ICOM

INSTRUCTION MANUAL

VPN ROUTER

SR-VPN1

INTRODUCTION

1 BEFORE USING THE SR-VPN1

2 ABOUT THE INTERNET CONNECTION

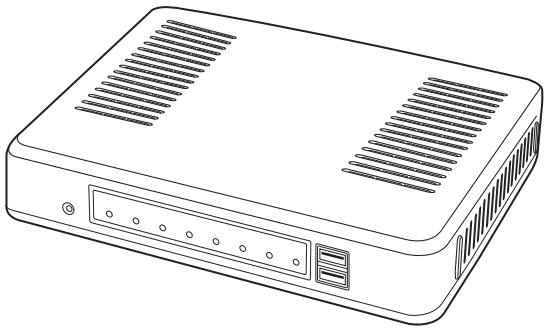
3 IPsec Wizard

4 OTHER BASIC FUNCTIONS

5 ABOUT THE SETTING SCREEN

6 MAINTENANCE

7 FOR YOUR INFORMATION



Icom Inc.

INTRODUCTION

Thank you for purchasing this Icom product. The SR-VPN1 VPN ROUTER is designed and built with Icom's IP network technology.
We hope you agree with Icom's philosophy of "technology first." Many hours of research and development went into the design of your SR-VPN1.

INTRODUCTION

FEATURES

- Secure, protected IPsec tunneling connecting up to 32 locations.
- Proven to work with IDAS multi-site systems.
- Supports FTTH, xDSL line. (WAN)
  Note: An interface converter is separately required.
- 10/100/1000 BASE-T Ethernet ports.
- 4 [LAN] ports with a switching HUB.
- WAN Failover function.
  Dual WAN ports for fail safe configuration, maintains VPN connection if either of the two network connection is working.
  Notes:
  - This function is disabled as the default.
  - When the same network address is assigned to the WAN1 (Main line) and WAN2 (Sub line), this function doesn't properly work.
  - Icom is not responsible for any result of using this function.
- Supports SNMP.
- Access restriction with the IP Filter function.
- Automatic Restore using a USB flash drive
- Multicast packets (IPv4) will reach every other end point.
  Note: For only VE-PG2 and VE-PG3.

INTRODUCTION

DEFAULT VALUES

(As of February 2013)

Menu	Screen	Item	Item name	Value
Network Settings	IP Address	IP Address	IP Address	192.168.0.1
			Subnet Mask	255.255.255.0
	DHCP Server	DHCP Server	DHCP Server	Enable
Router Settings	WAN1/WAN2	Connection Type	Connection Type	None
	WAN Failover	WAN Failover	WAN1 Failure Detection	Disable
Management	Administrator	Administrator	Username	admin (fixed)
			Current Password	admin
	Firmware Update	Automatic Update	Automatic Update	Enable

• See Section 5 for the default values other than above.

To prevent unauthorized access:
You must be careful when choosing your password, and change it occasionally.
• Choose one that is not easy to guess.
• Use numbers, characters and letters (both lower and upper case).

INTRODUCTION

SETTING PROCEDURE

Set up the SR-VPN1 following the procedure below.

Step.1	Connect to a PC and turn ON the power	**CONNECTION GUIDE (Separated)**
Step.2	Access the setting screen	**CONNECTION GUIDE (Separated)/Section 1**
Step.3	Configure the network connection	**Section 2**
Step.4	Configure the internet connection	**Section 3**
Step.5	Configure the VPN connection using the IPsec Wizard	**Section 4**

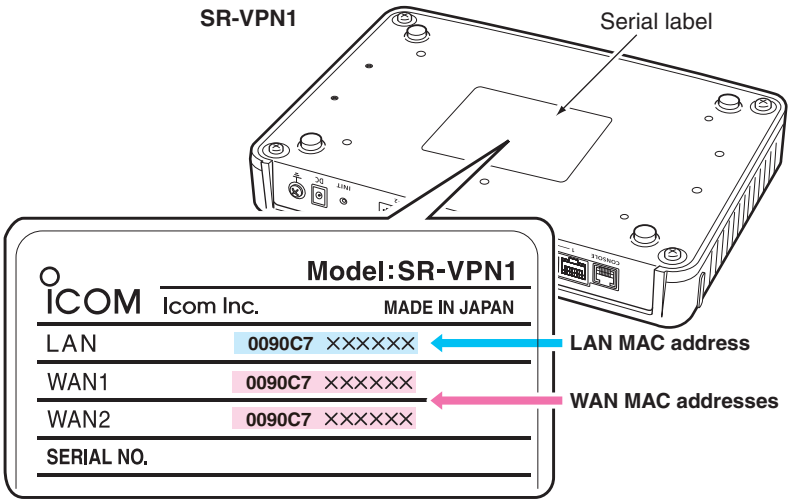
ABOUT THE MAC ADDRESS

The WAN/LAN MAC addresses are printed on the sticker on the bottom.

- MAC addresses are also displayed on the setting screen. (☞P5-5)

In the following cases, you need to know the MAC addresses

- When cloning the SR-VPN1s settings using a USB flash drive, you need to create folders whose names are each SR-VPN1's LAN MAC address. (☞P6-11)
- When your ISP requires you to register the MAC address.



(This is an example.)

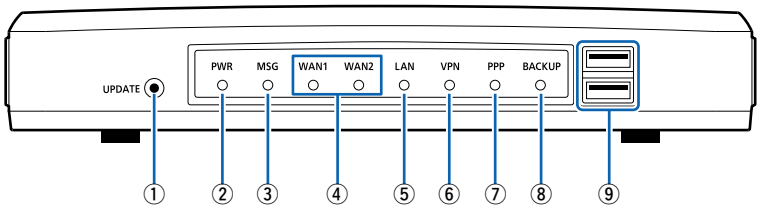
BEFORE USING THE SR-VPN1

Section 1

1. Panel description 1-2
■ Front panel 1-2
■ Rear panel 1-4
2. Feature description 1-5
■ About the Routing function 1-5
■ About the VPN function..... 1-6

1. Panel description

■Front panel



①[UPDATE] button …… When [MSG] lights green, a firmware update is ready.
To download and install the new firmware, hold down this button until [MSG] blinks.

- To use the Firmware Update function, an internet connection, DNS and default gateway settings are necessary.

②[PWR]……

Doesn't light:	Power is OFF
Lights green:	Power is ON
Lights orange:	An error has occurred or the SR-VPN1 is booting.
Blinks orange:	Initialization is in progress. (Green and Orange LEDs alternately light.)

Firmware update is in progress.

③[MSG]……

Lights green:	A firmware update is ready.
Blinks green:	Downloading new firmware.
Lights orange:	Accessing the USB flash drive.

④[WAN](1/2)……

Doesn't light: Not connected

[1000BASE-T connection]

Lights green:	Connected to the WAN
Blinks green:	The WAN line is communicating.

[10BASE-T/100BASE-TX connection]

Lights orange:	Connected to the WAN
Blinks orange:	The WAN line is communicating.

⑤[LAN] ……

Doesn't light: Not connected

[1000BASE-T connection]

Lights green: Connected to the LAN

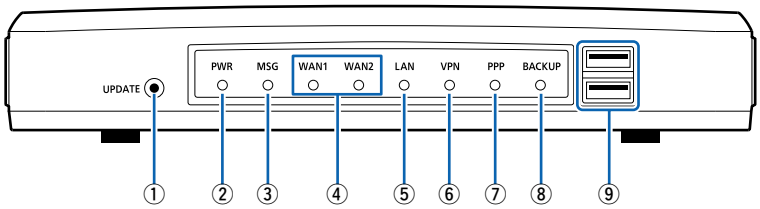
[10BASE-T/100BASE-TX connection]

Lights orange: Connected to the LAN

- You can check the communication status for each [LAN] port by the [LAN] LED on the rear panel. (☞P1-4)

1. Panel description (continued)

■ Front panel (continued)



⑥[VPN] …… Lights green: An IPsec connection is established.

⑦[PPP] …… Lights green: PPP is established.

⑧[BACKUP] …… Lights green: The backup line is communicating.

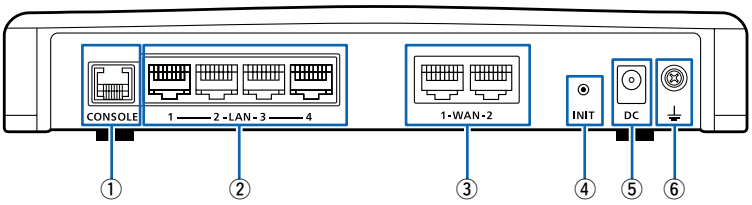
⑨[USB] ports …… (USB2.0×2) CAUTION: Turn OFF the power before inserting or removing the USB flash drive.

About the USB flash drive

- A USB flash drive such as one with biometric authentication, or one with password protection is not supported.
- Turn OFF the SR-VPN1's power before inserting or removing the USB flash drive, to prevent data corruption.
- Either one of the USB slots accepts the USB flash drive, but insert only one USB flash drive at a time.
- Insert the USB flash drive securely.
- NEVER remove the USB flash drive or turn OFF the SR-VPN1's power, while transferring data. It will cause data corruption, or damage the USB flash drive.
- After the firmware updating is finished, check the firmware version on the setting screen to verify that the update was correctly done.
- When importing setting data from the USB flash drive to the SR-VPN1, the originally programmed setting data is automatically saved as “bakdata.sav” in the USB flash drive, as a backup.

1. Panel description (continued)

■Rear panel



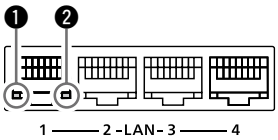
①[CONSOLE] port …… (RJ-11 type)

Connect an RS-232C serial communication interface to externally configure the SR-VPN1.
(Optional OPC-1402 is required.)

②[LAN] ports …… (RJ-45 type×4)

Connect the network devices such as a HUB.

[LED indication]



Lights: Connected to the LAN line.
Blinks: The LAN line is communicating.
❶Green: 1000BASE-T
❷Yellow: 10BASE-T/100BASE-TX

③[WAN] ports …… (RJ-45 type ×2)

The Routing function is disabled as the default.
Connect the modem (ADSL, VDSL, CATV) or ONU (Optical Network Unit) to the [WAN1] port, and then select the network line type (DHCP client/PPPoE/Static IP) as specified by your internet service provider (ISP). (☞P2-3)
• The [WAN2] port can be used as the backup line. (☞P2-9)

④[INIT] button ……

If you cannot access the setting screen, push this button to initialize the SR-VPN1.
• See the "PRECAUTIONS" leaflet for details.
• Initializing clears all the settings.

⑤DC jack ……

Connect the supplied AC adapter.

⑥Ground terminal ……

Connect to the ground.

2. Feature description

■ About the Routing function

The SR-VPN1 has a router function that allows the devices on the LAN to access the internet.

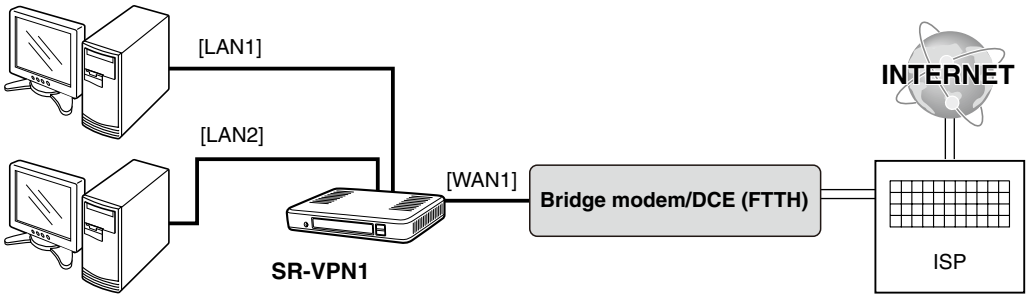
• The Routing function is disabled as the default.

• Ask your internet provider (ISP) for the network line type.

[Connecting a Bridge modem]

Connect the modem (ADSL, VDSL, CATV) or ONU (Optical Network Unit) to the [WAN1] port, and then select the network line type (DHCP client/PPPoE/Static IP) as specified by your ISP.

• The [WAN2] port can be used as the backup line. (☞P2-9)

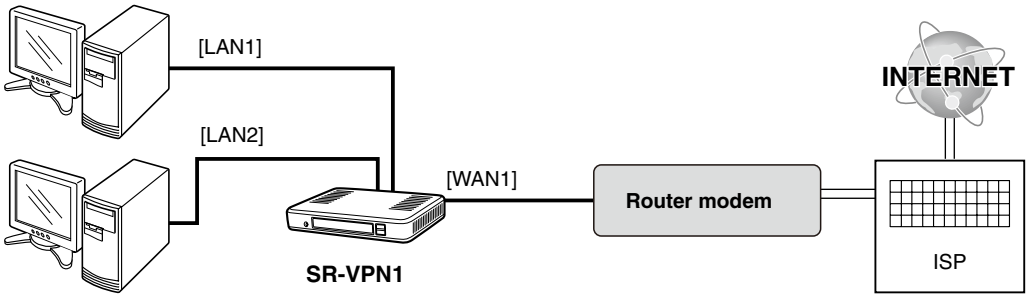


[Connecting a Router modem]

Connect the router modem to the [WAN1] port.

Select the network line type (DHCP client/PPPoE/Static IP) as specified by your ISP.

• The [WAN2] port can be used as the backup line. (☞P2-9)



NOTE

If a private WAN IP address is assigned to the SR-VPN1*, you need to use a modem which has the IPsec Pass Through function, or use the NAT Traversal function (☞P5-64).

*Example; When using a router which doesn't have the PPPoE Bridge function.

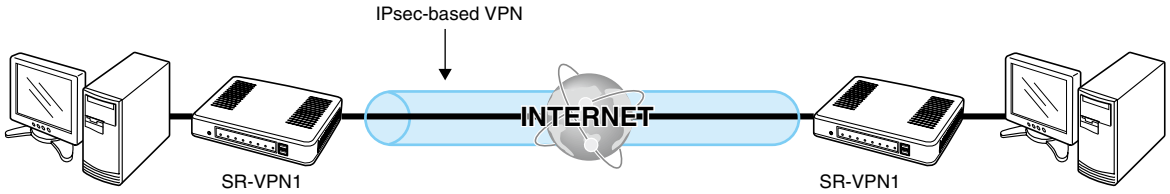
2. Feature description (continued)

■ About the VPN function

A VPN (Virtual Private Network) enables a host computer to send and receive data across shared or public networks like the Internet as if it were a private network.

You can easily configure the VPN connection using the IPsec Wizard. (☞P3-1)

- Connect the WAN line to the [WAN] port, and then configure the Router function to use the VPN function. (☞P3-3)
- You can perform further settings on the [IPsec] or [IPsec Setting Details] screen. (☞P5-51 to P5-65)



ABOUT THE INTERNET CONNECTION

Section 2

Step 1. About the ISP (Internet Service Provider) 2-2
Step 2. About the type of modem 2-2
Step 3. Selecting the internet connection method 2-3
Step 4. Connecting the modem 2-3
Step 5. Select the network line type 2-4
■ When the IP address is obtained by DHCP 2-4
■ When using a static IP address 2-5
■ When the IP address is obtained in the PPPoE method 2-7
Information About the WAN Failover function 2-9
■ About the problem detecting method 2-9

Step 1. About the ISP (Internet Service Provider)

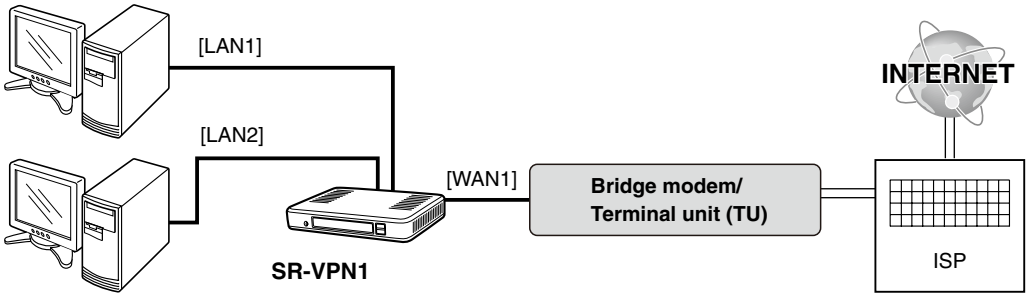
Before configuring the SR-VPN1, ask your ISP or dealer for the required equipment and network connection method.

Step 2. About the type of modem

[Connecting a Bridge modem]

Connect a Bridge modem or DCE (FTTH) to the [WAN1] port.

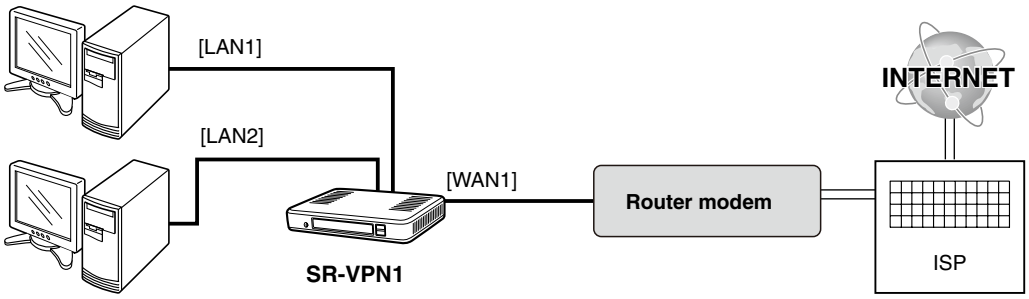
• The [WAN2] port can be used as a backup line. (☞P2-9)



[Connecting a Router modem]

Connect a Router modem to the [WAN1] port.

• The [WAN2] port can be used as a backup line. (☞P2-9)



Step 3. Selecting the internet connection method

Select the internet connection method and settings, depending on your network environment.

• The connection method may be specified by your SIP.

[The IP address is obtained by DHCP] (☞P2-4)

The WAN IP address is automatically obtained by a DHCP server.

[Using a static IP address] (☞P2-5)

The WAN IP address is specified by your ISP.

[The IP address is obtained in the PPPoE method] (☞P2-7)

The WAN IP address is specified by your ISP in the PPPoE method.

[When using a Router mode]

When the router modem's LAN IP address is the same as that of the SR-VPN1, you need to change the SR-VPN1's LAN IP address (default: 192.168.0.1). (☞P2-5)

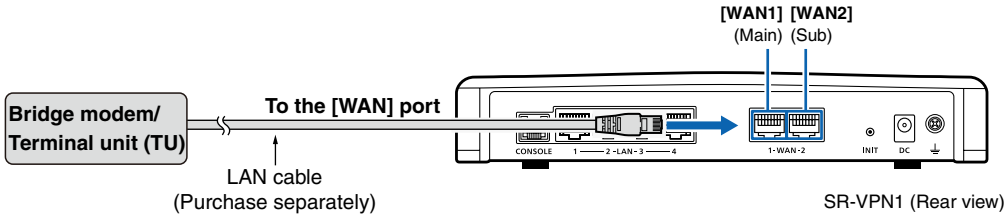
• See the modem's instruction manual for the LAN IP address.

Step 4. Connecting the modem

Connect the modem to the [WAN1] port.

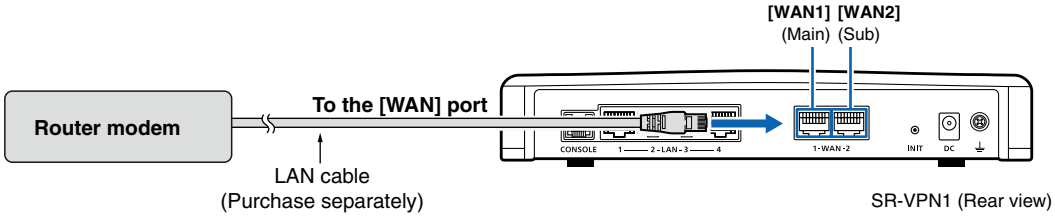
[Bridge modem]

Connect the Bridge modem or DCE (FTTH) to the [WAN1] port.



[Router modem]

Connect the Router modem to the [WAN1] port.



Step 5. Select the network line type

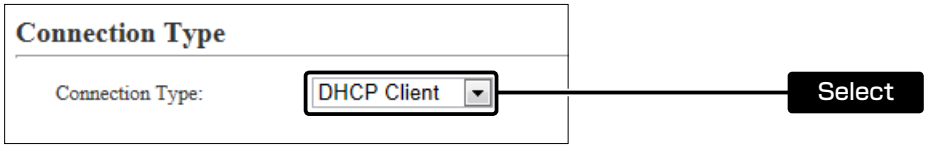
Select the network line type.

■ When the IP address is obtained by DHCP

1 Click [Router Settings], then [WAN1].

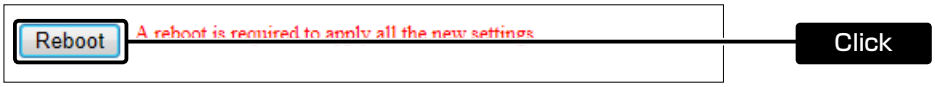
• The [WAN1] screen appears.

2 Select [DHCP Client] in the [Connection Type] item.



3 Click <Apply>.

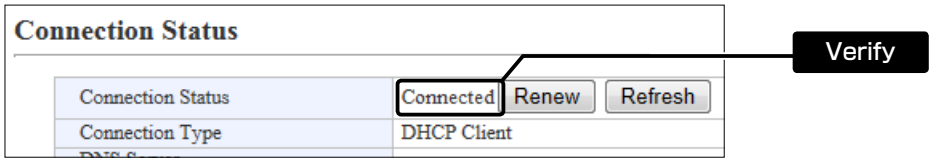
4 Click <Reboot>.



• When you are asked to reboot the SR-VPN1, follow the instructions.

5 After rebooting, verify that "Connecting" appears in the [Connection Status] item.

• Click <Refresh> to update the screen.



• If “Connected” doesn't appear, verify the setting.

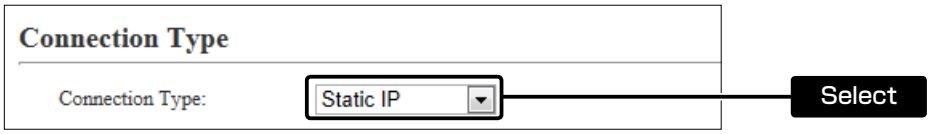
Step 5. Select the network line type (continued)

When using a static IP address

1 Click [Router Settings], then [WAN1].

• The [WAN1] screen appears.

2 Select [Static IP] in the [Connection Type] item.



3 Enter the values into the items in the [Connection Settings] field, as specified by your ISP.

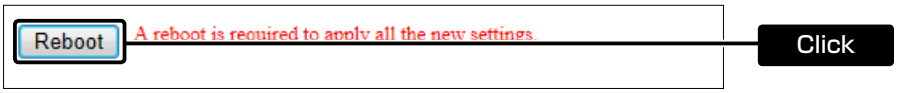
4 Click <Apply>.

(Continued on the next page.)

Step 5. Select the network line type (continued)

■ When using a static IP address (continued)

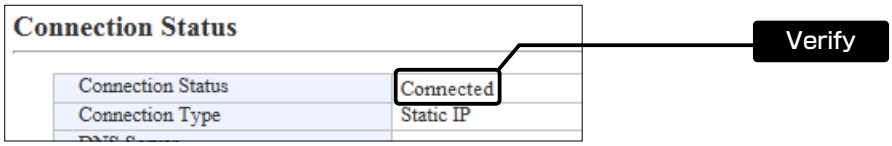
5 Click <Reboot>.



• When you are asked to reboot the SR-VPN1, follow the instructions.

6 After rebooting, verify that "Connecting" appears in the [Connection Status] item.

• Click <Refresh> to update the screen.



• If “Connected” doesn't appear, verify the setting.

Step 5. Select the network line type (continued)

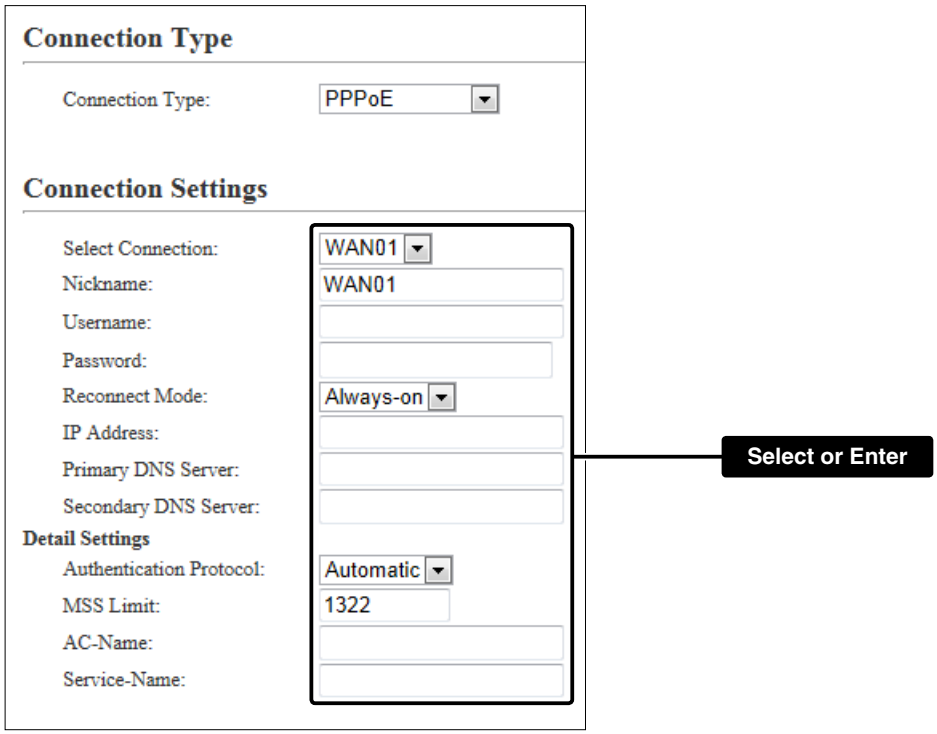
■ When the IP address is obtained in the PPPoE method

1 Click [Router Settings], then [WAN1].

• The [WAN1] screen appears.

2 Select [PPPoE] in the [Connection Type] item.

3 Select or enter the value into the items in the [Connection Settings] field.



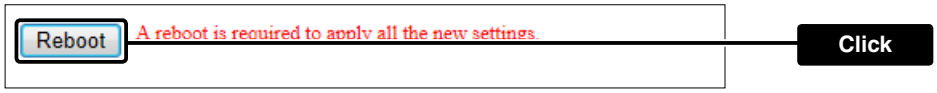
4 Click <Apply>.

(Continued on the next page.)

