ICOM

INSTRUCTION MANUAL

WIRELESS ACCESS POINT

AP-95M

IEEE802.11ac Wave 2 standard

Icom Inc.

INTRODUCTION

Thank you for choosing this Icom product. The AP-95M WIRELESS ACCESS POINT 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 AP-95M.
The AP-95M complies with the IEEE802.11ac Wave 2 standards, and enables you to communicate in dual bands.

- The 'IEEE802.11ac' standard can be used only on the 5 GHz band (Wireless 2).

ALL RIGHTS RESERVED. This document contains material protected under International and Domestic Copyright Laws and Treaties. Any unauthorized reprint or use of this material is prohibited. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without express written permission from Icom Incorporated.

All stated specifications and design are subject to change without notice or obligation.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.
Icom, Icom Inc. and the Icom logo are registered trademarks of Icom Incorporated (Japan) in Japan, the United States, the United Kingdom, Germany, France, Spain, Russia, Australia, New Zealand, and/or other countries.
All other products or brands are registered trademarks or trademarks of their respective holders.

INTRODUCTION

■ About the wireless LAN standards

The AP-95M’s wireless LAN standards and the maximum communication rates are shown in the table below.

NOTE: The bandwidth that can be used differs, depending on the country.

Frequency band	Wireless LAN standard	Bandwidth	Maximum communication rate (theory)
5 GHz	IEEE802.11ac	80 MHz	867 Mbps
		40 MHz	400 Mbps
		20 MHz	173 Mbps
	IEEE802.11n	40 MHz	300 Mbps
		20 MHz	144 Mbps
	IEEE802.11a		54 Mbps
2.4 GHz	IEEE802.11n	40 MHz	400 Mbps*
		20 MHz	173 Mbps*
	IEEE802.11g		54 Mbps
	IEEE802.11b		11 Mbps

*The client wireless LAN station must be compatible with 256QAM modulation.

About the Wireless LAN information

- The maximum communication rate is written based on the maximum theoretical rate of the IEEE802.11 wireless LAN standard, and is not the actual data communication rate.
- The actual data communication rate differs, depending on the condition in which the AP-95M is used, such as distance, obstacles, PC specifications, network vacancy, and so on.

The AP-95M’s wireless LAN standards and the maximum communication distance is shown in the table below.

The wireless communication distance differs, depending on the installed location, or the frequencies used. Refer to the table below as a reference.

Frequency band	Wireless LAN standard	Indoor	Outdoor*
5 GHz	IEEE802.11ac	Approximately 30 m: 32 yd	Approximately 100 m: 109 yd
	IEEE802.11n		
	IEEE802.11a		
2.4 GHz	IEEE802.11n	Approximately 30 m: 32 yd	Approximately 100 m: 109 yd
	IEEE802.11g		
	IEEE802.11b		

*This product has the frequency range approved only for indoor use. Follow the restrictions of the laws and regulations of each country.

■ About the wireless LAN standards (Continued)

Bandwidth and Channel

The AP-95M has 2 wireless LAN units inside: 2.4 GHz band (Wireless 1) and 5 GHz band (Wireless 2).
Set the desired "Channel" and "Bandwidth."

- When setting multiple access points with the 80 MHz bandwidth on 5 GHz, or 20/40 MHz bandwidth on 2.4 GHz, set the channels away from each other, to prevent signal interference.

Frequency band	Bandwidth
5 GHz	80 MHz
	40 MHz
	20 MHz
2.4 GHz	40 MHz
	20 MHz

INTRODUCTION

■ Features

- ➥ A communication can be made at the maximum rate of 867 Mbps (theoretical) based on the [IEEE802.11ac] and the [IEEE802.11n] standards.
  - • The [IEEE802.11ac] standard can only be used for Wireless 2 (5 GHz band).
  - • The [IEEE802.11ac] and the [IEEE802.11n] standards are enabled when “None” or “AES” are set for “Encryption.”
- ➥ Dual band communications using the 5 GHz and 2.4 GHz bands can be made, based on the [IEEE802.11a] and the [IEEE802.11b/g] standards.
- ➥ To use multiple wireless devices that are based on different wireless LAN standards at the same time, protection mechanisms are built into the AP-95M, for communication rate maintenance.
- ➥ The authentication system supports “Open System,” “Shared Key,” “IEEE802.1X,” “WPA,” “WPA2,” “WPA-PSK,” and “WPA2-PSK.”
- ➥ If “IEEE802.1X,” “WPA” or “WPA2” is selected, the RADIUS authentication server can be used.
- ➥ Web authentication function, which authorizes wireless LAN stations, is built into the AP-95M.
- ➥ The AP-95M complies with the Power over Ethernet (PoE) power reception function based on the [IEEE802.3af] standard. Therefore, power can be received using a HUB (user supplied) that supports the [IEEE802.3af] standard.
- ➥ With the function that the “Wi-Fi Alliance” proposes, SSID and Security (WPA-PSK/WPA2-PSK) can automatically be set to the AP-95M (virtual AP) and the wireless LAN station that supports the Wi-Fi Protected Setup (WPS) function.
  - • This device is not certified by the Wi-Fi alliance. (As of November 2018)
- ➥ Supports the 10BASE-T/100BASE-TX/1000BASE-T automatic switching function.
- ➥ Auto MDI/MDI-X system for the port polarity.
- ➥ Supports the SNMP system for the network management.
- ➥ No license nor certificate is needed to use this product.

■ About default settings

Menu	Setting screen	Setting	Title	Default setting
Network Settings	IP Address	IP Address	IP Address	192.168.0.1
			Subnet Mask	255.255.255.0
	DHCP Server	DHCP Server	DHCP Server	Disable
Wireless Settings	Wireless LAN	Wireless LAN	Channel	001CH (2412 MHz) (Wireless 1)
				036CH (5180 MHz) (Wireless 2)
			Bandwidth	20 MHz
	Virtual AP	Virtual AP	Interface	ath0 (Wireless 1)
				ath1 (Wireless 2)
			SSID	WIRELESSLAN-0
		Security	Authentication	Open System/Shared Key
			Encryption	None
Management	Administrator	Administrator Password	Username	admin (Cannot be changed)
			Current Password	admin (Lower case letters)

To prevent unauthorized access

You must carefully chose your password, and change it occasionally.

- Choose one that is not easy to guess.
- Use numbers, characters and letters (both lower and upper case).

■ Setting procedures

Follow the procedures below to set up the AP-95M.

1 Main functions ☞p.1-4 ~

↓

2 Installation ☞p.1-10 ~

↓

3 Wireless communication settings ☞p.2-2 ~

↓

4 Date, time and other settings ☞p.3-119 ~

↓

5 Checking and saving the settings ☞p.4-2 ~

↓

6 Restoring the factory defaults ☞p.4-4 ~

↓

7 Troubleshooting ☞p.5-2 ~

TABLE OF CONTENTS

Section 1 BEFORE USING THE AP-95M

Section 2 PREPARATION

Section 3 SETTING SCREEN

Section 3 SETTING SCREEN

Section 3 SETTING SCREEN

TABLE OF CONTENTS

Section 4 MAINTENANCE

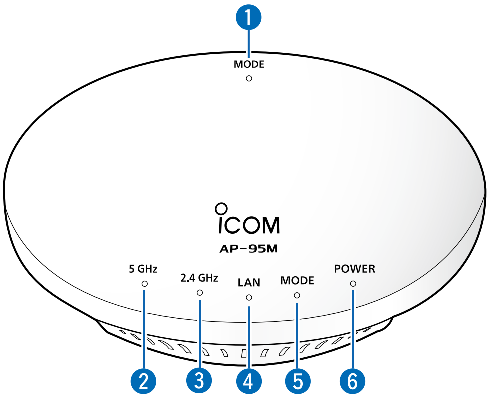
Section 5 INFORMATION

BEFORE USING THE AP-95M

Section 1

1. Panel description

■ Top panel



① MODE button .... Used to reset the AP-95M to its default settings. (p. 4-4)
• We recommend that you use a pen to hold down this button.

② 5GHz ....

●	Lights green:	1 or more unit (5 GHz) connection*/WPS succeeded.
	No light:	Condition other than above.

③ 2.4GHz ....

●	Lights green:	1 or more unit (2.4 GHz) connection*/WPS succeeded.
	No light:	Condition other than above.

④ LAN ....

●	Lights green:	LAN is connected (1000BASE-T)
☼	Blinks green:	LAN is communicating (1000BASE-T)
●	Lights orange:	LAN is connected (10BASE-T/100BASE-TX)
☼	Blinks orange:	LAN is communicating (10BASE-T/100BASE-TX)
	No light:	Condition other than above.

⑤ MODE ....

●	Lights green:	The [MODE] button is hold down.
☼	Blinks green:	WPS is running.
●	Lights orange:	A firmware update is ready (Online update).
☼	Blinks orange:	WPS failed. (Turns OFF after 30 seconds passed)
	No light:	Condition other than above.

⑥ POWER.....................

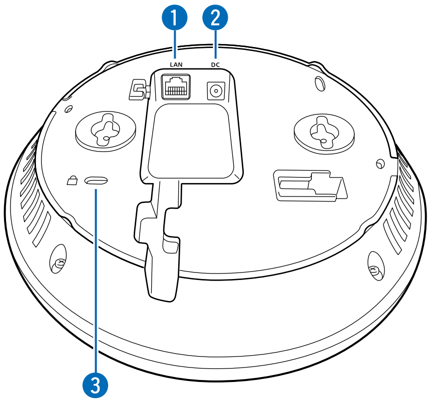
●	Lights green:	Power is ON.
☼	Blinks green:	Firmware loading.
	No light:	Condition other than above.

*When there is no wireless LAN station to connect with the AP-95M, or no wireless communication is made while “Wireless Unit” is enabled, these indicators will turn OFF. The time when the LED turns OFF differs, depending on the communication status.

NOTE:
When the LED function is enabled, all LED indicators are OFF. (Default: Disable)

1. Panel description

Rear panel/Back side



❶ [LAN] port (RJ-45 type) Connect to network devices such as a network switch (HUB). (p. 3-45)

- If the power is supplied through PoE, connect a HUB (IEEE802.3af) regardless of the connection type.
- When "LAN port" (Default) is selected as the Connection type:
  Used as a LAN port that accepts network devices such as HUB (VLAN switch, and so on.) or router modem.
- When "DHCP Client," "Static IP" or "PPPoE":
  Used as a WAN port that accepts a bridge modem (ADSL, VDSL, CATV) or ONU (Optical Network Unit).

❷ DC jack .... Connect to the supplied or optional power adapter.

- When you use the power from the Ethernet cable (PoE), you do not need a separate power adapter.

❸ Security slot .... Attach a security wire (user supplied).
Refer to the instruction manual that comes with the security wire for details.

2. Main functions

■ Access Point function

The AP-95M is a wireless access point that complies with the “IEEE802.11ac” and “IEEE802.11n” standards. It is designed for dual band communications in the 2.4 GHz and 5 GHz bands.

■ Wireless LAN (SSID)

SSIDs are set to AP-95M and wireless LAN stations, to distinguish (groups) the wireless network. (p. 2-2)

- The AP-95M is equipped with 2 wireless LAN units. When using multiple virtual APs, the same SSIDs cannot be set in a wireless LAN unit.

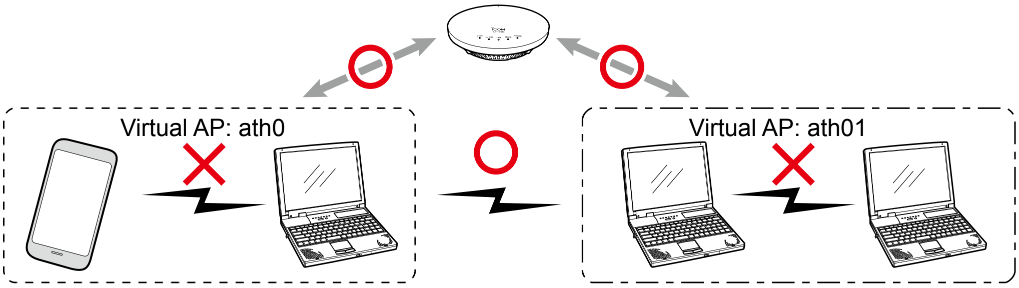
■ Maximum Number of Stations

This function limits the number of wireless LAN stations that can be connected at a time to each Virtual AP. This prevents the communication traffic speed from being reducing. (p. 3-70)

■ Privacy Separator

This function blocks the communication between wireless LAN stations that use the same virtual AP.

- If this function is set to "Enable," all communications between wireless devices in the same Virtual AP are inhibited. (p. 3-70)
- To inhibit the communication between wireless devices that are in a different virtual AP, set the Packet Filter function (p. 3-20).



■ ‘IEEE802.11ac’ standard

With data communication using a quadruple frequency bandwidth (channel) and multiple antennas, communication with a maximum speed of 867 Mbps* (theoretical value) can be made.

* The ‘IEEE802.11ac’ standard can be used only when Encryption is set to “None” or “AES.”
The ‘IEEE802.11ac’ standard can be used only on the 5 GHz band (Wireless 2).
In addition, the Bandwidth must be set to “80 MHz” to use the maximum 867 Mbps. (p. 2-11)

- The ‘IEEE802.11ac’ is compatible with the ‘IEEE802.11n/a’ standard.

■ ‘IEEE802.11n’ standard

With data communication using a double frequency bandwidth (channel) and multiple antennas, communication with a maximum speed of 400 Mbps* (theoretical value) can be made.

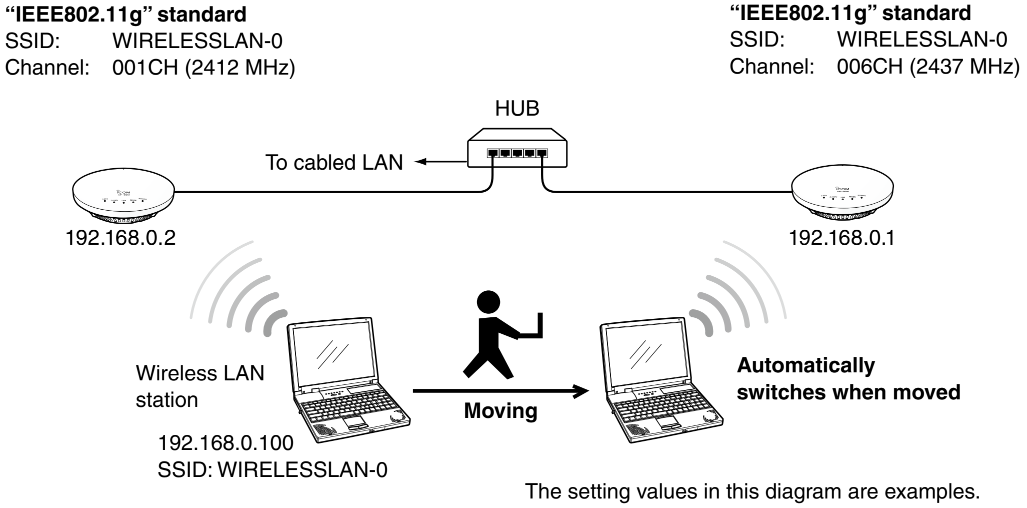
* The ‘IEEE802.11n’ standard can be used only when Encryption is set to “None” or “AES.”
In addition, the client wireless LAN station must be compatible with 256QAM modulation, and the Bandwidth must be set to “40 MHz” to use the maximum of 400 Mbps. (p. 2-11)

- The ‘IEEE802.11n’ is compatible with the ‘IEEE802.11a/b/g’ standard.

2. Main functions

■ Roaming function

Even if you moved a wireless LAN station, this function enables a wireless LAN station to automatically switch to the access point (AP-95M) with the best signal. This enables you to use the wireless LAN station in larger areas.



The setting values in this diagram are examples.

Using the roaming function

- Set the identical SSID, security settings to both the AP-95M and the wireless LAN station.
- When using this function in a area that many wireless LAN devices are used, set a channel where there is no interference, or set "Automatic" for "Channel" in the Wireless LAN screen.
  In the wireless LAN standard (IEEE802.11g) used in the example above, set more than 4 channels between access points.
  ➥ Set the roaming threshold value on the wireless LAN station according to the equipment used.

Using the Beam Forming function and MU-MIMO function

The Beam Forming function sends the signal in the direction of the device that it will communicate with.
The MU-MIMO function provides concurrent communications with plural wireless devices without interference.

2. Main functions

■ Wireless Bridge function

The wireless bridging function enables you to connect Icom’s wireless access points together.
• The access point that can communicate with differs, depending on the integrated wireless LAN unit.

<Compatibility table> (As of January 2019)

AP-95M's Wireless LAN unit	Band	AP-90M	AP-95M
Wireless 1 (WBR)	2.4 GHz	Yes (Wireless 2 (WBR))	Yes
Wireless 2 (WBR)	5 GHz	Yes (Wireless 2 (WBR))	Yes

• AP-90M's Wireless 1 (WDS) and AP-95M's Wireless 1/2 (WBR) do not communicate each other.

➥ If the channel is set to "Automatic" (p. 2-10), the wireless Bridge function cannot be used.
➥ Set the virtual AP (ath0 or ath1) on the master side, and then build a star-shaped network.
  • Multiple clients can be connected to the master.
  • A client can only be connected to one master.
➥ Check the client’s “BSSID” on the “Wireless Bridging (WBR)” screen, and then enter in the “Peer BSSID” field.
  • A maximum of 8 clients can be registered to the master.
  • The master’s SSID and security settings can be set on the “Virtual AP” screen.
➥ The client scans the matching SSID and security settings.
  • Set the master’s SSID and security settings on the client’s “Wireless Bridging” screen.

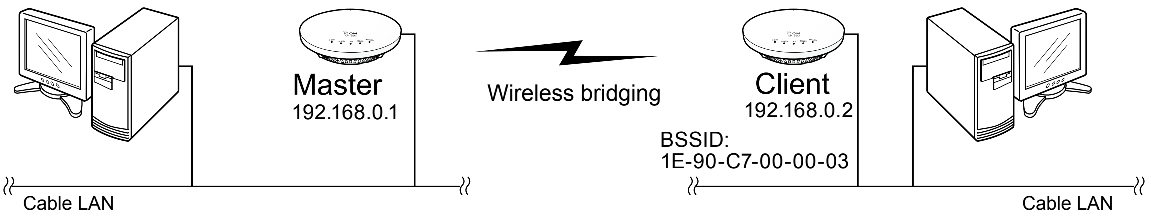
Master settings

Channel:	001CH (2412 MHz)
Virtual AP:	ath0
SSID:	WIRELESSLAN-0
Authentication:	WPA2-PSK
Encryption:	AES
PSK:	wirelessmaster
BSSID:	1E-90-C7-00-00-03 (Client BSSID)

Client settings

SSID:	WIRELESSLAN-0
Authentication:	WPA2-PSK
Encryption:	AES
PSK:	wirelessmaster

• These values are examples.



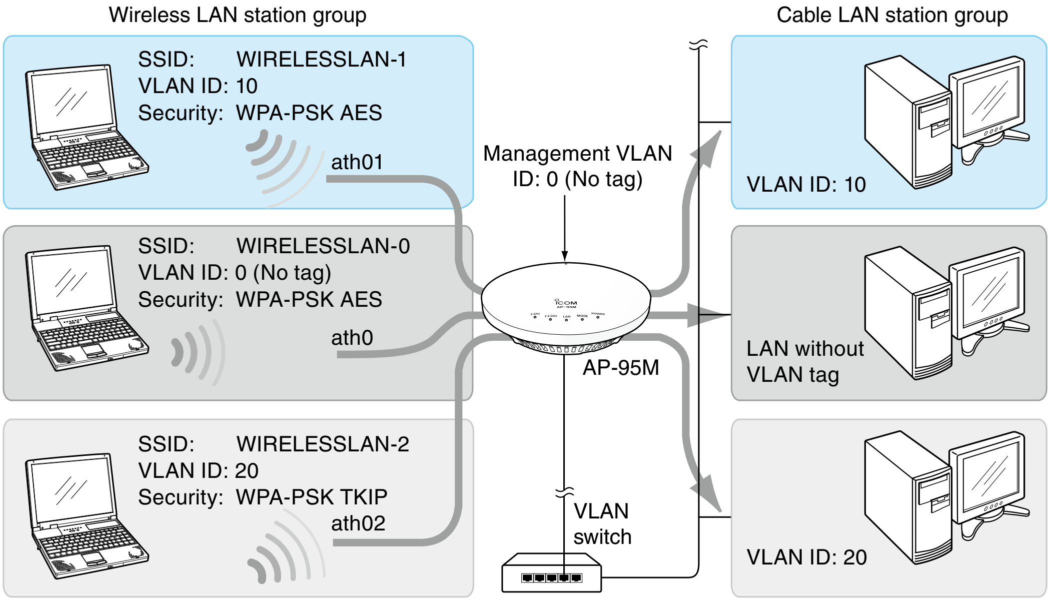
• The client side automatically changes to Master channels.
• When the AP-95M operates as a client, the channel and WMM Advanced settings are invalid.
• If there are multiple masters, the master to connect will depend on the radio signal strength.
• Roaming will not be performed unless the signal is cut off, even if the signal strength is changed.

2. Main functions

■ Virtual AP function

With an AP-95M, you can make multiple wireless station groups by their settings (SSID/Security/VLAN ID).

- The VLAN function and Router function cannot be used at the same time.
- The illustration below is an example of using “ath0,” “ath01” and “ath02” for different wireless station groups’ virtual AP.
- To prevent lower a communication rate, using Wireless 1 and Wireless 2 (for each) with 4 or fewer Virtual APs is recommended.



Using the Virtual AP function

➥ Using a Virtual AP*, you can create a wireless network with up to 16 groups.
  * If you want to create an IEEE802.11ac standard wireless network, set the Virtual AP (ath1, ath11 to ath17) on the “Virtual AP” screen of Wireless 2 (5 GHz band).

➥ When using multiple Virtual AP functions, the same [SSID] cannot be set to Virtual APs on both wireless LAN units.

➥ You can set VLAN IDs (0 to 4094) to the virtual AP’s wireless station groups.

➥ [Management VLAN ID] is set to “0” as the default. Therefore, you cannot access the setting screen from the network with the VLAN ID set other than "0" (default).

2. Main functions

About the Router function

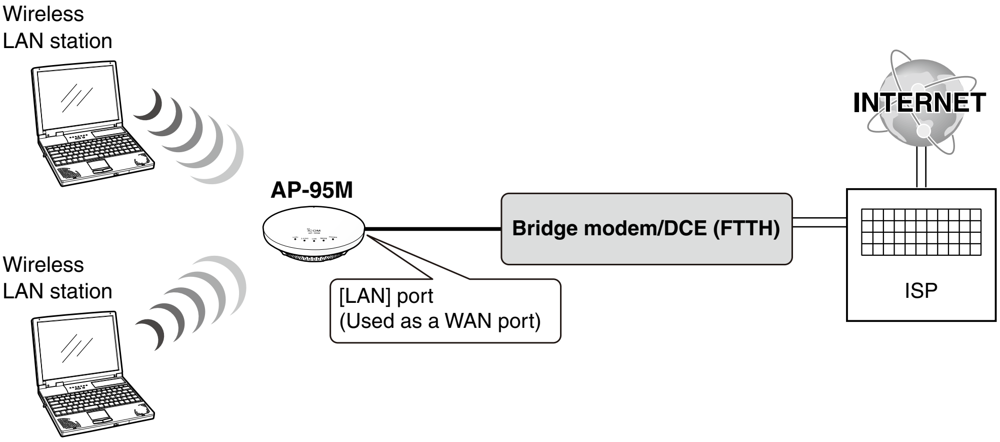
The AP-95M has a router function that enables the wireless devices on the LAN to access the internet.

- The [Connection Type] item is set to "LAN Port" as the default.
  If your modem is a router modem, the AP-95M's Router function is not necessary. Set the [Connection Type] item to "LAN Port."
- Ask your Internet provider (ISP) for the connection type.

[Connecting a Bridge modem]

Select the Connection Type (DHCP client/PPPoE/Static IP) as specified by your ISP, and then connect a modem (ADSL, VDSL, CATV) or ONU (Optical Network Unit) to the [LAN] port.

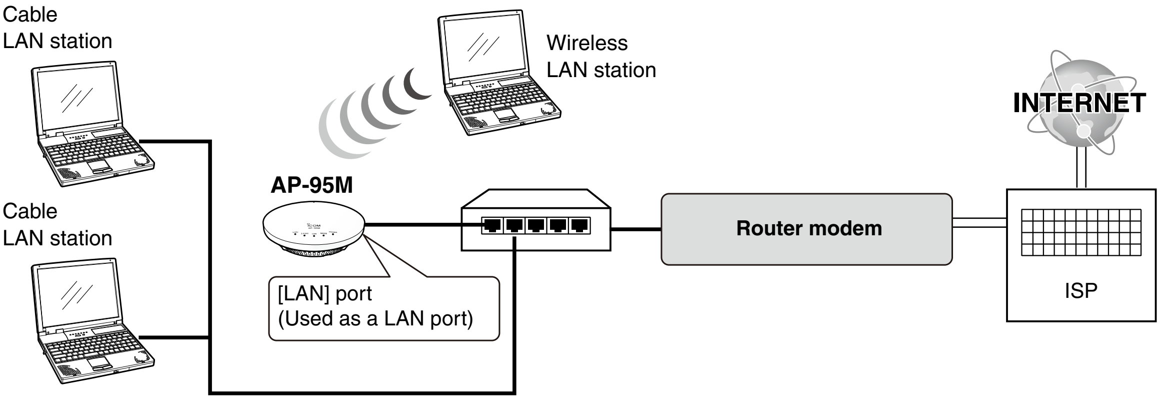
- The [LAN] port can be used as a WAN port.



[Connecting a Router modem]

Connect a router modem to the [LAN] port.
Select LAN Port for the Connection Type.

- The [LAN] port can be used as a LAN port.



2. Main functions

■ WPS function

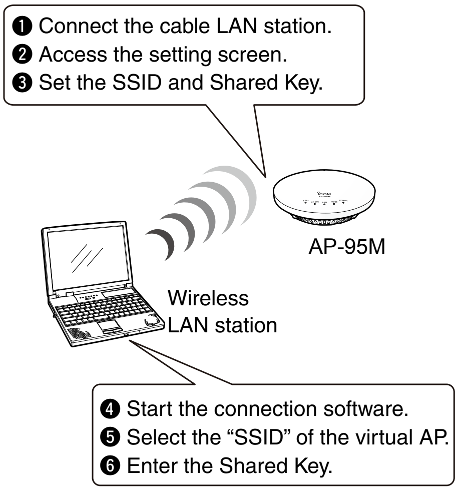
With the function that the “Wi-Fi Alliance” proposed, SSID and Security (WPA-PSK/WPA2-PSK) can automatically be set to the wireless LAN station that supports the WPS (Wi-Fi Protected Setup) function.

• To automatically set it and start the WPS function, select either of the following methods.

➥ Clicking <Start> on the setting screen. (p. 2-12)
(Push Button)

➥ Setting the communicator’s PIN code.
(PIN (Personal Identification Number))

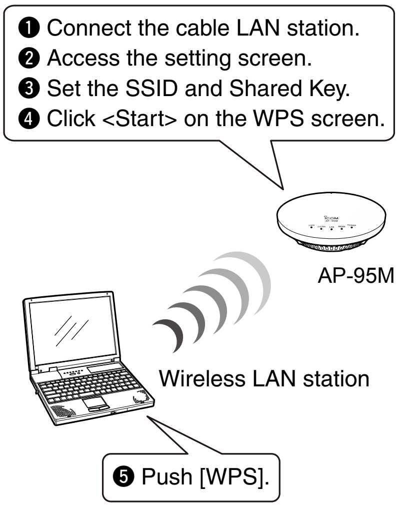
Not using the WPS function



❶ Connect the cable LAN station.
❷ Access the setting screen.
❸ Set the SSID and Shared Key.

❹ Start the connection software.
❺ Select the “SSID” of the virtual AP.
❻ Enter the Shared Key.

Using the WPS function



❶ Connect the cable LAN station.
❷ Access the setting screen.
❸ Set the SSID and Shared Key.
❹ Click <Start> on the WPS screen.

❺ Push [WPS].

Using the WPS function

➥ Use a wireless LAN station that supports the WPS function.

➥ If your wireless LAN station has no [WPS] button, use the application that supports WPS, or a regular wireless network connection using Windows (Windows 7 or later).

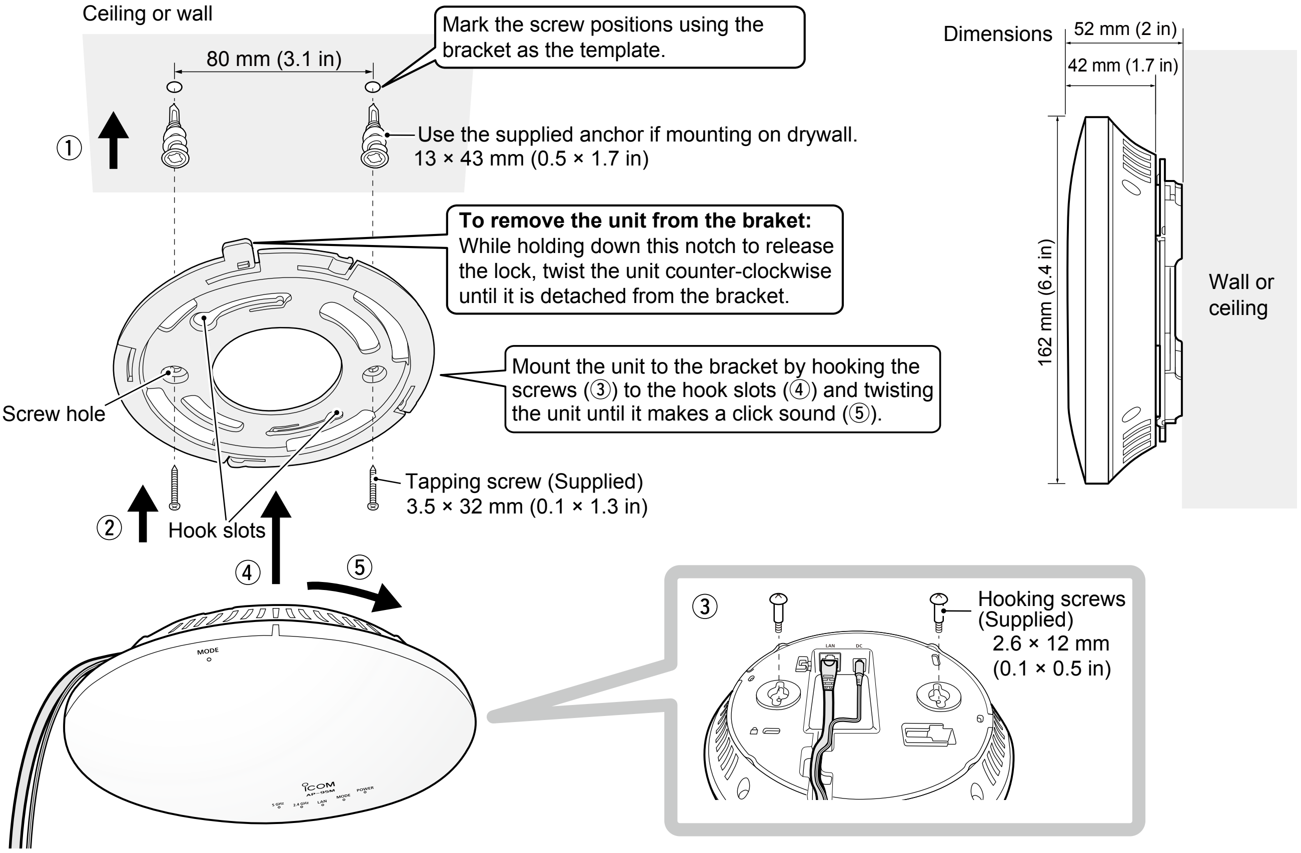
➥ Enable and set the SSID and security to the virtual AP and select it as “Interface” to use the WPS function. (p. 3-70)
If you select an invalid virtual AP for “Interface,” the WPS function cannot be used.

3. Installation

This product radiates or receives radio wave from its top surface, so we recommend mounting on a wall or ceiling.
You can mount on the wall or ceiling using the supplied bracket, by following procedure ① to ⑤ below.

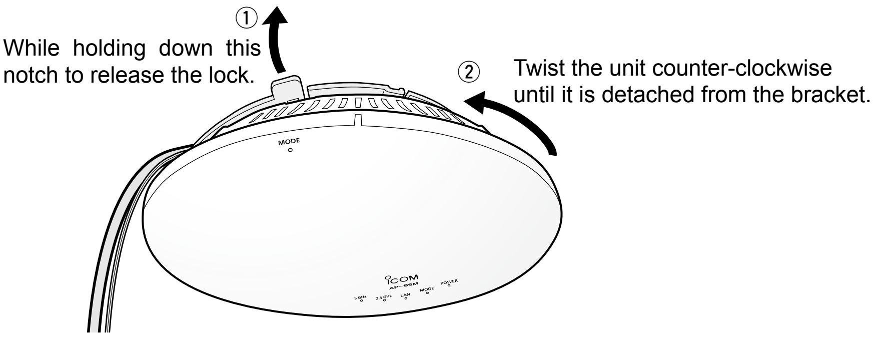
ⓘ To use the security wire, refer to the instruction manual on our website.

⚠DANGER!
Mount the unit securely to a thick surface that can support more than 600 g (1.3 lb).


Ceiling or wall
80 mm (3.1 in)
Mark the screw positions using the bracket as the template.
①
Use the supplied anchor if mounting on drywall.
13 × 43 mm (0.5 × 1.7 in)
To remove the unit from the braket:
While holding down this notch to release the lock, twist the unit counter-clockwise until it is detached from the bracket.
Mount the unit to the bracket by hooking the screws (③) to the hook slots (④) and twisting the unit until it makes a click sound (⑤).
Screw hole
Tapping screw (Supplied)
3.5 × 32 mm (0.1 × 1.3 in)
②
Hook slots
④
⑤
MODE
ICOM
AP-95M
5 GHz 2.4 GHz LAN MODE POWER
③
Hooking screws (Supplied)
2.6 × 12 mm
(0.1 × 0.5 in)
LAN DC
Dimensions
52 mm (2 in)
42 mm (1.7 in)
162 mm (6.4 in)
Wall or ceiling

To remove the unit from the bracket:

Be careful of not to break your finger nail.

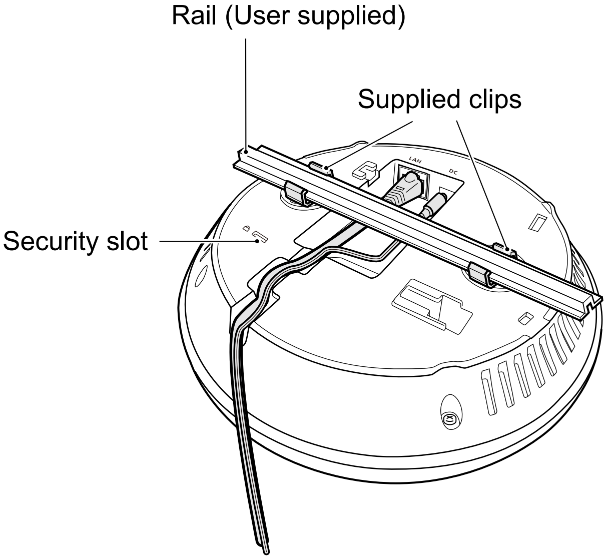

①
While holding down this notch to release the lock.
②
Twist the unit counter-clockwise until it is detached from the bracket.
MODE
ICOM
AP-95M
5 GHz 2.4 GHz LAN MODE POWER

3. Installation

■ Installing the AP-95M on a rail

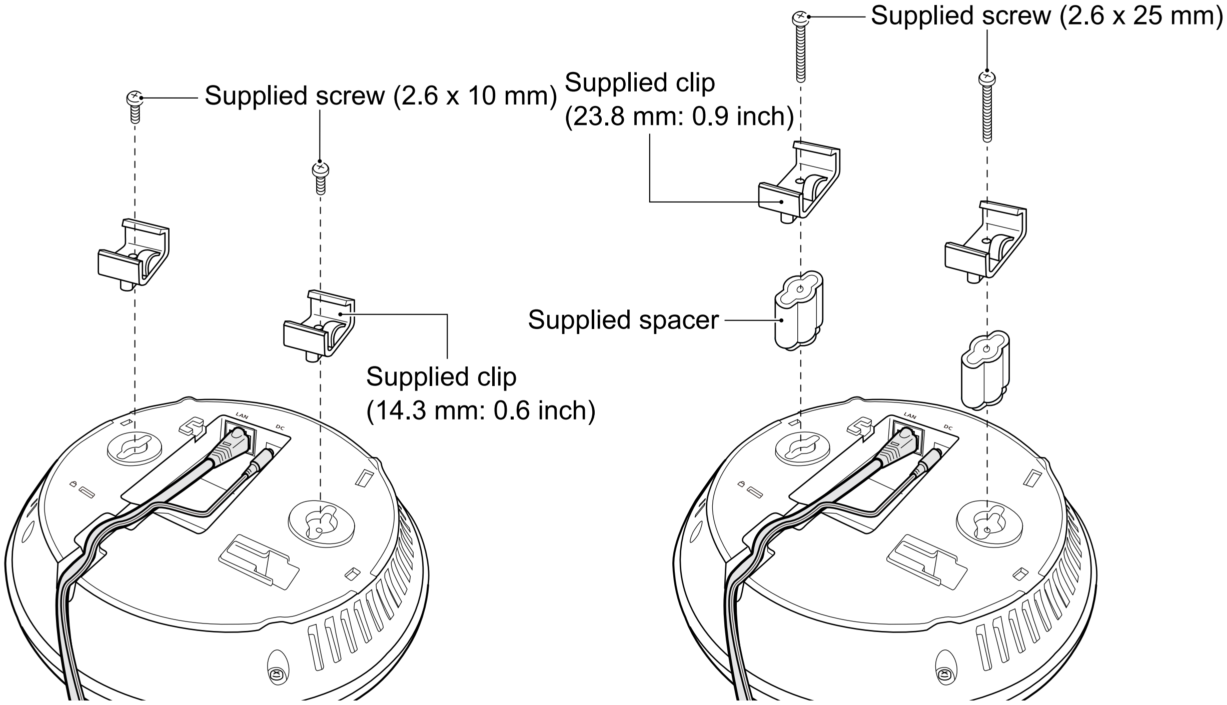
The supplied rail clip enables you to install the AP-95M to a rail.
Attach rails clips to the AP-95M's bottom panel, then push them into the rail until it makes a click sound.

- If you attach a security wire (user supplied), attach the AP-95M to a rail in advance.



Attaching rail clips:

2 types of rail clips are supplied with the AP-95M. Use the appropriate type according to the rail to attach the AP-95M. The supplied spacers can be used to make a gap between the AP-95M and the ceiling.



4. Setting

Setting a static IP address to a PC

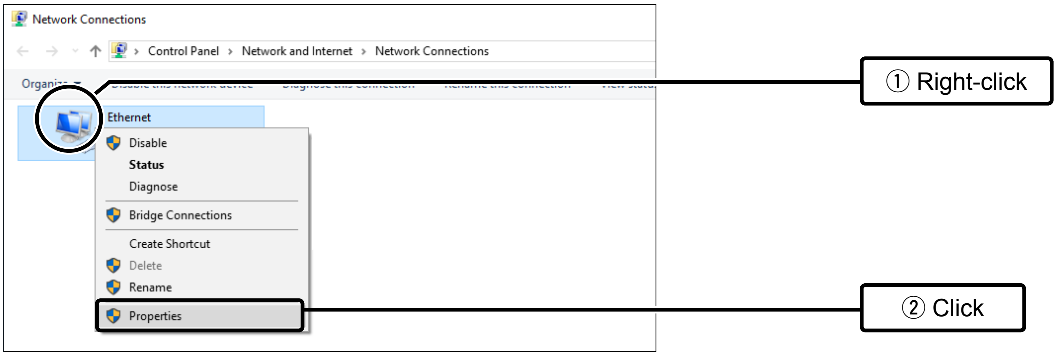
The following procedures describe how to set a static IP address (example: 192.168.0.100), based on Microsoft Windows 10.
The AP-95M’s IP address is set to “192.168.0.1,” and the DHCP server is set to “Disable,” as the default.

1 Click [Start] (Windows logo) and then click [Control Panel].

2 In the [Control Panel] window, click [Network and Internet] and then click [Network and Sharing Center].

3 Click [Change adapter settings].

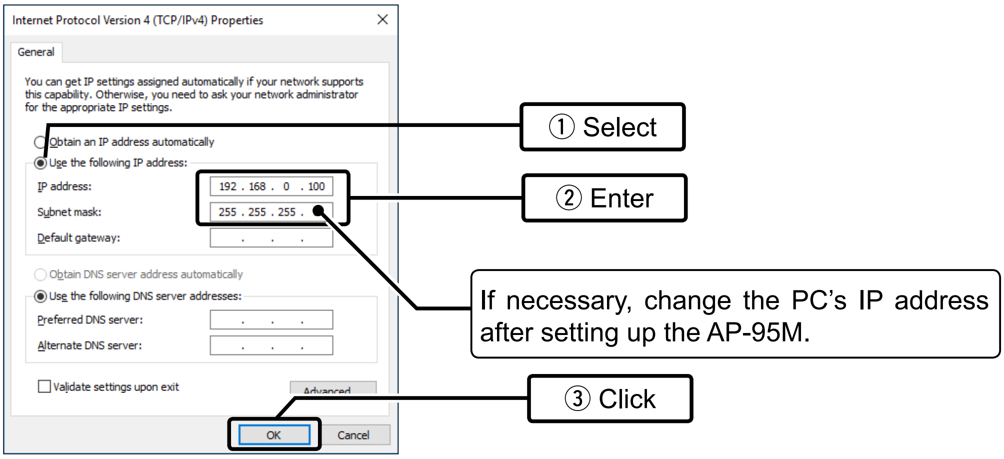
4 Right-click [Local Area Connection] (cable LAN station) or [Wireless Network Connection] (wireless LAN station), and then click [Properties] in the displayed menu list.



5 If the [User Account Control] message appears, click [Yes] to continue.

6 In the [Local Area Connection Properties] (for a cable LAN station) or the [Wireless Network Connection Properties] (for a wireless LAN station) screen, select “Internet Protocol Version 4 (TCP/IPv4),” and then click [Properties].
The “Internet Protocol Version 4 (TCP/IPv4) Properties” screen is displayed.

