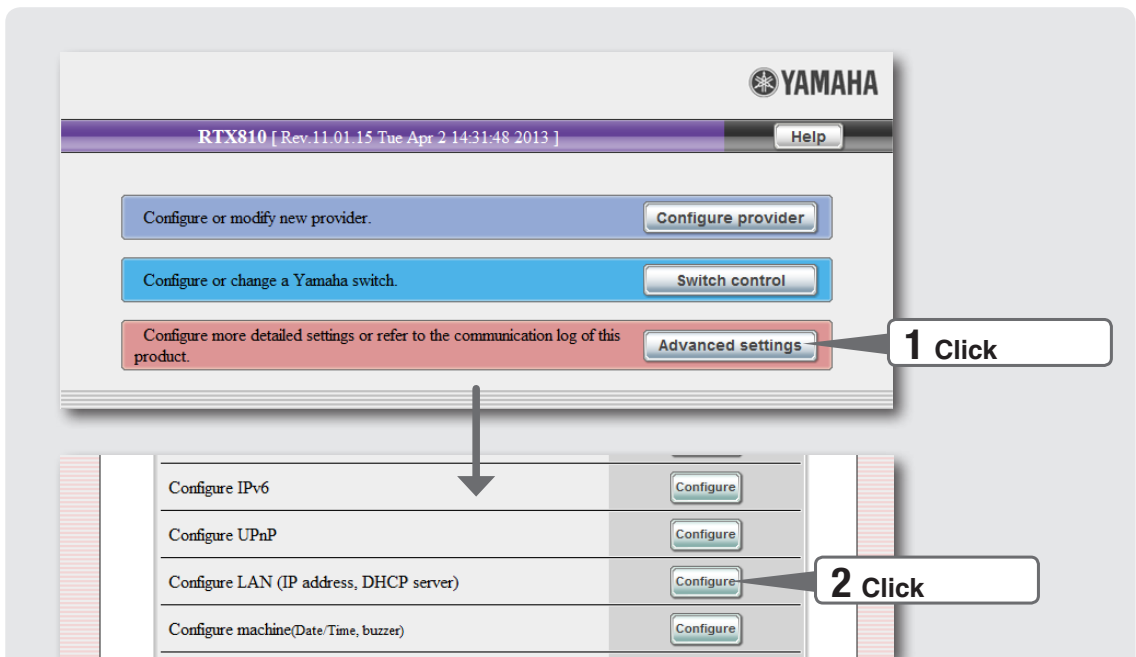
Making preparations

Configuring the IP address on the LAN side

To connect LANs at different locations via broadband connections, make sure the network addresses for LANs do not overlap. Determine a new network address for each LAN and configure the IP address and netmask according to the new network address on the product and PC.

Note

If a different network address has already been configured, give the product the IP address and netmask according to that network address. Make sure the product has the IP address that do not overlap with the one assigned to other device installed within the LAN.



1

Click “Advanced settings” on the top page of “Basic configuration page”.

The “Advanced settings” screen appears.

2

Click “Configure LAN (IP address, DHCP server)”.

The “Configure LAN” screen appears.

The screenshot shows the 'Configure LAN' page under 'Advanced settings'. It has three main sections: 'LAN port IP address setup', 'WAN port (LAN2) IP address setup', and 'DHCP server functions'. A 'Submit' button is at the bottom. Callouts indicate: '3 Fill in' pointing to the Primary IP address field, '4 Fill in' pointing to the DHCP server functions table, and '5 Click' pointing to the Submit button.

LAN port IP address setup

Primary IP address: 192.168.100.1 (255.255.255.0 (24 Bit)) DHCP client

Secondary IP address: [] (255.255.255.0 (24 Bit)) DHCP client

WAN port (LAN2) IP address setup

Use the WAN port (LAN2) as a LAN
 Do not use the WAN port (LAN2) as a LAN

DHCP server functions

Use DHCP server function

	Assigned IP address range	Netmask bit number	Delete	scope
1	192.168.100.2~192.168.100.191	255.255.255.0 (24 Bit)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	255.255.255.0 (24 Bit)	<input type="checkbox"/>	<input type="checkbox"/>

Submit

3

Enter the IP address on the LAN side of the product in “LAN port IP address setup”.

Primary IP address

Enter the IP address according to the new network address you determined, and select the netmask.

4

Enter the IP address you want to assign to a PC within the LAN in “DHCP server functions”.

Assigned IP address range

Entering “1” in identification number overwrites the setting.

Enter the range of IP addresses that do not overlap with the IP address of the product. Select the same value as the netmask of the product for the netmask bit number.

5

Click “Submit”.

A confirmation screen appears.

6

Click “Execute” before changing the IP addresses of PCs.

For information on changing the IP addresses of PCs, refer to the description on page 31 onward.

Changing the IP addresses of PCs in LAN

If you change a LAN network address, you also need to change IP addresses and netmasks of PCs in the LAN. If you have devices other than PCs in the LAN, you also need to change their IP addresses and netmasks. For information on setting these devices, please refer to their instruction manuals.

Note

If you do not change the network address of the LAN to which the product is attached, you do not need to change IP addresses of PCs in the LAN.

The way to change the IP address of a PC depends on the version of the operating system.

Please refer to “Changing the IP addresses of PCs” (page 163) for more details.

Selecting your Internet connection mode

The product supports different Internet connection modes. Necessary broadband contract or a contract with an Internet service provider varies depending on the connection mode. Please read instructions regarding connection modes.

Permanently connecting to the Internet through a broadband line ▶ Page **33**

Permanently connecting to the Internet using network connection service ▶ Page **43**

- Network PPPoE connection: Page 43
- Unnumbered connection: Page 43

Connecting to the Internet using a USB data communication terminal ▶ Page **49**

Note

- After canceling/changing your provider contract please be sure to delete or reconfigure the connection configuration of the product. Failure to observe this could result in unexpected charges from your telephone carrier or provider.
- Before using the product as a router (or before signing a new contract with your provider), be sure to determine whether simultaneous connections of multiple PCs through a router are permitted by your provider. Some providers do not allow simultaneous connections or require that you sign a separate contract. If you use the product in violation of the terms and conditions of the contract with your provider, you may be charged unexpected fees. If simultaneous connections are prohibited by your provider, sign a separate contract with your provider or sign a contact with a provider that allows simultaneous connections.

Connection 1

Permanently connecting to the Internet through a broadband line (PPPoE/CATV)

Specify the destination in the “Basic configuration page” to connect to the Internet. If you use a network PPPoE connection or an unnumbered connection, refer to “Permanently connecting to the Internet using network connection service” (page 43).

Before configuring the settings

Note

- After canceling/changing your provider contract please be sure to delete or reconfigure the connection configuration of the product. Failure to observe this could result in unexpected charges from your telephone carrier or provider.
- A constant Internet connection increases the risk of illegal access or attack. Be sure to use the product with extra attention to your network security. For more information, see “Enhancing security” (page 92).
- The descriptions in this manual use Windows 7 and Internet Explorer 9 screens as examples. For other environments, you have slightly different screen displays, though operations stay the same.

You need the setup document supplied by the provider.

To configure destinations and connect to the Internet, you are required to have the following information provided by your provider (some connection modes may not need all of the information).

- User ID (authentication ID and account name)
- Passwords (authentication password and initial password)
- IP address
- Netmask
- Name server addresses (DNS server address, name server IP address, and DNS server IP address)
- Default gateway address

1 Checking the connection mode

The screenshot shows the Yamaha RTX810 web interface. At the top, the Yamaha logo and 'RTX810 [Rev.11.01.15 Tue Apr 2 14:31:48 2013]' are visible. Below the header, there are three main configuration options:

- Configure or modify new provider.** (with a 'Configure provider' button)
- Configure or change a Yamaha switch.** (with a 'Switch control' button)
- Configure more detailed settings or refer to the communication log of this product.** (with an 'Advanced settings' button)

A callout box labeled '1 Click' points to the 'Switch control' button. Below these options, a section titled 'Configure providers' shows 'No provider configured.' An arrow points from this section to a dialog box titled 'Configure provider 1/4 : Type of line and connection method'. This dialog box contains the instruction 'Configure the type of line and connection mode in this order.' and three radio button options:

- Terminal broadband connection over PPPoE
- Terminal broadband connection over DHCP (i.e. CATV internet)
- Mobile Internet connection

At the bottom of the dialog box, there are 'Next' and 'Abort' buttons. A callout box labeled '3 Click' points to the 'Next' button. A text box above the dialog box states 'The line type is automatically detected.'

1 Click "Configure provider" on the top page of "Basic configuration page".

The broadband line auto-distinction function works to show the window for the connection mode selected for the connected line.

Note

Note that the broadband line auto-distinction process takes place only once. Be sure to check that the broadband line is connected to the WAN port of the product before performing this function.

2

Check the connection mode that is automatically determined and then click “Next”.

3

Click “Next”.

The setting screen corresponding to the connected line appears.

The following configurations vary depending on the connected line. For details, refer to the description for the connection line you selected.

If no line was chosen

▶ **Failed to automatically determine broadband line.**

Select “Terminal broadband connection over PPPoE” or “Terminal broadband connection over DHCP (i.e. CATV internet)” to your connection type and then click “Next”.

If you are not sure which connection type you use currently, check the contract or contact your provider.


A

When “Terminal broadband connection over PPPoE” is selected:

▶ See page 36

B

When “Terminal broadband connection over DHCP (i.e. CATV Internet)” is selected:

▶ See page 40

2 - Specifying your provider information

Configure provider 2/4 : Input information on the subscribed to provider Help

Ensure to enter while referring to the contract supplied by the provider.
(Columns with * are mandatory.)

New provider registration		
Configuration name	(optional)	PPPoE
User ID	(or account name) *	username@provider.ne.jp
Connect password	(line connection) *

Back Next

1 Fill in

2 Fill in

3 Fill in

4 Click

1

Enter the configuration name.

Enter a descriptive destination name. It is a good idea to name the configuration so that you can easily identify it when it needs to be modified.

2

Enter the user ID.

Enter the connection user ID specified by the provider. Be sure to check the relevant document when entering it.

3

Enter your connect password.

Enter the password specified by the provider (or the password you changed). The password is case sensitive and should be in alphanumeric characters.

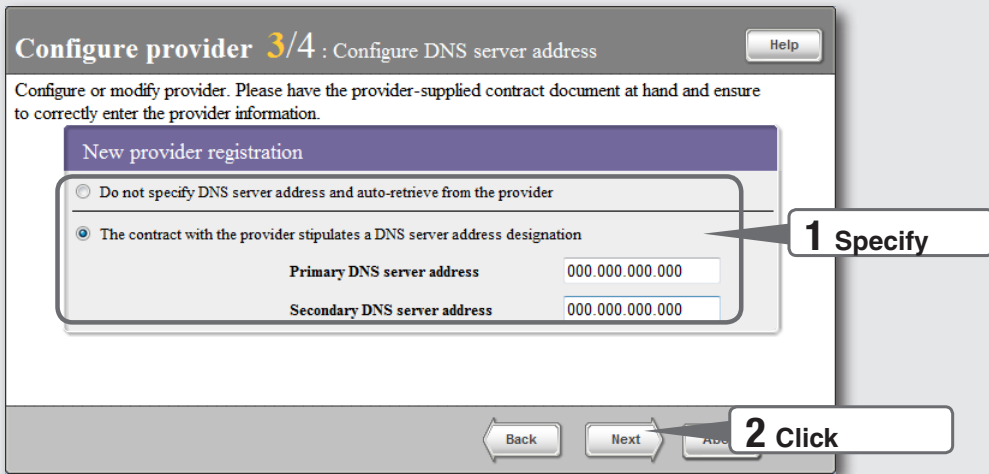
Each password character entered is represented by a black dot.

4

Click "Next".

The "Configure provider 3/4" screen appears.

3 - Specifying the DNS server address



1

Specify the DNS server address.

If the DNS server address is not assigned by your provider:

Click “Do not specify DNS server address and auto-retrieve from the provider” to select it.

If the DNS server address is assigned by your provider:

Click “The contract with the provider stipulates a DNS server address designation” to select it and then set the following addresses.

- Primary DNS server address: Enter the DNS server address assigned by your provider in numeric characters.
- Secondary DNS server address: Enter the secondary DNS server address if your provider provides you with two DNS server addresses (if your provider provides you with only one DNS server address, leave this field blank).

2

Click “Next”.

The “Configure provider 4/4” screen appears.

4 - Checking the setting information

Configure provider 4/4 : Confirm setting Help

After reviewing the configuration press the [Submit] button.

New provider registration	
Connection type	Terminal broadband connection over PPPoE
Configuration name	PPPoE
User ID (or account name)	username@provider.ne.jp
Connect password (line connection)	aaaaaaa
DNS server address	0.0.0.0

Back Submit 2 Click

1 Check

Register provider Help

DNS server IP address configured.
Provider to connect to registered.

To connect press the [Connect] button.

Connect Return to top

1

Ensure that the entries displayed on the screen comply with the information provided by your provider.

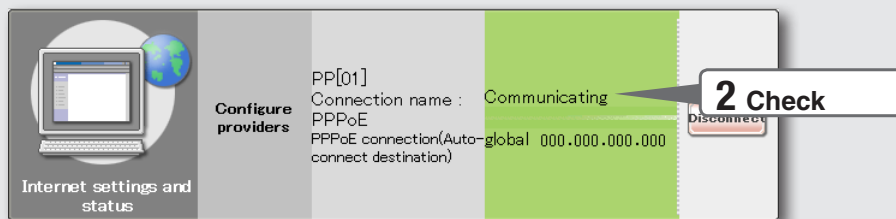
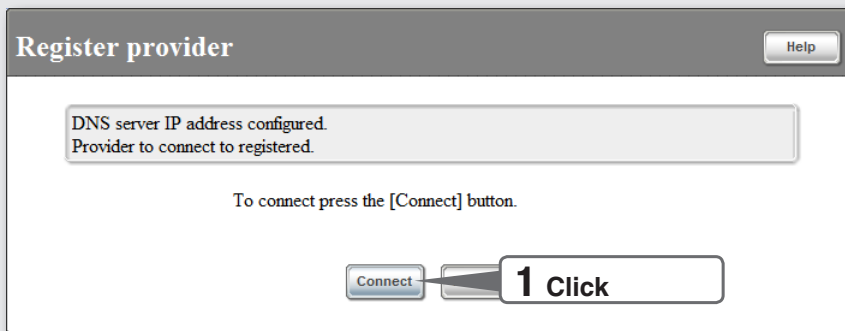
If an incorrect setting has been made, click “Back” to bring up the necessary setting screen to set it correctly.

2

Click “Submit”.

The “Register provider” screen appears.

5 - Connecting to the Internet



1

Click “Connect”.

The product connects to the Internet and shows the “Connect/disconnect provider” screen. Click “Return to top” to return to the top page of the “Basic configuration page”.

2

Check whether the product is connected to the Internet.

Check that the product is connected to the Internet by viewing the status of Internet connection on the lower part of the screen.

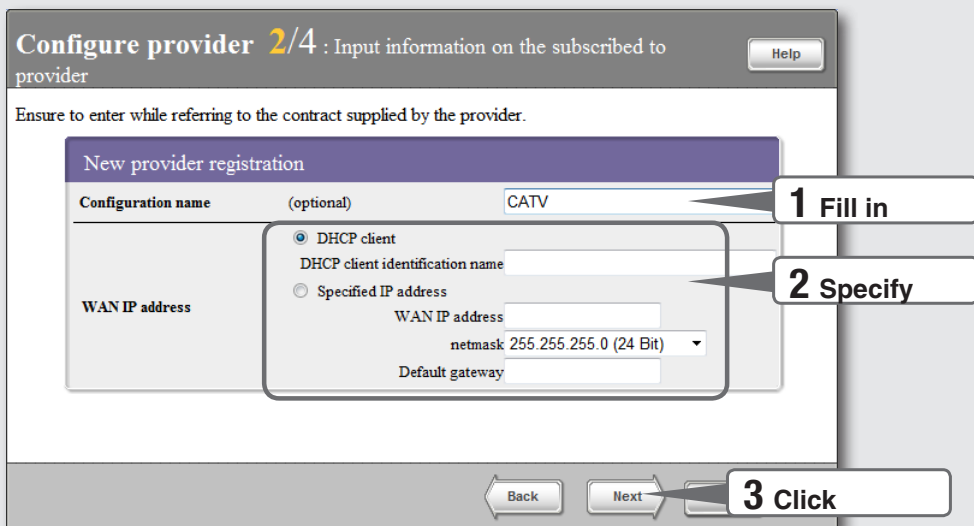
Configurations are completed.

Configuration settings for your Internet connection are now complete.

▶ If you cannot connect to the Internet:

- Check 1 Check the connection between the product and your PC, ADSL modem or ONU.
- Check 2 Check the entries again on pages 36 and 37.
- Check 3 If you still have difficulties, refer to “Troubleshooting” for solutions (page 139).

2 - Specifying your provider information



1

Enter the configuration name.

Enter a descriptive destination name. It is a good idea to name the configuration so that you can easily identify it when it needs to be modified.

2

Specify the WAN IP address.

If the IP address is not assigned by your provider:

Click “DHCP client” to select it.

If the DHCP client identification name is assigned by your provider, enter that identification name in the “DHCP client identification name” (there is no need to enter it if it is not assigned by your provider).

If the IP address is assigned by your provider:

Click “Specified IP address” and then configure the following settings.

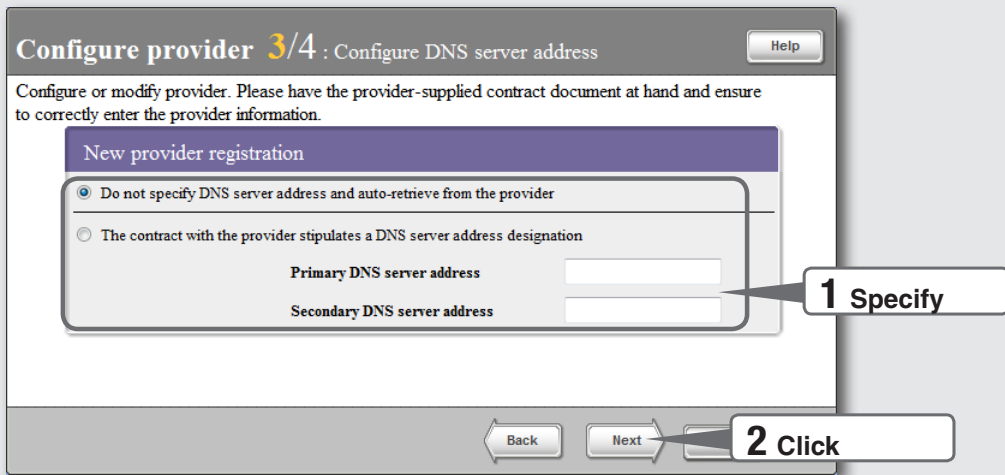
- **WAN IP address:** Enter the IP address assigned by your provider in numeric characters.
- **Netmask:** Select the netmask assigned by your provider.
- **Default gateway:** Enter the default gateway address assigned by your provider in numeric characters.

3

Click “Next”.

The “Configure provider 3/4” screen appears.

3 - Specifying the DNS server address



1

Specify the DNS server address.

If the DNS server address is not assigned by your provider:

Click “Do not specify DNS server address and auto-retrieve from the provider” to select it.

If the DNS server address is assigned by your provider:

Click “The contract with the provider stipulates a DNS server address designation” to select it and then set the following addresses.

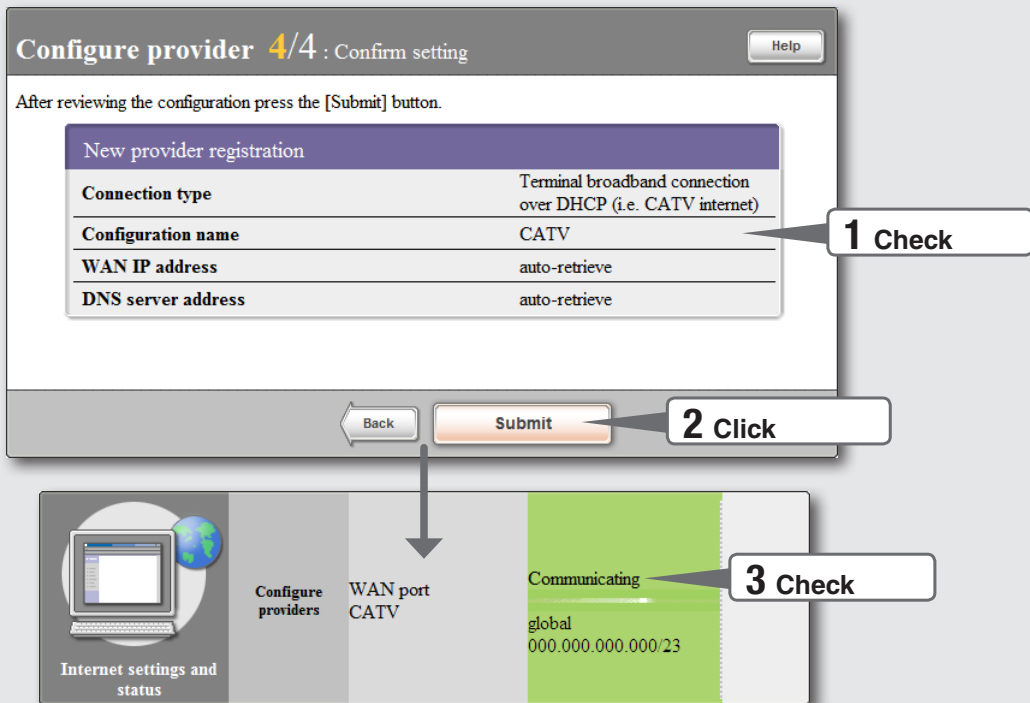
- **Primary DNS server address:** Enter the DNS server address assigned by your provider in numeric characters.
- **Secondary DNS server address:** Enter the secondary DNS server address if your provider provides you with two DNS server addresses (if your provider provides you with only one DNS server address, leave this field blank).

2

Click “Next”.

The “Configure provider 4/4” screen appears.

4 - Confirming the entries before connecting to the Internet



1 Ensure that the entries displayed on the screen comply with the information provided by your provider.

If an incorrect setting has been made, click “Back” to bring up the necessary setting screen to set it correctly.

2 Click “Submit”.

If you click “Return to top” in the confirmation screen that appears, the product automatically connects to the Internet and returns to the top page of the “Basic configuration page”.

3 Check whether the product is connected to the Internet.

Check that the product is connected to the Internet by viewing the status of Internet connection on the lower part of the screen.

Configurations are completed.

Configuration settings for your Internet connection are now complete.

► If you cannot connect to the Internet:

- Check 1 Check the connection between the product and your PC, ADSL modem or cable modem.
- Check 2 Check the entries again on pages 36 and 37.
- Check 3 If you still have difficulties, refer to “Troubleshooting” for solutions (page 139).

Permanently connecting to the Internet using network connection service

Specify the destination in the “Basic configuration page” to connect to the Internet.

The following description also applies when you use unnumbered connections.

If you use an ADSL connection service or a fiber optic Internet service that assigns only one IP address, refer to “Permanently connecting to the Internet through a broadband line (PPPoE/CATV)” (page 33).

Before configuring the settings

Note

- After canceling/changing your provider contract please be sure to delete or reconfigure the connection configuration of the product. Failure to observe this could result in unexpected charges from your telephone carrier or provider.
- A constant Internet connection increases the risk of illegal access or attack via the Internet. Be sure to use the product with extra attention to your network security. For more information, see “Enhancing security” (page 92).
- The descriptions in this manual use Windows 7 and Internet Explorer 9 screens as examples. For other environments, you have slightly different screen displays, though operations stay the same.

You need the setup document supplied by the provider.

To configure destinations and connect to the Internet, you are required to have the following information provided by your provider (some connection modes may not need all of the information).

- User ID (authentication ID and account name)
- Passwords (authentication password and initial password)
- IP address
- Netmask
- Name server addresses (DNS server address, name server IP address, and DNS server IP address)
- Default gateway address

1 Specifying the connection mode

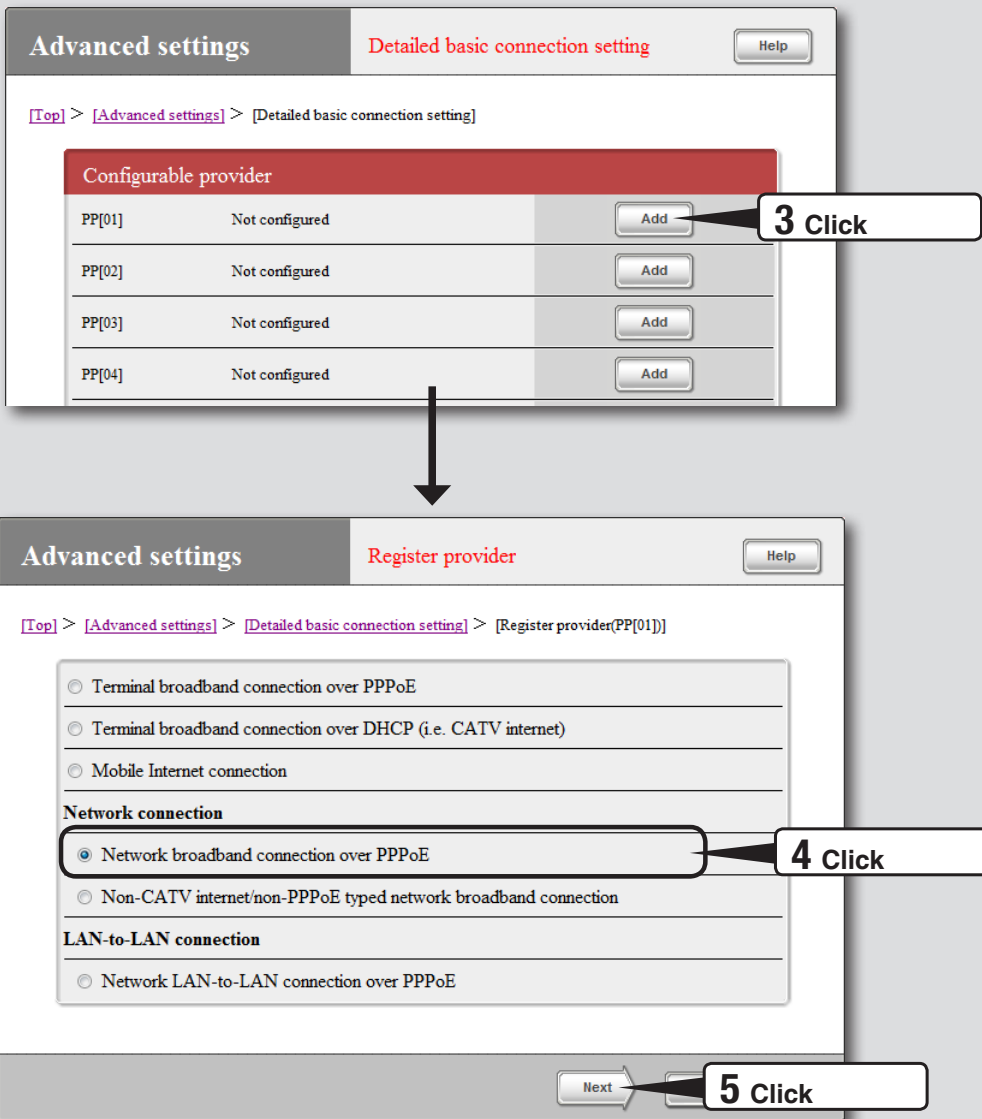
The image shows two screenshots of the Yamaha RTX810 configuration interface. The top screenshot shows the main configuration screen with three main options: 'Configure or modify new provider.', 'Configure or change a Yamaha switch.', and 'Configure more detailed settings or refer to the communication log of this product.' The 'Advanced settings' button is highlighted with a callout box labeled '1 Click'. Below this, the 'Advanced settings' screen is shown, with the 'Configure' button for 'Detailed basic connection setting' highlighted with a callout box labeled '2 Click'.

1 Click “Advanced settings”.

The “Advanced settings” screen appears.

2 Click “Configure” to the right of “Detailed basic connection setting”

The “Detailed basic connection setting” screen appears.

**3****Click “Add”.**

The “Register provider” screen appears.

4**Click the “Network broadband connection over PPPoE”.****5****Click “Next”.**

The “Register provider” screen appears.

2 Specifying your provider information

The screenshot shows a web interface for configuring a provider. At the top, there are tabs for 'Advanced settings' and 'Register provider', with a 'Help' button. Below the tabs, there is a breadcrumb trail: [Top] > [Advanced settings] > [Detailed basic connection setting] > [Register provider(PP[01])]. The main heading is 'Configure providers using the following interface. (Network broadband connection over PPPoE)'. There is a list item '• PP[01]Interface'. Below that, it says 'Modify the input or selected items of each column. After checking them press the [Submit] button.' Underneath is a section '•Basic matters' containing a form titled 'Register provider'. The form has three rows: 'Configuration name' (optional) with the value 'NetworkADSL', 'User ID' (or account name) with the value 'username', and 'Connect password' (line connection) with a masked password '.....'. Three callout boxes labeled '1 Fill in', '2 Fill in', and '3 Fill in' point to the input fields for the configuration name, user ID, and connect password respectively.

Register provider		
Configuration name	(optional)	NetworkADSL
User ID	(or account name)	* username
Connect password	(line connection)	*

1

Enter the configuration name.

Enter a descriptive destination name. It is a good idea to name the configuration so that you can easily identify it when it needs to be modified.

2

Enter the user ID.

Enter the connection user ID specified by the provider. Be sure to check the relevant document when entering it.

3

Enter your connect password.

Enter the password specified by the provider (or the password you changed). The password is case sensitive and should be in alphanumeric characters.

Each password character entered is represented by a black dot.

4

Specify the Network Address Translation (NAT) configuration.

Dynamic address translation (NAT)

Select a method for translating the line's address into a LAN address and vice versa.

- Enable NAT: Select when translating a line's address and the LAN address on a one-to-one basis.
- Enable IP masquerade: Select when translating a line's address and the LAN address on a one-to-many basis.
- Use NAT and IP masquerade in parallel: Select when a mix of global IP and private IP addresses are configured for equipment on the LAN side.
- do not use: Select when not using any address translation function.

External NAT address range

Enter shared global IP addresses assigned to the line side.

Internal NAT address range

Enter the range of private IP addresses to be address translated.

5

Specify the DNS server address.

If the DNS server address is not assigned by your provider:

Select "Automatically retrieve upon connecting".

If the DNS server address is assigned by your provider:

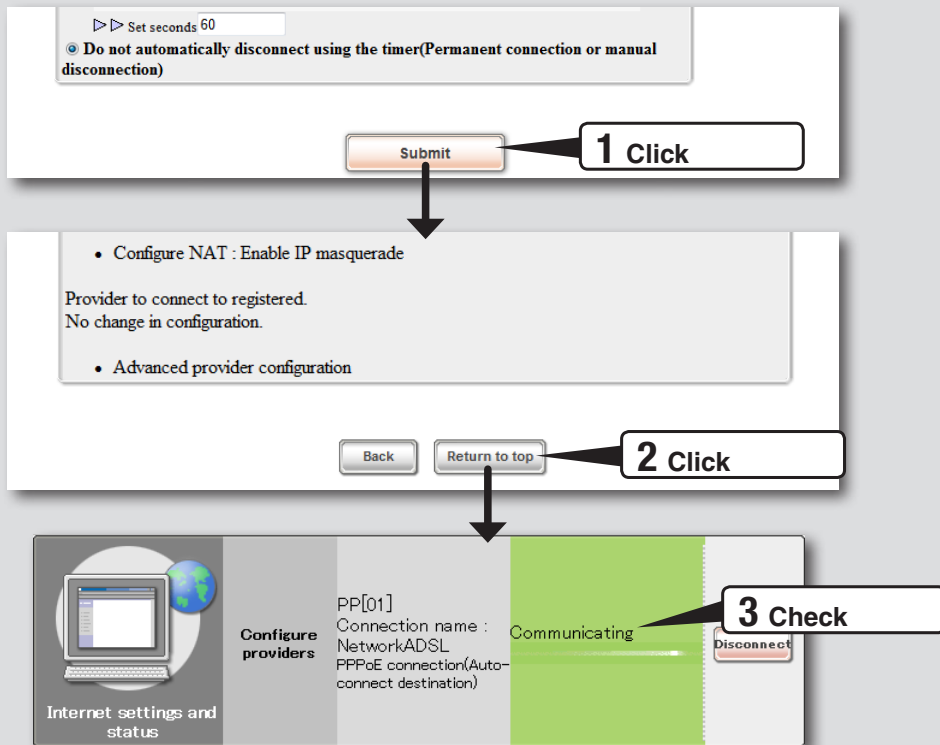
Select "Specify IP address" and then configure the following settings.