Step 5. Select the network line type (continued)

■When the IP address is obtained in the PPPoE method (continued)

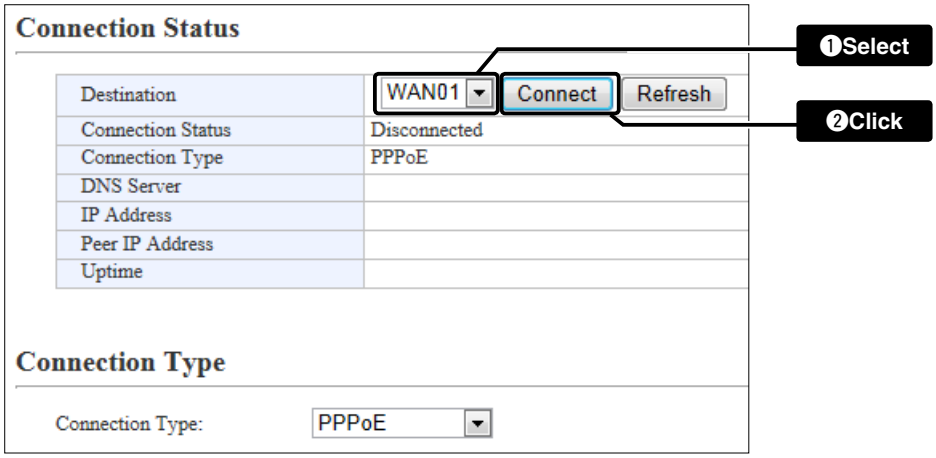
5 Click <Reboot>.



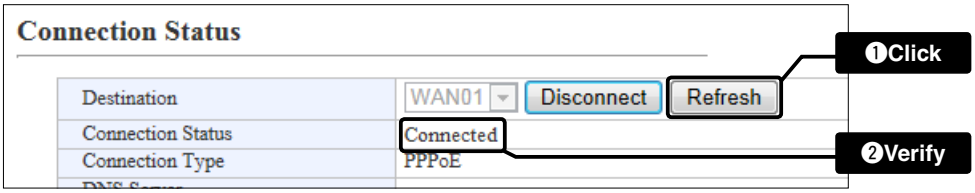
• When you are asked to reboot the SR-VPN1, follow the instructions.

6 After rebooting, select the destination and then click <Connect>.

Note: You cannot change the destination if one of the PPPoE connections is established.



7 Click <Refresh> to update the screen.



Note: If “Connected” doesn’t appear, check the entries set in Step 3.

Information About the WAN Failover function

The WAN Failover function automatically switches the default gateway port to maintain Internet connectivity.
If a connectivity failure occurs on the [WAN1] port (the main port), the WAN Failover function automatically routes all traffic through the [WAN2] (the backup port) port.

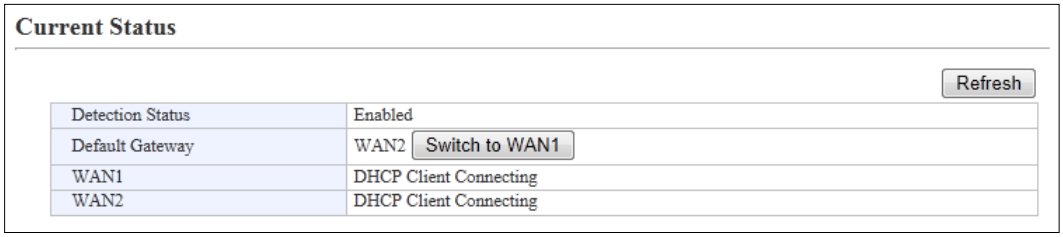
■About the problem detecting method

To use the WAN Failover function, you need to select the failure detecting method. (Default: Disabled)

①Connect the modems to the [WAN1] and [WAN2] ports. (☞2-3)
②Select the connection type for the [WAN1] and [WAN2] ports on the [WAN1/2] screen. (☞2-4)
③Click [WAN Failover] in the [Router Settings] menu.
④Select the detecting option in the [WAN Failure Detection] item, depending on your network environment. (☞5-31)

- Disable : Don't use the WAN Failover function.
- LINK Status : Detects the failure by the link status.
  The detecting method differs, depending on the connection type.
  DHCP Client: The IP address has not been obtained.
  Static IP: Connectivity of the [WAN1] port.
  PPPoE: Connectivity of the PPPoE line.
- DNS Lookup : Detects the failure by the query response from the DNS server.
  No failure is detected while either of the primary or secondary DNS server returns a query response.
- Ping : Detects the failure by the Ping response.
  - Enter the IP address to send the Ping packets to into the [Host] item.

⑤Click <Apply>.
⑥Click <Reboot>.
⑦After rebooting, you can monitor the connectivity status in the [Current Status] field.



NOTE
- When the same subnet mask is assigned to the [WAN1] and [WAN2] ports, the WAN Failover function may not properly work.
- Icom is not responsible for the result of using the WAN Failover function.

IPsec Wizard

Section 3

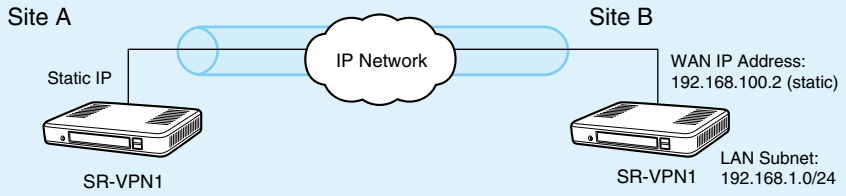
Step 1. About the network connection type 3-2
Step 2. About the setting items 3-3
Step 3. Configure the IPsec tunnel 3-4

Step 1. About the network connection type

The setting parameters differ, depending on your network environment.

Static IP–Static IP

Static WAN IP addresses are assigned to both SR-VPN1.

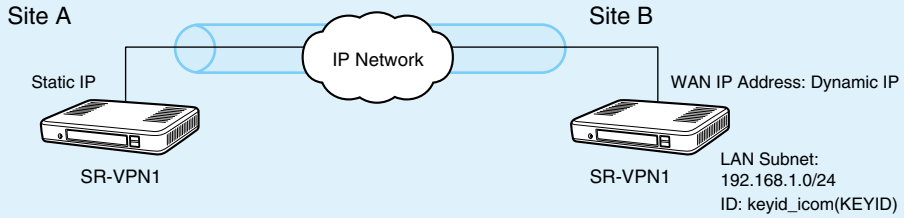


Static IP to Static IP connection

Static IP–Dynamic IP

Static WAN IP address is assigned to one SR-VPN1 (Site A).

Dynamic WAN IP address is assigned to the other SR-VPN1 (Site B).

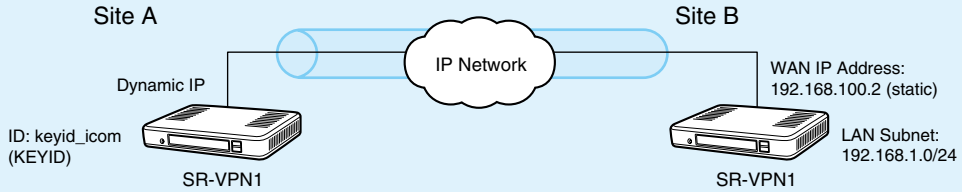


Static IP to Dynamic IP connection

Dynamic IP–Static IP

Dynamic WAN IP address is assigned to one SR-VPN1 (Site A).

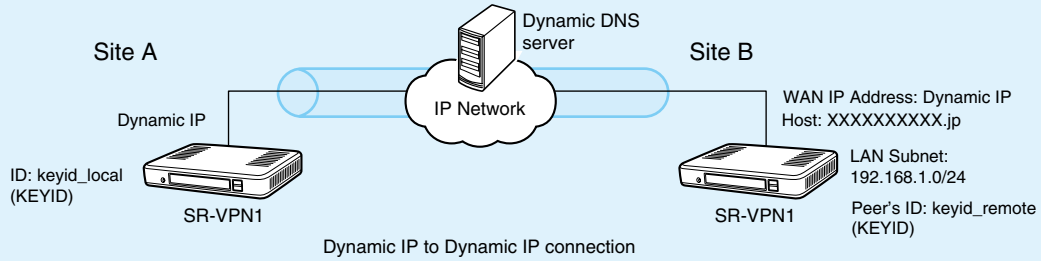
Static WAN IP address is assigned to the other SR-VPN1 (Site B).



Dynamic IP to Static IP connection

Dynamic IP–Dynamic IP

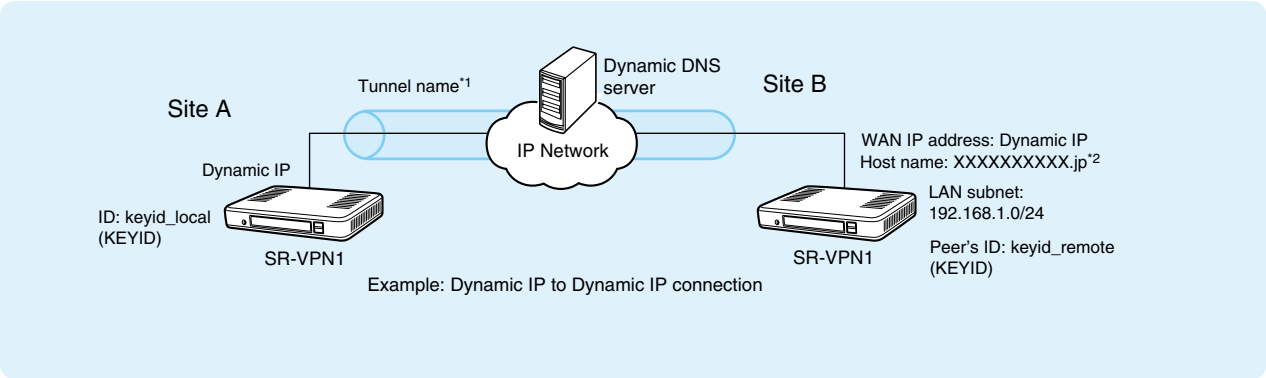
Dynamic WAN IP addresses are assigned to both SR-VPN1.



Dynamic IP to Dynamic IP connection

Step 2. About the setting items

The setting parameters differ, depending on the network connection method.



(This is an example.)

Tunnel name*1

The name of the VPN tunnel. (Up to 63 characters)

The address of the other SR-VPN1 (Site B) Except Static IP–Dynamic IP

The WAN IP address or host name*2 of the other SR-VPN1 (Site B).

Pre-Shared Key

The key which is shared with the other SR-VPN1 (Site B). (Up to 128 characters)

The LAN subnet (IP address or Subnet mask) of the other SR-VPN1 (Site B)

The LAN IP address for the network address and subnet mask of the other SR-VPN1 (Site B) .

ID Dynamic IP–Static IP Dynamic IP–Dynamic IP

Type: KEYID/FQDN/USER-FQDN String: Up to 128 characters.

The ID of the other SR-VPN1 (Site B) Static IP–Dynamic IP Dynamic IP–Dynamic IP

Type: KEYID/FQDN/USER-FQDN String: Up to 128 characters.

*1: Optional

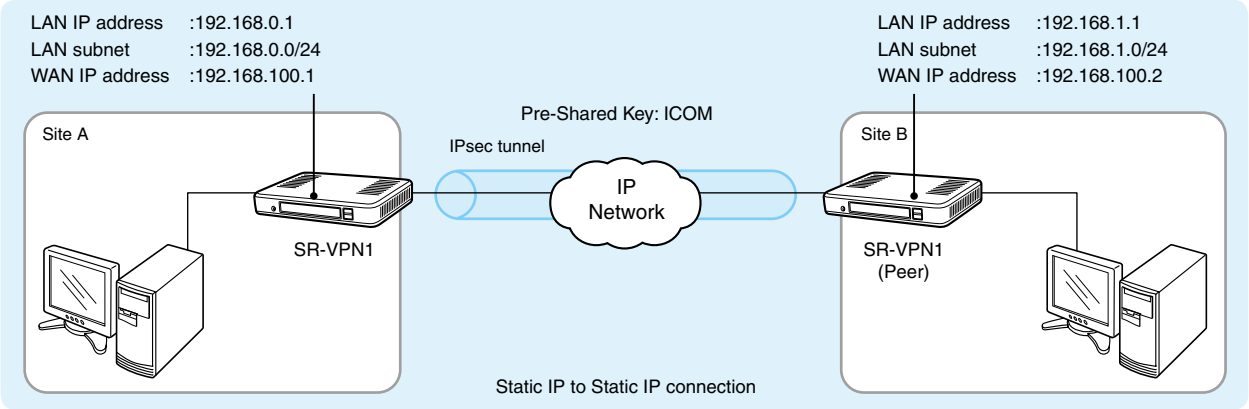
*2: When the dynamic WAN IP addresses are assigned to both SR-VPN1s, enter the host name of the other SR-VPN1 (Site B).

- One or the other SR-VPN1 needs to be registered to the dynamic DNS server and obtain the host name.
  If the SR-VPN1 (Site A) has been registered to the dynamic DNS server and is ready for the IPsec connection, leave the [Remote Address] item blank.
  If the other SR-VPN1 (Site B) has obtained a host name, enter the name into the [Remote Address] item.

Step 3. Configure the IPsec tunnel

The following procedure is an example to configure the IPsec tunnel connecting two sites (A and B), using static IP addresses.

• Configure both SR-VPN1 by following the same procedure.



(This is an example.)

NOTE

• Before configuring the IPsec tunnel, configure the Router function for the WAN in the [Router Settings] menu.

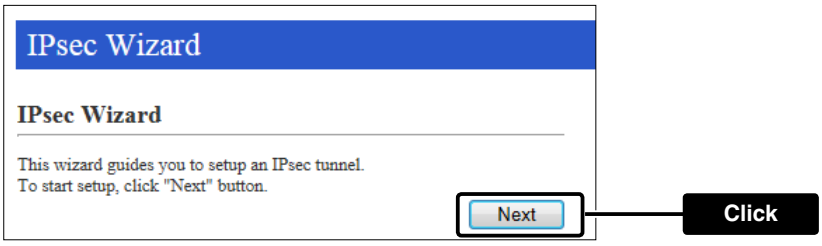
• You can use this wizard to configure the basic operation of the IPsec tunnel.
You can also perform further settings on the [IPsec] or [IPsec Setting Details] screen. (☞P5-51 to P5-65)

• Up to 32 IPsec tunnels can be created.

1 Click the [VPN Settings] menu, then [IPsec Wizard].

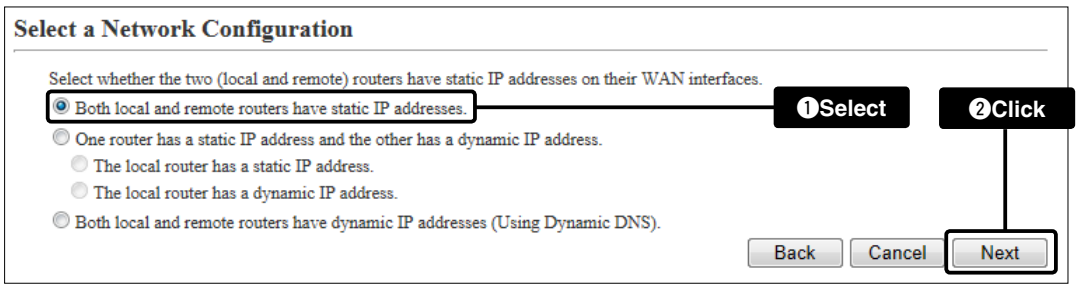
The [IPsec Wizard] screen appears.

2 Click <Next>.



• If an error message appears, check the Router function settings. See section 3 for the details.

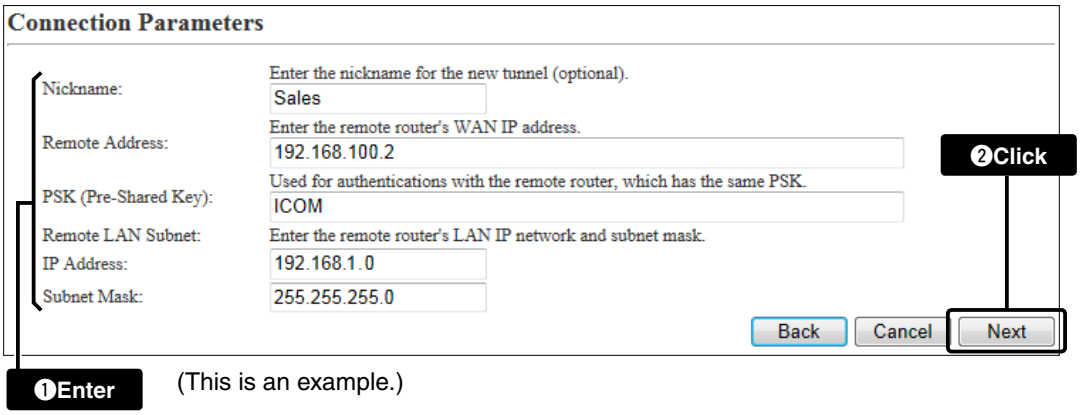
3 Select [Both local and remote routers have static IP addresses.], and then click <Next>.



(Continued on the next page.)

Step 3. Configure the IPsec tunnel (continued)

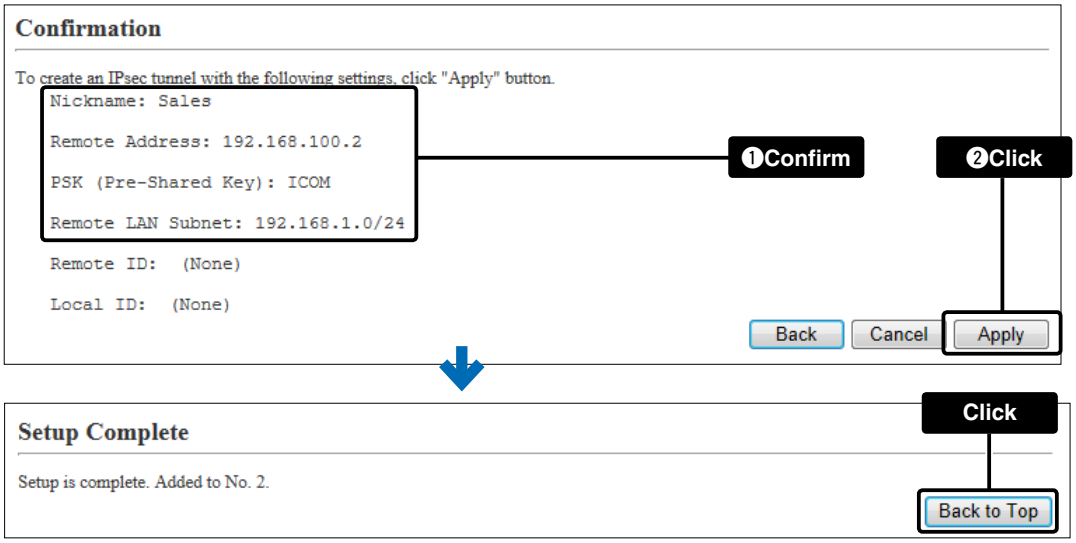
4 Enter the values, and then click <Next>.



(This is an example.)

5 Confirm the entry, and the click <Apply>.

- Click <Back> if you want to change the entry.



- If you want to create another tunnel, click <Back to Top>.
- You can monitor the status of tunnels on the [IPsec] or [IPsec Setting Details] screen. (☞P5-51 to P5-65)

OTHER BASIC FUNCTIONS

Section 4

1. How to restrict access 4-2
   Setting password 4-2
2. How to set the SR-VPN1's internal clock time 4-3
   Setting date and time (Manual setting) 4-3
   Setting date and time (Automatic setting) 4-3
3. Changing the IP Pool Start Address 4-4
   Setting example 4-4

About the DHCP server function

The SR-VPN1's DHCP server function is enabled as the default.

- Before connecting the SR-VPN1 to a network, make sure that the addresses of the devices on the network don't overlap or conflict.
  If a DHCP server is already connected to the network, and there is an address conflict, a network problem will occur. See the Troubleshooting section for possible solutions.

About the HUB

100BASE-TX or faster is recommended.

1. How to restrict access

If you set a new administrator password, you can restrict access to the SR-VPN1's setting screen.
The default administrator password is "admin."

Setting password

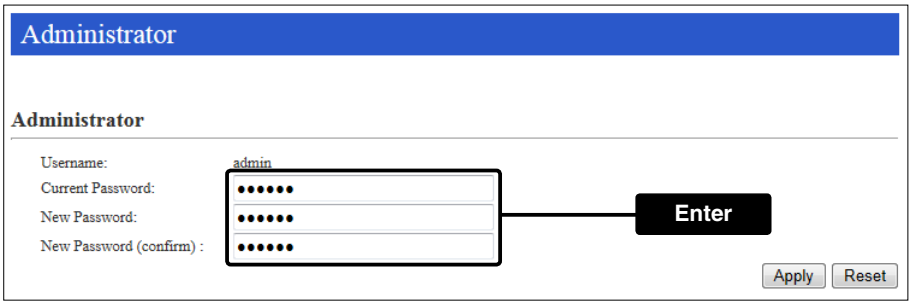
1 Click the [Management] menu, then [Administrator].

• The [Administrator] screen appears.

2 Enter [Current Password], [New Password] and [New Password (confirm)] in their respective input fields.

• The password can be composed of up to 31 characters (0–9, a–z and A–Z).

• The entered characters are displayed as an * (asterisk) or a • (dot).



3 Click <Apply>.

To prevent unauthorized access

You must be careful when choosing your password, and change it occasionally.

• Choose one that is not easy to guess.

• Use numbers, characters and letters (both lower and upper case).

2. How to set the SR-VPN1's internal clock time

You can set the SR-VPN1's internal clock time.

Setting date and time (Manual setting)

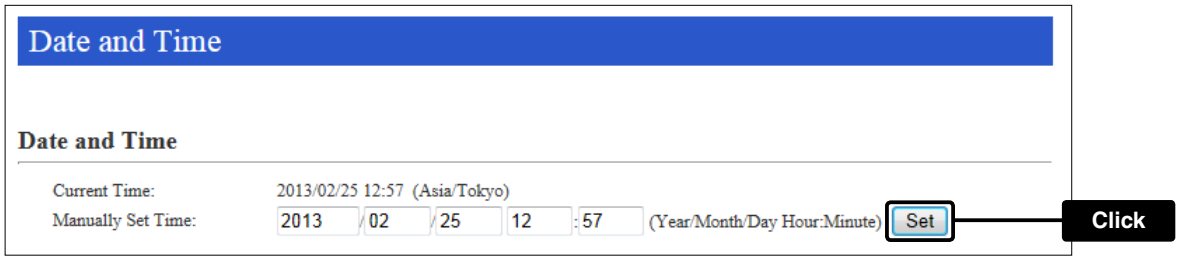
1 Click the [Management] menu, then [Date and Time].

• The [Date and Time] screen appears.

2 The current time is displayed in [Date and Time].

Click <Apply> to synchronize the internal clock with the current time.

• You can also enter the time in the [Manually Set Time] item.



Setting date and time (Automatic setting)

The Automatic Clock Synchronize function automatically synchronizes the internal clock with the time management server (NTP).

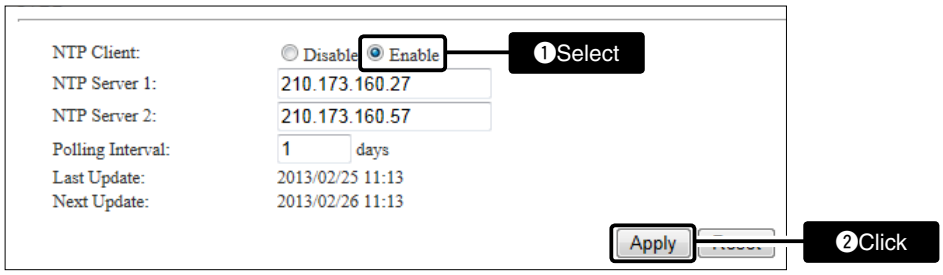
• To use this function, an internet connection and default gateway settings are necessary.

1 Click the [Management] menu, then [Date and Time].

• The [Date and Time] screen appears.

2 Select the appropriate Time Zone.

3 Select "Enable," and then click <Apply>.



Note: The default NTP servers are provided by INTERNET MULTIFEED Co.

3. Changing the IP Pool Start Address

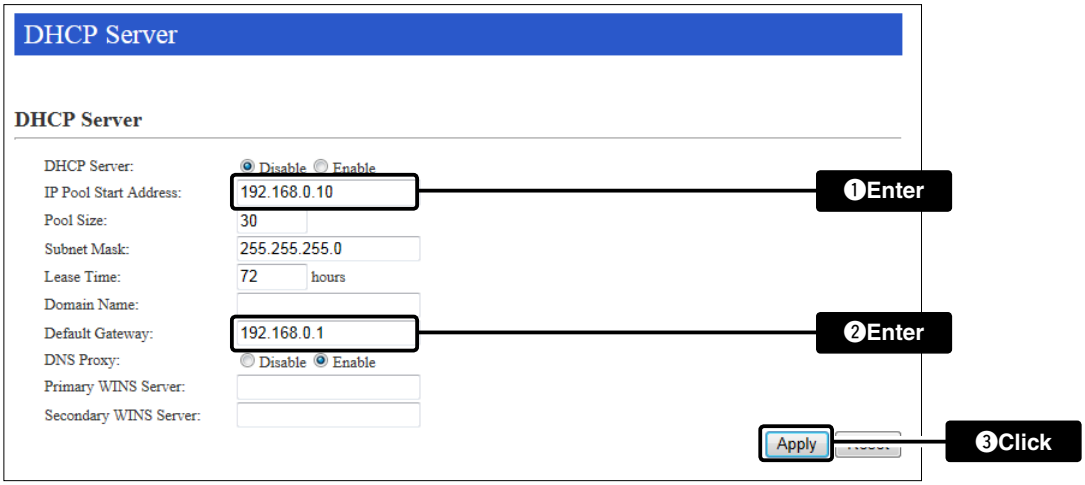
You can change the IP pool start address by following the procedure below.

Setting example

1 Click the [Network Settings] menu, then [DHCP Server].

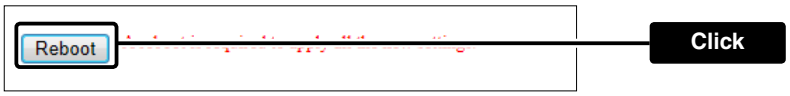
• The [DHCP Server] screen appears.

2 Enter the new IP pool start address and default gateway, and then click <Apply>.



3 Click <Reboot>.

• When you are asked to reboot the SR-VPN1, follow the instructions.



About the DHCP server function

The SR-VPN1's DHCP server function is enabled as the default.

• Before connecting the SR-VPN1 to a network, make sure that the addresses of the devices on the network don't overlap or conflict.
  If a DHCP server is already connected to the network, and there is an address conflict, a network problem will occur. See the Troubleshooting section for possible solutions.

About the maximum number of the IP addresses

Up to 128 addresses can be automatically assigned by the DHCP server function.
Another 32 addresses can be manually assigned.

ABOUT THE SETTING SCREEN

Section 5

1. About the setting screen 5-4
2. [TOP] Menu 5-5
   - System Status 5-5
   - Network Status 5-5
   - Port Status 5-6
3. [Information] Menu 5-7
   - SYSLOG 5-7
   - IPsec Status 5-8
   - IPsec Status 5-9
   - IPsec Route Status 5-10
   - Memory Usage 5-11
   - Traffic Statistics 5-12
4. [Network Settings] Menu 5-14
   - Host Name 5-14
   - IP Address 5-15
   - DHCP Server 5-16
   - Static DHCP 5-18
   - Static DHCP Table 5-18
   - Routing Table 5-19
   - Static Routing 5-20
   - List of Static Routing Entries 5-20

(Continued on the next page.)