7 Select “Use the following IP address” and enter the IP address (example: 192.168.0.100) and the Subnet mask (example: 255.255.255.0), and then click [OK].



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 0 . 100
Subnet mask: 255 . 255 . 255 .
Default gateway: . . .
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .
□ Validate settings upon exit

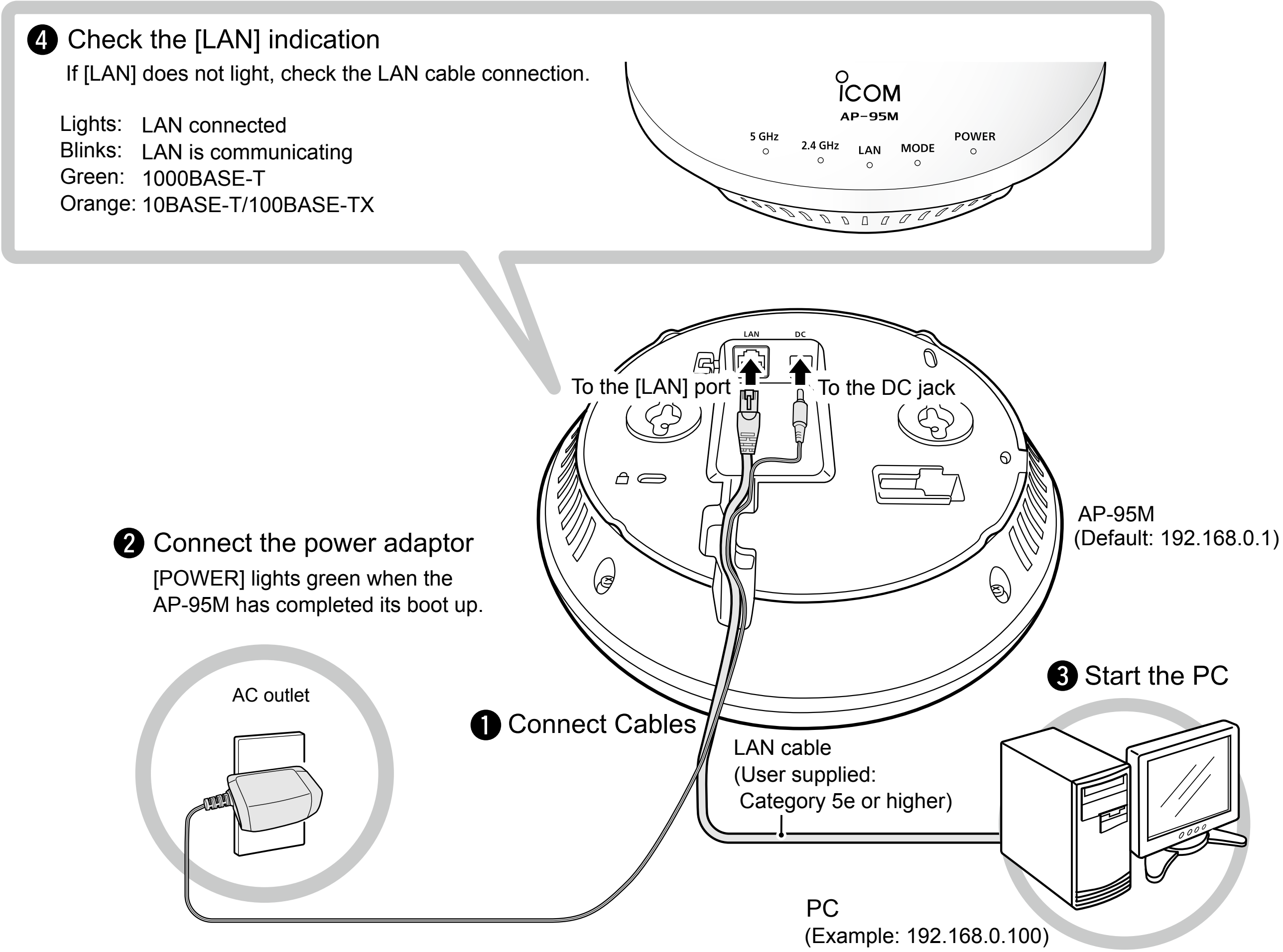
If necessary, change the PC’s IP address after setting up the AP-95M.

8 Close the window.

4. Setting

■ Connecting a PC

• When using a Cable LAN device:
Follow the procedures ❶ to ❹ to connect with the AP-95M, and check the indications described below.



❹ Check the [LAN] indication

If [LAN] does not light, check the LAN cable connection.

Lights:	LAN connected
Blinks:	LAN is communicating
Green:	1000BASE-T
Orange:	10BASE-T/100BASE-TX

❷ Connect the power adaptor

[POWER] lights green when the AP-95M has completed its boot up.

❶ Connect Cables

❸ Start the PC

LAN cable
(User supplied:
Category 5e or higher)

AP-95M
(Default: 192.168.0.1)

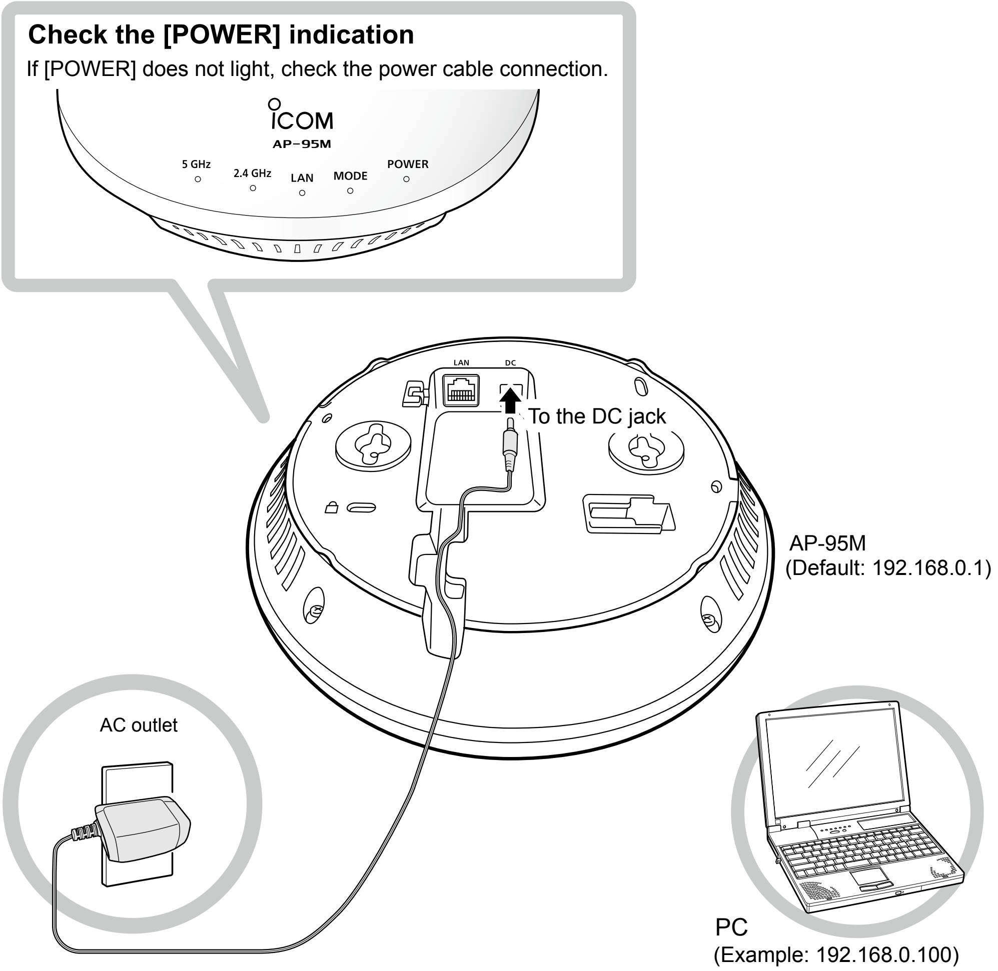
PC
(Example: 192.168.0.100)

4. Setting

Connecting a PC

• When using a Wireless LAN device:

1 Turn ON the AP-95M's power.

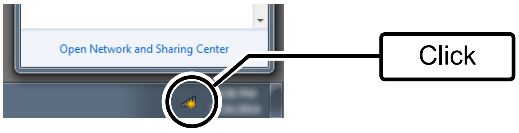


Check the [POWER] indication

If [POWER] does not light, check the power cable connection.

2 Click the wireless network connection icon on the PC.

• It may take a few minutes until the icon appears.

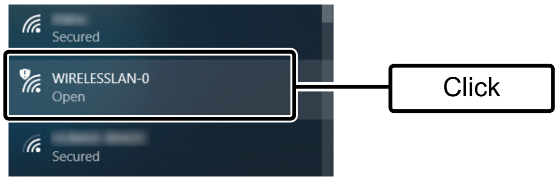


4. Setting

■ Connecting a PC

• When using a Wireless LAN device:

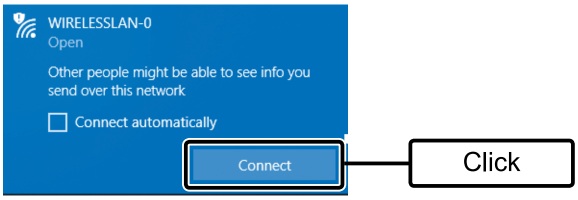
3 Select the SSID assigned to the AP-95M (example: WIRELESSLAN-0) and click [Connect].
• “Connect to a Network” is displayed.



Secured

WIRELESSLAN-0
Open

Secured

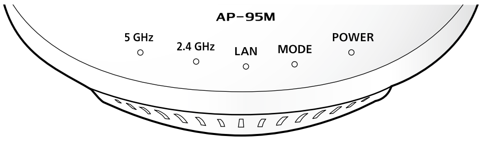


WIRELESSLAN-0
Open

Other people might be able to see info you send over this network

□ Connect automatically

4 The setting is completed when [5GHz] or [2.4GHz] lights green ●.



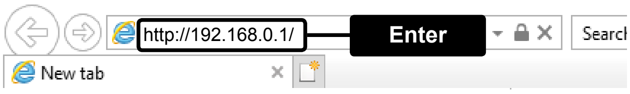
(Continued on the next page.)

4. Setting

Accessing the setting screen

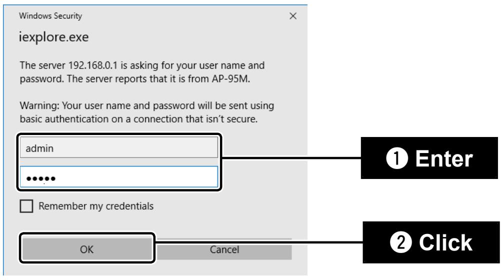
- The following procedures describe how to use the AP-95M setting screen using a web browser.

1 Open your web browser, then enter the IP address* of the AP-95M into the address bar.



*The default IP address is “192.168.0.1.”

2 Push the [ENTER] key.
- The Login Authentication screen will appear.


Windows Security

iexplore.exe

The server 192.168.0.1 is asking for your user name and password. The server reports that it is from AP-95M.

Warning: Your user name and password will be sent using basic authentication on a connection that isn’t secure.

admin

•••••

□ Remember my credentials

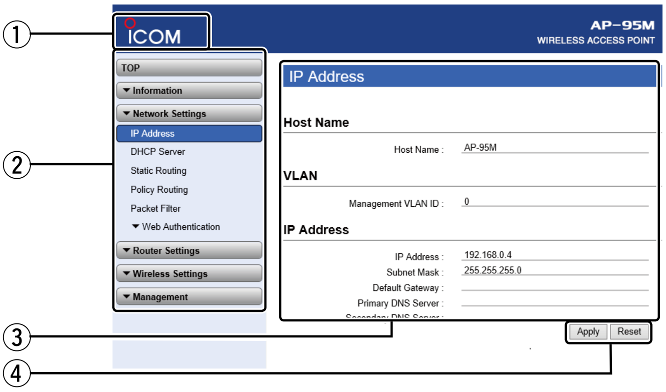
3 Enter “admin” (fixed username) and “admin” (default password) in their respective input fields in the Login Authentication window, and then click [OK].

- When accessing the web browser for the first time, setting the time zone is required. (Setting country is also required only in Europe.) See the “Setting the Time Zone and Country” leaflet for details.

4. Setting

Accessing the setting screen

- When using a Wireless LAN device:



IP Address

Host Name

Host Name : AP-95M

VLAN

Management VLAN ID : 0

IP Address

IP Address : 192.168.0.4

Subnet Mask : 255.255.255.0

Default Gateway :

Primary DNS Server :

Secondary DNS Server :

① Link to the Icom web site

If your PC is connected to the Internet, click the Icom logo to open the Icom web site.

② Setting menu

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

③ Setting screen

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

④ Setting buttons

Save or cancel the setting values.

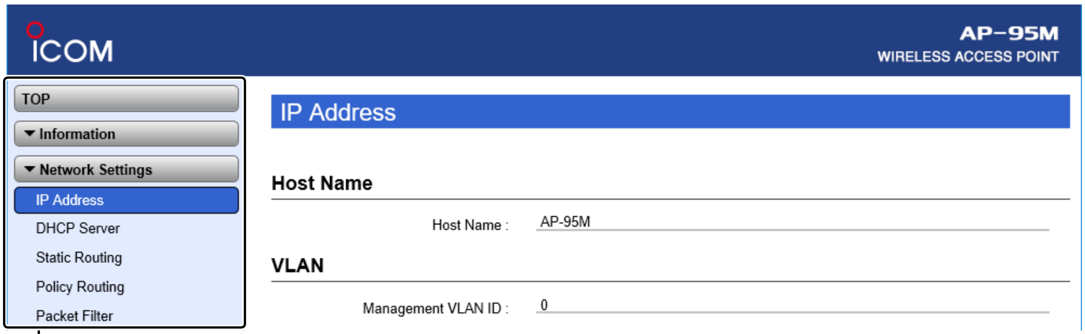
- Items and buttons may differ, depending on the setting.

4. Setting

■ About the setting screen layout

The screen automatically re-sized and aligned according to the web browser window size.
You can adjust the window size, depending on your PC screen size.

Screen size: Large



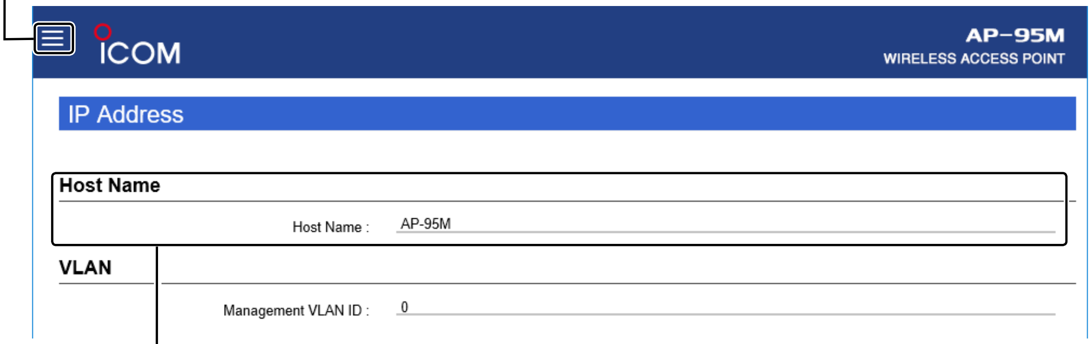
Host Name

Host Name : AP-95M

VLAN

Management VLAN ID : 0

Screen size: Middle



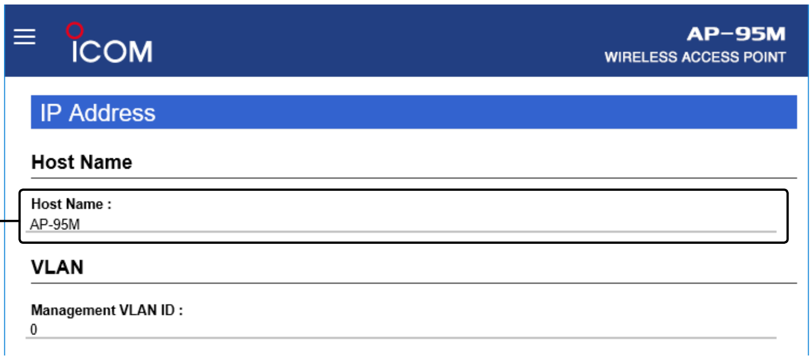
Host Name

Host Name : AP-95M

VLAN

Management VLAN ID : 0

Screen size: Small



Host Name

Host Name :
AP-95M

VLAN

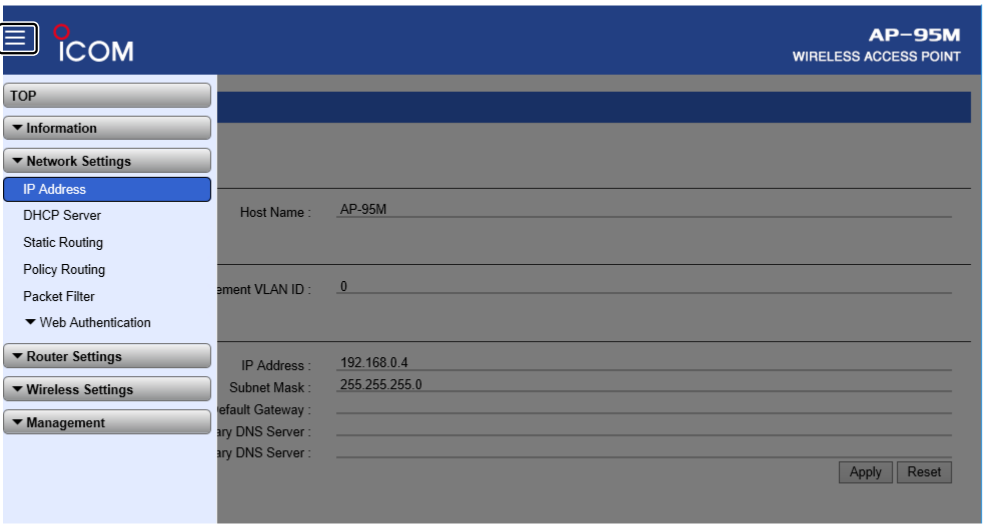
Management VLAN ID :
0

4. Setting

■ About the setting screen layout

The hidden menu appears by clicking "☰."

Click



Host Name : AP-95M

ement VLAN ID : 0

IP Address : 192.168.0.4

Subnet Mask : 255.255.255.0

efault Gateway :

ary DNS Server :

ary DNS Server :

4. Setting

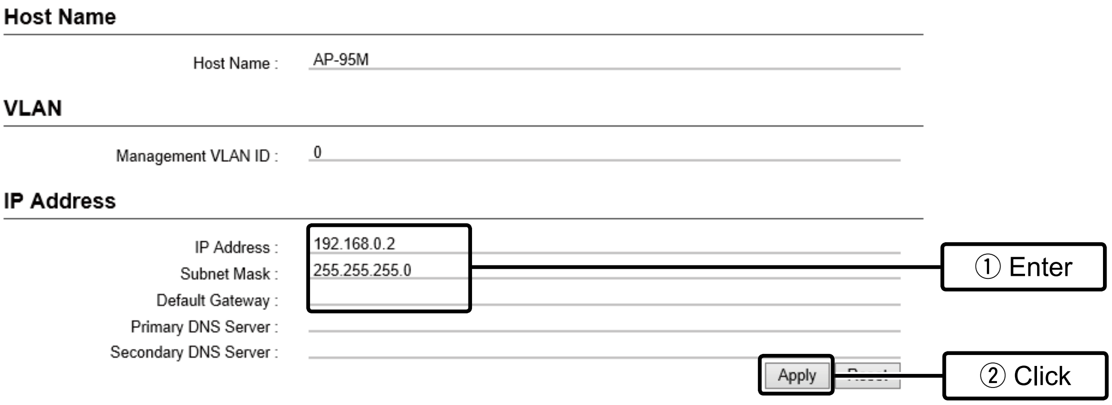
Network Settings > IP Address > IP Address

■ Changing the IP address

Make sure the AP-95M’s IP address is not the same as other network device’s address.

1 Click [Network Settings], and then click [IP Address].

2 In the “IP Address” screen, change the “IP Address” settings and then click [Apply].
- The changes are saved.



Host Name

Host Name : AP-95M

VLAN

Management VLAN ID : 0

IP Address

IP Address : 192.168.0.2
Subnet Mask : 255.255.255.0
Default Gateway :
Primary DNS Server :
Secondary DNS Server :

① Enter

② Click

- If you have changed the “Network (example: 192.168.0)” digits on the AP-95M’s IP address, also change the PC’s network digits on the IP address to the same value.

IP Address assigning
An IP Address consists of two parts, the “Network” and “Host.”
For example, in the AP-95M’s IP address “192.168.0.1” (Class C), the digits “192.168.0” are the network digits and the “1” at the end is the host digit.
Network devices with the same network numbers are recognized as belonging to the same network.
Furthermore, the network devices in the network are identified by the host part.

Assign the IP Address considering the following points.

- Set the identical network digits for all the devices that you want to add into the network.
- Do not set the same host digit to network devices in the same network.
- Do not set the network address whose the first digit of the host part is “0.”
- Do not set the broadcast address whose the last digit of the host part is “255.”

PREPARATION

Section 2

NOTE:
All the wireless connections will be temporally disconnected when you click <Apply> on the [Wireless LAN Setting] screen.

1. WIRELESS LAN CONNECTION [Basic]

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

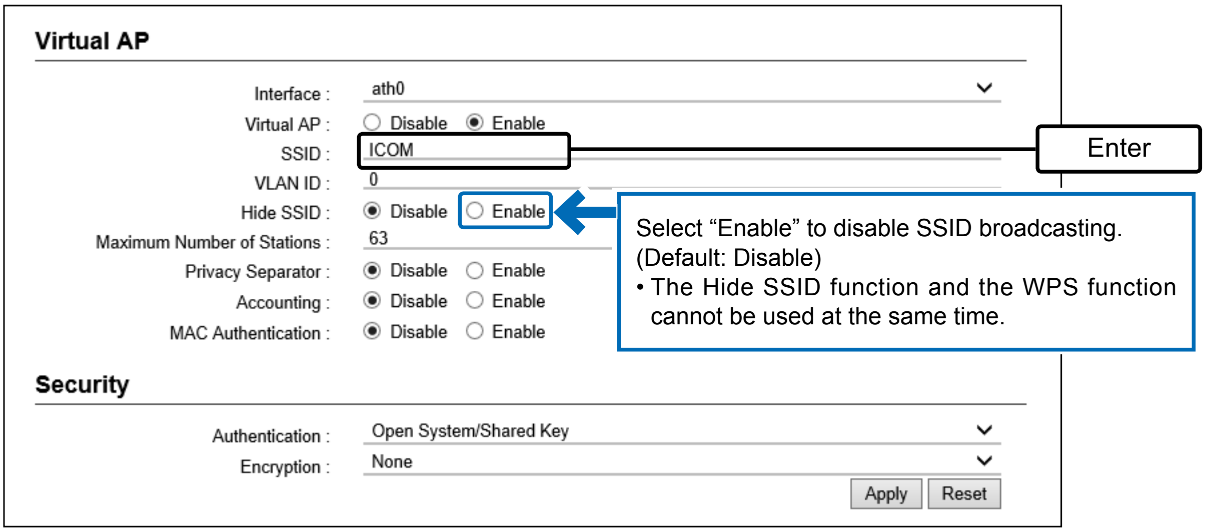
■ Entering the SSID

Entering the SSID is required for a wireless LAN station to identify the wireless network.

- Communicating with Wireless 1 “ath0” is used as an example.
  (Default: WIRELESSLAN-0)

1 Click [Wireless 1] in the “Wireless Settings” menu, and then click [Virtual AP].

2 In the “Virtual AP” menu, enter an SSID of up to 32 characters. (Example: ICOM)



Virtual AP

Interface : ath0

Virtual AP : ○ Disable ● Enable

SSID : ICOM

VLAN ID : 0

Hide SSID : ● Disable ○ Enable

Maximum Number of Stations : 63

Privacy Separator : ● Disable ○ Enable

Accounting : ● Disable ○ Enable

MAC Authentication : ● Disable ○ Enable

Security

Authentication : Open System/Shared Key

Encryption : None

Enter

Select “Enable” to disable SSID broadcasting.
(Default: Disable)

- The Hide SSID function and the WPS function cannot be used at the same time.

3 Click <Apply>.

About the Hide SSID function

You can prevent the connection from unknown wireless stations.

- If the “Hide SSID” item is set to “Enable,” the AP-95M’s SSID will not be displayed in the Wireless Network Connection item on the PC screen.
- We recommend that you change this setting only if it is necessary.

1. WIRELESS LAN CONNECTION [Basic]

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Entering the security settings

Enter the same security settings for the wireless LAN station.

• Communicating with Wireless 1 (2.4 GHz) “ath0” is used as an example.

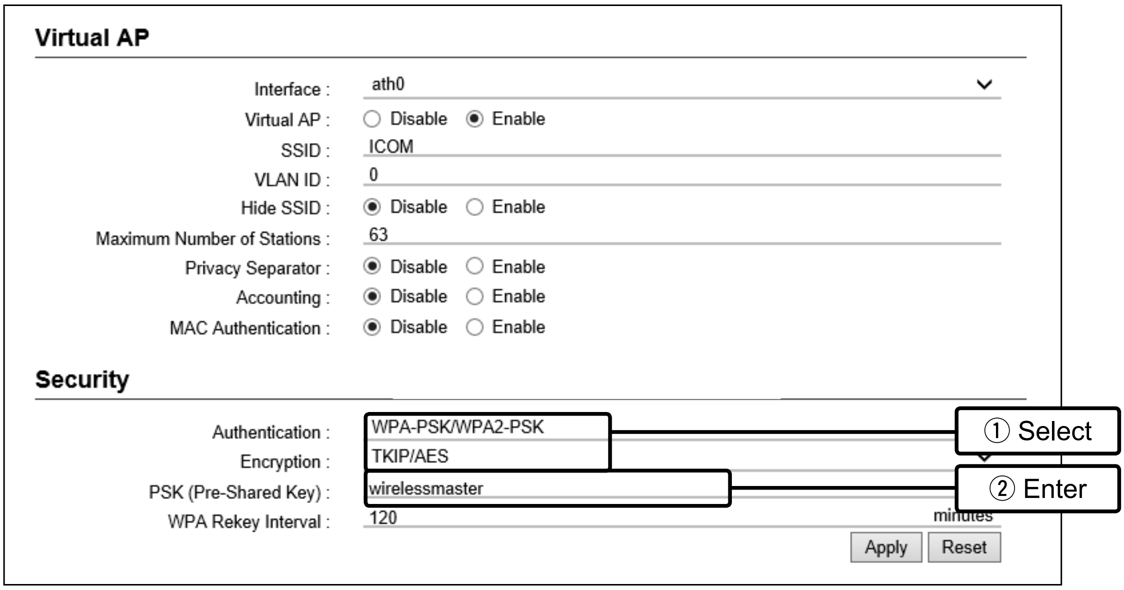
Authentication:	WPA-PSK/WPA2-PSK
Encryption:	TKIP/AES
PSK (Pre-Shared Key):	wirelessmaster

(See page 2-4 for details on the security settings that are not mentioned in this instruction.)

1 Select “WPA-PSK/WPA2-PSK” for Authentication and “TKIP/AES” for Encryption, and then enter “wirelessmaster” in the PSK (Pre-Shared Key) field.

• The entry mode (hexadecimal digits/ASCII characters) is automatically differentiated, according to the number of digits or characters entered in the “PSK (Pre-Shared Key)” field.

- ASCII: 8 ~ 63 characters
- Hexerdecimal: 64 digits



Virtual AP

Interface : ath0

Virtual AP : ○ Disable ● Enable

SSID : ICOM

VLAN ID : 0

Hide SSID : ● Disable ○ Enable

Maximum Number of Stations : 63

Privacy Separator : ● Disable ○ Enable

Accounting : ● Disable ○ Enable

MAC Authentication : ● Disable ○ Enable

Security

Authentication : WPA-PSK/WPA2-PSK

Encryption : TKIP/AES

PSK (Pre-Shared Key) : wirelessmaster

WPA Rekey Interval : 120 minutes

① Select

② Enter

2 Click <Apply>.

1. WIRELESS LAN CONNECTION [Basic]

■ Setting the “WEP RC4” encryption

There are three ways to configure the “WEP RC4” encryption.

- Directly entering the hexadecimal encryption keys. (p. 2-5)
- Directly entering the ASCII lettered encryption keys.
- Generating the encryption keys according to the entered “Key Generator” character strings. (p. 2-7)

ⓘ “Encryption” is not set as a default.

ⓘ If you cannot set “WEP RC4,” the WPS function may be set to the Virtual AP (ath0 to ath7) used. (p. 2-12)

■ About the WEP Key

The number of digits or characters that can be entered differs, depending on the “Encryption” setting and the bit number in the parenthesis.

The entry mode (hexadecimal digits/ASCII characters) is automatically selected, according to the number of entered digits or characters.

Authentication		Encryption	Entry mode	
Open System	Shared Key		Hexadecimal	ASCII
✓		None (Default)	—	—
✓	✓	WEP RC4 64 (40) bit	10 digits	5 characters
✓	✓	WEP RC4 (104) bit	26 digits	13 characters
✓	✓	WEP RC4 152 (128) bit	32 digits	16 characters

■ ASCII characters and hexadecimal digits

If “Encryption” cannot be set for the communicator’s entry mode, enter characters according to the following table.

For example, “4153434949” (10 hexadecimal digits) in the hexadecimal code will be “ASCII” (5 numbers and letters) in the ASCII characters.

ASCII		!	”	#	$	%	&	’	(	)	*		,	-	.	/
Hexadecimal	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
ASCII	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
Hexadecimal	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
ASCII	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Hexadecimal	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
ASCII	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
Hexadecimal	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
ASCII	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Hexadecimal	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
ASCII	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
Hexadecimal	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	

To prevent unauthorized access

You must carefully choose your password, and change it occasionally.

- Choose one that is not easy to guess.
- Use numbers, characters and letters (both lower and upper case).

1. WIRELESS LAN CONNECTION [Basic]

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

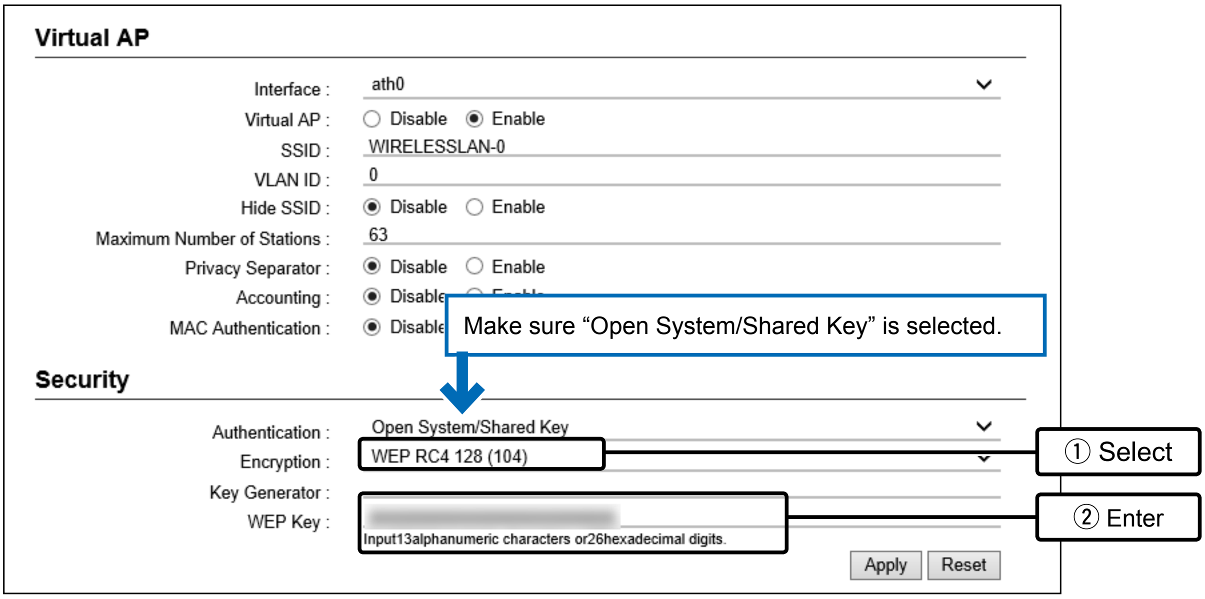
■ Entering the WEP Key with hexadecimal digits

The following example is when Wireless 1 (2.4 GHz) is set to “ath0.”

Authentication:	Open System/Shared Key (default)
Encryption:	WEP RC4 128 (104)
WEP Key:	26 digits or characters (0 to 9, a to f or A to F)

1 Click [Wireless Settings] and [Wireless 1], and then click [Virtual AP].

2 Select [WEP RC4 128 (104)] for “Encryption,” and then enter the 26 digit or characters WEP Key.



Virtual AP

Interface : ath0

Virtual AP : ○ Disable ● Enable

SSID : WIRELESSLAN-0

VLAN ID : 0

Hide SSID : ● Disable ○ Enable

Maximum Number of Stations : 63

Privacy Separator : ● Disable ○ Enable

Accounting : ● Disable

MAC Authentication : ● Disable

Security

Authentication : Open System/Shared Key

Encryption : WEP RC4 128 (104)

Key Generator :

WEP Key : Input13alphanumeric characters or26hexadecimal digits.

Make sure “Open System/Shared Key” is selected.

① Select

② Enter

3 Click <Apply>.

1. WIRELESS LAN CONNECTION [Basic]

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

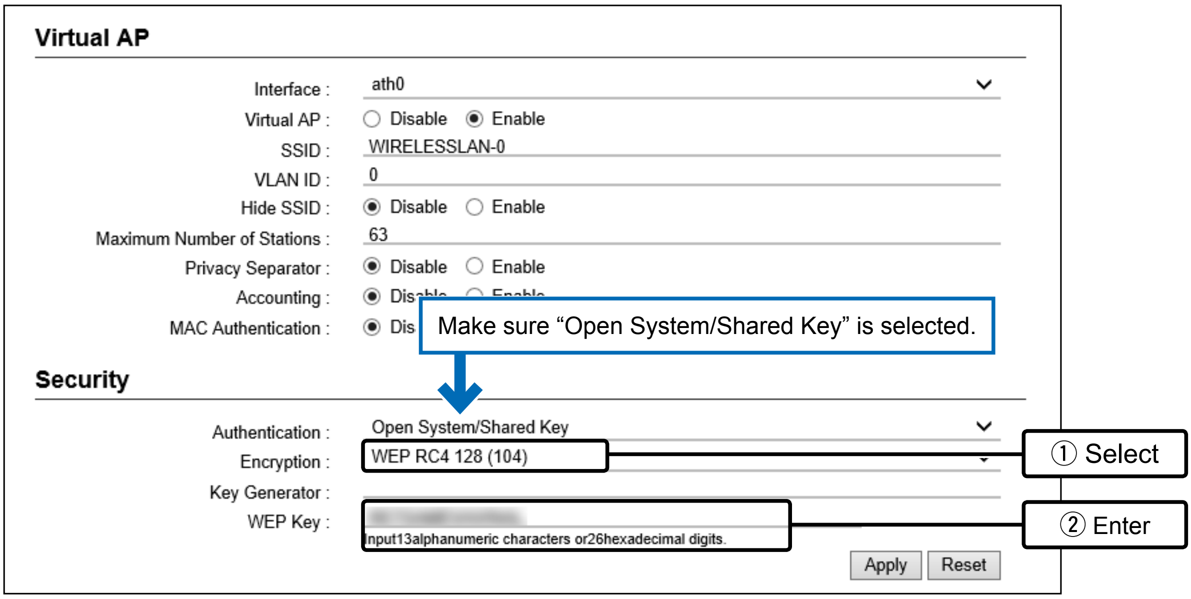
■ Entering the WEP Key with ASCII characters

The following example is when Wireless 1 (2.4 GHz) is set to “ath0.”

Authentication:	Open System/Shared Key (default)
Encryption:	WEP RC4 128 (104)
WEP Key:	13 characters (example: RETSAMEVAWNAL)

1 Click [Wireless Settings] and [Wireless 1], and then click [Virtual AP].

2 Select [WEP RC4 128 (104)] for “Encryption,” and then enter the 13 characters WEP Key.



Virtual AP

Interface : ath0

Virtual AP : ○ Disable ● Enable

SSID : WIRELESSLAN-0

VLAN ID : 0

Hide SSID : ● Disable ○ Enable

Maximum Number of Stations : 63

Privacy Separator : ● Disable ○ Enable

Accounting : ● Disable ○ Enable

MAC Authentication : ● Dis

Make sure “Open System/Shared Key” is selected.

Security

Authentication : Open System/Shared Key

Encryption : WEP RC4 128 (104)

Key Generator :

WEP Key : [redacted]

Input13alphanumeric characters or26hexadecimal digits.

3 Click <Apply>.

1. WIRELESS LAN CONNECTION [Basic]

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

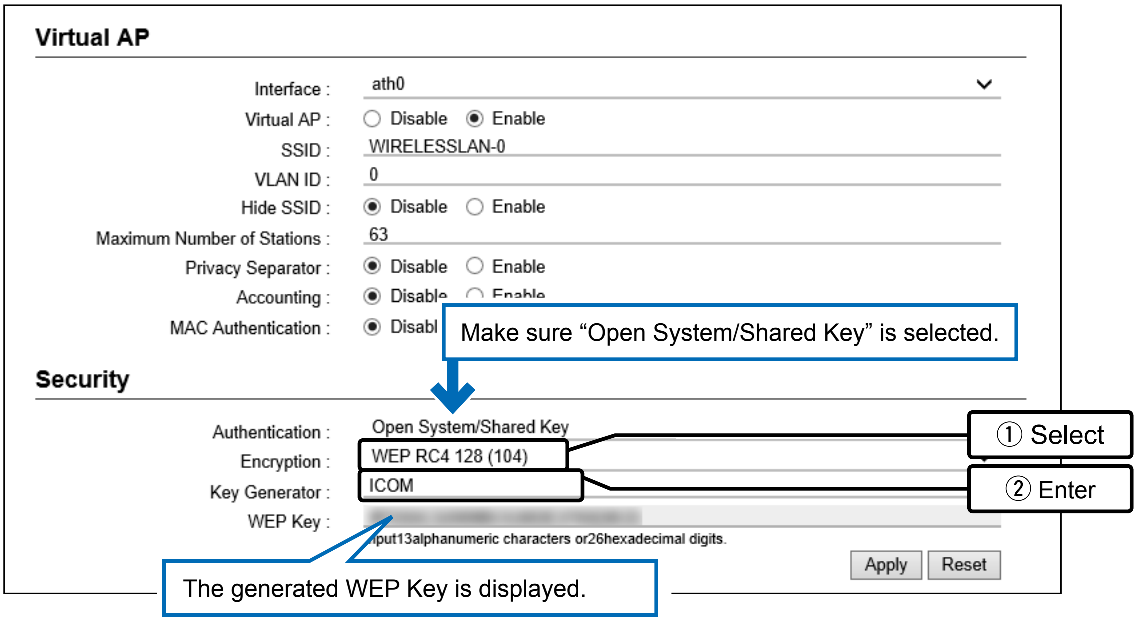
■ Generating the WEP Key

The following example is when Wireless 1 (2.4 GHz) is set to “ath0.”

Authentication:	Open System/Shared Key (default)
Encryption:	WEP RC4 128 (104)
Key Generator:	Desired character string of up to 31 characters (example: ICOM)

1 Click [Wireless Settings] and [Wireless 1], and then click [Virtual AP].

2 Select [WEP RC4 128 (104)] for “Encryption,” and then enter the desired character string of up to 31 characters into “Key Generator.”



Virtual AP

Interface : ath0

Virtual AP : ○ Disable ● Enable

SSID : WIRELESSLAN-0

VLAN ID : 0

Hide SSID : ● Disable ○ Enable

Maximum Number of Stations : 63

Privacy Separator : ● Disable ○ Enable

Accounting : ● Disable ○ Enable

MAC Authentication : ● Disabl

Make sure “Open System/Shared Key” is selected.

Security

Authentication : Open System/Shared Key

Encryption : WEP RC4 128 (104)

Key Generator : ICOM

WEP Key : [redacted]

nput13alphanumeric characters or26hexadecimal digits.

① Select

② Enter

The generated WEP Key is displayed.

3 Click <Apply>.

About the Key Generator

- The Key Generator is not compatible non-Icom products.
- Enter the desired characters to automatically generate the WEP key into the text box.
- The generated digits or characters differ, depending on the “Encryption” setting.

1. WIRELESS LAN CONNECTION [Basic]

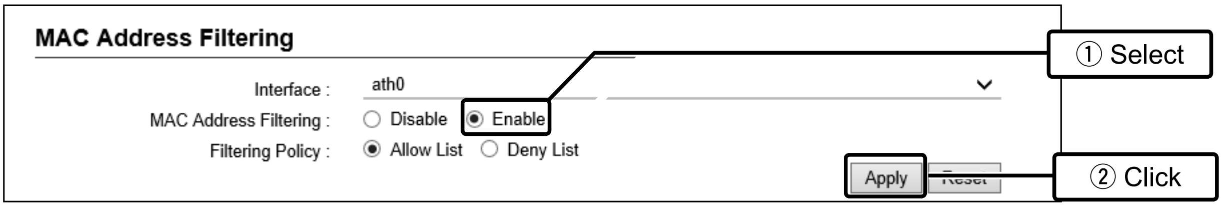
Wireless Settings > Wireless 1/Wireless 2 > MAC Address Filtering

You can set the AP-95M to allow or deny the access from wireless LAN stations, for each virtual AP (up to 1024 stations).

- The following steps describe how to set to allow or deny access, using Wireless 1's (2.4 GHz) virtual AP (ath0) as an example.