- Primary DNS server address: Enter the DNS server address assigned by your provider in numeric characters.
- Secondary DNS server address: Enter the secondary DNS server address if your provider provides you with two DNS server addresses (if your provider provides you with only one DNS server address, leave this field blank).

If a domain name is assigned by your provider:

Enter the specified domain name in the "DNS domain name" field.

3 Connecting to the Internet



1

Click “Submit”.

The “Register provider” screen appears.

2

Click “Return to top”.

The product is automatically connected to the Internet. The screen returns to the top page of the “Basic configuration page”.

3

Check whether the product is connected to the Internet.

Check that the product is connected to the Internet by viewing the status of Internet connection on the lower part of the screen.

Configurations are completed.

Configuration settings for your Internet connection are now complete.

▶ If you cannot connect to the Internet:

- Check 1 Check the connection between the product and your PC, ADSL modem or ONU.
- Check 2 Check the entries again on pages 46 and 47.
- Check 3 If you still have difficulties, refer to “Troubleshooting” for solutions (page 139).

Connecting to the Internet using a USB data communication terminal

The product can be connected to the Internet by connecting a commercially-available data communication terminal that supports USB ports to the USB port. Connect a USB data communication terminal to the product before specifying the destination in the “Basic configuration page” to connect to the Internet.

Before configuring the settings

Note

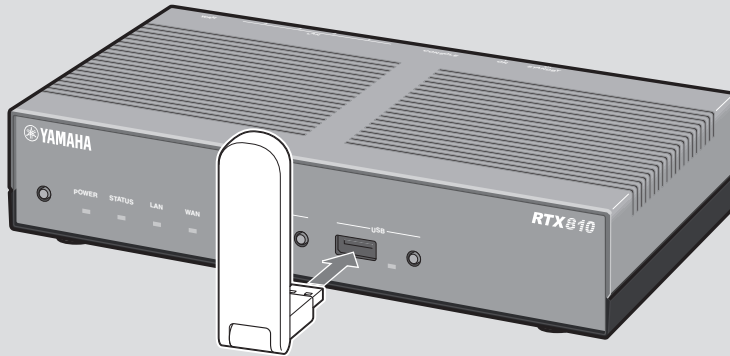
- After canceling/changing your provider contract please be sure to delete or reconfigure the connection configuration of the product. Failure to observe this could result in unexpected charges from your telephone carrier or provider.
- If your data (packet) communications service contract is based on a pay-as-you-go plan or your flat-rate contract does not cover data communications, prolonged communications or transfer of large amount of data result in hefty fees. Pay careful attention to the communication charges before using your communications service. The product have a function that issues an alert or restricts communication by monitoring communication time and communications traffic for each connection or on a cumulative basis. Please use it as necessary.
- A constant Internet connection increases the risk of illegal access or attack via the Internet. Be sure to use the product with extra attention to your network security. For more information, see “Enhancing security” (page 92).
- Be sure to use a communication terminal as instructed in its instruction manual and under environmental conditions specified therein.
- This function does not support 64K data communications.
- The descriptions in this manual use Windows 7 and Internet Explorer 9 screens as examples. For other environments, you have slightly different screen displays, though operations stay the same.

You need the setup document supplied by the provider.

To configure destinations and connect to the Internet, you are required to have the following information provided by your provider (some connection modes may not need all of the information).

- User ID (authentication ID and account name)
- Passwords (authentication password and initial password)
- IP address
- Netmask
- Name server addresses (DNS server address, name server IP address, and DNS server IP address)
- Default gateway address
- Access point name
- CID (Context Identifier)

1 Connecting a USB data communication terminal



Connect a USB data communication terminal to the USB port of the product.

The USB lamp lights up and flashes.

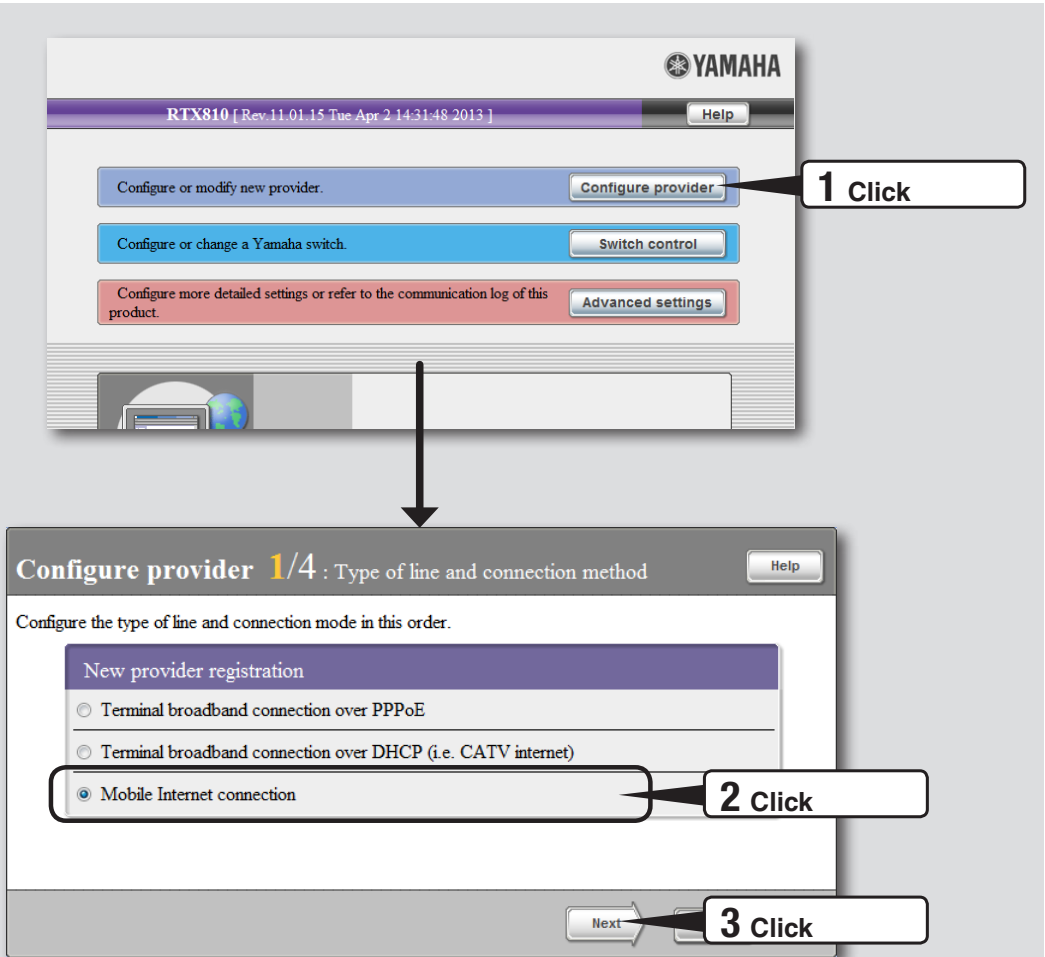
 **Tip**

A buzzer beeps when the USB data communication terminal is connected. Please check “Changing the buzzer settings” (page 126) for beeps.

USB data communication terminals that are known to work

For a list of latest USB data communication terminals that are known to work, please <http://www.yamaha.com/products/en/network/> and go to the product information page on RTX810.

2 Specifying the connection mode



1 Click “Configure provider” on the top page of “Basic configuration page”.

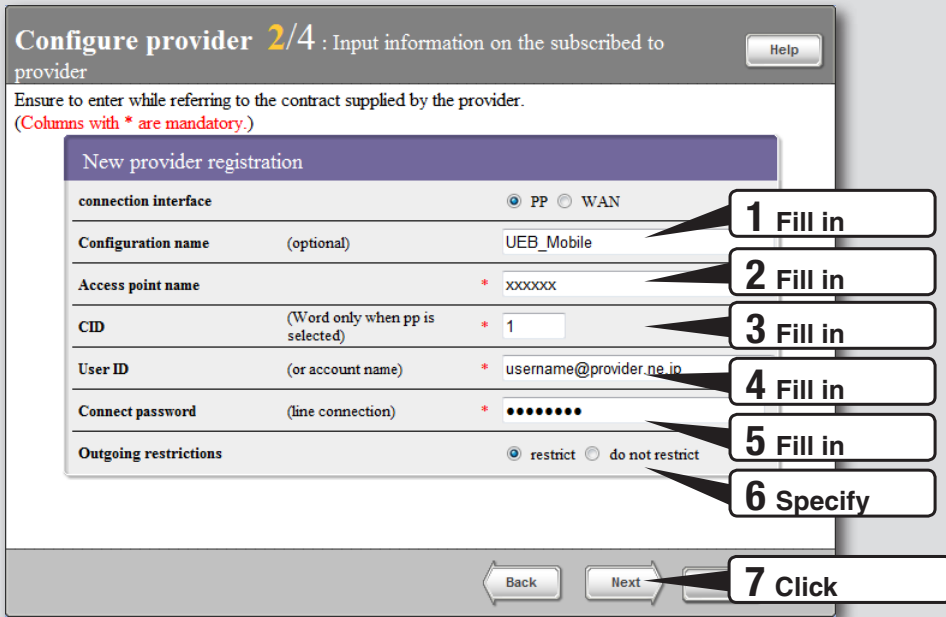
The “Configure provider 1/4” screen appears.

2 Click “Mobile Internet connection”.

3 Click “Next”.

The “Configure provider 2/4” screen appears.

3 Specifying your provider information



1 Enter the configuration name.

Enter a descriptive destination name. It is a good idea to name the configuration so that you can easily identify it when it needs to be modified.

2 Enter the access point name.

Enter the access point name provided by your carrier or provider. Entries may vary depending on your contract plan. Be sure to check the relevant document when entering it.

3 Enter the CID (Context Identifier).

Enter the CID number provided by your carrier or provider. Entries may vary depending on your contract plan. Be sure to check the relevant document when entering it.

4 Enter the user ID.

Enter the user ID provided by your provider. Be sure to check the relevant document when entering it.

5 Enter your connect password.

Enter the password specified by the provider (or the password you changed). The password is case sensitive and should be in alphanumeric characters.

Each password character entered is represented by a black dot.

6

Configure outgoing restrictions.

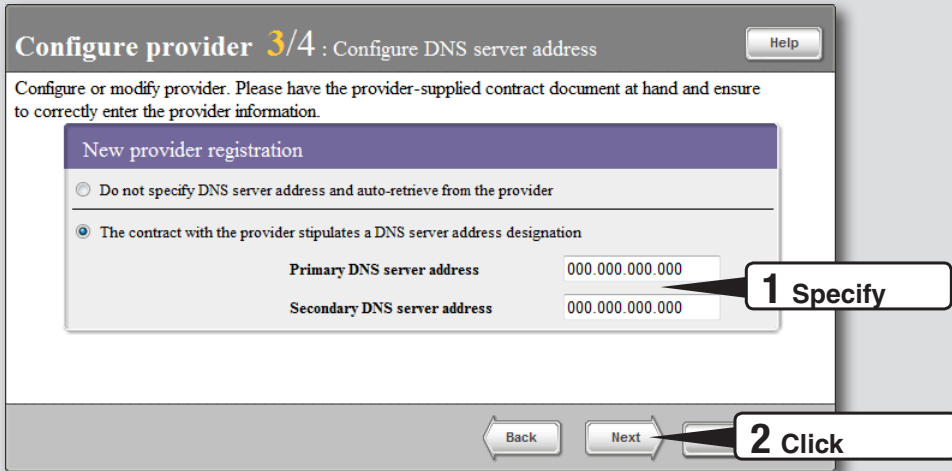
Configure the outgoing restrictions based on the cumulative send/received data and the cumulative connection period. Depending on your contract plan, unusual billing can occur due to long connection times. Be sure to check your contract plan before configuring it.

7

Click “Next”.

The “Configure provider 3/4” screen appears.

4 Specifying the DNS server address



1

Specify the DNS server address.

If the DNS server address is not assigned by your provider:

Click “Do not specify DNS server address and auto-retrieve from the provider” to select it.

If the DNS server address is assigned by your provider:

Click “The contract with the provider stipulates a DNS server address designation” to select it and then set the following addresses.

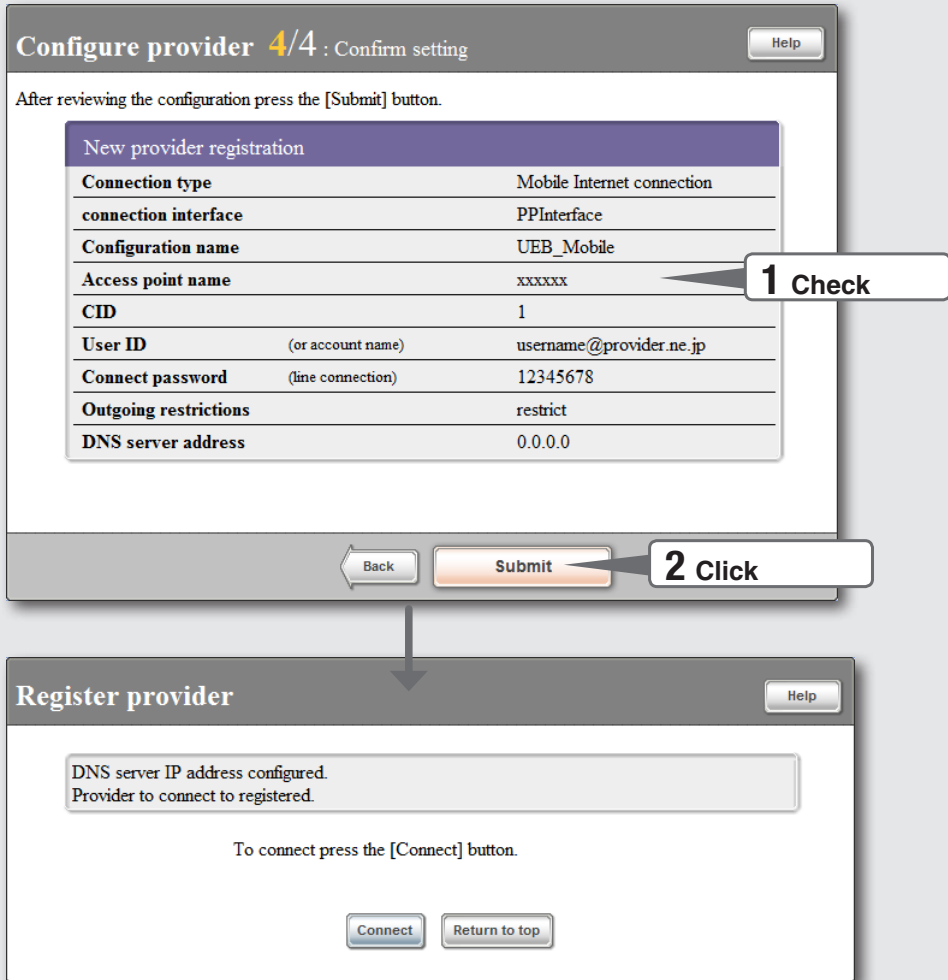
- Primary DNS server address: Enter the DNS server address assigned by your provider in numeric characters.
- Secondary DNS server address: Enter the secondary DNS server address if your provider provides you with two DNS server addresses (if your provider provides you with only one DNS server address, leave this field blank).

2

Click “Next”.

The “Configure provider 4/4” screen appears.

5 Checking the setting information



1

Ensure that the entries displayed on the screen comply with the information provided by your provider.

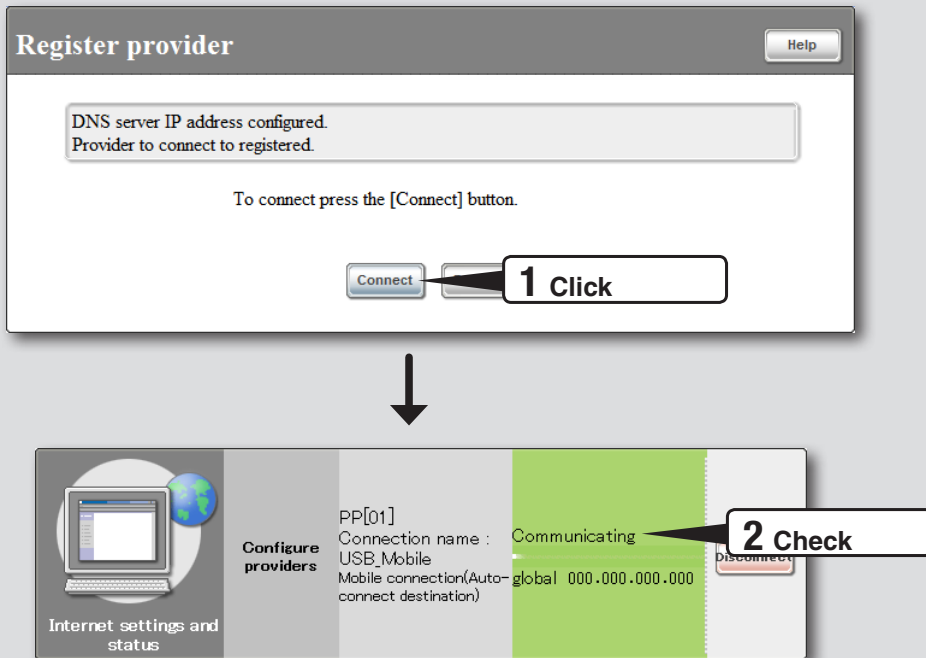
If an incorrect setting has been made, click “Back” to bring up the necessary setting screen to set it correctly.

2

Click “Submit”.

The “Register provider” screen appears.

6 Connecting to the Internet



1

Click “Connect”.

The product connects to the Internet and shows the “Connect/disconnect provider” screen. Click “Return to top” to return to the top page of the “Basic configuration page”.

2

Check whether the product is connected to the Internet.

Check that the product is connected to the Internet by viewing the status of Internet connection on the lower part of the screen.

Configurations are completed.

Configuration settings for your Internet connection are now complete.

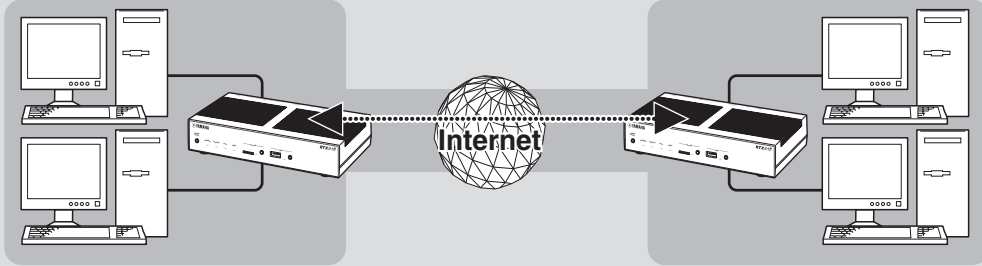
► If you cannot connect to the Internet:

- Check 1 Check the connection between the product and your PC and between the product and the USB data communication terminal.
- Check 2 Check the entries again on pages 52 and 53.
- Check 3 If you still have difficulties, refer to “Troubleshooting” for solutions (page 139).

Creating a Virtual Private Network (VPN) using IPsec (IPsec LAN-to-LAN connection)

You can create a Virtual Private Network (VPN) to connect LANs if the product is connected to a broadband Internet connection. LAN-to-LAN connection using IPsec ensures secure connection via the Internet.

A VPN can be created using conventional broadband connections such as ADSL. Thus, VPNs are cheaper than real private networks using dedicated lines. The LAN-to-LAN connection of the product supports TCP/IP server software.



Create a Virtual Private Network (VPN) using IPsec

Creating a Virtual Private Network (VPN) using IPsec (IPsec LAN-to-LAN connection) (continued from the previous page)

IPsec that can be used with the product

- Internet Key Exchange (IKE) is used as the key exchange protocol. Required keys are automatically generated by IKE. It will be necessary to register pre-shared keys as the seed (ipsec ike pre-shared key command).
- Management information containing keys, key lifetimes, encryption and authentication algorithms is managed with a security association (SA).
- Note the revision of the program for the destination equipment that is a security gateway. Although there is an interconnectivity of IPsec between releases 2 and 3, the settings of the latter must be adjusted to the settings of the former. The identifiers of the security gateways that are available for the product are 1 through 50. Similarly, tunnel interface numbers are 1 through 50.
- The product supports both Main Mode and Aggressive Mode. However, you cannot freely choose a mode.
 - If the both routers that form a VPN have fixed global IP addresses, use the Main Mode. If only one router has a fixed global IP address (e.g., a dial-up VPN), use the Aggressive Mode.
 - When using the Main Mode, it will be necessary to configure the IP address of the router on the other side.
 - When using the Aggressive Mode, the settings depend on whether or not the routers have fixed global IP addresses.
- For information on the IPsec specifications and configuration commands of the product, please refer to “Command reference” (included in the attached CD-ROM).

Note

- Because IPsec tunnels are to be configured with the router connected to a broadband connection, it will be necessary to configure the broadband connections before setting up the LAN-to-LAN connection using IPsec.
- IPsec-based LAN-to-LAN connection can be used only in an environment where a global IP address is assigned by your provider. Note that the following IP addresses are not global IP addresses:
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- When using the LAN-to-LAN connection, be sure to configure adequate security settings to maintain data integrity. Inadequate security settings may cause PCs in the LAN to be hacked, sniffed, intercepted, or destroyed, or their data to be lost.
- The LAN-to-LAN connection of the product does not support Windows NetBEUI protocol or Apple's Mac OS AppleTalk protocol.
- To share files in Windows, you need to use NetBIOS over TCP/IP protocol or have a Windows Internet Name Service (WINS) server.
- To share files in Macintosh, open System Preferences, select “Sharing” and select “File Sharing” check box.

IPsec has two communication modes.

There are basically two types of modes in IPsec-based communications: tunnel mode and transport mode. These two modes can be used in combination, but it is not possible to doubly apply each mode.

Tunnel mode

This is a communications mode that is provided to use a IPsec-based VPN. The router, acting as a security gateway, encrypts IP packet data passing on the LAN to exchange data with the security gateway on the other side. Since the router performs all processes necessary for IPsec, no special settings are required for hosts being the start or end points on the LAN.

To use the tunnel mode, define a virtual interface called “tunnel interface” and configure the routes so that IP packets to be processed flow through the tunnel interface. Each tunnel interface is managed by its tunnel interface number.

Transport mode

This is a special communications mode that ensures the security of communications in which the router itself is the start or end point. This mode can be used in a special case where a router accesses a remote router using telnet.

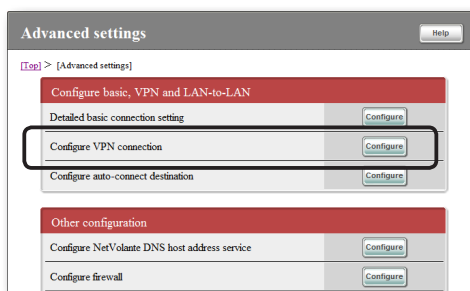
Before configuring the settings

- To connect LANs, it will be necessary to configure a different network address for each LAN to avoid overlapping. Change the product's LAN network address in advance.
- To attach the product to a LAN with a different network address assigned, change the configuration of the product according to the network you install. Please refer to “Configuring the IP address on the LAN side” (page 29) for more information.

Configuring the product to use IPsec

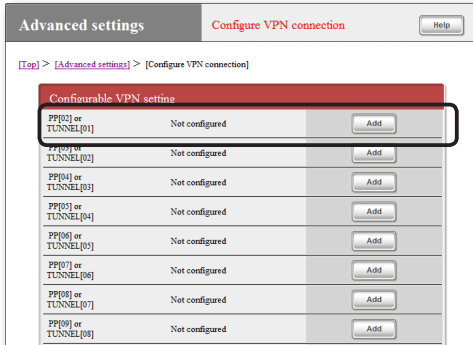
Configure the settings required for IPsec communication with the product.

- 1 On the top page of “Basic configuration page”, click “Advanced settings”, then click “Configure” to the right of “Configure VPN connection”.



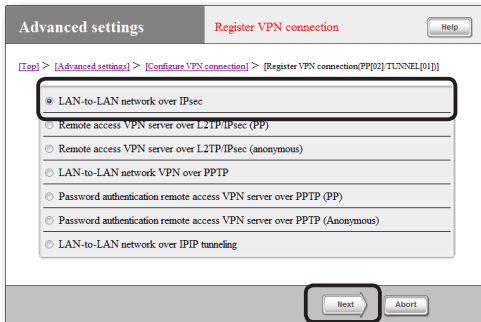
Creating a Virtual Private Network (VPN) using IPsec (IPsec LAN-to-LAN connection) (continued from the previous page)

- 2 Click “Add” to the right of the destination you want to register.



- 3 Select “LAN-to-LAN network over IPsec” and then click “Next”.

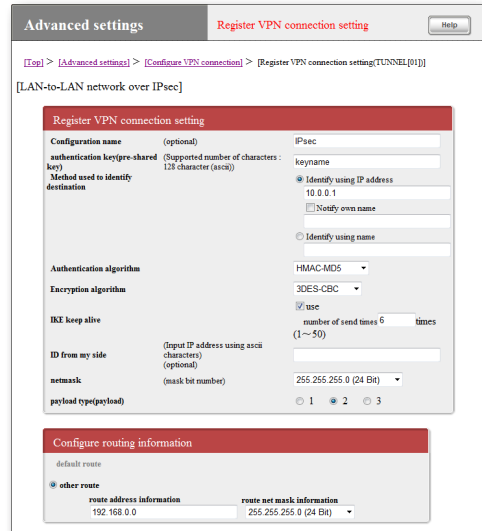
The “Register/modify VPN connection setting” screen appears.



- 4 Configure the required settings and then click “Submit”.

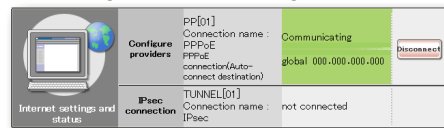
The connection destination is registered.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.



Connecting with IPsec

If authentication succeeds on both sites, the IPsec communication is automatically established (no manual operations are required). Once the IPsec connections are complete, the top page of the “Basic configuration page” shows a message, “Communicating”.



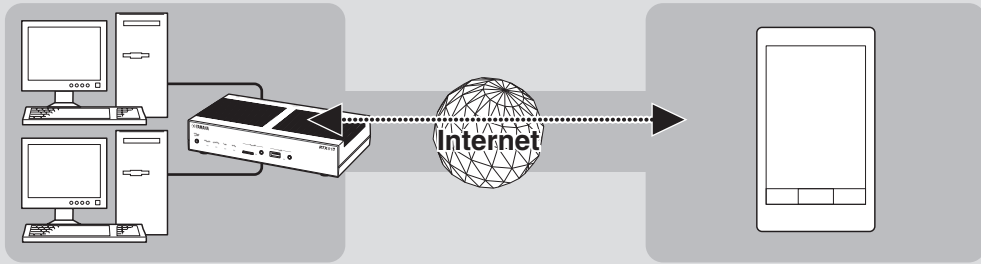
Note

- For the IPsec connection, both sites must have the same pre-shared key.
- A pre-shared key is a password that provides important information. Any pre-shared key must be long and not be easily guessed by outsiders. Use a combination of alphanumeric characters, lower and upper cases, and symbols. Great care is needed in managing these keys.

Gaining remote access using L2TP/IPsec

The product supports L2TP (Layer-2 Tunneling Protocol)/IPsec. If it is connected to a broadband connection, it works as a virtual private network (VPN), allowing users in remote locations (like on the road) to access a PC on the LAN. IPsec VRN connections are more secure than PPTP.

For remote access, register remote users' user IDs and passwords with the product and configure VPN connections on a remote PC.



Gaining remote access using L2TP/IPsec

Gaining remote access using L2TP/IPsec

(Continued from the previous page)

L2TP/IPsec that can be used with the product

- The product supports data encryption for IPsec.
- Internet Key Exchange (IKE) is used as the key exchange protocol. Required keys are automatically generated by IKE. It will be necessary to register pre-shared keys as the seed (ipsec ike pre-shared key command).
- Management information containing keys, key lifetimes, encryption and authentication algorithms is managed with a security association (SA).
- A disconnection timer monitors the communication and an L2TP/IPsec session is disconnected if data does not pass through an L2TP/IPsec tunnel for a certain amount of time.

Note

- Because L2TP/IPsec tunnels are to be configured with the router connected to a broadband connection, it will be necessary to configure the broadband connections before setting up remote access using L2TP/IPsec.
- L2TP/IPsec-based remote access can be used only in an environment where a global IP address is assigned by your provider. Note that the following IP addresses are not global IP addresses:
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- When using the remote access, be sure to configure adequate security settings to maintain data integrity. Inadequate security settings may cause PCs in the LAN to be hacked, sniffed, intercepted, or destroyed, or their data to be lost.
- The remote access function of the product does not support Windows NetBEUI protocol or Apple's Mac OS AppleTalk protocol.
- To share files in Windows, you need to use NetBIOS over TCP/IP protocol or have a Windows Internet Name Service (WINS) server.
- To share files in Macintosh, open System Preferences, select "Sharing" and select "File Sharing" check box.

Required settings

For remote access, a router, a PC or a smartphone needs to be configured as shown below.

Router settings

- Configuring the broadband connection
 - The WAN or PP side of the product must be assigned a global IP address.
 - For the terminal connection in which WAN or PP address is dynamically assigned, it will be necessary to obtain host names that are available using the netvolante DNS service (page 104).
 - For the network connection, check the global IP address that is assigned to the WAN or PP side of the product.
- Registering connection destinations (next section)

Settings required for a server or PC in the LAN

- Configure a fixed IP address.
- Changing the settings of the file server software

Settings required for a smartphone that remotely accesses a PC

Changing the settings of a smartphone that remotely accesses a PC (pages 65 and 67)

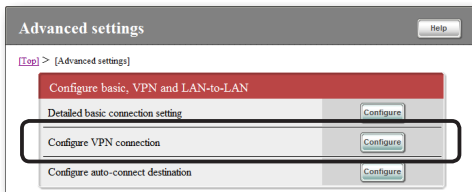
Registering connection destinations

Register connection destinations.

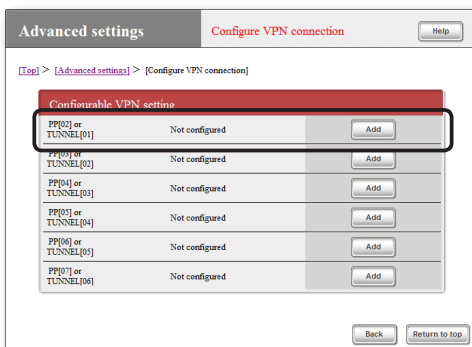
Note

- Up to ten users can be registered for PP connection. There are up to 50 L2TP/IPsec tunnel connections at a time, including the ones used in anonymous connections.
- Although any number of users can be registered with anonymous connections, there are up to 50 L2TP/IPsec tunnel connections at a time, including the ones used in PP connections.