About the connection type

Some items differ, depending on the connection type selected in the [Connection Type] item.

DHCP Client appears when [DHCP Client] is selected.

Static IP appears when [Static IP] is selected.

PPPoE appears when [PPPoE] is selected.

(Continued from the previous page)

5. [Router Settings] Menu 5-21
- Connection Status DHCP Client 5-21
- Connection Status Static IP 5-22
- Connection Status PPPoE 5-23
- Connection Type 5-24
- Connection Settings DHCP Client 5-25
- Connection Settings Static IP 5-26
- Connection Settings PPPoE 5-27
- List of Connection Settings 5-30
- WAN Failover 5-31
- Current Status 5-33
- NAT 5-34
- DMZ Host 5-34
- Port Forwarding 5-35
- List of Port Forwarding Entries 5-35
- IP Filter Setting 5-36
- List of IP Filter Entries 5-45
- Dynamic DNS 5-46
- Dynamic DNS Updates 5-48

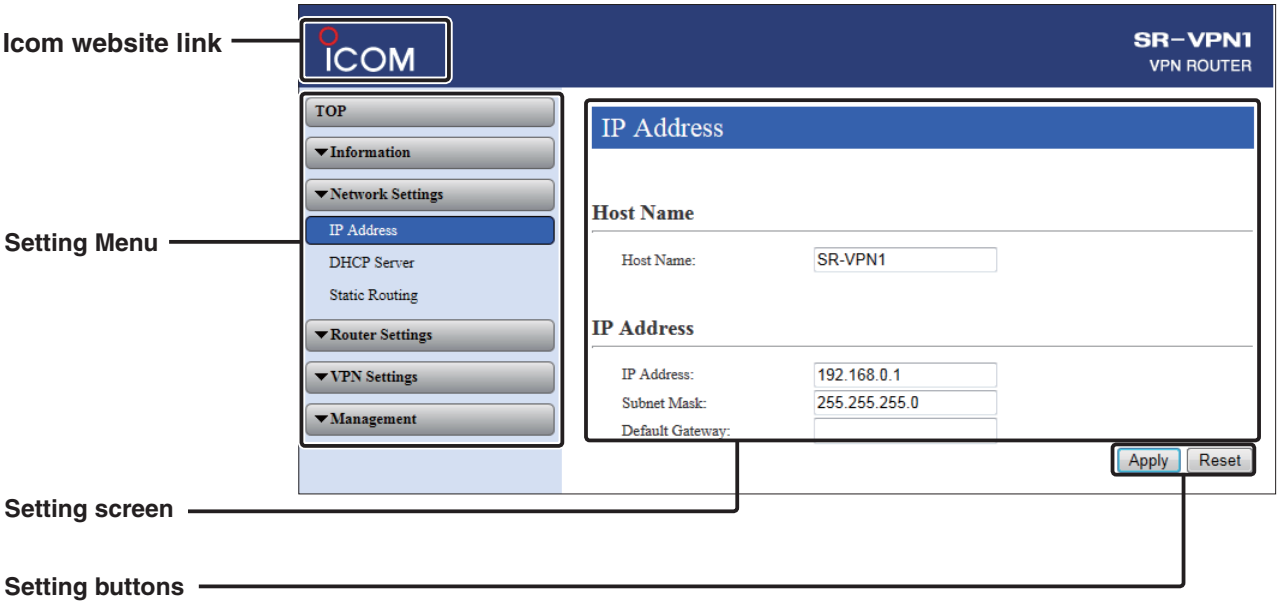
6. [VPN Settings] Menu 5-49
- IPsec Wizard 5-49
- IPsec Common Settings 5-50
- Tunnel 5-51
- Routes 5-53
- List of IPsec Settings 5-54
- IPsec (Detail) 5-56
- About the IKE version 5-64
- List of IPsec Settings 5-65
- Multicast 5-66
- Setting example 5-68
- Status Client 5-69
- Status Server 5-70

(Continued on the next page.)

(Continued from the previous page)

7. [Management] Menu 5-71
- Administrator 5-71
- USB 5-72
- HTTP/HTTPS 5-73
- Telnet/SSH 5-74
- SSH Public Key Management 5-75
- SSH Public Key Registration Status 5-75
- Date and Time 5-76
- Time Zone 5-77
- NTP 5-78
- SYSLOG 5-79
- SNMP 5-80
- Ping Test 5-83
- Traceroute Test 5-84
- Reboot 5-85
- Backup Settings 5-86
- Restore Settings 5-86
- List of Settings 5-87
- Factory Defaults 5-88
- Firmware Status 5-89
- Online Update 5-90
- Automatic Update 5-91
- Manual Update 5-91

1. About the setting screen



Link to the Icom website

Click the Icom logo to open the Icom website if your PC is connected to the Internet.

Setting menu

Displays the screen name list on the menu line. When you click the menu title, a list of items drops down which you can use to select the desired setting item.

Setting screen

Displays the settings and values when you click the screen name.

Setting buttons

Save or cancel setting values.

If “A reboot is required to apply all the new settings.” is displayed on the screen when you click the [Apply] button, click the [OK] button.

The SR-VPN1 reboots, and the setting items and values are updated.

The following message is displayed on the screen while the SR-VPN1 is rebooting.

Now rebooting.

Wait XX seconds for startup.

If this page doesn’t automatically refresh after rebooting, click [Back].

- If the setting screen does not automatically return, click [Back] in about 30 seconds after the “Now rebooting.” message appears.
- Items and buttons may differ, depending on the settings.

2. [TOP] Menu [TOP]

System Status

Displays the firmware version and MAC addresses (WAN/LAN).

System Status

Host Name	SR-VPN1
IPL	[redacted]
Version	Ver. [redacted] Copyright 2007-2012 Icom Inc.
WAN1 MAC Address	00- [redacted]
WAN2 MAC Address	00- [redacted]
LAN MAC Address	00- [redacted]

(This is an example.)

• The MAC addresses are also printed on the label on the bottom of the SR-VPN1.

Network Status

Displays the network information such as IP addresses (WAN/LAN).

Network Status

WAN1 Mode	No Connection
WAN1 Status	-
WAN2 Mode	No Connection
WAN2 Status	-
LAN IP Address	[redacted]
DHCP Server	Disabled

(This is an example.)

2. [TOP] Menu (continued) [TOP]

Port Status

Displays the communication rate and mode for each port (WAN/LAN).

Port Status

WAN1	Disconnected
WAN2	Disconnected
LAN1	Disconnected
LAN2	Disconnected
LAN3	Disconnected
LAN4	1000BASE-T full-duplex

(This is an example.)

NOTES

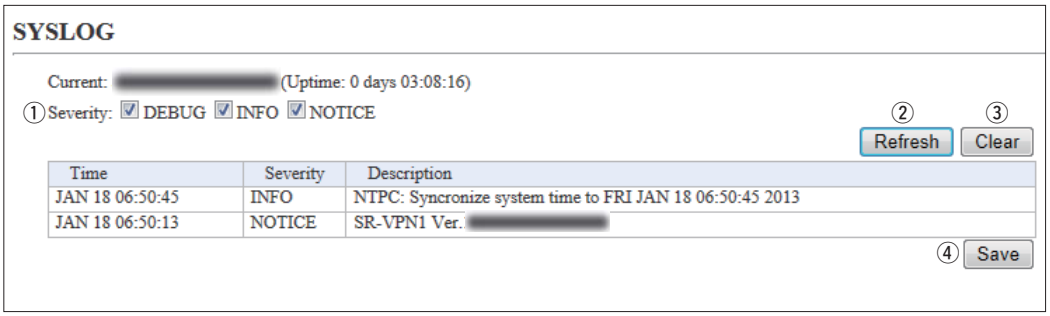
- The SR-VPN1's [LAN] and [WAN] ports are auto-negotiation enabled and can automatically select the optimal speed and duplex mode if the peer devices are auto-negotiation enabled as well.
- We recommend to always enable auto-negotiation on the peer devices. If a peer device is fixed to full-duplex mode, auto-negotiation enabled devices (including the SR-VPN1) may generally take it for half-duplex mode and cannot communicate properly.

3. [Information] Menu

[Information]–[SYSLOG]

■SYSLOG

Displays the log information. The latest 500 log entries are displayed.



(This is an example.)

①**Severity**..... Select the log information to display.
- Enter a check mark to display the log entries.
- Remove the check mark and click <Refresh> to hide the entries.

(Default: ☑ DEBUG ☑ INFO ☑ NOTICE)

Note: The selection is not stored, and reset when you leave this screen.

②**<Refresh>**..... Click to refresh the log screen.

③**<Clear>** ..... Click to delete all log entries.

Note: All log entries are also deleted when the SR-VPN1 is turned OFF or initialized.

④**<Save>** ..... Click to save the log to a PC with a text file (extension: “txt”).
- Click this button, and then select a folder to save the file.

3. [Information] Menu (continued)

[Information]–[VPN Status]

■IPsec Status

Displays the IPsec tunnel status.

IPsec Status

①

Refresh

② No.	③ Name	④ Status	⑤ Remote ID	⑥ Local ID	⑦
1	Icom	Constructing	None	None	Details

(This is an example.)

①**<Refresh>**..... Click to refresh the status screen.

②**No.** ..... The tunnel number.

③**Name** ..... The tunnel name.

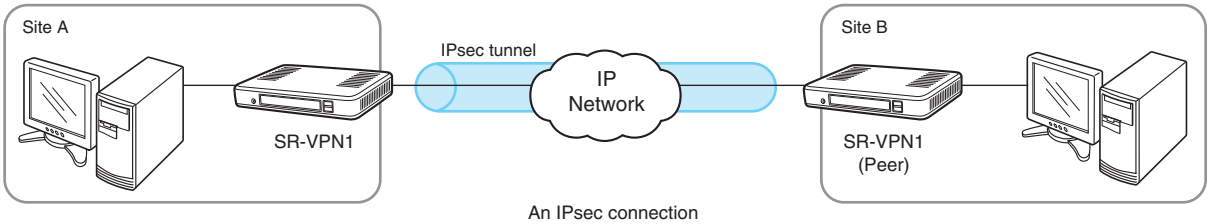
④**Status** ..... The tunnel status.

- **Connected**
  Connected.
- **Waiting**
  Connection ready.
- **Constructing**
  Connection in progress.
- **Disconnected/Down**
  Disconnected.
- **IPsec Disabled**
  The SR-VPN1's IPsec function is disabled.

⑤**Remote ID** ..... The ID of the SR-VPN1 (Site B in the illustration below).

⑥**Local ID**..... The ID of the SR-VPN1 (Site A in the illustration below).

⑦**<Detail>**..... Click to open the tunnel details window. (☞P5-9)



An IPsec connection

3. [Information] Menu (continued)

[Information]–[VPN Status]

■IPsec Status

Displays the details of each IPsec tunnel.

IPsec Status (Detail)

① Uptime:
② Session:
③ IKE Version:
④ Local IP Address:
⑤ Remote IP Address:
Phase1 (ISAKMP SA)
⑥ Integrity Algorithm:
⑦ Encryption Algorithm:
⑧ DH Group:
Phase2 (IPsec SA)
⑥ Integrity Algorithm:
⑦ Encryption Algorithm:

(This is an example.)

①Uptime ..... The elapse time (in second) from the time when the connection has been made.

②Session..... The operation mode of the IPsec IKE.

- **Initiator**
  The SR-VPN1 is the Initiator.
- **Responder**
  The SR-VPN1 is the Responder.

③IKE Version ..... The version of the IKE used for the tunnel.

④Local IP Address ..... The WAN IP address of the SR-VPN1 (Site A in the illustration below).

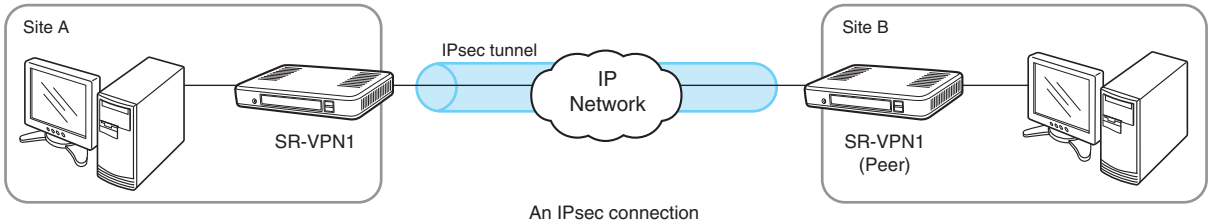
⑤Local IP Address ..... The WAN IP address of the SR-VPN1 (Site B in the illustration below).

Phase1 (ISAKMP SA)/Phase2 (IPsec SA)

⑥Integrity Algorithm ..... The authentication algorithm used for the IKE phase 1/2.

⑦Encryption Algorithm ... The encryption algorithm used for the IKE phase 1/2.

⑧DH Group ..... The DH group used for the IKE phase 1.



An IPsec connection

3. [Information] Menu (continued)

[Information]–[VPN Status]

■IPsec Route Status

Displays the IPsec routing status.

IPsec Route Status

① Destination	② Subnet Mask	③ Route
192.168.1.0	255.255.255.0	No.1

(This is an example.)

①**Destination** ..... The network address of the route's destination network.

②**Subnet Mask** ..... The subnet mask of the route's destination network.

③**Route**..... The tunnel number of the route.

3. [Information] Menu (continued)

[Information]–[Statistics]

■Memory Usage

Display a statistical graph of the memory usage.

• These setting items are reset when you leave this screen.

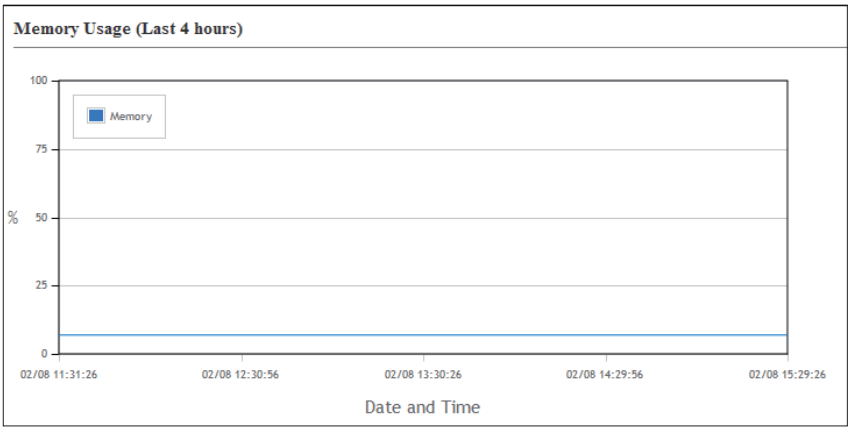
①Plot Interval ..... Select the plot interval. (Default: 2 minutes)

②Refresh Automatically ... Select "Enable" to periodcally refresh the graph. (Default: Enable)

• The graph is refreshed according to the set interval in [Plot Interval] (①).

③<Open> ..... Click to open the memory usage graph window.

• The X axis represents the date and time, and the Y axis represents the usage (%).



(This is an example.)

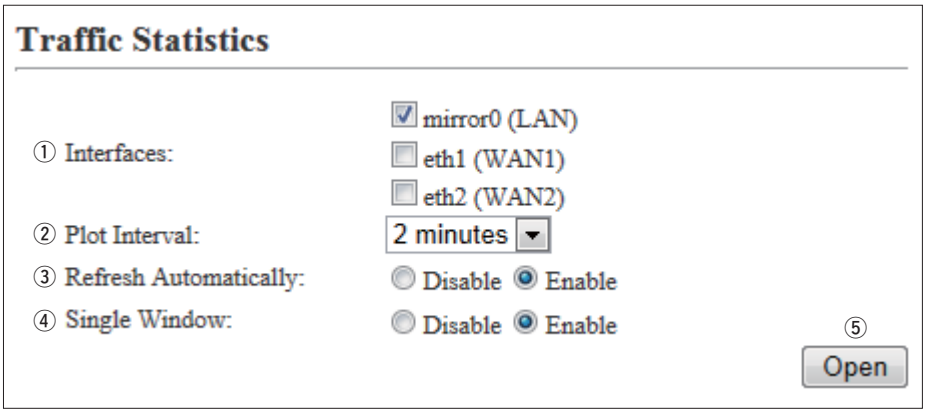
3. [Information] Menu (continued)

[Information]–[Statistics]

■Traffic Statistics

Displays the traffic graph for each port (WAN/LAN).

• These setting items are reset when you leave this screen.



①Interfaces ..... Select the interface to display the graph.

• Enter a check mark to display a graph.

• Remove the check mark to hide the graph.

(Default: ☑ mirror0(LAN) ☐ eth1(WAN1) ☐ eth2(WAN2))

②Plot Interval ..... Select the plot interval. (Default: 2 minutes)

③Refresh Automatically ... Select "Enable" to periodically refresh the graph. (Default: Enable)

• The graph is refreshed according to the set interval in [Plot Interval] (②).

④Single Window ..... Select "Enable" to display all graphs on the same window.

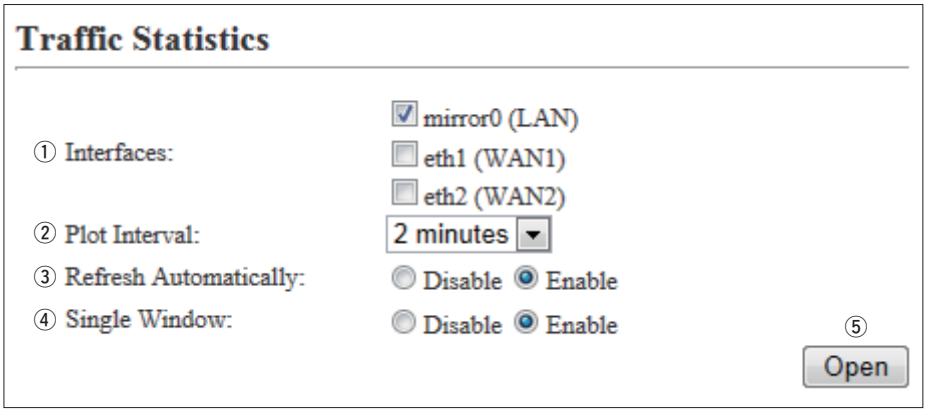
(Default: Enable)

• When “Disable” is selected, the graphs are separately displayed in the different windows.

3. [Information] Menu

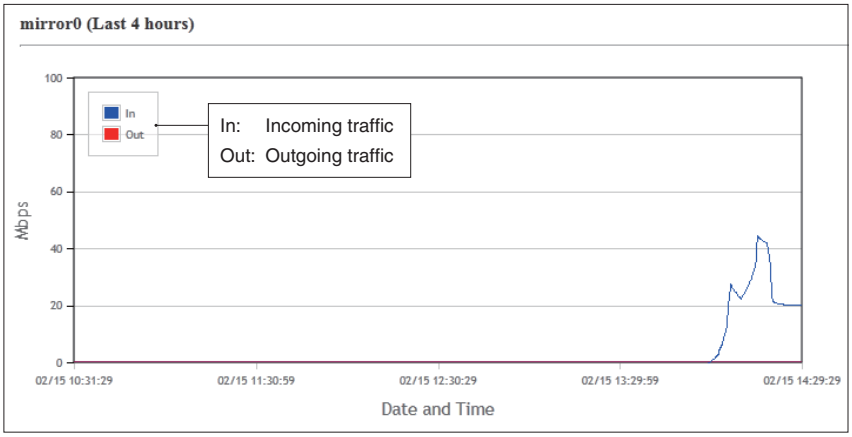
[Information]–[Statistics]

■Traffic Statistics (continued)



⑤**<Open>** ..... Click to open the traffic graph window.

- The X axis represents the date and time, and the Y axis represents the usage (%).



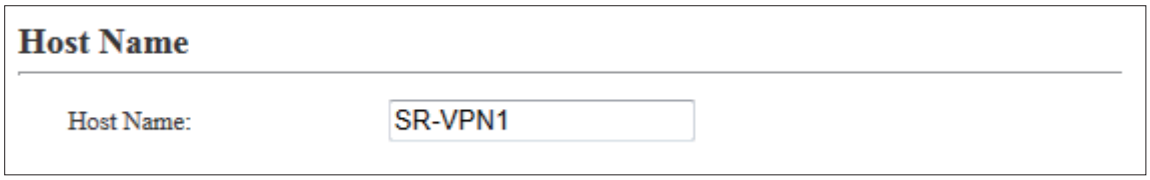
(This is an example.)

4. [Network Settings] Menu

[Network Settings]–[IP Address]

■Host Name

Enter the host name.



Host Name ..... Enter the host name. (Up to 31 characters) (Default: SR-VPN1)

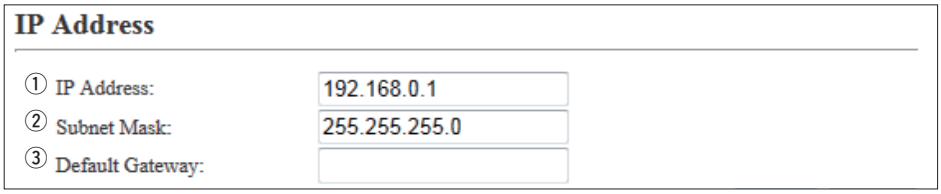
Note: The name must start with an alphanumeric character, and must NOT start or end with a "–."

4. [Network Settings] Menu (continued)

[Network Settings]–[IP Address]

■IP Address

Enter the SR-VPN1's IP Address.



①IP Address ..... Enter the LAN IP address according to your network environment.
(Default: 192.168.0.1)

Note: When using the DHCP Server function, the network part of the IP address must be the same as that set in the [IP Pool Start Address] item in the [DHCP Server] menu. (☞P5-16)

②Subnet Mask ..... Enter the subnet mask according to your network environment.
(Default: 255.255.255.0)

③Default Gateway ..... If a default gateway device (such as a router) is connected to the LAN port, enter the device's IP address.

- If the default gateway is set to the LAN side, the network route is on the WAN side when the default gateway is set to the WAN side.

4. [Network Settings] Menu (continued)

[Network Settings]–[DHCP Server]

■DHCP Server

Configure the DHCP Server function.

DHCP Server

① DHCP Server:	◉ Disable ○ Enable
② IP Pool Start Address:	192.168.0.10
③ Pool Size:	30
④ Subnet Mask:	255.255.255.0
⑤ Lease Time:	72 hours
⑥ Domain Name:	
⑦ Default Gateway:	192.168.0.1
⑧ DNS Proxy:	○ Disable ◉ Enable
⑨ Primary WINS Server:	
⑩ Secondary WINS Server:	

①DHCP Server ..... Select “Enable” to use the DHCP Server function. (Default: Enable)

②IP Pool Start Address ... Enter the IP pool start address. (Default: 192.168.0.10)

③Pool Size ..... Enter the size of IP pool. (Default: 30)

Note: Up to 128 addresses can be automatically assigned by the DHCP server function. Another 32 addresses can be manually assigned.

④Subnet Mask ..... Enter the subnet mask for the IP pool start address set in the [IP Pool Start Address] item (②). (Default: 255.255.255.0)

⑤Lease Time ..... Enter the lease time period. (Default: 72)

- Range: 1–9999 (hours)

⑥Domain Name ..... Enter the network address domain name. (Up to 127 characters)

4. [Network Settings] Menu

■ DHCP Server (continued)

DHCP Server

① DHCP Server:	◉ Disable ○ Enable
② IP Pool Start Address:	192.168.0.10
③ Pool Size:	30
④ Subnet Mask:	255.255.255.0
⑤ Lease Time:	72 hours
⑥ Domain Name:	
⑦ Default Gateway:	192.168.0.1
⑧ DNS Proxy:	○ Disable ◉ Enable
⑨ Primary WINS Server:	
⑩ Secondary WINS Server:	

⑦Default Gateway ..... Enter the default gateway IP address.

⑧DNS Proxy ..... Select “Enable” to use the DNS Proxy function. (Default: Enable)
When “Enable” is selected, you don’t need to change the DHCP clients’ setting even when the DNS server address has changed.

⑨Primary WINS Server ... Enter the WINS server’s primary address.

⑩Secondary WINS Server Enter the WINS server’s secondary address.

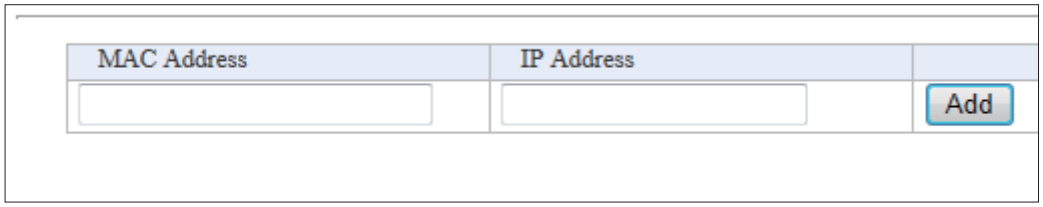
4. [Network Settings] Menu (continued)

[Network Settings]–[DHCP Server]

■Static DHCP

Enter MAC and static IP addresses to the DHCP server.

• You can enter up to 32 entries.

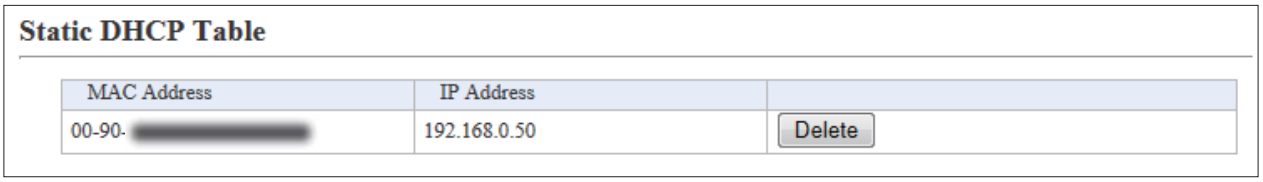


Static DHCP ..... Enter the MAC and IP addresses, and then click <Add>.

Note: Make sure that the addresses of the devices on the network don't overlap or conflict. If a DHCP server is already connected to the network, and there is an address conflict, a network problem will occur. See the Troubleshooting section for possible solutions.

■Static DHCP Table

Displays the static DHCP entries.



(This is an example.)

<Delete> ..... Click <Delete> to remove the entry.

4. [Network Settings] Menu (continued)

[Network Settings]–[Static Routing]

■Routing Table

Displays the routing information.

Routing Table

① Destination	② Subnet Mask	③ Gateway	④ Interface	⑤ Owner
127.0.0.1	255.255.255.255	127.0.0.1	lo0	host
192.168.0.0	255.255.255.0	192.168.0.1	mirror0	misc
192.168.0.1	255.255.255.255	192.168.0.1	lo0	host

①**Destination** ..... The network address of the route's destination network.

②**Subnet Mask** ..... The subnet mask of the route's destination network.

③**Gateway** ..... The route's gateway address.

④**Interface** ..... The routing interface.