1 Click [Wireless Settings] and [Wireless 1], and then click [MAC Address Filtering].

2 Select [Enable] for "MAC Address Filtering," and then click <Apply>.



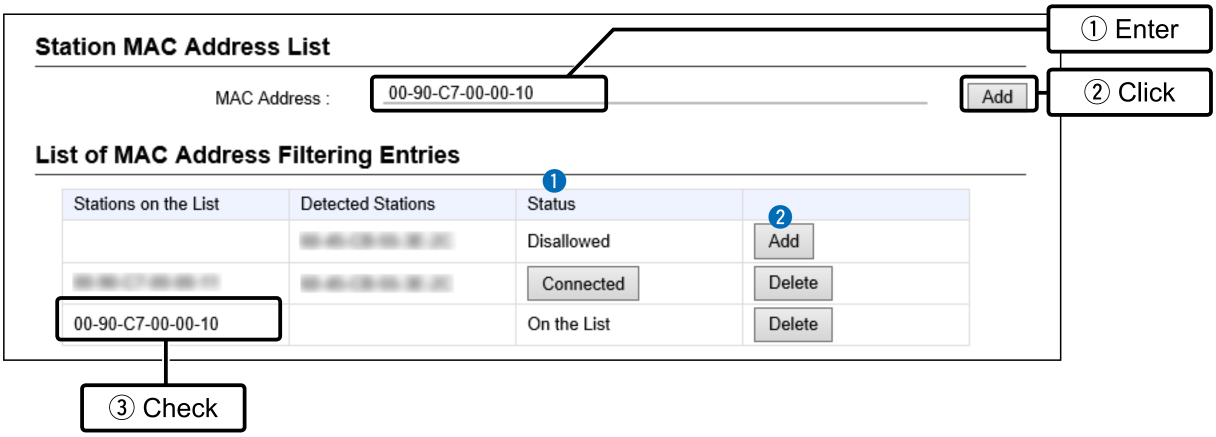
MAC Address Filtering

Interface : ath0

MAC Address Filtering : ○ Disable ● Enable

Filtering Policy : ● Allow List ○ Deny List

3 Enter the MAC address of the wireless LAN station that you want to allow access, and then click [Add].



Station MAC Address List

MAC Address : 00-90-C7-00-00-10

List of MAC Address Filtering Entries

Stations on the List	Detected Stations	Status ❶	❷
	[redacted]	Disallowed	Add
[redacted]	[redacted]	Connected	Delete
00-90-C7-00-00-10		On the List	Delete

❶ **Status** ....Displays the wireless communication status.

<Connected>: While communicating with the AP-95M, the [Connected] button is displayed.

- If you click [Connected], the communication status and wireless LAN stations are displayed.

Disallowed: Displayed when communication is denied by the AP-95M.

On the List: Displayed if the MAC address is registered but not connected.

❷ **<Add>/<Delete>** ....Adds the MAC address of the displayed wireless LAN station to the list, or deletes the address from the list.

1. WIRELESS LAN CONNECTION [Basic]

Wireless Settings > Wireless 1/Wireless 2 > Wireless LAN

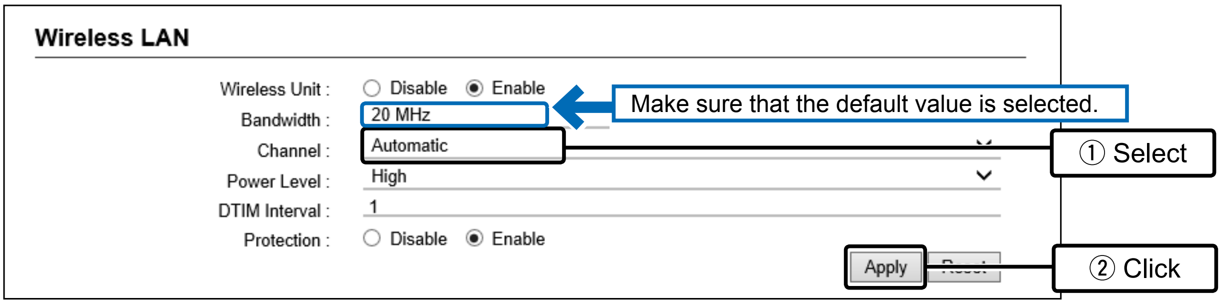
■ Automatically setting the channels in the 2.4 GHz band

Setting the Wireless 1 is used as an example.

- You can select “Automatic” only when “20 MHz” is selected in the [Bandwidth] item.
- You can confirm the channel in use on the setting screen.
  When clicking <Apply> on the Wireless LAN screen, the channel is scanned and the channel is automatically set.
- When managing the AP-95M by the RS-AP3, the channel is not be automatically set.

1 Click [Wireless Settings] and [Wireless 1], and then click [Wireless LAN].

2 Select [Automatic] for “Channel,” and then click <Apply>. (Default: 001 CH (2412 MHz))



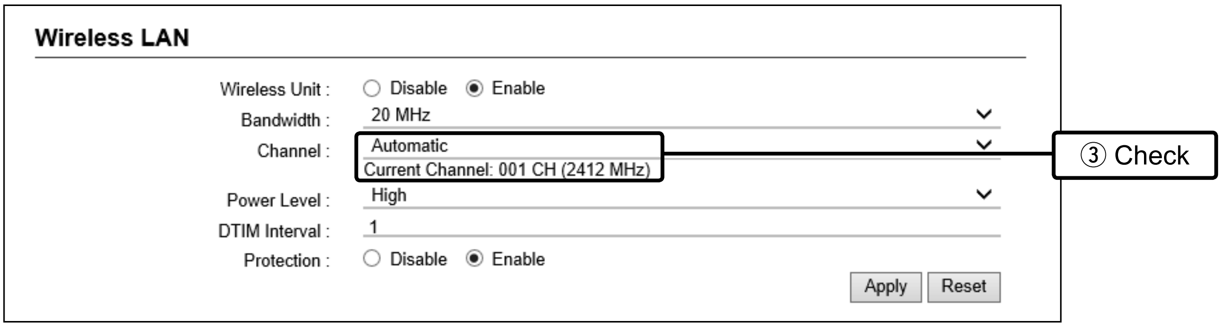
Wireless LAN

Wireless Unit : ○ Disable ● Enable
Bandwidth : 20 MHz
Channel : Automatic
Power Level : High
DTIM Interval : 1
Protection : ○ Disable ● Enable

Make sure that the default value is selected.

① Select

② Click



Wireless LAN

Wireless Unit : ○ Disable ● Enable
Bandwidth : 20 MHz
Channel : Automatic
Current Channel: 001 CH (2412 MHz)
Power Level : High
DTIM Interval : 1
Protection : ○ Disable ● Enable

③ Check

1. WIRELESS LAN CONNECTION [Basic]

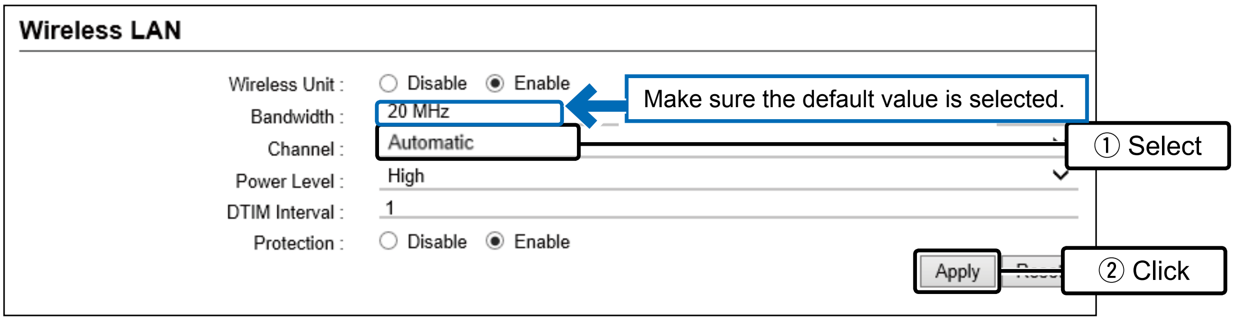
Wireless Settings > Wireless 1/Wireless 2 > Wireless LAN

■ Automatically setting the channels in the 5 GHz band

Setting Wireless 2 is used as an example.

1 Click [Wireless Settings] and [Wireless 2], and then click [Wireless LAN].

2 Select [Automatic] for “Channel,” and then click <Apply>. (Default: 036CH (5180 MHz))



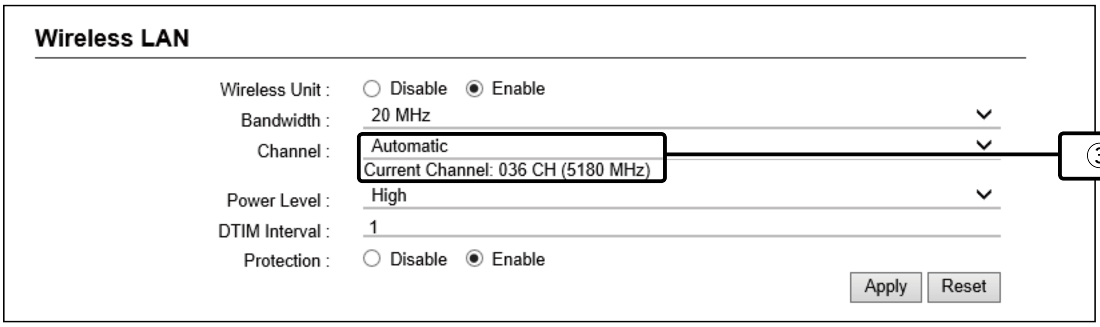
Wireless LAN

Wireless Unit : ○ Disable ● Enable
Bandwidth : 20 MHz
Channel : Automatic
Power Level : High
DTIM Interval : 1
Protection : ○ Disable ● Enable

Make sure the default value is selected.

① Select

② Click



Wireless LAN

Wireless Unit : ○ Disable ● Enable
Bandwidth : 20 MHz
Channel : Automatic
Current Channel: 036 CH (5180 MHz)
Power Level : High
DTIM Interval : 1
Protection : ○ Disable ● Enable

③ Check

Precautions on using the AP-95M outdoors
Use the AP-95M outdoors according to your local regulations.

1. WIRELESS LAN CONNECTION [Basic]

Wireless Settings > Wireless 2 > Wireless LAN

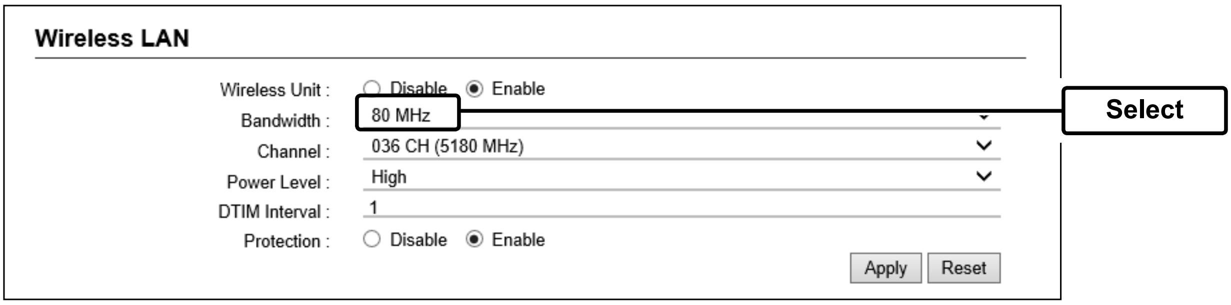
■ Communicating in the 80 MHz bandwidth

The [IEEE802.11ac] standard can be used when “5 GHz” is selected for Wireless 2 and “None” or “AES” is selected as “Encryption” on the “Virtual AP” screen.

- If “Encryption” is set to “WEP RC4” or “TKIP,” the communication is made in the [IEEE802.11a/b/g] standard, according to the set Frequency Band.

1 Click [Wireless Settings] and [Wireless 2], and then click [Wireless LAN].

2 Select “80 MHz” for the Bandwidth. (Default: 20 MHz)



Wireless LAN

Wireless Unit : ○ Disable ● Enable
Bandwidth : 80 MHz
Channel : 036 CH (5180 MHz)
Power Level : High
DTIM Interval : 1
Protection : ○ Disable ● Enable

3 Click <Apply>.

40 MHz/80 MHz bandwidth communication

- When you are using the 40 MHz or 80 MHz bandwidth mode on the wireless LAN, first check nearby frequencies in order to not to interfere other radio stations.
- If your are interfered with a radio station using this device, set the “Bandwidth” to “20 MHz (default).”

1. WIRELESS LAN CONNECTION [Basic]

This topic explains how to automatically assign the SSID and PSK (Pre-Shared Key), that are set to the Virtual AP, to a wireless LAN station by the WPS (Wi-Fi Protected Setup) function.

- See page 2-3 for the SSID and security setting details.
- The Authentications that can be used for the WPS function are “WPA-PSK” and “WPA2-PSK.”

Wireless Settings > WPS

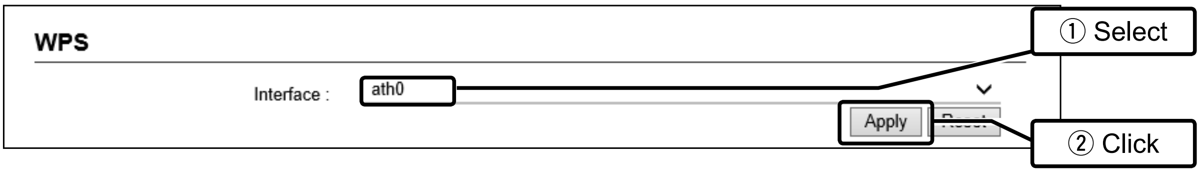
■ Enabling the WPS function

“Push Button” is used in this example. (p. 3-111)

- If the WPS function is enabled, the <Start> button will appear on the setting screen.

1 Click [Wireless Settings], and then click [WPS].

2 Select “Interface” (example: ath0) to use the WPS function, and then click <Apply>. (Default: None)



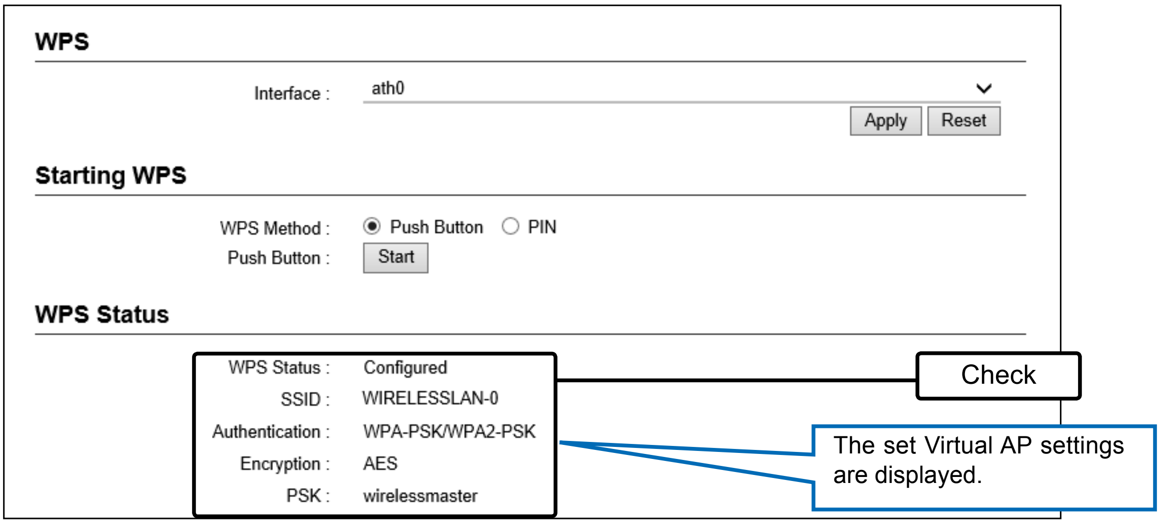
WPS

Interface : ath0

① Select

② Click

3 Check “WPS Status.”



WPS

Interface : ath0

Starting WPS

WPS Method : ● Push Button ○ PIN

Push Button : Start

WPS Status

WPS Status : Configured

SSID : WIRELESSLAN-0

Authentication : WPA-PSK/WPA2-PSK

Encryption : AES

PSK : wirelessmaster

Check

The set Virtual AP settings are displayed.

(Continued on the next page)

1. WIRELESS LAN CONNECTION [Basic]

This page describes how to assign the automatic setting by using the [WPS] function.
(Automatically sets the SSID and PSK (Pre-Shared Key) contents to the wireless LAN station.)

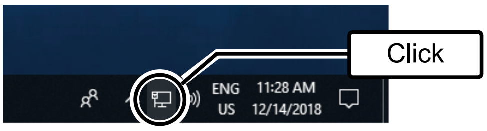
Wireless Settings > WPS

■ Automatically setting the wireless LAN using the WPS function

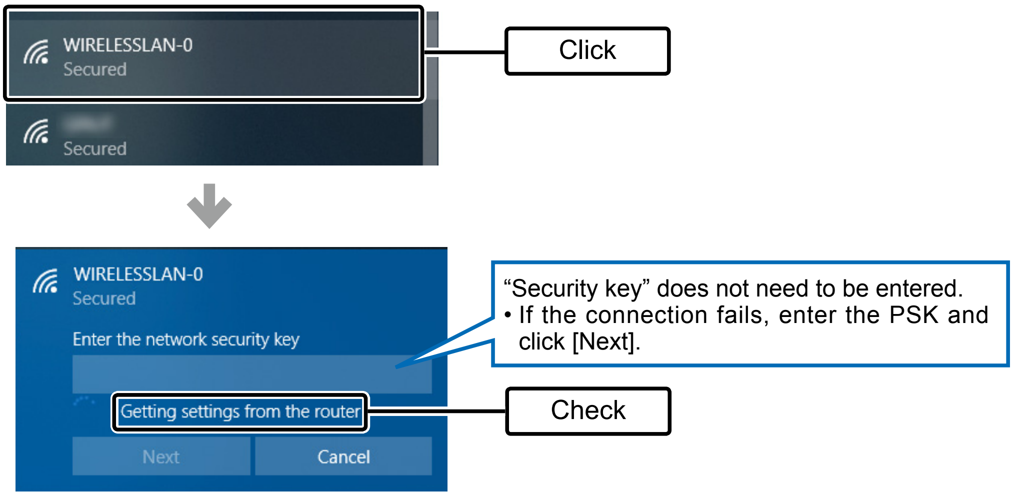
A Windows 10’s regular network connection is used as an example to describe how to automatically set up the wireless LAN station using the WPS function.

- See the wireless station’s instruction manual for more details.
- If [MODE] blinks orange ☀ and settings cannot be made, set “None” for “Interface” (p. 2-12) to manually set the station.

1 Click the wireless network connection icon on the PC.
- It may take a few minutes until the icon appears.

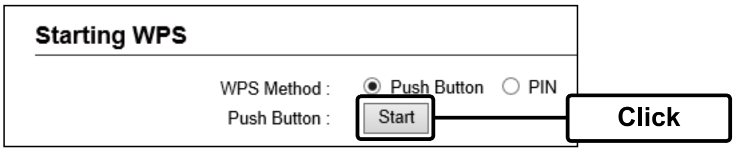


2 Select the SSID assigned to the AP-95M (example: WIRELESSLAN-0) and click [Connect].
- “Connect to a Network” is displayed.



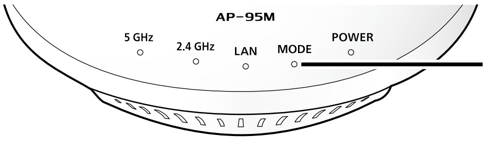
“Security key” does not need to be entered.
- If the connection fails, enter the PSK and click [Next].

3 Push [WPS] on the AP-95M.
[MODE] slowly blinks green ☀.


Starting WPS

WPS Method : ● Push Button ○ PIN
Push Button : Start

4 The setting is completed when [5GHz] or [2.4GHz] lights green ●.



[MODE]

☀ Blinks green:	WPS is running
☀ Blinks in orange:	WPS failed (turns OFF after 30 seconds)

2. WIRELESS LAN CONNECTION [Advanced]

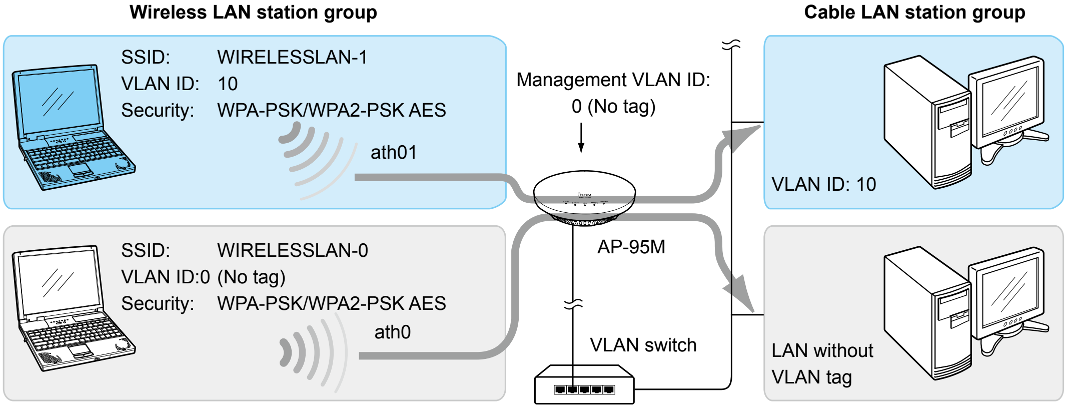
Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Setting the Virtual AP

Setting the wireless LAN station (ath01) illustrated in light blue is used as an example.

- The Virtual LAN function and Routing function cannot be used at the same time.

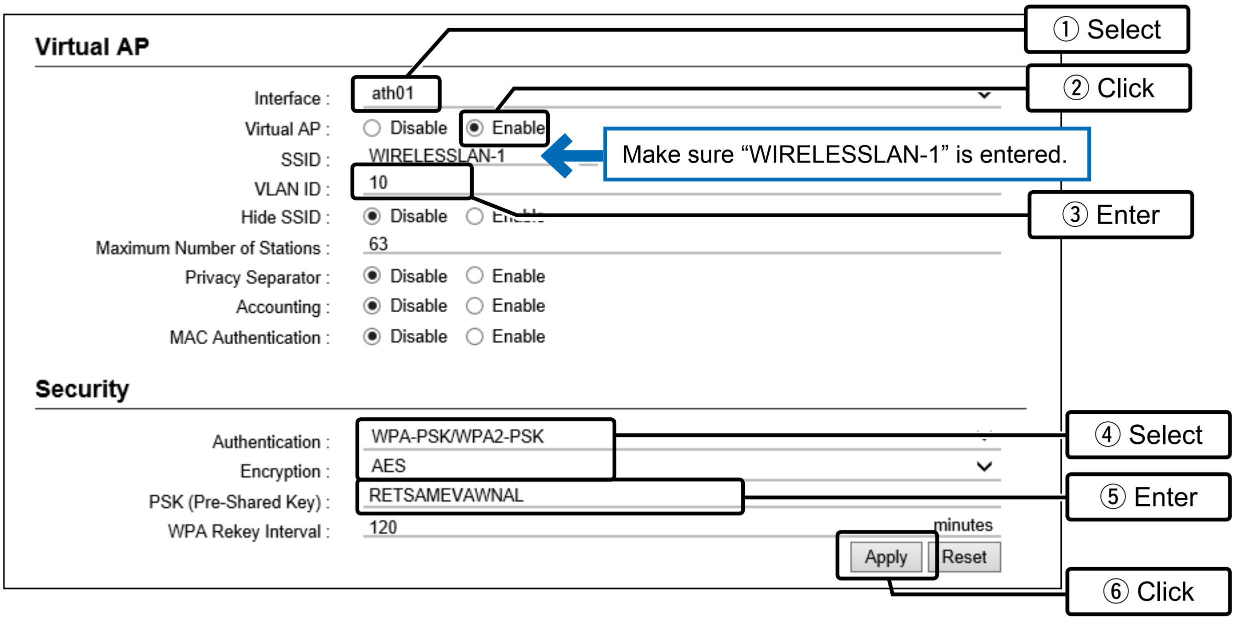
[Virtual AP]	Interface:	ath01
	Virtual AP:	Enable
	SSID:	WIRELESSLAN-1 (Default)
	VLAN ID:	10
[Security]	Authentication:	WPA-PSK/WPA2-PSK
	Encryption:	AES
	PSK (Pre-Shared Key):	RETSAMEVAWNAL



- Virtual AP “ath0” is assumed to have been already configured in this example.
- See “Virtual AP function” for more details. (p. 1-7)

1 Click [Wireless Settings] and [Wireless 1], and then click [Virtual AP].

2 Select “ath01” for “Interface,” and then set the other settings, as in the examples described above.



Virtual AP

Interface : ath01 — ① Select

Virtual AP : ○ Disable ● Enable — ② Click

SSID : WIRELESSLAN-1 — Make sure “WIRELESSLAN-1” is entered.

VLAN ID : 10 — ③ Enter

Hide SSID : ● Disable ○ Enable

Maximum Number of Stations : 63

Privacy Separator : ● Disable ○ Enable

Accounting : ● Disable ○ Enable

MAC Authentication : ● Disable ○ Enable

Security

Authentication : WPA-PSK/WPA2-PSK — ④ Select

Encryption : AES

PSK (Pre-Shared Key) : RETSAMEVAWNAL — ⑤ Enter

WPA Rekey Interval : 120 minutes

(Continued on the next page)

2. WIRELESS LAN CONNECTION [Advanced]

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging (WBR)

■ Using the Wireless Bridging (WBR) function

Setting two AP-95Ms (illustration: master (ath0) and client) with the following settings are used as an example.

- Refer to “Wireless Bridging function” for how to use the function. (p. 2-16)
- The client unit channel automatically changes to the master unit channel. The channel “001CH (2412 MHz)” (Wireless 1) is set as the default, and it is used as the example in this description.
- The client virtual AP (ath07, ath17) cannot be used when the wireless bridging function is set.
- The IP address which was set in “Changing the IP address” (p. 1-16) is used as an example.

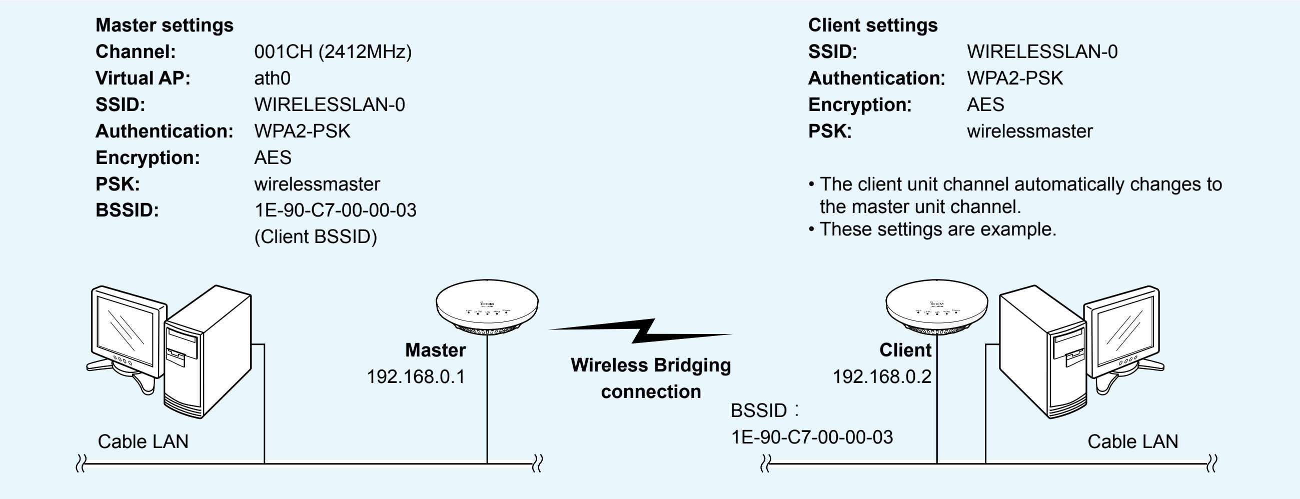
Master (p. 2-16)

[Wireless LAN]	Channel:	001CH (2412 MHz) (default)
[Virtual AP]	Interface:	ath0 (Communication is done on the SSID and security settings that are set in the Master station (Virtual AP setting: ath0 (Wireless 1) and ath1 (Wireless 2).)
	Virtual AP:	Enable (default)
	SSID:	WIRELESSLAN-0 (default)
[Security]	Authentication:	WPA2-PSK
	Encryption:	AES
	PSK (Pre-Shared Key):	wirelessmaster
[Wireless Bridging]	Wireless Bridging:	Enable
	Operating Mode:	Master
	Interface:	wbr0
	Client BSSID:	1E-90-C7-00-00-03 (Client BSSID) • Check the Client BSSID by enabling “Wireless Bridging” on the client’s “Wireless Bridging (WBR)” screen.

Client (p. 2-18)

[Wireless Bridging]	Wireless Bridging:	Enable
	Operating Mode:	Client
[Client Settings]	SSID:	WIRELESSLAN-0 (default)
	Authentication:	WPA2-PSK
	Encryption:	AES
	PSK (Pre-Shared Key):	wirelessmaster

- The client’s “Interface” cannot be changed from “wbr16” (wireless 1) or “wbr17” (wireless 2).



Master settings

Channel:	001CH (2412MHz)
Virtual AP:	ath0
SSID:	WIRELESSLAN-0
Authentication:	WPA2-PSK
Encryption:	AES
PSK:	wirelessmaster
BSSID:	1E-90-C7-00-00-03 (Client BSSID)

Client settings

SSID:	WIRELESSLAN-0
Authentication:	WPA2-PSK
Encryption:	AES
PSK:	wirelessmaster

- The client unit channel automatically changes to the master unit channel.
- These settings are example.

(Continued on the next page)

2. WIRELESS LAN CONNECTION [Advanced]

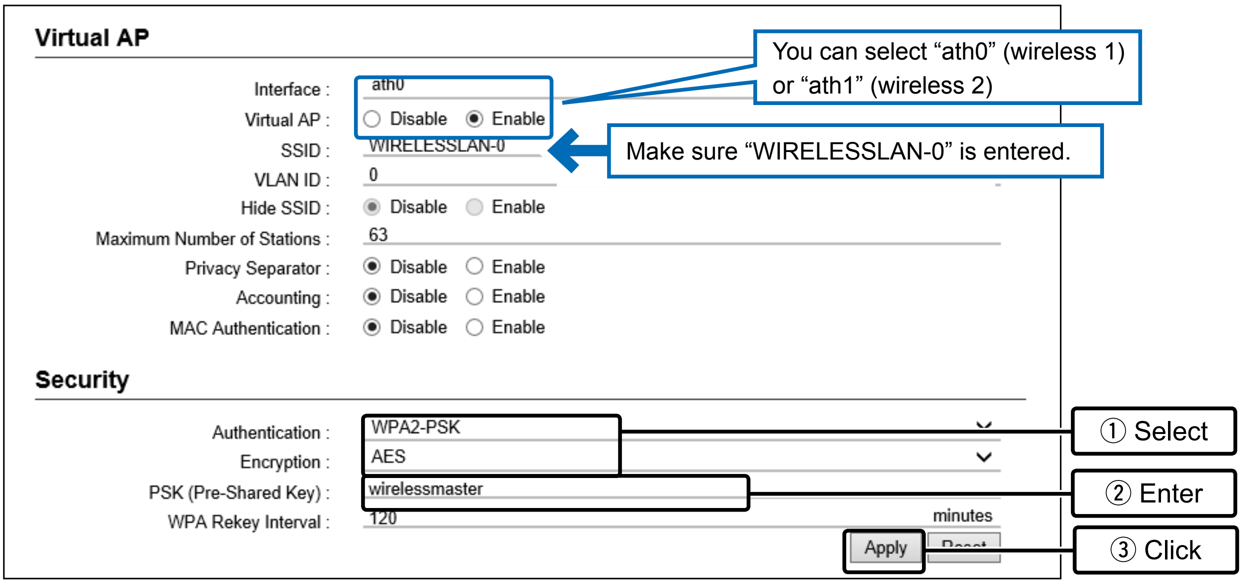
Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging (WBR)

■ Setting the Master unit

Follow the steps below to set the master unit to use with the Wireless Bridging function.

1 Click [Wireless Settings] and [Wireless 1], and then click [Virtual AP].

2 Set “ath0” for the interface, and then enable the virtual AP.



Virtual AP

Interface : ath0
Virtual AP : ○ Disable ● Enable
SSID : WIRELESSLAN-0
VLAN ID : 0
Hide SSID : ● Disable ○ Enable
Maximum Number of Stations : 63
Privacy Separator : ● Disable ○ Enable
Accounting : ● Disable ○ Enable
MAC Authentication : ● Disable ○ Enable

Security

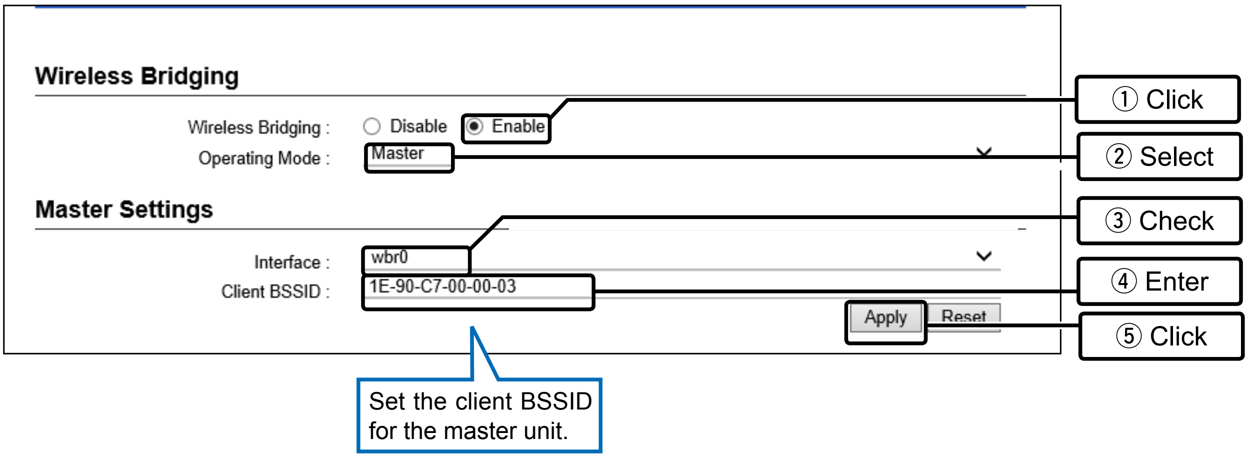
Authentication : WPA2-PSK
Encryption : AES
PSK (Pre-Shared Key) : wirelessmaster
WPA Rekey Interval : 120 minutes

You can select “ath0” (wireless 1) or “ath1” (wireless 2)

Make sure “WIRELESSLAN-0” is entered.

3 Click [Wireless Settings] and [Wireless 1], and then click [Wireless Bridging (WBR)].

4 Set wireless bridging settings for the master unit.



Wireless Bridging

Wireless Bridging : ○ Disable ● Enable
Operating Mode : Master

Master Settings

Interface : wbr0
Client BSSID : 1E-90-C7-00-00-03

Set the client BSSID for the master unit.

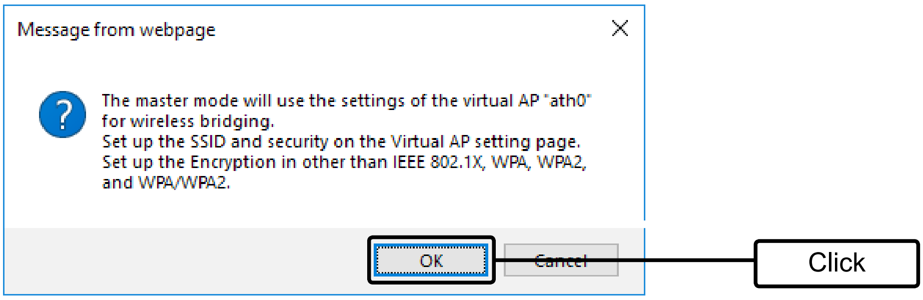
(Continued on the next page)

2. WIRELESS LAN CONNECTION [Advanced]

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging (WBR)

■ Setting the Master unit (Continued)

5 Click <OK>.

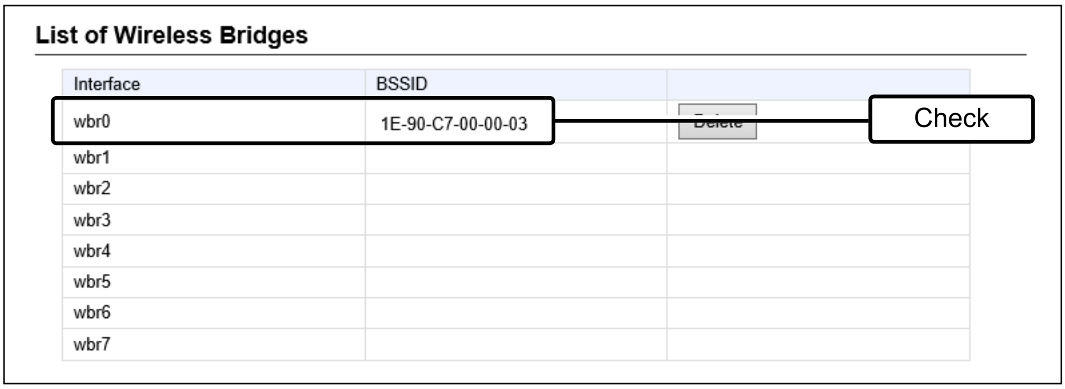


Message from webpage

The master mode will use the settings of the virtual AP "ath0" for wireless bridging.
Set up the SSID and security on the Virtual AP setting page.
Set up the Encryption in other than IEEE 802.1X, WPA, WPA2, and WPA/WPA2.

- For Wireless 1, the wireless bridging is made using the SSID and Security settings set to the virtual AP (ath0) on the master unit.
- The client unit scans the master unit that has the matching SSID and security settings.

6 Check the “List of Wireless Bridges.”



List of Wireless Bridges

Interface	BSSID	
wbr0	1E-90-C7-00-00-03	Delete
wbr1		
wbr2		
wbr3		
wbr4		
wbr5		
wbr6		
wbr7		

2. WIRELESS LAN CONNECTION [Advanced]

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging (WBR)

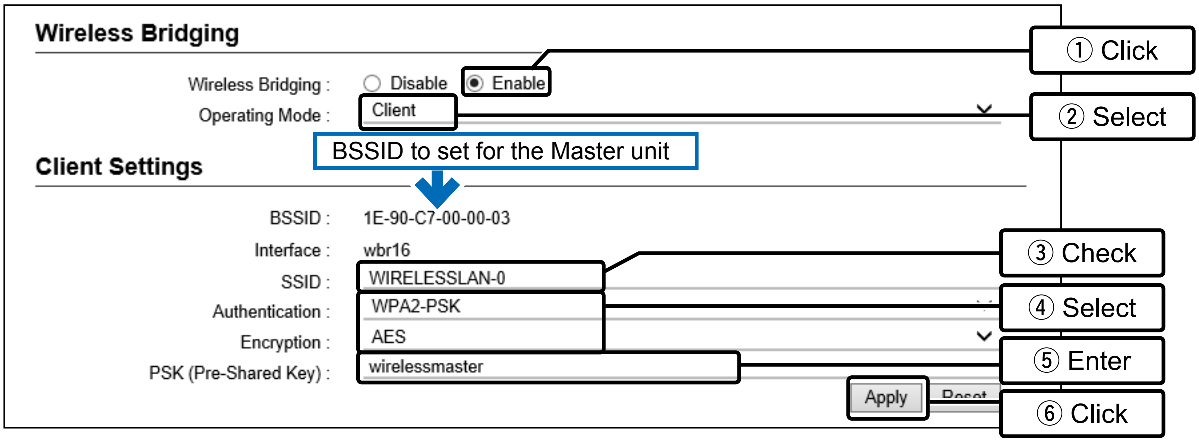
■ Setting the Client unit

Follow the steps below to set the client unit to use with the Wireless Bridging function.

- The wireless bridging is made using the SSID and Security settings that are set to the virtual AP (ath0) (Wireless 1) or (ath1) (Wireless 2) on the master unit.
- The client unit scans the master unit that has the matching SSID and security settings.
- During a scan with the client unit, the wireless LAN station cannot be connected to the other virtual APs.
- The client’s virtual AP (ath07) (Wireless 1) and (ath17) (Wireless 2) cannot be used when the Wireless Bridging function is set.

1 Click [Wireless Settings] and [Wireless 1], and then click [Wireless Bridging (WBR)].

2 Set client’s security settings.



Wireless Bridging

Wireless Bridging : ○ Disable ● Enable

Operating Mode : Client

Client Settings

BSSID : 1E-90-C7-00-00-03

Interface : wbr16

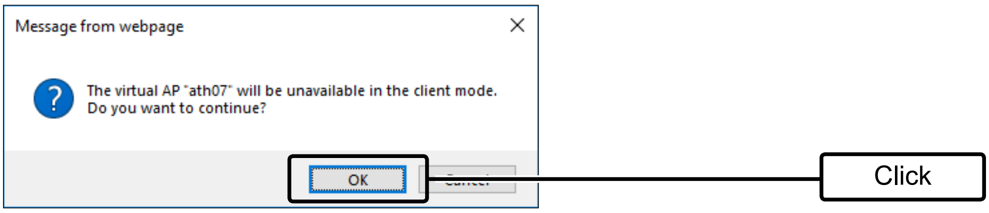
SSID : WIRELESSLAN-0

Authentication : WPA2-PSK

Encryption : AES

PSK (Pre-Shared Key) : wirelessmaster

3 Click [OK].



Message from webpage

The virtual AP "ath07" will be unavailable in the client mode.
Do you want to continue?

2. WIRELESS LAN CONNECTION [Advanced]

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging (WBR)

Management > Management Tools

■ Setting the Wireless Bridging function to the AP-95M for the RS-AP3 (Option) management

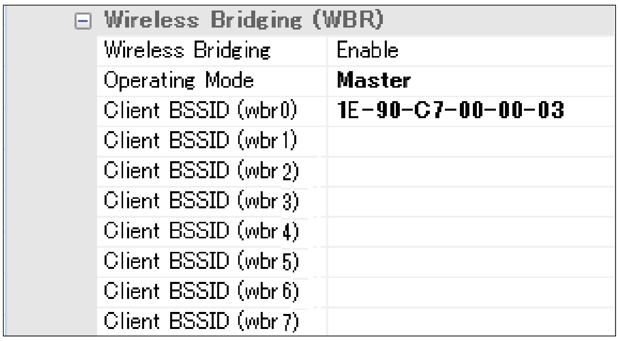
①Set the Wireless Bridging function on the AP-95M setting screen (Wireless 1 or Wireless 2) to enable the communication.

②Enable "Management Tools" on the setting screen.

③Before starting the access point management using the RS-AP3, set the AP-95M setting values on the "Individual Configurations" screen and "Common Configurations" screen* of the RS-AP3.