- 1 On the top page of “Basic configuration page”, click “Advanced settings”, then click “Configure” to the right of “Configure VPN connection”.



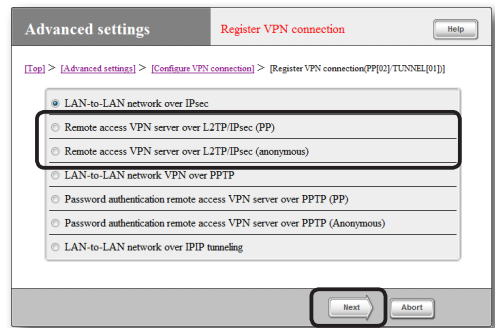
- 2 Click “Add ” to the right of the destination you want to register.



- 3 Select your desired authentication method and then click “Next”.

The “Register VPN connection setting” screen appears.

- **PP:** Only the specified host name or IP address is allowed as the destination, and the user ID and password are used for authentication.
- **Anonymous:** The destination does not get restricted, and the user ID and password are used for authentication.



Gaining remote access using L2TP/IPsec

(Continued from the previous page)

4 Configure the settings required and then click “Submit”.

The connection destination is registered.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

Configuring a server or PC in the LAN

Remote access requires settings that provide you with access to the server or PCs in the LAN via TCP/IP protocol.

Note

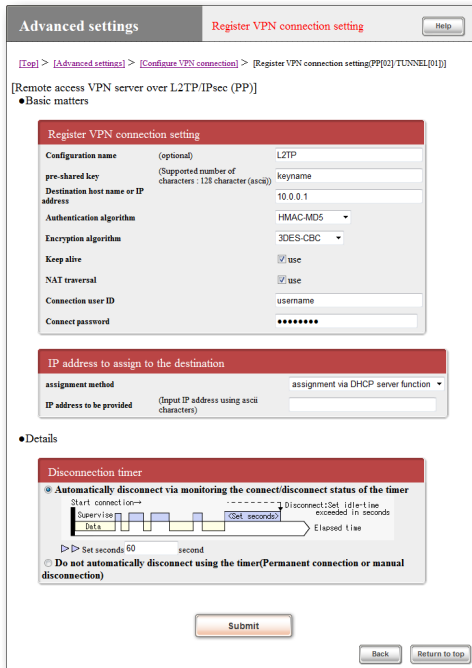
- The remote access function of the product does not support Windows NetBEUI protocol or Apple's Mac OS AppleTalk protocol.
- To share files in Windows, you need to use NetBIOS over TCP/IP protocol or have a Windows Internet Name Service (WINS) server.
- To share files in Macintosh, open System Preferences, select “Sharing” and select “File Sharing” check box.

Configuring the IP addresses of the server and PCs

Assign a fixed private IP address to each PC that allows the servers or PCs on the LAN to gain external access.

Changing the settings of the file server software

Configure a network share on a server or a PC exposed to the Internet and set folders, user IDs and passwords exposed to the Internet.



(Example of screen displayed when “PP” is selected in Step 3)

Gaining remote access via iOS

Changing the settings for a device (such as a smartphone) that remotely accesses a PC

1 Tap on “Settings”.



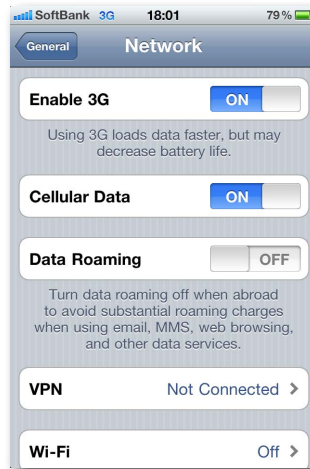
2 Tap on “General”.



3 Tap on “Network”.



4 Tap on “VPN”.



Gaining remote access using L2TP/IPsec

(Continued from the previous page)

4

Implementing site-to-site VPN connections

5 Tap on “Add VPN Configuration”.



RSA SecurID

Set it to Off.

Password

Enter the authentication password you set in Step 4 on page 64.

Secret

Enter the shared key that is configured on the product.

Send All Traffic

Set it to On.

Proxy

Set it to Off.

7 Tap on “Save”.

Now, the setting up of a remote access connection is complete.

6 Select “L2TP” and enter the necessary setup information.



Description

Type “Yamaha-vpn” as the L2TP client name.

Server

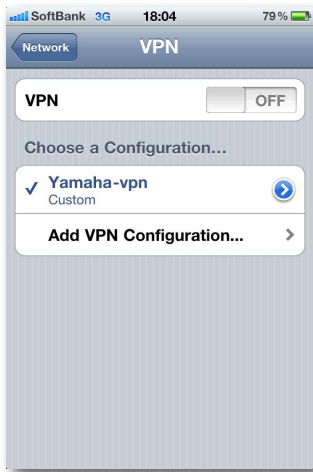
Enter the host address obtained with the netvolante DNS service or the WAN IP address of the product.

Account

Enter the authentication user ID you set in Step 4 on page 64.

Accessing the product

- 1 Configure broadband connections and connect the product to the Internet.
- 2 Tap on “Settings”.
- 3 Tap on “General”.
- 4 Tap on “Network”.
- 5 Tap on “VPN”.
- 6 Tap on “Yamaha-vpn” and slide “VPN” On.



VPN connection to the product now begins.

Gaining remote access from Android

Note

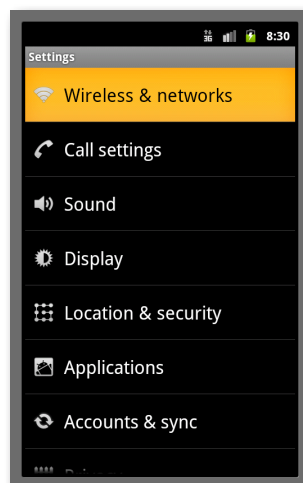
Some of the screens on your terminal may differ from the screens used to describe the operations on Android.

Changing the settings for a device (such as a smartphone) that remotely accesses a PC

- 1 Press the Home icon, press “Menu” and tap on “Settings”.



- 2 Tap on “Wireless & networks”.



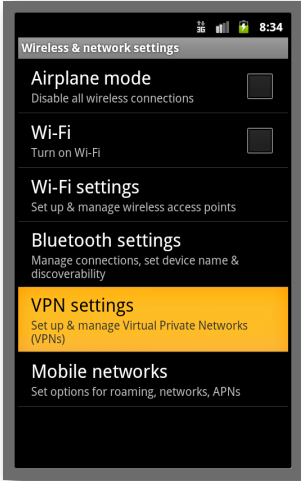
Gaining remote access using L2TP/IPsec

(Continued from the previous page)

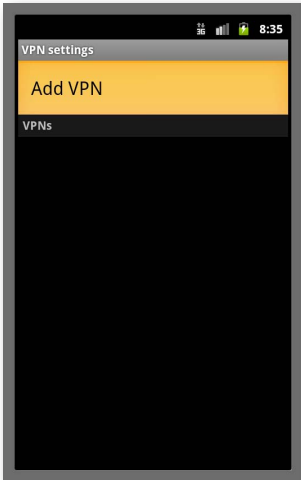
4

Implementing site-to-site VPN connections

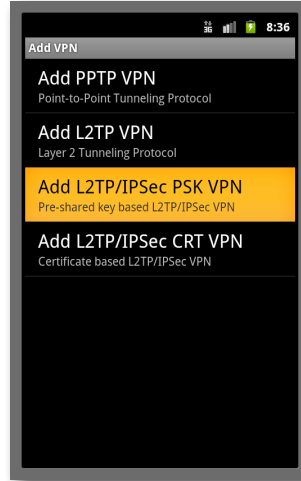
3 Tap on “VPN settings”.



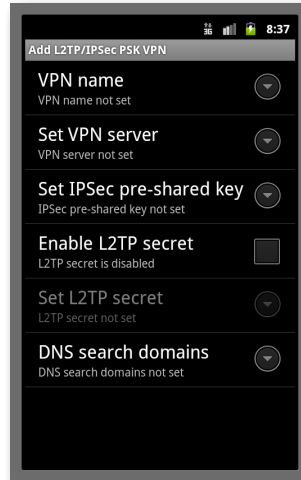
4 Tap on “Add VPN”.



5 Tap on “Add L2TP/IPsec PSK VPN”.



6 Enter necessary setup information.



VPN name

Type “Yamaha-vpn” as the L2TP client name.

Set VPN server

Enter the host address obtained with the netvolante DNS service or the WAN IP address of the product.

Set IPsec pre-shared key

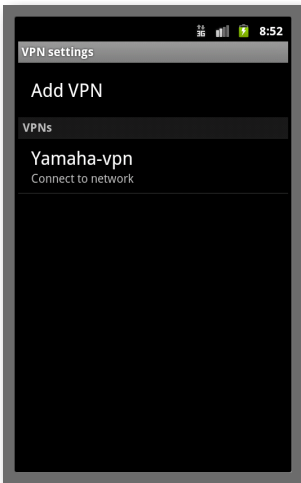
Enter the shared key that is configured on the product.

7 Tap Back key.

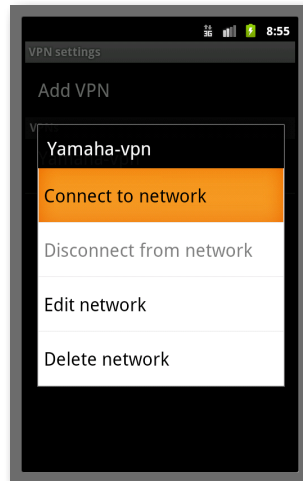
Now, the setting up of a remote access connection is complete.

Accessing the product

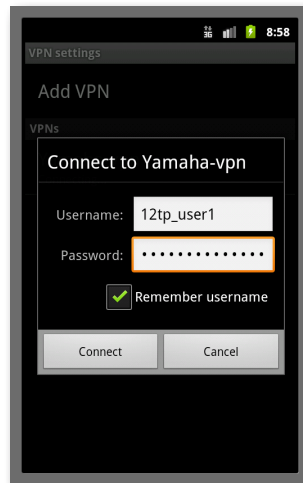
- 1 Configure broadband connections and connect the product to the Internet.
- 2 Press the Home icon, press “Menu” and tap on “Settings”.
- 3 Tap on “Wireless & networks”.
- 4 Tap on “VPN settings”.
- 5 Tap on “Yamaha-vpn”.



6 Tap on “Connect to Network”.



7 Enter the authentication user ID in “Username” and password in “Password” you set in Step 4 on page 64 and tap on “Connect”.



VPN connection to the product now begins.

Note

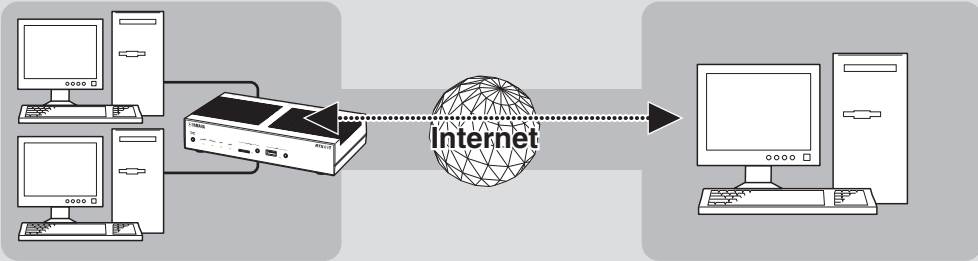
If you select the “Remember username” check box, you no longer need to enter the user ID. If you do not select it, you need to enter the user ID each time you connect to the VPN.

Gaining remote access using PPTP

The product supports PPTP (Point to Point Tunneling Protocol). If it is connected to a broadband connection, you can use it as a virtual private network (VPN) router to access a PC on the LAN from a remote location. For remote access, register remote users' user IDs and passwords with the product and configure VPN connections on a remote PC.

4

Implementing site-to-site VPN connections



Gain remote access using PPTP

PPTP that can be used with the product

- The product supports data encryption for PPTP. The RC4 (either 40- or 128-bit keys) is used as the encryption algorithm.
- The product supports user and password authentication based on MS-CHAP and MS-CHAP v2.
- You can specify whether or not to block incoming traffics if an MPPE encryption does not come into effect (access control).
- The product does not support compression. In the PPP setup on the PPTP client side, deselect the “Enable software compression” check box.
- PPTP uses TCP port 1723 for tunnel control and GRE protocol number 47 for data communication. When a PPTP server is installed inside of a firewall or use NAT in combination with a remote access VPN server, be sure to pass TCP port number 1723 and GRE protocol number 47. For details, contact your network administrator.
- A disconnection timer monitors the communication and a PPTP session is disconnected if data does not pass through a PPTP tunnel for a certain amount of time.
- The product does not support PPP forwarding.

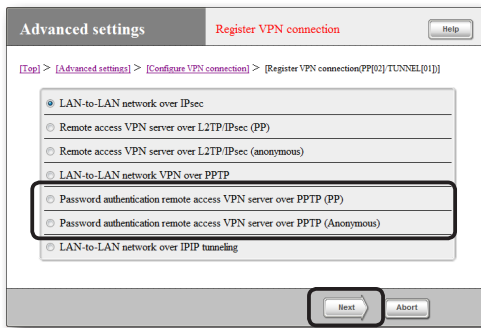
Note

- Because PPTP tunnels are to be configured with the router connected to a broadband connection, it will be necessary to configure the broadband connections before setting up remote access using PPTP.
- Remote access via PPTP is available only in an environment where a global IP address is assigned by your provider. Note that the following IP addresses are not global IP addresses:
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- When using the remote access, be sure to configure adequate security settings to maintain data integrity. Inadequate security settings may cause PCs in the LAN to be hacked, sniffed, intercepted, or destroyed, or their data to be lost.
- The remote access function of the product does not support Windows NetBEUI protocol or Apple's Mac OS AppleTalk protocol.
- To share files in Windows, you need to use NetBIOS over TCP/IP protocol or have a Windows Internet Name Service (WINS) server.
- To share files in Macintosh, open System Preferences, select “Sharing” and select “File Sharing” check box.

3 Select your desired authentication method and then click “Next”.

The “Register VPN connection setting” screen appears.

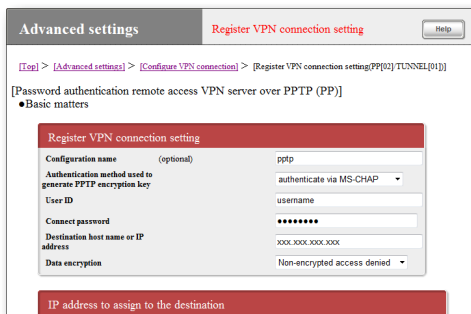
- **PP:** Only the specified host name or IP address is allowed as the destination, and the user ID and password are used for authentication.
- **Anonymous:** The destination does not get restricted, and the user ID and password are used for authentication.



4 Configure the settings required and then click “Submit”.

The connection destination is registered.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.



(Example of screen displayed when “PP” is selected in Step 3)

Configuring a server or PC in the LAN

Remote access requires settings that provide you with access to the server or PCs in the LAN via TCP/IP protocol.

Note

- The remote access function of the product does not support Windows NetBEUI protocol or Apple’s Mac OS AppleTalk protocol.
- To share files in Windows, you need to use NetBIOS over TCP/IP protocol or have a Windows Internet Name Service (WINS) server.
- To share files in Macintosh, open System Preferences, select “Sharing” and select “File Sharing” check box.

Configuring the IP addresses of the server and PCs

Assign a fixed private IP address to each PC that allows the servers or PCs on the LAN to gain external access.

Changing the settings of the file server software

Configure a network share on a server or a PC exposed to the Internet and set folders, user IDs and passwords exposed to the Internet.

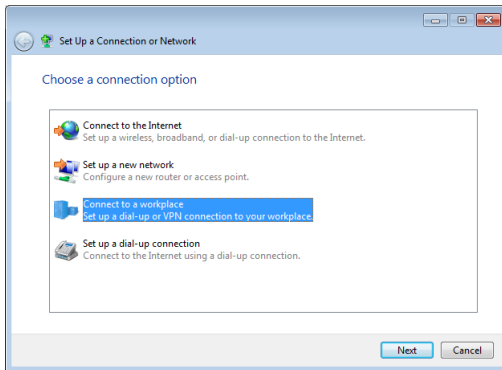
Gaining remote access using PPTP

(Continued from the previous page)

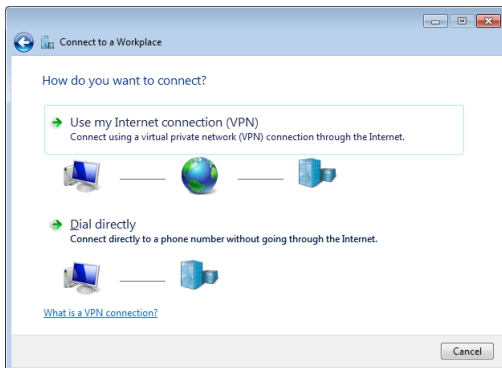
Gaining remote access from a PC that has Windows 7 installed

Changing the settings of a PC for remote accessing

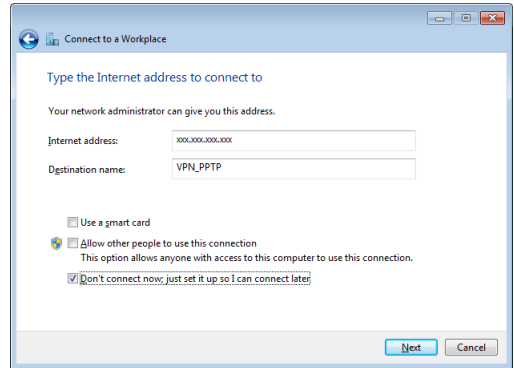
- 1 Click “View network status and tasks” in “Control Panel”.
- 2 Click “Set up a new connection or network”.
- 3 Select “Connect to a workplace” and then click “Next”.



- 4 Click “Use my Internet connection (VPN)”.



- 5 In “Internet address”, enter the host address obtained with the netvolante DNS service or the WAN IP address of the product.
- 6 Type “VPN_PPTP” in “Destination name”.

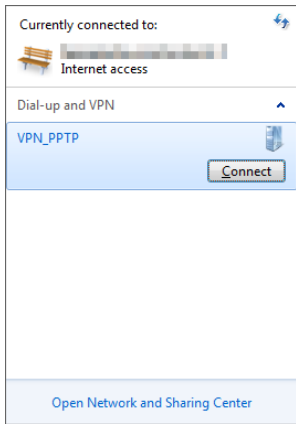


- 7 Select “Don't connect now, just set it up so I can connect later” and then click “Next”.
- 8 Click “Create” button.
- 9 Click “Close” button.

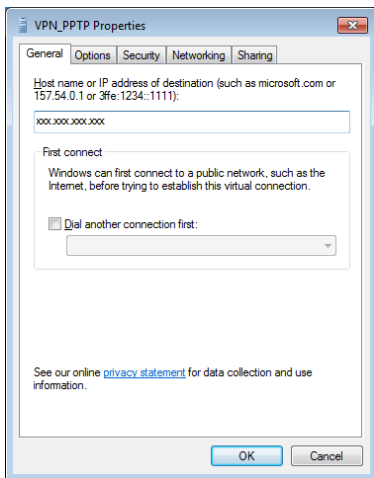
Now, the setting up of a remote access connection is complete.

Accessing the product

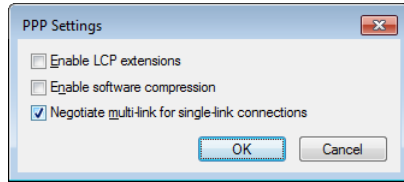
- 1 Configure broadband connections and connect the product to the Internet.
- 2 Click “View network status and tasks” in “Control Panel”.
- 3 Click “Connect to a network”.
- 4 Select “VPN_PPTP” icon and then click “Connect”.



- 5 Click “Properties”.
- 6 Click “General” tab and check that the host address obtained with the netvolante DNS service or the WAN IP address of the product has been entered in “Host name or IP address of destination”.



- 7 Click “Options” tab, and then click “PPP Settings”.
- 8 Select the check box as shown below and then click “OK”.

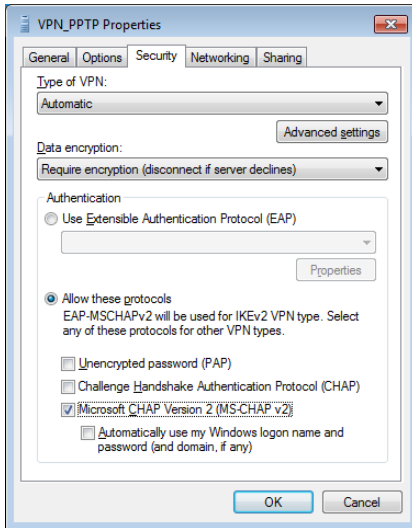


- Enable LCP extensions: Unchecked
 - Enable software compression: Unchecked
 - Negotiate multi-link for single-link connections: Checked
- 9 Click “Security” tab and then select “Automatic” for “Type of VPN”.
 - 10 Select the encryption mode according to the setting you made in Step 4 on page 73.
 - If “Non-encrypted access denied” is selected with the product: Select “Require encryption (disconnect if server declines).”
 - If “Non-encrypted access allowed” is selected with the product: Select your desired encryption level.

Gaining remote access using PPTP

(Continued from the previous page)

11 Under “Authentication”, select “Allow these protocols”, select the check boxes as shown below and then click “OK”.



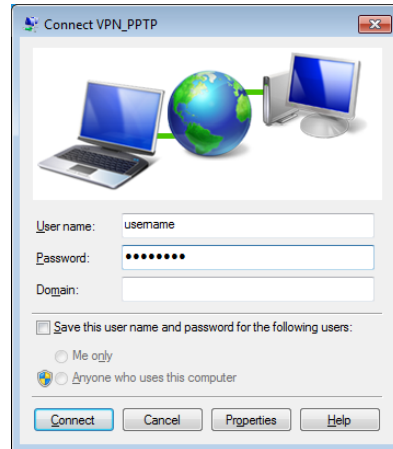
- Unencrypted password (PAP): Unchecked
- Challenge Handshake Authentication Protocol (CHAP): Unchecked
- Microsoft CHAP Version 2 (MS-CHAPv2): Checked
- Automatically use my Windows logon name and password (and domain, if any): Unchecked

Note

Windows 7 does not support Microsoft CHAP Version 1 (MS-CHAP). Note the settings you configured in Step 4 on page 76.

12 Click “OK” in “VPN_PPTP Properties” window and close the window.

13 Enter the authentication user ID in “User name” and password in “Password” you set in Step 4 on page 73 and click “Connect”.



VPN connection to the product now begins.

Note

If you select “Save this user name and password for the following users:” check box, you no longer need to enter the password. If you do not select it, you need to enter the password each time you connect to the VPN.

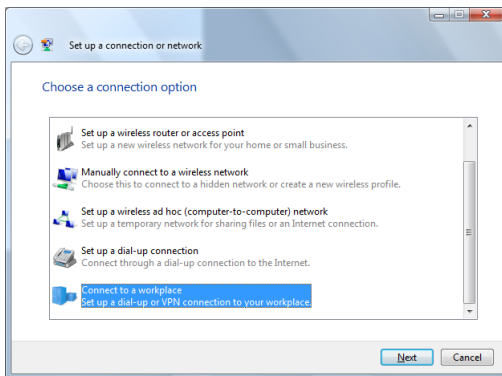
14 To disconnect from a VPN connection, click “Disconnect”.

This breaks a connection to the product.

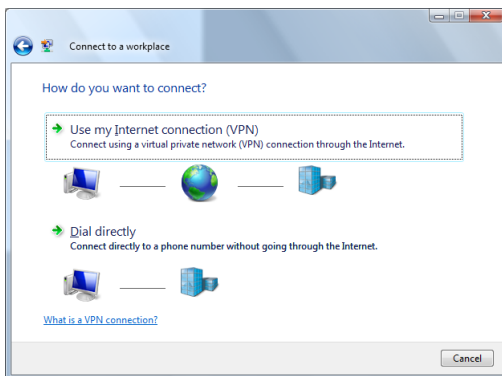
Gaining remote access from a PC that has Windows Vista installed

Changing the settings of a PC for remote accessing

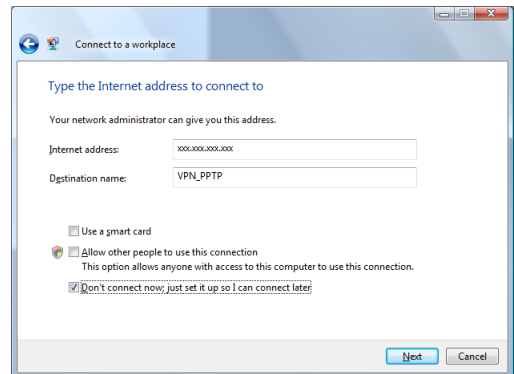
- 1 Click “View network status and tasks” in “Control Panel”.
- 2 Click “Set up a connection or network”.
- 3 Select “Connect to a workplace” and then click “Next”.



- 4 Click “Use my Internet connection (VPN)”.



- 5 In “Internet address”, enter the host address obtained with the netvolante DNS service or the WAN IP address of the product.
- 6 Type “VPN_PPTP” in “Destination name”.



- 7 Select “Don't connect now, just set it up so I can connect later” and then click “Next”.
- 8 Click “Create” button.
- 9 Click “Close” button.

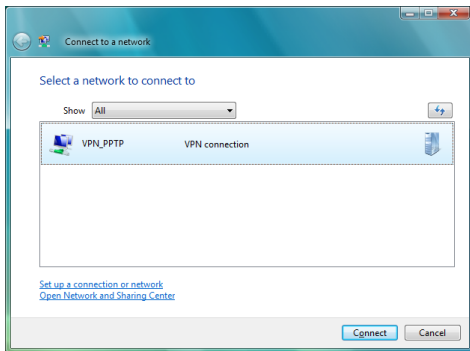
Now, the setting up of a remote access connection is complete.

Gaining remote access using PPTP

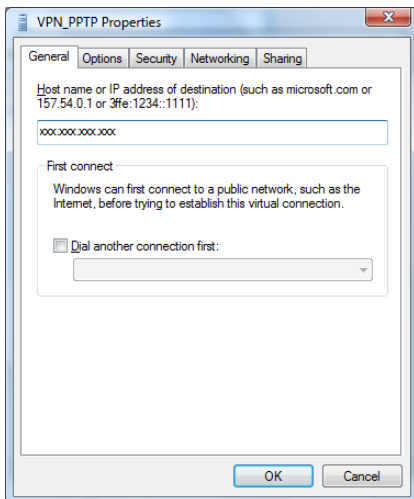
(Continued from the previous page)

Accessing the product

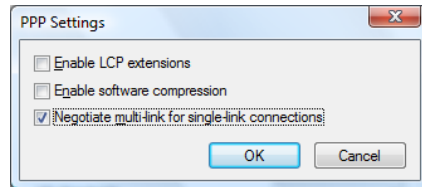
- 1 Configure broadband connections and connect the product to the Internet.
- 2 Click “View network status and tasks” in “Control Panel”.
- 3 Click “Connect to a network”.
- 4 Select “VPN_PPTP” icon and then click “Connect”.



- 5 Click “Properties”.
- 6 Click “General” tab and check that the host address obtained with the netvolante DNS service or the WAN IP address of the product has been entered in “Host name or IP address of destination”.

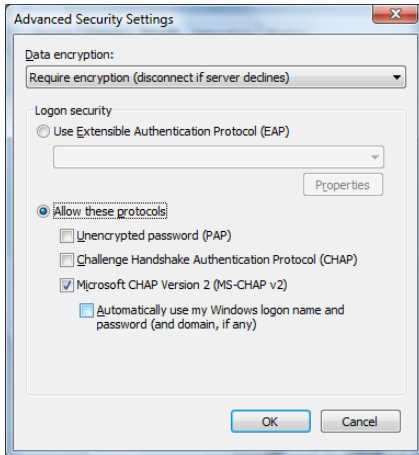


- 7 Click “Options” tab, and then click “PPP Settings”.
- 8 Select the check box as shown below and then click “OK”.



- Enable LCP extensions: Unchecked
 - Enable software compression: Unchecked
 - Negotiate multi-link for single-link connections: Checked
- 9 Click “Security” tab, select “Advanced (custom settings)” under Security options, and then click “Settings”.
 - 10 Select the encryption mode according to the setting you made in Step 4 on page 73.
 - If “Non-encrypted access denied” is selected with the product: Select “Require encryption (disconnect if server declines)”.
 - If “Non-encrypted access allowed” is selected with the product: Select your desired encryption level.

- 11 Under “Logon security”, select “Allow these protocols”, select the check box as shown below and then click “OK”.



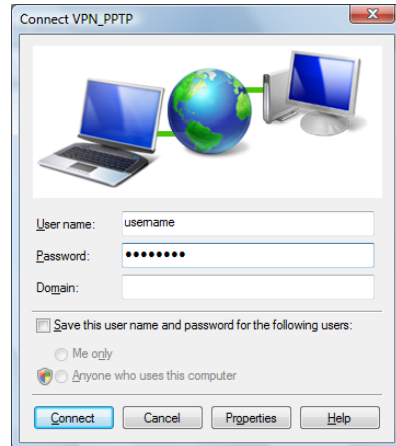
- Unencrypted password (PAP): Unchecked
- Challenge Handshake Authentication Protocol (CHAP): Unchecked
- Microsoft CHAP Version 2 (MS-CHAP v2): Checked
- Automatically use my Windows logon name and password (and domain, if any): Unchecked

Note

Windows Vista does not support Microsoft CHAP Version 1 (MS-CHAP). Note the settings you configured in Step 4 on page 73.

- 12 Click “Networking” tab and then select “Automatic” for “Type of VPN”.
- 13 Click “OK” in “VPN_PPTP Properties” window and close the window.

- 14 Enter the authentication user ID in “User name” and password in “Password” you set in Step 4 on page 73 and click “Connect”.



VPN connection to the product now begins.

Note

If you select “Save this user name and password for the following users:” check box, you no longer need to enter the password. If you do not select it, you need to enter the password each time you connect to the VPN.

- 15 To disconnect from a VPN connection, click “Disconnect”.

This breaks a connection to the product.

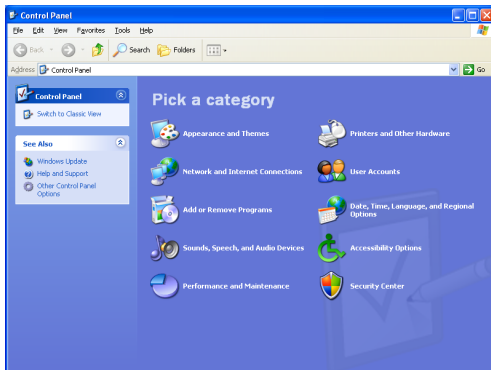
Gaining remote access using PPTP

(Continued from the previous page)

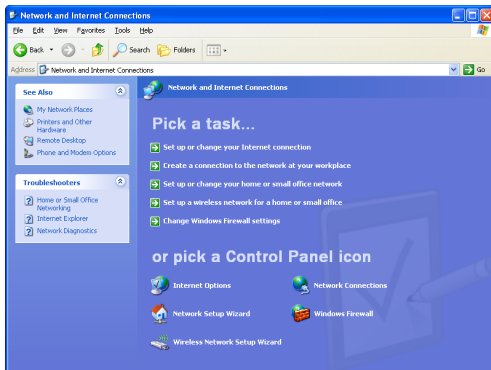
Gaining remote access from a PC that has Windows XP installed

Changing the settings of a PC for remote accessing

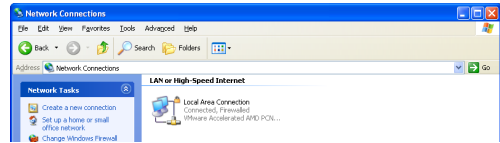
- 1 In "Control panel", click "Network and Internet Connections".