- **lo0:** Loop back interface
- **eth1:** Static IP or DHCP client (WAN1)
- **eth2:** Static IP or DHCP client (WAN2)
- **pppoe0:** PPPoE (WAN1)
- **pppoe1:** PPPoE (WAN2)
- **mirror0:** LAN

⑤**Owner** ..... The type of routing path.

- **static:** Static route
- **misc:** Broadcast frame
- **host:** Host route

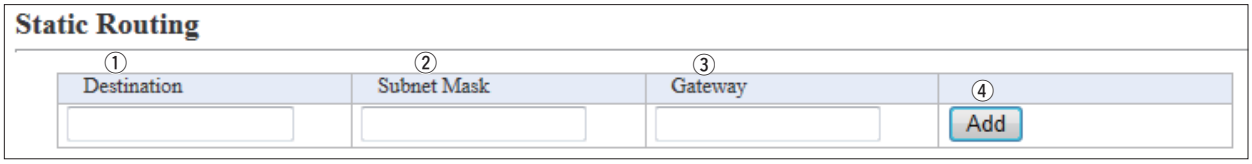
4. [Network Settings] Menu (continued)

[Network Settings]–[Static Routing]

■Static Routing

Enter the static routing destinations.

• You can enter up to 32 entries.



(This is an example.)

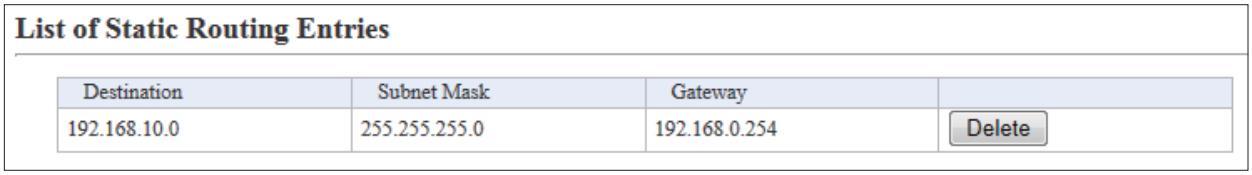
①**Destination** ..... The network address of the route's destination network.

②**Subnet Mask** ..... The subnet mask of the route's destination network.

③**Gateway** ..... The route's gateway address.

④**<Add>** ..... Click to add the entry.

■List of Static Routing Entries



(This is an example.)

<Delete> ..... Click <Delete> to remove the entry.

5. [Router Settings] Menu

[Router Settings]–[WAN1/WAN2]

■Connection Status DHCP Client

Displays the WAN connection status.

Connection Status

①Connection Status	Connecting Renew Refresh
②Connection Type	DHCP Client
③DNS Server	
④IP Address	
⑤Peer IP Address	
⑥Uptime	

①**Connection Status**..... Displays the WAN connection status.

<Renew>

Click to connect to the network.

<Refresh>

Click to refresh the screen.

②**Connection Type** ..... Displays the WAN connection type.

③**DNS Server** ..... Displays the DNS server's IP address.

④**IP Address** ..... Displays the SR-VPN1's WAN IP address.

⑤**Peer IP Address** ..... Displays the gateway IP address obtained by the DHCP.

⑥**Uptime** ..... Displays the elapsed time the SR-VPN1 has been connected to the network.

• Click <Refresh> to refresh.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN1/WAN2]

■Connection Status Static IP

Displays the WAN connection status.

Connection Status

① Connection Status	Disconnected
② Connection Type	Static IP
③ DNS Server	
④ IP Address	
⑤ Peer IP Address	
⑥ Uptime	

①**Connection Status**..... Displays the WAN connection status.

②**Connection Type** ..... Displays the WAN connection type.

③**DNS Server** ..... Displays the DNS server's IP address.

④**IP Address** ..... Displays the SR-VPN1's WAN IP address.

⑤**Peer IP Address** ..... Displays the gateway IP address which is manually set.

⑥**Uptime** ..... Displays the elapsed time the SR-VPN1 has been connected to the network.
• Click <Refresh> to refresh.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN1/WAN2]

■Connection Status PPPoE

Displays the WAN connection status.

Connection Status

① Destination	WAN01 Connect Refresh
② Connection Status	Disconnected
③ Connection Type	PPPoE
④ DNS Server	
⑤ IP Address	
⑥ Peer IP Address	
⑦ Uptime	

①**Destination** ..... Select the WAN connection to display the connection status.

<Connect>/<Disconnect>

Click to connect or disconnect the selected WAN port.

<Refresh>

Click to refresh the status.

②**Connection Status**..... Displays the connection status. ([Disconnected], [Connecting] or [Connected])

③**Connection Type** ..... Displays the WAN connection type.

④**DNS Server** ..... Displays the DNS server's IP address.

⑤**IP Address** ..... Displays the SR-VPN1's WAN IP address.

⑥**Peer IP Address** ..... Displays the IP address specified by your service provider.

⑦**Uptime** ..... Displays the elapsed time the SR-VPN1 has been connected to the network.

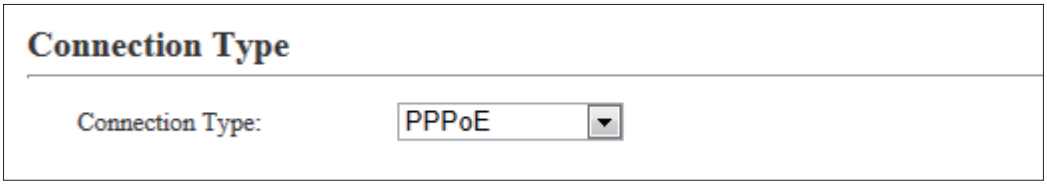
• Click <Refresh> to refresh.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN1/WAN2]

■Connection Type

Select the WAN connection type.



Connection Type ..... Select the WAN connection type as specified by your ISP.

(Default: No Connection)

- "No Connection"
  Select this when the WAN port is not connected to the network.

- "DHCP Client"
  The WAN IP address is automatically obtained by a DHCP server.

- "Static IP"
  The WAN IP address is specified by your ISP.

- "PPPoE"
  The WAN IP address is specified by your ISP in the PPPoE method.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN1/WAN2]

■Connection Settings DHCP Client

Configure the WAN connection.

①**Nickname** ..... Enter the name of the connection. (Up to 31 characters)

②**Primary DNS Server** ..... Enter the primary DNS server address as specified by your ISP.

③**Secondary DNS Server**... Enter the secondary DNS server address as specified by your ISP.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN1/WAN2]

■Connection Settings Static IP

Configure the WAN connection.

Connection Settings

① Nickname:	
② IP Address:	
③ Subnet Mask:	
④ Default Gateway:	
⑤ Primary DNS Server:	
⑥ Secondary DNS Server:	

①**Nickname**	Enter the ISP's name. (Up to 31 characters)
②**IP Address**	Enter the WAN IP address as specified by your ISP.
③**Subnet Mask**	Enter the subnet mask as specified by your ISP.
④**Default Gateway**	Enter the default gateway address as specified by your ISP.
⑤**Primary DNS Server**	Enter the primary DNS server address as specified by your ISP.
⑥**Secondary DNS Server**...	Enter the secondary DNS server address as specified by your ISP.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN1/WAN2]

■Connection Settings PPPoE

Configure the WAN connection. (Up to 8 destinations can be registered.)

Connection Settings

① Select Connection:	WAN01
② Nickname:	WAN01
③ Username:	
④ Password:	
⑤ Reconnect Mode:	Always-on
⑥ IP Address:	
⑦ Primary DNS Server:	
⑧ Secondary DNS Server:	
Detail Settings	
⑨ Authentication Protocol:	Automatic
⑩ MSS Limit:	1322
⑪ AC-Name:	
⑫ Service-Name:	

①Select Connection ..... Select the WAN connection. (Default: WAN01)

②Nickname ..... Enter the ISP's name. (Up to 31 characters)

③Username ..... Enter a login user name or account name.

④Password ..... Enter a login password.
• The entered characters are displayed as an * (asterisk) or a • (dot).

⑤Reconnect Mode ..... Select the PPPoE connection method. (Default: Always-on)

• **Manual**
The PPPoE line can be manually connected or disconnected, by clicking <Connect> or <Disconnect>. (☞P5-23)

• **Always-on**
The PPPoE line is always connected.

5. [Router Settings] Menu

[Router Settings]–[WAN1/WAN2]

■ Connection Settings PPPoE (continued)

Connection Settings

① Select Connection: WAN01
② Nickname: WAN01
③ Username:
④ Password:
⑤ Reconnect Mode: Always-on
⑥ IP Address:
⑦ Primary DNS Server:
⑧ Secondary DNS Server:

Detail Settings

⑨ Authentication Protocol: Automatic
⑩ MSS Limit: 1322
⑪ AC-Name:
⑫ Service-Name:

⑥**IP Address**	Enter the WAN IP address, if specified by your ISP.
⑦**Primary DNS Server**	Enter the primary DNS server address as specified by your ISP.
⑧**Secondary DNS Server**...	Enter the secondary DNS server address as specified by your ISP.
⑨**Authentication Protocol**	Enter the authentication protocol as specified by your ISP. (Default: Automatic) • Select "Automatic" if not specified.

5. [Router Settings] Menu

[Router Settings]–[WAN1/WAN2]

■ Connection Settings PPPoE (continued)

Connection Settings

① Select Connection: WAN01
② Nickname: WAN01
③ Username:
④ Password:
⑤ Reconnect Mode: Always-on
⑥ IP Address:
⑦ Primary DNS Server:
⑧ Secondary DNS Server:

Detail Settings

⑨ Authentication Protocol: Automatic
⑩ MSS Limit: 1322
⑪ AC-Name:
⑫ Service-Name:

⑩**MSS Limit**..... Enter the MSS limit, if specified by your ISP. (Default: 1322)
Range: "536"–"1452" (Bytes)

⑪**AC-Name** ..... Enter the access concentrator name, if specified by your ISP.

⑫**Service-Name** ..... Enter the service name, if specified by your ISP.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN1/WAN2]

■List of Connection Settings

List of Connection Settings

Nickname	Username	Reconnect Mode	
WAN01	Icom	Always-on	Delete

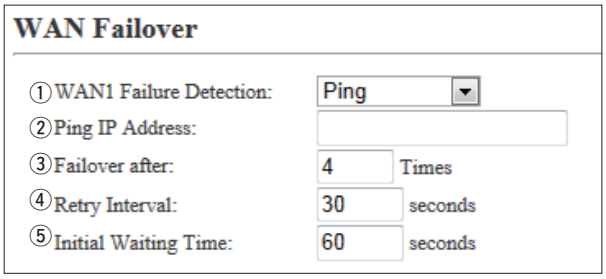
<Delete> ..... Click to delete the entry.

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN Failover]

■WAN Failover

Configure the WAN Failover function.
The WAN Failover function automatically switches the default gateway port to maintain Internet connectivity. (☞P2-9)



Note: This screen appears when "Ping" is selected in the [WAN1 Failure Detection] item.

①WAN1 Failure Detection

Select the detecting option, depending on your network environment.
(Default: Disable)

- **Disable**
  Don't use the WAN Failover function.
- **Link Status**
  Detects the failure of the link status.
  The detecting method differs, depending on the connection type.
  DHCP Client: The IP address has not been obtained.
  Static IP: Connectivity of the [WAN1] port.
  PPPoE: Connectivity of the PPPoE line.
- **DNS Lookup**
  Detects the failure of the query response from the DNS server.
  No failure is detected while either the primary or secondary DNS server returns a query response.
- **Ping**
  Detects the failure of the Ping response.
  - Enter the IP address to send the Ping packets to into the [Ping IP Address] item (②).

②Ping IP Address ……
PING

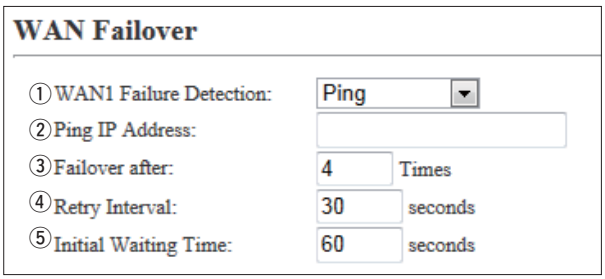
Enter the IP address to send the Ping packets.

(Continued on the next page.)

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN Failover]

■ WAN Failover (continued)



③Failover after ..... Enter the maximum number of retry attempts. (Default: 4)
Range: "1"–"10"

④Retry Interval ..... Enter the retry period. (Default: 30)
Range: "1"–"300" (seconds)

⑤Initial Waiting Time ..... Enter the waiting time before the Failover function starts to monitor the connectivity status after booting. (Default: 60)
Range: "1"–"300" (seconds)

5. [Router Settings] Menu (continued)

[Router Settings]–[WAN Failover]

■Current Status

Displays the WAN Failover function and WAN connection status.

Current Status

① Refresh

②Detection Status	Disabled
③Default Gateway	WAN1
④WAN1	PPPoE Disconnected
⑤WAN2	No Connection

(This is an example.)

①**<Refresh>**..... Click to refresh the screen.

②**Detection Status**..... Displays the monitoring status. ("Disabled," "Enabled (Suspending)" or "Enabled")

③**Default Gateway** ..... Displays the default gateway port. ("LAN," "WAN1" or "WAN2")

④**WAN1**..... Displays the [WAN1] port IP address, connection type and connection status.
Example: 172.22.75.90 (Static IP)

⑤**WAN2**..... Displays the [WAN2] port IP address, connection type and connection status.
Example: DHCP Client Disconnected

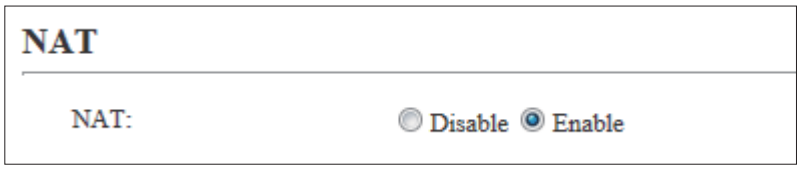
5. [Router Settings] Menu (continued)

[Router Settings]–[NAT]

■NAT

Configure the NAT function.

• This function can be used when the connection type (☞P5-24) is set to [DHCP Client], [Static IP] or [PPPoE].



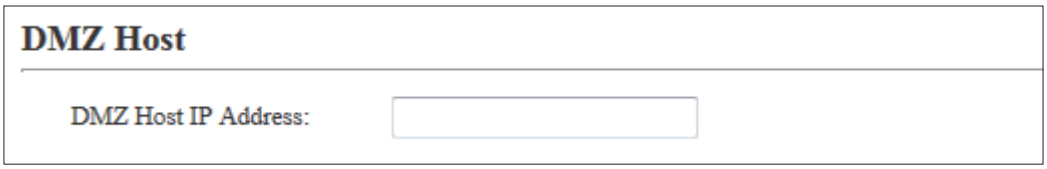
NAT ..... Select "Enable" to use the NAT function. (Default: Enable)

• The NAT function converts the WAN global address into the private address.

■DMZ Host

Configure the DMZ Host function.

• The NAT function can be used when the connection type (☞P5-24) is set to [DHCP Client], [Static IP] or [PPPoE].



DMZ Host IP Address ..... Enter the DMZ host IP address.

5. [Router Settings] Menu (continued)

[Router Settings]–[NAT]

■Port Forwarding

The Port Forwarding function forwards the packets from a masquerade IP (Router Global IP) address to a private IP address.

Port Forwarding

① WAN Port	② LAN IP Address	③ LAN Port	④ Protocol	⑤
Custom		Custom	TCP	Add

①**WAN Port** ..... Select the mnemonic for the WAN port number.
Note: Select "Custom" to set the WAN port by number.

②**LAN IP Address** ..... Enter the private IP address.

③**LAN Port** ..... Select "Custom," if you select the LAN port by the number.

④**Protocol** ..... Select the protocol.

⑤**<Add>** ..... Click to submit the entry.
• Up to 32 tables can be submitted.

■List of Port Forwarding Entries

List of Port Forwarding Entries

WAN Port	LAN IP Address	LAN Port	Protocol	①	②
FTP	192.168.0.200	FTP	TCP/UDP	Edit	Delete
Web	192.168.0.100	Web	TCP/UDP	Edit	Delete

(This is an example.)

①**<Edit>** ..... Click to edit the entry.
• The entry contents are loaded to the Port Forwarding field above.

②**<Delete>** ..... Click to remove the entry.

5. [Router Settings] Menu (continued)

[Router Settings]–[IP Filter]

■IP Filter Setting

Configure the Packet Filtering function.

• This function can be used when the connection type (☞P5-24) is set to [DHCP Client], [Static IP] or [PPPoE].

IP Filter

① No.:
② Entry: ○ Disable ◉ Enable
③ Action: ○ Block ◉ Pass
④ Direction: ◉ In ○ Out
⑤ Interface: Any
⑥ Source IP Address: Mask 32
⑦ Destination IP Address: Mask 32
⑧ Protocol: TCP Custom Value:
⑨ Source Port: Any Custom Value: -
⑩ Destination Port: Any Custom Value: -
⑪ TCP Flags: ☐ URG ☐ ACK ☐ PSH ☐ RST ☐ SYN ☐ FIN

Options

⑫ Stateful Packet Inspection (SPI) ◉ Disable ○ Enable
⑬ Quick: ○ Disable ◉ Enable
⑭ SYSLOG: ◉ Disable ○ Enable

①No. ..... Select the filtering order.
The filter function checks/inspects the packets in the selected order according to the filter setting in [List of IP Filter Entries].
Range: "1"–"64"

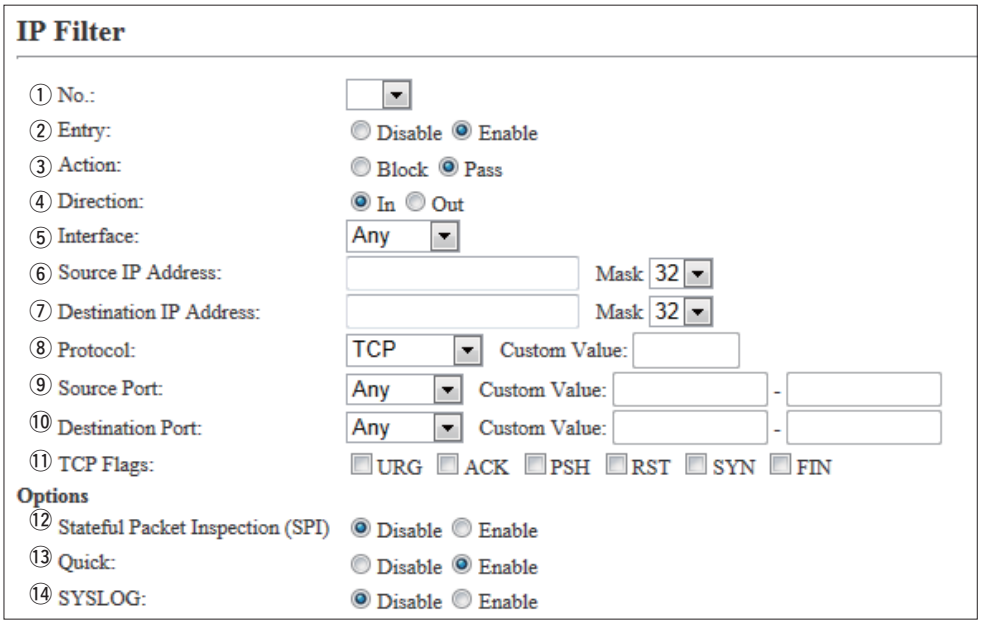
②Entry ..... Select "Enable" to apply the filter setting. (Default: Disable)
Select "Disable" in the unused filter entry.
"1(off)" appears on a disabled filter setting in the [No.] item on the [List of IP Filter Entries].

No.	Action / Direction	Interface / Protocol	Source IP Address (Source Port) / Destination IP Address (Destination Port)	SPI / Quick / SYSLOG	
1 (off)	Block	Any	* (*)	Disable	Edit Delete
	In	Any	* (*)	Disable / Disable	

5. [Router Settings] Menu

[Router Settings]–[IP Filter]

■ IP Filter Setting (continued)



③**Action** ..... Select the filtering method. (Default: Pass)

- **Block:** Blocks all packets matched to the filtering condition.
- **Pass:** Passes all packets matched to the filtering condition.

④**Direction** ..... Select the filtering direction. (Default: IN)

- **In:** Filters the incoming packets from the WAN interfaces.
- **Out:** Filters the outgoing packets to the WAN interfaces.

⑤**Interface** ..... Select the filtering interface. (Default: Any)

- **Any:** All WAN interfaces
- **eth1:** Static IP or DHCP client (WAN1)
- **eth2:** Static IP or DHCP client (WAN2)
- **pppoe0:** PPPoE (WAN1)
- **pppoe1:** PPPoE (WAN2)

5. [Router Settings] Menu

[Router Settings]–[IP Filter]

■IP Filter Setting (continued)

IP Filter

① No.:
② Entry: ○ Disable ◉ Enable
③ Action: ○ Block ◉ Pass
④ Direction: ◉ In ○ Out
⑤ Interface: Any
⑥ Source IP Address: Mask 32
⑦ Destination IP Address: Mask 32
⑧ Protocol: TCP Custom Value:
⑨ Source Port: Any Custom Value: -
⑩ Destination Port: Any Custom Value: -
⑪ TCP Flags: ☐ URG ☐ ACK ☐ PSH ☐ RST ☐ SYN ☐ FIN

Options

⑫ Stateful Packet Inspection (SPI) ◉ Disable ○ Enable
⑬ Quick: ○ Disable ◉ Enable
⑭ SYSLOG: ◉ Disable ○ Enable

⑥Source IP Address.....

Enter the source IP Address (and mask) to filter.
The all packets from the entered IP address are filtered (blocked or passed).
Leave this item blank to filter all packets.
Mask range: "1"–"32"

⑦Destination IP Address

Enter the destination IP Address (and mask) to filter.
The all packets to the entered IP address are filtered (blocked or passed).
Leave this item blank to filter all packets.
Mask range: "1"–"32"

⑧Protocol .....

Select the transport layer's protocol to filter. (Default: Any)

- **Any:** Any protocols
- **TCP:** Only TCP
- **UDP:** Only UDP
- **TCP/UDP:** TCP and UDP

(Continued on the next page.)

5. [Router Settings] Menu

■IP Filter Setting (continued)

IP Filter

① No.:
② Entry: Disable Enable
③ Action: Block Pass
④ Direction: In Out
⑤ Interface: Any
⑥ Source IP Address: Mask 32
⑦ Destination IP Address: Mask 32
⑧ Protocol: TCP Custom Value:
⑨ Source Port: Any Custom Value: -
⑩ Destination Port: Any Custom Value: -
⑪ TCP Flags: URG ACK PSH RST SYN FIN

Options

⑫ Stateful Packet Inspection (SPI) Disable Enable
⑬ Quick: Disable Enable
⑭ SYSLOG: Disable Enable

⑧Protocol (continued) ..... • **ICMP:** Only ICMP

Enter the ICMP type and code to the [Type] and [Code] items.

Range: "0"–"255"

Protocol: ICMP Custom Value:
Type:
Code:

• **IGMP:** Only IGMP

• **Custom:** Specified by the protocol number.

Enter the upper layer protocol number into the [Custom Value] item.

Range: "0"–"255"

5. [Router Settings] Menu

[Router Settings]–[IP Filter]

■ IP Filter Setting (continued)

IP Filter

① No.:
② Entry: Disable Enable
③ Action: Block Pass
④ Direction: In Out
⑤ Interface: Any
⑥ Source IP Address: Mask 32
⑦ Destination IP Address: Mask 32
⑧ Protocol: TCP Custom Value:
⑨ Source Port: Any Custom Value: -
⑩ Destination Port: Any Custom Value: -
⑪ TCP Flags: URG ACK PSH RST SYN FIN

Options

⑫ Stateful Packet Inspection (SPI) Disable Enable
⑬ Quick: Disable Enable
⑭ SYSLOG: Disable Enable

⑨**Source Port** ..... Select the source port, or enter the TCP/UDP source port number.

5. [Router Settings] Menu

■IP Filter Setting (continued)

IP Filter

① No.:
② Entry: Disable Enable
③ Action: Block Pass
④ Direction: In Out
⑤ Interface: Any
⑥ Source IP Address: Mask 32
⑦ Destination IP Address: Mask 32
⑧ Protocol: TCP Custom Value:
⑨ Source Port: Any Custom Value: -
⑩ Destination Port: Any Custom Value: -
⑪ TCP Flags: URG ACK PSH RST SYN FIN

Options

⑫ Stateful Packet Inspection (SPI) Disable Enable
⑬ Quick: Disable Enable
⑭ SYSLOG: Disable Enable

⑩**Destination Port** ..... Select the destination port, or enter the TCP/UDP destination port number.

5. [Router Settings] Menu

[Router Settings]–[IP Filter]

■IP Filter Setting (continued)

IP Filter

① No.:
② Entry: ○ Disable ◉ Enable
③ Action: ○ Block ◉ Pass
④ Direction: ◉ In ○ Out
⑤ Interface: Any
⑥ Source IP Address: Mask 32
⑦ Destination IP Address: Mask 32
⑧ Protocol: TCP Custom Value:
⑨ Source Port: Any Custom Value: -
⑩ Destination Port: Any Custom Value: -
⑪ TCP Flags: ☐URG ☐ACK ☐PSH ☐RST ☐SYN ☐FIN

Options

⑫ Stateful Packet Inspection (SPI) ◉ Disable ○ Enable
⑬ Quick: ○ Disable ◉ Enable
⑭ SYSLOG: ◉ Disable ○ Enable

⑪TCP Flags…… Select the TCP flags.

- The selected flags' first character is displayed in [List of IP Filter Entries] (☞P5-45).

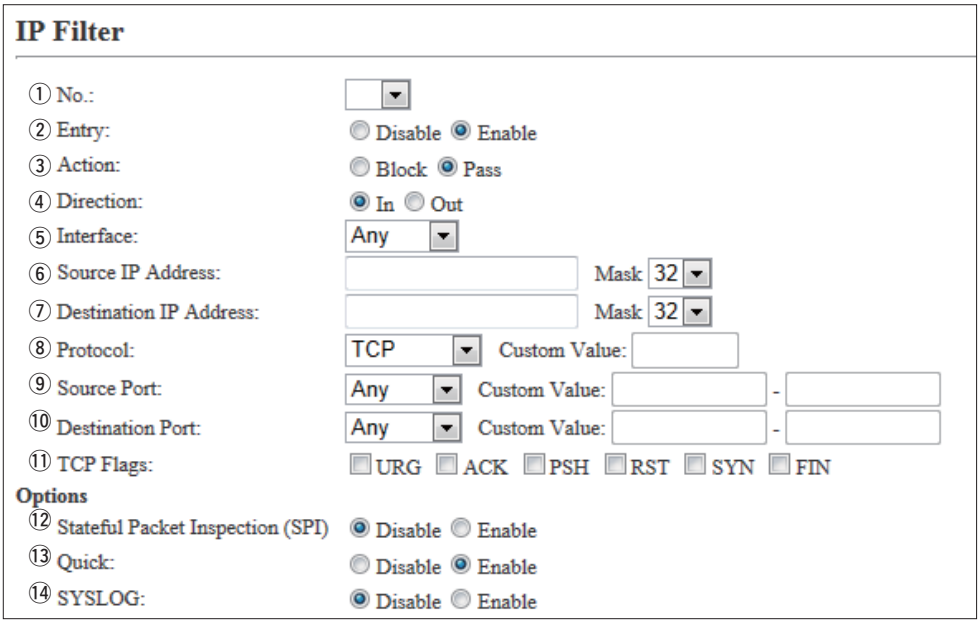
No.	Action / Direction	Interface / Protocol	Source IP Address (Source Port) / Destination IP Address (Destination Port)	SPI / Quick / SYSLOG	
1	Block / In	Any / TCP (AR)	* (*) / * (*)	Disable / Disable / Disable	Edit Delete

(Example: "**A**CK" and "**R**ST" are selected.)