* Configure the master unit's SSID and security settings on the "Common Configuration" screen.

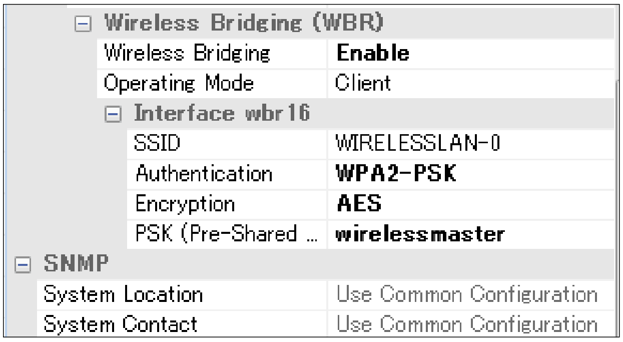
Master settings on the "Individual Configuration" screen.



⊟ Wireless Bridging (WBR)

Wireless Bridging	Enable
Operating Mode	**Master**
Client BSSID (wbr0)	**1E-90-C7-00-00-03**
Client BSSID (wbr1)	
Client BSSID (wbr2)	
Client BSSID (wbr3)	
Client BSSID (wbr4)	
Client BSSID (wbr5)	
Client BSSID (wbr6)	
Client BSSID (wbr7)	

Client settings on the "Individual Configurations" screen.



⊟ Wireless Bridging (WBR)

Wireless Bridging	**Enable**
Operating Mode	Client

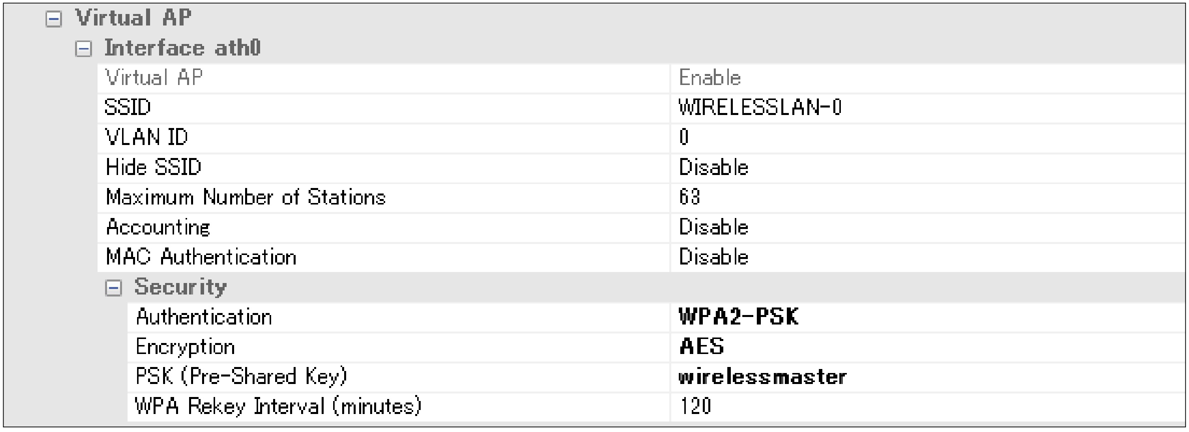
⊟ Interface wbr16

SSID	WIRELESSLAN-0
Authentication	**WPA2-PSK**
Encryption	**AES**
PSK (Pre-Shared ...	**wirelessmaster**

⊟ SNMP

System Location	Use Common Configuration
System Contact	Use Common Configuration

"Common Configuration" screen.



⊟ Virtual AP

⊟ Interface ath0

Virtual AP	Enable
SSID	WIRELESSLAN-0
VLAN ID	0
Hide SSID	Disable
Maximum Number of Stations	63
Accounting	Disable
MAC Authentication	Disable

⊟ Security

Authentication	**WPA2-PSK**
Encryption	**AES**
PSK (Pre-Shared Key)	**wirelessmaster**
WPA Rekey Interval (minutes)	120

When managing the AP-95M using the optional RS-AP3

- You cannot change Router (WAN side) settings until "End Management" is selected on the RS-AP3 screen. (See the RS-AP3 Instruction Manual for detail)
- If you use the Router function, set "Connection Type" to Static IP, then set a static IP address to the WAN side IP address item.
- When the Connection Type is set to "DHCP Client," you have to configure the network environment so that the same IP address is always provided by the Static DHCP server.
- When the Connection Type is set to "PPPoE," AP-95M cannot be managed by the RS-AP3.

2. WIRELESS LAN CONNECTION [Advanced]

■ Setting the accounting

Setting "Accounting" is required for compiling the network status information (connection, disconnection, MAC address, and so on) of the wireless LAN station that communicate with, and then sending it to the accounting server.

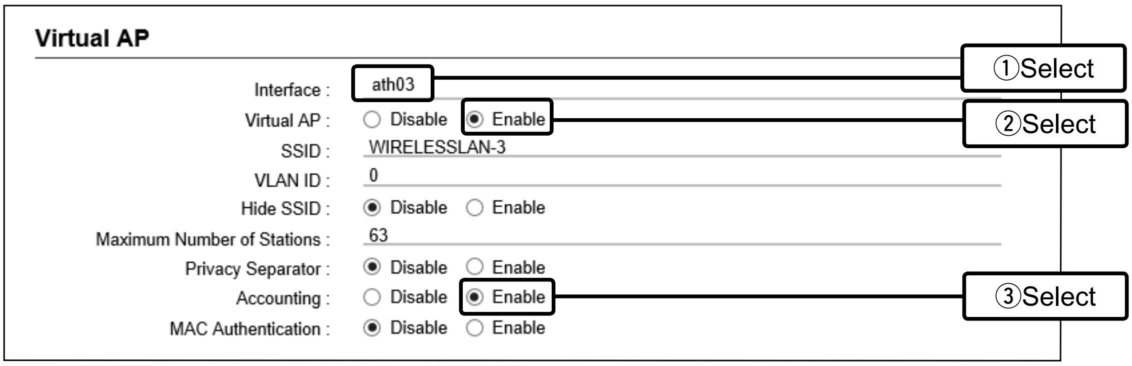
• To use this function, you must set an accounting server.

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

Individually setting the virtual AP (ath03) on the Wireless 1 (2.4 GHz) is used as an example.

1 Click [Wireless Settings] and [Wireless1], and then click [Virtual AP].

2 Select [Enable] for "Accounting." (Default: Disable)



Virtual AP

Interface : ath03
Virtual AP : ○ Disable ● Enable
SSID : WIRELESSLAN-3
VLAN ID : 0
Hide SSID : ● Disable ○ Enable
Maximum Number of Stations : 63
Privacy Separator : ● Disable ○ Enable
Accounting : ○ Disable ● Enable
MAC Authentication : ● Disable ○ Enable

①Select

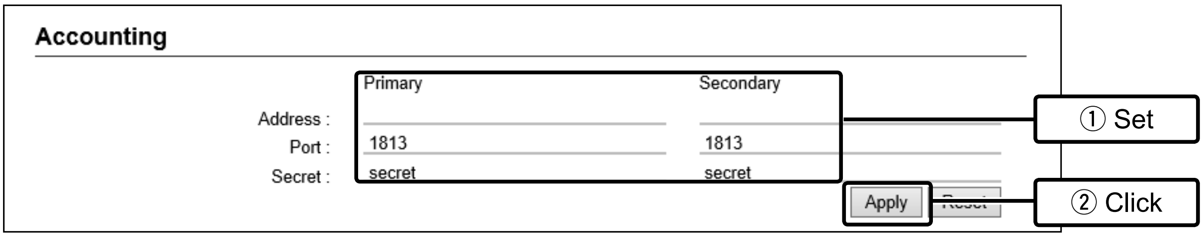
②Select

③Select

3 Select "Enable" for "Use per Virtual AP Settings," and then enter the accounting server data.

• Depending on the system you use, the port number may differ from the default settings.

• Set the same password for the AP-95M in "Secret" for the primary and secondary accounting servers.



Accounting

	Primary	Secondary
Address :		
Port :	1813	1813
Secret :	secret	secret

① Set

② Click

2. WIRELESS LAN CONNECTION [Advanced]

■ Setting the MAC Authentication Server (RADIUS)

Set the MAC Authentication Server to authorize wireless station's MAC address on the RADIUS server.

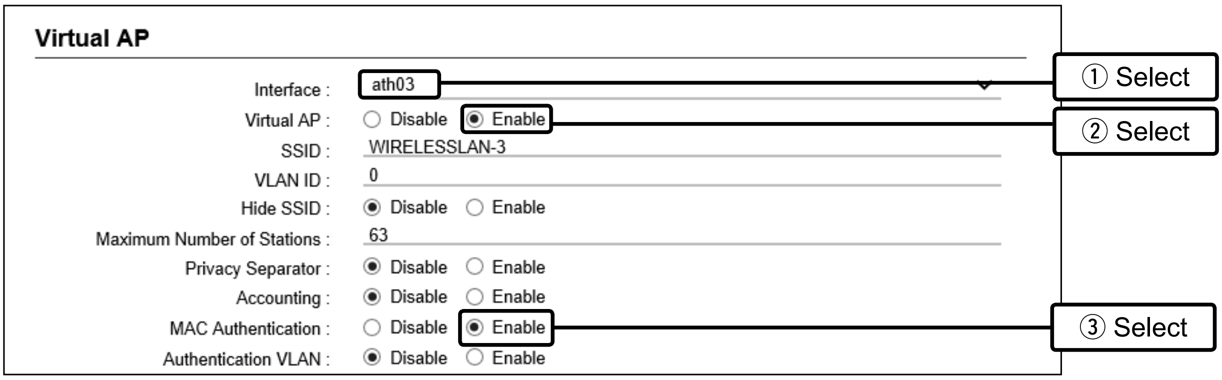
- To use this server, you must set the RADIUS server for each Virtual AP.
- You can select to either set the virtual APs individually or all together, on the "Virtual AP" screen.
- With the MAC authentication function, you can use the both "Authentication" and "Encryption" combined of your choice.
- The wireless LAN station's MAC address needs to be registered to the RADIUS server beforehand.
  If the MAC address is "00-AB-12-CD-34-EF," the Username/Password is "00ab12cd34ef."

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

Individually setting the virtual AP (ath03) on Wireless1 (2.4 GHz) is used as an example.

1 Click [Wireless Settings] and [Wireless1], and then click [Virtual AP].

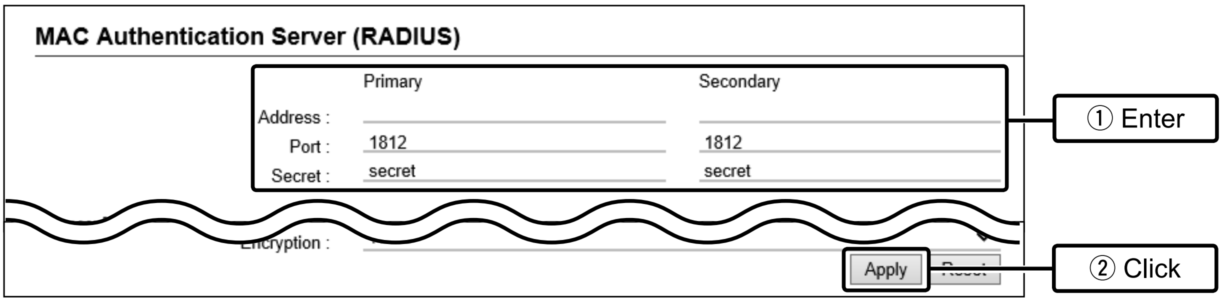
2 Select [Enable] for "MAC Authentication." (Default: Disable)



Virtual AP

Interface : ath03
Virtual AP : ○ Disable ● Enable
SSID : WIRELESSLAN-3
VLAN ID : 0
Hide SSID : ● Disable ○ Enable
Maximum Number of Stations : 63
Privacy Separator : ● Disable ○ Enable
Accounting : ● Disable ○ Enable
MAC Authentication : ○ Disable ● Enable
Authentication VLAN : ● Disable ○ Enable

3 Enter the RADIUS server data.
- Depending on the system you use, the port number may differ from the default settings.
- Set the same password for the AP-95M in "Secret" for the primary and secondary RADIUS servers.



MAC Authentication Server (RADIUS)

	Primary	Secondary
Address :		
Port :	1812	1812
Secret :	secret	secret

Encryption :

2. WIRELESS LAN CONNECTION [Advanced]

■ About the RADIUS setting

Set the RADIUS for authorizing the WPA, WPA2, or IEEE802.1X.

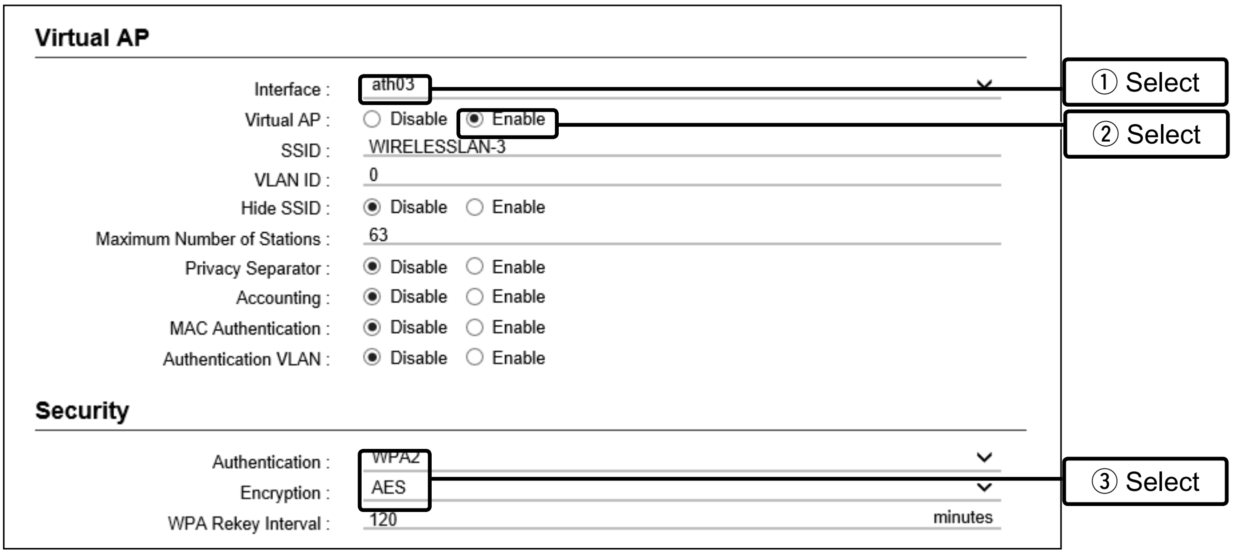
- To use this server, you must set the RADIUS server.
- See the RADIUS server or wireless LAN device's manual for the EAP authentication.

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

Individually setting the virtual AP (ath03) on Wireless 1 (2.4 GHz) is used as an example.

1 Click [Wireless Settings] and [Wireless1], and then click [Virtual AP].

2 Set the "Authentication" and "Encryption." (Authentication example: WPA2)



Virtual AP

Interface : ath03

Virtual AP : ○ Disable ● Enable

SSID : WIRELESSLAN-3

VLAN ID : 0

Hide SSID : ● Disable ○ Enable

Maximum Number of Stations : 63

Privacy Separator : ● Disable ○ Enable

Accounting : ● Disable ○ Enable

MAC Authentication : ● Disable ○ Enable

Authentication VLAN : ● Disable ○ Enable

Security

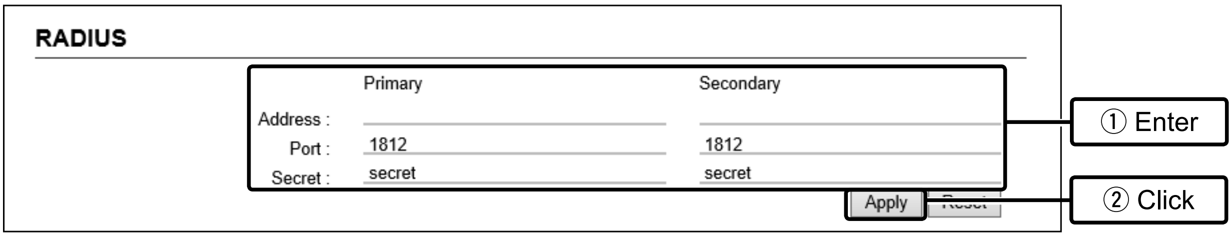
Authentication : WPA2

Encryption : AES

WPA Rekey Interval : 120 minutes

3 Select "Enable" for "Use per Virtual AP Settings," and then enter the RADIUS server data.

- Depending on the system you use, the port number may differ from the default settings.
- Set the same password for the AP-95M in "Secret" for the primary and secondary RADIUS servers.



RADIUS

	Primary	Secondary
Address :		
Port :	1812	1812
Secret :	secret	secret

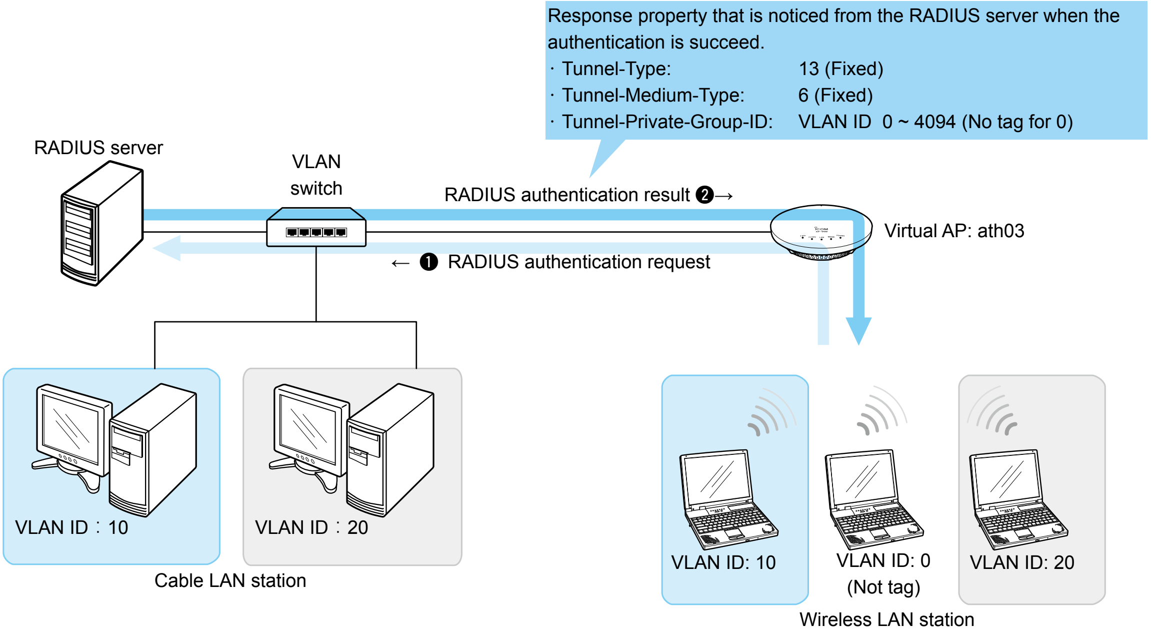
2. WIRELESS LAN CONNECTION [Advanced]

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ About the Authentication VLAN

When the Authentication VLAN is enabled, you can group the wireless LAN station's VLAN ID, according to the RADIUS authenitication result (Response property).

- You have to set the RADIUS server settings for each Virtual AP.
- To enable the Authentication VLAN, select "Enable" in the [MAC Authentication], or select an authentication type (WPA/ WPA2/IEEE802.1X) in the [Authentication] item. (p. 2-24)
- Network authentication takes priority when both network authentication and MAC authentication are enabled, and the VLAN ID was obtained from both network authentication and MAC authentication.
  When the response property is invalid or not obtained, the VLAN ID that is set to the Virtual AP is valid.
- This function cannot be configured on the RS-AP3's MAC Authentication server (RADIUS) function.



Response property that is noticed from the RADIUS server when the authentication is succeed.
· Tunnel-Type: 13 (Fixed)
· Tunnel-Medium-Type: 6 (Fixed)
· Tunnel-Private-Group-ID: VLAN ID 0 ~ 4094 (No tag for 0)

These settings are examples.

INFO
You can check the wireless station’s VLAN ID on the [Wireless Status] screen.
Click <Detail> at the [Station Status] item to check the ID. (p. 3-8)

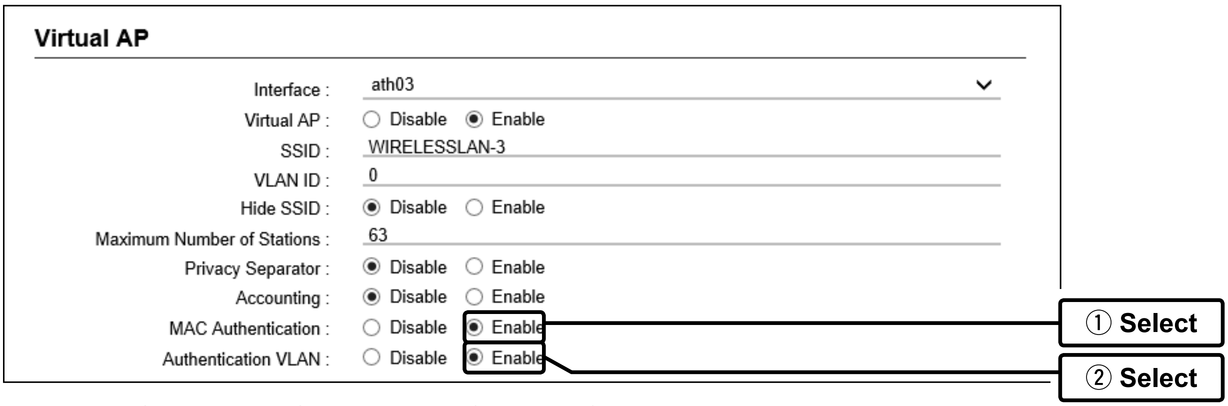
2. WIRELESS LAN CONNECTION [Advanced]

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ About the Authentication VLAN

When using the MAC authentication

Set the MAC Authentication and Authentication VLAN to "Enable" in the Virtual AP item on the Virtual AP screen.



Virtual AP

Interface : ath03
Virtual AP : ○ Disable ● Enable
SSID : WIRELESSLAN-3
VLAN ID : 0
Hide SSID : ● Disable ○ Enable
Maximum Number of Stations : 63
Privacy Separator : ● Disable ○ Enable
Accounting : ● Disable ○ Enable
MAC Authentication : ○ Disable ● Enable
Authentication VLAN : ○ Disable ● Enable

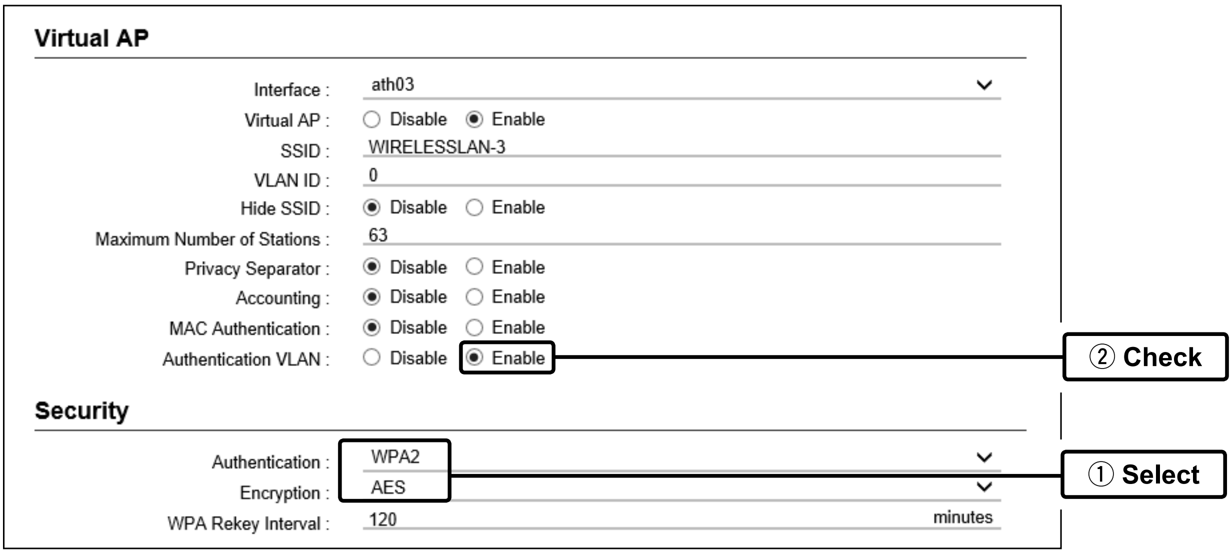
① Select

② Select

- See page 2-22 for the RADIUS server setting for the MAC authentication.
- With the MAC authentication function, you can use the both “Authentication” and “Encryption” combined of your choice.
- The wireless LAN station’s MAC address needs to be registered to the RADIUS server beforehand.
  If the MAC address is “00-AB-12-CD-34-EF,” the Username/Password is “00ab12cd34ef.”

When using the network authentication (WPA/WPA2/IEEE802.1X)

Set the Network authentication and encryption in the Encryption item on the Security screen, and the authentication VLAN enable in the Virtual AP item. (Example: WPA2)



Virtual AP

Interface : ath03
Virtual AP : ○ Disable ● Enable
SSID : WIRELESSLAN-3
VLAN ID : 0
Hide SSID : ● Disable ○ Enable
Maximum Number of Stations : 63
Privacy Separator : ● Disable ○ Enable
Accounting : ● Disable ○ Enable
MAC Authentication : ● Disable ○ Enable
Authentication VLAN : ○ Disable ● Enable

② Check

Security

Authentication : WPA2
Encryption : AES
WPA Rekey Interval : 120 minutes

① Select

- To use this server, you must set the RADIUS server.
- See the RADIUS server or wireless LAN device’s manual for the EAP authentication.

SETTING SCREEN

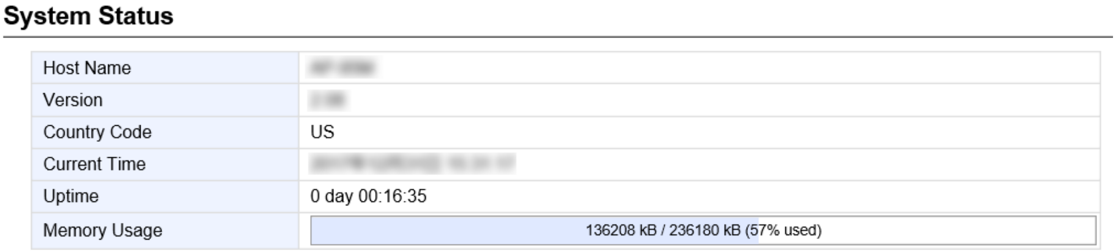
Section 3

[TOP] Screen

TOP

System Status

Displays the firmware version, current time, uptime and memory usage.



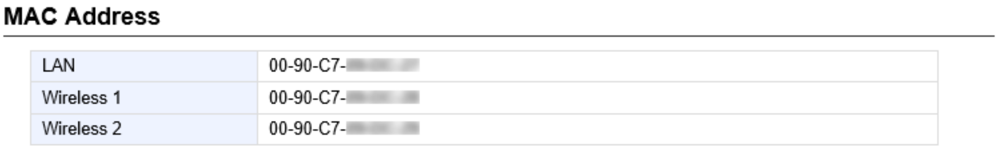
System Status

Host Name	[redacted]
Version	[redacted]
Country Code	US
Current Time	[redacted]
Uptime	0 day 00:16:35
Memory Usage	136208 kB / 236180 kB (57% used)

TOP

MAC Address

AP-95M's MAC addresses (LAN/Wireless) are displayed.



MAC Address

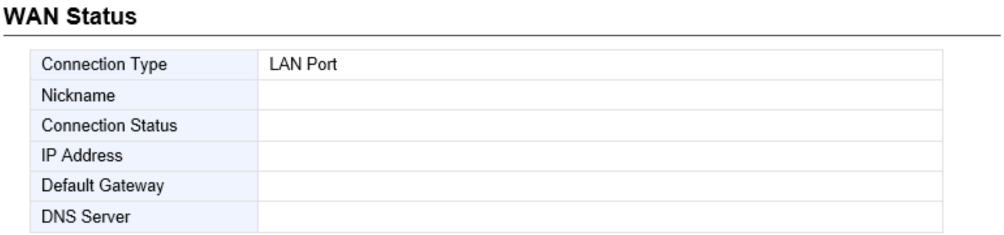
LAN	00-90-C7-[redacted]
Wireless 1	00-90-C7-[redacted]
Wireless 2	00-90-C7-[redacted]

- MAC address is a 12-digit unique number (00-90-C7-××-××-××) assigned to network devices.

TOP

WAN Status

The WAN Network connection status is displayed.



WAN Status

Connection Type	LAN Port
Nickname	
Connection Status	
IP Address	
Default Gateway	
DNS Server	

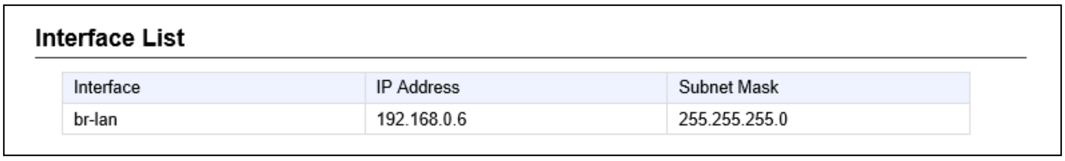
(Default screen)

[Network Status] screen

Information > Network Status

Interface List

Displays the details of the interface that is set in the ［Interface］item on the「Static Routing」screen.



Interface List

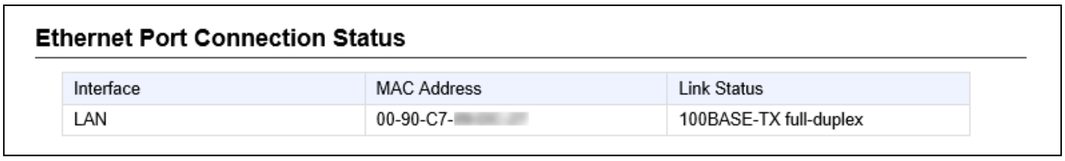
Interface	IP Address	Subnet Mask
br-lan	192.168.0.6	255.255.255.0

(This is an example.)

Information > Network Status

Ethernet Port Connection Status

Displays the communication rate and mode for each port.



Ethernet Port Connection Status

Interface	MAC Address	Link Status
LAN	00-90-C7-[redacted]	100BASE-TX full-duplex

(This is an example.)

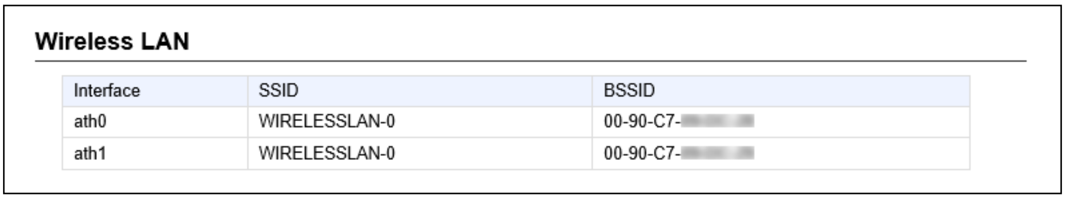
- The AP-95M’s [LAN] ports are auto-negotiation enabled, and can automatically select the optimal speed and duplex mode if the peer devices are auto-negotiation enabled as well.
- We recommend to always enable auto-negotiation on the peer devices. If a peer device is fixed in the full-duplex mode, auto-negotiation enabled devices (including the AP-95M) may generally take it for half-duplex mode and cannot communicate properly.

[Network Status] screen

Information > Network Status

■ Wireless LAN

Displays the details of virtual APs that the AP-95M has.



Wireless LAN

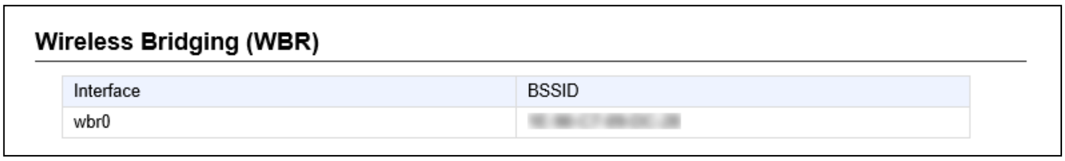
Interface	SSID	BSSID
ath0	WIRELESSLAN-0	00-90-C7-[redacted]
ath1	WIRELESSLAN-0	00-90-C7-[redacted]

- Wireless LAN stations that are disabled in the [Wireless LAN] item (p. 3-66) or [Virtual AP Settings] item (p. 3-68) is not displayed.

Information > Network Status

■ Wireless Bridging (WBR)

Displays the details of APs that communicates with the AP-95M through WBR.



Wireless Bridging (WBR)

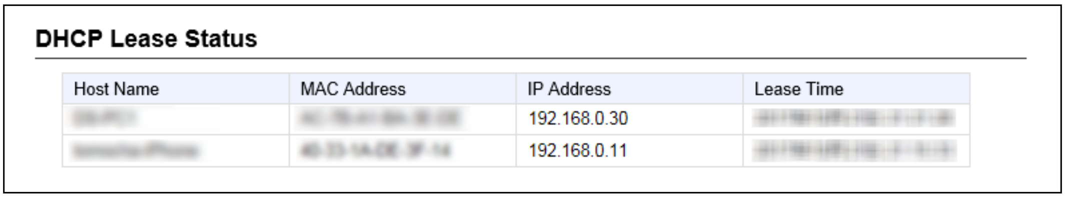
Interface	BSSID
wbr0	[redacted]

- The interface name and BSSID of the AP that communicates with the AP-95M are displayed. (p. 3-91)

Information > Network Status

■ DHCP Lease Status

Displays the status and lease time of the IP addres assigned to devices that are connecting to the AP-95M when the DHCP Server function (p. 3-18) is enabled.



DHCP Lease Status

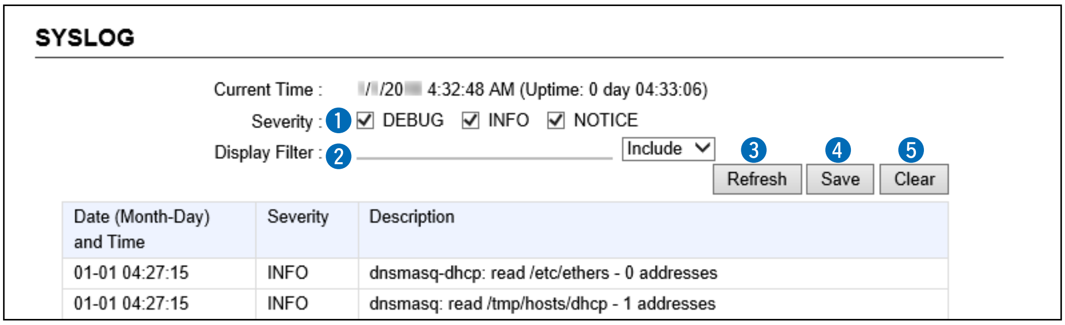
Host Name	MAC Address	IP Address	Lease Time
[redacted]	[redacted]	192.168.0.30	[redacted]
[redacted]	[redacted]	192.168.0.11	[redacted]

[SYSLOG] screen

Information > SYSLOG

You can check the AP-95M’s SYSLOG on the “SYSLOG” screen in the “Information” menu.

- On this screen, only the log information severity (DEBUG/INFO/NOTICE) that is set to “enable” on the “SYSLOG” screen in the “Management” menu is displayed.



SYSLOG

Current Time : [redacted]/[redacted]/20[redacted] 4:32:48 AM (Uptime: 0 day 04:33:06)

Severity : ❶ ☑ DEBUG ☑ INFO ☑ NOTICE

Display Filter : ❷ ______ Include

Date (Month-Day) and Time	Severity	Description
01-01 04:27:15	INFO	dnsmasq-dhcp: read /etc/ethers - 0 addresses
01-01 04:27:15	INFO	dnsmasq: read /tmp/hosts/dhcp - 1 addresses

❶ **Severity** .... Click to remove the check mark to hide.
(Default: ☑ DEBUG/ ☑ INFO/ ☑ NOTICE)

- The check box status settings will not be saved.
  The settings are reset as the defaults each time you access the setting screen.

❷ **Display Filter** .... Click to filter the displayed item.

- Enter a keyword (Example: dhcp), and select “include” or “not include” to filter the log to display.

❸ **<Refresh>** .... Click to update the SYSLOG information of the check box status set in the [Severity] (❶) item.

- A maximum of 1000 log entries can be memorized.
  When the entry amount exceeds 1000, the logs entries will be sequentially deleted starting from the oldest.

❹ **<Save>** .... Click to save all the latest log entries in the AP-95M.

- You can save the log entries in the text format by following the instructions displayed on the screen after clicking <Save>. (Format: txt)

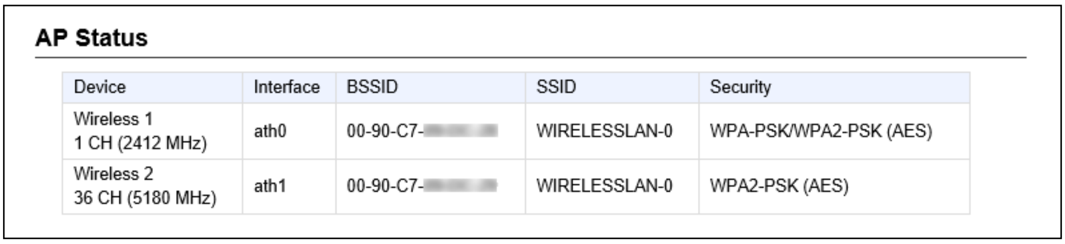
❺ **<Clear>**........................... Click to clear the displayed log information.

[Wireless Status] screen

Information > Wireless Status

AP Status

Displays the channel and settings for each virtual AP.



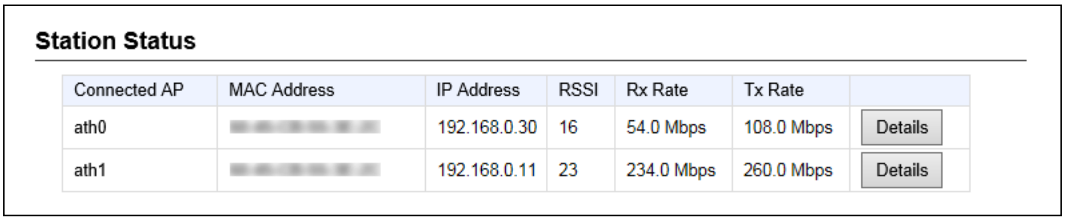
AP Status

Device	Interface	BSSID	SSID	Security
Wireless 1 1 CH (2412 MHz)	ath0	00-90-C7-[redacted]	WIRELESSLAN-0	WPA-PSK/WPA2-PSK (AES)
Wireless 2 36 CH (5180 MHz)	ath1	00-90-C7-[redacted]	WIRELESSLAN-0	WPA2-PSK (AES)

Information > Wireless Status

Station Status

Displays the communication status of the wireless LAN stations that are connected to the AP-95M.



Station Status

Connected AP	MAC Address	IP Address	RSSI	Rx Rate	Tx Rate	
ath0	[redacted]	192.168.0.30	16	54.0 Mbps	108.0 Mbps	Details
ath1	[redacted]	192.168.0.11	23	234.0 Mbps	260.0 Mbps	Details

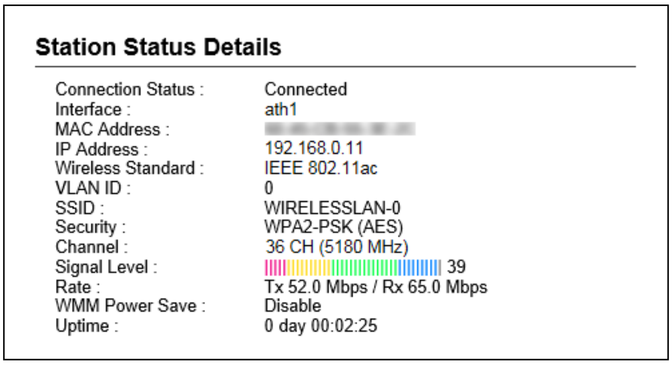
- The IP address of the wireless LAN station is displayed when it has been obtained by the AP-95M’s DHCP server function.
  The IP address is displayed also when the ARP proxy answering function is set to “Enable.” (p.3-106)
  A “–” is displayed instead of the IP address when the AP-95M has not obtained the IP address by the DHCP server function or ARP proxy is disabled.
- Click <Details> for the details of the ongoing communication status. (See the next page)

[Wireless Status] screen

Information > Wireless Status > Station Status Details

Station Status Details

This screen is displayed when you click <Details> on the [Wireless LAN Status] screen.



Station Status Details

```
Connection Status :   Connected
Interface :           ath1
MAC Address :         [redacted]
IP Address :          192.168.0.11
Wireless Standard :   IEEE 802.11ac
VLAN ID :             0
SSID :                WIRELESSLAN-0
Security :            WPA2-PSK (AES)
Channel :             36 CH (5180 MHz)
Signal Level :        39
Rate :                Tx 52.0 Mbps / Rx 65.0 Mbps
WMM Power Save :      Disable
Uptime :              0 day 00:02:25
```

Indication	[Red]	[Yellow]	[Green]	[Blue]
Level	0 ~ 4	5 ~ 14	15 ~ 29	30 and higher

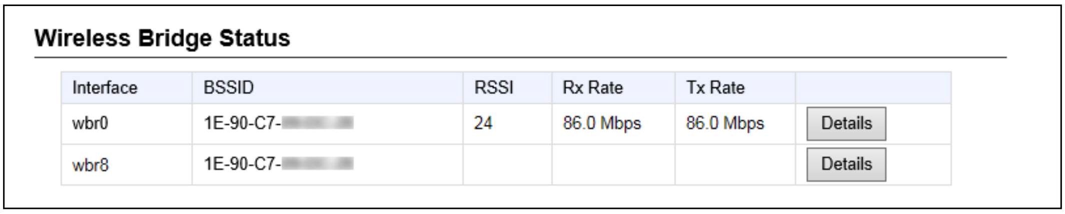
- The received signal strength is indicated by the meter and value.
  For stable communication, more than “15 (Green)” is needed. (No unit)
  Even if the signal strength is high, the communication may be unstable, depending on the adjacent active wireless LAN.
  The signal indication is just for reference.