- 2 Click "Network Connections".



- 3 Click "Create a new connection".



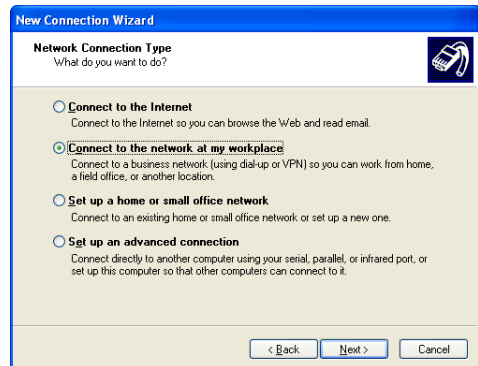
The "Welcome to the New Connection Wizard" will launch.

If the "Location Information" screen appears, enter your area code, and click "OK".

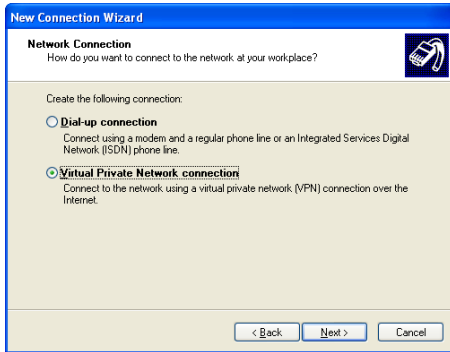
- 4 Click "Next".



- 5 Select "Connect to the network at my workplace" and then click "Next".



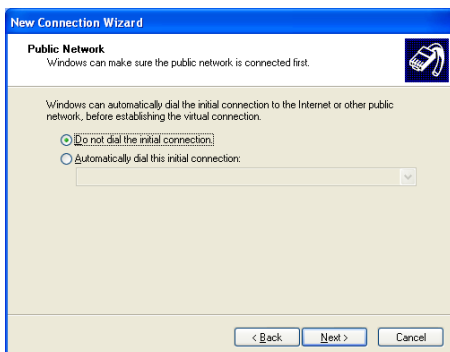
- 6 Select “Virtual Private Network connection” and then click “Next”.



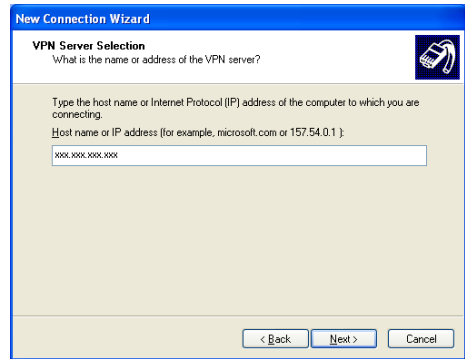
- 7 Type “VPN_PPTP” in “Company Name” and then click “Next”.



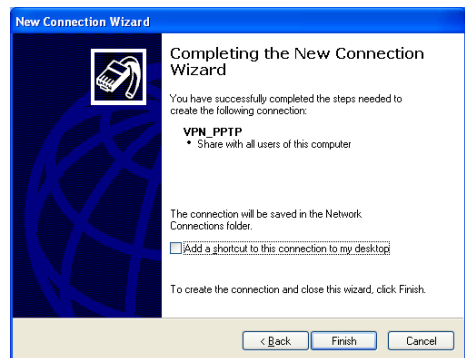
- 8 Select “Do not dial the initial connection” or “Automatically dial this initial connection” and then click “Next”.



- 9 Enter the host address obtained with the netvolante DNS service or the WAN IP address of the product and then click “Next”.



- 10 Click “Finish”.



Now, the setting up of a remote access connection is complete.



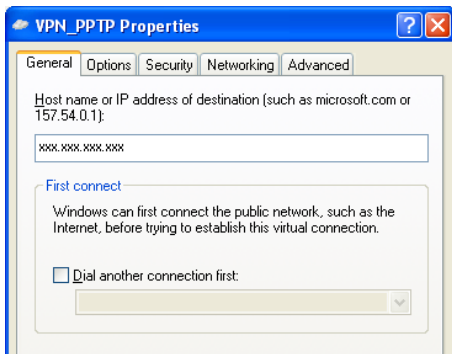
Tip
This screen appears if different dial-up settings already exist. Otherwise, it does not appear.

Gaining remote access using PPTP

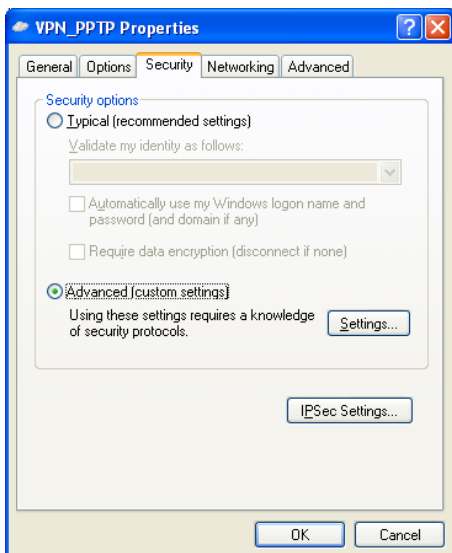
(Continued from the previous page)

Accessing the product

- 1 Configure broadband connections and connect the product to the Internet.
- 2 Double-click “VPN_PPTP” icon to bring up the “Connections” window.
- 3 Click “Properties”.
- 4 Click “General” tab and check that the host address obtained with the netvolante DNS service or the WAN IP address of the product has been entered in “Host name or IP address of destination”.

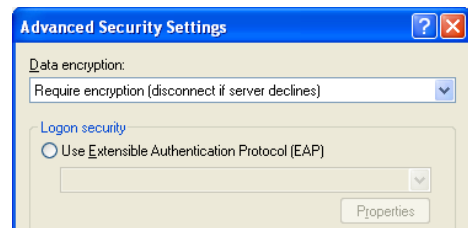


- 5 Click “Security” tab, select “Advanced (custom settings)” under Security options, and then click “Settings”.



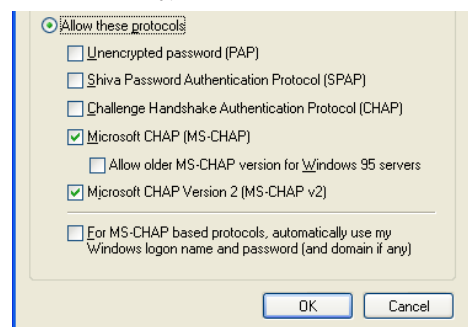
- 6 Select the encryption mode according to the setting you made in Step 4 on page 73.

- If “Non-encrypted access denied” is selected with the product: Select “Require encryption (disconnect if server declines)”.
- If “Non-encrypted access allowed” is selected with the product: Select your desired encryption level.

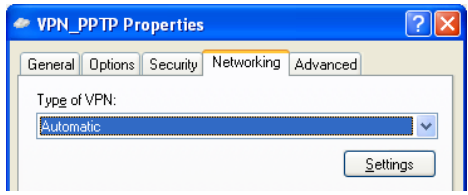


- 7 Under “Logon security”, select “Allow these protocols”, select the check boxes as shown below and then click “OK”.

- Unencrypted password (PAP): Unchecked
- Shiva Password Authentication Protocol (SPAP): Unchecked
- Challenge Handshake Authentication Protocol (CHAP): Unchecked
- Microsoft CHAP (MS-CHAP): Checked
- Allow older MS-CHAP version for Windows 95 servers: Unchecked
- Microsoft CHAP Version 2 (MS-CHAP v2): Checked
- For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain, if any): Unchecked

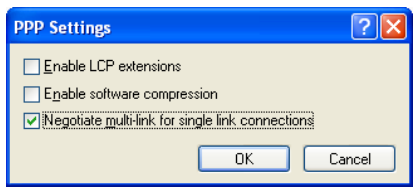


8 Click “Networking” tab, select “Automatic” for “Type of VPN” and then click “Settings”.



9 Select the check box as shown below and then click “OK”.

- Enable LCP extensions: Unchecked
- Enable software compression: Unchecked
- Negotiate multi-link for single-link connections: Checked



10 Click “OK” in “VPN_PPTP Properties” window and close the window.

11 Enter the authentication user ID in “User name” and password in “Password” you set in Step 4 on page 73.



12 Click “Connect”.



VPN connection to the product now begins.

Note
If you select the “Save this user name and password for the following users” check box, you no longer need to enter the password.

13 To disconnect from a VPN connection, click “Disconnect”.

This breaks a connection to the product.

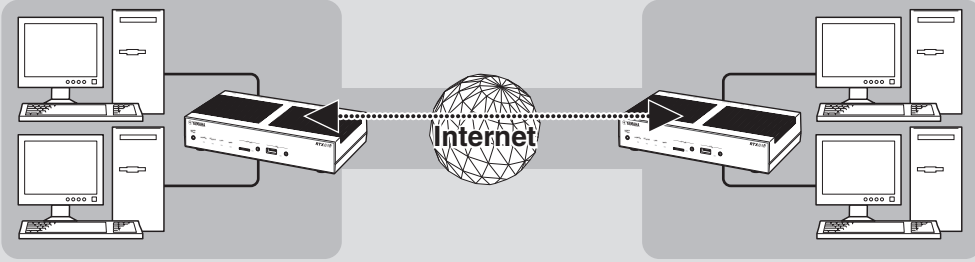
Creating a Virtual Private Network (VPN) using PPTP (PPTP-LAN-to-LAN connection)

You can create a Virtual Private Network (VPN) to connect LANs if the product is connected to a broadband Internet connection. LAN-to-LAN connection using PPTP ensures secure connection via the Internet.

A VPN can be created using conventional broadband connections such as ADSL. Thus, VPNs are cheaper than real private networks using dedicated lines. The LAN-to-LAN connection of the product supports TCP/IP server software.

4

Implementing site-to-site VPN connections



Creating a Virtual Private Network (VPN) using PPTP

PPTP that can be used with the product

- The product supports data encryption for PPTP. The RC4 (either 40- or 128-bit keys) is used as the encryption algorithm.
- The product supports user and password authentication based on MS-CHAP and MS-CHAP v2.
- You can specify whether or not to block incoming traffics if an MPPE encryption does not come into effect (access control).
- The product does not support compression. In the PPP setup on the PPTP client side, deselect the “Enable software compression” check box.
- PPTP uses TCP port 1723 for tunnel control and GRE protocol number 47 for data communication. When a PPTP server is installed inside of a firewall or use NAT in combination with a remote access VPN server, be sure to pass TCP port number 1723 and GRE protocol number 47. For details, contact your network administrator.
- A disconnection timer monitors the communication and a PPTP session is disconnected if data does not pass through a PPTP tunnel for a certain amount of time.
- The product does not support PPP forwarding.

Note

- Because PPTP tunnels are to be configured with the router connected to a broadband connection, it will be necessary to configure the broadband connections before setting up the LAN-to-LAN connection using PPTP.
- PPTP-based LAN-to-LAN connection can be used only in an environment where a global IP address is assigned by your provider. Note that the following IP addresses are not global IP addresses:
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- When using the LAN-to-LAN connection, be sure to configure adequate security settings to maintain data integrity. Inadequate security settings may cause PCs in the LAN to be hacked, sniffed, intercepted, or destroyed, or their data to be lost.
- The LAN-to-LAN connection of the product does not support Windows NetBEUI protocol or Apple's Mac OS AppleTalk protocol.
- To share files in Windows, you need to use NetBIOS over TCP/IP protocol or have a Windows Internet Name Service (WINS) server.
- To share files in Macintosh, open System Preferences, select “Sharing” and select “File Sharing” check box.

Before configuring the settings

- To connect LANs, it will be necessary to configure a different network address for each LAN to avoid overlapping. Change the product's LAN network address in advance.
- To attach the product to a LAN with a different network address assigned, change the configuration of the product according to the network you install. Please refer to “Configuring the IP address on the LAN side” (page 29) for more information.

Creating a Virtual Private Network (VPN) using PPTP (PPTP-LAN-to-LAN connection) (continued from the previous page)

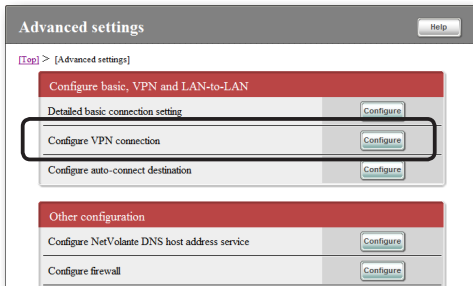
4

Implementing site-to-site VPN connections

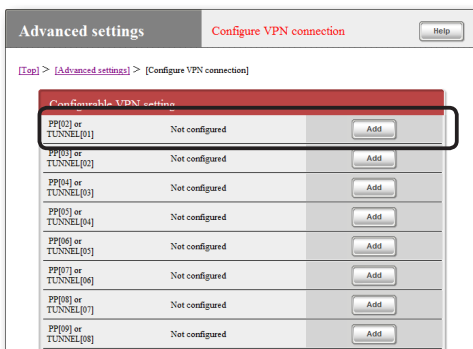
Configuring the product to use PPTP

Configure the settings required for the product to act as a PPTP server or client. Configure the RTX810 attached to the LAN on the connecting end as a PPTP client and the RTX810 attached to the LAN on the connected end as a PPTP server.

- 1 On the top page of “Basic configuration page”, click “Advanced settings”, then click “Configure” to the right of “Configure VPN connection”.

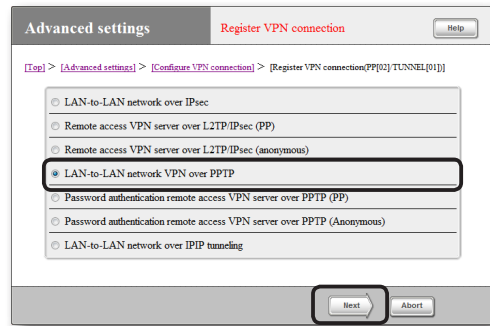


- 2 Click “Add” to the right of the destination you want to register.



- 3 Select “LAN-to-LAN network VPN over PPTP” and then click “Next”.

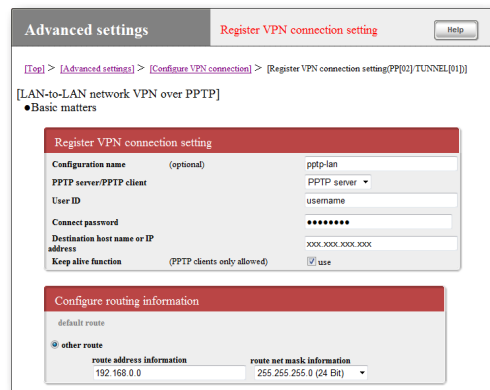
The “Register VPN connection setting” screen appears.



- 4 Configure the required settings and then click “Submit”.

The connection destination is registered.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.



Connecting with PPTP

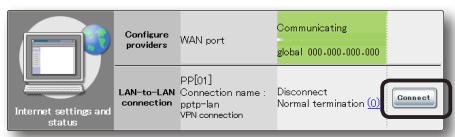
Connect to a PPTP server.

Note

- To connect to a PPTP server, the product for which you perform the following operation must be configured as a PPTP client.
- The “Connect” and “Disconnect” buttons appear when the product is configured as a PPTP client.

On the top page of “Basic configuration page”, click “Connect” to the right of the PPTP settings you want connect to under “LAN-to-LAN connection”.

Connect to the registered PPTP server to create a PPTP-LAN-to-LAN connection.



To disconnect a PPTP-LAN-to-LAN connection:
Click “Disconnect” under “LAN-to-LAN connection” on the top page of “Basic configuration page”.

Note

Clicking “Disconnect” only ends a PPTP session and the connection with your provider is not terminated.

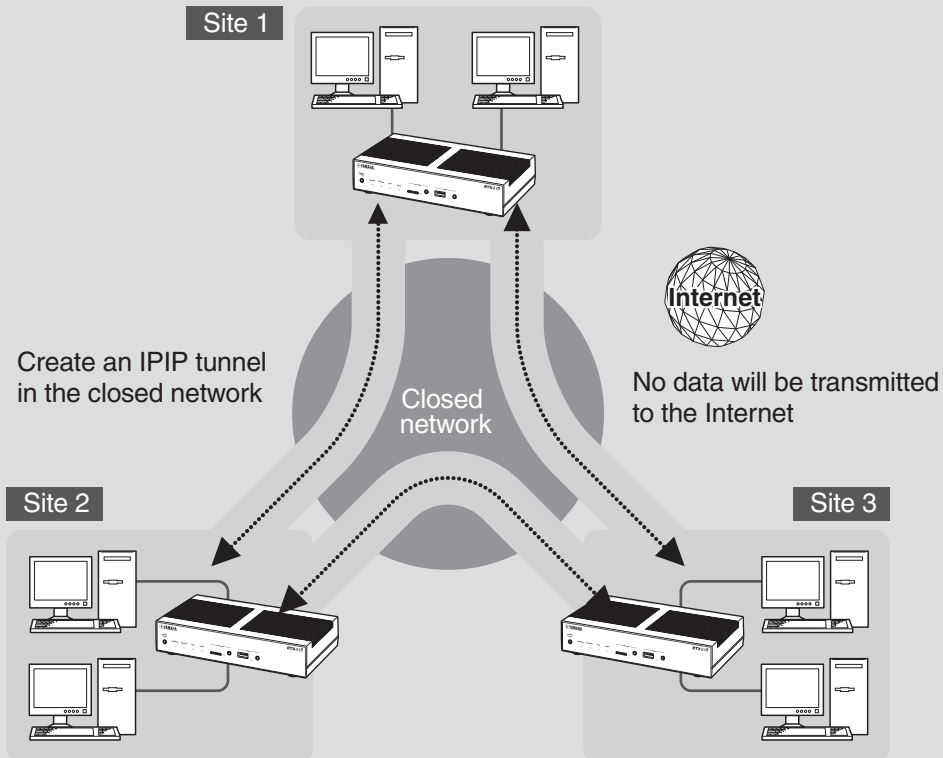
Linking LANs together through IPIP tunnels using a closed network

LAN-to-LAN connections via the Internet involve the risk of data wiretapping or tampering. Thus, it will be necessary to encrypt data. For a highly confidential network such as a closed network, the need for data encryption is reduced. Because of this IPIP tunnel connections assure data confidentiality.

The following explains how to set up LAN-to-LAN connections with IPIP tunnels by connecting to a closed network based on a contract in which only one fixed IP address is issued.

4

Implementing site-to-site VPN connections



Before configuring the settings

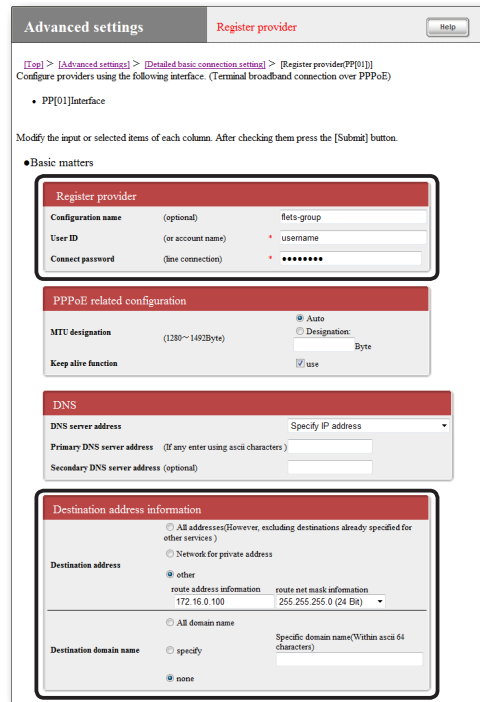
- To connect LANs, it will be necessary to configure a different network address for each LAN to avoid overlapping. Change the product's LAN network address in advance.
- To attach the product to a LAN with a different network address assigned, change the configuration of the product according to the network you install. Please refer to “Configuring the IP address on the LAN side” (page 29) for more information.

Note

- With IPIP tunnel connections, data is transferred without being encrypted. The use of IPIP tunnel connections with no data encryption on the Internet is very dangerous. Do not use the IPIP tunnel connections on the Internet.
- Before configuring the IPIP tunnel connections, it is required to configure the connection to a closed network.
- When using the LAN-to-LAN connection, be sure to configure adequate security settings to maintain data integrity. Inadequate security settings may cause PCs in the LAN to be hacked, sniffed, intercepted, or destroyed, or their data to be lost.
- The LAN-to-LAN connection of the product does not support Windows NetBEUI protocol or Apple's Mac OS AppleTalk protocol.
- To share files in Windows, you need to use NetBIOS over TCP/IP protocol or have a Windows Internet Name Service (WINS) server.
- To share files in Macintosh, open System Preferences, select “Sharing” and select “File Sharing” check box.

Configuring the product to connect to a closed network

To connect the product to a closed network, configure the required settings in the “Terminal broadband connection over PPPoE” screen.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Terminal broadband connection over PPPoE” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” to the right of “Detailed basic connection setting”
- ▶ “Add” to the right of the destination you want to add settings
- ▶ Select “Terminal broadband connection over PPPoE” and then click “Next”.

Linking LANs together through IPIP tunnels using a closed network (Continued from the previous page)

1 Enter necessary setup information.

Configuration name

Enter a descriptive destination name.

User ID

Enter the specified user ID.

Connect password

Enter the specified password (or the password you changed).

Destination address information

- Destination address: Click “other” and then configure the following settings.
 - route address information: Enter the IP address assigned to the connection destination
 - route net mask information: Select “255.255.255.255 (32 bits)”.
- Destination domain name: Click “none”.

2 Click “Submit”.

The “Register provider” screen appears.

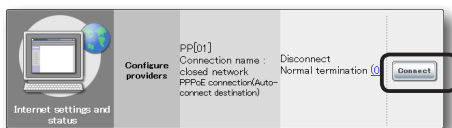
3 To connect the product to multiple LANs, click “Back” and repeatedly configure “Destination address information”.

Specify all IP addresses assigned to the connection destinations for the route.

After you have set all destination addresses for the connection destinations, click “Return to top” to return to the top page of the “Basic configuration page”.

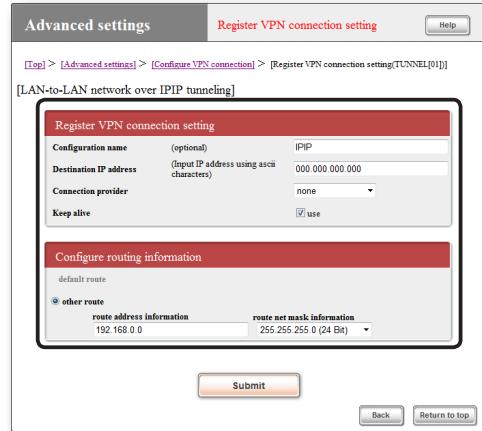
Connecting to a closed network

On the top page of “Basic configuration page”, click “Connect” to the right of the setting for the closed network connection under “Configure providers”.



Configuring the product to use IPIP tunnels

To use the product and destination equipment by connecting them with IPIP tunnels, configure the required settings in the “LAN-to-LAN network over IPIP tunneling” screen.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “LAN-to-LAN network over IPIP tunneling” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” to the right of “Configure VPN connection”
- ▶ “Add” to the right of the VPN destination you want to add settings
- ▶ Select “LAN-to-LAN network over IPIP tunneling” and then click “Next”

- 1 Enter necessary setup information.

Configuration name

Enter a descriptive destination name.

Destination IP address

Enter the IP address assigned to the connection destination.

Connection provider

Specify the configurations used for a closed network connection (configurations you set on page 89).

Note

When separately configuring the PPPoE connection for Internet access, you should exercise care not to incorrectly specify the connection setting for Internet access.

Configure routing information

Enter the network address of the destination LAN in “route address information” and “route net mask information”.

- 2 Click “Submit”.

The “Register VPN connection setting” screen appears.

- 3 To connect the product to multiple LANs, click “Back” and repeatedly configure “Configure routing information”.

Configure the routing information for each connection destination.

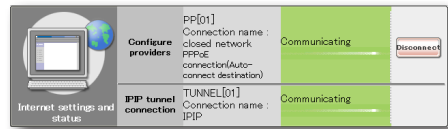
Note

Correctly set a combination of the IP addresses assigned to connection destinations and network address of its destination LAN.

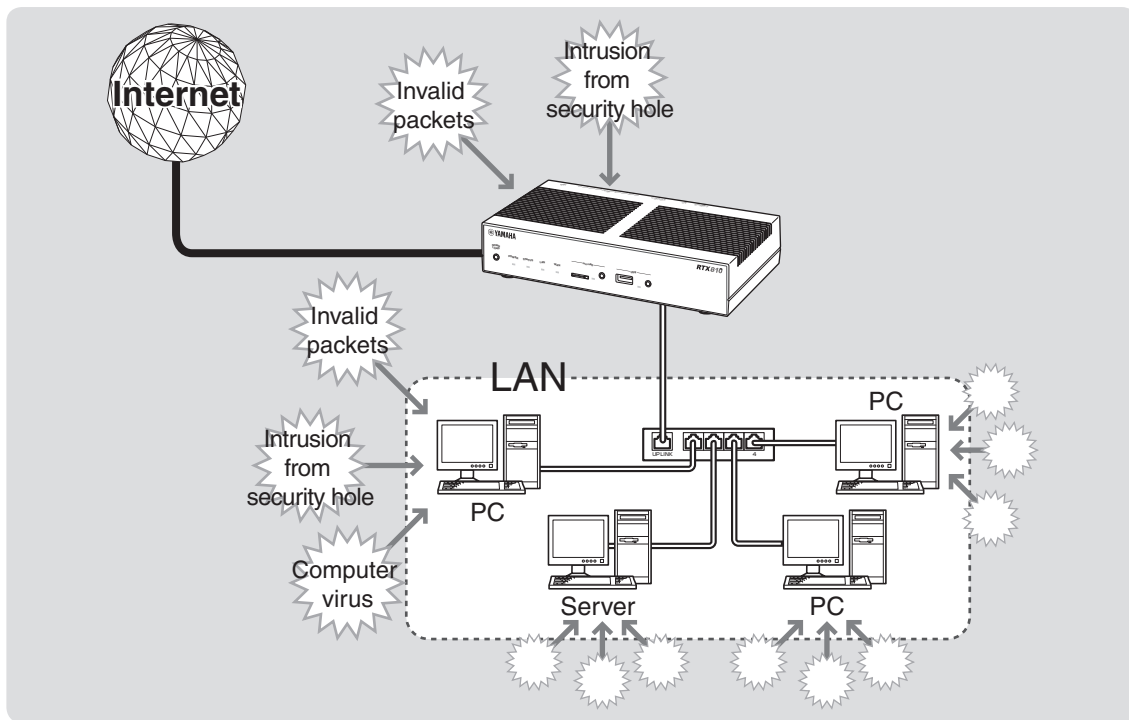
After you have set all routing information for the connection destinations, click “Return to top” to return to the top page of the “Basic configuration page”.

Creating IPIP tunnel connections

Once the above configurations have been completed, IPIP tunnel communications are automatically established (no manual operations are required). Once the IPIP tunnel connections are complete, the top page of the “Basic configuration page” shows a message, “Communicating”.



Outline of unauthorized accesses and security measures



What is unauthorized access from the Internet?

- While you are accessing the Internet, malicious individuals may attack (gain unauthorized access to) your PC or router to destroy the data or use the line without permission. If a router is installed between your PC and the Internet, then NAT, IP masquerade, and other address conversion functions of the router can provide security to a certain degree. However, even in such an environment, possible setting errors or inadequate settings pose a similar risk.
- In addition to unauthorized accesses via the Internet, you should also be aware of the risk of attacks by computer viruses.
- Should the settings of the product be modified or the PC system or data be destroyed, a massive amount of data and monetary damages would be resulted. You must configure filter settings of the product or take other security measures to protect your system.

A particular attention is required if a global IP address is assigned to your LAN

Malicious individuals mainly use “global IP addresses” to gain a foothold for attack. The longer the same global IP address is used, the higher the probability of unauthorized access to the LAN.

When using a fixed IP address service, or using a network that keeps using a dynamic address assigned upon connection with the Internet, we recommend that you configure adequate security settings.

You should also give heed to the password setting

Using the product without setting a password will pose a great risk for security. Be sure to set the password, and change it periodically.

Addressing unauthorized accesses

Unauthorized accesses to the Internet can be divided into several types. The following shows each type of unauthorized access and measures to be taken against it.

Note

- New unauthorized access methods and security loopholes (security holes) are constantly being discovered. We would like you to understand that there is no completely infallible security measures that can solve all the problems, and that connecting to the Internet always involves risk. The functions included in the product are no exception. Thus, we strongly recommend that you constantly obtain the latest information and enhance the security settings under your own responsibility.
- Please note that Yamaha cannot accept any liability for any losses or damage resulting from incorrect use.

1. Intrusions using invalid packets

- The most effective action is disconnecting the Internet or changing the global IP address.
- Using a packet filtering firewall to block unwanted packets is also effective to a certain extent.
- It is also considerably effective to use the firewall software of application gateway type because it blocks inconsistent packets, or dubious ActiveX and Java applets from entering PCs. Virus detection software can be used in combination with it. In this case, however, you should set up a firewall server where to install the firewall software of application gateway type.

Measures to be taken in the product

- Enable the auto-disconnect function so that an assigned dynamic IP address can be changed each time the product is disconnected/connected. However, this measure is difficult to implement when you use the product for the purpose of having a public server in place. In that case, take appropriate measures in the server.
- You may be able to block a certain type of attack by configuring a filter to block specific types of packets (page 96) used for the attack.

2. Intrusions exploiting security holes of the operating system or server software

This type of unauthorized access can be prevented at a high rate by upgrading the operating system or server software, configuring proper settings, or conducting adequate management.

Measures to be taken in the product

- Changing a product setting by malicious third persons can be prevented by restricting hosts that can change the product settings (page 100).
- You may be able to block a certain type of attack by configuring a filter to block specific types of packets (page 96) used for the attack.

3. Intrusions as e-mail attachment files (computer viruses)

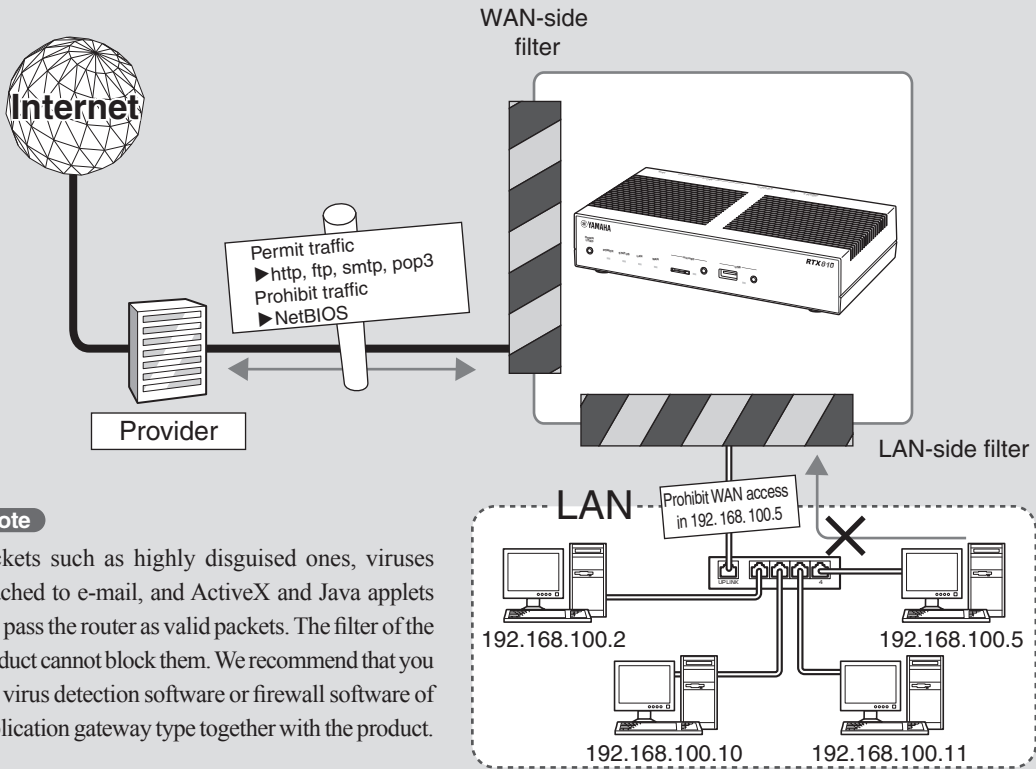
Your PC is infected with a virus by opening an attached file. Do not open any dubious attachment files, and install virus detection software on PCs to detect viruses and clean them at an early stage so that damage can be minimized.