5. [Router Settings] Menu

[Router Settings]–[IP Filter]

■IP Filter Setting (continued)



⑫Stateful Packet Inspection (SPI)

..... Select "Enable" to temporary pass through the response packets.

(Default: Disable)

⑬Quick

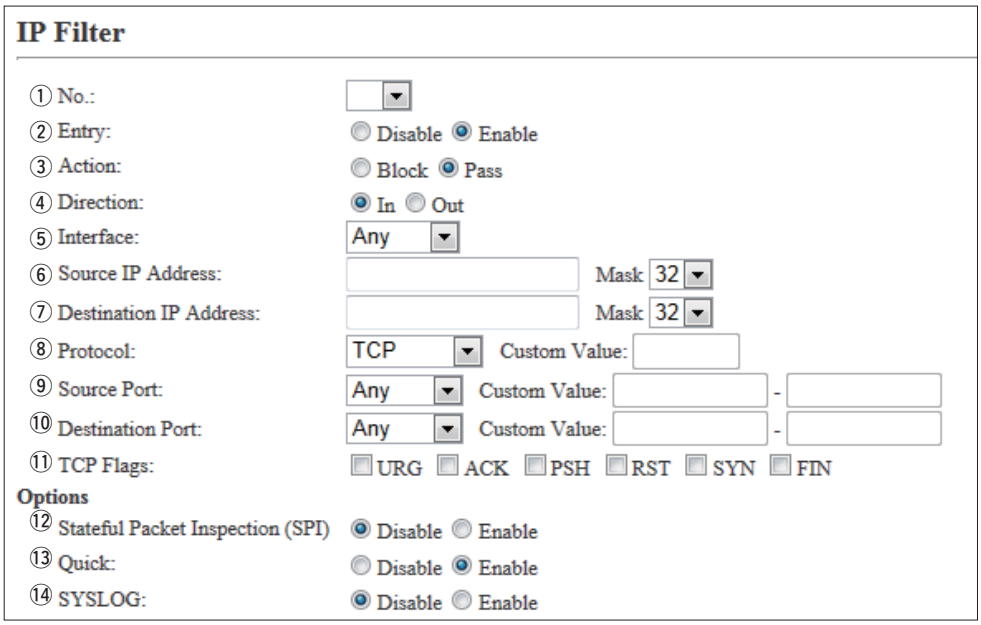
..... Select whether to stop or continue matching when a packet matches a filtering condition. (Default: Enable)

- **Enable:** Stops matching when the packet is matched to the filtering condition. The packet is filtered by the filtering entry and no more filtering conditions will be processed.
- **Disable:** Continues matching when the packet is matched to the filtering condition.
  - If the packet matches no other filtering conditions, the packet is filtered by the filtering entry.
  - If the packet matches other filtering conditions, the packet is filtered by the last-matched filtering entry.

See "①No." (☞P5-36) for the filtering order.

5. [Router Settings] Menu

■IP Filter Setting (continued)



⑭SYSLOG ..... Select "Enable" to output the SYSLOG. (Default: Disable)

- The log information is displayed on the [SYSLOG] screen in the [Information] Menu. (☞P5-7)

Note: This function may affect the system performance. We recommend not using this except for the testing purpose.

5. [Router Settings] Menu (continued)

[Router Settings]–[IP Filter]

■List of IP Filter Entries

List of IP Filter Entries

No.	Action / Direction	Interface / Protocol	Source IP Address (Source Port) / Destination IP Address (Destination Port)	SPI / Quick / SYSLOG	
1	Block	Any	* (*)	Disable	① Edit ② Delete
	In	Any	* (*)	Disable / Disable	
64	Block	Any	* (137-139)	Disable	Edit Delete
	Out	UDP	* (137-139)	Disable / Disable	

(This is an example.)

①**<Edit>** ..... Click to edit the entry.

- The entry contents are loaded to the IP Filter Setting field (☞P5-36).

②**<Delete>** ..... Click to remove the entry.

[About the default filtering conditions]

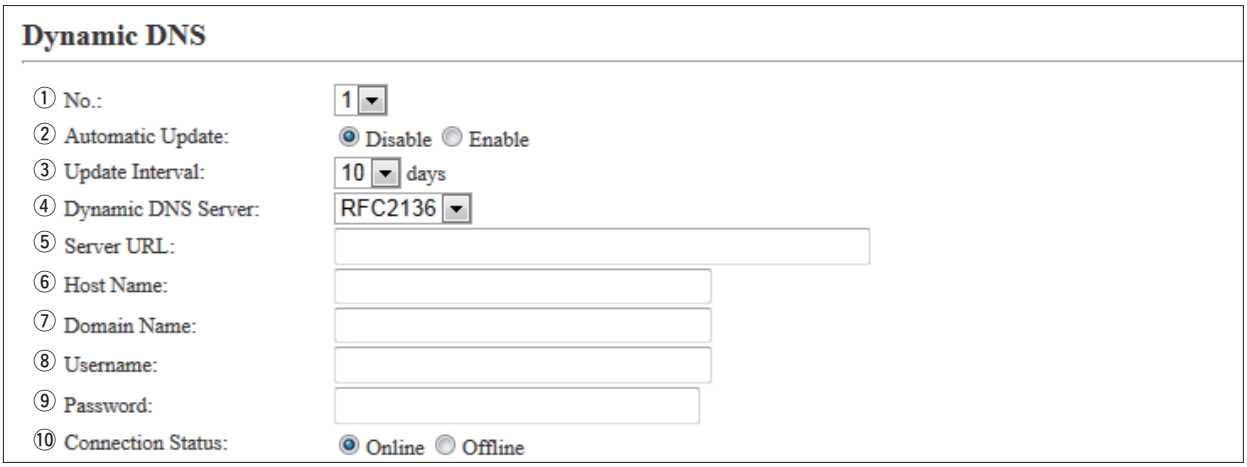
- No. 1: Blocks all incoming packets.
- No. 2: Passes all outgoing packets and its response packets.
  Note: The outgoing packets' response packets are not blocked by the filter No. 1.
- No. 58: Passes the FTP packets.
- No. 59–64: These filtering conditions prevent the Windows applications from the remote access, and leaking information caused by the File Sharing.
- "*" matches all values.

5. [Router Settings] Menu (continued)

[Router Settings]–[Dynamic DNS]

■Dynamic DNS

Configure the dynamic DNS client.



①No. ..... Select the entry number. (Default: 1)

②Automatic Update ..... Select "Enable" to automatically notify the dynamic DNS server of the change of the SR-VPN1's global IP address. (Default: Disable)

③Update Interval ..... Select the update interval. (Default: 10)
Range: "1"–"99" (days)

④Dynamic DNS Server ... Select "RFC2136" to use the RFC2136 dynamic DNS server. (Default: None)

⑤Server URL ..... Enter the RFC2136 dynamic DNS server's URL. (Up to 127 characters)

5. [Router Settings] Menu

[Router Settings]–[Dynamic DNS]

■ Dynamic DNS (continued)

Dynamic DNS

① No.: 1
② Automatic Update: Disable Enable
③ Update Interval: 10 days
④ Dynamic DNS Server: RFC2136
⑤ Server URL:
⑥ Host Name:
⑦ Domain Name:
⑧ Username:
⑨ Password:
⑩ Connection Status: Online Offline

⑥**Host Name** ..... Enter the SR-VPN1's host name. (Up to 31characters)

⑦**Domain Name** ..... Enter the SR-VPN1's domain name. (Up to 31characters)

⑧**Username**..... Enter the user ID to access the dynamic DNS server. (Up to 31characters)

⑨**Password** ..... Enter the password to access the dynamic DNS server. (Up to 31characters)
• The entered characters are displayed as an * (asterisk) or a • (dot).

⑩**Connection Status**..... Select "Offline" to inform the dynamic DNS server of the SR-VPN1's offline status. (Default: Online)

5. [Router Settings] Menu (continued)

[Router Settings]–[Dynamic DNS]

■Dynamic DNS Updates

Displays the update status of the dynamic DNS servers.

Dynamic DNS Updates

⑤ Refresh

① No.	② Time	③ Status	④ Host Address	IP Address	⑥
1	----/--/-- --:--	Not Updated	-	-	Update the Server
2	----/--/-- --:--	Not Updated	-	-	Update the Server

①**Time** ..... Displays the time when the SR-VPN1 notified the dynamic DNS server of the SR-VPN1's global IP address.

②**Status** ..... Displays the update status.
Note: If an error message appears, check the setting following the message.

③**Host Address** ..... Displays the host name that is registered to the dynamic DNS server.

④**IP Address** ..... Displays the global IP address that is registered to the dynamic DNS server.

⑤**<Refresh>**..... Click to refresh the screen.

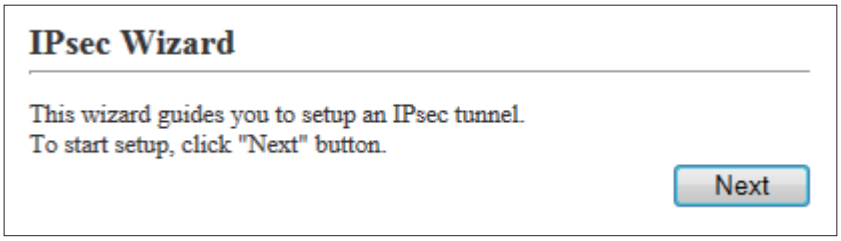
⑥**<Update the Server>** ..... Click to send the SR-VPN1's WAN IP address to the dynamic DNS server.

6. [VPN Settings] Menu

[VPN Settings]–[IPsec Wizard]

■IPsec Wizard

The IPsec Wizard allows you to easily configure the VPN connection.
See Section 3 for details.



NOTE

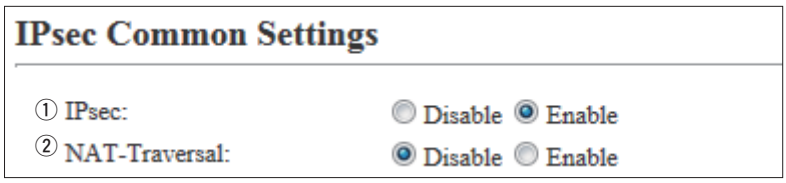
- Connect the WAN line to the [WAN] port, and then configure the Router function to use the VPN function.
- You can perform further settings on the [IPsec] or [IPsec Setting Details] screen (☞P5-51 to P5-65).

6. [VPN Settings] Menu (continued)

[VPN Settings]–[VPN]

■IPsec Common Settings

Configure the IPsec common settings.



①**IPsec** ..... Select "Enable" to use the IPsec function. (Default: Enable)

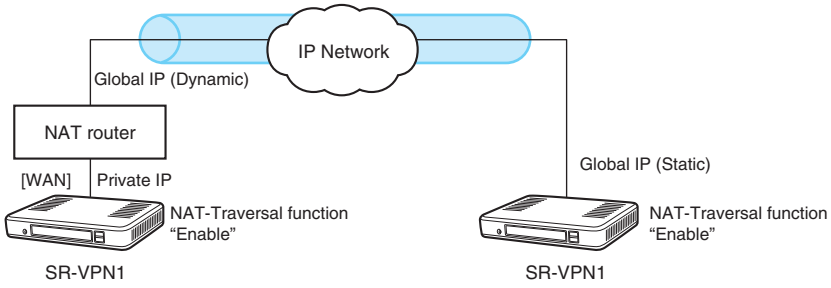
②**NAT-Traversal**..... Select "Enable" to use the NAT-Traversal (NAT passthrough) function. (Default: Disable)

About the NAT-Traversal function.
Two SR-VPN1s with an IPsec connection must have global IP addresses. An IPsec connection is basically impossible if one of them has a private IP address.

This is because the NAT (Network Address Translation) of the upper router of the SR-VPN1 with a private IP address overwrites the port number of the IPsec packets.

The NAT-Traversal function detects the NAT translation, and maintains the IPsec connection appropriately.

To use this function, select "Enable" at [NAT-Traversal] in the both SR-VPN1s.



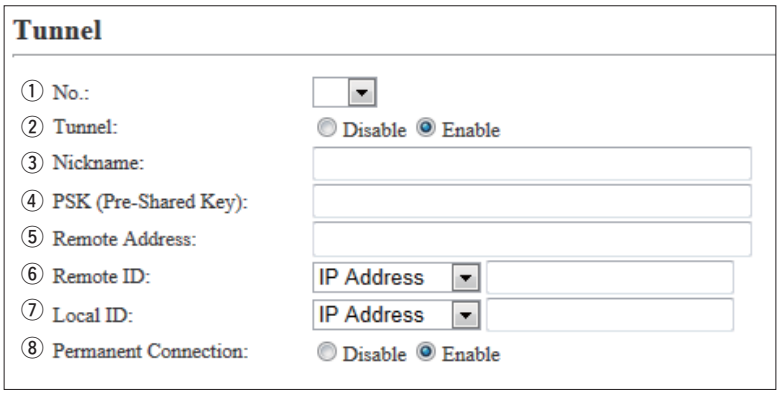
NAT-Traversal example

6. [VPN Settings] Menu (continued)

[VPN Settings]–[IPsec]

■Tunnel

Creates the IPsec tunnel.



①**No** ..... The tunnel number. (1–32)

②**Tunnel** ..... Select "Enable" to use the tunnel entry. (Default: Enable)

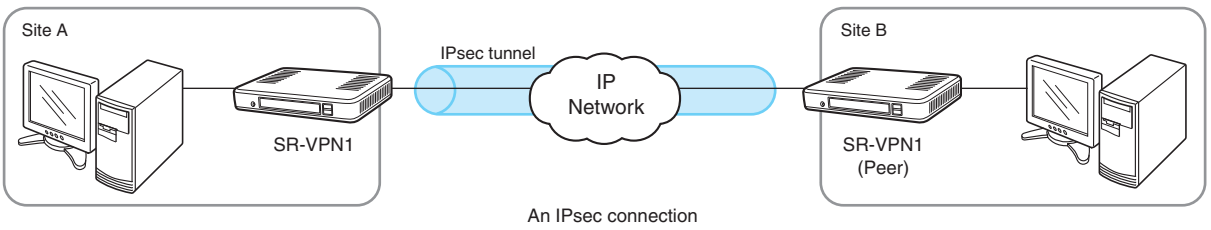
③**Nickname** ..... Enter the tunnel name.

④**PSK (Pre-Shared Key)** ... Enter the key of the other SR-VPN1 (Site B in the illustration below). (Up to 128 characters)

⑤**Remote Address** ..... Enter the IP address or host name of the other SR-VPN1 (Site B in the illustration below).

⑥**Remote ID** ..... Select the ID of the other SR-VPN1 (Site B in the illustration below).
(Default: IP address)
Type: KEYID/FQDN/USER-FQDN String: Up to 128 characters.

⑦**Local ID**..... Select the ID of the SR-VPN1 (Site A in the illustration below).
(Default: IP address)
Type: KEYID/FQDN/USER-FQDN String: Up to 128 characters.

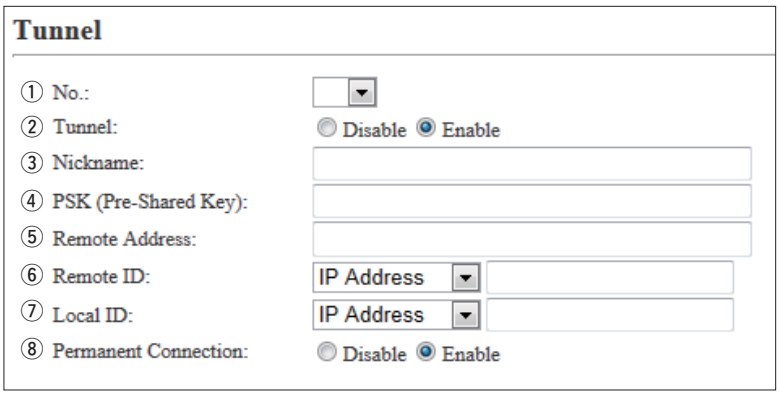


(Continued on the next page.)

6. [VPN Settings] Menu

[VPN Settings]–[IPsec]

■ Tunnel (continued)



⑧**Permanent Connection**… Select the IPsec tunnel connection type. (Default: Enable)

- **"Enable"**
  Connects to the IPsec tunnel when the WAN IP address is obtained.
- **"Disable"**
  Connects to the IPsec tunnel only when clicking <Connect> in the [List of IPsec Settings] item. (Not automatically connected)

6. [VPN Settings] Menu (continued)

[VPN Settings]–[IPsec]

■Routes

Enter the subnet to connect to the IPsec tunnel.

Routes

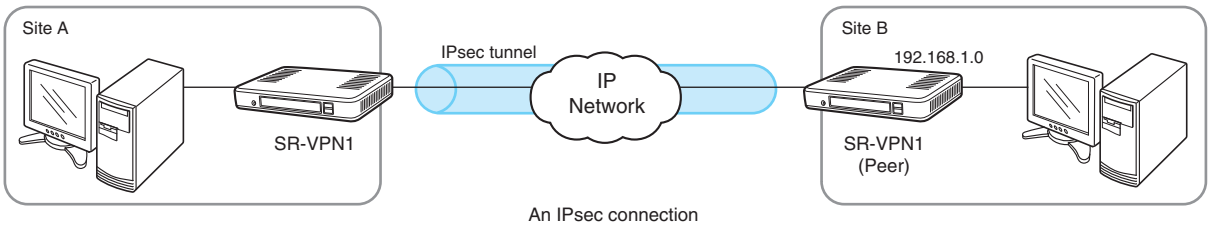
①Destination	②Subnet Mask	③
192.168.1.0	255.255.255.0	+ -

(This is an example.)

①**Destination** ..... Enter the network address of the other SR-VPN1 (Site B in the illustration below).

②**Subnet Mask** ..... Enter the subnet mask to connect to the IPsec tunnel.

③**<+>/<–>** ..... Click to increase or decrease the number of routing paths. You can add up to 5 routing paths for each tunnel.



6. [VPN Settings] Menu (continued)

[VPN Settings]–[IPsec]

■List of IPsec Settings

List of IPsec Settings

①Refresh

②No.	③Nickname	④Status	⑤Remote ID	⑥Local ID	
1	Icom	Constructing ⑦ Disconnect	None	None	⑧Edit ⑨Delete

(This is an example.)

①**<Refresh>**..... Click to update the screen.

②**No.** ..... The tunnel entry number.

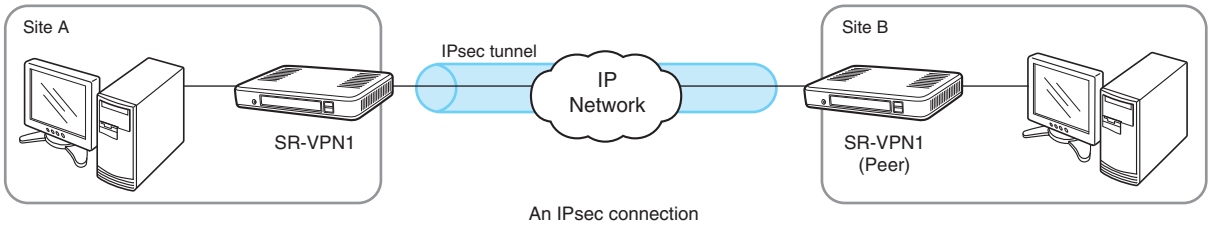
③**Nickname** ..... The tunnel name.

④**Status** ..... The tunnel status.

- **Connected**
  Connected.
- **Waiting**
  Connection ready.
- **Constructing**
  Connection in progress.
- **Disconnected/Down**
  Disconnected.
- **Disabled**
  The tunnel is disabled.
- **IPsec Disabled**
  The SR-VPN1's IPsec function is disabled.

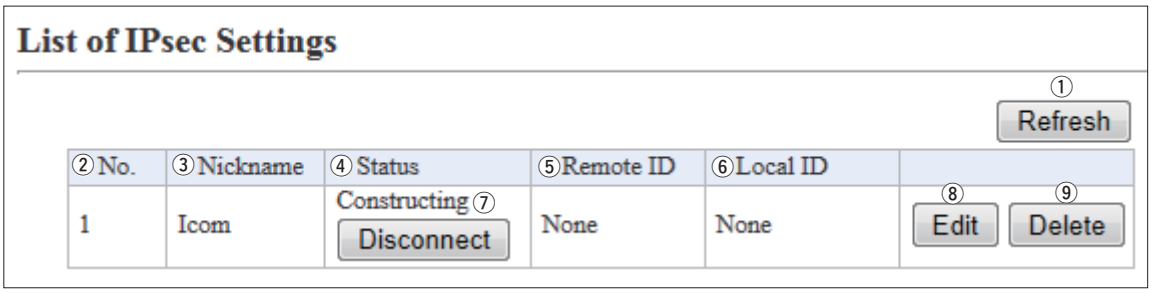
⑤**Remote ID** ..... The ID of the SR-VPN1 (Site B in the illustration below).

⑥**Local ID**..... The ID of the SR-VPN1 (Site A in the illustration below).



6. [VPN Settings] Menu

■ List of IPsec Settings (continued)



(This is an example.)

⑦**Status button** ..... **<Disconnect>/<Down>**
Click to disconnect.
<Connect>/<Up>
Click to connect.

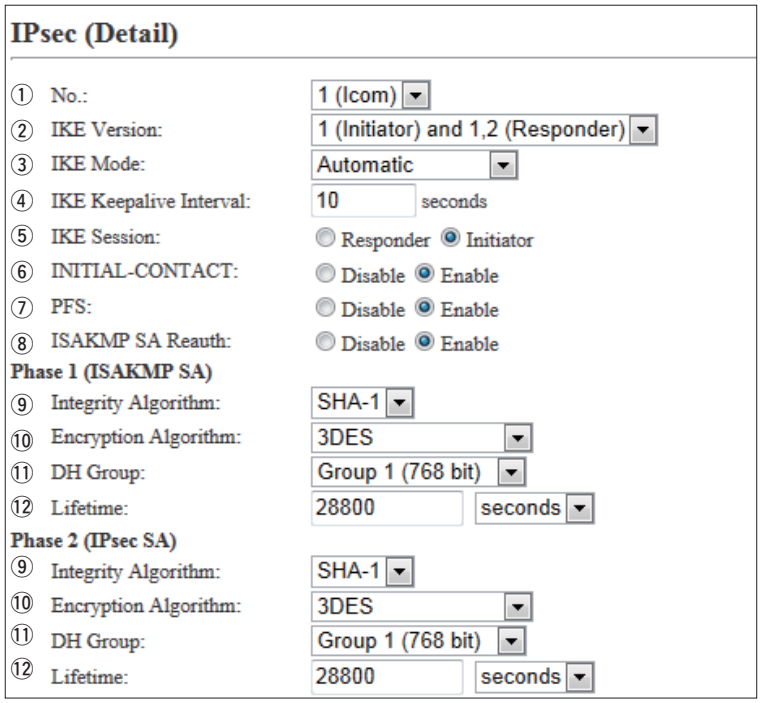
⑧**<Edit>** ..... Click to edit the entry.
• The edited contents are loaded into the [Tunnel] and [Routes] fields.

⑨**<Delete>** ..... Click to delete the entry.

6. [VPN Settings] Menu (continued)

■IPsec (Detail)

Configure the IPsec tunnel details.



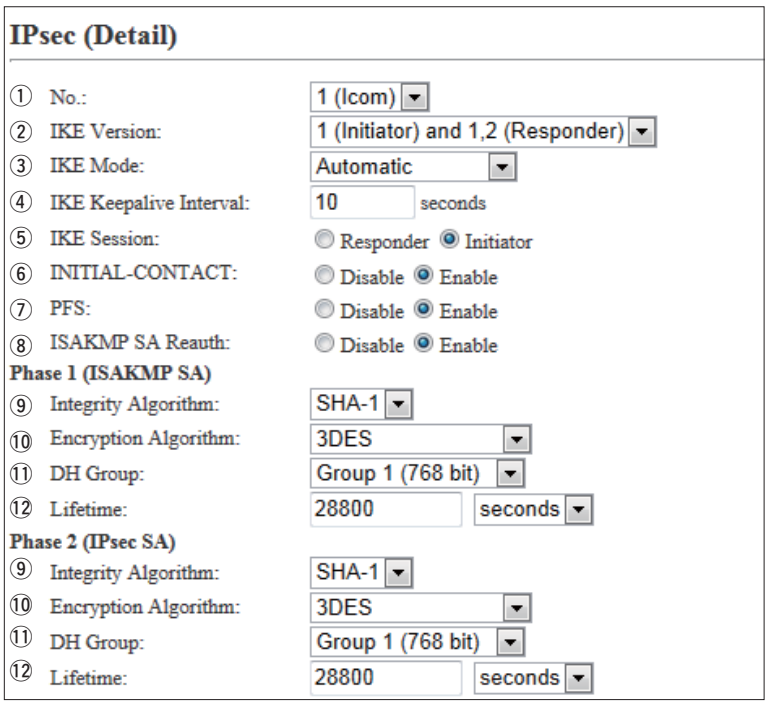
①No ..... Select the tunnel entry number.

- The selected tunnel's settings are reloaded.

(Continued on the next page.)

6. [VPN Settings] Menu

■ IPsec (Detail) (continued)



②IKE Version ..... Select the IKE (Internet Key Exchange) version to use.

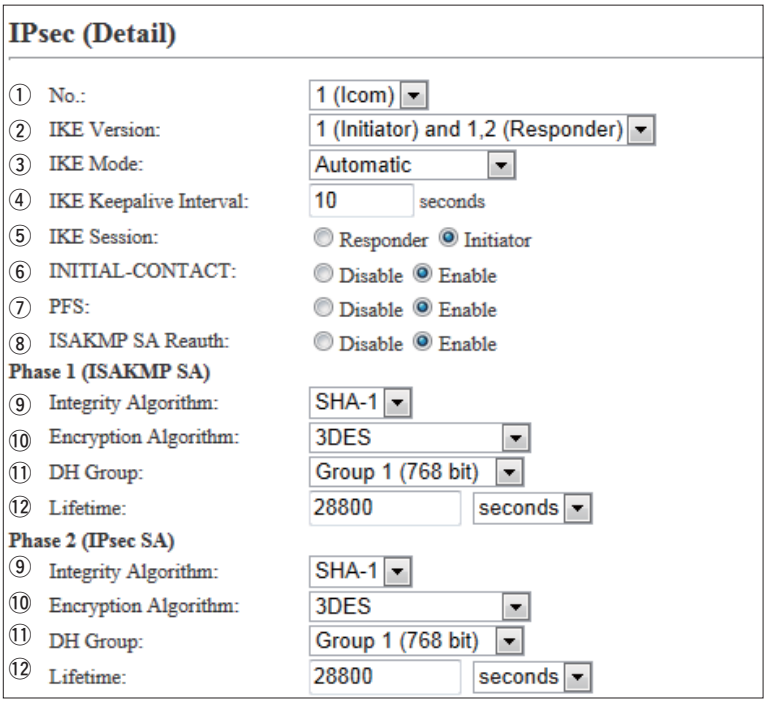
(Default: 1 (Initiator) and 1, 2 (Responder))

- The SR-VPN1 supports IKE versions 1 and 2.