[Wireless Status] screen

Information > Wireless Status

Wireless Bridge Status

Displays the status of APs that communicates with the AP-95M in the Bridge mode.



Wireless Bridge Status

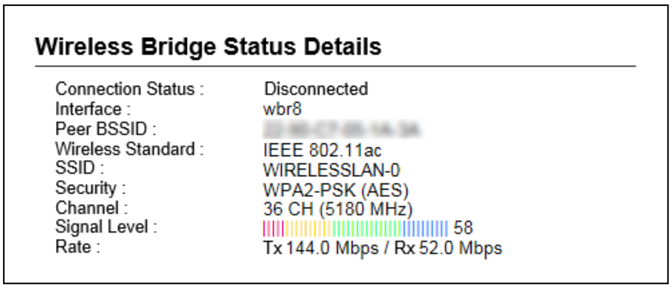
Interface	BSSID	RSSI	Rx Rate	Tx Rate	
wbr0	1E-90-C7-[redacted]	24	86.0 Mbps	86.0 Mbps	Details
wbr8	1E-90-C7-[redacted]				Details

- Interface: When the AP-95M is a Client, “wbr16” (Wireless 1) and “wbr17" (Wireless 2) are displayed.
- BSSID: BSSID of the AP that communicates with the AP-95M in the Bridge mode.
- Click <Details> for the details of the ongoing communication status. (See below)

Information > Wireless Status > Wireless Bridge Details

Wireless Bridge Status Details

This screen is displayed when you click <Details> on the [Wireless LAN Status] screen.



Wireless Bridge Status Details

Connection Status :	Disconnected
Interface :	wbr8
Peer BSSID :	[redacted]
Wireless Standard :	IEEE 802.11ac
SSID :	WIRELESSLAN-0
Security :	WPA2-PSK (AES)
Channel :	36 CH (5180 MHz)
Signal Level :	58
Rate :	Tx 144.0 Mbps / Rx 52.0 Mbps

Indication	[Red]	[Yellow]	[Green]	[Blue]
Level	0 ~ 4	5 ~ 14	15 ~ 29	30 and higher

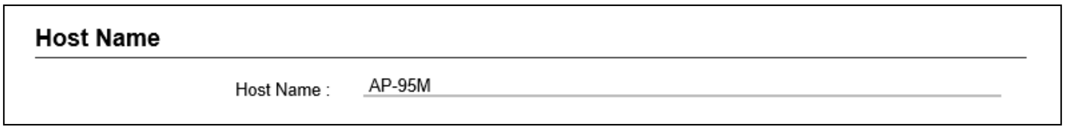
- The received signal strength is indicated by the meter and value.
  For stable communication, more than “15 (Green)” is needed. (No unit)
  Even if the signal strength is high, the communication may be unstable, depending on the adjacent active wireless LAN.
  The signal indication is just for reference.

[IP Address] Screen

Network Settings > IP Address

■Host Name

Enter the host name.



Host Name

Host Name : AP-95M

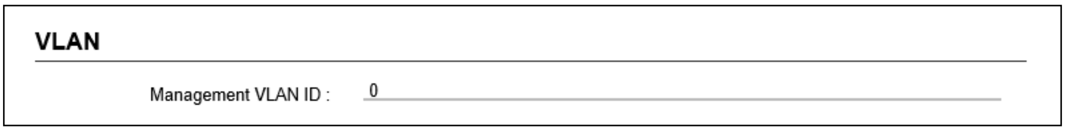
Host Name .... Enter a host name of up to 31 characters. (Default: AP-95M)

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

Network Settings > IP Address

■ VLAN

Enter the VLAN ID.



VLAN

Management VLAN ID : 0

Management VLAN ID .... Enter the VLAN ID. Permits access from devices on the network that have a matching ID. (Default: 0)

(Range: 0 ~ 4094)

- Enter "0" when permitting access from devices that have no VLAN ID assigned.

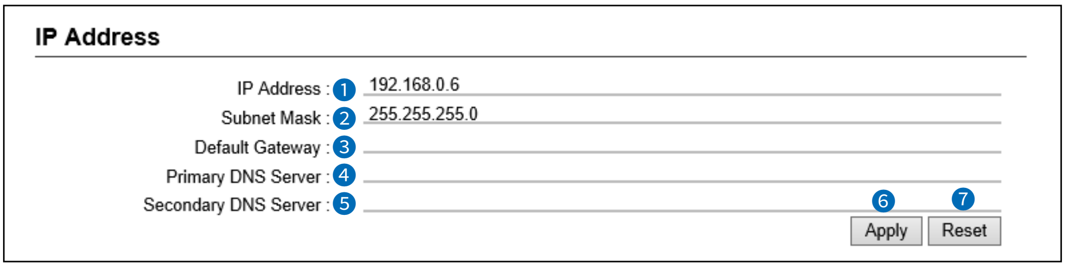
NOTE: You may not be able to access the setting screen, depending on the setting or condition.

[IP Address] Screen

Network Settings > IP Address

IP Address

Enter the AP-95M’s IP Address.



IP Address

IP Address : ❶ 192.168.0.6

Subnet Mask : ❷ 255.255.255.0

Default Gateway : ❸

Primary DNS Server : ❹

Secondary DNS Server : ❺

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

- 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. (p. 3-13)

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

- Set the subnet mask according to an existing LAN, when connecting the AP-95M to the LAN.

❸**Default Gateway** .... If a default gateway device, such as a router, is connected to the LAN port, enter the device’s IP address.

- Even if the default gateway is set to LAN, the network routing is set to WAN when the default gateway is set to WAN.

❹**Primary DNS Server** ...... Enter the DNS server address specified by your service provider.
Even if you have two DNS server addresses, enter the primary address.

❺**Secondary DNS Server**… If you have two DNS server addresses, enter the secondary DNS server address.

❻**<Apply>** .... Click to apply entries.

❼**<Reset>**....................... Click to reset the settings.

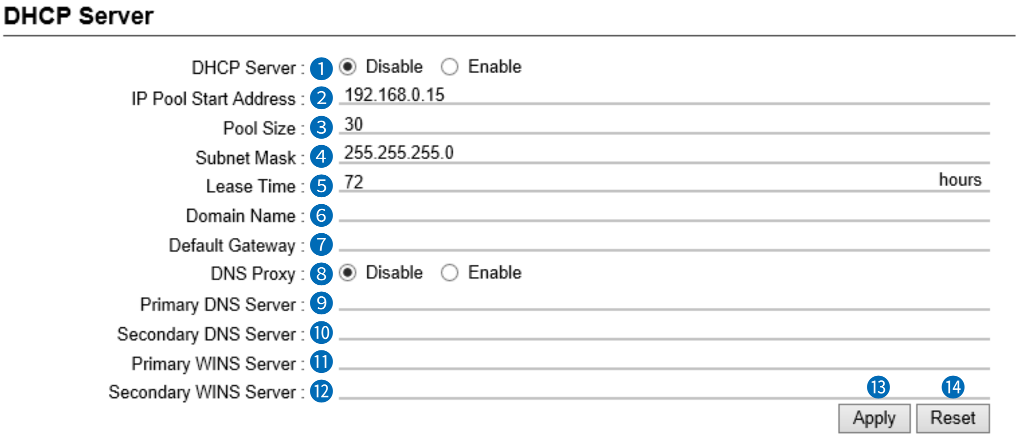
- You cannot reset after clicking <Apply>.

[DHCP Server] Screen

Network Settings > DHCP Server

■DHCP Server

Configure the DHCP Server function.



DHCP Server

DHCP Server : ① ● Disable ○ Enable

IP Pool Start Address : ② 192.168.0.15

Pool Size : ③ 30

Subnet Mask : ④ 255.255.255.0

Lease Time : ⑤ 72 hours

Domain Name : ⑥

Default Gateway : ⑦

DNS Proxy : ⑧ ● Disable ○ Enable

Primary DNS Server : ⑨

Secondary DNS Server : ⑩

Primary WINS Server : ⑪

Secondary WINS Server : ⑫

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

- If "Enable" is selected, the DHCP server functions according to the settings set in the [IP Pool Start Address] (❷) item and the [Pool Size] (❸) item.

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

❸Pool Size .... Enter the size of the 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.

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

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

Specify the lease time of IP address that is assigned by the DHCP server.

(Range: 1 ~ 9999 (hours))

❻Domain Name .... Enter a network address domain name of up to 253 characters.

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

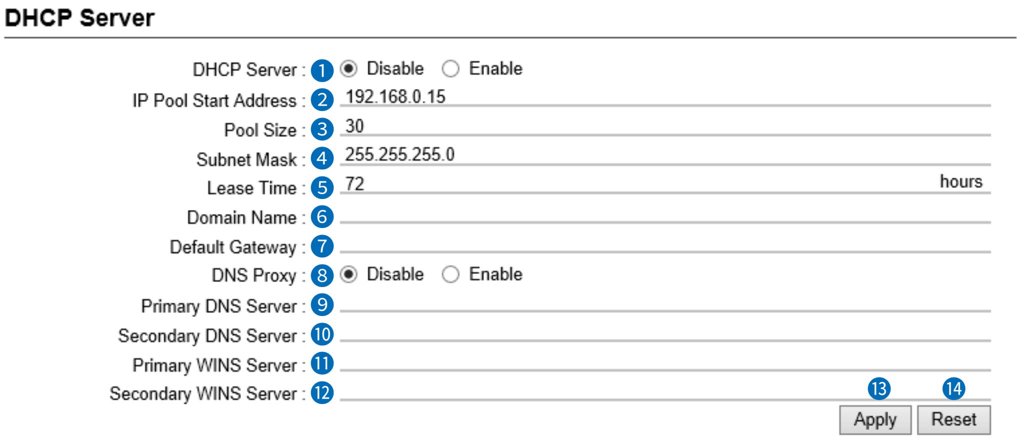
When the DHCP Server function is used, entered default gateway address is notified to the client.

- If this item is left blank, no gateway address is notified.

[DHCP Server] Screen

Network Settings > DHCP Server

■DHCP Server



DHCP Server

DHCP Server : ● Disable ○ Enable

IP Pool Start Address : 192.168.0.15

Pool Size : 30

Subnet Mask : 255.255.255.0

Lease Time : 72 hours

Domain Name :

Default Gateway :

DNS Proxy : ● Disable ○ Enable

Primary DNS Server :

Secondary DNS Server :

Primary WINS Server :

Secondary WINS Server :

⑧**DNS Proxy** .... Select "Enable" to use the DNS function. (Default: Disable)
The DNS function transfers the DNS request from a network device to the ISP's DNS server.
If you select "Enable," you do not have to change the network device settings, even when the DNS server address is changed.

⑨**Primary DNS Server** ...... Enter the DNS server address specified by your service provider.
If you have two DNS server addresses, enter the primary address.
- Entered address is notified to the DHCP client.

⑩**Secondary DNS Server**... If you have two DNS server addresses, enter the secondary DNS server address.

⑪**Primary WINS Server** ... Enter the WINS server's address. If you have two WINS server addresses, enter the primary address.

⑫**Secondary WINS Server**... If you have two WINS server addresses, enter the WINS server's secondary address.

⑬**<Apply>** .... Click to apply entries.

⑭**<Reset>**....................... Click to reset the settings.
- You cannot reset after clicking <Apply>.

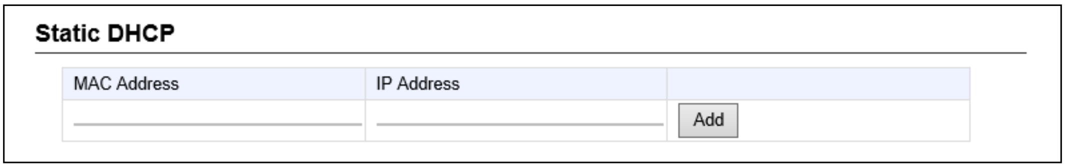
[DHCP Server] Screen

Network Settings > DHCP Server

■Static DHCP

Enter the MAC and static IP addresses to the DHCP server.

- You can enter up to 32 entries.



Static DHCP

MAC Address	IP Address	
		Add

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

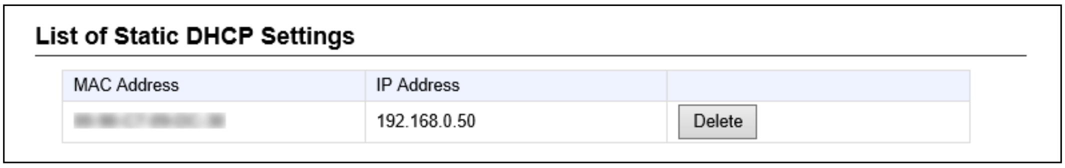
Note: Make sure that the addresses of the devices on the network don’t overlap or conflict. If a DHCP server is already connected to the network, and there is an address conflict, a network problem will occur. See the Troubleshooting section for possible solutions.

- This setting is valid when the DHCP Server function is enabled. (p. 3-13)

Network Settings > DHCP Server

■List of Static DHCP Settings

Displays the static DHCP entries.



List of Static DHCP Settings

MAC Address	IP Address	
[redacted]	192.168.0.50	Delete

(This is an example.)

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

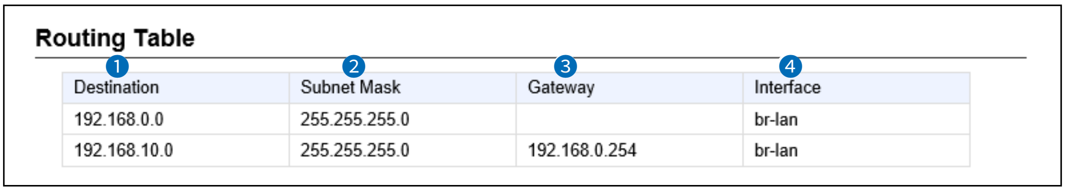
[Static Routing] Screen

Network Settings > Static Routing

■Routing Table

Displays the routing information.

- Only currently valid routing is displayed.



Routing Table

❶ Destination	❷ Subnet Mask	❸ Gateway	❹ Interface
192.168.0.0	255.255.255.0		br-lan
192.168.10.0	255.255.255.0	192.168.0.254	br-lan

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

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

❸**Gateway** .... The route’s gateway address.

❹**Interface** .... The routing interface to the destination IP address.

- **br-lan:** LAN interface
- **ppp0 ~ ppp7:** WAN01 ~WAN08 interface

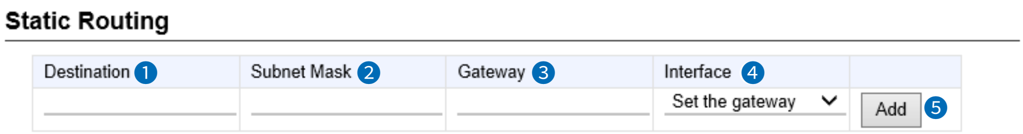
[Static Routing] Screen

Network Settings > Static Routing

Static Routing

Enter the static routing destinations.

- You can enter up to 32 entries.



Static Routing

Destination ❶	Subnet Mask ❷	Gateway ❸	Interface ❹	
			Set the gateway ∨	Add ❺

(This is an example.)

❶**Destination** .... Enter the network address of the route's destination network.

❷**Subnet Mask** .... Enter the subnet mask of the route's destination network.

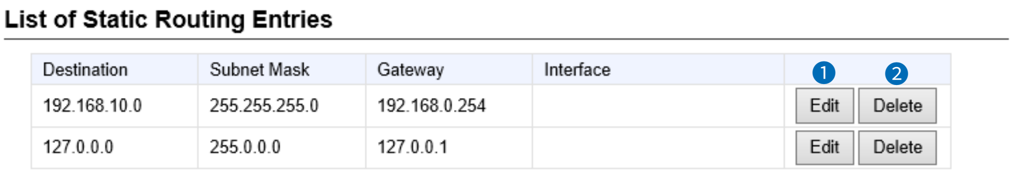
❸**Gateway** .... Enter the route’s gateway address.

❹**Interface** .... Select the destination interface from [Set the gateway], [ppp0(WAN01) ~ ppp7(WAN08).

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

Network Settings > Static Routing

List of Static Routing Entries



List of Static Routing Entries

Destination	Subnet Mask	Gateway	Interface	❶	❷
192.168.10.0	255.255.255.0	192.168.0.254		Edit	Delete
127.0.0.0	255.0.0.0	127.0.0.1		Edit	Delete

(This is an example.)

❶**<Edit>** .... Click <Edit> to Edit the entry.

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

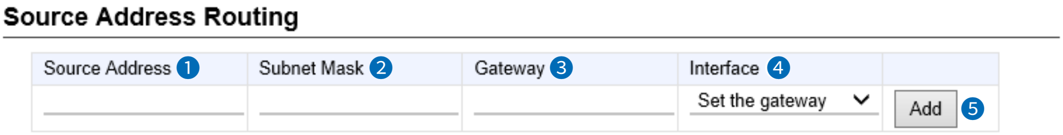
[Policy Routing] Screen

Network Settings > Policy Routing

Source Address Routing

Enter the routing source address.

- You can enter up to 32 entries.



Source Address Routing

Source Address ①	Subnet Mask ②	Gateway ③	Interface ④	
			Set the gateway	Add ⑤

①**Source Address** .... Enter the network address of the route's source network

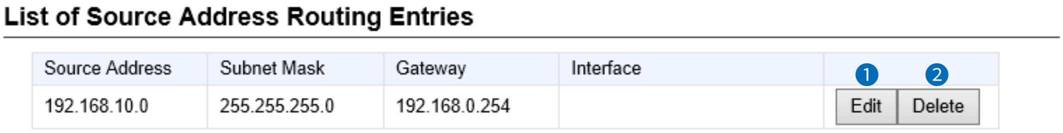
②**Subnet Mask** .... Enter the subnet mask of the route's source network.

③**Gateway** .... Enter the route’s gateway address.

④**Interface** .... Select the destination interface that the packet is transfered to, from [Set the gateway], [ppp0(WAN01) ~ ppp7(WAN08)].

⑤**<Add>** .... Click to add the entry.

List of Source Address Routing Entries



List of Source Address Routing Entries

Source Address	Subnet Mask	Gateway	Interface	① ②
192.168.10.0	255.255.255.0	192.168.0.254		Edit Delete

(This is an example.)

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

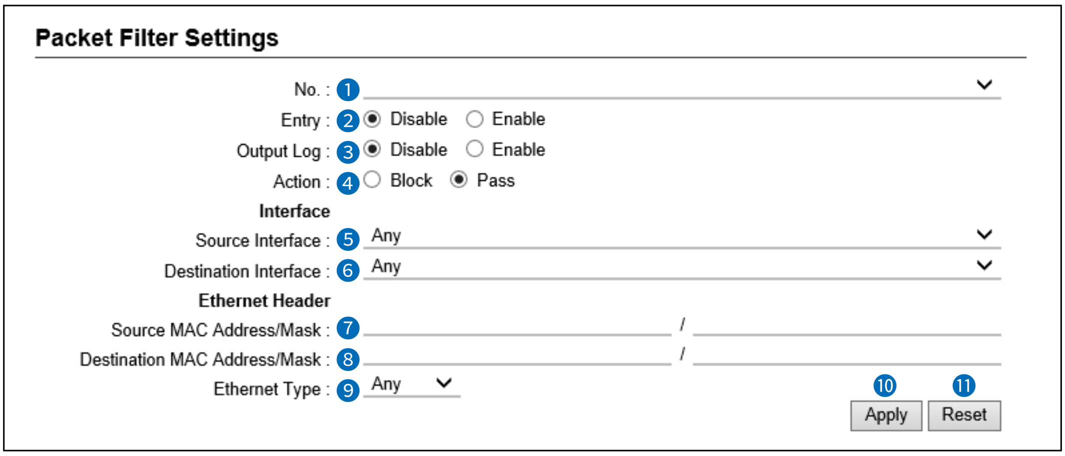
②**<Delete>** .... Click <Delete> to remove the entry.

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

Configure the Packet Filtering function.



Packet Filter Settings

No. : ①

Entry : ② ● Disable ○ Enable

Output Log : ③ ● Disable ○ Enable

Action : ④ ○ Block ● Pass

Interface

Source Interface : ⑤ Any

Destination Interface : ⑥ Any

Ethernet Header

Source MAC Address/Mask : ⑦ /

Destination MAC Address/Mask : ⑧ /

Ethernet Type : ⑨ Any

① No. .... Select the filtering order.
The Packet Filter function filters the receive, transmit or transfer packets in the selected order, according to the filtering criteria set in [List of Packet Filter Entries] (p. 3-31).
(Range: 1 ~ 64)
- When more than one filter settings are entered, filtering is executed in order of entry number. The least entry number in the matched filtering entries is executed and the rest of filtering entries are not executed.
- Filtering IPv6 packets is not supported.

② Entry .... Select "Enable" to apply the filter criteria. (Default: Disable)
Select "Disable" in the unused filter entry.

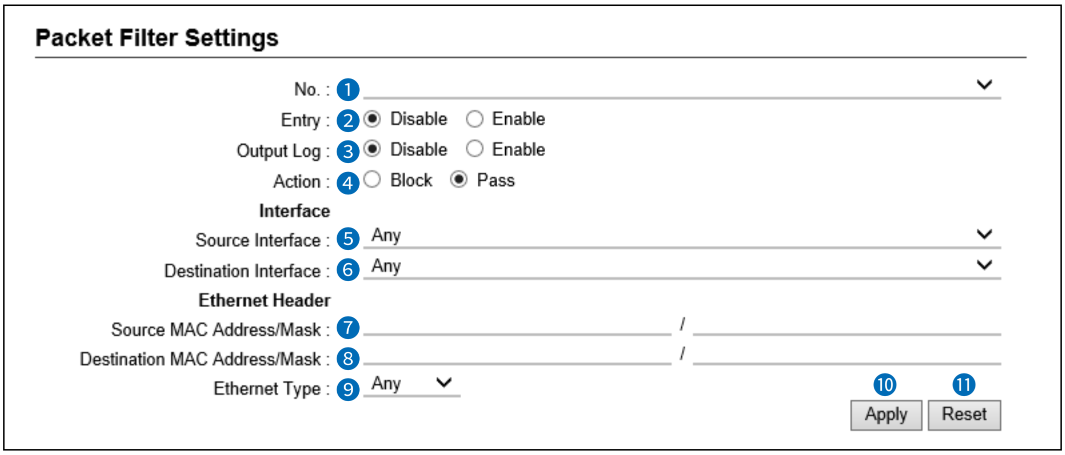
③ Output Log .... Select “Enable” to output the SYSLOG. (Default: Disable)
- The log information is displayed on the [SYSLOG] Screen in the [Information] menu.
- This function may affect the system performance when a huge amount of packets is processed. Using this only for testing purpose is recommended.

④ Action .... Select the filtering method. (Default: Pass)
- **Block:** Blocks all packets matched to the filtering criteria.
- **Pass:** Passes all packets matched to the filtering criteria.

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings



Packet Filter Settings

No. : ①

Entry : ② ● Disable ○ Enable

Output Log : ③ ● Disable ○ Enable

Action : ④ ○ Block ● Pass

Interface

Source Interface : ⑤ Any

Destination Interface : ⑥ Any

Ethernet Header

Source MAC Address/Mask : ⑦ /

Destination MAC Address/Mask : ⑧ /

Ethernet Type : ⑨ Any

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

- br-lan: Interface is AP-95M
- eth1: Interface is cable LAN
- ath0, ath01 ~ ath07: Interface is Wireless 1 (2.4 GHz)
- ath1, ath11 ~ ath17: Interface is Wireless 2 (5 GHz)
- wbr0 ~ wbr17: Interface is Bridging (WBR)
- If you select "Any," all these interfaces are set as the destination interface.

⑥Destination Interface...... Select the filtering interface. (Default: Any)

- br-lan: Interface is AP-95M
- eth1: Interface is cable LAN
- ath0, ath01 ~ ath07: Interface is Wireless 1 (2.4 GHz)
- ath1, ath11 ~ ath17: Interface is Wireless 2 (5 GHz)
- wbr0 ~ wbr17: Interface is Bridging (WBR)
- If you select "Any," all these interfaces are set as the destination interface.

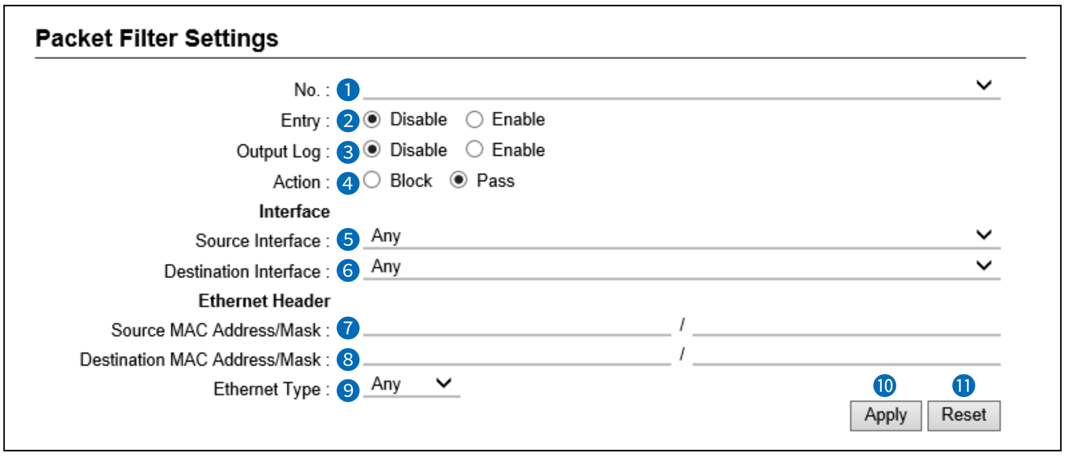
⑦Source MAC Address/Mask Set the source MAC address range as the filtering criteria.

- Enter the MAC address of 12 digits in hexadecimal.
- When this item is left blank, all MAC addresses are filtered.

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings



Packet Filter Settings

No. : ①

Entry : ② ● Disable ○ Enable

Output Log : ③ ● Disable ○ Enable

Action : ④ ○ Block ● Pass

Interface

Source Interface : ⑤ Any

Destination Interface : ⑥ Any

Ethernet Header

Source MAC Address/Mask : ⑦ /

Destination MAC Address/Mask : ⑧ /

Ethernet Type : ⑨ Any

⑩ Apply ⑪ Reset

⑧Destination MAC Address/Mask

Set the destination MAC address range as the filtering criteria.
- Enter the MAC address of 12 digits in hexadecimal.

(Format: "MAC address" + "/" + "Mask")

Example of enterig a MAC address and mask value:

Entered characters are automatically capitalized.

Example 1) Destination MAC Address/Mask

"00-90-C7-3C-00-64/(Blank)"

The following MAC address will be displayed in the [List of Packet Filter Entriess] item. (p.3-31)

"00-90-C7-3C-00-64/FF-FF-FF-FF-FF-FF"

- When the Mask part is not entered, "FF-FF-FF-FF-FF-FF" is automatically set.
- In this example, the network device whose MAC address is "00-90-C7-3C-00-64" will be filtered (locked out).

Example 2) Destination MAC Address/Mask

"00-90-C7-3C-00-64/FF-FF-FF-00-00-00"

The following MAC address will be displayed in the [List of Packet Filter Entriess] item (p. 3-31).

"00-90-C7-00-00-00/FF-FF-FF-00-00-00"

- Since the logical AND of the mask value is "0," the network device whose part of MAC address is "00-90-C7" will be filtered (locked out).

Expample 3) Destination MAC Address/Mask

"00-90-C7-3C-00-64/FF-FF-FF-00-00-FF"

The following MAC address is displayed in the [List of Packet Filter Entriess] item (p. 3-31).

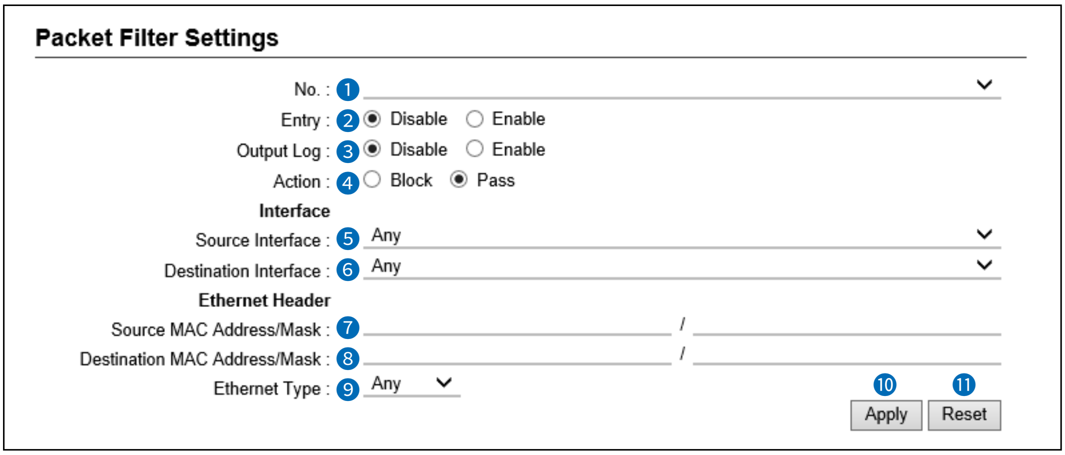
"00-90-C7-00-00-64/FF-FF-FF-00-00-FF"

- The network device whose MAC address is between "00-90-C7-00-00-64" to "00-90-C7-FF-FF-64" will be filtered (locked out).

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings



Packet Filter Settings

No. : ❶

Entry : ❷ ● Disable ○ Enable

Output Log : ❸ ● Disable ○ Enable

Action : ❹ ○ Block ● Pass

Interface

Source Interface : ❺ Any

Destination Interface : ❻ Any

Ethernet Header

Source MAC Address/Mask : ❼ /

Destination MAC Address/Mask : ❽ /

Ethernet Type : ❾ Any

❾**Ethernet Type** .... Select the transport layer’s protocol to filter. (Default: Any)

• If "Custom" is selected, a text box appears. Enter the ethernet type in hexadecimal (0600 ~ FFFF) in the box.

(Entered characters are automatically capitalized.)

• See following pages for each network type.

VLAN:	Page 3-23 ~ 3-27
ARP:	Page 3-28
IPv4:	Page 3-29 and 3-30

❿**<Apply>** .... Click to save the entry.

⓫**<Reset>**........................ Click to reset the entry.

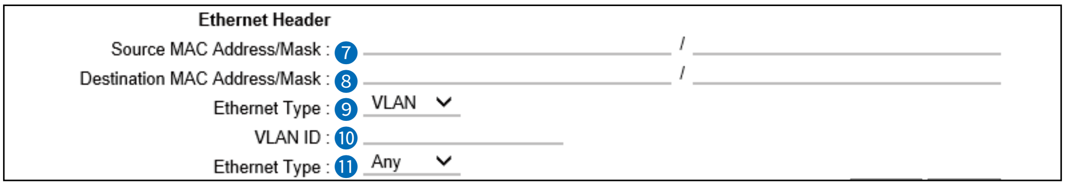
You cannot reset the entries after pushing <Apply>.

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

This screen is displayed when "VLAN" is selected in the [Ethernet Type] (❾) item, and "Any" is selected in the [Ethernet Type] (⓫) item.



Ethernet Header

Source MAC Address/Mask : ❼ /

Destination MAC Address/Mask : ❽ /

Ethernet Type : ❾ VLAN

VLAN ID : ❿

Ethernet Type : ⓫ Any

❿ VLAN ID .... Enter the VLAN ID as the filtering criteria. (Default: (blank))
(Range: 1 ~ 4094)

- If this item is left blank, any VLAN ID is filtered.

⓫ Ethernet Type .... Select the Ethernet type name (Any/ARP/IPv4/Custom) as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered. (Default: Any)

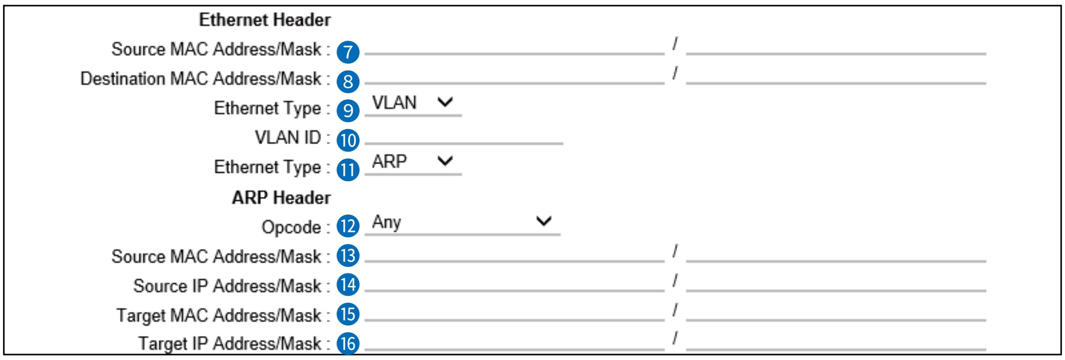
- If "Custom" is selected, a text box appears. Enter the ethernet type in hexadecimal (0600 ~ FFFF) in the box.
- See following pages for each network type.
  ARP: Page 3-24
  IPv4: Page 3-25 ~ 3-27

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

This screen is displayed when "VLAN" is selected in the [Ethernet Type] (❾) item, and "ARP" is selected in the [Ethernet Type] (⓫) item.



Ethernet Header
Source MAC Address/Mask : ❼ /
Destination MAC Address/Mask : ❽ /
Ethernet Type : ❾ VLAN
VLAN ID : ❿
Ethernet Type : ⓫ ARP
ARP Header
Opcode : ⓬ Any
Source MAC Address/Mask : ⓭ /
Source IP Address/Mask : ⓮ /
Target MAC Address/Mask : ⓯ /
Target IP Address/Mask : ⓰ /

⓬ Opcode................................ Select the ARP type (Any, request, reply or Custom) as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered. (Default: Any)

- If "Any" is selected, any ARP type is filtered.
- If "Custom" is selected, a text box appears. Enter the opcode in decimal (0 ~ 65535) in the box.

⓭ Source MAC Address/Mask ... Set the source MAC address range as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered.

- Enter the MAC address of 12 digit in hexadecimal.

⓮ Source IP Address/Mask......... Set the source IP Address range as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered.

⓯ Target MAC Address/Mask...... Set the Target MAC address range as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered.

- Enter the MAC address of 12 digit in hexadecimal.

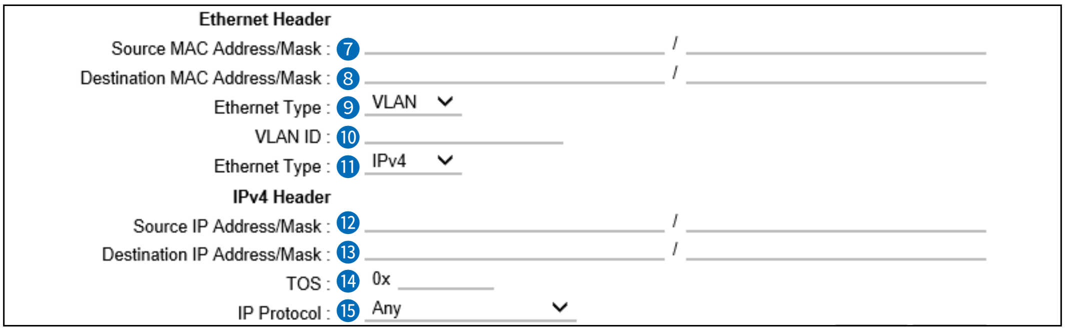
⓰ Target IP Address/Mask .... Set the Target IP address range as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered.

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

This screen is displayed when "VLAN" is selected in the [Ethernet Type] (❾) item, or "IPv4" is selected in the [EthernetType] (⓫) item, and "Any," "ICMP" or "IGMP" is selected in the [IP Protocol] (⓯) item.



Ethernet Header

Source MAC Address/Mask : ❼ /

Destination MAC Address/Mask : ❽ /

Ethernet Type : ❾ VLAN

VLAN ID : ❿

Ethernet Type : ⓫ IPv4

IPv4 Header

Source IP Address/Mask : ⓬ /

Destination IP Address/Mask : ⓭ /

TOS : ⓮ 0x

IP Protocol : ⓯ Any

⓬ **Source IP Address/Mask ....** Set the source IP Address range as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered.

- Set the range by the mask (subnet mask).
- For example, when "192.168.0.0/255.255.255.0" is set, the packet whose IP address, that is in the range of 192.168.0.0 ~ 192.168.0.255, is filtered.
- If the mask is not set, only exactly-matching IP address is filtered.

⓭ **Destination IP Address/Mask** Set the range of the destination IP Address as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered.

- Set the range by the mask (subnet mask).
- For example, "192.168.0.0/255.255.255.0" is entered, the packet whose IP address, that is in the range of 192.168.0.0 ~ 192.168.0.255, is filtered.
- If the mask is not set, only exactly-matching IP address is filtered.

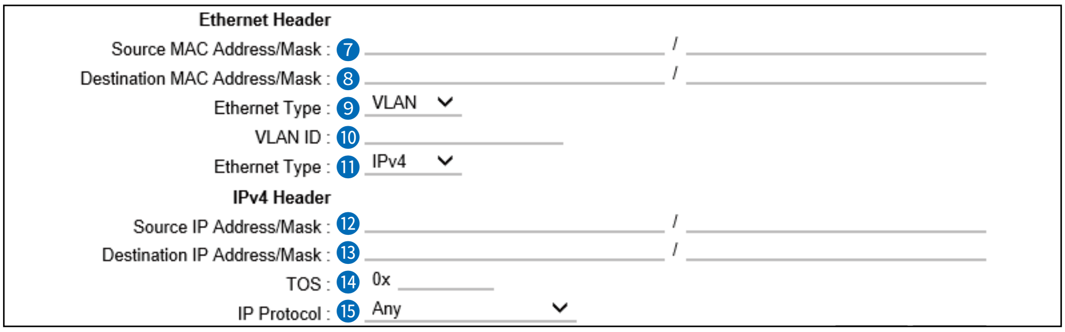
⓮ **TOS ....** Set the value of the TOS (Type Of Service) as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered (Range: 00 ~ FF)

- Entered characters are automatically capitalized.

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings



Ethernet Header

Source MAC Address/Mask : ⑦ /

Destination MAC Address/Mask : ⑧ /

Ethernet Type : ⑨ VLAN

VLAN ID : ⑩

Ethernet Type : ⑪ IPv4

IPv4 Header

Source IP Address/Mask : ⑫ /

Destination IP Address/Mask : ⑬ /

TOS : ⑭ 0x

IP Protocol : ⑮ Any

⑮ **IP Protocol** .... Set the protocol, that is located in the transport layer, as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (⑩) item, is to be filtered. (Default: Any)

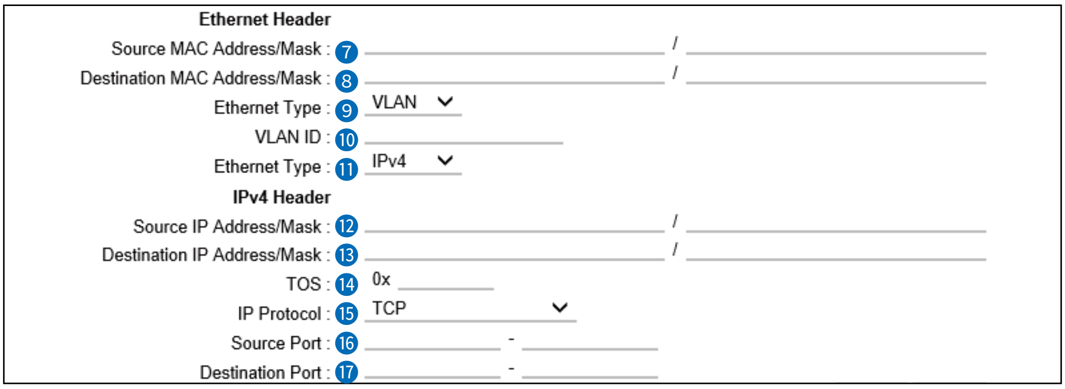
Any:	Any protocol
ICMP:	Only ICMP
IGMP:	Only IGMP
TCP:	Only TCP
UDP:	Only UDP
Custom:	Enter the protocol number located in the transport layer. (Range: 0 ~ 255 in decimal)

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

This screen is displayed when "VLAN" is selected in the [Ethernet Type] (❾) item, or "IPv4" is selected in the [Ethernet Type] (⓫) item, and "TCP" or "UDP" is selected in the [IP Protocol] (⓯) item.



Ethernet Header

Source MAC Address/Mask : ❼ /
Destination MAC Address/Mask : ❽ /
Ethernet Type : ❾ VLAN
VLAN ID : ❿
Ethernet Type : ⓫ IPv4

IPv4 Header

Source IP Address/Mask : ⓬ /
Destination IP Address/Mask : ⓭ /
TOS : ⓮ 0x
IP Protocol : ⓯ TCP
Source Port : ⓰ -
Destination Port : ⓱ -

⓰ **Source Port**........................... Set the source TCP or UDP port numbers (start and end points) as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is filtered.

To specify only one port, set only the start, point or enter the same port number in both start and end points.

(Range: 0 ~ 65535)

⓱ **Destination Port**..................... Set the Destination TCP or UDP port number (start and end points) as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item, is to be filtered.

To specify only one port, set only the start, point or enter the same port number in both start and end points.

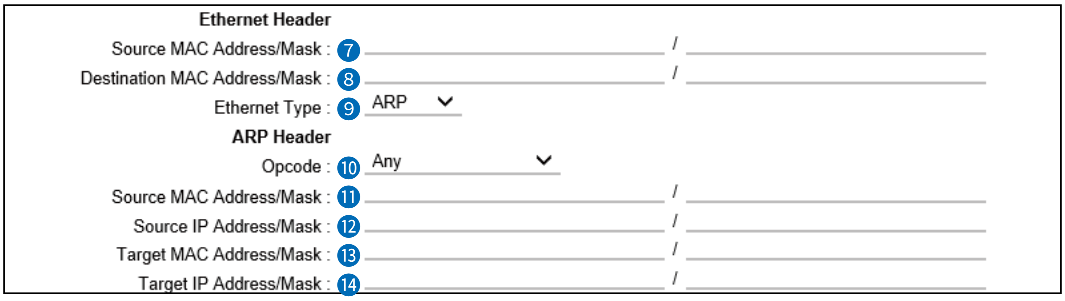
(Range: 0 ~ 65535)

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

This screen is displayed when "ARP" is selected in the [Ethernet Type] (❾) item.