Measures to be taken in the product

- Security enhancement functions included in the product are not effective against computer viruses.
- Prepare PC virus detection software separately.

Configuring the filter settings

In the product, up to 100 filters can be set for each connection destination. Each filter can block packets depending on the packet transmission source or destination, the protocol type, or the direction. Invalid packets can be prevented from entering your LAN by setting impossible packets or packets that may be used for unauthorized accesses to be discarded when they pass the router.



Note

Packets such as highly disguised ones, viruses attached to e-mail, and ActiveX and Java applets can pass the router as valid packets. The filter of the product cannot block them. We recommend that you use virus detection software or firewall software of application gateway type together with the product.

What is “Packet”?

A packet is a unit of data that flows through the network. Data flowing through the network is divided in units of a packet, and each packet has information about the transmission source/destination and the data type.

The filter function of the router enables you to set packet conditions to prevent unwanted connections, or specify destinations of the packets to configure different connection destination settings.

Features of the filter of the product

Static filter and dynamic filter

The following two types of filters can be configured in the product. Use advantages of each type together to configure your settings.

- **Static filter:** Once this filter has been configured, it is constantly enabled irrespective of presence of data or communication.
- **Dynamic filter:** This filter monitors the communication status and is enabled on an as-needed basis. For example, you can configure a setting such as “normally prohibiting all data from the Internet to LAN, but permitting only when an access from LAN to ftp occurs”.

When a connection destination is registered in “Basic configuration page”, the basic filter is applied

Only by registering a connection destination with “Basic configuration page”, the following filter is automatically applied according to the connection type. In addition to this basic filter, you can add, register, and apply filters if necessary.

Note

- Security levels and settings are subject to change without notice.
- If you specify a connection destination using the console, no filter is registered.

For provider configuration

Seven security levels are defined as filter combination patterns. When a new provider is registered, the security level 6 settings are automatically applied. The security level can be changed at a later time if necessary. (page 96)

Filter number indication

You can use almost unlimited filter function numbers of the product. In “Basic configuration page”, up to 100 numbers (0 to 99) can be set for each destination. The following shows the correspondence between areas and filter numbers used in “Basic configuration page”.

Assigned area	Console command filter numbers
LAN/WAN port area	100000 - 199999
Connection destination setting area (PP01 -)	200000 - 299999
Filter type routing area	500000 - 599999

Note

- Before changing a filter setting, you should fully understand the function to assure security.
- Applying too many filters may complicate the processing, causing the Internet access speed to be slow.

Configuring filter settings (Continued from the previous page)

Registering a filter

The concept of filter settings intended for security

We recommend that you configure filter settings based on the following point of view:

In principle, permit accesses from the LAN to the Internet, and prohibit some accesses if necessary

If you strictly control accesses from the LAN to the Internet, the system would be extremely difficult to use, and it would subsequently create problems in terms of management and changing settings. Therefore, permit any access in principle and, if there is a problem, only restrict access related to the problem.

In principle, prohibit accesses from the Internet to the LAN, and permit some accesses if necessary

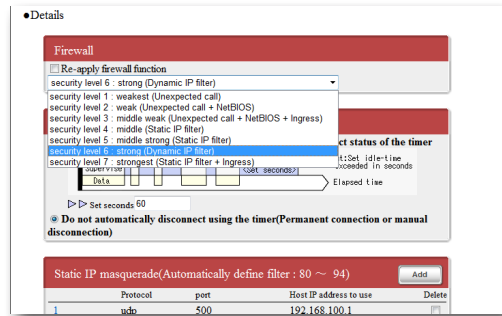
Prohibit accesses from the Internet to the LAN in principle so that external accesses can be prevented. Permit the external accesses only if necessary, for example, to your public web server.

Note

The access from the Internet indicates a packet with which the request is started from the Internet. A packet responded to a request packet sent from the LAN has an identifier called ACK flag, which can be differentiated from accesses from the Internet and allowed to pass the filter.

Select a default filter set (security level)

In the product “Basic configuration page”, seven security levels are defined by combining filters. When you register a new provider, a security level is set automatically according to the connection type (page 95). The set security level can be changed from the “Register/Modify provider” screen.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Register/Modify provider” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

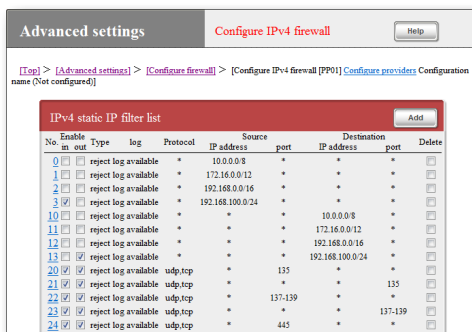
- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Detailed basic connection setting”
- ▶ “Configure” of the destination of which settings you want to change

Create a filter manually in “Basic configuration page”

To configure filter settings, use the “Configure firewall” screen.

Note

- When you select LAN, PCs connected to the LAN ports and all PCs connected to the hubs that are connected to the LAN ports are the targets.
- Please refer to “Command reference” (included in the attached CD-ROM) for examples of actual filter settings.



No.	Enable	in	out	Type	log	Protocol	Source IP address	Source port	Destination IP address	Destination port	Delete
0	<input type="checkbox"/>			reject log available	*	*	10.0.0.0/8	*	*	*	<input type="checkbox"/>
1	<input type="checkbox"/>			reject log available	*	*	172.16.0.0/12	*	*	*	<input type="checkbox"/>
2	<input type="checkbox"/>			reject log available	*	*	192.168.0.0/16	*	*	*	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>			reject log available	*	*	192.168.100.0/24	*	*	*	<input type="checkbox"/>
10	<input type="checkbox"/>			reject log available	*	*	*	10.0.0.0/8	*	*	<input type="checkbox"/>
11	<input type="checkbox"/>			reject log available	*	*	*	172.16.0.0/12	*	*	<input type="checkbox"/>
12	<input type="checkbox"/>			reject log available	*	*	*	192.168.0.0/16	*	*	<input type="checkbox"/>
13	<input checked="" type="checkbox"/>			reject log available	*	*	*	192.168.100.0/24	*	*	<input type="checkbox"/>
20	<input checked="" type="checkbox"/>			reject log available	udp	tcp	*	135	*	*	<input type="checkbox"/>
21	<input checked="" type="checkbox"/>			reject log available	udp	tcp	*	*	135	*	<input type="checkbox"/>
22	<input checked="" type="checkbox"/>			reject log available	udp	tcp	*	137-139	*	*	<input type="checkbox"/>
23	<input checked="" type="checkbox"/>			reject log available	udp	tcp	*	*	*	137-139	<input type="checkbox"/>
24	<input checked="" type="checkbox"/>			reject log available	udp	tcp	*	445	*	*	<input type="checkbox"/>

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure firewall” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure firewall”
- ▶ “Configure” of the interface for which you want to configure the firewall (“Configure” of “IPv4 filter” for setting with IPv4, or “Configure” of “IPv6 filter” for setting with IPv6).

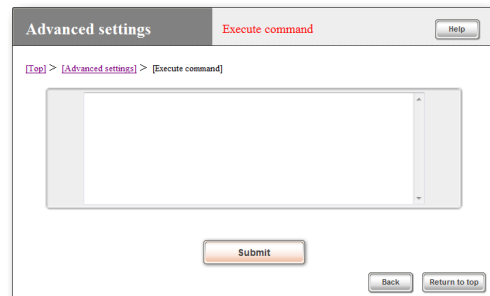
Create a filter by entering a filter command directly

You can also enter a filter command directly to create a filter. Creating a filter command previously by using a text editor program is convenient when you want to apply a filter to multiple routers.

To enter a filter command directly, use the “Execute command” screen in the “Basic configuration page”.

Tip

For examples of more professional filter settings and the grammar, please refer to “Command reference” (included in the attached CD-ROM) or the Yamaha network peripheral equipment website (<http://www.yamaha.com/products/en/network/>).



To open the “Execute command” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Execute” of “Execute command”

Detecting unauthorized accesses and warning about them

The intrusion detection function detects intrusions and attacks from the Internet and warns you about them. It helps enhance security by configuring a filter that can block suspicious transmission sources and applications to based on the detected information.



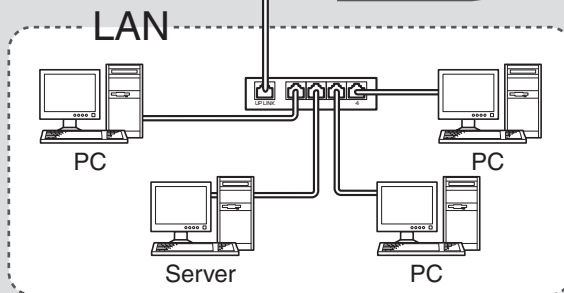
This function compares packets passing through the router with the database of intrusion/attack patterns in the router, and records/discards a packet if unauthorized access is suspected.

Invalid access database

- XXXXXXXXXXXX
- XXXXX
- XXXXXXXX
- XXXXXX

Note

- Note that new unauthorized access methods and intrusion/attack patterns are constantly being discovered and thus no completely infallible prevention method exists. We would like you to understand that not all of unauthorized accesses can be detected by this function.
- As this function detects accesses that are similar to intrusions/attack patterns, some unauthorized accesses may not be detected due to timing or a range of other reasons. On the other hand, a detected pattern does not automatically mean that a serious unauthorized access has occurred. Please understand this and use this function only as a guide for your security management.
- This function can apply to each interface and I/O.
- Using this function decreases the speed of accessing the Internet, etc.

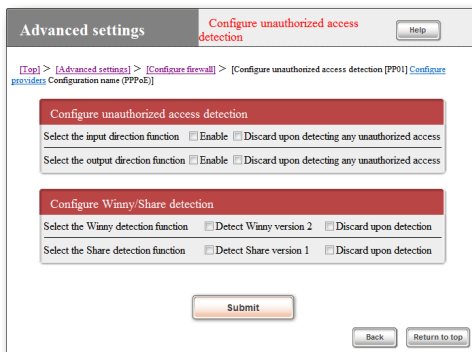


Configuring the intrusion detection function

In the “Configure unauthorized access detection”, you can set the direction of packets to be detected and the processing method upon detection, for each PP (provider or other external connection) or LAN (LAN connection) interface.

Note

The intrusion detection function can apply to each interface and I/O, but the larger number of applications may decrease the speed of accessing the Internet, etc.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure unauthorized access detection” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure firewall”
- ▶ “Configure” of “Illegal access detection” of the interface of which intrusion detection function settings you want to change.

Checking the history of illegal access detection

The history of illegal access detection can be checked in the “Intrusion detection information” field of the “Generate report on system information” screen.

Note

- The “Intrusion detection information” field of the “Generate report on system information” screen is displayed only when the illegal access detection is enabled.
- Note that new unauthorized access methods and intrusion/attack patterns are constantly being discovered and thus no completely infallible prevention method exists. We would like you to understand that not all of unauthorized accesses can be detected by this function.
- As this function detects accesses that are similar to intrusions/attack patterns, some unauthorized accesses may not be detected due to timing or a range of other reasons. On the other hand, a detected pattern does not automatically mean that a serious unauthorized access has occurred. Please understand this and use this function only as a guide for your security management.

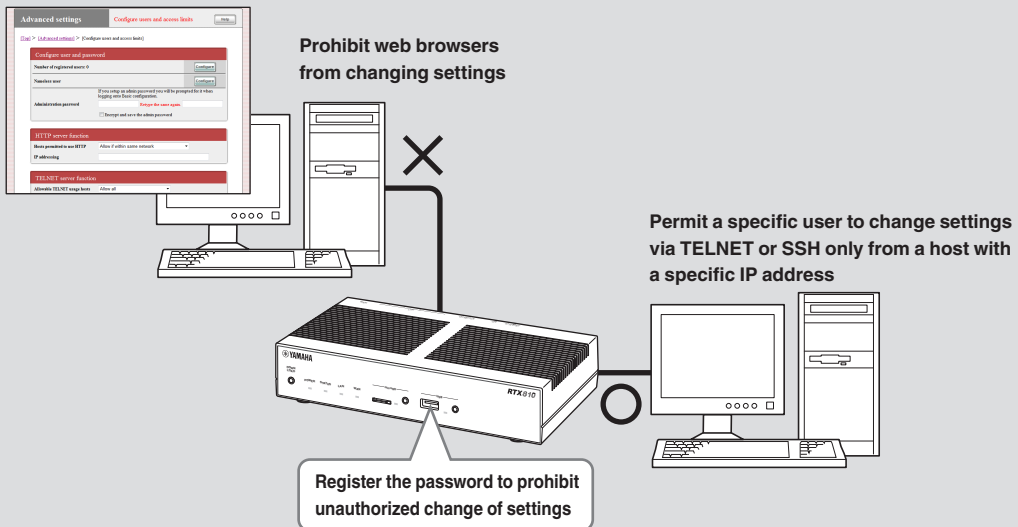
To open the “Generate report on system information” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Execute” of “Generate report on system information”

Restrict hosts that can change product settings

The product is equipped with password function and host restricting function to assure the security of the product itself. Using those functions enables you to prevent third persons from changing a router setting without permission. The product can be accessed by means of the web browser (HTTP), TELNET, SSH, or SFTP software. You can configure the restriction individually for each of them.



Setting the restriction for each individual service

In the “Configure users and access limits” screen, you can restrict hosts that can change a product setting using the web browser (HTTP), TELNET, SSH, or SFTP software. In addition to restricting the IP addresses of hosts that can access the product for each individual service, you can also restrict the number of users allowed to connect simultaneously.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

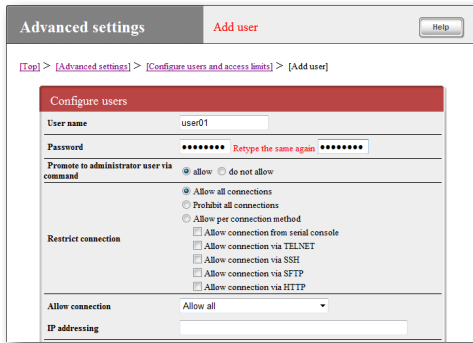
To open the “Configure users and access limits” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure users and access limits (HTTP, TELNET, SSH, SFTP)”

Registering users logging in the product

You can register users on the “Add user” screen, and restrict users who can log in the product. This function enables you to specify available services and other detailed rights for each user, and therefore is convenient when you want to set detailed access restrictions.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

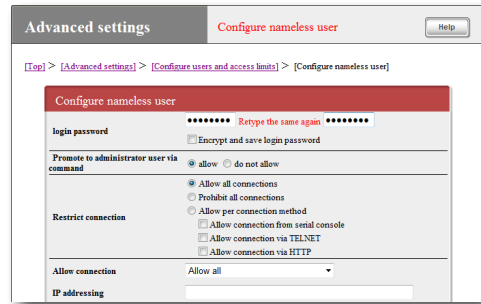
To open the “Add user” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure users and access limits(HTTP, TELNET, SSH, SFTP)”
- ▶ “Configure” of the “Number of registered users” field

You can also restrict access from anonymous users

Access restriction for using anonymous users can be defined by configuring the settings on the “Configure nameless user” screen.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure nameless user” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure users and access limits(HTTP, TELNET, SSH, SFTP)”
- ▶ “Configure” of the “Nameless user” field

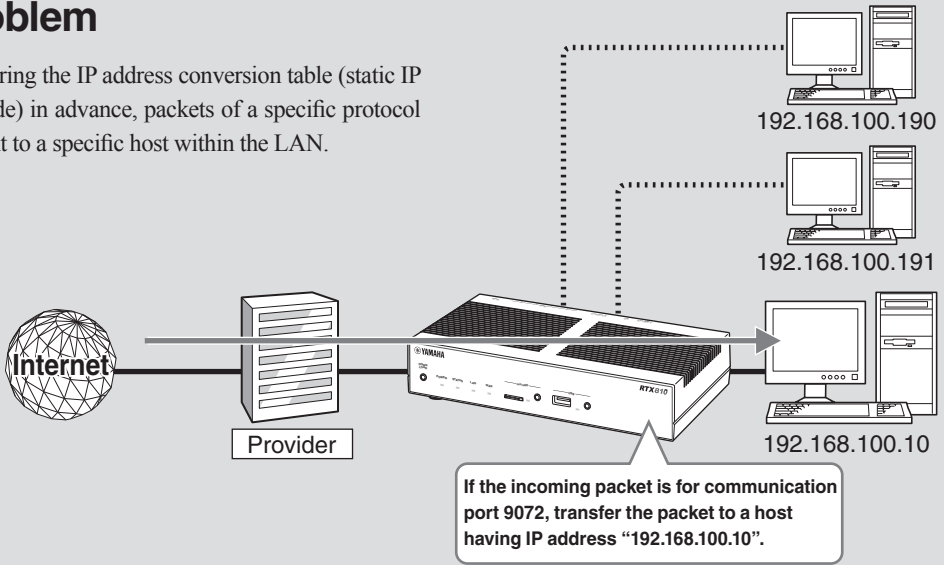
Using a service requiring a global IP address within LAN

When you attempt to use an application program that requires a global IP address from your LAN via the router, the program may not operate correctly. You can solve the problem using either of the following methods.

1. Registering the conversion table of protocol, port number and the host IP address. (Static IP masquerade).
2. Using the DMZ host function.

1. Using the static IP masquerade setting to solve the problem

By registering the IP address conversion table (static IP masquerade) in advance, packets of a specific protocol can be sent to a specific host within the LAN.



1. Set the IP addresses of PCs.

Assign a fixed private IP address to the PC for which you want to permit external access.

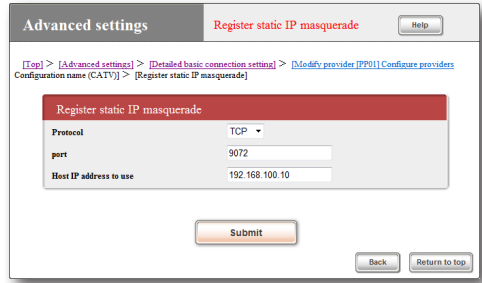
2. Register the IP address conversion table.

In the "Register static IP masquerade" screen, register the conversion table of protocol, port number and the host IP address. (Static IP masquerade settings)

Note

- For information about the protocol and port number, please refer to the manual of the software or service to be used.
- So far as representative software programs are concerned, you can click "Help" on the "Register static IP masquerade" screen to confirm the port number to be used and other setting examples.

For more details on the settings, click "Help" on the setup screen and refer to the description displayed.



To open the "Register static IP masquerade" screen

From "Basic configuration page", click the buttons on the setup screen in the following order:

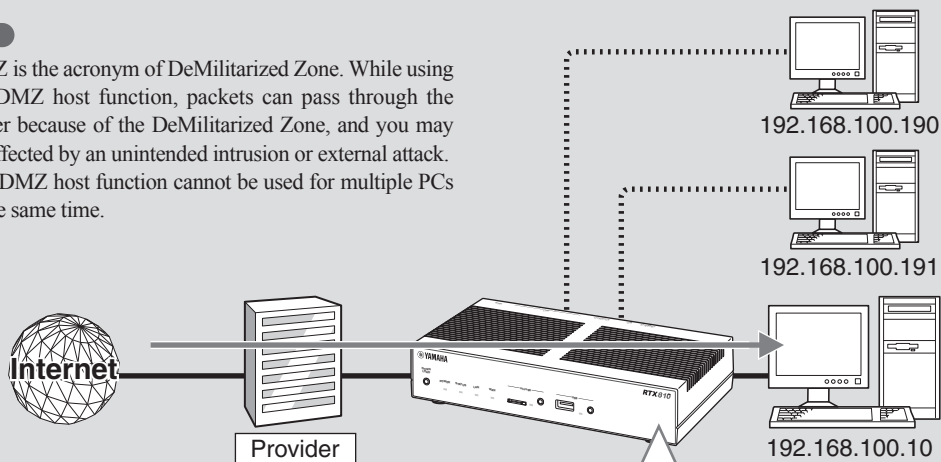
- ▶ "Advanced settings" in the top page
- ▶ "Configure" of "Detailed basic connection setting"
- ▶ "Configure" of the destination of which settings you want to change
- ▶ "Add" in the "Static IP masquerade" field

2. Using the DMZ host function to solve the problem

When the product receives a packet sent to an address that is not registered in the NAT/IP masquerade table, the packet will be transferred to a host with a specific IP address. This setting is possible owing to the DMZ host function.

Note

- DMZ is the acronym of DeMilitarized Zone. While using the DMZ host function, packets can pass through the router because of the DeMilitarized Zone, and you may be affected by an unintended intrusion or external attack.
- The DMZ host function cannot be used for multiple PCs at the same time.



Tip

By separating the IP address of a public server from internal addresses, you can prevent damage to other hosts with an internal address even if the public server should be attacked externally.

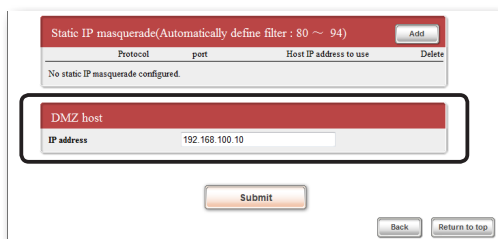
If the incoming packet is for an address unregistered in NAT/IP masquerade table, transfer the packet to a host having IP address "192.168.100.10".

1. Set the IP addresses of PCs.

Assign a fixed private IP address to the PC for which you want to permit external access.

2. Specify the address of the DMZ host.

On the "Register/Modify provider" screen, set the DMZ host IP address.



To open the "Register/modify provider" screen

From "Basic configuration page", click the buttons on the setup screen in the following order:

- ▶ "Advanced settings" in the top page
- ▶ "Configure" of "Detailed basic connection setting"
- ▶ "Configure" of the destination of which settings you want to change

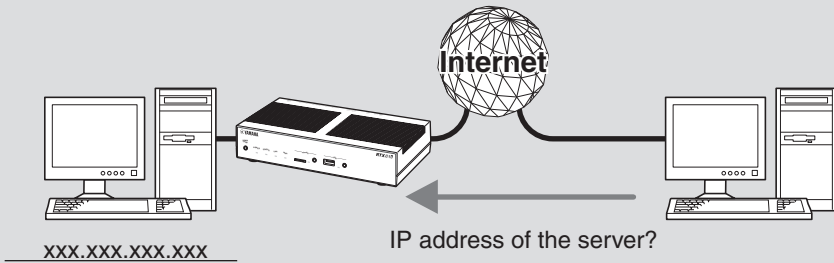
For more details on the settings, click "Help" on the setup screen and refer to the description displayed.

Using the netvolante DNS service

What is the netvolante DNS service?

To construct a server to publish your website, or share a working file via the Internet, the global IP address of the server must be known.

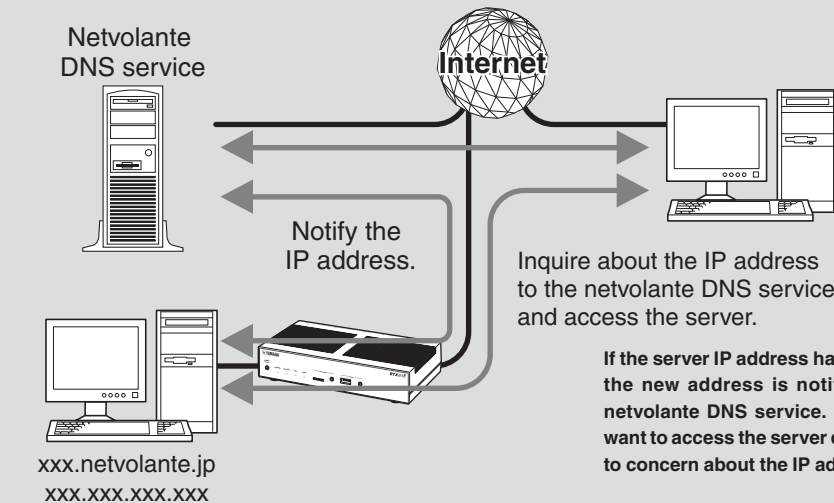
However, an assigned global IP address may be changed upon reconnection or after a certain time even if permanent connection to the Internet has been established. Therefore, it was difficult to construct a public server when using a connection service where a fixed global IP address was not assigned.



As the server IP address tends to change, users who want to access the server must check the new address.

If you use the netvolante DNS service,

the global IP address, each time it is changed, is notified to the netvolante DNS service, and a fixed host name assigned by the netvolante DNS service can be used for accessing the server. Accordingly, the contract of fixed IP address service is not required to operate various servers using a proprietary domain, or construct a VPN using IPsec or PPTP to exchange data with external systems.



If the server IP address has changed, the new address is notified to the netvolante DNS service. Users who want to access the server do not have to concern about the IP address.

Host names assigned by the netvolante DNS service

When using the netvolante DNS service, you can obtain a host name in the format of “(Your desired host name).xxx.netvolante.jp”, where “xxx” is an arbitrary string automatically assigned by the netvolante DNS server. This function is convenient because you do not have to change settings each time the global IP address is changed.

Note

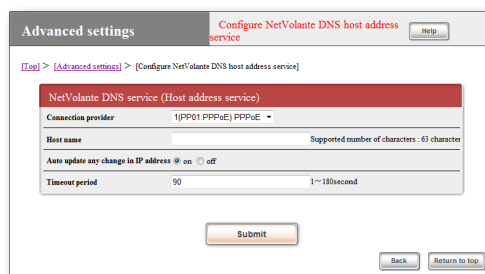
- The netvolante DNS service can be set only for terminal provider connection. It cannot be set for network connection or LAN-to-LAN connection. Even for terminal CATV provider connection, it cannot be set if the IP address is fixed on the WAN side.
- Only a single host address can be obtained for a unit of router.
- Note that your desired host name is not always available.
- Lookup of the obtained host address is possible, but reverse lookup is not possible.
- The netvolante DNS service uses a Yamaha original protocol, and the obtained host address cannot be registered with external dynamic DNS servers.
- The netvolante DNS service can be used only in an environment where a global IP address is assigned by a provider. Note that the following IP addresses are not global IP addresses:
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- Depending on the provider you are currently using, the registered/updated host name settings may not be reflected on the netvolante DNS service immediately.

Obtaining a host address from the netvolante DNS service

Use the “Configure NetVolante DNS host address service” screen to use the netvolante DNS service.

Note

- Only a single host address can be obtained for a unit of router.
- To set the Host address service, enter only your desired host name in the “Host name” field.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure NetVolante DNS host address service” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

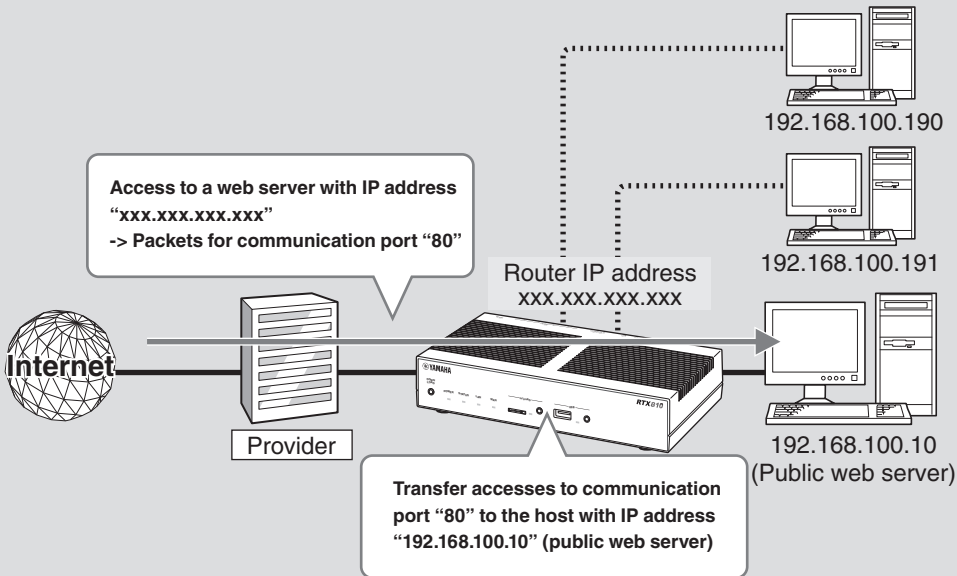
- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure NetVolante DNS host address service”

When you cannot obtain a host address

- Depending on the provider, name resolution is not possible immediately after registration/update. Retry after a while.
- Check whether a global IP address has been assigned by the provider.
- Check whether the IP address of the DNS server that you specified during provider configuration is correct.

Publishing a server

If you want to publish a server to the Internet, first assign a fixed private IP address to the server to be published, and register the IP address conversion table (Static IP masquerade). Then, configure a filter in the product to permit access from outside the LAN. This allows packets of a specific protocol to be sent to the server in the LAN, and thus the server can be accessed from the Internet.



6

Maximizing use of the product

Note

When publishing the server to the outside of your LAN, be sure to configure adequate security settings to maintain data integrity. Inadequate security settings may cause PCs in the LAN to be hacked, sniffed, intercepted, or destroyed, or their data to be lost.

Tip

You can use the netvolante DNS service to publish and operate a server even when using a connection service that cannot assign a fixed global IP address. Please refer to "Using the netvolante DNS service" (page 104) for more information.

Flow of settings

Following settings are required for publishing a server.

Router settings:

- Register the conversion table of protocol, port number and the server IP address (Static IP masquerade, page 107).
- Change the settings to permit access (page 107).

Server settings:

- Set the server IP address.
- Change the settings of web, ftp, and other file server software programs according to the services to be published.

Registering the IP address conversion table

On the “Register static IP masquerade” screen, register the conversion table of protocol, port number and the server IP address (Static IP masquerade settings).

Note

- For information about the protocol and port number, please refer to the manual of the software or service to be used.
- So far as representative software programs are concerned, you can click “Help” in the “Register static IP masquerade” screen to confirm the port number to be used and other setting examples.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Register static IP masquerade” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Detailed basic connection setting”
- ▶ “Configure” of the destination of which settings you want to change
- ▶ “Add” in the “Static IP masquerade” field

Changing settings to permit access

To permit access to the server, configure a filter intended for the server IP address and communication protocol. The settings do not allow external access to other PCs in the LAN. To configure filter settings, use the “Configure firewall” screen.

Note

- If you want to restrict users that can access the server, specify the user’s IP address in the “Source IP address” field.
- Set “Destination port number” to the protocol of the server application to be used.
- Up to 100 filter numbers, 0 to 99, are available for each connection destination. For more details on filter and protocol, please refer to “Command reference” (included in the attached CD-ROM).