- **1:**
  The initiator and responder use version 1.
- **2:**
  The initiator and responder use version 2.
- **1 (Initiator) and 1, 2 (Responder):**
  If the SR-VPN1 is set as the responder, the IKE version is automatically selected according to the initiator's version.
  If the SR-VPN1 is set as the initiator, version 1 is used.
- **2 (Initiator) and 1, 2 (Responder):**
  If the SR-VPN1 is set as the initiator, version 2 is used.

6. [VPN Settings] Menu

■ IPsec (Detail) (continued)



③IKE Mode ..... Select the IKE key exchange mode. (Default: Automatic)

- **Automatic**
  The exchange mode is automatically selected.
- **Main Mode**
  A more secure exchange mode than the aggressive mode.
- **Aggressive Mode**
  The mode normally used.

6. [VPN Settings] Menu

[VPN Settings]–[IPsec (Detail)]

■ IPsec (Detail) (continued)

IPsec (Detail)

①	No.:	1 (Icom)
②	IKE Version:	1 (Initiator) and 1,2 (Responder)
③	IKE Mode:	Automatic
④	IKE Keepalive Interval:	10 seconds
⑤	IKE Session:	○ Responder ◉ Initiator
⑥	INITIAL-CONTACT:	○ Disable ◉ Enable
⑦	PFS:	○ Disable ◉ Enable
⑧	ISAKMP SA Reauth:	○ Disable ◉ Enable
Phase 1 (ISAKMP SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds
Phase 2 (IPsec SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds

④IKE Keepalive Interval … Enter the IKE keepalive (DPD) interval.
Range: "0"–"600" (Default: 10)
• Select "0" to disable the IKE keepalive.

⑤IKE Session …… Select the IKE key exchange method. (Default: Initiator)
• **Responder**
The SR-VPN1 waits for the key exchange from other SR-VPN1s.
• **Initiator**
The SR-VPN1 initiates the key exchange procedure.

6. [VPN Settings] Menu

■ IPsec (Detail) (continued)

IPsec (Detail)

①	No.:	1 (Icom)
②	IKE Version:	1 (Initiator) and 1,2 (Responder)
③	IKE Mode:	Automatic
④	IKE Keepalive Interval:	10 seconds
⑤	IKE Session:	○ Responder ◉ Initiator
⑥	INITIAL-CONTACT:	○ Disable ◉ Enable
⑦	PFS:	○ Disable ◉ Enable
⑧	ISAKMP SA Reauth:	○ Disable ◉ Enable
Phase 1 (ISAKMP SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds
Phase 2 (IPsec SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds

⑥INITIAL-CONTACT ..... Select "Enable" to send the INITIAL-CONTACT notification message. (Default: Enable)

Note: Only for IKE version 1.

⑦PFS ..... Select "Enable" to use the PFS (Perfect Forward Security) function for a more secure SA key exchange. (Default: Enable)

Note: Only for IKE version 1.

6. [VPN Settings Menu

[VPN Settings]–[IPsec (Detail)]

■ IPsec (Detail) (continued)

IPsec (Detail)

①	No.:	1 (Icom)
②	IKE Version:	1 (Initiator) and 1,2 (Responder)
③	IKE Mode:	Automatic
④	IKE Keepalive Interval:	10 seconds
⑤	IKE Session:	Responder / Initiator
⑥	INITIAL-CONTACT:	Disable / Enable
⑦	PFS:	Disable / Enable
⑧	ISAKMP SA Reauth:	Disable / Enable
Phase 1 (ISAKMP SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds
Phase 2 (IPsec SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds

⑧ISAKMP SA Reauth …… Select "Enable" to negotiate a new SA on the ISAKMP SA re-authentication. (Default: Enable)

Note: Only for IKE version 2.

- **Enable**
  Create a new ISAKMP SA for IKE phase 1.
- **Disable**
  Update the ISAKMP SA for IKE phase 1.

Phase 1 (ISAKMP SA)/2 (IPsec SA)

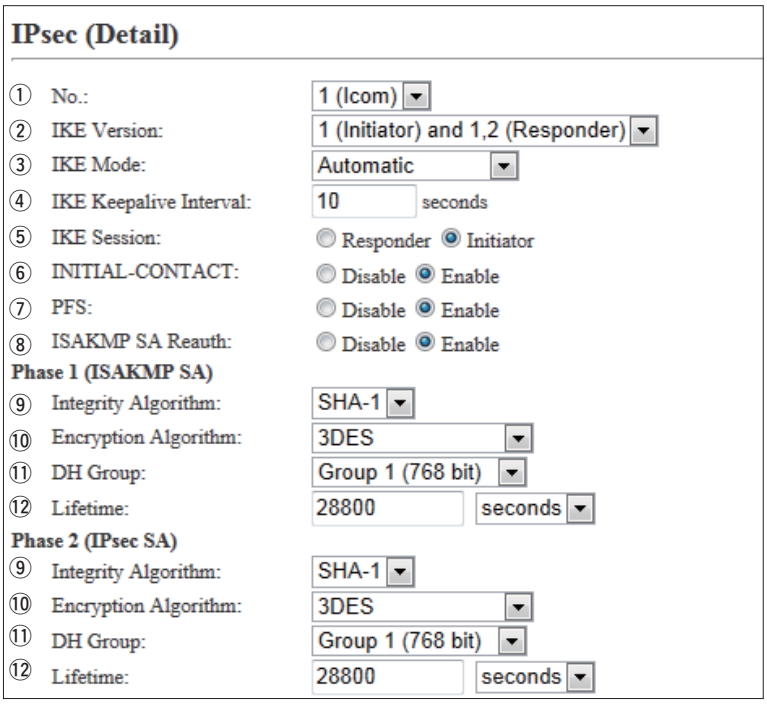
⑨Integrity Algorithm …… Select the integrity algorithm. (Default: SHA-1)

Note: Set the same algorithm to both SR-VPN1s.

- **MD5**
  Use MD5 (Message Digest 5, 128 bit).
- **SHA-1**
  Use SHA-1 (Secure Hash Algorithm 1, 160 bit).

6. [VPN Settings] Menu

■ IPsec (Detail) (continued)



⑩Encryption Algorithm … Select the encryption algorithm. (Default: 3DES)
Note: Set the same algorithm to both SR-VPN1s.

- **3DES**
  Use 3DES (Triple DES, 168 bit).
- **AES-CBC (128 bit)**
  Use AES-CBC (Advanced Encryption Standard - Cipher Block Chaining, 128 bit).
- **AES-CBC (192 bit)**
  Use AES-CBC (192 bit).
- **AES-CBC (256 bit)**
  Use AES-CBC (256 bit).

⑪DH Group …… Select the DH (Diffie-Hellman) group. (Default: Group 1 (768 bit))
Note: The SR-VPN1 supports Group 1 (768 bit) and Group 2 (1024 bit).

6. [VPN Settings] Menu

■ IPsec (Detail) (continued)

IPsec (Detail)

①	No.:	1 (Icom)
②	IKE Version:	1 (Initiator) and 1,2 (Responder)
③	IKE Mode:	Automatic
④	IKE Keepalive Interval:	10 seconds
⑤	IKE Session:	○ Responder ◉ Initiator
⑥	INITIAL-CONTACT:	○ Disable ◉ Enable
⑦	PFS:	○ Disable ◉ Enable
⑧	ISAKMP SA Reauth:	○ Disable ◉ Enable
Phase 1 (ISAKMP SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds
Phase 2 (IPsec SA)		
⑨	Integrity Algorithm:	SHA-1
⑩	Encryption Algorithm:	3DES
⑪	DH Group:	Group 1 (768 bit)
⑫	Lifetime:	28800 seconds

⑫ Lifetime..... Enter the SA lifetime.

Note: Specify the lifetime or lifesize.

(Default: 28800 (seconds))

Phase 1:

- **Seconds**
  Range: "300"–"691200" (seconds)
- **kbytes**
  Range: "100"–"100000" (kB)
  Note: If you set the lifetime by the transfer packet size, enter it into the [Lifetime] item in the [Phase 2] field in Mbytes.

Phase 2:

- **Seconds**
  Range: "300"–"691200" (seconds)
- **Mbytes**
  Range: "100"–"100000" (MB)

6. [VPN Settings] Menu (continued)

■About the IKE version

The setting items differ, depending on the IKE version.

	IKE version 1	IKE version 2
IKE Mode	Yes	No
IKE Keepalive Interval	Yes	Yes
IKE Session	Yes	Yes
INITIAL-CONTACT	Yes	No
PFS	Yes	No
ISAKMP SA Reauth	No	Yes

6. [VPN Settings] Menu (continued)

[VPN Settings]–[IPsec (Detail)]

■List of IPsec Settings

List of IPsec Settings

① Refresh

② No.	③ Nickname	④ Status	⑤ Phase 1	⑥ Phase 2	⑦
1	Icom	Constructing	SHA-1 3DES Group 1 (768 bit)	SHA-1 3DES Group 1 (768 bit)	Edit

(This is an example.)

①**<Refresh>**..... Click to refresh the screen.

②**No.** ..... The tunnel entry number.

③**Nickname** ..... The tunnel name.

④**Status** ..... The tunnel status.

- **Connected**
  Connected.
- **Waiting**
  Connection ready.
- **Constructing**
  Connection in progress.
- **Disconnected/Down**
  Disconnected.
- **Disabled**
  The tunnel is disabled.
- **IPsec Disabled**
  The SR-VPN1's IPsec function is disabled.

⑤**Phase 1** ..... Displays the phase 1 (ISAKMP SA) settings in three lines.

⑥**Phase 2** ..... Displays the phase 2 (IPsec SA) settings in three lines.

⑦**<Edit>** ..... Click to edit the entry.

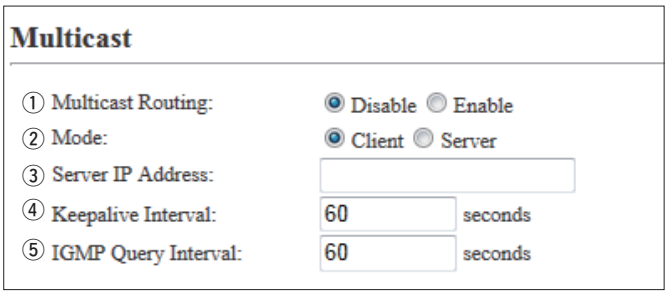
- The entry contents is loaded to the [IPsec (Detail)] field above.

6. [VPN Settings] Menu (continued)

[VPN Settings]–[Multicast]

■Multicast

Configure the IPsec tunnel to pass through the multicast packets.



①Multicast Routing ..... Select "Enable" to use the Multicast Routing function.
(Default: Disable)

②Mode ..... Select the Multicast Routing function mode. (Default: Client)

- **Client**
  The received multicast packets are routed to the server.
- **Server**
  The received multicast packets are routed to the all clients.

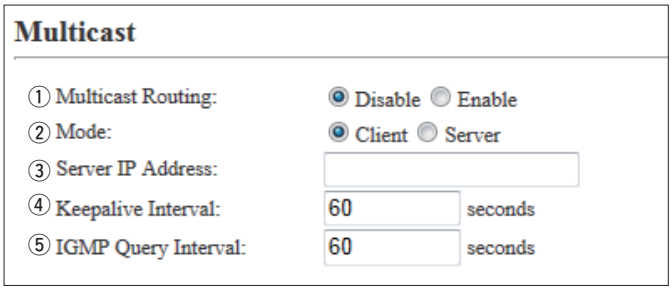
③Server IP Address ..... Enter the routing destination IP address.

④Keepalive Interval ..... Enter the keepalive interval. (Default: 60)
Range: "30"–"28800" (seconds)

6. [VPN Settings] Menu

[VPN Settings]–[Multicast]

■ Multicast (continued)



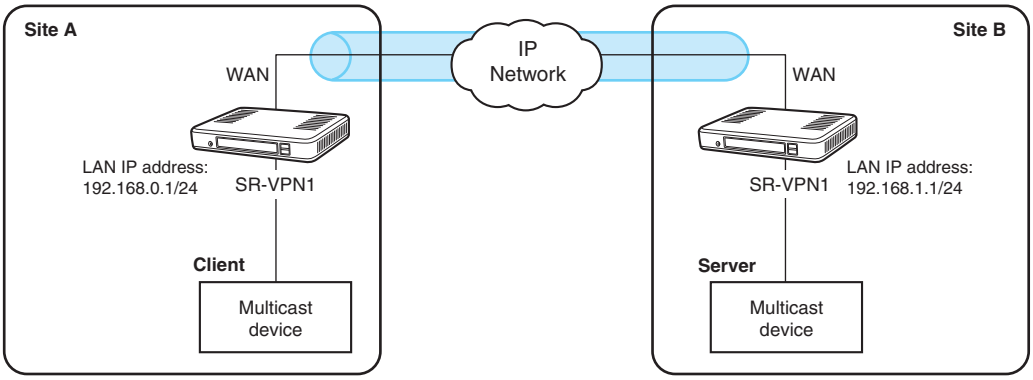
⑤IGMP Query Interval …… Enter the IGMP query interval. (Default: 60)
Range: "30"–"28800" (seconds)

6. [VPN Settings] Menu (continued)

[VPN Settings]–[Multicast]

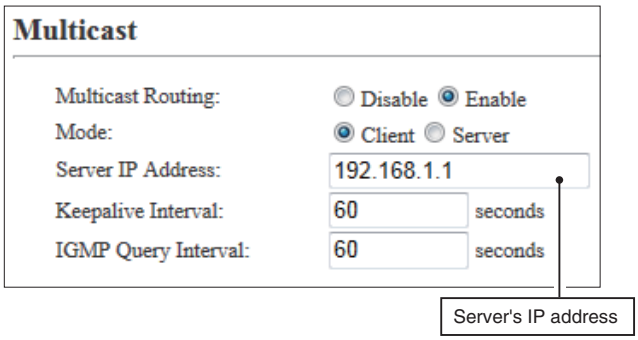
■Setting example

This is an example to configure the IPsec tunnel connecting two sites (A and B) in the Multicast mode.

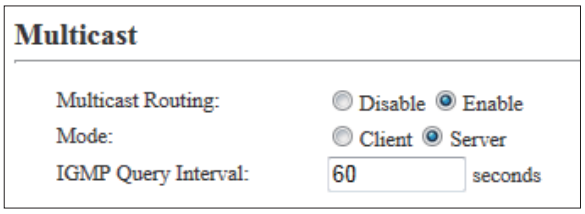


Multicast configuration example

Client (Site A)



Server (Site B)



NOTE

- The client (A) and the server (B) are assumed to be connected through the IPsec VPN.
- Enter the Site B's (server's) LAN IP address into the [Server IP Address] item.
- You don't need to set the same IGMP Query Interval to the Server/Client SR-VPN1s.

6. [VPN Settings] Menu

[VPN Settings]–[Multicast]

■Status Client

Displays the multicast device's status.

Status

①Server IP Address	②Connection Status
192.168.0.1	Disconnected

③IP Address	④Group Address	Lifetime
[redacted] AN)	228.5.6.7 229.111.112.12 239.255.255.1 239.255.255.250	-

(This is an example.)

①Server IP Address ..... The server's IP address set in the [Multicast] field.

②Connection Status..... Server connections status.

- **Connected**
  The keepalive packet has been reached to the server, and then the appropriate response packet is received by the client.
- **Disconnected**
  The IPsec tunnel is disconnected or the server is not activated.

③IP Address ..... The SR-VPN1's LAN IP address.

④Group Address ..... The multicast group addresses of the devices which are connected to the SR-VPN1's LAN port.

- These addresses are notified to the server.

6. [VPN Settings] Menu

[VPN Settings]–[Multicast]

■Status Server

Displays the multicast device's status.

Status

①IP Address	②Group Address	③Lifetime
192.168.1.1 (LAN)	225.6.7.8 239.255.255.250	-
192.168.0.1	239.255.255.1 239.255.255.250	161 seconds

(This is an example.)

①IP Address ..... Displays the list of client IP addresses to transfer multicast packets to.
Note: The SR-VPN1's LAN IP address is displayed on the first line.

②Group Address ..... Displays the multicast group addresses.
- The multicast packets are transferred to the client according to this setting.

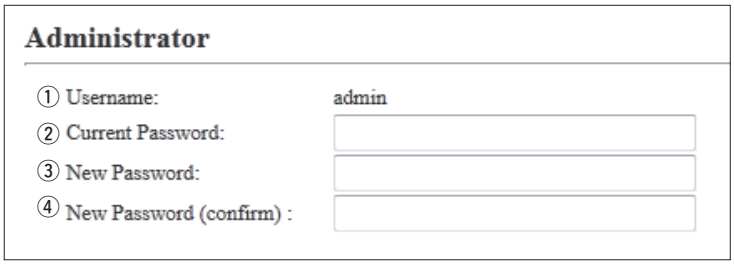
③Lifetime..... Displays the lifetime of the client's group addresses.
- The lifetime is updated when a notice is received.
- If the lifetime is set to 60 seconds (default), the actual is three times of set time (180 seconds).
- When the lifetime is 0 second, the client's group addresses are discarded and the packet transfer is stopped.
- The lifetime is maintained for each client.

7. [Management] Menu

[Management]–[Administrator]

■ Administrator

Set the administrator password.



①**Username**..... Displays the administrator login ID (“admin”).

②**Current Password** ..... Enter the current password, when you change it. (Default: admin)
• The entered characters are displayed as an * (asterisk) or a • (dot).

③**New Password** ..... Enter a new password up to 31 characters.
• The entered characters are displayed as an * (asterisk) or a • (dot).

④**New Password (confirm)** Enter the new password again.

CAUTION
If you have forgotten the password, you cannot access the SR-VPN1’s setting screen again.
In this case, you have to initialize the SR-VPN1 using the <INIT> button. See the supplied “Precautions“ leaflet for details.

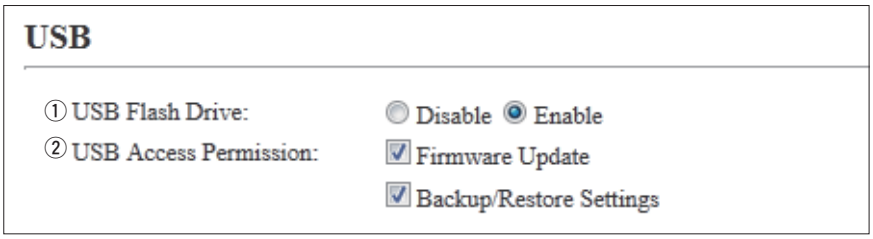
To prevent unauthorized access
You must be careful when choosing your password. A good policy is to occasionally change it.
• Choose one that is not easy to guess.
• Use numbers, characters and letters (both lower and upper case).

7. [Management] Menu (continued)

[Management]–[Management Tools]

■USB

Select the USB flash drive option.



①**USB Flash Drive** …… Select "Enable" to use a USB flash drive. (Default: Enable)

Note: If you use the Automatic firmware update function or Automatic Setting Load function, select “Enable.”

② **USB Access Permission** … Select the USB flash drive access option.

(Default: ☑ Firmware Update
☑ Backup/Restore Settings)

- Firmware Update (☞P6-15)
- Backup/Restore Settings (☞P6-12)

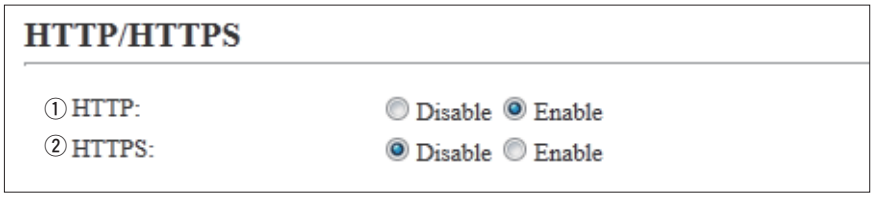
7. [Management] Menu (continued)

[Management]–[Management Tools]

■HTTP/HTTPS

Select the protocol to access the SR-VPN1's setting screen.

Note: If you select "Disable" in both [HTTP] (①) and [HTTPS] (②), you cannot access the SR-VPN1's setting screen again. In this case, you have to initialize the SR-VPN1 using the <INIT> button. See the supplied “Precautions“ leaflet for details.
Or you can reset this setting using the Telnet. See page 7-3 for details.

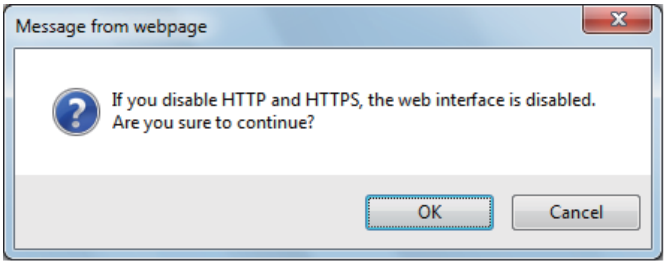


①**HTTP** …… Select “Disable” to block the HTTP protocol. (Default: Enable)

②**HTTPS** …… Select “Enable” to accept the HTTPS protocol. (Default: Disable)
• HTTPS is a more secure protocol than HTTP.

NOTE

If you select "Disable" in both [HTTP] (①) and [HTTPS] (②), a warning message appears.
Click <OK> to continue, or click <Cancel> to cancel.

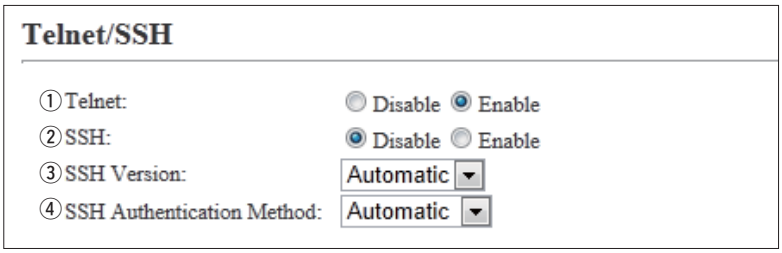


7. [Management] Menu (continued)

[Management]–[Management Tools]

■Telnet/SSH

Select the protocol option to access the SR-VPN1's setting screen from a Telnet or SSH client.



①**Telnet**..... Select "Disable" to block the Telnet protocol. (Default: Enable)
See the 7-3 page for the Telnet details.

② **SSH** ..... Select "Enable" to accept the SSH protocol. (Default: Disable)
- The SSH protocol encrypts the communication between the SR-VPN1 and SSH client.

③ **SSH Version** ..... Select the SSH version. (Default: Automatic)
- **1:** Version 1
- **2:** Version 2
- **Automatic:** The appropriate version is automatically selected

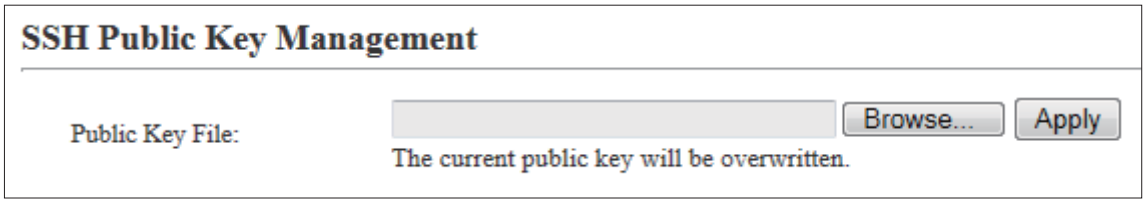
④ **SSH Authentication Method** Select the authentication method. (Default: Automatic)
- **Password:** Password authentication.
- **Public key:** Public key authentication.
- **Automatic:** The authentication method is automatically selected.

7. [Management] Menu (continued)

[Management]–[Management Tools]

■SSH Public Key Management

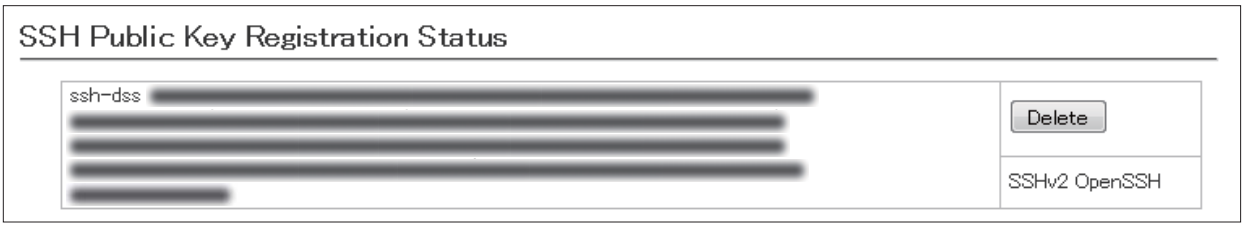
Submit the SSH public key.



Public Key File ..... Select a public key file to submit.

1. Click <Browse...> and then select the file location to save the key in.
2. Click <Apply>.
   The key registration status is displayed in the [SSH Public Key Registration Status] field.

■SSH Public Key Registration Status



(This is an example.)

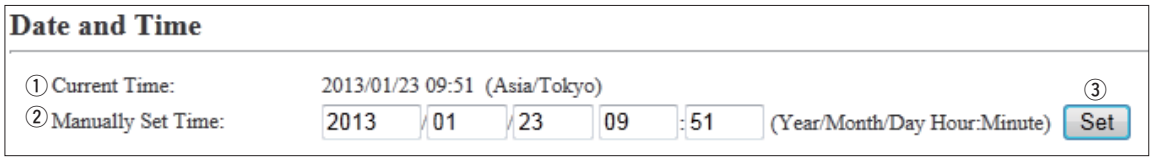
<Delete> ..... Click to cancel the submitted registration.

7. [Management] Menu (continued)

[Management]–[Date and Time]

■Date and Time

You can set the SR-VPN1's internal clock time. (See Section 4 for details.)



①**Current Time** ..... Displays the current time.

②**Manually Set Time** ..... Displays the time when you have opened this screen.
Note: Refresh the browser screen to refresh the time.

③**<Set>** ..... Click to set the internal clock to the time displayed in [Manually Set Time] item (②).
• Before clicking <Set>, refresh the browser screen.

7. [Management] Menu (continued)

[Management]–[Date and Time]

■Time Zone

Select the appropriate Time Zone.

①**Time Zone** …… Select the appropriate Time Zone. (Default: Asia/Tokyo)

②**Use Daylight Savings Time** Select "Disable" if not necessary. (Default: Enable)

- If "Enable" is selected, the SR-VPN1 automatically adjusts the time according to your time zone.
- If the Daylight Savings Time is not used in your area, this selection doesn't affect the time setting.