Ethernet Header

Source MAC Address/Mask : ❼ /

Destination MAC Address/Mask : ❽ /

Ethernet Type : ❾ ARP

ARP Header

Opcode : ❿ Any

Source MAC Address/Mask : ⓫ /

Source IP Address/Mask : ⓬ /

Target MAC Address/Mask : ⓭ /

Target IP Address/Mask : ⓮ /

❿ Opcode................................ Select the ARP type (Any, request, reply or custom) as the filtering criteria. The packet encapsulated by a VLAN ID, that is set in the [VLAN ID] (❿) item (p.3-23), is filtered. (Default: Any)

- If "Any" is selected, any ARP type is filtered.
- If "Custom" is selected, a text box appears. Enter the opcode in decimal (0 ~ 65535).

⓫ Source MAC Address/Mask ... Set the range of the source MAC address as the filteing criteria.

- Enter the MAC address of 12 digits in hexadecimal.

⓬ Source IP Address/Mask .... Set the range of the source IP Address as the filteing criteria.

⓭ Target MAC Address/Mask ...... Set the range of the Target MAC address as the filteing criteria.

- Enter the MAC address of 12 digits in hexadecimal.

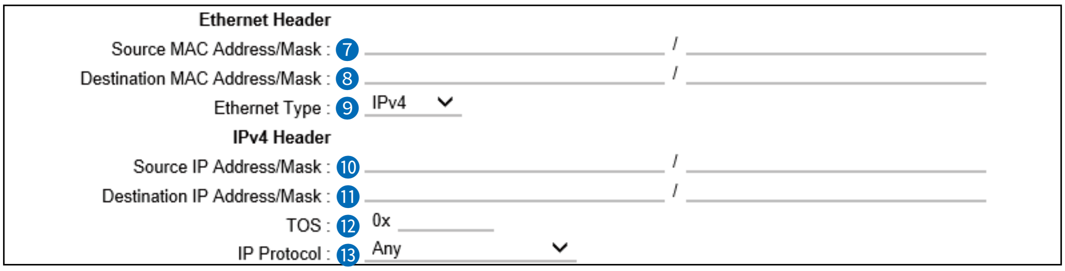
⓮ Target IP Address/Mask .... Set the range of the Target IP address as the filteing criteria.

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

This screen is displayed when "IPv4" is selected in the [Ethernet Type] (⑨) item, and "Any," "ICMP" or "IGMP" is selected in the [IP Protocol] (⑬) item.



Ethernet Header

Source MAC Address/Mask : ⑦ /

Destination MAC Address/Mask : ⑧ /

Ethernet Type : ⑨ IPv4

IPv4 Header

Source IP Address/Mask : ⑩ /

Destination IP Address/Mask : ⑪ /

TOS : ⑫ 0x

IP Protocol : ⑬ Any

⑩ **Source IP Address/Mask** .... Set the range of the source IP Address in the IPv4 header as the filteing criteria.

- Set the range by the mask (subnet mask).
- For example, when "192.168.0.0/255.255.255.0" is set, the packet whose IP address, that is in the range of 192.168.0.0 ~ 192.168.0.255, is filtered.
- If the mask is not set, only exactly-matching IP address is filtered.

⑪ **Destination IP Address/Mask** .... Set the range of the destination IP Address in the IPv4 header as the filteing criteria.

- Set the range by the mask (subnet mask).
- For example, when "192.168.0.0/255.255.255.0" is set, the packet whose IP address, that is in the range of 192.168.0.0 ~ 192.168.0.255, is filtered.
- If the mask is not set, only exactly-matching IP address is filtered.

⑫ **TOS** .... Set the TOS (Type Of Service) in the IPv4 header as the filteing criteria.
(Range: 00 ~ FF in hexadecimal)

- Entered characters are automatically capitalized.

⑬ **IP Protocol** .... Set the protocol, that is located in the transport layer in the IPv4 header, as the filtering criteria. (Default: Any)

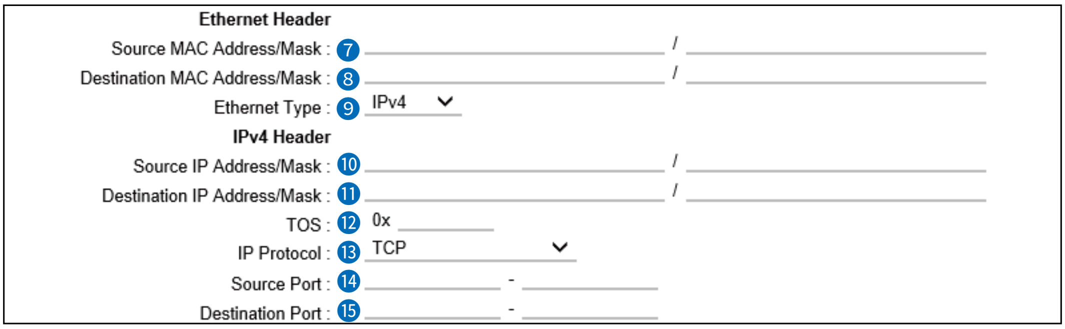
Any: Any protocol
ICMP: Only ICMP
IGMP: Only IGMP
TCP: Only TCP
UDP: Only UDP
Custom: Enter the protocol number located in the transport layer.
(Range: 0 ~ 255 in decimal)

[Packet Filter] Screen

Network Settings > Packet Filter

■Packet Filter Settings

This screen is displayed when IPv4" is selected in the [Ethernet Type] (❾) item, and "TCP" or "UDP" is selected in the [IP Protocol] (⓭) item.



Ethernet Header

Source MAC Address/Mask : ❼ /

Destination MAC Address/Mask : ❽ /

Ethernet Type : ❾ IPv4

IPv4 Header

Source IP Address/Mask : ❿ /

Destination IP Address/Mask : ⓫ /

TOS : ⓬ 0x

IP Protocol : ⓭ TCP

Source Port : ⓮ -

Destination Port : ⓯ -

⓮ Source Port.......................... Set the source TCP or UDP port number (start and end points) as the filtering criteria.
To specify only one port, set only the start, point or enter the same port number to both start and end points.
(Range: 0 ~ 65535)

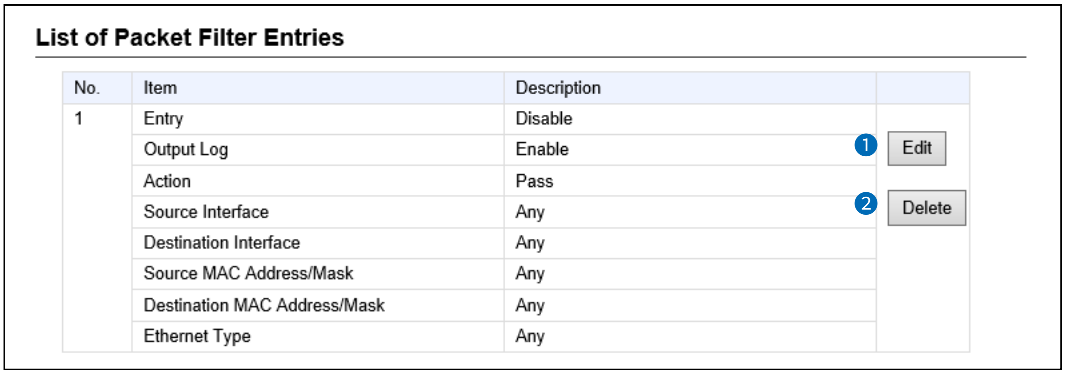
⓯ Destination Port..................... Set the destination TCP or UDP port number (start and end points) as the filtering criteria.
To specify only one port, set only the start, point or enter the same port number to both start and end points.
(Range: 0 ~ 65535)

[Packet Filter] Screen

Network Settings > Packet Filter

■ List of Packet Filter Entries

Displays the packet filter entries.



List of Packet Filter Entries

No.	Item	Description	
1	Entry	Disable	
	Output Log	Enable	❶ Edit
	Action	Pass	
	Source Interface	Any	❷ Delete
	Destination Interface	Any	
	Source MAC Address/Mask	Any	
	Destination MAC Address/Mask	Any	
	Ethernet Type	Any	

❶ **<Edit>** .... Click to edit the packet filter entry.
• The Packet Filter setting screen (p.3-19) opens.

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

Using the Packet Filter

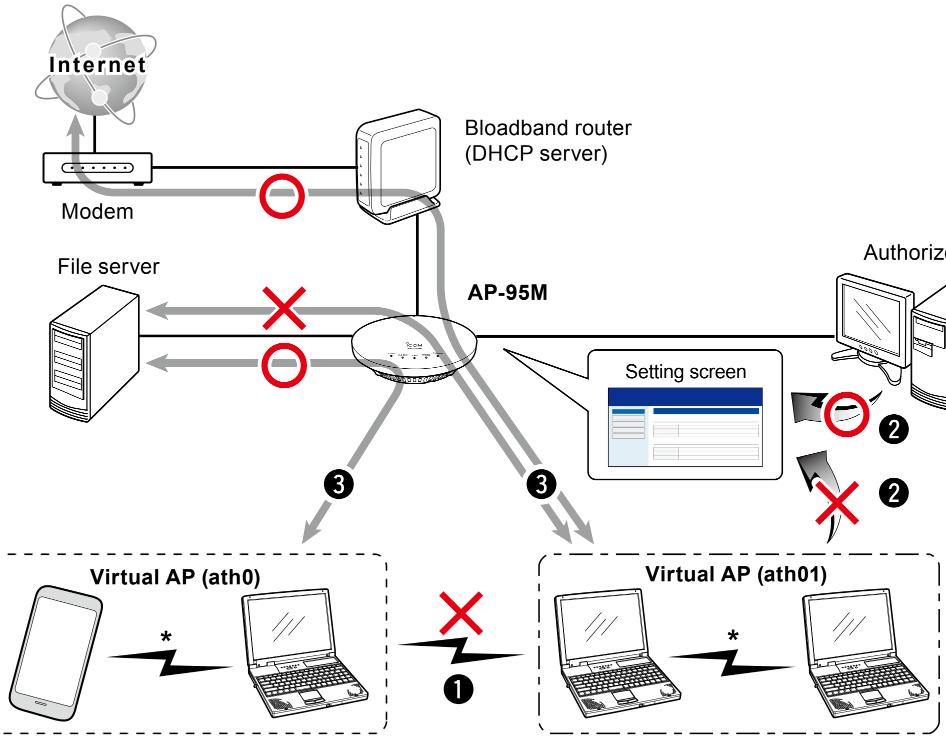
Network Settings > Packet Filter

■ Packet Filtering Examples

Example 1) Inhibiting the communication between stations that are in different Virtual APs (Example: ath0 and ath01). (P.3-33)

Example 2) Limiting the access to the AP-95M setting screen. (P.3-34)

Example 3) Inhibiting the connection to a cable LAN through the virtual AP, but permitting access to the Internet. (P.3-35)



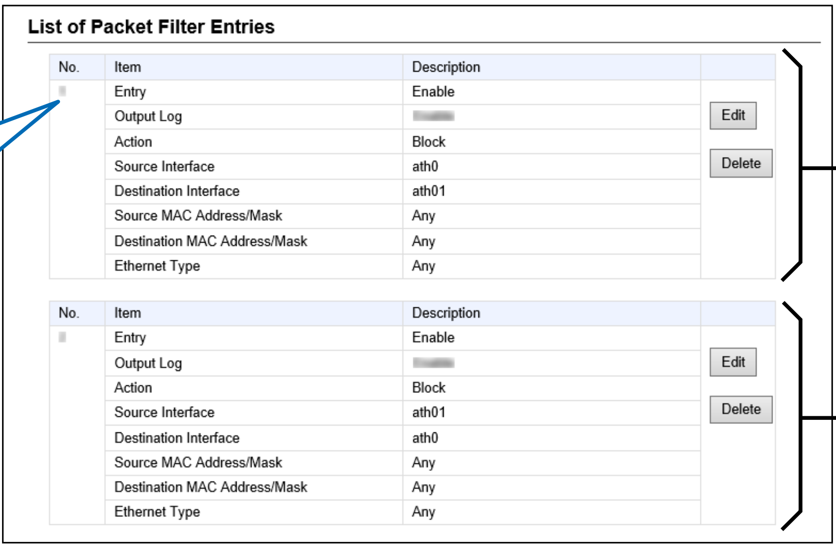
* To inhibit the communication between wireless LAN stations in a Virtual AP's wireless network, select "Enable" in the [Privacy Separator] item on the Virtual AP (Example: ath0 and ath01) setting screen. (p. 3-70)
The Packet Filter function cannot inhibit communication in the same Virtual AP's wireless network.

Using the Packet Filter

Network Settings > Packet Filter

Example 1) Inhibiting communication between stations that are in different Virtual APs (Example: ath0 and ath01).

You need to add the 2 packet filter setting entries below (❶ and ❷).



List of Packet Filter Entries

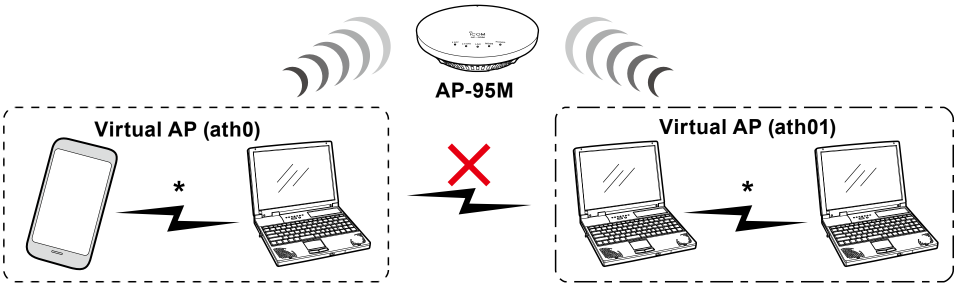
No.	Item	Description	
[illegible]	Entry	Enable	
	Output Log	[illegible]	Edit
	Action	Block	
	Source Interface	ath0	Delete
	Destination Interface	ath01	
	Source MAC Address/Mask	Any	
	Destination MAC Address/Mask	Any	
	Ethernet Type	Any	

No.	Item	Description	
[illegible]	Entry	Enable	
	Output Log	[illegible]	Edit
	Action	Block	
	Source Interface	ath01	Delete
	Destination Interface	ath0	
	Source MAC Address/Mask	Any	
	Destination MAC Address/Mask	Any	
	Ethernet Type	Any	

Filter setting entry number

❶ Blocks packets from Virtual AP "ath0" to Virtual AP "ath01."

❷ Blocks packets from Virtual AP "ath01" to Virtual AP "ath0."



* To inhibit the communication between wireless LAN stations in a Virtual AP's wireless network, select "Enable" in the [Privacy Separator] item on the Virtual AP (Example: ath0 and ath01) setting screen. (p. 3-70)
The Packet Filter function cannot inhibit communication in the same Virtual AP's wireless network.

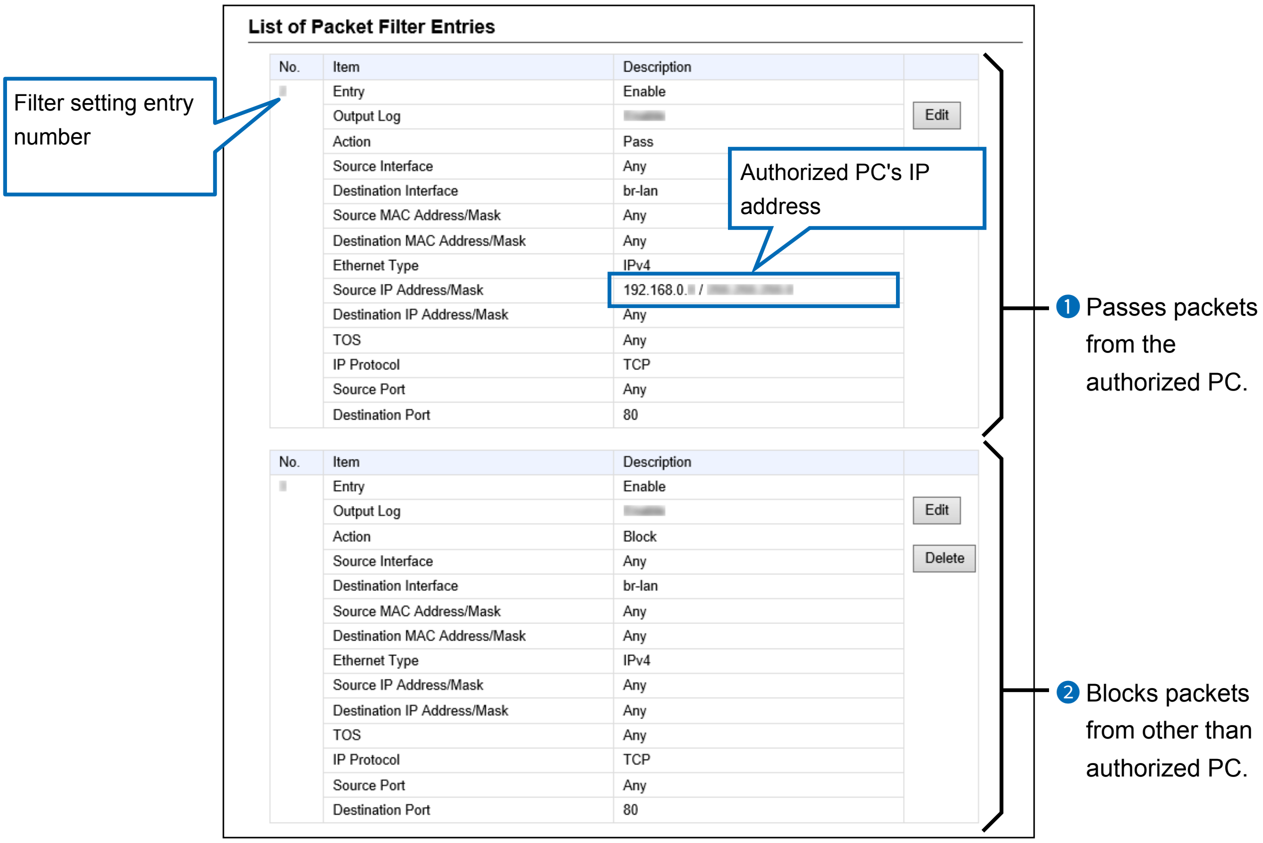
Using the Packet Filter

Network Settings > Packet Filter

Example 2) Limiting the access to the AP-95M setting screen.

You need to add the 2 packet filter setting entries below (❶ and ❷).

- This is an example of setting the Management ID (VLAN setting) to "0."
- Enter a transparent setting entry first, then enter a blocking setting entry.
  When deleting entries, delete the blocking setting entries first, then delete the transparent setting entries. Otherwise, the PC used to configure the AP-95M may not access the settings screen again.



List of Packet Filter Entries

No.	Item	Description	
[redacted]	Entry	Enable	
	Output Log	[redacted]	Edit
	Action	Pass	
	Source Interface	Any	
	Destination Interface	br-lan	
	Source MAC Address/Mask	Any	
	Destination MAC Address/Mask	Any	
	Ethernet Type	IPv4	
	Source IP Address/Mask	192.168.0.[redacted] / [redacted]	
	Destination IP Address/Mask	Any	
	TOS	Any	
	IP Protocol	TCP	
	Source Port	Any	
	Destination Port	80	

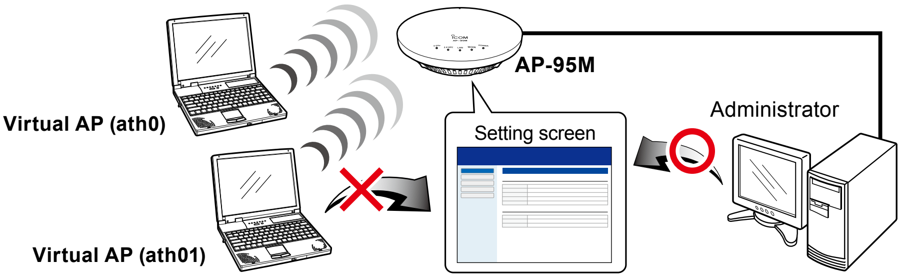
No.	Item	Description	
[redacted]	Entry	Enable	
	Output Log	[redacted]	Edit
	Action	Block	Delete
	Source Interface	Any	
	Destination Interface	br-lan	
	Source MAC Address/Mask	Any	
	Destination MAC Address/Mask	Any	
	Ethernet Type	IPv4	
	Source IP Address/Mask	Any	
	Destination IP Address/Mask	Any	
	TOS	Any	
	IP Protocol	TCP	
	Source Port	Any	
	Destination Port	80	

Filter setting entry number

Authorized PC's IP address

❶ Passes packets from the authorized PC.

❷ Blocks packets from other than authorized PC.



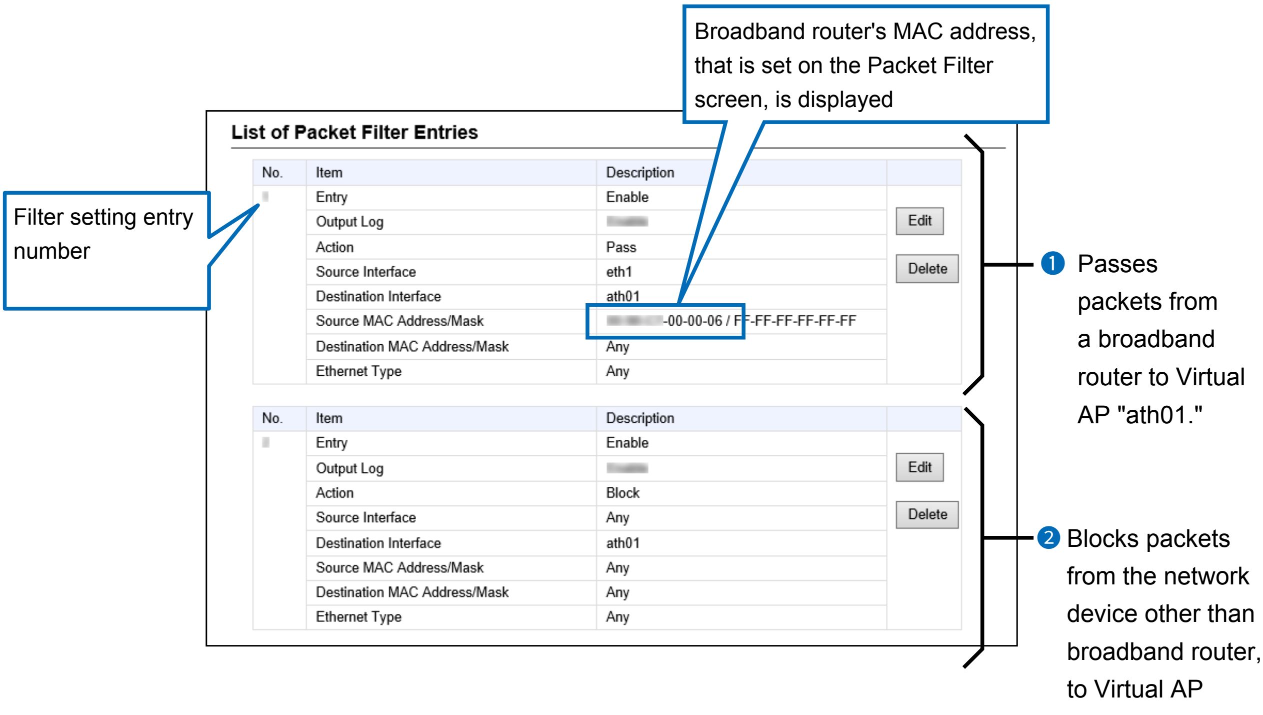
Using the Packet Filter

Network Settings > Packet Filter

Example 3) Inhibiting the connection to a cable LAN through the virtual AP, but permitting the access to the Internet.

You need to add the 2 filter setting entries below (❶ and ❷).

- Add the transparent settings, depending on the DHCP server.



Broadband router's MAC address, that is set on the Packet Filter screen, is displayed

Filter setting entry number

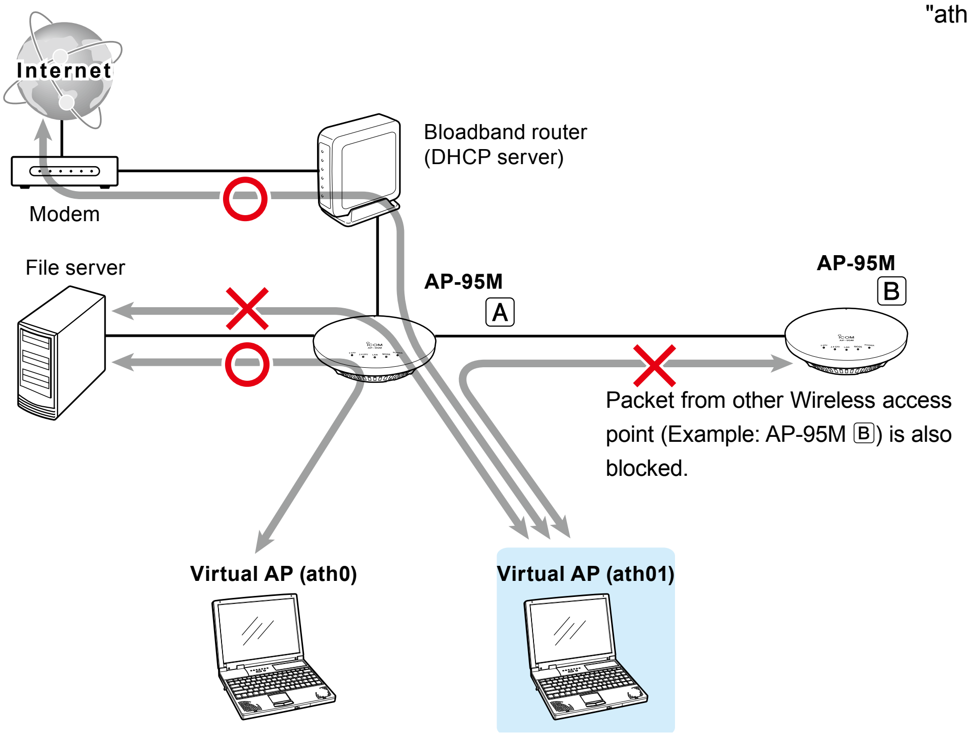
List of Packet Filter Entries

No.	Item	Description	
[redacted]	Entry	Enable	
	Output Log	[redacted]	Edit
	Action	Pass	
	Source Interface	eth1	Delete
	Destination Interface	ath01	
	Source MAC Address/Mask	[redacted]-00-00-06 / FF-FF-FF-FF-FF-FF	
	Destination MAC Address/Mask	Any	
	Ethernet Type	Any	

❶ Passes packets from a broadband router to Virtual AP "ath01."

No.	Item	Description	
[redacted]	Entry	Enable	
	Output Log	[redacted]	Edit
	Action	Block	
	Source Interface	Any	Delete
	Destination Interface	ath01	
	Source MAC Address/Mask	Any	
	Destination MAC Address/Mask	Any	
	Ethernet Type	Any	

❷ Blocks packets from the network device other than broadband router, to Virtual AP "ath01."



Packet from other Wireless access point (Example: AP-95M B) is also blocked.

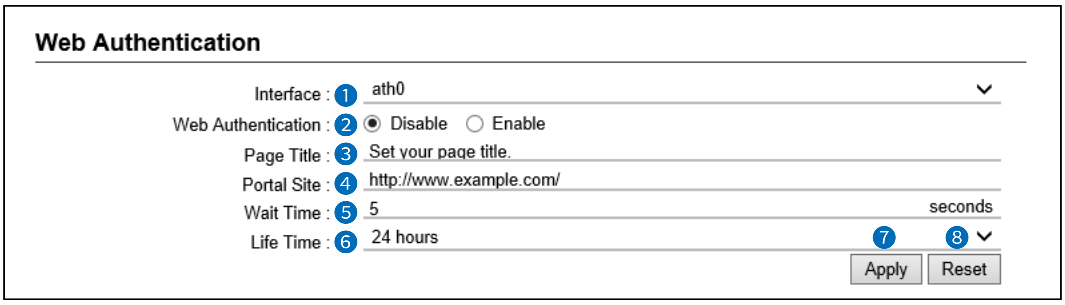
[Web Authentication Basic] Screen

Network Settings > Web Authentication > Basic

■ Web Authentication

The Web Authentication function displays the authentication screen on the client's (network user's) web browser when the network user attempts to access a web site, through the AP-95M. On the authentication screen, the user will be required to enter the User name and Password to continue.

- Set both “Basic” and “Advanced” screens.
- When the network user accessed a web site whose URL starts with "https://," the authentication screen is not displayed.



Web Authentication

Interface : ath0

Web Authentication : ● Disable ○ Enable

Page Title : Set your page title.

Portal Site : http://www.example.com/

Wait Time : 5 seconds

Life Time : 24 hours

❶ **Interface** .... Select a Virtual AP to change the setting. (Default: ath0)

- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.
- Each interface has setting items, as shown below.
  - [Web Authentication] item
  - [Custom Page] item (p. 3-38)
  - Each item on the [Web Authentication Detail] Screen (p. 3-42)

❷ **Web Authentication** .... Select "Enable" to use the Web Authentication function for the interface that is selected in the [Interface] (❶) item. (Default: Disable)

- To use the Web Authentication function, the Virtual AP is also enabled.
- If JavaScript is disabled in the web browser, items and values may not be correctly displayed.

❸ **Page Title**.............................. Enter the Web authentication screen title. (In 255 characters)
(Default: "Set your page title.")

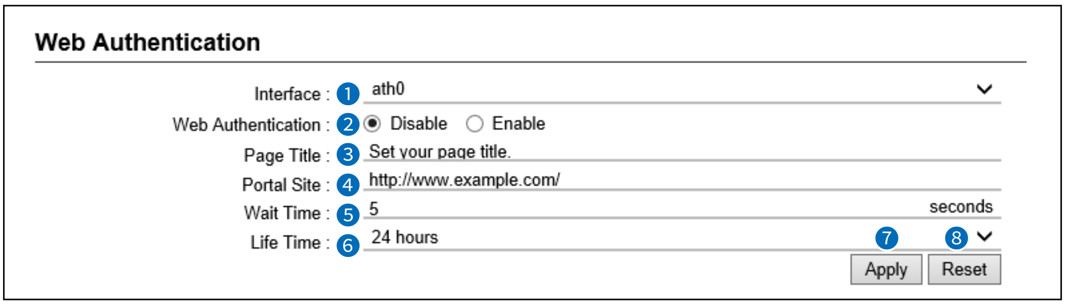
❹ **Portal Site** .... Enter the portal site URL that the web browser automatically accesses after the authentication is successful. (In 255 characters)
(Default: http://www.example.com/)

[Web Authentication Basic] Screen

Network Settings > Web Authentication > Basic

■ Web authentication

- Set both “Basic” and “Advanced” screens.
- When the network user access a web site whose URL starts with "https://," the authentication screen is not displayed.



Web Authentication

Interface : ① ath0

Web Authentication : ② ● Disable ○ Enable

Page Title : ③ Set your page title.

Portal Site : ④ http://www.example.com/

Wait Time : ⑤ 5 seconds

Life Time : ⑥ 24 hours

⑤ Wait Time .... Enter the delay time until the browser automatically accesses the portal site after authentication is successful. (Default: 5)
(Range: 0 ~ 60 seconds)

⑥ Life Time .... Set the web authentication valid period. (Default: 24 hours)
After the set time is expired, reauthentication required.
(Options: 5, 10, 15, 30 minutes, 1, 2, 4, 8, 12 or 24 hours)

⑦ <Apply> .... Click to save the entry.

⑧ <Reset>................................ Click to reset the entry.
- You cannot reset the entries after pushing <Apply>.

NOTE: Before leaving the setting screen
Before leaving the setting screen, click <Apply> to save. Otherwise, all the changes have been made will be discarded.

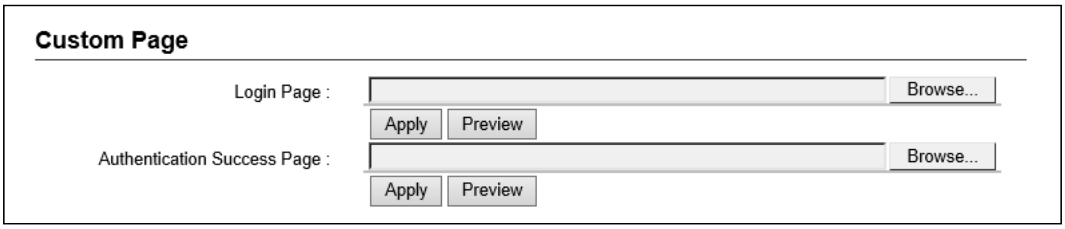
[Web Authentication Basic] Screen

Network Settings > Web Authentication > Basic

■ Custom Page

You can change the Web authentication screen by modifying the page source code (extension: tmpl). See the next page for details.

- The source code size is up to 32 kB.

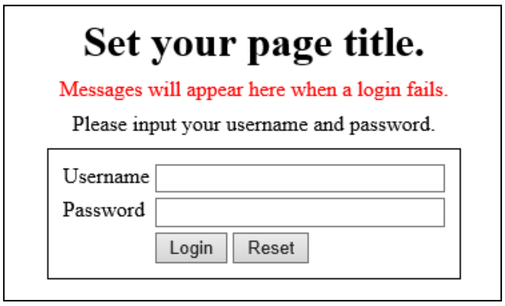


How to modify the custom page:

1. Click <Browse> and select the location to save the source code (Extention: tmpl).
2. Click <Apply>.
   - Click <Preview> to display the page.
   - Click <Reset> to restore the page to the default.
     (You cannot restore the page even after pushing <Apply>.)

Information: About the default authentication screen

- The default Log-in screen

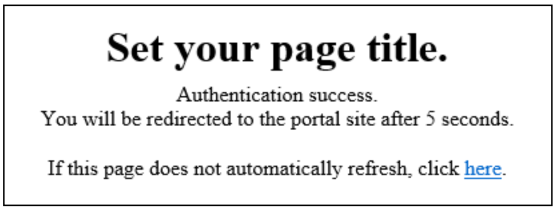


Set your page title.

Messages will appear here when a login fails.

Please input your username and password.

- The default authentication success screen



Set your page title.

Authentication success.
You will be redirected to the portal site after 5 seconds.

If this page does not automatically refresh, click here.

[Web Authentication Basic] Screen

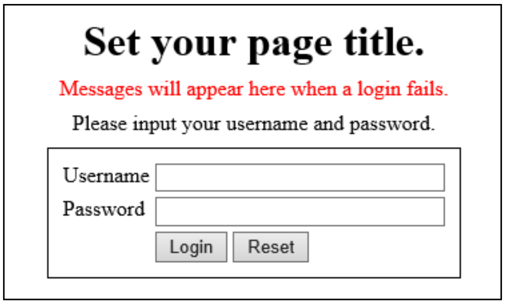
Network Settings > Web Authentication > Basic

■ Custom Page

Modify the default source code, to make your own authentication screen.

- The character code must be UTF-8.
- You cannot make a hyper link to any web site.

Log-in page suorce code:



Set your page title.

Messages will appear here when a login fails.

Please input your username and password.

Username

Password

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="Content-Style-Type" content="text/css">
    <meta http-equiv="Pragma" content="no-cache">
    <style type="text/css">
    <!--
      body {
          text-align: center;
      }
      table {
          margin-right: auto;
          margin-left: auto;
      padding: 8px;
      border: 1px solid;
              border-color: black;
      width: auto;
      }
      td {
          vertical-align: top;
          white-space: nowrap;
      border: 0px;
      }
      .main {
          text-align: left;
      }
      .title {
          text-align: center;
      margin: 8px;
      }
      .notice {
          text-align: center;
      margin: 8px;
      color: red;
      }
      .info {
          text-align: center;
      margin: 8px;
```

[Web Authentication Basic] Screen

Network Settings > Web Authentication > Basic

■ Custom Page

Log-in page source code:

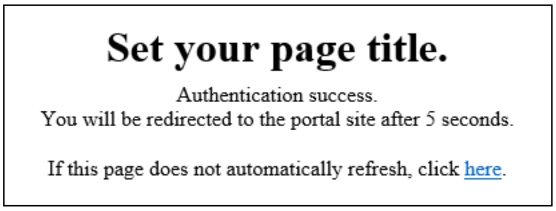
```
   }
   .center {
     text-align: center;
   }
   .input {
   width: 16em;
   }
  -->
  </style>
  <title>Set your page title.</title>
 </head>
 <body>
  <form target="_self" method="POST">
   <div class="main">
    <h1 class="title">Set your page title.</h1>
    <div class="notice">
     Messages will appear here when a login fails.
    </div>
    <div class="info">
     Please input your username and password.
    </div>
    <table>
     <tr>
      <td>Username</td>
      <td>
       <input class="input" type="text" maxlength="128" name="user">
      </td>
     </tr>
     <tr>
      <td>Password</td>
      <td>
       <input class="input" type="password" maxlength="128" name="pass">
      </td>
     </tr>
     <tr>
      <td></td>
      <td>
       <input type="button" value="Login">
       <input type="reset" value="Reset">
      </td>
     </tr>
    </table>
   </div>
  </form>
 </body>
</html>
```

[Web Authentication Basic] Screen

Network Settings > Web Authentication > Basic

■ Custom Page

Authentication success page source code:



Set your page title.

Authentication success.
You will be redirected to the portal site after 5 seconds.

If this page does not automatically refresh, click here.

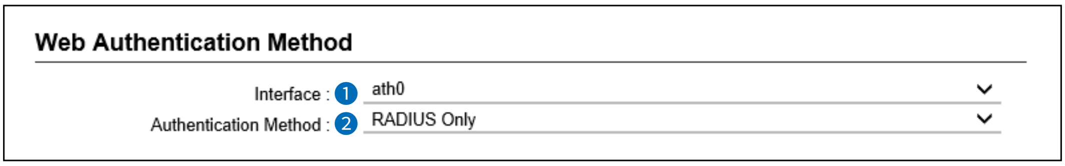
```
<!DOCTYPE HTML PUBLIC · -//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
 <head>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta http-equiv="Content-Style-Type" content="text/css">
  <meta http-equiv="Pragma" content="no-cache">
  <meta http-equiv="Refresh" content="5;URL=http:&#47;&#47;www.example.com&#47;">
  <style type="text/css">
  <!--
   body {
   text-align: center;
   }
   .main {
   text-align: left;
   }
   .title {
   text-align: center;
   margin: 8px;
   }
   .info {
   text-align: center;
   margin: 8px;
   }
  -->
  </style>