(Examples of what to enter to publish the web server)

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

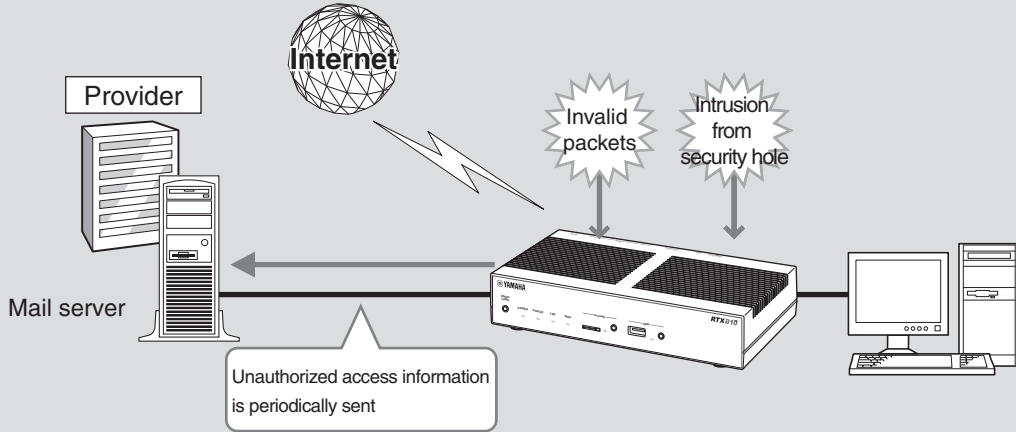
To open the “Register IP filter” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure firewall”
- ▶ “Configure” of the interface for which you want to configure the firewall (“Configure” of “IPv4 filter” unless IPv6 is used for connection).
- ▶ “Add” on the “IPv4 static IP filter list” screen

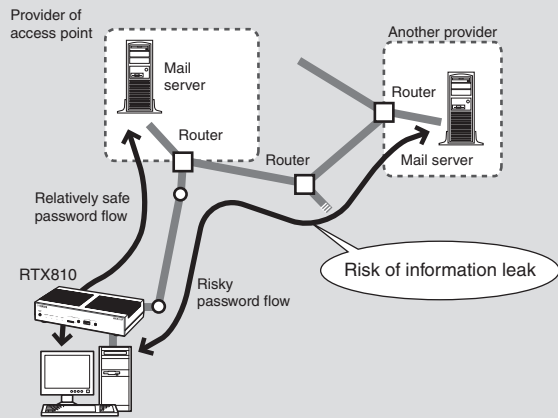
Using mail notification

The record of unauthorized accesses detected by firewall (page 92) of the product can be sent to the specified e-mail address periodically (Mail notification).



Note

During connection with the provider, if you use this function for a mail server of another provider, password and other data flow out to the Internet without being encrypted. Please exercise care not to do so.



Registering a mail server used for mail notification

On the “Configure mail server” screen, register a mail server used for sending e-mail to the notification destination.

Note

The destination's provider is that set on the provider configuration screen.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure mail server” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure mail notifications”
- ▶ “Add” in the “Configure mail server” field

To delete the registration of mail server

On the “Configure mail notifications” screen, click “Delete” of the mail server of which registration you want to delete.

Notifying of illegal access detection by e-mail

The record of unauthorized accesses detected by firewall (page 92) of the product can be sent to the specified e-mail address periodically. This is convenient when you check, while out the door, any unauthorized access or unintended automatic connection.

On the “Configure content of notifications” screen, specify the transmission destination and date/time.

Note

The destination's provider is that set as the auto-connect destination.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure content of notifications” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure mail notifications”
- ▶ “Add” in the “Configure content of notifications” field

Using in the IPv6 environment

The product supports “IPv6” (Internet Protocol Version 6), an internet protocol of the next generation. As IPv6 inherits functions related to traditional “IPv4”, you can use the new protocol without affecting the existing network.

Note

If your provider does not support IPv6, you cannot connect to the Internet in the IPv6 environment. Confirm in advance whether your provider provides an IPv6 connection service.

Introducing IPv6 into PCs

Introduce IPv6 in a Windows 7 or Windows Vista environment

Windows 7 and Windows Vista can use IPv6 without additional settings.

Introduce IPv6 in a Windows XP environment

Enter the following command from the command prompt:

```
ipv6 install
```

Tip

For more details on introducing the IPv6 environment, please refer to the Windows XP Help that is displayed by clicking “Start” - “Help and Support”. Enter “IPv6” in the “Search” field to display relevant information.

Before introducing IPv6

To use both the IPv6 and IPv4 environments

IPv6 is not compatible with IPv4. To mix those two protocols on a network, therefore, a mechanism generally called “transition mechanism” is required. Multiple steps are usually required for transition from IPv4 to IPv6, and an appropriate transition technology is required for each step. As transition technologies, the product supports “IPv6 over IPv4 tunneling” for connecting an IPv6 network via an IPv4 network, and “IPv4 over IPv6 tunneling” for connecting an IPv4 network via an IPv6 network.

Check configuration information from the provider

When you contract an IPv6 connection service, the provider provides the following information:

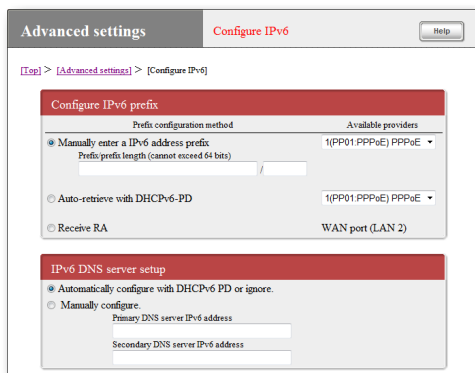
- Prefix (Address block)
- Connection method (native connection/dual-stack connection/tunnel connection)
- Tunnel terminal address (for tunnel connection)
- Routing control method (whether to use RIPng. RIPng is not used unless specifically described.)
- Method to check connection (address of the other side of ping6, website to be browsed, etc.)

Configuring the product to use IPv6

Before beginning configuration, register the connection destination (provider) using IPv6 on the “Configure IPv6” screen.

Note

If the provider is not registered, your IPv6 connecting operation will result in an error.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure IPv6” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure IPv6”

Checking the IPv6 connection

Take the following steps to check whether the IPv6 environment has been correctly configured.

Tip

The product and a PC can be communicated with each other once they are connected with a LAN cable. No particular settings are required in the PC.

1 Checking the connection of LAN

From a PC connected to a LAN port, execute “ping6” to the LAN1 address of the product.

If a response is returned, IPv6 has been configured correctly.

Tip

The LAN1 address of this product is a prefix address with “1” is added to it.

Example: If the prefix is “fec0:12ab::/64”,

- The LAN1 address is “fec0:12ab::1/64”.
- To execute “ping6” to the LAN1 address of the product, enter “ping6 fec0:12ab::1” from the command prompt of the PC and press the Enter key.

2 Checking the connection between LAN and WAN

Execute “ping6” to the provider, view the special website, or take other checking procedure specified by the provider.

Changing the operation settings of UPnP function

What is UPnP function?

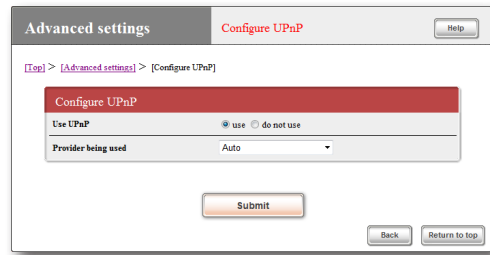
UPnP is the acronym of Universal Plug and Play, a mechanism where the UPnP-supported operating system automatically detects UPnP-supported devices in the network to facilitate mutual connection. The product supports UPnP. Therefore, if your LAN has the product installed, Windows PCs within the LAN can use the audio chat of Windows Live Messenger and other features.

Note

- Note that not all of the functions provided by UPnP Forum are supported by the UPnP function of the product.
- If the IP address assigned by the provider is a private IP address, the Windows Live Messenger audio chat using the UPnP function is not available.
- To configure the UPnP function in “Basic configuration page”, you must register the connection provider in advance.
- If you have not registered the provider before starting software such as Windows Live Messenger that requires the UPnP environment, it may take some time to communicate with the router. In this case, register the connection provider or stop the UPnP function.
- If Windows Live Messenger is exited and started repeatedly, or the UPnP function information becomes different between the PC and the router after the router has been restarted or the line has been disconnected, the connection may not be established normally.
In this case, sign out Windows Live Messenger once with the line connected, and then restart it. If you still cannot establish the connection, restart the PC.

Configuring the setting to use UPnP function

The UPnP function of the product is set to “Do not use” by factory default. Change the setting to start the function.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure UPnP” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure UPnP”

Checking whether your PC can use the UPnP function

Take the following steps to check whether your PC can use the UPnP function.

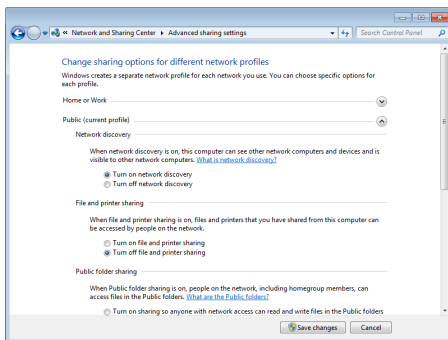


Tip

For more details on introducing the UPnP environment, please refer to Help that is displayed by clicking “Start” - “Help and Support”. In the “Search” field, enter “Network Discovery” for Windows 7 or Windows Vista, or “UPnP” for Windows XP to display relevant information.

For Windows 7

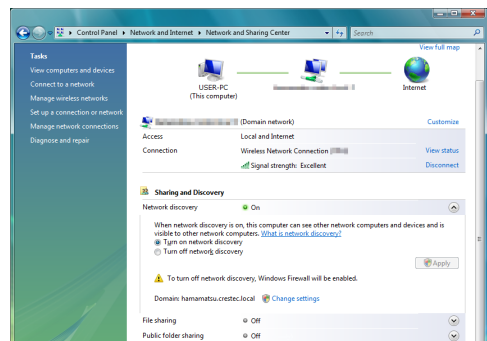
- 1 Click the “Start” button, then click “Control Panel”.
- 2 From “Network and Internet”, click “View network status and tasks”.
- 3 Click “Change advanced sharing settings”, and confirm whether the “Turn on network discovery” checkbox is selected in “Network Discovery”.



- If this checkbox is selected, the UPnP function is available in the PC.
- If the checkbox is not selected, select it and click “Save Changes”.

For Windows Vista

- 1 Click the “Start” button, then click “Control Panel”.
- 2 From “Network and Internet”, click “View network status and tasks”.
- 3 Click “Network discovery” in “Sharing and Discovery”, and confirm whether the “Turn on network discovery” checkbox is selected.



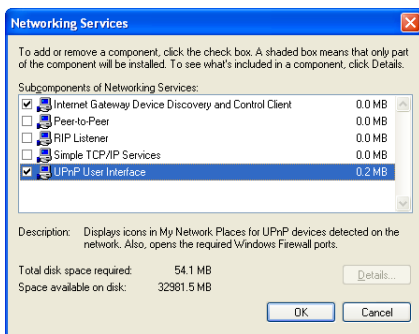
- If this checkbox is selected, the UPnP function is available in the PC.
- If the checkbox is not selected, select it and click “Apply”.

Changing the operation settings of UPnP function

(Continued from the previous page)

For Windows XP

- 1 Click the “Start” button, then click “Control Panel”.
- 2 Click “Add or Remove Programs”.
- 3 Click “Add/Remove Windows Components” on the left of the screen.
- 4 Click “Networking Services”, then click “Details”.
- 5 Confirm whether the “UPnP User Interface” box is selected.



- If this checkbox is selected, the UPnP function is available in the PC.
- If the checkbox is not selected, continue step 6 and subsequent operation.

- 6 Select the “UPnP User Interface” checkbox, and click “OK”.
- 7 Click “Next”.

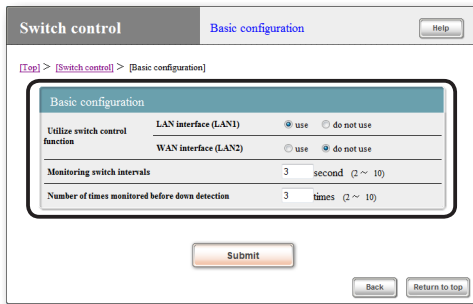
Then, follow the on-screen instruction to continue installation.

Controlling Yamaha switches

From the setup screen of the product, you can change settings or check the status of Yamaha switches.

To change settings or check the status of Yamaha switches, take the following steps.

- 1 On the “Basic configuration” screen of switch control, change required setup items.



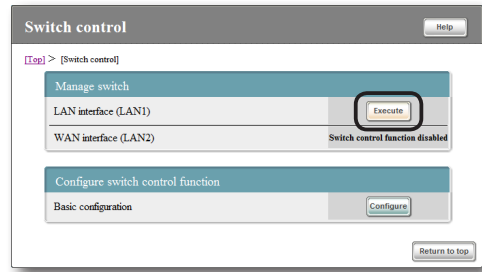
For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Basic configuration” screen of switch control

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Switch control” in the top page
- ▶ “Configure” of “Basic configuration”

- 2 Click “Submit”, then click “Return to top”.
- 3 On the “Switch control” screen, click “Execute” of the LAN interface to which Yamaha switches are connected.



Yamaha switches connected to the selected LAN interface is displayed in tree view.

Please refer to the instruction manual of Yamaha switches for more details on settings.

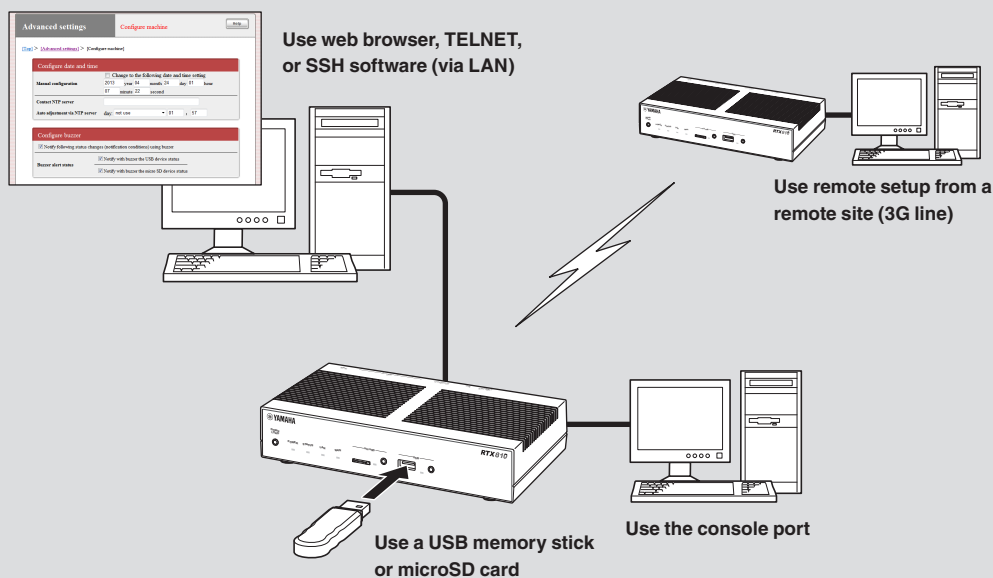
To open the “Switch control” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Switch control” in the top page

Changing the product settings

The following shows the methods to configure the product functions or check the configuration. Use the easiest method according to your environment.



Types of configuration methods available

Using the web browser of PC (page 20)

If a PC is connected to the product, you can use the web browser to open “Basic configuration page” included in the product to view the product status or configure various function settings.

Using console commands (page 117)

You can use TELNET or SSH software to enter commands from the console screen to check the product status or configure various functions.

You can also enter commands from a PC connected to the console port of the product using a serial cable. Using console commands enables you to configure more detailed settings than using other methods.

Using an external memory device (page 123)

You can load a configuration file stored in a commercially-available external memory device (USB memory stick or microSD card) to the product to change settings.

Configuring setting with console commands

The product functions can be configured by sending commands (console commands) directly. You can change settings via TELNET or SSH, and also enter console commands from “Basic configuration page” to configure settings. If you change settings via TELNET or SSH, prepare an appropriate software program supporting your TELNET or SSH environment.

What is console command?

The console command is a method to configure functions by directly sending instructions to the router. Using console commands enables you to configure more detailed settings than using other methods. Please refer to “Command reference” (included in the attached CD-ROM) for more details on console commands.

Note

You should fully understand the behavior of a console command before using it. After configuring a setting in “Basic configuration page”, if you change the setting with a console command, an unintended operation may be resulted. Be sure to check whether the command behaves as you intended after changing the setting.

Tip

The product can be configured with console commands from a PC that is connected to the console port of the product using a serial cable (page 121).

Register TELNET, SSH, or SFTP users

In the “Add user” screen, register users to be permitted to log in using TELNET or SSH. TELNET allows a user to log in as an anonymous user even if s/he is not registered, but SSH allows only registered users to log in.

The screenshot shows the 'Add user' configuration screen. At the top, there are tabs for 'Advanced settings' and 'Add user', with a 'Help' button. Below the tabs, a breadcrumb trail reads: [Top] > [Advanced settings] > [Configure users and access limits] > [Add user]. The main content area is titled 'Configure users' and contains the following fields and options:

- User name:** A text input field containing 'username'.
- Password:** A password input field with masked characters and a red prompt: 'Retype the same again'.
- Promote to administrator user via command:** Radio buttons for 'allow' (selected) and 'do not allow'.
- Allow all connections:** Radio buttons for 'Allow all connections' (selected) and 'Prohibit all connections'.
- Allow per connection method:** Radio buttons for 'Allow per connection method' (selected) and 'Allow connection from serial console'.
- Restrict connection:** Checkboxes for 'Allow connection via TELNET', 'Allow connection via SSH', 'Allow connection via SFTP', and 'Allow connection via HTTP'.
- Allow connection:** A dropdown menu currently set to 'Allow all'.
- IP addressing:** A text input field.
- Connect multiple users with the same user name:** Radio buttons for 'allow' (selected) and 'do not allow'.

At the bottom of the form, there are three buttons: 'Submit', 'Back', and 'Return to top'.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Add user” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure users and access limits(HTTP, TELNET, SSH, SFTP)”
- ▶ “Configure” of “Number of registered users” in the “Configure user and password” field

Changing the product settings (Continued from the previous page)

Configure settings to permit login with SSH

The SSH server function of the product is set to “do not use” by factory default. To permit login using SSH, in the “SSH and SFTP server function” field on the “Configure users and access limits” screen, change the setting to “use”.

The screenshot shows a web-based configuration interface for a device. The main heading is "Configure users and access limits". It is divided into several sections:

- Configure user and password:** Includes fields for "Number of registered users: 0", "Nameless user", and "Administration password". There are "Configure" buttons for the first two fields. A note states: "If you setup an admin password you will be prompted for it when logging onto Basic configuration." A red error message says "Retype the same again." There is a checkbox for "Encrypt and save the admin password".
- HTTP server function:** Includes "Hosts permitted to use HTTP" (set to "Allow if within same network") and "IP addressing".
- TELNET server function:** Includes "Allowable TELNET usage hosts" (set to "Allow all"), "IP addressing", and "Number of simultaneous users" (set to 8).
- SSH and SFTP server function:** This section is highlighted. It has a "SSH and SFTP server function" dropdown set to "use". Below it are "Allowable SSH usage hosts" (set to "Allow all"), "IP addressing", and "Allowable SFTP usage hosts" (set to "Allow all"). At the bottom, there is a list of "Encryption algorithm" options: aes128-ctr (checked), aes192-ctr (checked), aes256-ctr (checked), aes128-cbc, aes192-cbc, aes256-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, and arcfour.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure users and access limits” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure users and access limits(HTTP, TELNET, SSH, SFTP)”

Connect with SSH

Follow the instructions of the SSH software to be used.

Connect with TELNET

The following explains an example of connection from a PC, using TELNET included as standard in Windows 7.

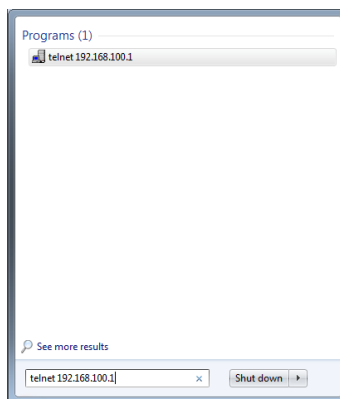
Tip

In Windows 7, TELNET must be enabled by the following procedure:

- 1 From “Control Panel”, select “Programs” - “Programs and Features” - “Turn Windows features on or off”.
- 2 In the “Windows Features” screen, select the “Telnet Client” checkbox, and click “OK”.

1 From the “Start” menu, select “Search programs and files”.

2 Type in “telnet 192.168.100.1”, and click “OK”.



If you have changed the IP address of the product, type in the changed address instead of “192.168.100.1”.

3 When “Password:” is displayed, type in the login password and press the Enter key.

If nothing appears on the screen, press the Enter key once.

The password to be entered here for TELNET is the login password for anonymous users.

If you want to log in as a registered user instead of an anonymous user

Do not type in character and only press the Enter key. Then a “Username:” prompt is displayed. If you have already logged in as an anonymous user, or logging in as anonymous users is prohibited, a “Username:” prompt is displayed in the first step.

When you enter a registered user name in “Username:”, a “Password:” prompt is displayed. Enter the login password of the user.

When you log in as an anonymous user for which no password has been set

Do not type in any character in “Username:” and following “Password:”. Only press the Enter key.

When “>” is displayed, you can enter a console command.

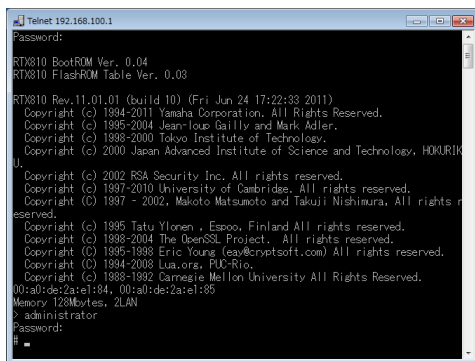
Tip

- To view the explanation of key operations, type in “help” and press the Enter key.
- To view the command list, type in “show command” and press the Enter key.

4 Type in “administrator”, and press the Enter key.

5 When “Password:” is displayed, enter the administration password.

When “#” is displayed, you can enter various types of console commands.



```

Telnet 192.168.100.1
Password:
RTX810 BootROM Ver. 0.04
RTX810 FlashROM Table Ver. 0.03
RTX810 Rev.11.01.01 (build 10) (Fri Jun 24 17:22:33 2011)
Copyright (c) 1994-2011 Yamaha Corporation. All Rights Reserved.
Copyright (c) 1995-2004 Jean-Loup Gailly and Mark Adler.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIKI
U.
Copyright (c) 2002 RSA Security, Inc. All rights reserved.
Copyright (c) 1997-2010 University of Cambridge. All rights reserved.
Copyright (c) 1997 - 2002, Makoto Matsumoto and Takujii Nishinura, All rights reserved.
Copyright (c) 1995 Tatu Ylonen . Espoo, Finland All rights reserved.
Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
Copyright (c) 1996-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
Copyright (c) 1994-2008 Lua.org, PUC-Rio.
Copyright (c) 1988-1992 Carnegie Mellon University All Rights Reserved.
0:aa:de:2a:el:04, 00:aa:de:2a:el:05
Memory 128Kbytes, 2LAN
> administrator
Password:
#
  
```

6 Enter console commands to configure settings.

7 After the configuration is completed, type in “save” and press the Enter key.

The settings configured using the console commands will be saved to the memory included in the product.

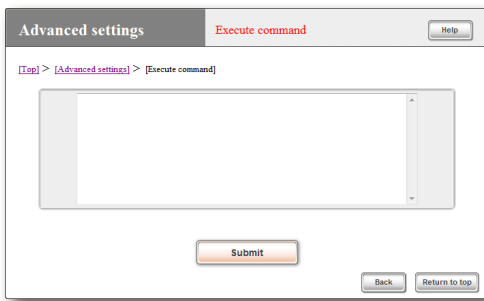
8 To exit the settings, type in “quit” and press the Enter key.

9 To exit the console screen, type in “quit” again and press the Enter key.

Changing the product settings (Continued from the previous page)

Use console commands in “Basic configuration page”

Use commands on the “Execute command” screen. When you type in a console command and click “Execute”, the result of command execution is displayed.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Execute command” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Execute” of “Execute command”

Using the console port

The product can be configured with console commands from a PC that is connected to the console port of the product using a serial cable.

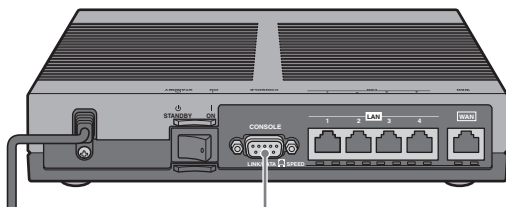
- In the “Configure users and access limits” screen, you can prohibit access from web browser (HTTP), TELNET, SSH, and SFTP software programs (page 100) to make the product accessible only by means of physical connection. This restricts users who can change settings, and helps enhance security.
- You can also specify, from the terminal software, a configuration file to be used upon startup.

Note

- The following explains an operation using Windows XP and Hyper Terminal. As Windows Vista and other later Windows operating systems do not include the hyper terminal utility, you should use a terminal software program supplied from a vendor to control its serial devices.
- For more details on how to use the terminal software, please refer to the instruction manual attached to each software program.

Connect the console port to your PC

Connect the console port of the product to the serial port of your PC with a cross type serial cable.



Console port

Tip

One of the connectors attached to the serial cable must be 9-pin D-sub male (to fit the product port), and the other connector must match the port type of your PC.

Check the console port number

Check the COM port number to which the serial port of your PC is assigned.

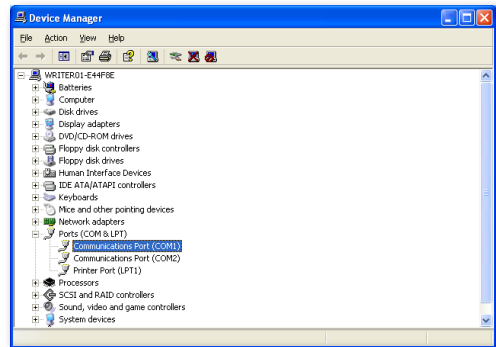
- 1 From the “Start” menu, click “My Computer”.
- 2 On the left of the “My Computer” screen, click “View system information” in the “System Tasks” field.

The “System Properties” screen appears.

- 3 Click the “Hardware” tab.
- 4 Click “Device Manager”.

The “Device Manager” screen appears.

- 5 Expand “Ports (COM & LPT)” and check the “Communication Port Number” (COMx).



Normally, “COM1” is assigned.

- 6 Close the “Device Manager” screen and the “System Properties” screen.

Changing the product settings (Continued from the previous page)

Specify the console port to connect

From the PC connected to the console port, log in the product using a terminal software program, and send console commands to configure settings. The following explains an example using Windows XP and Hyper Terminal.

Note

You should fully understand the behavior of a console command before using it. After configuring a setting in “Basic configuration page”, if you change the setting with a console command, an unintended operation may be resulted. Be sure to check whether the command behaves as you intended after changing the setting.



Tip

Please refer to “Command reference” (included in the attached CD-ROM) for more details on console commands.

7

Operating and managing the product

1 From the “Start” menu, click “All Programs” - “Accessories” - “Communications” - “Hyper Terminal”.

The “Connect To” screen appears.

2 Type a connection name into the “Name” field, and click “OK”.

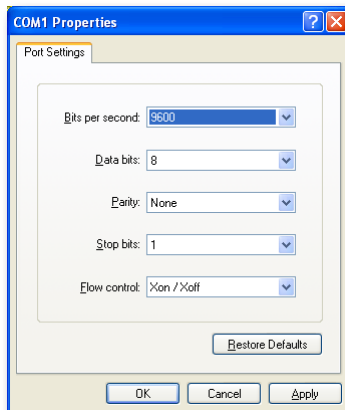
You can specify a desired connection name.

3 After selecting the serial port number confirmed in the previous page, click “OK”.



The “COMx properties” screen appears.

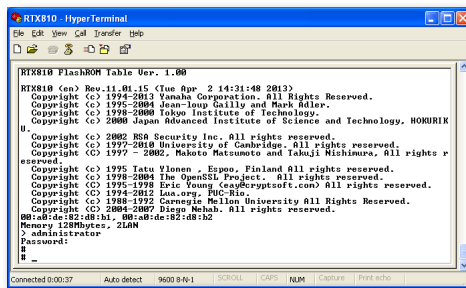
4 Change the communication settings to the following values:



- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Xon/Xoff

5 Click “OK”.

The Hyper Terminal screen appears.



The subsequent procedure is the same as step 3 of “Connect with TELNET” (page 118).

Using an external memory device

You can load a configuration file stored in a commercially-available external memory device (USB memory stick or microSD card) to the product to change settings. This is convenient when you want to change the settings of multiple units of the product.

Note

- External memory devices used for the product must be formatted in FAT or FAT32.
- You cannot use a USB hub to connect two or more USB memory sticks or other external memory devices to the product.
- Some types of USB extension cables may not be able to work normally. Use the USB memory stick by inserting it directly into the USB port of the product.
- Do not remove the external memory device while the USB lamp or microSD lamp of the product is lit up or flashing. Doing so may damage data in the external device. Before removing the external device, hold down the USB button or microSD button for two seconds and make sure that the USB lamp or microSD lamp has gone off.

Change settings so that the configuration file in the external memory device can be loaded to the product

In the “Startup via external memory” field on the “Configure external device” screen, select “do not allow”. Also in the “Configuration file name” field, specify the name of the configuration file to be copied to the product.

To open the “Configure external device” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure external device”

Press the button on the product front panel to load a configuration file

1 Prepare an external memory device storing a configuration file.

Specify the same file name as that specified in the “Configuration file name” field on the “Configure external device” screen.

2 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

3 While holding down the USB button or microSD button, hold down the DOWNLOAD button for three seconds.

The configuration file prepared in step 1 is loaded to the product. After the file has been loaded, the product restarts automatically. After the restart, the product operates using settings of the loaded configuration file.

Note

If “allow” is selected in the “Startup via external memory” field on the “Configure external device” screen, the product starts by using the configuration file in the external memory device. In this case, do not remove the external device.

Tip

If a firmware file having the name specified in the “Firmware file name” field on the “Configure external device” screen is included in the external memory device, the firmware file begins to be copied to the product continuously.

4 Hold down the USB button or microSD button for two seconds.

The USB lamp or microSD lamp of the product goes off.

5 Remove the external memory device.

Note

If loading the configuration file from the external device fails, check “Unable to use USB device” (page 160).

Changing the product settings (Continued from the previous page)

Load a configuration file included in an external memory device from “Basic configuration page”

1 Prepare an external memory device storing a configuration file.

2 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

3 In the “Source file name to copy” field on the “Copy configuration and firmware files” screen, specify the file name you want to load from the external memory device to the product.



To open the “Copy configuration and firmware files” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Execute” of “Copy configuration and firmware files”

4 In the “Copied file name” field, select “Internal non-volatile memory” and specify a config number.

Tip

If you specify another external memory device instead of “Internal non-volatile memory”, you can copy the configuration file to the external device using the product.

5 Click “Execute”.

A confirmation screen appears.

6 Click “Execute”.

The configuration file prepared in step 1 is loaded to the product. After the configuration file has been loaded, the product restarts automatically.