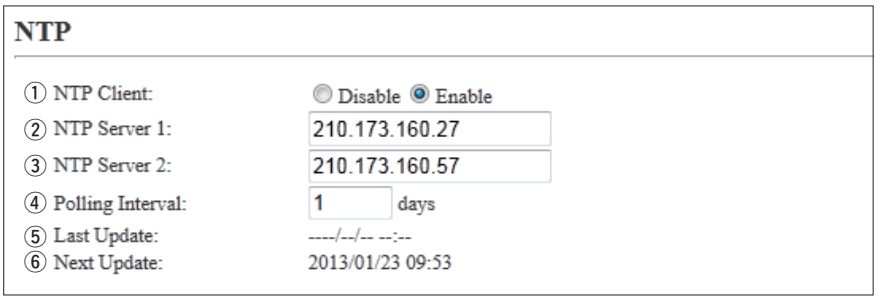
7. [Management] Menu (continued)

[Management]–[Date and Time]

■NTP

The Automatic Clock Synchronize function automatically synchronizes the internal clock with the time server (NTP).

• To use this function, an internet connection and default gateway settings are necessary.



①**NTP Client** …… Select “Enable” to use the Automatic Clock Synchronize function.
(Default: Enable)

②**NTP Server 1** …… Enter the time management server’s IP address.
(Default: 210.173.160.27)

• If the SR-VPN1 cannot access this address, then the address set in the [NTP Server 2] (③) item is used.

Note: The default NTP servers are provided by INTERNET MULTIFEED Co.

③**NTP Server 2** …… Enter the second time management server’s IP address.
(Default: 210.173.160.57)

④**Polling Interval** …… Enter the time synchronization interval. (Default: 1)
Range: 1 to 99 (day)

⑤**Last Update** …… Displays the date and time when the SR-VPN1 has last accessed the time management server.

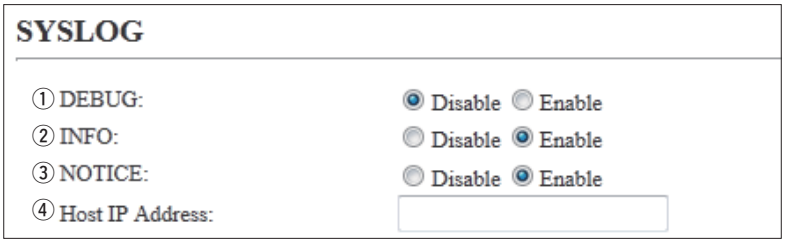
⑥**Next Update** …… Displays the scheduled date and time when the SR-VPN1 accesses the time management server next.

7. [Management] Menu (continued)

[Management]–[SYSLOG]

■SYSLOG

Select the information to be saved to the SYSLOG host.



①**DEBUG** …… Select “Enable” to display the debug information. (Default: Disable)

②**INFO** …… Select “Enable” to display the INFO messages. (Default: Enable)

③**NOTICE**…… Select “Enable” to display the NOTICE messages. (Default: Enable)

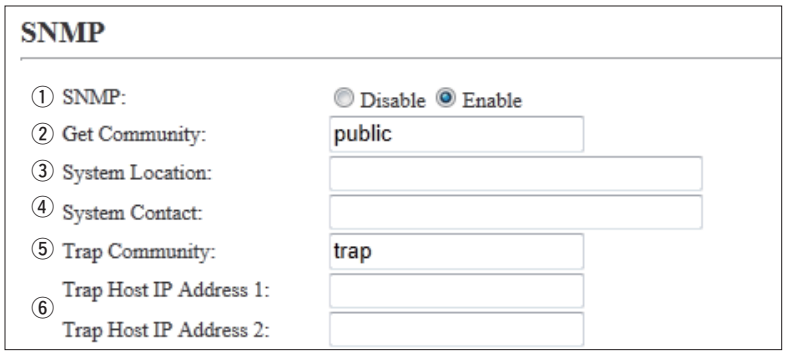
④**Host IP Address**…… Enter the SYSLOG host’s address.

7. [Management] Menu (continued)

[Management]–[SNMP]

■SNMP

Configure the SNMP function.



①**SNMP**..... Select "Enable" to use the SNMP function. (Default: Enable)

②**Get Community** ..... Enter the SNMP GET community string. (Up to 31 characters) (Default: public)

③**System Location** ..... Enter the SNMP system location. (Up to 127 characters)

④**System Contact** ..... Enter the SNMP system contact. (Up to 127 characters)

⑤**Trap Community**..... Enter the SNMP trap community string. (Up to 31 characters) (Default: trap)
The entered string is sent to the address set in item (⑥), in the events below.
- When [WAN1] (Main line) and [WAN2] (Backup line) are toggled.
- When the IPsec tunnel is Up or Down.
- When a new firmware is found. (Online Update function)

⑥ **Trap Host IP Address 1**
Trap Host IP Address 2 ... Enter the trap host's address.

7. [Management] Menu

■SNMP (continued)

The following is the SNMP information.

Note: This information may be changed without notice.

```
-- ***********************************************************************
-- * ICOM Private MIB
-- ***********************************************************************
ICOM-MIB DEFINITIONS ::= BEGIN
    IMPORTS
      MODULE-IDENTITY, OBJECT-TYPE,
      Counter32, Gauge32, TimeTicks
              FROM SNMPv2-SMI
      DisplayString, MacAddress
              FROM SNMPv2-TC
      enterprises
              FROM RFC1155-SMI
      TRAP-TYPE
              FROM RFC-1215;
-- ***********************************************************************
-- *  MODULE IDENTITY
-- ***********************************************************************
icom MODULE-IDENTITY
    LAST-UPDATED     "200901210000Z"
    ORGANIZATION     ""
    CONTACT-INFO     ""
    DESCRIPTION      ""
    ::= { enterprises 11905 }

-- ***********************************************************************
-- *  Major sections
-- ***********************************************************************
events                    OBJECT IDENTIFIER ::= { icom 21 }

-- ***********************************************************************
-- *  events sections
-- ***********************************************************************
value                     OBJECT IDENTIFIER ::= { events 1 }
trap          OBJECT IDENTIFIER ::= { events 2 }

ipsec                     OBJECT IDENTIFIER ::= { value 2 }

--===============================================================================
-- Object Types
--===============================================================================
vDualwanGate OBJECT-TYPE
    SYNTAX  INTEGER                {
      wan1(1),       -- gateway port wan1
      wan2(2)        -- gateway port wan2
    }
    MAX-ACCESS  read-only
    STATUS  current
    DESCRIPTION
      "The dualwan state."
    ::= { value 1 }

vTunnelId OBJECT-TYPE
    SYNTAX  INTEGER
```

(☞Continued on the next page)

7. [Management] Menu

■SNMP (continued)

```
    MAX-ACCESS  read-only
    STATUS  current
    DESCRIPTION
      "IPsec tunnel interface number."
    ::= { ipsec 1 }

vTunnelOper OBJECT-TYPE
    SYNTAX  INTEGER {
      up(1),       -- ready to pass packets
      down(2),
      testing(3)   -- in some test mode
    }
    MAX-ACCESS  read-only
    STATUS  current
    DESCRIPTION
      "The desired state of the IPsec tunnel interface."
    ::= { ipsec 2 }

vNewfirmMsg OBJECT-TYPE
    SYNTAX                          DisplayString (SIZE (0..255))
    MAX-ACCESS        read-only
    STATUS            current
    DESCRIPTION
      "A textual string containing information about the
      new firmware detect."
    ::= { value 3 }

-- ***********************************************************************
-- *  Trap Types
-- ***********************************************************************
icomDualwanTrap TRAP-TYPE
    ENTERPRISE        trap
    VARIABLES { vDualwanGate }
    DESCRIPTION
      "a dual wan switch event."
::= 1

icomIpsecTrap TRAP-TYPE
    ENTERPRISE        trap
    VARIABLES { vTunnelId, vTunnelOper }
    DESCRIPTION
      "a ipsec if up/down event."
::= 2

icomNewfirmTrap TRAP-TYPE
    ENTERPRISE        trap
    VARIABLES { vNewfirmMsg }
    DESCRIPTION
      "a new firmware detect event."
::= 3

-- ***********************************************************************
-- *   End of ICOM MIB
-- ***********************************************************************
END
```

7. [Management] Menu (continued)

[Management]–[Network Test]

■Ping Test

Run the Ping test.

①**Host** ..... Enter the IP address to send the Ping packets to.

②**Number of Times** ..... Select the number of times to send. (Default: 4)

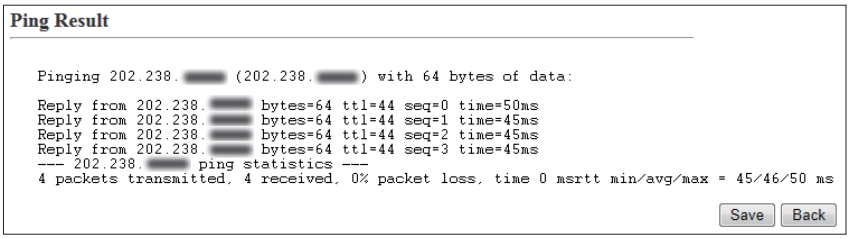
③**Packet Size** ..... Select the size of the packet's data part. (Default: 64)

④**Timeout** ..... Select the Ping response time. (Default: 1000)

Note: If there is no response within the selected time, a time out error is returned.

⑤**<Ping>** ..... Click to run the Ping test.

- The test result is displayed as shown below.



(This is an example.)

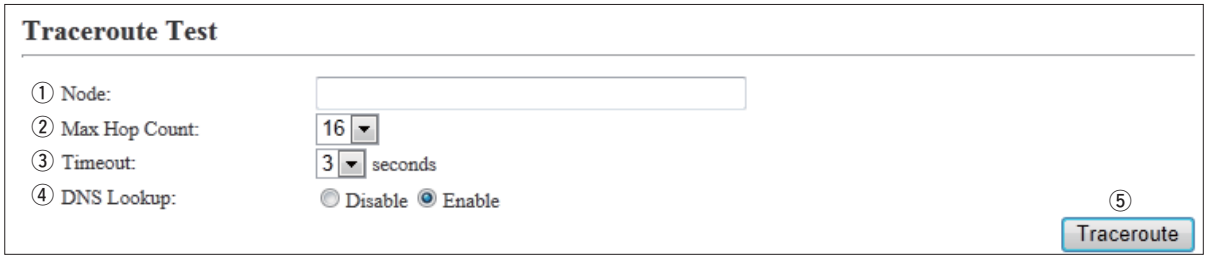
- Click <Save> to save the result to a PC as a text file (extension: "txt").
  Note: The file is saved as "ping_*host's address*.txt."
- Click <Back> to return to the Ping Test screen.

7. [Management] Menu (continued)

[Management]–[Network Test]

■Traceroute Test

Run the Traceroute test.



①**Node** ..... Enter the node's (device's) IP address.

②**Max Hop Count** ..... Select the maximum hop number. (Default: 16)

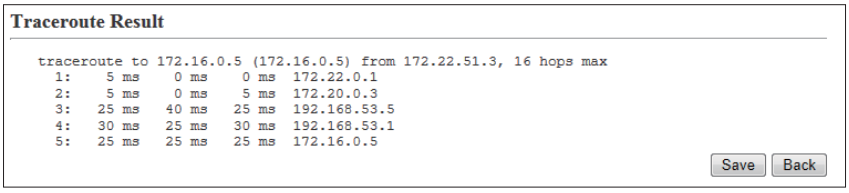
③**Timeout** ..... Select the response time. (Default: 3)

Note: If there is no response within the selected time, a time out error is returned.

④**DNS Lookup** ..... Select “Enable” to convert the node’s (device’s) IP address into the host name. (DNS name resolution) (Default: Enable)

⑤**<Traceroute>** ..... Click to run the traceroute test.

• The test result is displayed as shown below.



(This is an example.)

• Click to save the result to a PC as a text file (extension: “txt”).
• The file is saved as "tracert_*node's address*.txt."
• Click <Back> to return to the Traceroute Test screen.

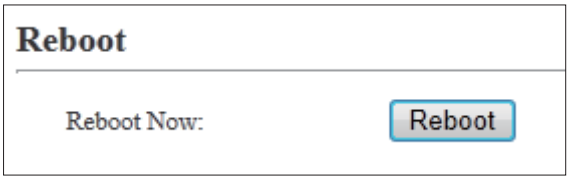
7. [Management] Menu (continued)

[Management]–[Reboot]

■Reboot

Click <Reboot> to reboot the SR-VPN1.

• When clicking <Reboot>, the "Do you want to reboot the system?" message appears. Click <OK> to continue.

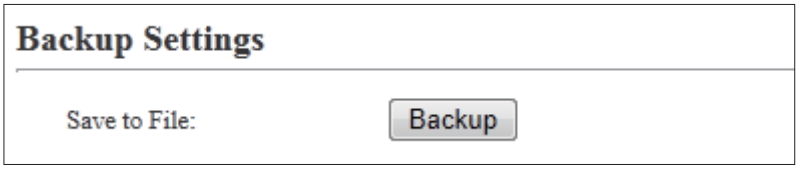


7. [Management] Menu (continued)

[Management]–[Backup/Restore Settings]

■Backup Settings

Save the SR-VPN1's settings to a PC as a backup.

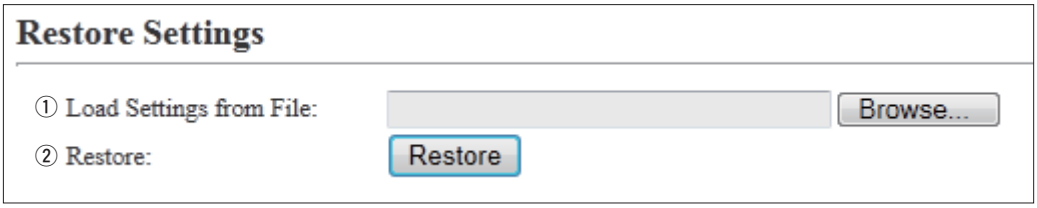


Save to File ..... Click <Backup> to save the settings to a PC as a backup file (Extension: sav).
See the topic below to load the saved file into the SR-VPN1.

> **NOTE**
> DO NOT write the saved file to any other devices.

■Restore Settings

Load the setting file (Extension: "sav") to the SR-VPN1.
Note: Loading takes a few minutes.



①Load Settings from File Click <Browse...> to select the setting file.

② Restore..... Click <Restore> to load the setting into the SR-VPN1.
Notes:
• The SR-VPN1's setting is overwritten.
• After loading, the SR-VPN1 automatically reboots.
Caution: A modified setting file will damage the SR-VPN1.

7. [Management] Menu (continued)

[Management]–[Backup/Restore Settings]

■List of Settings

Displays the changed settings.

Note: The list is clear when the SR-VPN1 is initialized.

List of Settings

```
daylight off
lang en
timezone "Asia/Tokyo"
```

(This is an example.)

7. [Management] Menu (continued)

[Management]–[Factory Defaults]

■Factory Defaults

Click <Restore> to return all settings to the factory default.

Note: If you cannot access the SR-VPN1's setting screen, initialize the SR-VPN1 using the <INIT> button. See the supplied "Precautions" leaflet for details.

NOTES

- After the SR-VPN1 is initialized, the IP address is returned to the default (192.168.0.1), and you must configure the interface Language and Time Zone. See the supplied leaflet for details.
- If the network part of the PC IP address is different from that of the SR-VPN1, you cannot access the SR-VPN1 setting screen. In such case, change the PC IP address according to your network environment,

7. [Management] Menu (continued)

[Management]–[Firmware Update]

NOTES
- NEVER turn OFF the power until the updating has been completed. Otherwise, the SR-VPN1 may be damaged.
- Ask your dealer for updated function or specification details.

■Firmware Status

Displays the firmware version.

Firmware Status

IPL:	Rev. 8
Version:	SR-VPN1 Ver. [redacted] Copyright 2007-2013 Icom Inc.

(This is an example.)

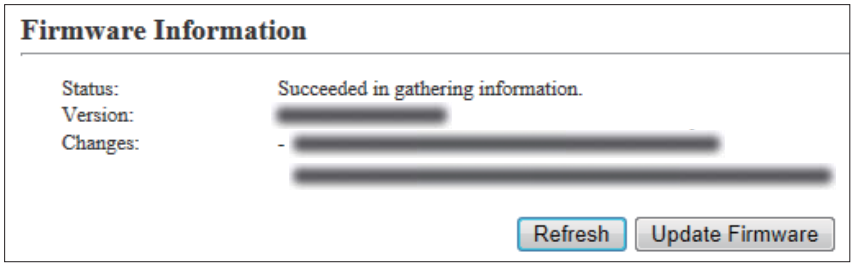
7. [Management] Menu (continued)

[Management]–[Firmware Update]

■Online Update

Downloads the firmware through the internet, and automatically updates it.
Note: To use this function, an internet connection, DNS and default gateway settings are necessary.

Check for Updates ..... Click <Check> to access the update management server.
When the SR-VPN1 has successfully accessed the server, the latest firmware version is displayed as shown below.



(This is an example.)

About the firmware information:

- When there is a newly updated firmware, the <Update Firmware> button is displayed.
- When there is no updated firmware, "Firmware already up-to-date" is displayed.
- When an error message appears, check the internet connectivity.

7. [Management] Menu (continued)

[Management]–[Firmware Update]

■Automatic Update

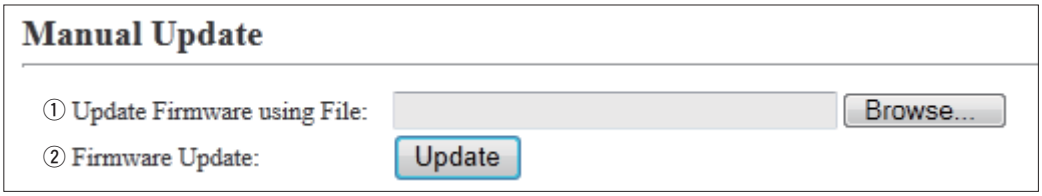
The firmware can be automatically downloaded and updated.

Automatic Update …… Select "Enable" to use the Automatic Update function. (Default: Enable)

• Select "Disable" if you don't desire to automatically update the firmware.

■Manual Update

The firmware can be updated using the saved firmware.



①Update Firmware using File

Click <Browse...> to select the firmware file (extension: "dat").

• The selected file appears in the [Update Firmware using File] item.

② Firmware Update …… Click <Update> to update the firmware.

Note: After updating, the SR-VPN1 automatically reboots.

MAINTENANCE

Section 6

1. How to save the SR-VPN1's setting to a PC 6-2
   Saving the setting 6-2
2. How to load the saved file to a SR-VPN1 6-3
   Reloading the settings file into the SR-VPN1 6-3
3. How to restore the settings 6-4
   A: Using the <INIT> button 6-4
   B: Using the SR-VPN1's setting screen 6-5
4. How to update the firmware 6-6
   ABOUT THE FIRMWARE 6-6
   A: Update the firmware on the setting screen 6-7
   B: Use the Firmware Update function 6-8
5. About the Automatic Restore using a USB flash drive 6-9
6. How to restore the configuration using a USB flash drive 6-12
   Saving the settings file to a USB flash drive 6-12
   Loading the settings from the USB flash drive 6-13
7. How to update the firmware using a USB flash drive 6-15
   Updating the firmware 6-15

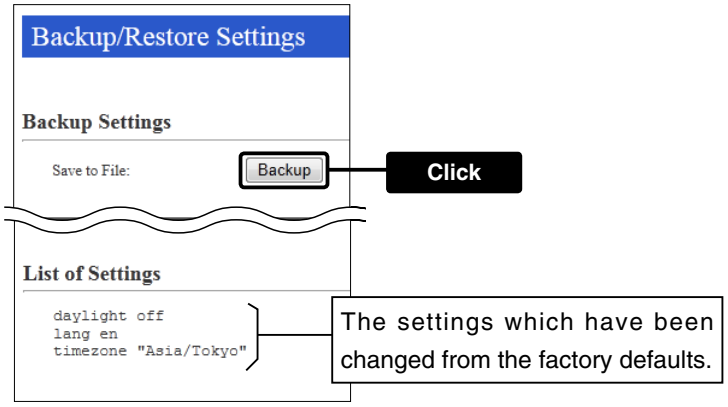
1. How to save the SR-VPN1's setting to a PC

You can save the SR-VPN1's settings to a PC or USB flash drive.
The saved settings can be used to recover the configuration.
• The settings can be directly loaded into the SR-VPN1 from the USB flash drive.

Saving the setting

1 Click [Management], then [Backup/Restore Settings].
• The [Backup/Restore Settings] screen appears.

2 Click <Backup>.
• The File Saving window appears.



3 Select the desired folder/location, then click [Save] in the File Saving window.
• The setting file (extension: "sav") is saved to the selected folder.
• The default file name is composed of the model name (SR-VPN1), version number and date.

2. How to load the saved file to a SR-VPN1

You can load the SR-VPN1's settings from a PC.

• The settings can be directly loaded into the SR-VPN1 from the USB flash drive. (☞P6-12)

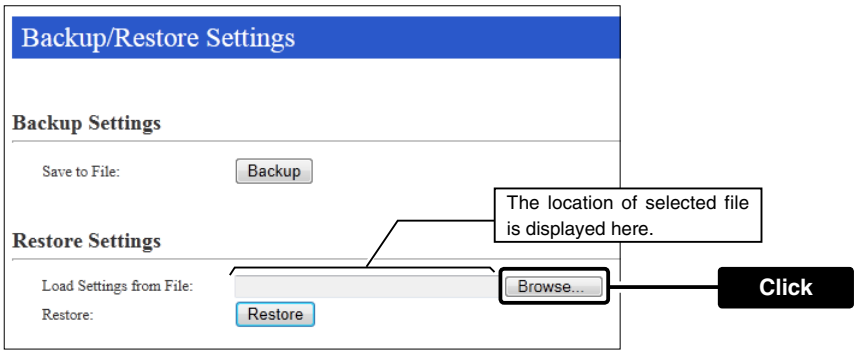
Reloading the settings file into the SR-VPN1

1 Click [Management], then [Backup/Restore Settings].

• The [Backup/Restore Settings] screen appears.

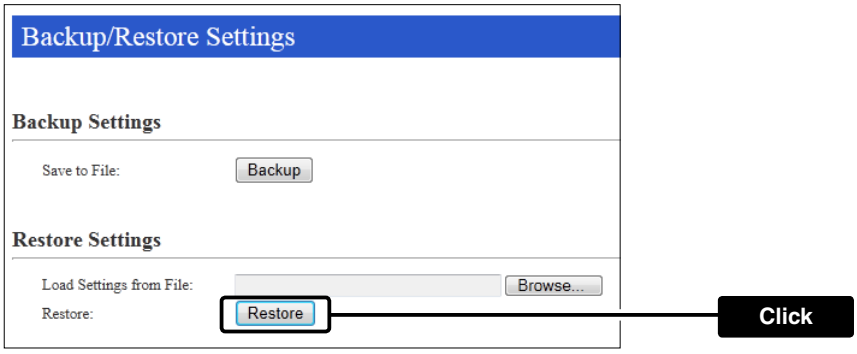
2 Click <Browse...>.

• The File Selection window appears.



3 Select the setting file (extension: “sav”), and then click <Restore>.

• After loading the setting, the SR-VPN1 automatically reboots.



NOTE:
DO NOT write the saved file to any other devices.

3. How to restore the settings

There two ways to initialize the SR-VPN1.

• Set the SR-VPN1's IP address again after the SR-VPN1 is initialized.

A: Using the <INIT> button.

If you cannot access the SR-VPN1 setting screen, initialize the SR-VPN1 using the <INIT> button.

B: Initialize on the SR-VPN1's setting screen.

If you can access the SR-VPN1 setting screen, initialize the SR-VPN1 on the setting screen. (☞P5-88)

A: Using the <INIT> button

Initializing clears all the settings.

• If the network part of the PC IP address is different from that of the SR-VPN1, you cannot access the SR-VPN1 setting screen. In such case, change the PC IP address according to your network environment.
See the supplied "Precautions" leaflet for details.

About the initializing condition

You can restore all the SR-VPN1's settings. The SR-VPN1's IP address is set to "192.168.0.1," when initialized. Set the PC's IP address to "192.168.0.xxx." (You can set xxx to any number from 2 to 254.)
And you must configure the interface Language and Time Zone. See the supplied leaflet for detail.

3. How to restore the settings(continued)

B: Using the SR-VPN1's setting screen

1 Click [Management], then [Factory Defaults].

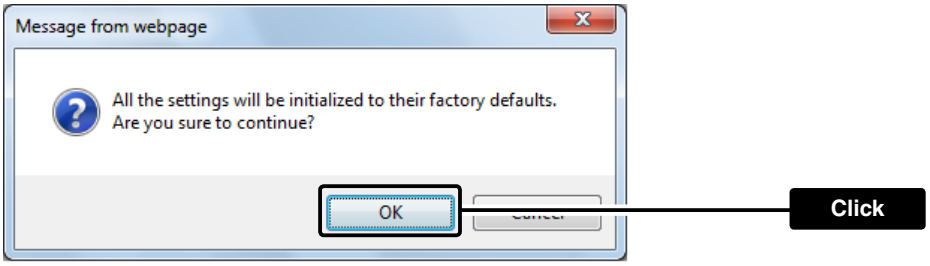
• The [Factory Defaults] screen appears.

2 Click <Restore>.

• The warning window appears.

3 Click <OK>.

• The SR-VPN1 automatically reboots.



About the initializing condition

You can restore all the SR-VPN1's settings. The SR-VPN1's IP address is set to "192.168.0.1," when initialized. Set the PC's IP address to "192.168.0.xxx." (You can set xxx to any number from 2 to 254.)

And you must configure the interface Language and Time Zone. See the supplied leaflet for details.

4. How to update the firmware

There are two ways to update the firmware.

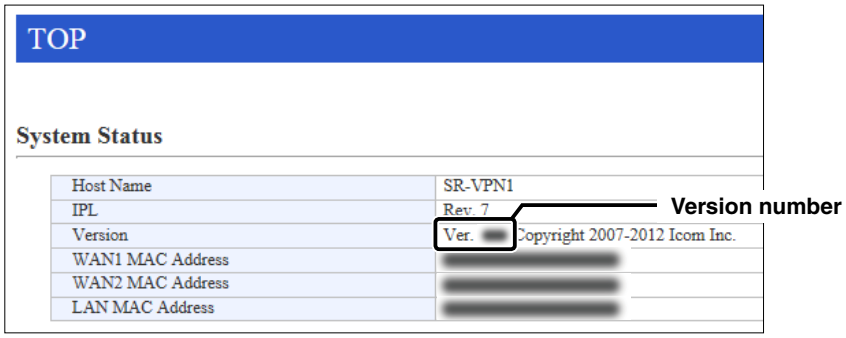
A: Updating on the setting screen.
Update the firmware on the setting screen.

B: Use the Firmware Update function. (☞P6-8)
The firmware can be automatically downloaded and updated.