  <title>Set your page title.</title>
 </head>
 <body>
  <div class="main">
   <h1 class="title">Set your page title.</h1>
   <div class="info">
    Authentication success.<br>
    You will be redirected to the portal site after 5 seconds.<br>
    <br>
    If this page does not automatically refresh, click <a href="http://www.example.com/">here</a>.
   </div>
  </div>
 </body>
</html>
```

[Web Authentication Advanced] Screen

Network Settings > Web Authentication > Advanced

■ Web Authentication Method

Set the Web authentication method for each Virtual AP.



Web Authentication Method

Interface : ① ath0

Authentication Method : ② RADIUS Only

① Interface .... Select a Virtual AP to change the setting. (Default: ath0)

- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.

② Authentication Method .... Select the Web authentication method for the interface that is set in the [Interface] (①) item. (Default: RADIUS Only)

RADIUS Only:

Use only the RADIUS server for the authentication.

- Set the RADIUS server first. (p. 3-43)

Local List Only:

Use the user information (Displayed on the [List of Users] Screen (p. 3-44)) for the authentication.

- Set the local list first.

Local List First:

Use the user information (Displayed on the [List of Users] Screen (pp. 3-43 and 3-44)) for authentication.

If the user information is not obtained the RADIUS server that is set on the [RADIUS] Screen will be used for authentication.

- Set the RADIUS server and local list first.

RADIUS First:

Use the RADIUS server for authentication.

If the response from the RADIUS server is not obtained, the user information (Displayed on the [List of Users] Screen (pp. 3-43 and 3-44)) will be used for authentication.

- Set the RADIUS server and local list first.
- If JavaScript is disabled in the web browser, items and values may not be correctly displayed.

[Web Authentication Advanced] Screen

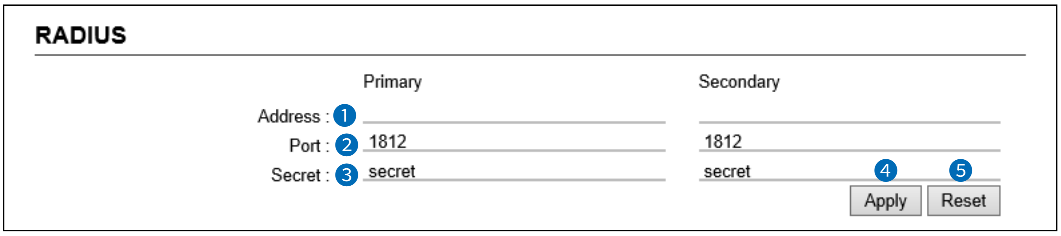
Network Settings > Web Authentication > Advanced

RADIUS

Set the web authentication method for each Virtual AP.

If there is second RADIUS server, set items for the second RADIUS server too.

- This screen is not displayed when "Local List Only" is selected in the [Authentication Method] item. (p. 3-42)



RADIUS

	Primary	Secondary
Address : ❶		
Port : ❷	1812	1812
Secret : ❸	secret	secret

❶ **Address** .... Enter the RADIUS server address.

❷ **Port** .... Enter the authentication port. (Default: 1812)
(Range: 1 ~ 65535)
- The default value may differ, depending on the system configuration.

❸ **Secret** .... Enter the Key for communication between the AP-95M and the RADIUS server. (Default: secret)
Set the same Key to the AP-95M and RADIUS server of up to 64 characters.

❹ **<Apply>** .... Click to save the entry.

❺ **<Reset>** .... Click to reset the entry.
- You cannot reset the entries after pushing <Apply>.

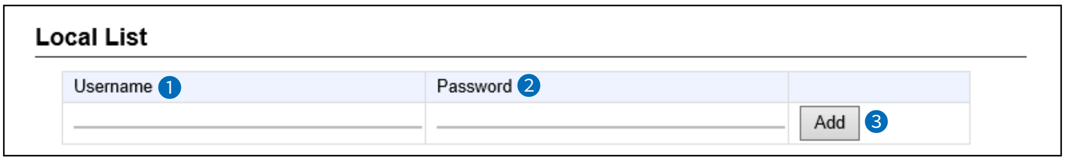
[Web Authentication Advanced] Screen

Network Settings > Web Authentication > Advanced

Local List

Enter the User name and Password for the Web authentication.

- Up to 32 users can be registered.
- This screen is not displayed if [RADIUS] is selected in the [Authentication Method] item. (p. 3-42)



Local List

Username ①	Password ②	
		Add ③

① **Username** .... Enter a User name of up to 128 alphanumeric characters.
- You cannot leave this item blank.

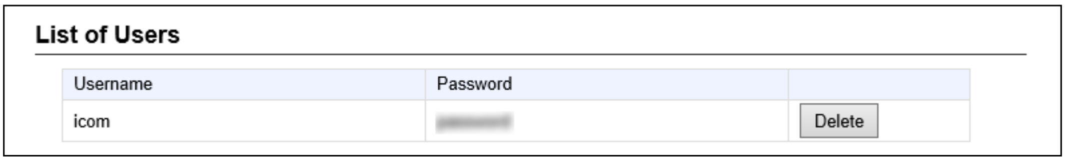
② **Password**............................. Enter a Password of up to 128 alphanumeric characters.
- You cannot leave this item blank.

③ **<Add>** .... Click to save the entry.

Network Settings > Web Authentication > Advanced

List of Users

Displays the all entries set on the [Local List] Screen.



List of Users

Username	Password	
icom	[redacted]	Delete

(This is an example.)

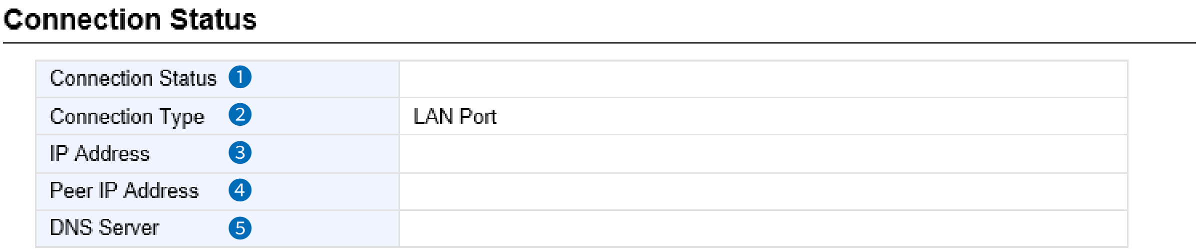
<Delete> .... Click to delete the entry.

5. [WAN] Screen

Router Settings > WAN

■Connection Status LAN Port

Displays the WAN connection status.



Connection Status

Connection Status ❶	
Connection Type ❷	LAN Port
IP Address ❸	
Peer IP Address ❹	
DNS Server ❺	

❶**Connection Status**......... This item is blank when "LAN Port" is selected as the connection type.

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

❸**IP Address** .... This item is blank when "LAN Port" is selected as the connection type.

❹**Peer IP Address** .... This item is blank when "LAN Port" is selected as the connection type.

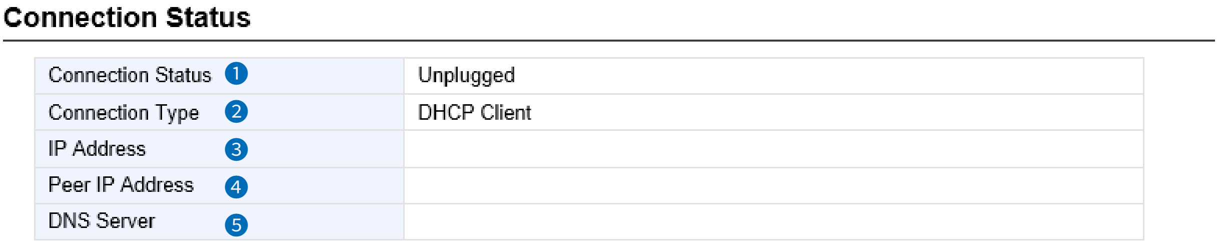
❺**DNS Server** .... This item is blank when "LAN Port" is selected as the connection type.

5. [WAN] Screen

Router Settings > WAN

■Connection Status DHCP Client

Displays the WAN connection status.



Connection Status

Connection Status ①	Unplugged
Connection Type ②	DHCP Client
IP Address ③	
Peer IP Address ④	
DNS Server ⑤	

①**Connection Status**......... Displays the WAN connection status (Connecting, Connected, Disconnected or Unplugged).

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

③**IP Address** .... Displays the AP-95M's WAN IP address.

④**Peer IP Address** .... Displays the gateway IP address obtained by the DHCP.

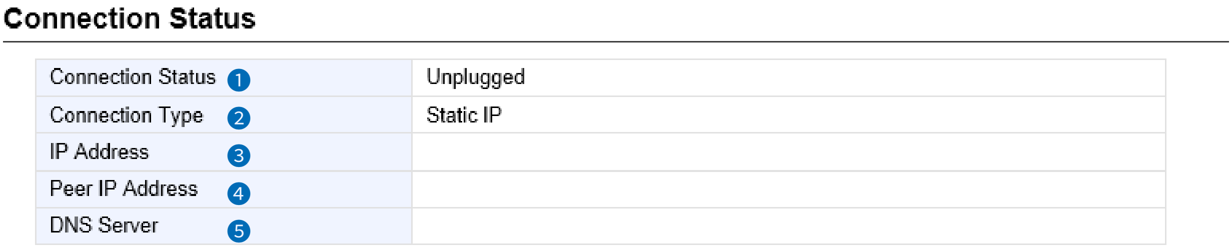
⑤**DNS Server** .... Displays the DNS server's IP address.

5. [WAN] Screen

Router Settings > WAN

■Connection Status Static IP

Displays the WAN connection status.



Connection Status

Connection Status ①	Unplugged
Connection Type ②	Static IP
IP Address ③	
Peer IP Address ④	
DNS Server ⑤	

①**Connection Status**......... Displays the WAN connection status (Connected, Disconnected or Unplugged).

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

③**IP Address** .... Displays the AP-95M's WAN IP address.

④**Peer IP Address** .... Displays the gateway IP address that is manually set.

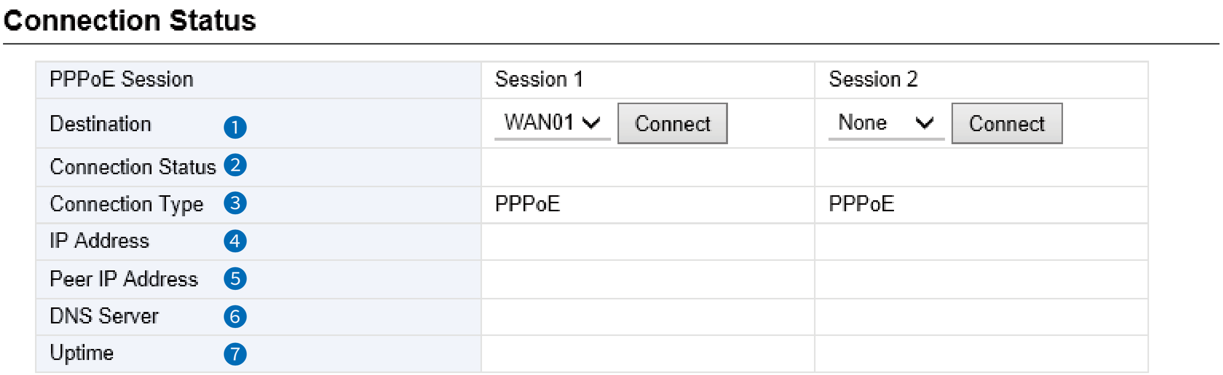
⑤**DNS Server** .... Displays the DNS server's IP address.

5. [WAN] Screen

Router Settings > WAN

■Connection Status PPPoE

Displays the WAN connection status for each session.



Connection Status

PPPoE Session	Session 1	Session 2
Destination ❶	WAN01 ⌄ Connect	None ⌄ Connect
Connection Status ❷		
Connection Type ❸	PPPoE	PPPoE
IP Address ❹		
Peer IP Address ❺		
DNS Server ❻		
Uptime ❼		

❶Destination .... Select the WAN connection to display the connection status.

- You cannot change this setting while the WAN is connected.

<Connect>

Click to connect to an unconnected session.

<Disconnect>

Click to disconnection the session.

❷Connection Status......... Displays the WAN connection status. (Connecting, Connected, Disconnected or Unplugged)

❸Connection Type .... Displays the WAN connection type.

❹IP Address .... Displays the AP-95M's WAN IP address.

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

❻DNS Server .... Displays the DNS server's IP address.

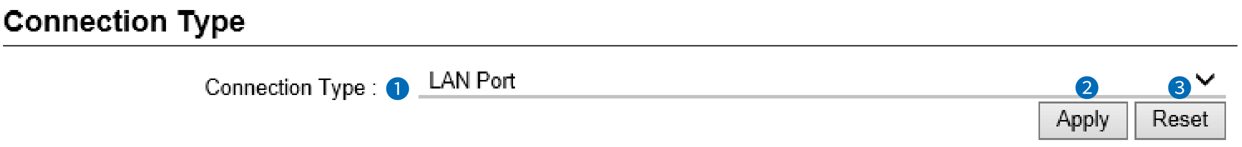
❼Uptime .... Displays the elapsed time the AP-95M has been connected to the network.

5. [WAN] Screen

Router Settings > WAN

■Connection Type

Select the WAN connection type.



Connection Type

Connection Type : ① LAN Port

①Connection Type .... Select the WAN connection type that is specified by your ISP.

(Default: LAN Port)

When "DHCP Client," "Static IP" or "PPPoE" is selected, the Router function is enabled.

When the AP-95M's WAN port is NOT connected to the Internet:

• "LAN Port"

Select this when you use the Ethernet port as a LAN port.

When the AP-95M's WAN port is connected to the Internet:

• "DHCP Client"

The WAN IP address is automatically obtained by your ISP in the DHCP method.

• "Static IP"

The WAN IP address (Static) is specified by your ISP.

• "PPPoE"

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

② <Apply> .... Click to apply entries.

③ <Reset> .... Click to reset the settings.

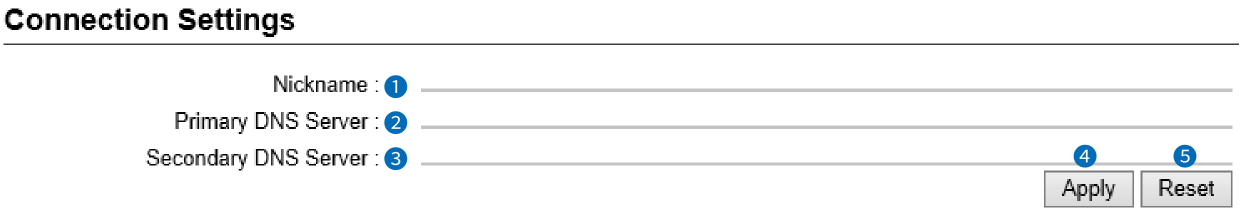
• You cannot reset after clicking <Apply>.

5. [WAN] Screen

Router Settings > WAN

■Connection Settings DHCP Client

Configure the WAN connection.


Connection Settings

Nickname : ①

Primary DNS Server : ②

Secondary DNS Server : ③

①**Nickname** .... Enter a connection name of 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.

④ **<Apply>** .... Click to apply entries.

⑤ **<Reset>** .... Click to reset the settings.
• You cannot reset the entries after pushing <Apply>.

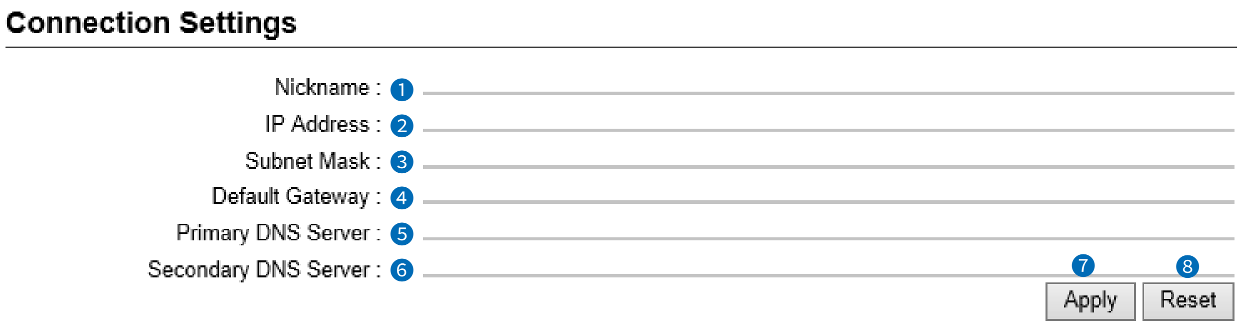
NOTE: About the obtaining IP address by the DHCP function
When the DHCP function is used and if both the Primary DNS Server item and Secondary DNS Server item are left blank, the IP address will be automatically obtained.

5. [WAN] Screen

Router Settings > WAN

■Connection Settings Static IP

Configure the WAN connection.



Connection Settings

Nickname : ①

IP Address : ②

Subnet Mask : ③

Default Gateway : ④

Primary DNS Server : ⑤

Secondary DNS Server : ⑥

❶**Nickname** .... Enter an ISP's name of up to 31 characters.

❷**IP Address** .... Enter the WAN IP address as specified by your ISP.

❸**Subnet Mask** .... Enter the subnet mask as specified by your ISP.

❹**Default Gateway**............ Enter the default gateway address as specified by your ISP.

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

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

❼ **<Apply>** .... Click to apply entries.

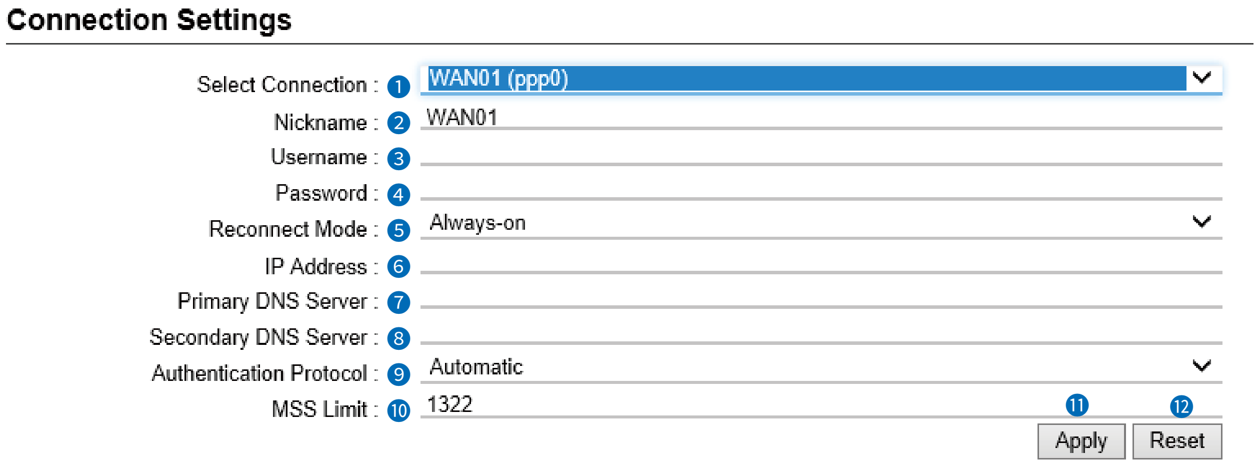
❽ **<Reset>** .... Click to reset the settings.
• You cannot reset the entries after pushing <Apply>.

5. [WAN] Screen

Router Settings > WAN

■Connection Settings PPPoE

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



Connection Settings

Select Connection : ❶ WAN01 (ppp0)

Nickname : ❷ WAN01

Username : ❸

Password : ❹

Reconnect Mode : ❺ Always-on

IP Address : ❻

Primary DNS Server : ❼

Secondary DNS Server : ❽

Authentication Protocol : ❾ Automatic

MSS Limit : ❿ 1322

❶Select Connection .... Select a WAN connecting destination to add, from "WAN01 (ppp0)" ~ "WAN08 (ppp7)". Up to 8 destination can be registered.

(Default: WAN01 (ppp0))

To change connection settings, select the destination by the nickname set in the "Nickname" item below.

❷Nickname .... Enter an ISP's name of up to 31 characters.

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

❹Password .... Enter a login password.

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

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

• Manual

The PPPoE line can be manually connected or disconnected, by clicking <Connect> or <Disconnect>. (p. 3-48)

- The line is disconnected on boot.

• Always-on

The PPPoE line is always connected.

The connection to the line that is set in the [Select Connection] (❶) item is maintained.

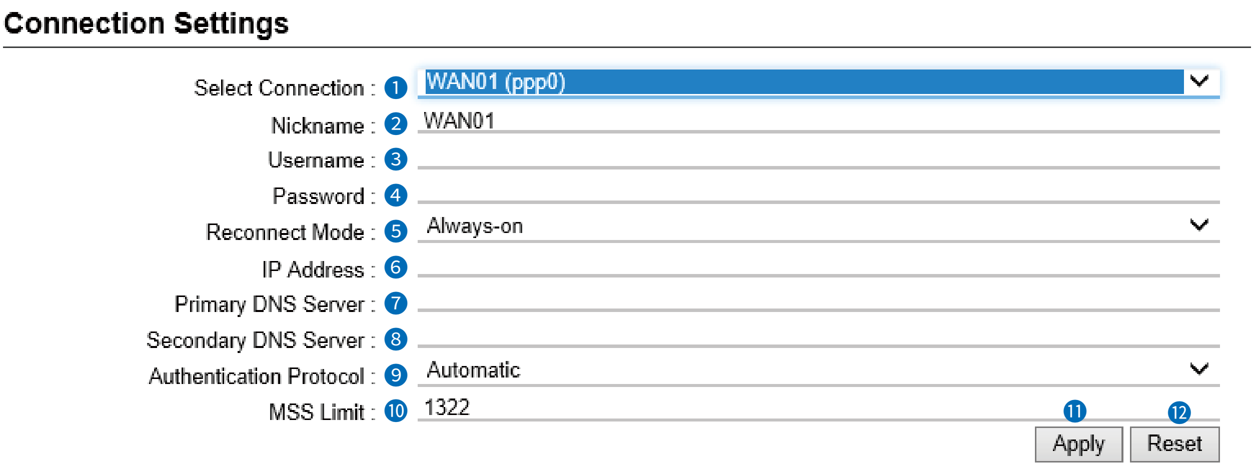
You can manually connect or disconnect by clicking <Connect> or <Disconnect> on the [Connection Status] screen. (p. 3-48)

❻IP Address .... Enter the WAN IP address if specified by your ISP.

5. [WAN] Screen

Router Settings > WAN

■Connection Settings PPPoE



Connection Settings

Select Connection : ❶ WAN01 (ppp0)
Nickname : ❷ WAN01
Username : ❸
Password : ❹
Reconnect Mode : ❺ Always-on
IP Address : ❻
Primary DNS Server : ❼
Secondary DNS Server : ❽
Authentication Protocol : ❾ Automatic
MSS Limit : ❿ 1322

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

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

❾**Authentication Protocol** Enter the authentication protocol as specified by your ISP. (Default: Automatic)

• Select "Automatic" if not specified by your ISP.

• **PAP**

The user is identified by the password. The entered password is NOT encrypted.

• **CHAP**

The authentication information is encrypted. This is a more securer protocol than PAP.

❿**MSS Limit....................** Enter the MSS limit value, if specified by your ISP. (Default: 1322)

(Range: 536 ~ 1452 in bytes)

The MSS value is the maximum size of TCP segment that the AP-95M can receive through the WAN port. Generally, a higher value is to be set as long as the fragment is not occurred.

But since the MTU size of PPPoE line is less than that of normal Ethernet (1500 bytes), setting a high value may block the packet going out on the Internet.

⓫ **<Apply>** .... Click to apply entries.

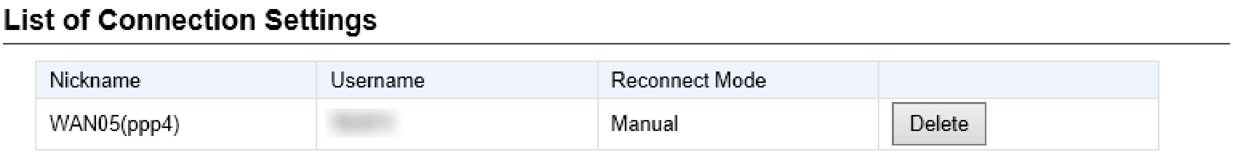
⓬ **<Reset>** .... Click to reset the settings.

• You cannot reset the entries after pushing <Apply>.

5. [WAN] Screen

Router Settings > WAN

■List of Connection Settings (PPPoE)



List of Connection Settings

Nickname	Username	Reconnect Mode	
WAN05(ppp4)	[redacted]	Manual	Delete

(This is an example.)

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

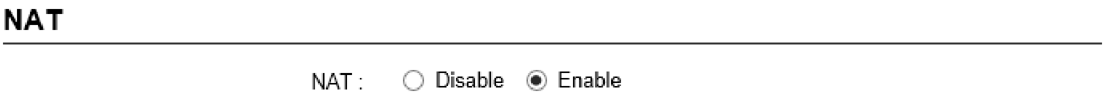
5. [NAT] Screen

Router Settings > NAT

■NAT

Configure the NAT function.

• This function can be used when the [Connection Type] (p. 3-49) is set to [DHCP Client], [Static IP] or [PPPoE].



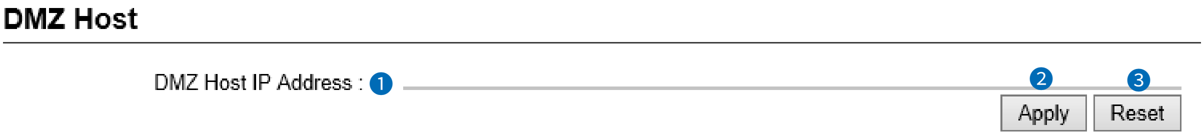
NAT .... Select "Enable" to use the NAT function. (Default: Enable)
• The NAT function converts the WAN global address into the private address.

Router Settings > NAT

■DMZ Host

Configure the DMZ Host function.

• The NAT function can be used when the [Connection Type] (p. 3-49) is set to [DHCP Client], [Static IP] or [PPPoE].



1 **DMZ Host IP Address** ... Enter the DMZ host IP address.
The DMZ function transfers the unknown IP frame, that is received through the WAN side (from Internet) port, to the IP address that is on the LAN side port. This function enables you to manage the server from a device connects to the AP-95M's LAN side port, or play online video games. Please note that the security level to the device on the LAN port side may be lower.
• The port forwarding setting takes priority when the DMZ function and the port forwarding function are used at the same time.

2 **<Apply>** .... Click to apply entries.

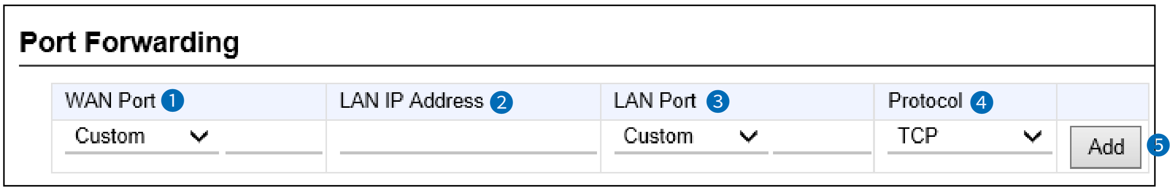
3 **<Reset>** .... Click to reset the settings.
• You cannot reset after clicking <Apply>.

5. [NAT] Screen

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

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

①**WAN Port** .... Select the mnemonic for the WAN port number.
Note: Select "Custom" to set the WAN port by number. You can select by the mnemonic (DNS, Finger, FTP, Gopher, NEWS, POP3,SMTP, Telnet, Web or Whois).

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

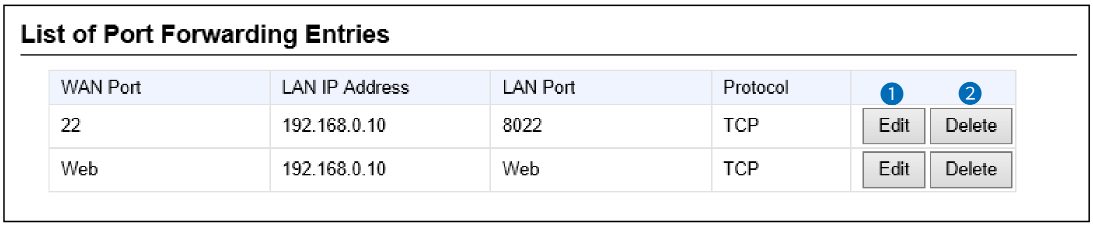
③**LAN Port** .... Select "Custom," if you select the LAN port by the number.
You can select by the mnemonic (DNS, Finger, FTP, Gopher, NEWS, POP3, SMTP, Telnet, Web or Whois).

④**Protocol** .... Select the protocol (TCP, UDP, TCP/UDP, GRE or ESP).

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

Router Settings > NAT

■List of Port Forwarding Entries



List of Port Forwarding Entries

WAN Port	LAN IP Address	LAN Port	Protocol	①	②
22	192.168.0.10	8022	TCP	Edit	Delete
Web	192.168.0.10	Web	TCP	Edit	Delete

(This is an example.)

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

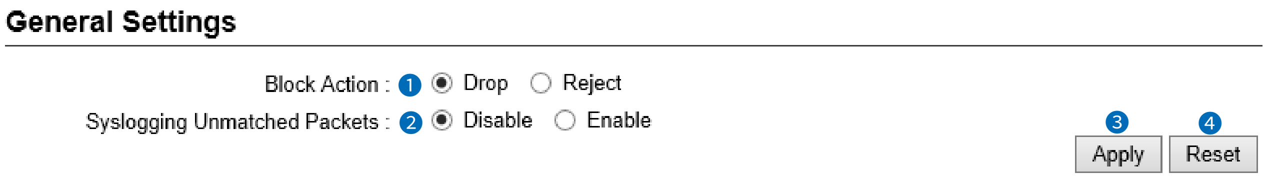
②**<Delete>** .... Click to remove the entry.

[IP Filter] Screen

Router Settings > IP Filter

■General Settings

Configure the IP Filtering function.



General Settings

Block Action : ① ● Drop ○ Reject

Syslogging Unmatched Packets : ② ● Disable ○ Enable

① Block Action .... Select the packet filtering method. (Default: Drop)

- **Drop:** Drops all packets and returns no packet.
- **Reject:** Reject all packets and returns the denied packets.

② Syslogging Unmatched Packets Select "Enable" to output the SYSLOG. (Default: Disable)

The packets that are not matched to any filtering criteria are blocked.

The blocked packets are reported in the SYSLOG.

Note: This function may affect the system performance when a huge amount of packets is processed. Using this only for the testing purpose is recommended.

③ <Apply> .... Click to apply entries.

④ <Reset> .... Click to reset the settings.

- You cannot reset after clicking <Apply>.

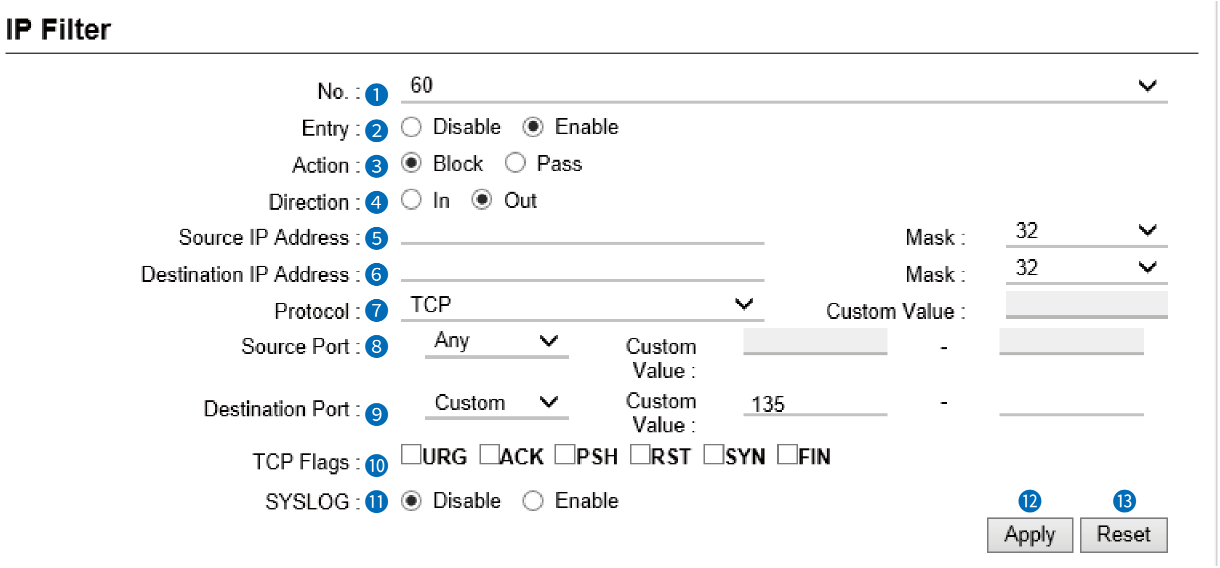
5. [IP Filter] Screen

Router Settings > IP Filter

IP Filter

Configure the IP Filtering function.

• This function can be used when the [Connection Type] (p.3-49) is set to [DHCP Client], [Static IP] or [PPPoE].



IP Filter

No. : ① 60

Entry : ② ○ Disable ● Enable

Action : ③ ● Block ○ Pass

Direction : ④ ○ In ● Out

Source IP Address : ⑤ Mask : 32

Destination IP Address : ⑥ Mask : 32

Protocol : ⑦ TCP Custom Value :

Source Port : ⑧ Any Custom Value : -

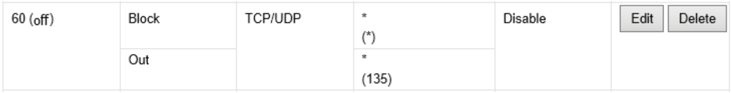
Destination Port : ⑨ Custom Custom Value : 135 -

TCP Flags : ⑩ □URG □ACK □PSH □RST □SYN □FIN

SYSLOG : ⑪ ● Disable ○ Enable

①**No.** .... Select the filtering order.
The filter function inspects the in coming or out going packet in the selected order, according to the filter setting in [List of Packet Filter Entries] (p.3-31).
(Range: 1 ~ 64)
• IPv6 packet is not supported.

②**Entry** .... Select "Enable" to apply the filter setting. (Default: Enable)
Select "Disable" for unused filter entry. " (off)" is displayed in the disabled entry in [List of Packet Filter Entries].



60 (off)	Block Out	TCP/UDP	* (*) * (135)	Disable	Edit Delete

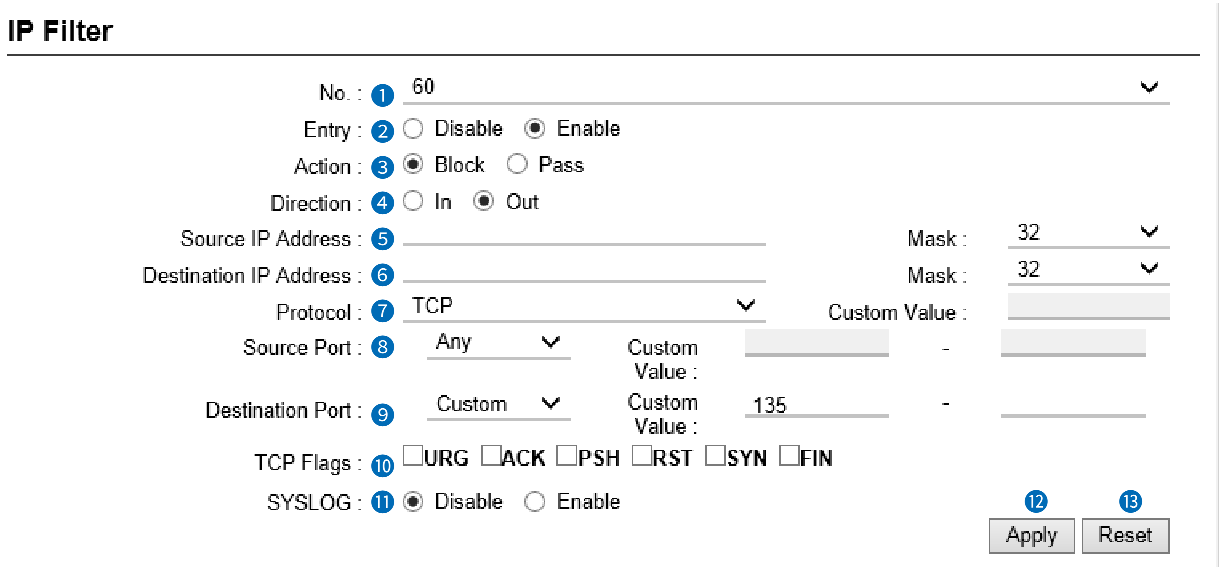
③**Action** .... Select the filtering method. (Default: Pass)

- **Block:** Blocks and discards all packets that is matched to the filtering criteria.
- **Pass:** Passes all packets that is matched to the filtering criteria.

5. [IP Filter] Screen

Router Settings > IP Filter

■IP Filter



IP Filter

No. : ① 60

Entry : ② ○ Disable ● Enable

Action : ③ ● Block ○ Pass

Direction : ④ ○ In ● Out

Source IP Address : ⑤ Mask : 32

Destination IP Address : ⑥ Mask : 32

Protocol : ⑦ TCP Custom Value :

Source Port : ⑧ Any Custom Value : -

Destination Port : ⑨ Custom Custom Value : 135 -

TCP Flags : ⑩ □URG □ACK □PSH □RST □SYN □FIN

SYSLOG : ⑪ ● Disable ○ Enable

⑫ Apply ⑬ Reset

④Direction .... Select the filtering direction. (Default: In)

- **In:** Filters all incoming packets.
- **Out:** Filters all out going packets.

⑤Source IP Address......... Enter the source IP Address and masking bits as the filtering criteria.
All packets come from the entered IP address are filtered (blocked or passed).
Leave this item blank to filter all packets regardless of the source IP address.
(Masking range: 1 ~ 32)

⑥Destination IP Address Enter the destination IP Address and masking bits as the filtering criteria.
All packets sent to the entered IP address are filtered (blocked or passed).
Leave this item blank to filter all packets regardless of the destination IP address.
(Masking range: 1 ~ 32)

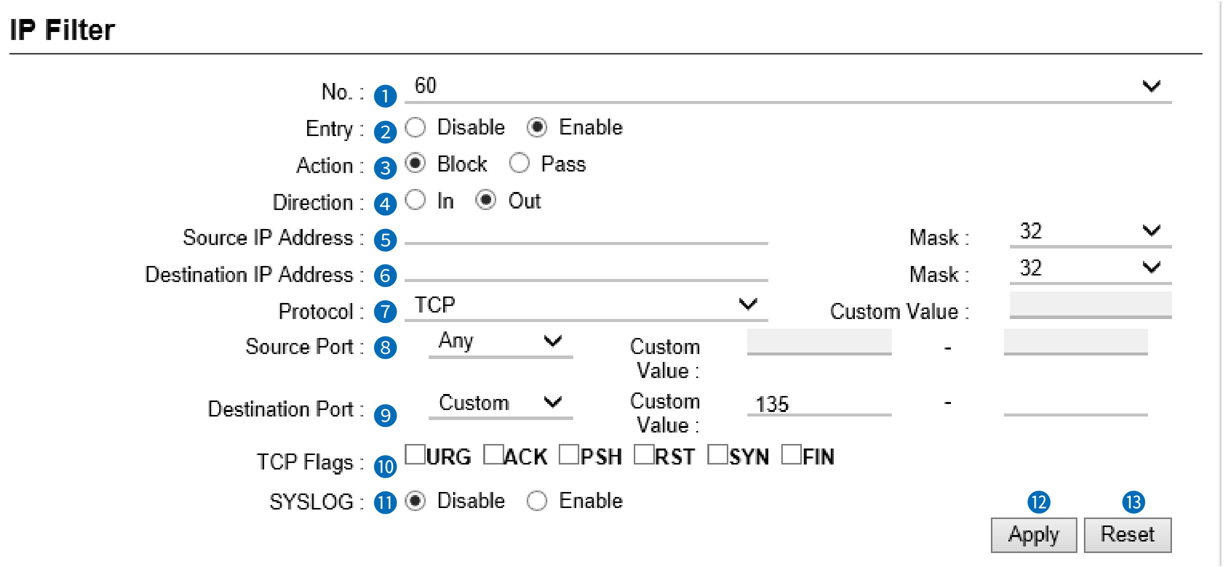
⑦Protocol .... Select the transport layer's protocol as the filtering criteria. (Default: Any)

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

5. [IP Filter] Screen

Router Settings > IP Filter

■IP Filter



IP Filter

No. : ① 60

Entry : ② ○ Disable ● Enable

Action : ③ ● Block ○ Pass

Direction : ④ ○ In ● Out

Source IP Address : ⑤ Mask : 32

Destination IP Address : ⑥ Mask : 32

Protocol : ⑦ TCP Custom Value :

Source Port : ⑧ Any Custom Value : -

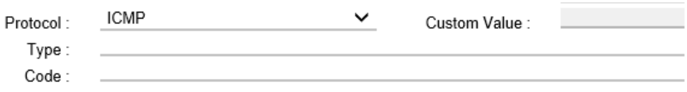
Destination Port : ⑨ Custom Custom Value : 135 -

TCP Flags : ⑩ □URG □ACK □PSH □RST □SYN □FIN

SYSLOG : ⑪ ● Disable ○ Enable

⑦Protocol (continued) ......

- **ICMP:** Only ICMP
  Enter the ICMP type and code into [Type] and [Code] items.
  (Range: 0 ~ 255)
  • Any type or code will be filtered when not entered.



Protocol : ICMP Custom Value :

Type :

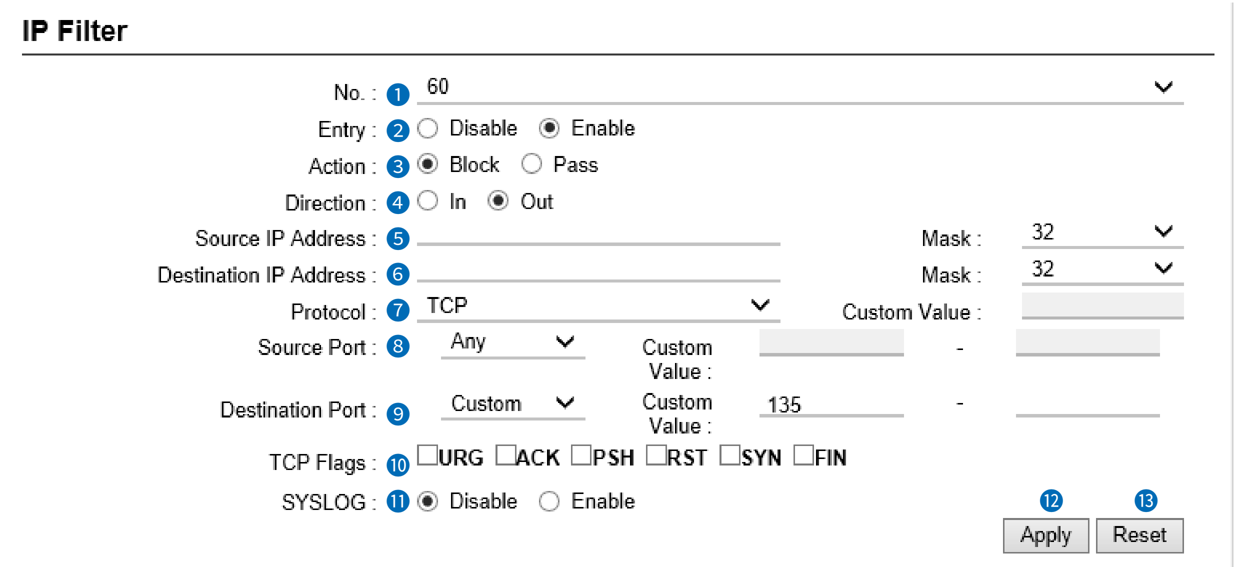
Code :

- **IGMP:** Only IGMP
- **Custom:** Specified by the protocol number.
  Enter the upper layer protocol number into the [Custom Value] item.
  (Range: 0 ~ 255)

5. [IP Filter] Screen

Router Settings > IP Filter

■IP Filter



IP Filter

No. : ① 60
Entry : ② ○ Disable ● Enable
Action : ③ ● Block ○ Pass
Direction : ④ ○ In ● Out
Source IP Address : ⑤ Mask : 32
Destination IP Address : ⑥ Mask : 32
Protocol : ⑦ TCP Custom Value :
Source Port : ⑧ Any Custom Value : -
Destination Port : ⑨ Custom Custom Value : 135 -
TCP Flags : ⑩ □URG □ACK □PSH □RST □SYN □FIN
SYSLOG : ⑪ ● Disable ○ Enable

⑧**Source Port** .... Select the source port, or enter the TCP/UDP source port number as the filtering criteria. (Default: Any)

- **Set by the port number**

1. Select "Custom."
2. Enter the port No. in the [Custom Value] item in the "(Start point) ~ (Stop point)" format.
   When you want set only one port, enter the same number to the [Custom Value] item.
   (Range: 1 ~ 65535)

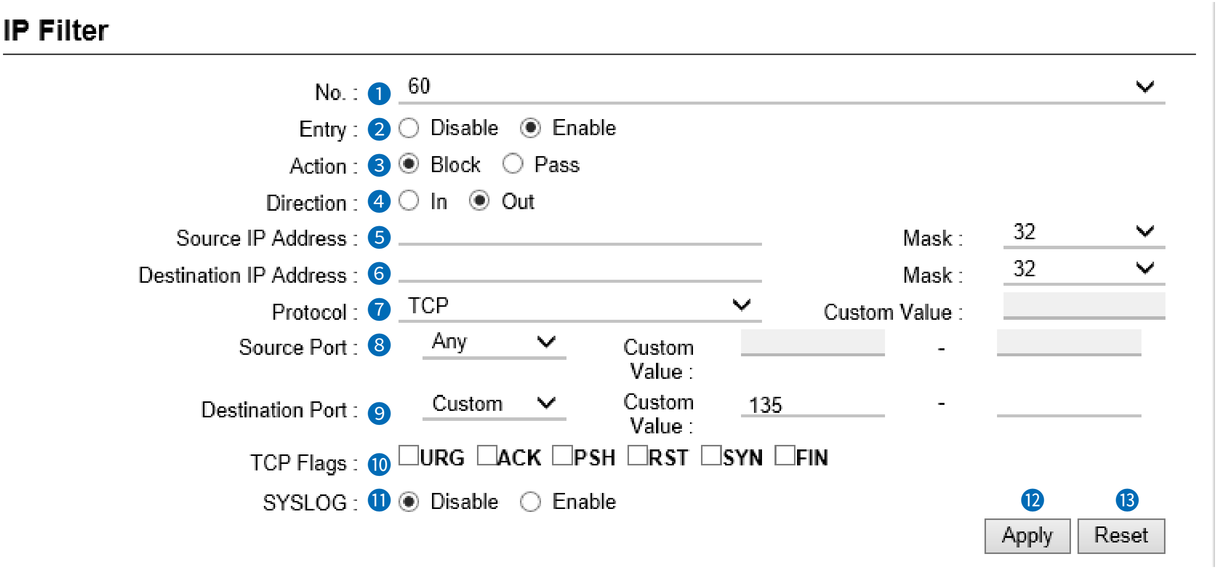
- **Set by mnemonic**

1. Select other than "Custom" and "Any."
2. Select a mnemonic directly (DNS, Finger, FTP, Gopher, NEWS, POP3, SMTP, Telnet, Web or Whois).
   - Select "Any" to filter the packet coming from any source port.

5. [IP Filter] Screen

Router Settings > IP Filter

■IP Filter



IP Filter

No. : ① 60

Entry : ② ○ Disable ● Enable

Action : ③ ● Block ○ Pass

Direction : ④ ○ In ● Out

Source IP Address : ⑤ Mask : 32

Destination IP Address : ⑥ Mask : 32

Protocol : ⑦ TCP Custom Value :

Source Port : ⑧ Any Custom Value : -

Destination Port : ⑨ Custom Custom Value : 135 -

TCP Flags : ⑩ □URG □ACK □PSH □RST □SYN □FIN

SYSLOG : ⑪ ● Disable ○ Enable