After the restart, the product operates using settings of the loaded configuration file.

Note

If “allow” is selected in the “Startup via external memory” field on the “Configure external device” screen, the product starts by using the configuration file in the external memory device. In this case, do not remove the external device.

7 Hold down the USB button or microSD button for two seconds.

The USB lamp or microSD lamp of the product goes off.

8 Remove the external memory device.

Note

If loading the configuration file from the external device fails, see “Unable to use USB device” (page 152).

Operating the product using a configuration file in an external memory device

You can operate the product using a configuration file stored in a commercially-available external memory device (USB memory stick or microSD card). This is convenient when you want to store a configuration file for emergency in an external device and use it only on an as-needed basis, without changing the configuration file in the product.

Change settings so that the product can be started by using a configuration file in an external device

In the “Startup via external memory” field on the “Configure external device” screen, select “allow”.

The screenshot shows a configuration screen titled "Configure configuration and firmware files". It has three main sections, each with a red header bar:

- Startup via external memory:** Includes radio buttons for "allow" (selected) and "do not allow", and a "Timeout before detecting external memory (1-30seconds)" field set to "1".
- Use buttons to copy files:** Includes radio buttons for "allow" (selected) and "do not allow".
- Configuration file name:** Includes a dropdown menu for "External memory1" (set to "All external memory"), a "File name1" field (containing "config.rtf"), and a "File name2" field (containing "config.txt"). There is also a "Password" field with a "do not use" option.
- Firmware file name:** Includes a dropdown menu for "External memory" (set to "All external memory") and a "File name" field (containing "rt810_en.bin").

To open the “Configure external device” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure external device”

Start the product using a configuration file in an external device

- 1 Prepare an external memory device storing a configuration file.

Specify the same file name as that specified in the “Configuration file name” field on the “Configure external device” screen.

- 2 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

- 3 Restart the product.

After the restart, the product automatically loads the configuration file specified in step 1.

Tip

The content of the configuration file stored in the product is not overwritten. However, if you change a setting after the restart, the changed setting is overwritten to the configuration file stored in the product.

Note

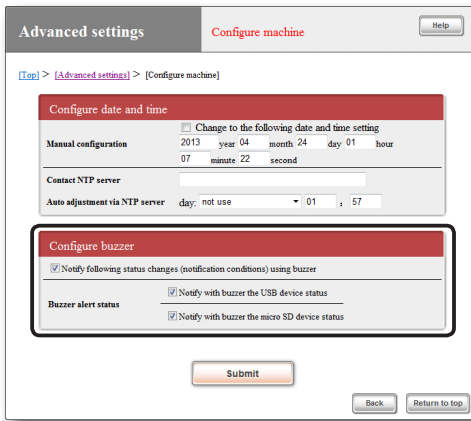
If loading the configuration file from the external device fails, see “Unable to use USB device” (page 152).

Changing the buzzer settings

The product includes a buzzer, and it is set to sound in the following cases by factory default:

- When the status of a USB device changes
- When the status of a microSD device changes

You can change the buzzer settings on the “Configure machine” screen.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

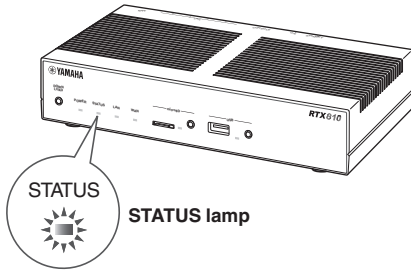
To open the “Configure machine” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure machine(Date/Time, buzzer)”

Checking the communication status with the STATUS lamp

If the keep alive function is set to valid in each connection setting, you can check whether communication with any connected equipment is active or not only by glancing the STATUS lamp of the product.



This is convenient as you can check the communication status without viewing the top page of the “Basic configuration page”.

Tip

- When you configure a provider connection or VPN connection (IPsec, L2TP/IPsec, PPTP LAN-to-LAN connection, or IPsec tunnel) from “Basic configuration page”, the keep alive function is set to “Valid” on the initial setup screen.
- To check whether the keep alive function is set to valid or not, view the setup screen of each connection.

Advanced settings Register provider Help

[Top] > [Advanced settings] > [Detailed basic connection settings] > [Register provider(PP[01])]
Configure providers using the following interface. (Terminal broadband connection over PPPoE)

- PP[01]Interface

Modify the input or selected items of each column. After checking them press the [Submit] button.

- Basic matters

Register provider

Configuration name	(optional)	FPPoE
User ID	(or account name)	* username@provider.ne.jp
Connect password	(line connection)	*****

PPPoE related configuration

MTU designation	(1280~1490Byte)	<input checked="" type="radio"/> Auto <input type="radio"/> Designation
Keep alive function		<input checked="" type="checkbox"/> use

Example of setup screen for the “Terminal broadband connection over PPPoE” connection

When the STATUS lamp lights up

In a connection setting where the keep alive function is set to valid, communication with any connected equipment is inactive.

Note

- The keep alive function takes time to detect an inactive state of communication. Accordingly, communication with a connected equipment may not be available even when the STATUS lamp does not light up.
- The STATUS lamp also lights up when you update the firmware revision using the DOWNLOAD button. For information about behavior of the product when you upgrade the firmware using the DOWNLOAD button, please refer to “Upgrading the firmware using the DOWNLOAD button” (page 128).

When the problem is resolved

The STATUS lamp goes off.

Using the latest function (Revision up)

From the Internet, you can download the program (firmware) managing the product functions to use the latest functions (Firmware upgrade or revision up).

Note

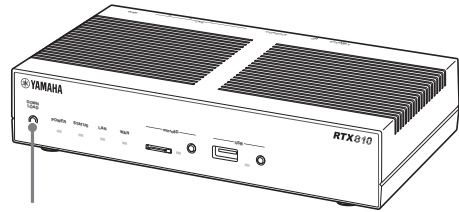
- When you have started a firmware upgrade process, be sure not to perform any other operations until the process is completed and the product restarts. Doing so stops the upgrade process and the product may become inoperable. Should this occur, please contact your retailer.
- During the firmware upgrade process, lamps on the front panel other than the POWER lamp flash in turn.
- All communications are disconnected during the upgrade process.
- Be sure not to remove cables during the upgrade process. Doing so may cause the product to be inoperable. Should this occur, please contact your retailer.
- In the “Execute revision up” screen of “Basic configuration page”, the firmware can be upgraded only to a formally-released revision. When using “Basic configuration page”, you cannot upgrade the firmware to a beta version for which Yamaha does not formally assure normal operation.

Tip

If you change the “Allow for revision down” setting to “allow” on the “Execute revision up” screen of “Basic configuration page”, you can downgrade the firmware to an older version (Revision down). Please refer to the Help on the “Execute revision up” screen for more information.

Upgrading the firmware using the DOWNLOAD button

If “Revision up” option is selected on the “Configure DOWNLOAD button” screen, the firmware can be upgraded simply by holding down the DOWNLOAD button on the product front panel for three seconds.



DOWNLOAD button

Note

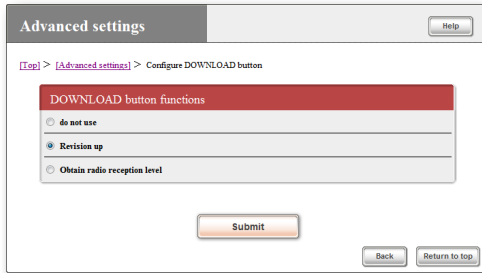
Before upgrading the firmware, confirm “Concerning software license contracts when using the DOWNLOAD button” (page 10).

Tip

While upgrading the firmware using the DOWNLOAD button, you can check the status of the process with the product lamps. When a firmware upgrade process has begun after downloading the firmware, lamps on the front panel other than the POWER lamp flash in turn.

Permit upgrading the firmware using the DOWNLOAD button

Use the “Configure DOWNLOAD button” screen.



If you want to upgrade the firmware using the DOWNLOAD button, select “Revision up”.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Configure DOWNLOAD button” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure DOWNLOAD button”

Upgrade the firmware by pressing the DOWNLOAD button

You can hold down the DOWNLOAD button for three seconds to find a new revision of firmware. If a new revision of firmware is found, it is automatically download to upgrade the existing firmware.

Note

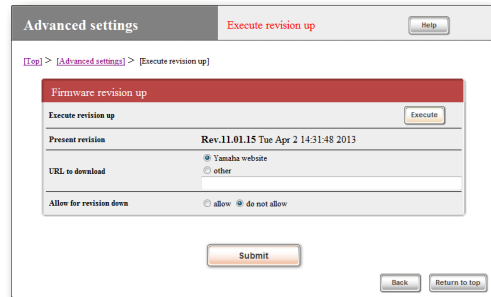
If downloading the firmware or upgrading the existing firmware fails, see “The DOWNLOAD button does not function” (page 151).

When the firmware has been upgraded

The product restarts.

Upgrading the firmware in “Basic configuration page”

Use the “Execute revision up” screen.



You can click “Execute” to find a new revision of firmware. If a new revision of firmware is found, the revision number is displayed on the screen together with the revision number of the existing firmware. In this state, click “Execute” again to download the new firmware and automatically upgrade the existing firmware.

For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

Tip

If you change the “Allow for revision down” setting to “allow” on the “Execute revision up” screen, you can downgrade the firmware to an older version (Revision down).

To open the “Execute revision up” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Execute” of “Execute revision up” screen

When the firmware has been upgraded

The product restarts.

Using the latest function (Revision up)

(Continued from the previous page)

Upgrading the firmware from an external memory device

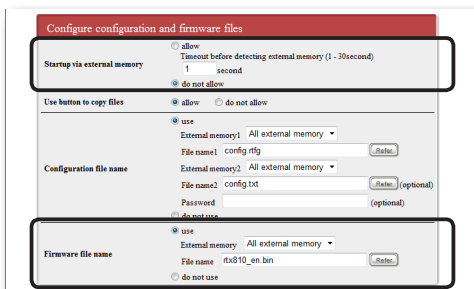
You can load a firmware stored in a commercially-available external memory device (USB memory stick or microSD card) to the product to upgrade the existing firmware. This is convenient when you want to manage firmware versions or change the firmwares of multiple units of the product.

Note

- External memory devices used for the product must be formatted in FAT or FAT32.
- You cannot use a USB hub to connect two or more USB memory sticks or other external memory devices to the product.
- Some types of USB extension cables may not be able to work normally. Use the USB memory stick by inserting it directly into the USB port of the product.
- Do not remove the external memory device while the USB lamp or microSD lamp of the product is lit up or flashing. Doing so may damage data in the external device. Before removing the external device, hold down the USB button or microSD button for two seconds and make sure that the USB lamp or microSD lamp has gone off.

Change settings so that the firmware can be upgraded from an external memory device

In the “Startup via external memory” field on the “Configure external device” screen, select “do not allow”. Also in the “Firmware file name” field, specify the file name of the firmware to be used for upgrading.



To open the “Configure external device” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure external device”

Upgrade the firmware by pressing the button on the product front panel

- 1 Prepare an external memory device containing firmware.

Specify the same file name as that specified in the “Firmware file name” field on the “Configure external device” screen.

- 2 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

- 3 While holding down the USB button or microSD button, hold down the DOWNLOAD button for three seconds.

The firmware prepared in step 1 is loaded to the product. After the firmware has been loaded, the firmware upgrade process begins.

After the upgrade process has been completed, the product restarts automatically.

Note

If “allow” is selected in the “Startup via external memory” field on the “Configure external device” screen, the product starts by using the firmware in the external memory device. In this case, do not remove the external device.



If a configuration file having the name specified in the “Configuration file name” field on the “Configure external device” screen is included in the external memory device, the configuration file begins to be copied prior to the firmware.

- 4 Hold down the USB button or microSD button for two seconds.

The USB lamp or microSD lamp of the product goes off.

- 5 Remove the external memory device.

Note

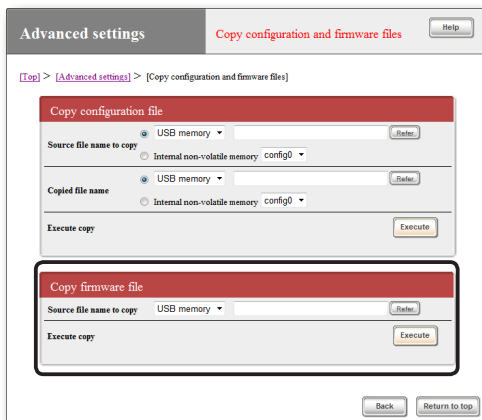
If upgrading the firmware from the external device fails, see “Unable to use USB device” (page 152).

Upgrade the firmware from “Basic configuration page” using a firmware in the external memory device

- 1 Prepare an external memory device containing firmware.
- 2 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

- 3 In the “Source file name to copy” field on the “Copy configuration and firmware files” screen, specify the firmware file name you want to load from the external memory device to the product.



To open the “Copy configuration and firmware files” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Execute” of “Copy configuration and firmware files”

- 4 Click “Execute”.

A confirmation screen appears.

- 5 Click “Execute”.

The firmware prepared in step 1 is loaded to the product. After the firmware has been loaded, the upgrade process begins.

After the upgrade process has been completed, the product restarts automatically.

Note

If “allow” is selected in the “Startup via external memory” field on the “Configure external device” screen, the product starts by using the firmware in the external memory device. In this case, do not remove the external device.

- 6 Hold down the USB button or microSD button for two seconds.

The USB lamp or microSD lamp of the product goes off.

- 7 Remove the external memory device.

Note

If upgrading the firmware from the external device fails, see “Unable to use USB device” (page 152).

Using the latest function (Revision up)

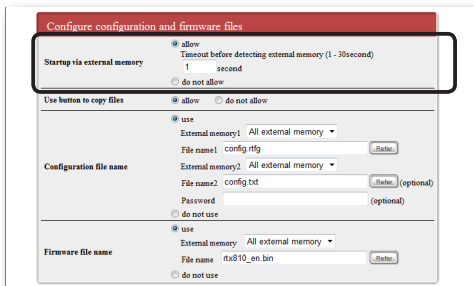
(Continued from the previous page)

Operating the product using a firmware in an external memory device

You can operate the product using a firmware stored in a commercially-available external memory device (USB memory stick or microSD card). This is convenient when you want to store a firmware for emergency or trial use in an external device and use it only on an as-needed basis, without upgrading the firmware in the product.

Change settings so that the product can be started by using a firmware file in an external device

In the “Startup via external memory” field on the “Configure external device” screen, select “allow”.



To open the “Configure external device” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure external device”

Start the product using a firmware in an external memory device

- 1 Prepare an external memory device containing firmware.

Specify the same file name as that specified in the “Firmware file name” field on the “Configure external device” screen.

- 2 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

- 3 Restart the product.

After the restart, the product automatically loads the firmware specified in step 1.



Tip

The firmware stored in the product is not overwritten.

Note

If loading the firmware file from the external device fails, see “Unable to use USB device” (page 152).

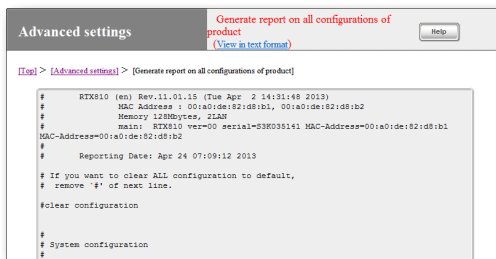
Checking the configuration information and log of the product

Checking configuration information of the product

Information required for connecting with the provider, and various types of configuration information are managed as a single configuration file (config) inside the product. It is convenient to save the configuration file to your PC because you can use it as the backup of settings or edit it with the PC. Furthermore, when you contact our support, being familiar with the content of the configuration file may help solve the problem at an early stage.

- 1 From the top page of “Basic configuration page”, click “Advanced settings”, then click “Execute” of “Generate report on all configurations of product”.

All of the configuration information of the product is displayed on the “Generate report on all configurations of product” screen.



- 2 Copy the displayed configuration information, and paste it to notepad or other software to save it.

Tip

If you want to transfer the configuration file edited in your PC to the product, copy the content of the configuration file in text format to the clip board in advance, and then paste it to the “Execute command” screen (page 120).

Checking the product log

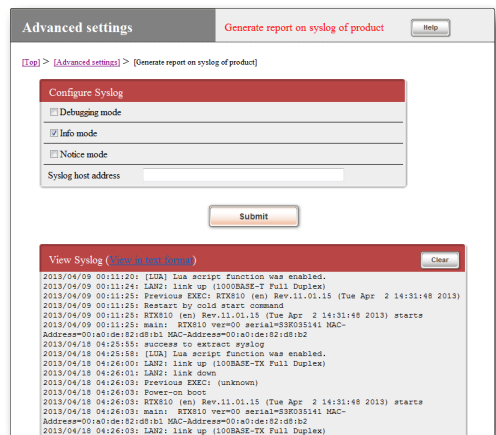
The history of the product operation is managed as a log file (Syslog). Checking the history of the product operation from the log file may give you a clue to solve a network problem.

Tip

There are several steps in the method of saving the log file. Please refer to “Command reference” (included in the attached CD-ROM) for more information.

- 1 From the top page of “Basic configuration page”, click “Advanced settings”, then click “Execute” of “Generate report on syslog of product”.

The product log is displayed on the “Generate report on syslog of product” screen.



- 2 Copy the displayed log, and paste it to notepad or other software to save it.

Checking the configuration information and log of the product

(Continued from the previous page)

Saving the configuration information and log to an external memory device

You can save the configuration information and log of the product to a commercially-available external memory device (USB memory stick or microSD card). Compared with backup via a PC, information required for operation and management can be collected more easily.

Note

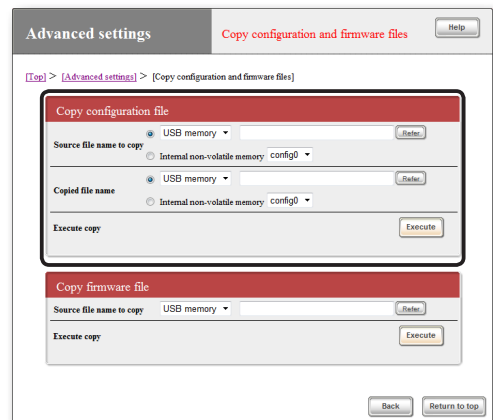
- External memory devices used for the product must be formatted in FAT or FAT32.
- You cannot use a USB hub to connect two or more USB memory sticks or other external memory devices to the product.
- Some types of USB extension cables may not be able to work normally. Use the USB memory stick by inserting it directly into the USB port of the product.
- Do not remove the external memory device while the USB lamp or microSD lamp of the product is lit up or flashing. Doing so may damage data in the external device. Before removing the external device, hold down the USB button or microSD button for two seconds and make sure that the USB lamp or microSD lamp has gone off.

Save the configuration information of the product to an external memory device

- 1 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

- 2 In the “Source file name to copy” field on the “Copy configuration and firmware files” screen, select “Internal non-volatile memory” and specify a config number.



To open the “Copy configuration and firmware files” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Execute” of “Copy configuration and firmware files”

- 3 In the “Copied file name” field, enter a file name used to save the configuration information of the product to the external memory device.

- 4 Click “Execute”.

A confirmation screen appears.

5 Click “Execute”.

The configuration file of the product is written to the external device.

Tip

You can encrypt the configuration file by selecting the “Encrypt the file” checkbox (The password entered on this screen will be required to load the encrypted configuration file.).

6 Hold down the USB button or microSD button for two seconds.

The USB lamp or microSD lamp of the product goes off.

7 Remove the external memory device.

Note

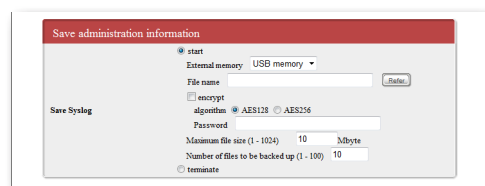
If saving of the configuration file to the external device fails, see “Unable to use USB device” (page 152).

Save the product log to an external memory device

1 Insert the external device into the USB port or microSD slot of the product.

The USB lamp or microSD lamp of the product lights up or flashes.

2 In the “Save Syslog” field on the “Configure external device” screen, select “start” and enter the log file name.



To open the “Configure external device” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure external device”

Tip

You can encrypt the log by selecting the “encrypt” checkbox (The password entered on this screen will be required to load the encrypted log.).

3 Click “Submit”.

The product log is written to the external device. Subsequently, the product log continues to be written to the external memory until you stop saving the log. Please refer to “Notes on the log to be saved” (page 136) for more details on the capacity and other information related to the log to be written.

Checking the configuration information and log of the product

(Continued from the previous page)

4 To stop saving the log, select “terminate” in the “Save Syslog” field on the “Configure external device” screen, and click “Submit”.

5 Hold down the USB button or microSD button for two seconds.

The USB lamp or microSD lamp of the product goes off.

6 Remove the external memory device.

Note

- The log is not recorded immediately after the start, immediately after inserting a USB memory stick, and right before removing the USB memory stick.
- The log cannot be written to the USB memory stick until it is ready to be written.
- If saving of the log to the external device fails, see “Unable to use USB device” (page 152).

Notes on the log to be saved

When you start saving the log, the following log files are generated in the USB memory stick or microSD card.

- A file to which the log is currently written: The file name is the same as that specified in the “Save administration information” field on the “Configure external device” screen.
- A backup file generated for each certain size: The file name is generated by adding saved date/time to the above file name.

Restriction of backup file

If the number of backup files has reached the defined upper limit, or the memory in the external memory device is full, the oldest backup file is deleted.

Note

If the external memory device does not have sufficient free space, the defined log file size or number of backup files may be different from that actually generated.

Customizing the operation according to your environment (Lua script/Custom GUI)

The product operation can be arranged to better fit your environment by using the Lua script or custom GUI function.

Lua scripts

You can run Lua scripts in the product. Embedding APIs unique to Yamaha routers into Lua scripts enables you to change settings or program actions according to the product status.

Example of script:

- Automatically configure settings from the config program settings.
- If transmission to a specific address fails, send e-mail to the administrator.
- If the tunnel is not available, change the route.

Please refer to the following URL for more details on Lua scripts available for the product:

<http://www.yamaha.com/products/en/network/>

Language specifications

Please refer to the following URL for information about specifications of Lua language implemented by Yamaha.

Grammar of Lua language:

<http://www.yamaha.com/products/en/network/>

Library functions:

<http://www.yamaha.com/products/en/network/>

Lua tutorial (for programming beginners):

<http://www.yamaha.com/products/en/network/>

Note

External memory devices and the internal non-volatile memory must be used only for the purpose of saving script files to be executed. Frequent writing to those device consumes them earlier. Please note that, if the internal non-volatile memory fails because of excessively frequent writing operation, in-warranty repair will not apply even within warranty period.

Tip

- Please refer to <http://www.lua.org/> for more details on Lua scripts. For more details on the specifications of the original Lua language, please refer to the Lua 5.1 Reference Manual (<http://www.lua.org/manual/5.1/>).
- The APIs unique to Yamaha routers are published in the following URL (New APIs will be added as needed): <http://www.yamaha.com/products/en/network/>

Customizing the operation according to your environment (Lua script/Custom GUI) (Continued from the previous page)

Custom GUI

You can design original GUIs (user interfaces supporting your web browser) for configuring the product settings, and embed them into the browser (Custom GUI).

- As the product prepares the interface used for transferring settings from the host via HTTP, you can create GUIs using JavaScript.
- Embedding multiple custom GUIs enables you to switch screens according to the login user.
- This is convenient because you can control the rights to access to the product, and also use the restriction of access to functions by changing GUIs.
- Please refer to the following URL for more details on how to specify custom GUIs:
<http://www.yamaha.com/products/en/network/>

When a problem is suspected

Refer to the individual pages that explain for each symptom.

- Q1: Lamps are off (page 140)
- Q2: Setting failed with the “Basic configuration page” (page 142)
- Q3: Internet connection cannot be established (page 144)
- Q4: VPN communication cannot be established (page 146)
- Q5: The DOWNLOAD button does not function (page 151)
- Q6: Unable to use USB device (page 152)
- Q7: Other problems (page 154)

Q1 Lamps are off

Symptom ▶	Cause ▶	Remedy
Lamps are all off.	The POWER switch is in STANDBY.	Turn on the POWER switch.
	The power cord is not plugged into an electrical outlet.	If the power cord is not plugged, plug it correctly.
	The main breaker or individual breaker is thrown.	<ul style="list-style-type: none">• If the breaker is “OUT”, turn it “IN”.• If the breaker is “IN”, turn it “OUT”, and then turn “IN” again.
	The power is out.	When the power is out, wait for service to be restored.
	No power is supplied to the electrical outlet. (Other electrical appliances do not function either.)	<ul style="list-style-type: none">• If other appliances do not function either, ask for repair of the electrical outlet or electrical wiring.• If other appliances function, ask for repair of the product.
The LAN lamp does not light up.	The hub or PC is not powered on. Although the device is connected to the LAN1 port correctly, the LAN1 lamp of the product will not light up unless the device power is off.	Power on the device connected to the product.
	The device is not connected correctly.	Disconnect the connectors from the product, PC and hub, and reconnect them until the connector clicks.
	The LAN cable is not used. The ISDN cable is used. (Attention is needed as the shape of the connector is exactly the same.)	Use the LAN cable.
	The LAN (network) card of the PC does not function correctly, or the connection mode does not match with that of the product.	<ul style="list-style-type: none">• Check that the LAN board (card) of the PC is installed correctly, and it functions correctly.• Check if the communication speed and connection (duplex) mode of the LAN board (card) of the PC matches with those of the product.
	The cable is disconnected.	Replace with another LAN cable.

Symptom ▶	Cause ▶	Remedy
The WAN lamp does not light up.	The ADSL modem, cable modem, or ONU is not powered on.	Power on.
	The product is not correctly connected to the ADSL modem, cable modem, or ONU.	Disconnect the WAN port of the product, and the cables of the ADSL modem, cable modem and ONU, and reconnect until the connector clicks.
	The correct cable is not used.	Use the same cable type that is used for connection of the ADSL modem, cable modem or ONU with the PC.

Q2 Setting failed with the “Basic configuration page”

Symptom ▶	Cause ▶	Remedy
Unable to display the “Basic configuration page”.	The product does not recognize the PC. (The LAN lamp does not light up.)	Troubleshoot according to the explanation of “The LAN lamp does not light up.” (page 140)
	The network setting of the PC is inappropriate. (Other PCs and network printers on the LAN do not function either.)	<ul style="list-style-type: none">● Try again to set the LAN board and LAN card settings, and restart the PC.● Reacquire the IP address.
	The product malfunctions.	Restore the product to the default state, and retry the setting (page 159).
	The IP address of the product has been changed.	<ul style="list-style-type: none">● Access the IP address specified for the product “http://(IP address of the product)”.● Restart all PCs connected to the product and the LAN. If the PCs cannot be restarted or powered off, connect only one PC to the product, disconnect all other LAN cables, and then power on the product and the PC.● Check that the IP address of the PC matches with the network address of the product, and also it does not conflict with the IP address of another device. If anything is wrong, change the IP address to an appropriate one.
	The URL of the product is inappropriate.	When the product is used for the first time, or after it has been restored to the factory default, access “http://192.168.100.1”.
	LAN is not specified for the connection path setting of the Web browser of the PC.	In case of the Windows version of Internet Explorer, if the dialup connection is enabled in “Internet Options” - “Connection” tab, you cannot access the “Basic configuration page”. Therefore, select “Never dial a connection”.
	Proxy server is used in the Web browser of the PC.	If the proxy setting is incorrect, the “Basic configuration page” cannot be displayed. Check the proxy setting.

Symptom ▶	Cause ▶	Remedy
Unable to display the “Basic configuration page”. (Continued from the previous page)	The PC is controlled remotely via Web browser.	<ul style="list-style-type: none"> ● If the access restriction function through IP address is enabled, when an access is attempted from an unauthorized host, the message “Error 503 This server is available to members only. I’m sorry, your host is not member.” is displayed. To remotely control the PC, change the setting of “Hosts permitted to use HTTP” (page 100).
The “Basic configuration page” does not appear after entering the password.	The password is not correct. (The password error is displayed.)	<ul style="list-style-type: none"> ● For password, the system distinguishes between single-byte and double-byte characters and between upper and lower cases. Always enter the password using single-byte characters and be aware of case sensitivity. ● If authentication information (user name, password) remains in the Web browser, such information will be sent and an error may result. Delete the user name before entering the password, or close the Web browser and reopen the “Basic configuration page”.
	The login password was entered. (The administration password should be used here.)	If password has been set, enter the administration password.
The setting is returned to the original state.	You did not click “Submit” after configuration.	If you have changed the setting in the “Basic configuration page”, you must click “Submit” to save the setting. If you fail to click “Submit” but click “Return to top” or close the window, the setting will not be saved.
	You have entered an invalid value or one that is outside the allowable range.	Enter a correct value.
The password cannot be saved in the Web browser when opening the “Basic configuration page”.	The “User name” field is empty in the screen prompting you to enter the user name and password.	Some Web browsers require user name entry to save password. In this case, enter an arbitrary character string.

Q3 Internet connection cannot be established

Symptom ▶	Cause ▶	Remedy
Broadband connection cannot be established.	The product does not recognize the broadband line. (The WAN lamp does not light up.)	Troubleshoot according to the explanation of “The WAN lamp does not light up.” (page 141)
	The user ID or password is not correct.	Refer to the setup document supplied by the provider, and enter the required information correctly.
The homepage is not displayed or the display speed is slow.	The DNS server address specified by the provider is not correct.	<ul style="list-style-type: none">● Check whether the DNS server address is specified in the provider connection setting.● Enter the IP address of the product in the DNS server address setting of each PC, and restart the PC.● The Web server or DNS server may be overloaded or suspended. Re-attempt access after a while.
	The filtering function of the product is enabled.	If the IP address given by the provider is a private address, and the security filter such as Firewall is applied, change the security level to 2, 4 or 6 (page 96).
	There is a problem with line type. (PPPoE method ADSL connection only)	Depending on the type of ADSL line, with the standard setting, you cannot receive some kind of homepage data or the data reception rate is very slow. Disconnect the connection, and in the “Basic configuration page”, click “Advanced settings” - “Detailed basic connection setting”. In the “Register/modify provider” screen, enter 1454 for MTU, enter other values, and then reconnect.
	The IP address given by the provider conflicts with the IP address specified for the product.	In the “Basic configuration page” - “Configure LAN” screen, change the IP address of the product so as not to conflict with the IP address given by the provider (page 29). In this case, the Firewall function of the product must be applied again.

Symptom ▶	Cause ▶	Remedy
The homepage is not displayed or the display speed is slow. (Continued from the previous page)	The network setting of the PC is inappropriate.	<ul style="list-style-type: none">● Try again to set the LAN board and LAN card settings, and restart the PC.● Reacquire the IP address.
	The line, provider, or the Web server is overloaded.	Transmission rate is very slow in some time zones. If the rate remains very slow for a long period of time compared to the line speed, contact your carrier or provider.