- You can update the firmware using a USB flash drive. (☞P6-15)
- When [MSG] lights green, a firmware update is ready. See the “Precautions“ leaflet for details.

ABOUT THE FIRMWARE

The firmware may be updated when the functions and specifications of the SR-VPN1 are improved.
Ask your dealer for updated function or specification details.



NOTE:

- NEVER turn OFF the power until the updating has been completed. Otherwise, the SR-VPN1 may be damaged.
- If the firewall is running, stop it before updating the firmware. If you want to stop the firewall, ask your network administrator for the detail.
- Icom is not responsible on the consequence of the updating the firmware.

4. How to update the firmware (continued)

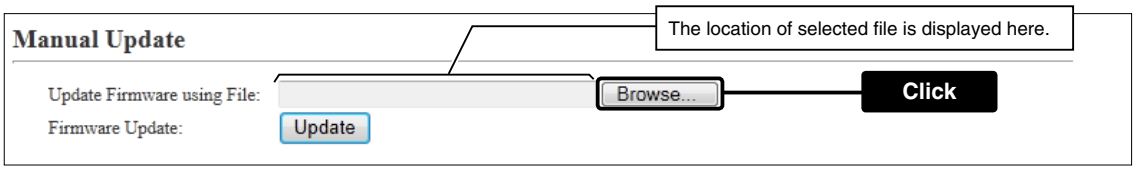
A: Update the firmware on the setting screen

We recommend that you save the current setting in the PC, before updating the firmware. (☞P6-12)
Note: Some settings may be returned to their default after the firmware update. Check Icom website for details.
• Restricting to access the setting screen is recommended. (☞P4-2)

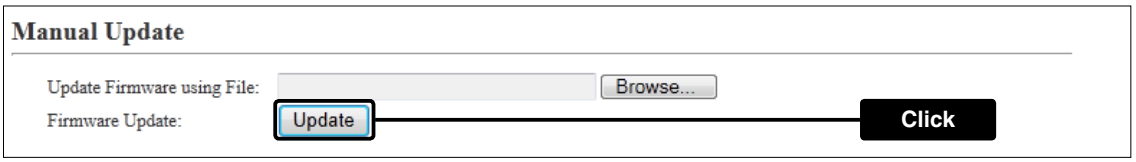
1 Download a new firmware (extension: “dat”) from Icom website.

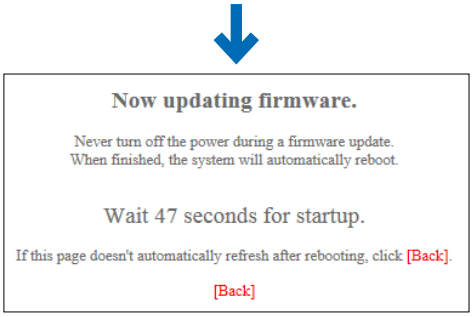
2 Click the [Management] menu, then [Firmware Update].
• The [Firmware Update] screen aeaprs.

3 Click <Browse...>, and then select the firmware file (Extension: dat).



4 Click <Update>.
• The "Now updating firmware" screen appears.





NOTE:
• NEVER turn OFF the power until the updating has been completed. Otherwise, the SR-VPN1 may be damaged.
• The SR-VPN1’s IP address is set to “192.168.0.1,” when initialized by the firmware update. Set the PC’s IP address to “192.168.0.xxx.” (You can set xxx to any number from 2 to 254.)
And you must configure the interface Language and Time Zone. See the supplied leaflet for details.

4. How to update the firmware (continued)

B: Use the Firmware Update function

When [MSG] lights green, a firmware update is ready.

See the “Precautions” leaflet for details.

- To use this function, an internet connection, DNS and default gateway settings are necessary.
- We recommend to save the setting file as the backup. (☞P6-12)

5. About the Automatic Restore using a USB flash drive

You can clone the SR-VPN1's settings and firmware using a USB flash drive.
• See pages 6-12 to 6-16 for details.

About the USB flash drive:
- Before using the USB flash drive, save the content to a PC as the backup.
- The USB flash drive is not supplied. Purchase separately.
- A USB flash drive such as one with biometric authentication, or one with password protection is not supported.
- Turn OFF the SR-VPN1's power before inserting or removing the USB flash drive, to prevent data corruption.
- Either one of the USB slots accepts the USB flash drive, but insert only one USB flash drive at a time.
- Insert the USB flash drive securely.
- NEVER remove the USB flash drive or turn OFF the SR-VPN1's power, while transferring data. It will cause data corruption, or damage the USB flash drive. While transferring data, the [MSG] LED blinks in orange.
- After the firmware updating is finished, check the firmware version on the setting screen to verify that the update was correctly done.
- When importing setting data from the USB flash drive to the SR-VPN1, the originally programmed setting data is automatically saved as "bakdata.sav" in the USB flash drive, as a backup.
- If both firmware and setting files are saved in a USB flash drive, the firmware and setting data are sequentially updated.

Supported USB specification:

Interface:	USB2.0
Device:	USB flash drive (USB Mass Storage Class)
File format:	FAT16/FAT32 (exFAT and NTFS are not supported.)

Note: Some USB flash drives are not guaranteed.

(Continued on the next page.)

5. About the Automatic Restore using a USB flash drive (continued)

[About the settings file name]

The settings file must be saved as “savedata.sav” in the USB flash drive.

The firmware file, which is downloaded from Icom website, must be saved as “firmware.dat” in the USB flash drive.

• Only the settings file saved on the SR-VPN1’s setting screen can be used. See page 7-4 for details.

[About the Automatic Settings Backup function]

The latest 10 backup files (revisions) are stored in the USB flash drive, as the file name “bakdata_X.sav” (X=Revision number).

(Example)
The oldest backup file’s name; “bakdata_10.sav”

• The firmware is not automatically saved as a backup.
• The latest settings backup file is saved as “bakdata.sav” (with no revision number).
• If the content of settings file is the same as the SR-VPN1’s current settings, no setting backup file is saved.

(Continued on the next page.)

5. About the Automatic Restore using a USB flash drive (continued)

[How to clone the settings and the firmware using a USB flash drive.]

A USB flash drive can contain settings and firmware files for different SR-VPN1s.

You need to create folders, whose names are each SR-VPN1's LAN MAC address (☞Pv, P5-5), and save the firmware and settings files to each folder.

Example: The SR-VPN1's LAN MAC address is "0090C7000001."

- Create the folder named "0090C7000001" in a USB flash drive, and then save the firmware and settings files to the folder.

  Insert the USB flash drive, into the SR-VPN1. Then the setting backup file is automatically created in the "0090C7000001" folder.

  The firmware and settings files are loaded from the "0090C7000001" folder.

  Note: The firmware and settings files in any other folders are not loaded.

- If inserting the USB flash drive (Figure 1 and 2 in the picture below) into the SR-VPN1 (0090C7000002), the setting backup file is automatically created in the root directory as there is no folder whose name is SR-VPN1's LAN MAC address.

  The firmware and settings files in the root directory are loaded.

Figure 1

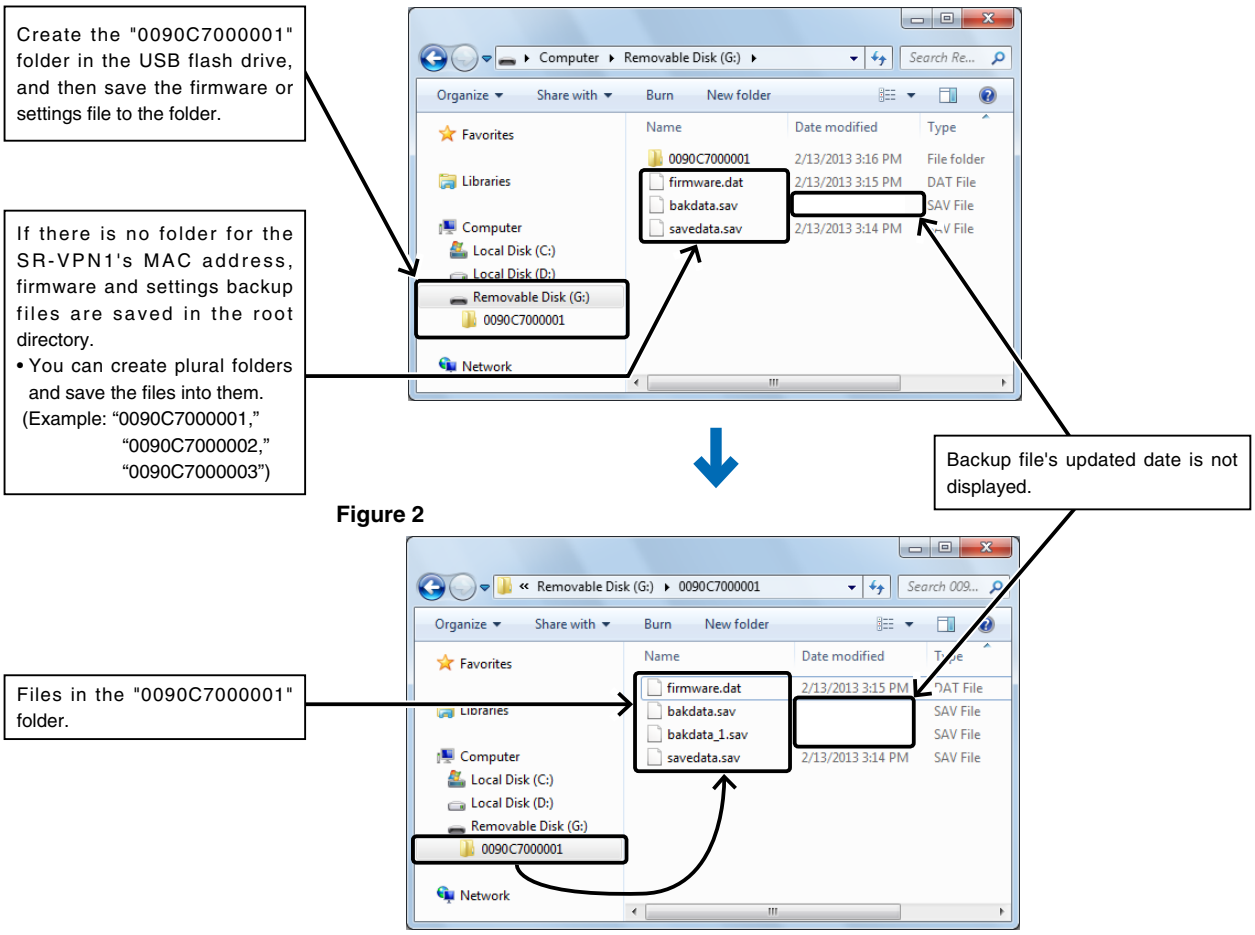


Figure 2

6. How to restore the configuration using a USB flash drive

You can clone the settings to other SR-VPN1s.
It is convenient when you sequentially configure plural SR-VPN1s.
Note: Before using a USB flash drive, see page 6-9.

Saving the settings file to a USB flash drive

1 Insert the USB flash drive securely to the PC.

2 Access the SR-VPN1's setting screen.

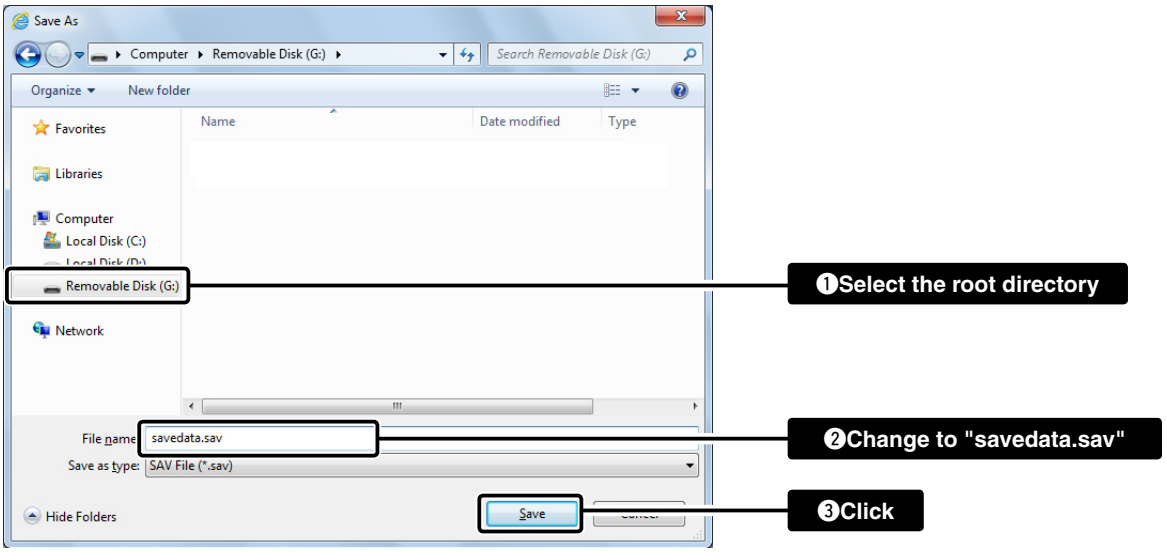
3 Click [Management], then [Backup/Restore Settings].

- The [Backup/Restore Settings] screen appears.

4 Click <Backup>.

5 Select the root directory of the USB flash drive, and save the settings file as “savedata.sav.“

- Any of other file name is not acceptable.



(Continued on the next page.)

6. How to restore the configuration using a USB flash drive (continued)

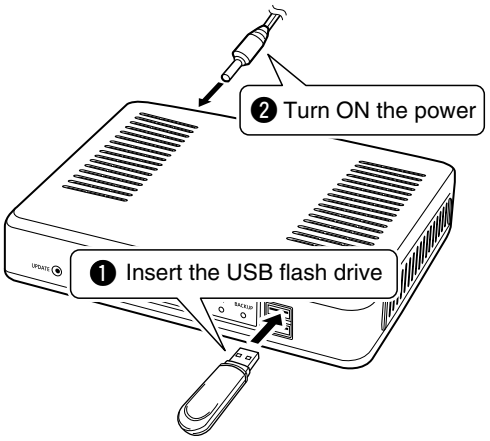
Loading the settings from the USB flash drive

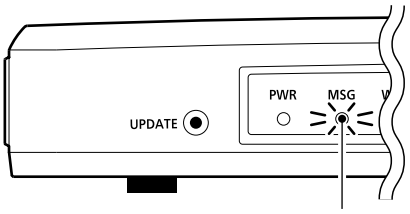
1 Remove the USB flash drive from the PC appropriately.

2 Prepare the SR-VPN1 to load the settings.

3 Turn OFF the power.
NOTE: Turn OFF the SR-VPN1's power, before inserting the USB flash drive.

4 Insert the USB flash drive, which contains the setting data (savedata.sav), to the [USB] port, and then turn ON the power.
• While transferring data, the [MSG] LED blinks.





Lights in orange
while accessing the device.

Note: NEVER remove the USB flash drive or turn OFF the SR-VPN1's power, while transferring data. It will cause data corruption, or damage the USB flash drive.

(Continued on the next page.)

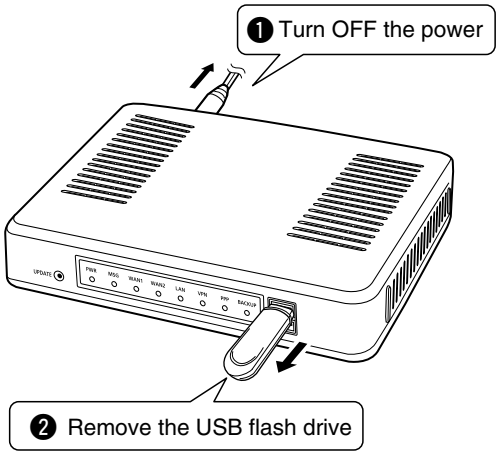
6. How to restore the configuration using a USB flash drive (continued)

Loading the settings from the USB flash drive (continued)

5 When the all data has been loaded into, the [MSG] LED blacks out and the SR-VPN1 automatically restarts.
Verify that the [PWR] LED lights green, then turn OFF the power.
Then remove the USB flash drive from the SR-VPN1.

Note: The SR-VPN1's old setting data is automatically saved in the USB flash drive as "bakdata.sav."

Note: NEVER remove the USB flash while the SR-VPN1's power is ON.



NOTE:
If "Disable" is selected in the [USB Flash Drive] item on the [USB] screen, this function cannot be used. (☞P5-72)

7. How to update the firmware using a USB flash drive

The firmware update can be done by using a USB flash drive.
Note: Before using a USB flash drive, see page 6-9.

Updating the firmware

1 Download a new firmware (extension: “dat”) from Icom website.

2 Insert the USB flash drive to the PC.

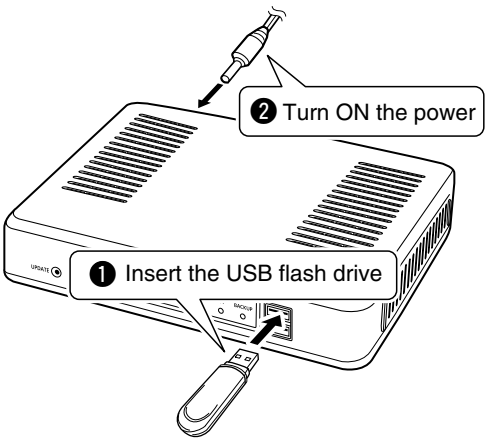
3 Select the root directory of the USB flash drive, and save the firmware file as “firmware.dat.“
- Any of other file name is not acceptable.

4 Remove the USB flash drive from the PC appropriately.

5 Prepare the SR-VPN1 to update the firmware.

6 Turn OFF the power.
Note: Turn OFF the SR-VPN1’s power, before inserting the USB flash drive.

7 Insert the USB flash drive to the [USB] port, and then turn ON the power.
- While transferring data, the [MSG] LED blinks.



NOTE:
- NEVER turn OFF the power until the updating has been completed. Otherwise, the SR-VPN1 may be damaged.
- Icom is not responsible on the consequence of the updating the firmware.

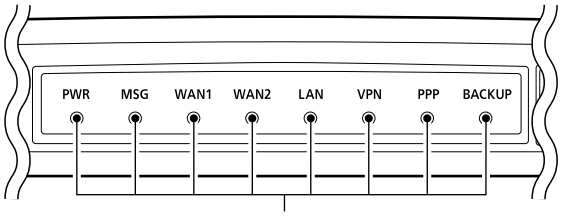
(Continued on the next page.)

7. How to update the firmware using a USB flash drive (continued)

Updating the firmware (continued)

8 All LEDs light while the firmware update is in progress.

Note: NEVER remove the USB flash drive or turn OFF the SR-VPN1's power

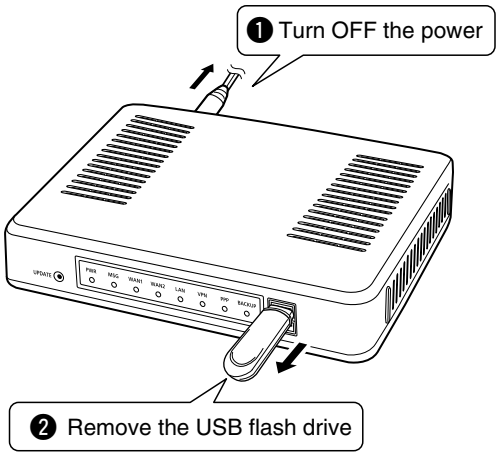


Lights in orange while updating the firmware.

9 When the update has been finished, the SR-VPN1 automatically reboots.

• After rebooting, verify that [PWR] lights green, and then turn OFF the power.

Note: NEVER remove the USB flash drive while the SR-VPN1's power is ON.



NOTE:
After the firmware updating is finished, check the firmware version on the setting screen to verify that the update was correctly done.

FOR YOUR INFORMATION

Section 7

1. Trouble shooting 7-2
2. How to connect to the SR-VPN1 using Telnet 7-4
   - ■ How to connect 7-4
   - ■ How to use the [CONSOLE] port 7-4
   - ■ About Telnet commands 7-4
   - ■ How to reset the protocol settings 7-4
5. Specifications 7-5
   - ■ General 7-5
   - ■ Communication Interfaces 7-5
   - ■ Networking 7-5

7 FOR YOUR INFORMATION

1. Trouble shooting

If the SR-VPN1 seems to be malfunctioning, please check the following before sending it to a service center.

The [PWR] LED does not light.

- **The AC adapter is not connected to the SR-VPN1.**
  - Verify that the AC adapter is securely connected.
- **The AC adapter is connected to the same AC outlet as the PC.**
  - Connect the AC adapter to a different AC outlet.

The [LAN] LED does not light.

- **The Ethernet cable is not properly connected to the SR-VPN1.**
  - Verify that the Ethernet cable is securely connected.
- **The HUB or PC is turned OFF.**
  - Turn ON the HUB or PC.

You cannot access the SR-VPN1's setting screen.

- **The PC's IP address is incorrect.**
  - Manually set the PC's IP address after you set the SR-VPN1 to the default setting.
- **The network part of PC's IP address is different from the SR-VPN1.**
  - Set the network part of PC's IP address to the same as the SR-VPN1.
- **A proxy server is used for the web browser setting.**
  - Set the web browser's proxy server setting to OFF.

The SR-VPN1's setting screen is not properly displayed.

- **The javascript or cookie functions are turned OFF.**
  - Set the javascript and cookie functions to ON.
- **Your browser is other than Microsoft Internet Explorer or the version is 8 or earlier.**
  - Use Microsoft Internet Explorer 9 or later.

Cannot connect to the Internet

- **The internet connection is currently out of service.**
  - Ask your ISP for the connection status.
- **The MAC address is not registered to your ISP.**
  - Some ISPs require WAN MAC address registration.
- **When using a Bridge modem or DCE (FTTH), the wrong connecting method is set.**
  - Ask your ISP for the connection type (DHCP Client, Static IP or PPPoE).
- **The broad band modem or DCE (FTTH) is not correctly connected to the SR-VPN1.**
  - If you use a Bridge modem or DCE (FTTH), select the connection type as specified by your ISP.

1. Trouble shooting (continued)

Cannot connect to the Internet (continued)

- **Failed to obtain a WAN IP address from the ISP.**
  - The obtained WAN IP address is displayed on the [TOP] screen.
- **The WAN line has been manually disconnected.**
  - To recover the connection, click <Connect> in the [Connection Status] item on the [WAN1]/[WAN2] screen.
- **The DNS server's IP is not correctly set.**
  - Check the DNS server setting in the [Router Settings] menu.

Cannot access the SR-VPN1's setting screen from WAN

- **The access is blocked by the default IP filter setting.**
  - Change the IP filter setting.
  - ⚠**Caution:** Icom is not responsible for the result of changing the IP filter setting.

Cannot establish a VPN connection

- **Cannot connect to the Internet.**
  - Check the network setting on the [WAN1]/[WAN2] port.
- **The IPsec function is disabled.**
  - Select "Enable" in the [IPsec Common Settings] item on the [VPN] screen. (☞P5-50)
- **The IPsec tunnel setting is wrong.**
  - Check the other SR-VPN1's WAN IP address (Host name), pre-shared key, LAN subnet, and so on.
  - Check the routes (☞5-53). (If the routes are incorrectly set, a VPN connection is successful but no communication is available.)
- **The IPsec connection is correctly set.**
  - Check the IPsec settings on the [IPsec (Detail)] screen.

2. How to connect to the SR-VPN1 using Telnet

For Windows® 7: Before performing the following procedure, turn ON [Telnet Client] on the [Turn Windows features on or off] window. ([Control Panel]>[Programs and Features]>[Turn Windows features on or off])

■ How to connect

①Start up Windows.
②Click the [Start] button, and then click [Run...].
Input “Telnet.exe” in the text box, and then click <OK>.
③The telnet screen appears, then input the appropriate address, as shown below.
Microsoft Telnet>open SR-VPN1's LAN IP address. (Example: open 192.168.0.1)
④Input login ID and password, then push [Enter].
login: admin
password: admin (The SR-VPN1's default password)
⑤When the telnet access is successful, “SR-VPN1 #” is displayed on the telnet screen.

■ How to use the [CONSOLE] port

The SR-VPN1 can be configured using a terminal software. (Optional OPC-1402 is required.)
Set the COM port as shown below, to communicate with the SR-VPN1.

COM port settings:

- COM port number: The port number which the optional OPC-1402 is connected to.
- Bits per second: 115200 (bps)
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

■ About Telnet commands

The following commands can be used for the Telnet function.

Command list …… Push the [Tab] key to display the telnet command list.
After typing a telnet command, push the [Tab] key to display the sub command list.

Command help …… After typing "help," enter a command to display the command description.
Example) "help save" ("save" command description is displayed.)

Automatic complement … After typing first few characters of the command, push the [Tab] key. The rest of the characters for the command are automatically entered.
Example) "n" + [Tab] -> network
Suggested commands are displayed.
Example) "res" + [Tab] -> **res**et **res**tart

■ How to re-enable HTTP (☞P5-73)

You can reset the protocol settings to access the setting screen.

①Type "SR-VPN1 **# network http on**" then push [Enter].
②Type "SR-VPN1 **# save**" then push [Enter].
③Type "SR-VPN1 **# restart**" then push [Enter].
④After rebooting, access the setting screen in your browser.

5. Specifications

Note: All specifications are the subject to change without notice.

General

Power supply:	DC12 V ±10% [Plug polarity: ⊖—◉—⊕] (Supplied AC adapter AC100 V ±10%) Less than 15 Watts
Usable condition:	Temperature; 0–40°C, Humidity; 5–95% (At no condensation)
Dimension:	Approximately 232 (W) × 38 (H) × 168 (D) mm; 9.1 (W) × 1.5 (H) × 6.6 (D) in (projections not included)
Weight:	Approximately 0.8 kg; 28 oz (without the supplied accessories)
Regulatory Compliance:	FCC Part15 Subpart B/Canada ICES-003 [USA-11] EN55022/EN55024/EN61000-3-2/EN61000-3-3 [EUR-12]
Interface:	LEDs; (PWR, MSG, WAN (1/2), LAN, VPN, PPP, BACKUP) Buttons; (UPDATE, INIT) [USB] port; (USB2.0) ×2

Communication Interfaces

Interface:	[WAN] port (RJ-45 type) × 2 (Auto MDI/MDI-X) • IEEE802.3/10BASE-T • IEEE802.3u/100BASE-TX • IEEE802.3ab/1000BASE-T [LAN] port (RJ-45 type) × 4 (Auto MDI/MDI-X) • IEEE802.3/10BASE-T • IEEE802.3u/100BASE-TX • IEEE802.3ab/1000BASE-T [CONSOLE] port (RJ-11 type) × 1 • RS-232C
Communication rate:	[WAN] port; 10/100/1000 Mbps (Automatic switching/Full duplex) [LAN] port; 10/100/1000 Mbps (Automatic switching/Full duplex)

Networking

IPv6:	Not supported (Only IPv4)
VPN:	IPsec IKEv1/IKEv2 (Main mode/Aggressive mode) AES128/192/256 3DES NAT Traversal Maximum number of tunnels; 32

Count on us!

A-7072-1EX

1-1-32 Kamiminami, Hirano-ku, Osaka 547-0003, Japan