Q4 VPN communication cannot be established

Symptom ▶	Cause ▶	Remedy
<p>In the top page of the “Basic configuration page”, the message “Communicating” is not displayed for the IPsec tunnel connection.</p>	<p>Internet connection cannot be established.</p>	<ul style="list-style-type: none"> • Check whether the setting for Internet connection has been configured. • Troubleshoot according to the explanation of “Q3 Internet connection cannot be established” (page 144).
	<p>Communication cannot be established with the destination of IPsec connection.</p>	<p>Execute the ping command to the destination IP address of IPsec, and check whether a response is returned. If no response is returned, check whether communication is enabled in the destination device.</p>
<p>VPN communication cannot be established through IPsec connection.</p>	<p>IPsec connection is not established.</p>	<ul style="list-style-type: none"> • Check whether the same pre-shared key as the IPsec connection destination is specified. • Check whether the correct IP address and correct name are specified in the method used to identify the destination. • Check whether the same authentication algorithm and encryption algorithm as the IPsec connection destination are specified.
	<p>Incorrect routing information has been configured.</p>	<p>Configure the correct destination LAN network address for the routing information.</p>
	<p>The setting is not correct in the PC connected to the destination LAN.</p>	<ul style="list-style-type: none"> • Check the setting of the application software used for communication. • If the Firewall function is enabled in the PC, change the Firewall setting so as not to block packets used for communication. In Windows 7, on the screen that appears by clicking “Start” - “Help and Support”, enter “Firewall” in the search field, and carry out a search. Relevant information is displayed. Troubleshoot according to the instruction.
<p>The VPN communication of the IPsec connection is slow.</p>	<p>The Internet connection is slow.</p>	<p>Troubleshoot according to the explanation of “Q3 Internet connection cannot be established” (page 144).</p>
<p>L2TP/IPsec cannot be configured for the terminal.</p>	<p>The terminal does not support L2TP/IPsec.</p>	<p>Prepare a terminal that supports L2TP/IPsec. For the configuration procedure, refer to the manual of the terminal.</p>

Symptom ▶	Cause ▶	Remedy
L2TP/IPsec connection or VPN connection cannot be established.	The service of L2TP/IPsec is not enabled.	Enable the service of L2TP/IPsec (Configure as "l2tp service on".).
	The IPsec setting is not correct.	<ul style="list-style-type: none"> ● Check if the pre-shared key of IPsec is correct. ● Check the type of tunnel interface (tunnel encapsulation l2tp).
	The PPP setting is not correct.	<ul style="list-style-type: none"> ● Check if the ID and password for the PPP authentication are correct. ● Check that the tunnel interface is bound in the PP interface (pp bind tunnel1).
	The terminal setting is not correct.	<ul style="list-style-type: none"> ● Check if the destination address and the host name are correct. ● Check if the pre-shared key of IPsec is correct. ● Check if the user ID and password for PPP authentication are correct. If user ID or password is not correct, change to the correct one. ● For the configuration of the terminal, refer to the manual of the terminal.
	Communication with the destination cannot be established.	<p>Execute the ping command to the destination IP address, and check whether a response is returned.</p> <p>If no response is returned, check whether communication is enabled in the destination device.</p>
L2TP/IPsec connection is disconnected immediately.	The signal quality of the terminal is poor.	Check the signal quality of the terminal, and move to a place where signal quality is good.
	The disconnection timer of L2TP/IPsec is set.	Set the disconnection timer of L2TP/IPsec to an appropriate time.
	The keep alive setting of L2TP/IPsec is inappropriate.	<p>Set the interval and count of the keep alive of L2TP/IPsec to an appropriate value.</p> <p>In places with poor signal quality, the response of keep alive may be lost temporarily.</p>

Q4 VPN communication cannot be established

(Continued from the previous page)

Symptom ▶	Cause ▶	Remedy
Communication with the terminal located within the VPN destination network cannot be established.	IP address has not been acquired.	Check on the terminal whether the IP address used in the VPN destination is acquired. For the confirmation procedure of IP address, refer to the manual of the terminal.
	Incorrect routing information has been configured.	Configure the correct destination LAN network address for the routing information.
	Proxy ARP setting is absent.	Run the proxy ARP in the VPN destination LAN (ip lan1 proxyarp on).
In the top page of the “Basic configuration page”, the message “Communicating” is not displayed for the PPTP tunnel connection.	A private IP address is assigned by the provider.	You cannot use the PPTP-related functions in the environment where no global IP is assigned to the product.
	Internet connection cannot be established.	<ul style="list-style-type: none">• Check whether the setting for Internet connection has been configured.• Troubleshoot according to the explanation of “Q3 Internet connection cannot be established” (page 144).
	Communication cannot be established with the destination of PPTP connection.	Execute the ping command to the destination IP address of PPTP, and check whether a response is returned. If no response is returned, check whether communication is enabled in the destination device.

Symptom ▶	Cause ▶	Remedy
VPN communication cannot be established through PPTP connection.	PPTP connection is not established.	<ul style="list-style-type: none"> ● Check whether the same user ID and connect password as the PPTP connection destination are specified. ● Check whether the correct values are specified in the destination host name and IP address.
	Incorrect routing information has been configured.	Configure the correct destination LAN network address for the routing information.
	The setting is not correct in the PC connected to the destination LAN.	<ul style="list-style-type: none"> ● Check the setting of the application software used for communication. ● If the Firewall function is enabled in the PC, change the Firewall setting so as not to block packets used for communication. In Windows 7, on the screen that appears by clicking “Start” - “Help and Support”, enter “Firewall” in the search field, and carry out a search. Relevant information is displayed. Troubleshoot according to the instruction.
In the top page of the “Basic configuration page”, the message “Communicating” is not displayed for the IPIP tunnel connection.	The product is not connected to a closed network.	Check whether the setting for connection to a closed network has been configured.
	Communication cannot be established with the destination of IPIP tunnel connection.	Execute the ping command to the destination IP address of IPIP tunnel, and check whether a response is returned. If no response is returned, check whether communication is enabled in the destination device.

Q4 VPN communication cannot be established


(Continued from the previous page)

Symptom ▶	Cause ▶	Remedy
VPN communication cannot be established through IPIP tunnel connection.	IPIP tunnel connection is not established.	<ul style="list-style-type: none">● Check whether the IP address issued for the destination by the closed network is correctly specified in the destination IP address.● In the “Basic configuration page”, select “Advanced settings” - “Configure VPN connection”. In the setting screen for IPIP tunnel connection, check whether the interface used for connection with the closed network is selected for “Connection provider”.
	Incorrect routing information has been configured.	Configure the correct destination LAN network address for the routing information.
	The setting is not correct in the PC connected to the destination LAN.	<ul style="list-style-type: none">● Check the setting of the application software used for communication.● If the Firewall function is enabled in the PC, change the Firewall setting so as not to block packets used for communication. In Windows 7, on the screen that appears by clicking “Start” - “Help and Support”, enter “Firewall” in the search field, and carry out a search. Relevant information is displayed. Troubleshoot according to the instruction.
The VPN communication of the IPIP tunnel connection is slow.	The closed network connection is slow.	Contact the carrier regarding problems with line condition.
Windows files cannot be shared.	Filter to NetBIOS traffics is enabled.	Click “Advanced settings” - “Configure firewall” screen, click “Configure” for the IPv4 filter of the LAN port. In the “Configure IPv4 firewall” screen, clear the check box for the filter of NetBIOS traffics in “IPv4 static IP filter list”, and then click “Submit”.

Q5 The DOWNLOAD button does not function

Symptom ▶	Cause ▶	Remedy
The firmware is not updated even after pressing the DOWNLOAD button.	Internet connection cannot be established.	Check whether the setting for Internet connection has been configured. Troubleshoot according to the explanation of “Q3 Internet connection cannot be established” (page 144).
	The download link URL of the firmware is not correct.	In the “Basic configuration page”, click “Advanced settings” - “Execute revision up”, and specify “URL to download” correctly.
	Use of the DOWNLOAD button is not permitted.	In the “Basic configuration page”, click “Advanced settings” - “Configure DOWNLOAD button”, and change the setting to permit upgrading.
	The latest version of the firmware is used.	Use as it is.
The lamps in the front side start to light up in turn.	The firmware is being written to the non-volatile memory (normal operation).	Wait a while. Do not disconnect the cable or power off.

Q6 Unable to use USB device

Symptom ▶	Cause ▶	Remedy
The USB lamp does not light up.	Use of the USB port is not permitted.	Change the setting to permit the use of the USB port.
	A device other than USB memory stick is inserted.	Insert a USB memory stick. Please refer to the following URL for more details on use of USB memory sticks: http://www.yamaha.com/products/en/network/
	The USB memory stick is not functioning correctly.	Check with a PC or others if the USB memory stick is usable.
	The USB memory stick is inserted via a hub.	The product does not support USB hub. Insert the USB memory stick directly into the USB port of the product.
USB memory sticks cannot be used while the lamp is flashing.	The USB memory stick is inserted via a USB extension cable.	Use the USB memory stick by inserting it directly into the USB port of the product.
	Use of the USB function is stopped by the overcurrent protection function.	Use a USB memory stick with low consumption current. To restore the function, press and hold the USB button for one second or more.
Data is not copied even after pressing the USB button and DOWNLOAD button.	File copy through button operation is now allowed.	Change the setting to permit file copying through button operation.
	No setting file or firmware file that allows copy through button operation exists in the USB memory stick.	Using a PC or others, copy the file that has been specified in the “Basic configuration page” to the USB memory stick.
There is missing information in the syslog saved in the USB memory stick.	The log is not recorded immediately after the start, immediately after inserting a USB memory stick, and right before removing the USB memory stick.	The log cannot be written to the USB memory stick until it is ready to be written.
	The amount of data in the syslog is too large to write to the USB memory stick in time.	Reduce the amount of data in the syslog by changing the save mode of log or others.  Tip If a USB 1.1-compatible USB memory stick is used, the symptom may be improved by using a USB 2.0-compatible USB memory stick.

Symptom ▶	Cause ▶	Remedy
Although the firmware has been copied manually by entering a command, the setting is not reflected.	Only copying the firmware manually by entering a command, the setting is not reflected in the actual operation.	Manually copy the firmware, and then restart the product.
Although the setting file has been copied manually by entering a command, the setting is not reflected.	Only copying the setting file manually by entering a command, the setting is not reflected in the actual operation.	Manually copy the setting file, and then restart the product.

Q7 Other problems

Symptom ▶	Cause ▶	Remedy
Time setting using NTP server cannot be made with the product or PC.	The NTP server IP address or domain name is not correct.	<ul style="list-style-type: none"> • Check that the setting is correct by comparing with the NTP server information you have obtained. • Execute the ping command to the NTP server, to make sure that the NTP server is running.
	The route to the registered NTP server is not specified.	Check the provider setting and routing setting.
	The security filter of the product is enabled.	<ol style="list-style-type: none"> 1. In the “Basic configuration page”, select “Advanced settings” - “Configure firewall” - “Configure IPv4 firewall” screen. Select both “in” and “out” check boxes in the pass filter (No. 36 and 37) that allows traffic to pass through the NTP port (port No. 123) which are displayed at the bottom of “IPv4 static IP filter list”. 2. Set the security level to 6 or 7 (page 103).
The host address cannot be obtained from the netvolante DNS service.	Depending on the provider, name resolution is not possible immediately after registration/update.	Retry after a while.
	The product is connected via a network provider connection.	If the product is connected via a network provider connection, the netvolante DNS service is not available. Directly specify the IP address for connection.
	A private IP address is assigned by the provider.	You cannot use the netvolante DNS service in the environment where no global IP is assigned to the product.
You have forgotten the password.		Troubleshoot by referring to “If you have forgotten the password” (page 161).

Communication charges of the USB data communication terminal is abnormal

Check the provider setting

Even if the USB data communication terminal contract is a flat-rate system any use of it with an incorrect configuration could be charged for under the measured-rate system. In the “Basic configuration page”, click “Advanced settings ” - “Detailed basic connection setting”. In the “Modify provider” screen, check that the setting is correct.

Check the communication history

If the Internet connection is made by the auto-connect function, Internet connection may be made automatically by software or a device of the PC. Also, certain types of software are activated automatically while the PC is starting. In this case, outgoing calls may be generated automatically without the user's knowledge. If the USB data communication terminal contract is the measured-rate system, you may be charged substantial fees. To prevent this, check the communication history frequently.

Be especially careful when you:

- start using the product;
- change any provider connection settings of the product;
- change the dial network setting of the PC;
- install new software on your PC;
- connect to the network with a new PC, network equipment, or peripheral equipment;
- update the firmware of the product; or
- perform any different operations than usual or sense a difference in the communication response.

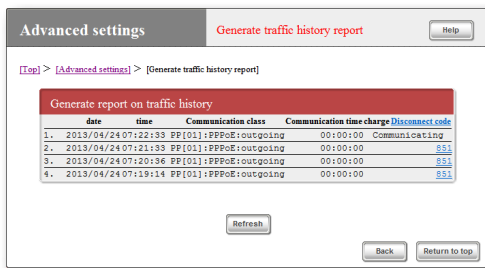
Note

- After cancelling or changing your provider contract please be sure to delete or reconfigure the connection configuration of the product. Failure to observe this could result in unexpected charges from your telephone carrier or provider.
- Unexpected communication charges could occur according to the status (change in access point, maintenance, error, etc.) of the provider side. Please be sure to pay constant attention to any notifications you receive from your provider.
- The screen and settings used here may vary by software version.

Communication charges of the USB data communication terminal is abnormal (Continued from the previous page)

Checking with the “Generate traffic history report” screen

In the “Basic configuration page”, click “Advanced settings”. In the “Generate traffic history report” screen, you can check the communication history for each port.



Date, time, communication class, communication time, and disconnect code are displayed for a maximum of 100 records in the reverse chronological order. If the communication class appears as PPxx, it is connected to the provider (or LAN-to-LAN connection pair).

Checking with log information

In the “Basic configuration page”, click “Advanced settings”. In the “Generate report on syslog of product” screen, you can check the access log that triggered auto connection.

If there is a number of unintended accesses, look for the row “IP Commencing” from the bottom in the syslog. Use the IP address of the PC or IP address of the access destination host, access time (or interval) in the “IP Commencing” row as a clue, locate the software (or device) that issued the access request, and identify the cause.

Access example 1

```
PP[01] IP Commencing :UDP 192.168.100.1 :53 > xxx.xxx.xxx.xxx :53  
(DNS Query [windowsmedia.com] from 192.168.100.2)
```

- PP [01]: Provider No.
- 192.168.100.2: IP address of PC
- xxx.xxx.xxx.xxx: Access destination IP address

In this example, when a PC (192.168.100.2) in the LAN issues an inquiry for the host (windowsmedia.com) IP address of the Internet to the DNS server, auto connection to the provider is triggered.

Access example 2

```
PP[01] IP Commencing : TCP 192.168.100.2:1311 > xxx.xxx.xxx.xxx:80
```

In this example, when a PC (192.168.100.2) in the LAN issues an access request for the Internet host (xxx.xxx.xxx.xxx), auto connection to the provider is triggered.

Checking the suspicious settings

The following settings are suspected as the cause of unintended Internet access: When you use a new operating system first time, or when you have installed new software, check the setting by using the following example as a reference.

If outgoing calls are generated frequently,

check the DNS setting value in the network setting of the PC. If an IP address of a DNS server located in the Internet is specified, Internet access may be made frequently.

If outgoing calls are generated every time the PC is started,

if there is any software that is started at the same time with the start of PC, depending on the setting, Internet access may be made every time the PC is started. Check the software setting, and if auto update or other functions are enabled, change the setting.

Setting of Windows XP

If a Web page is displayed on the desktop, Internet access may be made every time the PC is started, and the content of the Web page is updated. Therefore, you will be charged for communication every time the PC is started. If you do not need such setting, cancel the setting.

If outgoing calls are generated at regular intervals,

- If outgoing calls are generated many times a day: Windows Update may be used or the automatic e-mail transmission/reception may be enabled. Check the relevant software setting of the PC connected to the LAN of this product.
- If outgoing calls are generated several times a day: check the settings of the maintenance program of the hardware or NTP server (Internet automatic time server).

Home page banner advertising

If the homepage includes a banner advertising, the homepage may be updated automatically at regular intervals although no operation is performed. If you leave the Web browser with the page open, Internet connection is made at regular intervals, incurring fees each time. Close the Web browser each time, to prevent unintended Internet access.

Subscription of contents

If Internet Explorer fields and Web slices are used, Internet connection is made at specified intervals to update the contents. You will be charged every time the contents are updated. Therefore, when you subscribe a content, check the update interval carefully.

If you do not need such setting, cancel the setting.

Communication charges of the USB data communication terminal is abnormal

(Continued from the previous page)

E-mail software setting

E-mail software has a function to check incoming e-mail messages periodically. If this function is enabled, access to the mail server on the Internet is made at regular intervals, and you will be charged each time. When you use this function, carefully consider the e-mail check frequency.

If you do not need such setting, cancel the setting, and check e-mail manually.

Automatic updating of operating system

If the automatic updating function of the operating system is enabled, access to the server on the Internet is made at regular intervals, and you will be charged each time. If you do not need such setting, change the setting to manual update, and manually update while Internet connection is established.

If outgoing calls are generated every time the software is started,

check the environment setting (default setting) of the software you have installed, and if auto update or other functions are enabled, change the setting.

Software setting

If the automatic updating function of the software is enabled, access to the Internet is made every time the software is started, and you will be charged each time.

If you do not need such setting, cancel the setting.

Windows Media Player operating environment setting

If you have installed Windows Media Player, Internet connection is made every time Media Player is opened to obtain the information in the guide page. Therefore, you will be charged each time.

If you do not need such setting, cancel the setting according to the help page.

Initializing the product settings

You can restore the product settings to their factory defaults.

Note

When restoring the settings to their factory defaults, be sure to note the following:

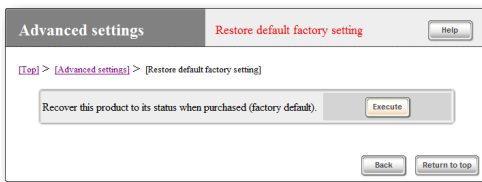
- All communications are disconnected immediately after the restoration is performed.
- Any setting that has default value is changed to the default value.
- Filter definitions and registered address are deleted.
- Non-volatile memory content are overwritten without the save command.
- You cannot restore the original setting once the operation is complete.

Tip

If you save the settings to an external memory before initialization, you can restore the original settings after initialization. Please refer to “Checking the configuration information and log of the product” (page 133) for the procedure to save setting.

Initializing from the “Basic configuration page”

If you want to restore the product settings to their factory defaults, you can initialize the setting in the “Restore default factory setting” screen.



For more details on the settings, click “Help” on the setup screen and refer to the description displayed.

To open the “Restore default factory setting” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ Executing the “Restore default factory setting” function

If you cannot initialize from the “Basic configuration page”

If you cannot initialize the setting from the “Basic configuration page” of the product, for example, when you have set a wrong IP address of the product, you can alternatively initialize the setting using the PC connected to the console port, or through button operation of the product.

Initializing from the PC connected to the console port

- 1 Power off the product.
- 2 Connect the console port of the product to the serial port of your PC with a serial cable.

Please refer to page 121 for details on the connection and setting of the PC.

- 3 Start the terminal software on the PC.

Please refer to page 122 for more information.

- 4 Power on the product.

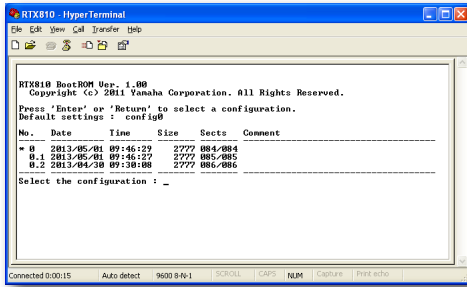
The version of the ROM of the product is displayed in the terminal software screen of the PC, pending for pressing the Enter key.

- 5 Press the Enter key before the count down of “Will start automatically in ...” ends.

If the count down of “Will start automatically in ...” ends, the product will start in normal procedure. If the product has started, power off the product once, wait for 10 seconds or more, and then power on again to operate.

Initializing the product settings (Continued from the previous page)

- 6 When the system goes into a pending status for selecting a setting file, select a setting file that is not shown, from 0 to 4.2, and press the Enter key.



If the firmware is started, the firmware version and other information is displayed.

- 7 Wait for around 10 seconds, and press the Enter key.

- 8 When "Password:" appears, press the Enter key.

When ">" is displayed, you can enter a console command.



If the login password has been set, enter the login password.

- 9 Type in "administrator", and press the Enter key.

- 10 When "Password:" appears, press the Enter key.



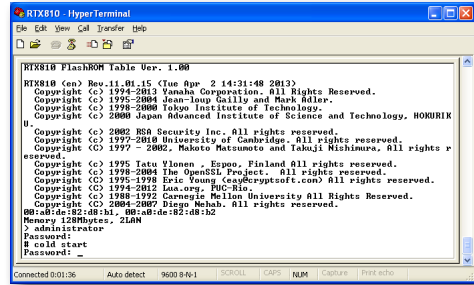
If an administration password has been set, enter the administration password.

- 11 When "#" appears, enter "cold start" and press the Enter key.

- 12 When "Password:" appears, press the Enter key.



If an administration password has been set, enter the administration password.

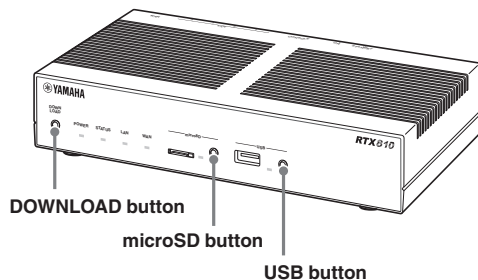


The product settings are initialized.

Initializing through button operation of the product

You can also restore the setting to their factory defaults by turning the power on while pressing the three buttons; DOWNLOAD, microSD, and USB buttons.

- 1 Turn the power on while pressing the three buttons; DOWNLOAD, microSD, and USB buttons.



The lamp at the front side of the main unit lights up and flashes several times.

- 2 Turn the power on, wait for 3 seconds, and then press the three buttons; DOWNLOAD, microSD, and USB buttons.

The product settings are initialized.

If you have forgotten the password

If you have forgotten the text strings specified as login password or administration password, you cannot login to the product. Even in this case, by entering the following emergency password from the serial terminal connected to the console port, you can login to the product.

Emergency password

“w,lXlma”



Tip

Please refer to page 121 for details on the connection to the console port and setting of the PC.

If you login to the product by using the emergency password, you will login with the administrator mode. Then set again the login password and administration password that you have forgotten. You can also use this emergency password for the old password that is requested when setting a password.

Note

You can disable this function by setting the security class command. You cannot login using this procedure if the second parameter is not set to “ON” in the security class command. In this case, initialize the procedure according to “Initializing through button operation of the product” (page 160). Please refer to “Command reference” (included in the attached CD-ROM) for more details on the security class command.

Major specifications

External dimensions (Width x Height x Depth):

220 mm x 42.6 mm x 160.5 mm
(not including any protrusions and cable terminals)

Weight:

Main unit: 870 g

Power supply:

AC100 to 240V (50/60Hz), 0.23A (max)

Power consumption:

Max. 11 W

Operating environment:

Ambient temperature: 0 to 50°C
Ambient humidity: 15 to 80% (no condensation)

Storage environment:

Ambient temperature: -20 to 50°C
Ambient humidity: 10 to 90% (no condensation)

Regulatory Compliance:

Safety: IEC 60950-1, EN 60950-1
EMC: EN 55022 Class A, EN 55024, VCCI Class A

LAN interface:

Ethernet (RJ-45)
10BASE-T/100BASE-TX/1000BASE-T
4-port switching hub
Straight/Cross auto-distinction

WAN interface:

Ethernet (RJ-45)
10BASE-T/100BASE-TX/1000BASE-T
1 port
Straight/Cross auto-distinction

Serial interface:

DTE fixed (cross cable for connecting to a PC)
Number of ports: 1
Asynchronous serial: RS-232C
Connector: D-sub 9 PIN
Data transfer speed: 9600bit/s
Data bit length: 8-bit
Parity check: None
Stop bit number: 1-bit
Flow control: software (Xon/Xoff)

USB interface:

High/Full/Low speed available
Feed current: Max. 500 mA
Number of ports: 1
Connector: USB Type-A connector

microSD interface:

Number of ports: 1
Connector: microSD slot

Indication function (LED)

Front panel: POWER, STATUS, LAN, WAN, microSD, USB
Rear panel: LINK/DATA, SPEED

Accessories:

LAN cable (3m, RJ-45, straight) (x1)
Please ensure to read this first.
CD-ROM (x1)
(includes “Please ensure to read this first”,
“Command reference”, etc.)

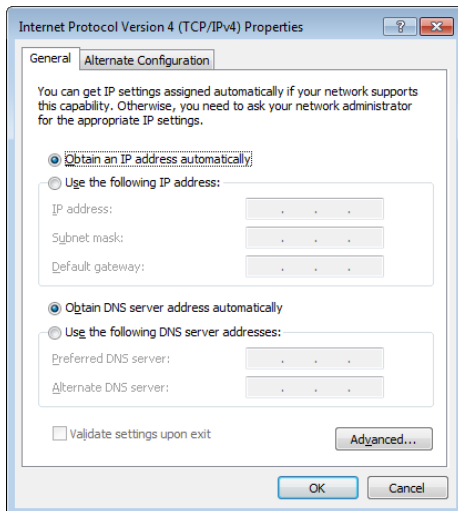
Changing the IP addresses of PCs

To change the IP address of the PC, take the following steps.

For Windows 7

- 1 Click the “Start” button, then click “Control Panel”.
- 2 Enter “Adapter” in the search field at the upper right in Control Panel, and under “Network and Sharing Center”, click “View network connections”.
- 3 Right-click the connection that you want to change. From the short cut menus that appear, click “Properties”.
- 4 Click the “Network” tab.
- 5 In the “This connection uses the following items” field, click to select “Internet Protocol Version 4 (TCP/IPv4)”, and then click “Properties”.

- 6 Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, and then click “OK”.
- 7 In the “Local Area Connection Properties” screen, click “OK”.
- 8 Click the “Start” button, then click “All Programs” - “Accessories” - “Command Prompt”.
- 9 Type in “ipconfig /release”, and press the Enter key.
The IP address assigned to the PC is released.
- 10 Type in “ipconfig /renew”, and press the Enter key.
New IP address is assigned to the PC.
- 11 Repeat steps 1 to 10 on all PCs in the LAN, so that all PCs have different IP addresses.



Changing the IP addresses of PCs

(Continued from the previous page)

For Windows Vista

- 1 Click the “Start” button, then click “Control Panel”.
- 2 Click “Network and Internet”.
- 3 Click “Network and Sharing Center”.
- 4 Click “Manage network connections” on the left of the screen.
- 5 Right-click the connection that you want to change. From the short cut menus that appear, click “Properties”.
- 6 Click the “Network” tab.
- 7 In the “This connection uses the following items” field, click to select “Internet Protocol Version 4 (TCP/IPv4)”, and then click “Properties”.

- 8 Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, and then click “OK”.
- 9 In the “Local Area Connection Properties” screen, click “OK”.
- 10 Click the “Start” button, then click “All Programs” - “Accessories” - “Command Prompt”. Right-click on it and select “Run as Administrator”.

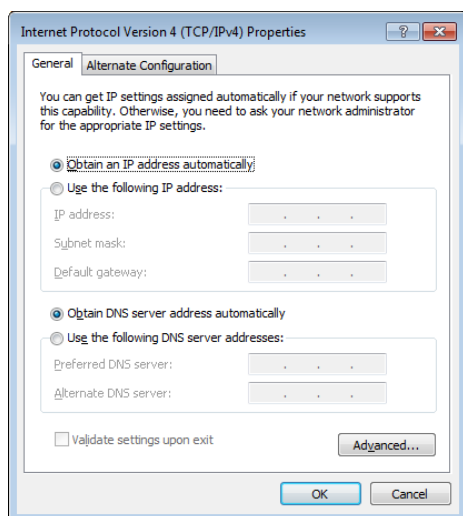
- 11 Type in “ipconfig /release”, and press the Enter key.

The IP address assigned to the PC is released.

- 12 Type in “ipconfig /renew”, and press the Enter key.

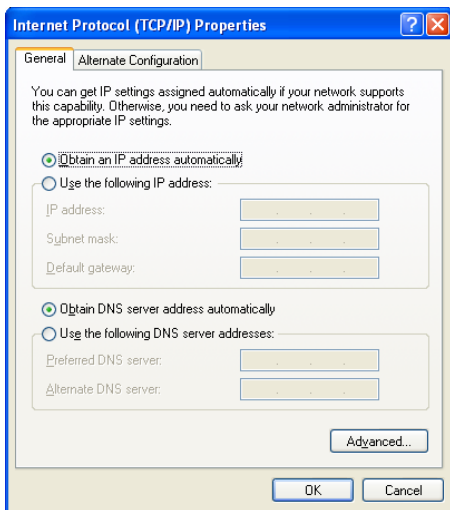
New IP address is assigned to the PC.

- 13 Repeat steps 1 to 12 on all PCs in the LAN, so that all PCs have different IP addresses.



For Windows XP

- 1 Click the “Start” button, then click “Control Panel”.
- 2 Click “Network and Internet Connections”.
- 3 Click “Network Connections”.
- 4 Click the “Local Area Connection” icon.
- 5 Click “Change settings of this connection”.
- 6 Select “Internet Protocol (TCP/IP)” and then click “Properties”.



- 7 Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, and then click “OK”.
- 8 In the “Local Area Connection Properties” screen, click “OK”.
- 9 Click the “Start” button, then click “All Programs” - “Accessories” - “Command Prompt”.

- 10 Type in “ipconfig /release”, and press the Enter key.

The IP address assigned to the PC is released.

- 11 Type in “ipconfig /renew”, and press the Enter key.

New IP address is assigned to the PC.

- 12 Repeat steps 1 to 11 on all PCs in the LAN, so that all PCs have different IP addresses.

Instructions on transferring/disposing of the product

If you transfer/dispose of the product you will need to perform the following operations.

- 1.Delete the netvolante DNS registration.
- 2.Initialize all the configurations.

Note

- If you initialize the configurations first, you will not be able to delete the host address registered in the netvolante DNS server. Be sure to delete the registration of netvolante DNS before initializing the configurations.
- Deletion of the netvolante DNS registration is necessary only for customers who have registered the netvolante DNS (host address service).
- If you transfer the product you will also need to transfer the accompanying instruction manuals.

Initialize all the configurations

The saved configurations include ID and password required for connection to the provider. If you transfer/dispose of the product without initializing the configurations, such information may be used for bad ends by a third party with knowledge.

Please refer to “Initializing the product settings” (page 159) for details on the initialization procedure.

Delete the netvolante DNS registration

For effective operation of the netvolante DNS service, your cooperation would be appreciated to delete the unnecessary netvolante DNS before transferring/disposing of the product.

In the “Configure NetVolante DNS host address service” screen, click “Delete”.

NetVolante DNS service (Host address service)	
Connection provider	1PP01 PPPoE
Host address	yamaha-test.as1.netvolante.jp
Auto update any change in IP address	<input checked="" type="radio"/> on <input type="radio"/> off
IP address	000.000.000.000
Last date/time update	2013/05/07 06:51:41
Timeout period	90 1~180second

Buttons: Submit, Execute, Delete, Back, Return to top

To open the “Configure NetVolante DNS host address service” screen

From “Basic configuration page”, click the buttons on the setup screen in the following order:

- ▶ “Advanced settings” in the top page
- ▶ “Configure” of “Configure NetVolante DNS host address service”

License terms and conditions

PCRE License

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the “BSD” licence, as specified below. The documentation for PCRE, supplied in the “doc” directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England.
Phone: +44 1223 334714.

Copyright © 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MT19937 License

A C-program for MT19937, with initialization improved 2002/1/26.

Coded by Takuji Nishimura and Makoto Matsumoto.

Before using, initialize the state by using `init_genrand(seed)` or `init_by_array(init_key, key_length)`.

Copyright © 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Any feedback is very welcome.

<http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html>

email: [m-mat @ math.sci.hiroshima-u.ac.jp](mailto:m-mat@math.sci.hiroshima-u.ac.jp) (remove space)

OpenSSL License

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

Copyright © 1998-2002 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,

OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Net-SNMP License

Copyright 1988, 1989, 1991, 1992 by Carnegie Mellon University All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