⑨Destination Port .... Select the source port, or enter the TCP/UDP destination port number.

(Default: Any)

• Set by the port number

1. Select "Custom."
2. Enter the port No. in the [Custom Value] item in the " (Start point) ~ (Stop point)" format.
   When you want set only one port, enter the same number to the [Custom Value] item.
   (Range: 1 ~ 65535)

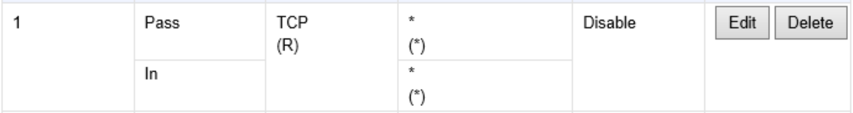
• Set by mnemonic

1. Select other than "Custom" and "Any."
2. Select a mnemonic directly (DNS, Finger, FTP, Gopher, NEWS, POP3, SMTP, Telnet, Web or Whois).
   • Select "Any" to filter the packet coming from any source port.

⑩TCP Flags..................... When "TCP" is selected in the [Protocol] (⑦) item, select the TCP control flags as the filtering criteria by entering a check mark. (Default: None)

The TCP control flags "URG," "ACK," "PSH," "RST," "SYN" and "FIN" can be set.

The set TCP flag (in abbreviated) is displayed in the [List of IP Filter Entries] item.



1	Pass	TCP (R)	* (*)	Disable	Edit Delete
	In		* (*)		

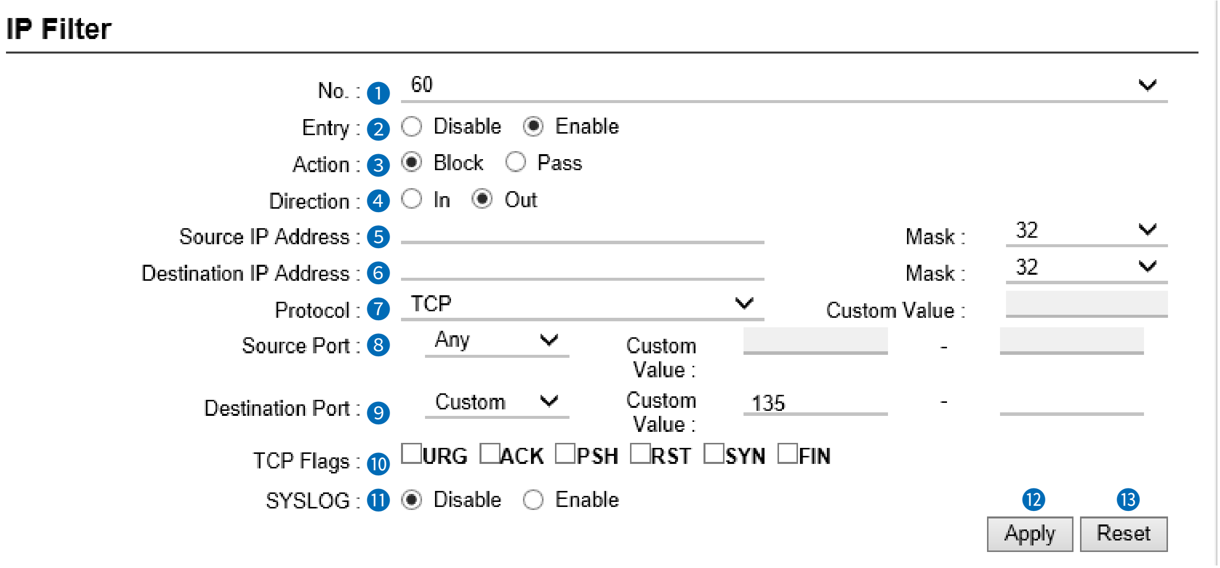
• When no TCP flag is selected, the TCP flag is not set as the filtering criteria.

5. [IP Filter] Screen

Router Settings > IP Filter

■IP Filter

• This screen is an example of when [Protocol] (⑦) is set to "TCP."



IP Filter

No. : ① 60

Entry : ② ○ Disable ● Enable

Action : ③ ● Block ○ Pass

Direction : ④ ○ In ● Out

Source IP Address : ⑤ Mask : 32

Destination IP Address : ⑥ Mask : 32

Protocol : ⑦ TCP Custom Value :

Source Port : ⑧ Any Custom Value : -

Destination Port : ⑨ Custom Custom Value : 135 -

TCP Flags : ⑩ □URG □ACK □PSH □RST □SYN □FIN

SYSLOG : ⑪ ● Disable ○ Enable

⑪**SYSLOG** .... Select "Enable" to output the SYSLOG. (Default: Disable)
Note: This function may affect the system performance. Using this only for the testing purpose is recommended.

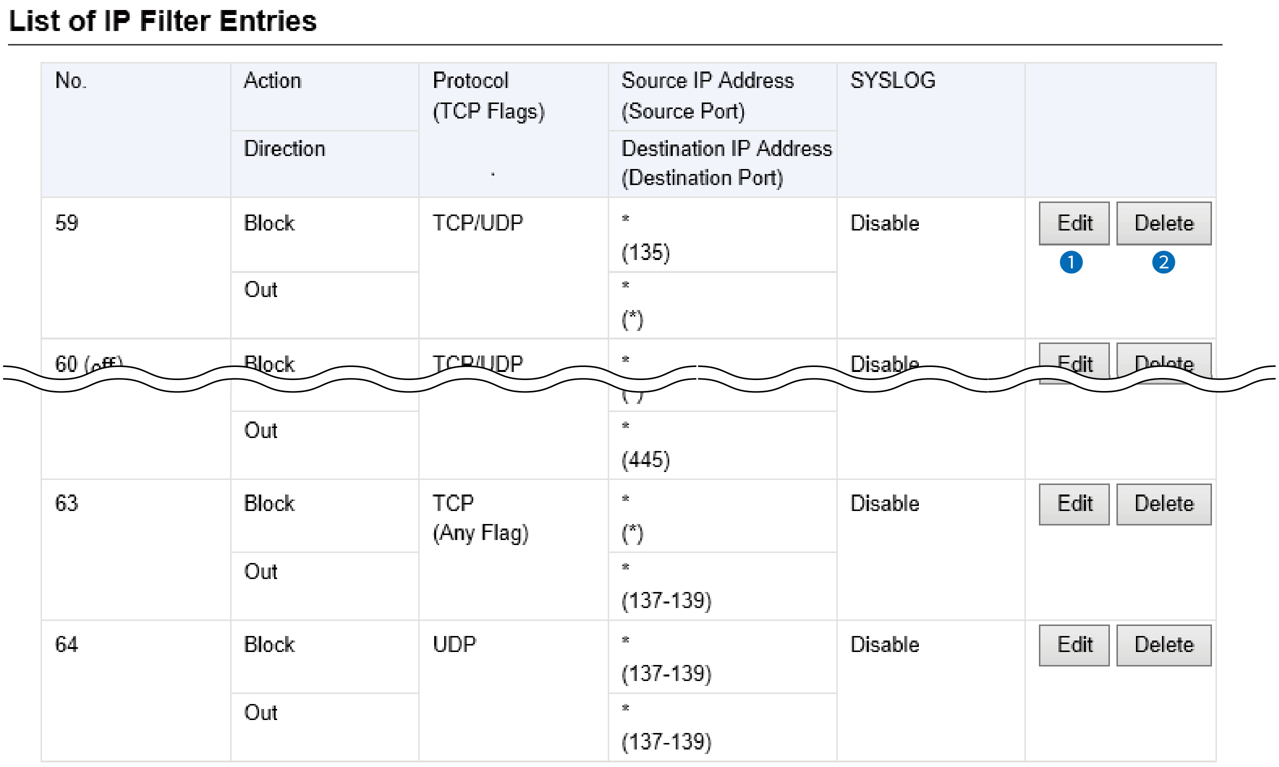
⑫ **<Apply>** .... Click to apply entries.

⑬ **<Reset>** .... Click to reset the settings.
• You cannot reset after clicking <Apply>.

5. [IP Filter] Screen

Router Settings > IP Filter

■ List of IP Filter Entries



List of IP Filter Entries

No.	Action Direction	Protocol (TCP Flags)	Source IP Address (Source Port) Destination IP Address (Destination Port)	SYSLOG	
59	Block	TCP/UDP	* (135)	Disable	Edit ❶ Delete ❷
	Out		* (*)		
60 (off)	Block	TCP/UDP	* ( )	Disable	Edit Delete
	Out		* (445)		
63	Block	TCP (Any Flag)	* (*)	Disable	Edit Delete
	Out		* (137-139)		
64	Block	UDP	* (137-139)	Disable	Edit Delete
	Out		* (137-139)		

(This is an example.)

[About the default filtering conditions]

- No. 59–64: These filtering criteria prevents the Windows applications from the remote access.
- "*" matches any value.

❶ **<Edit>** .... Click to edit the entry.
• The entry contents are loaded on the [IP Filter Setting] screen (p. 3-57).

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

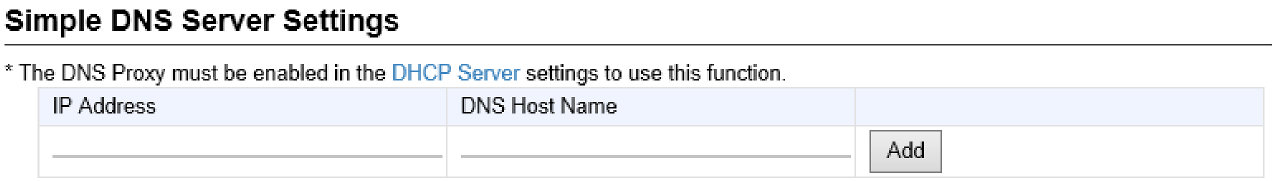
[Simple DNS] Screen

Router Settings > Simple DNS

■ Simple DNS Server Settings

Setting the Simple DNS Server function.

• You have to set the [DNS Proxy] item to "Enable" first. (p. 3-14)



Simple DNS Server Settings

* The DNS Proxy must be enabled in the DHCP Server settings to use this function.

IP Address	DNS Host Name	
		Add

Enter the host name and its IP address, then click <Add>.

DNS resolver searches the IP address by the domain name, or searches the domain name by the IP address.

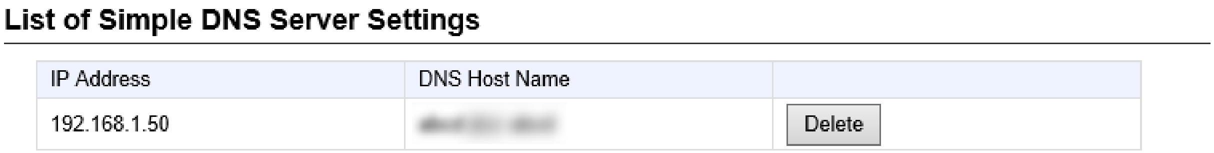
• Up 32 entries can be registered.

• If you register the local IP address and its host name, fixing the combination of MAC address and IP address using the static DHCP server is recommended.

Router Settings > Simple DNS

■ List of Simple DNS Server Settings

Displays the Simple DNS Server setting entries.



List of Simple DNS Server Settings

IP Address	DNS Host Name	
192.168.1.50	[redacted]	Delete

(This is an example.)

Click <Delete> to remove the entry.

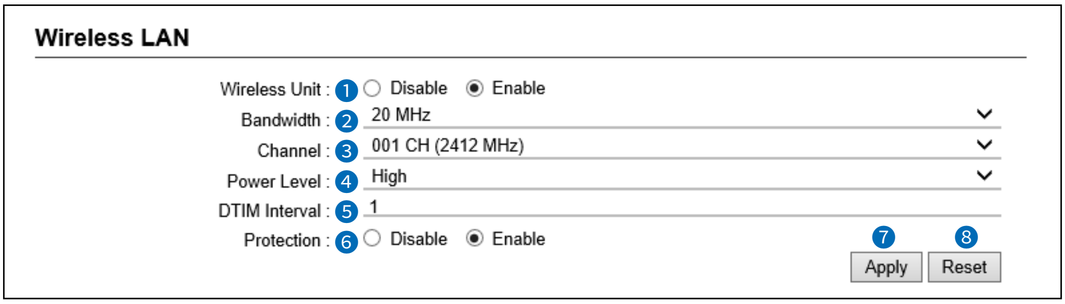
[Wireless LAN] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless LAN

■ Wireless LAN

Setting the internal wireless units.

- **Wireless 1:** 2.4 GHz band
- **Wireless 2:** 5 GHz band
- The screen is an example for Wireless 1.



Wireless LAN

Wireless Unit : ❶ ○ Disable ● Enable

Bandwidth : ❷ 20 MHz

Channel : ❸ 001 CH (2412 MHz)

Power Level : ❹ High

DTIM Interval : ❺ 1

Protection : ❻ ○ Disable ● Enable

❶ **Wireless Unit** .... Turn the Wireless LAN function ON or OFF. (Default: Enable)
Select "Enable" to use the Wireless LAN function.

❷ **Bandwidth** .... Select the bandwidth Communicating in. (Default: 20MHz)
Wireless 1: Select from 20 MHz and 40 MHz.
Wireless 2: Select from 20 MHz, 40 MHz and 80 MHz.

- When communicating in the 40 MHz or 80 MHz bandwidth, you are supposed to pay attention not to interfair other communincations.
- If the selected bandwidth is not supported by the client, the bandwidth that is supported by the client supports is used.

❸ **Channel** .... Select the channel Communicating on.
(Default: Wireless 1→001CH (2412MHz)
Wireless 2→036CH (5180MHz))

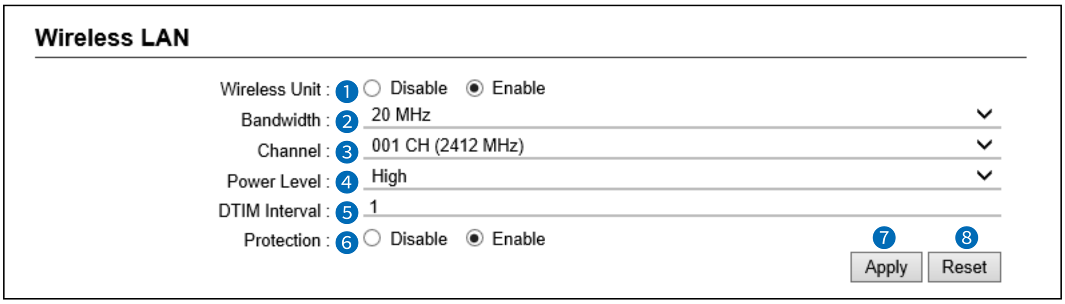
- Selectable channel differs, depending on the Bandwidth that is selected in the [Bandwidth] (❷). (p. iii)
- See page 5-2 for the interference on the 2.4 GHz band.

Wireless Bridging

Wireless Settings > Wireless 1/Wireless 2 > Wireless LAN

■ Wireless LAN

• The screen is an example for Wireless 1.



Wireless LAN

Wireless Unit : ❶ ○ Disable ● Enable

Bandwidth : ❷ 20 MHz

Channel : ❸ 001 CH (2412 MHz)

Power Level : ❹ High

DTIM Interval : ❺ 1

Protection : ❻ ○ Disable ● Enable

❹ **Power Level** .... Select the RF power level from High, Mid, Low and Lowest. (Default: High)
Select "High" for a long distance communication.
A lower power level makes the communication range sorter.

Set the power to a lower level when:

• you want to intentionally limit the communication range.
• you want to secure the communication by limiting the communication range.
• you want to reduce the interference to other communication devices.

❺ **DTIM Interval** .... Set the frequency that the DTIM (Delivery Traffic Indication Message) appears in the beacon frame. (Default: 1)
(Range: 1 ~ 50)
DTIM is the message that sends the Broadcast Multicast Packet transportation to the network device that is in the Power Save mode.
• Do not change this setting as long as it is unnecessary.

❻ **Protection** .... Select "Enable" when you want to reduce the decrease in communication speed caused by intermix of wireless LAN standard. (Default: Enable)

❼ **<Apply>** .... Click to apply entries.

❽ **<Reset>** .... Click to reset the settings.
• You cannot reset after clicking <Apply>.

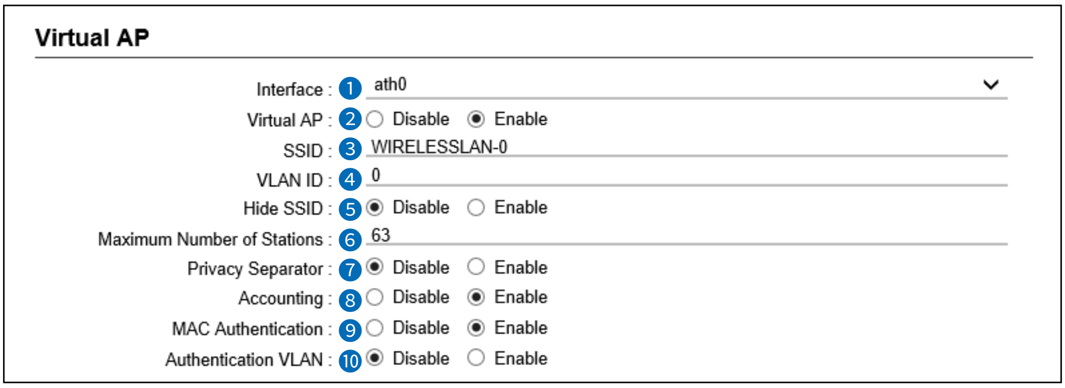
[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Virtual AP

Settings for the Virtual AP that provides different network access on one AP-95M.

- **Wireless 1:** 2.4 GHz band
- **Wireless 2:** 5 GHz band
- The screen is an example for Wireless 1.
- The screen is an example when the [Accounting] (❽) item and [MAC Authentication] (❾) item are set to "Enable."



Virtual AP

Interface : ❶ ath0

Virtual AP : ❷ ○ Disable ● Enable

SSID : ❸ WIRELESSLAN-0

VLAN ID : ❹ 0

Hide SSID : ❺ ● Disable ○ Enable

Maximum Number of Stations : ❻ 63

Privacy Separator : ❼ ● Disable ○ Enable

Accounting : ❽ ○ Disable ● Enable

MAC Authentication : ❾ ○ Disable ● Enable

Authentication VLAN : ❿ ● Disable ○ Enable

❶ **Interface** .... Select a Virtual AP to change setting. (Default: Wireless 1→ath0
Wireless 2→ath1)

- You can change the [Virtual AP] settings (❷ ~ ❼) and security settings for each Virtual AP.
- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.
- When you use "ath01" ~ "ath07" or "ath11" ~ "ath17," set "Enable"in the [Virtual AP] (❷) item.
- If JavaScript is disabled in your web browser, parameters may not be correctly displayed.

❷ **Virtual AP**.............................. Set the Virtual AP that is selected in the [Interface] (❶) item.
(Default: Wireless 1→ Enable (ath0), Disable (ath01 ~ ath07)
Wireless 2→Enable (ath1), Disable (ath11 ~ ath17)

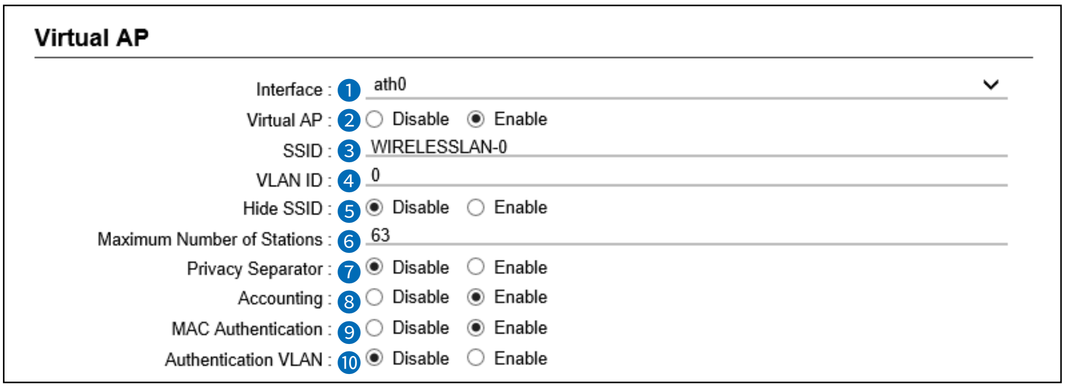
- "ath0" and "ath1" cannot be set to "Disable."
- To prevent the reduction in communication speed due to concentration of connections, disable the interface that is not used.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Virtual AP

- The screen is an example for Wireless 1.
- The screen is an example when the [Accounting] (❽) item and [MAC Authentication] (❾) item are set to "Enable."



Virtual AP

Interface : ❶ ath0

Virtual AP : ❷ ○ Disable ● Enable

SSID : ❸ WIRELESSLAN-0

VLAN ID : ❹ 0

Hide SSID : ❺ ● Disable ○ Enable

Maximum Number of Stations : ❻ 63

Privacy Separator : ❼ ● Disable ○ Enable

Accounting : ❽ ○ Disable ● Enable

MAC Authentication : ❾ ○ Disable ● Enable

Authentication VLAN : ❿ ● Disable ○ Enable

❸ **SSID** ....

Set the SSID of Virtual AP that is selected in the [Interface] (❶) item.
Enter the SSID of up to 32 characters. (Not case sensitive)

(Default: WIRELESSLAN-0 (ath0, ath1)
WIRELESSLAN-1 (ath01, ath11)
WIRELESSLAN-2 (ath02, ath12)
WIRELESSLAN-3 (ath03, ath13)
WIRELESSLAN-4 (ath04, ath14)
WIRELESSLAN-5 (ath05, ath15)
WIRELESSLAN-6 (ath06, ath16)
WIRELESSLAN-7 (ath07, ath17))

- The SSID groups the wireless network. Only wireless LAN stations with matching SSID can communicate each other.
- Each network group is identified by the SSID (Wireless network name) in a same wireless communication range.
- Set different SSID to each AP.
- In this manual, [SSID] and [ESSID] are assumed to be the same in meaning.

❹ **VLAN ID** ....

Enter the ID number of the wireless group that the Virtual AP, that is selected in the [Interface] (❶) item, belongs to. (Default: 0)
(Range: 0 ~ 4094)

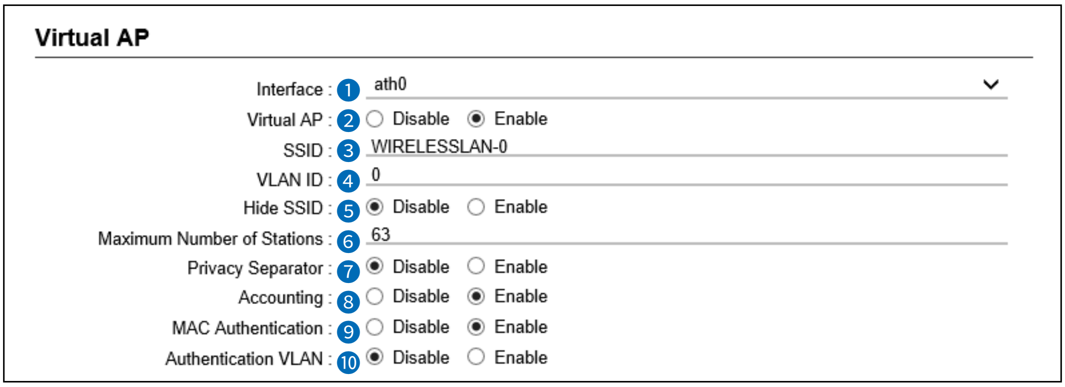
- If this item is left blank, "0" is automatically set.
- Only Virtual APs with matching ID can communicated each other.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Virtual AP

- The screen is an example for Wireless 1.
- The screen is an example when the [Accounting] (❽) item and [MAC Authentication] (❾) item are set to "Enable."



Virtual AP

Interface : ① ath0

Virtual AP : ② ○ Disable ● Enable

SSID : ③ WIRELESSLAN-0

VLAN ID : ④ 0

Hide SSID : ⑤ ● Disable ○ Enable

Maximum Number of Stations : ⑥ 63

Privacy Separator : ⑦ ● Disable ○ Enable

Accounting : ⑧ ○ Disable ● Enable

MAC Authentication : ⑨ ○ Disable ● Enable

Authentication VLAN : ⑩ ● Disable ○ Enable

❺ Hide SSID............................. Select "Enable" to hide the SSID and eject the access from the wireless station that is in the ANY mode. (Default: Disable)

- Do not change this setting as long as it is unnecessary.

❻ Maximum Number of Stations Set the maximum number of wireless LAN stations (clients) that connect to the Virtual AP at the same time. (Default: 63)

(Range: 1 ~ 128)

- By setting this value to a lower number, the reduction in communication speed due to concentration of connections can be prevented.
- Up to 128 clients can connect to a Virtual AP at the same time. However, the maximum number of clients is up to 128.

❼ Privacy Separator..................... Select "Enable" to inhibit the communication between wireless LAN stations that connect to the same Virtual AP. (Default: Disable)

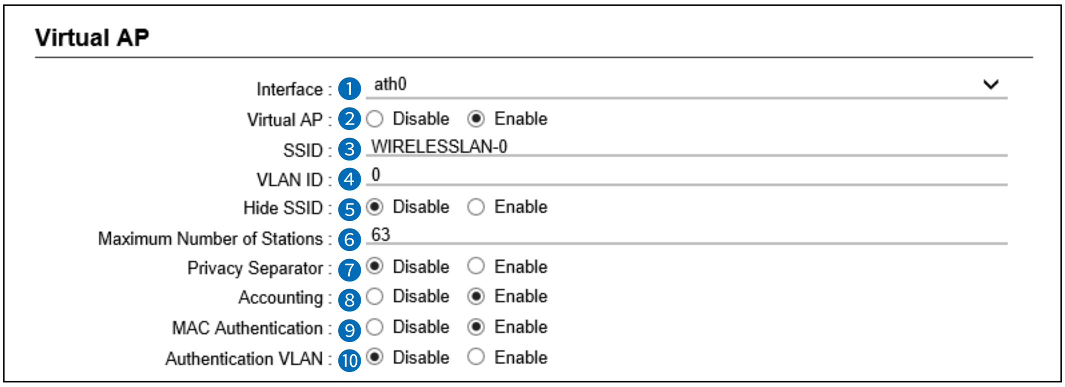
- To inhibit the communication between wireless LAN stations that connect to a different Virtual AP, use the Packet Filter function. (p. 3-19)

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Virtual AP

- The screen is an example for Wireless 1.
- The screen is an example when the [Accounting] (❽) item and [MAC Authentication] (❾) item are set to "Enable."



Virtual AP

Interface : ❶ ath0

Virtual AP : ❷ ○ Disable ● Enable

SSID : ❸ WIRELESSLAN-0

VLAN ID : ❹ 0

Hide SSID : ❺ ● Disable ○ Enable

Maximum Number of Stations : ❻ 63

Privacy Separator : ❼ ● Disable ○ Enable

Accounting : ❽ ○ Disable ● Enable

MAC Authentication : ❾ ○ Disable ● Enable

Authentication VLAN : ❿ ● Disable ○ Enable

❽ Accounting .... Select "Enable" to use the Accounting function.
The Accounting function collects the wireless LAN station's status (Connection, MAC address and so on), and send it to the accounting server.

(Default: Disable)

- If "Enable" is selected, you have to set the "Accounting" (p.3-82).

❾ MAC Authentication .... Select "Enable" to use the RADIUS server authentication.
The client access to the Virtual AP, that is selected in the [Interface] (❶) item, is authenticated by the RADIUS server, using the client's MAC address.

(Default: Disable)

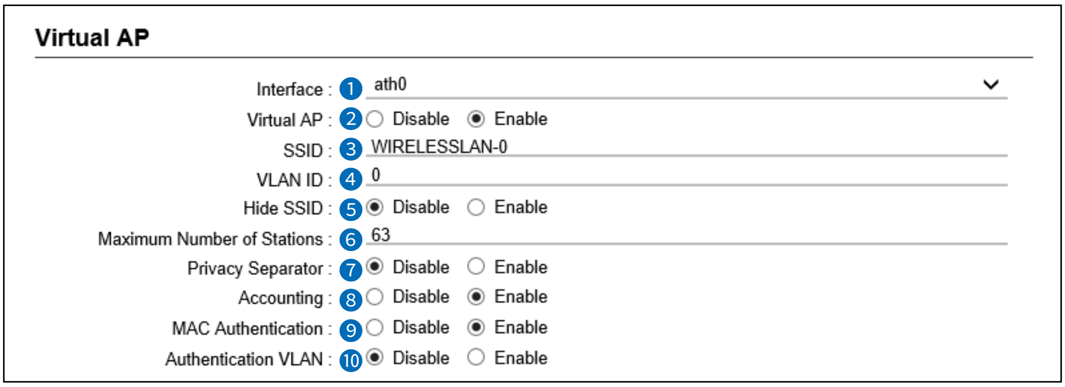
- If "Enable" is selected, you have to set the RADIUS server.
- You can use combination of any network authentication method and encryption for the MAC Authentication function.
- Wireless LAN MAC address must be registered to the RADIUS server in advance.
  (For example, if the MAC address is "00-AB-12-CD-34-EF," the user name and password will be "00ab12cd34ef."

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

Virtual AP

- The screen is an example for Wireless 1.
- The screen is an example when the [Accounting] (❽) item and [MAC Authentication] (❾) item are set to "Enable."



Virtual AP

Interface : ❶ ath0

Virtual AP : ❷ ○ Disable ● Enable

SSID : ❸ WIRELESSLAN-0

VLAN ID : ❹ 0

Hide SSID : ❺ ● Disable ○ Enable

Maximum Number of Stations : ❻ 63

Privacy Separator : ❼ ● Disable ○ Enable

Accounting : ❽ ○ Disable ● Enable

MAC Authentication : ❾ ○ Disable ● Enable

Authentication VLAN : ❿ ● Disable ○ Enable

❿ Authentication VLAN .... Select "Enable" to group the client's VLAN ID according to the result of RADIUS server authentication. The VLAN ID of the client that connects to the Virtual LAN (selected in the [Interface] (❶) item) is grouped. (Default: Disable)

- Configure the RADIUS server when selecting "Enable."
- Refer to page 2-23 for details.
- To configure the Authentication VLAN, select "Enable" in the [MAC Authentication] (❾) item, or select WEB Authentication (IEEE802.1X, WPA2, WPA/WPA2, WPA) on the [WEB Authentication] screen (p.3-36).

- **When the MAC authentication is enabled:**

  Configure the RADIUS server on the [MAC Authentication] screen. (p.3-73)

- **When "IEEE802.1X," "WPA2," "WPA/WPA2" or "WPA" is selected as the network authentication method:**

  Configure the RADIUS server on the [RADIUS Settings] screen. (p. 3-43)

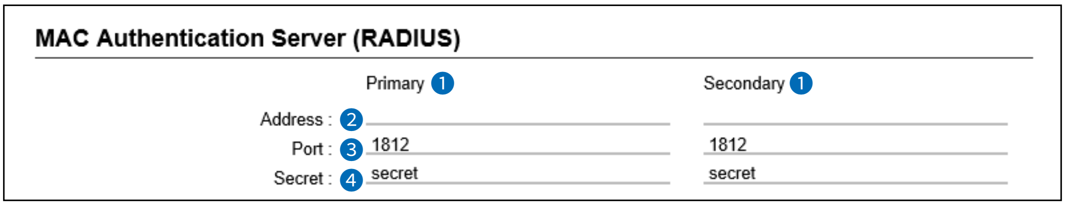
  - When the both network authentication and MAC authentication is enabled, the VLAN ID that is obtained by the network authentication will take priority.
  - If the response property is not obtained or invalid, the VLAN ID that is set in the Virtual LAN will be obtained.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ MAC Authentication Server (RADIUS)

Set the MAC Authentication Server to authorize wireless station’s Mac address on the RADIUS server.



MAC Authentication Server (RADIUS)

	Primary ❶	Secondary ❶
Address : ❷		
Port : ❸	1812	1812
Secret : ❹	secret	secret

❶ **Primary/Secondary** .... When no response is received from the RADIUS server that is set in [Primary], the RADIUS server that is set in [Secondary] will be used instead.

❷ **Address** .... Enter the RADIUS server address.

❸ **Port** .... Enter the RADIUS server's authentication port number. (Default: 1812)
(Range: 1 ~ 65535)
• The default port number may differ, depending on the presetting.

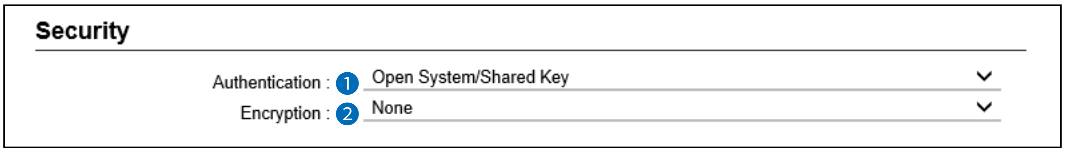
❹ **Secret** .... Enter the RADIUS server key of up to 64 characters. (Default: secret)

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Security

Configure the security settings.



Security

Authentication : ❶ Open System/Shared Key

Encryption : ❷ None

❶ **Authentication** .... Select the network authentication method, according to your network environment. (Default: Open System/Shared Key)

- When one of "IEEE802.1X," "WPA," "WPA2" or "WPA/WPA2" is selected, RADIUS server setting is necessary.

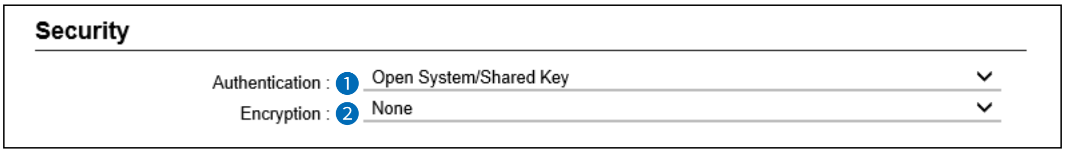
About the Authentication method:

- **Open System/Shared key**
  The authentication method (Open System/Shared Key) is automatically applied to the access that is in "WEP RC4."
- **Open System**
  No authentication method is automatically applied to the access that is in "WEP RC4."
- **Shared Key**
  Shared key is used for the authentication.
- **IEEE802.1X**
  Authentication by "WEP RC4." The authentication method for the RADIUS with IEEE802.1X
  - You have to configure the RADIUS server authentication setting.
- **WPA (Wi-Fi Protected Access)**
  Authentication by "TKIP/AES." The authentication method for the RADIUS server.
  - A more securer method than IEEE802.1X.
  - You have to configure the RADIUS server authentication setting.
- **WPA2**
  Authentication by "WPA2."
  - A more securer method than IEEE802.1X.
  - You have to configure the RADIUS server authentication setting.
  - You need a client that supports WPA2.
- **WPA/WPA2**
  The WPA authentication or WPA2 authentication is automatically distinguished.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Security



Security

Authentication : ① Open System/Shared Key

Encryption : ② None

① Authentication ....

- **WPA-PSK (Pre-Shared Key)**
  Shared key is used for the authentication.
  A simple authentication method without a RADIUS server.
- **WPA2-PSK**
  Shared key is used for the authentication.
  A simple authentication method without a RADIUS server.
- **WPA-PSK/WPA2-PSK**
  An automatic authentication method (WPA-PSK/WPA2-PSK).

② **Encryption** ....

Select the encryption type. (Default: None)
You can select from WEP RC4, TKIP or AES.

- The encryption type and number of bits must be matched with the network device that communicates with.
- Communication in IEEE802.11ac or IEEE802.11n is enabled only when "None" or "AES" is selected.

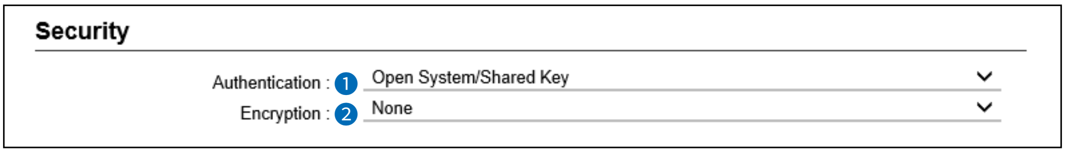
About the encryption type:

- **None**
  Communication is not encrypted.
  - You can select this option when "Open System/Shared Key" or "Open System" is selected in the [Authentication] (①) item.
  - Selecting other encryption option is recommended.
- **WEP RC4**
  Communication is encrypted using the encryption key.
  - Select the bit length from 64 (40)/128 (104)/152 (128) bits.
  - You can select this option when "Open System/Shared Key," "Open System" or "IEEE802.1X" is selected in the [Authentication] (①) item.
- **AES (Advanced Encryption Standard)**
  The encryption key is periodically updated. A more securer encryption method than "TKIP."
  - You can select this option when "WPA," "WPA2," "WPA-PSK" or "WPA2-PSK" is selected in the [Authentication] (①) item.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Security



Security

Authentication : ❶ Open System/Shared Key

Encryption : ❷ None

❷ Encryption ....

- **TKIP/AES**

  "TKIP/AES" is automatically applied to the access from a wireless LAN station.

  Only when "AES" is detected, the communication rate exceeds 54 Mbps.

  - You can select this option when "WPA," "WPA2," "WPA-PSK" or "WPA2-PSK" is selected in the [Authentication] (❶) item.

- **TKIP (Temporal Key Integrity Protocol)**

  The encryption key is periodically updated. A more securer encryption method than "WEP RC4."

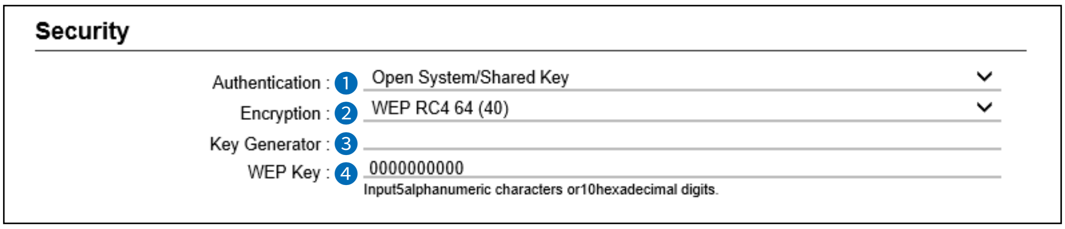
  - You can select this option when "WPA," "WPA2," "WPA-PSK" or "WPA2-PSK" is selected in the [Authentication] (❶) item.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Security

- Items ❸ and ❹ are displayed according to the value or option set in items ❶ and ❷. (pp. 3-74 ~ 3-76)



Security

Authentication : ❶ Open System/Shared Key

Encryption : ❷ WEP RC4 64 (40)

Key Generator : ❸

WEP Key : ❹ 0000000000

Input5alphanumeric characters or10hexadecimal digits.

❸ Key Generator ....

Displayed when "WEP RC4" is selected in the [Encryption] (❷) item (pp. 3-75, 3-76).

Enter the string to generate the key in hexadecimal. (Default: (blank))

Setting procedure:

1. Select "Open System/Shared Key," "Open System" or "Shared Key" in the Authentication item.
2. Select "WEP RC4 64 (40)," "WEP RC4 128 (104)" or "WEP RC4 152 (128)."
   - [Key Generator] (❸) and [WEP Key] (❹) appear.
3. Enter the key string of up to 31 characters into the [Key Generator] item. (case distinction)
   - The key is generated according to the entered string, and will be displayed in the [WEP] item in hexadecimal.
   - Before entering a key into the [WEP Key] (❹), delete the string in the [Key Generator] (❸) item.

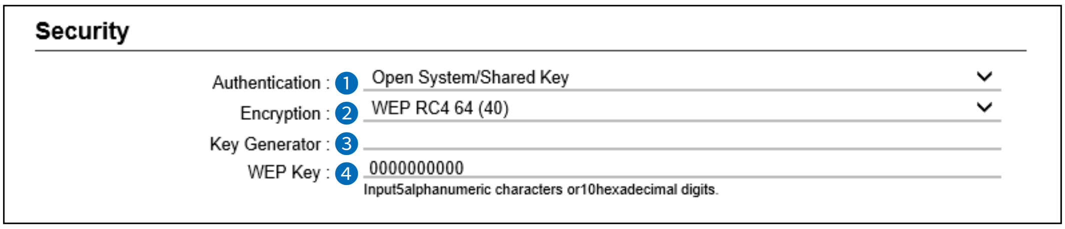
- Enter the same string to the client's (Icom's wireless LAN station) key generator input.
  The entered key is not compatible with a third-party device.
- If the generated key is not matched with that of client, communication between those devices is unable.
- The number of digits and characters may differ, depending on the option that is selected in the [Encryption] (❷) item.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Security

- Items ❸ and ❹ are displayed according to the value or option set in items ❶ and ❷. (pp. 3-74 ~ 3-76)



Security

Authentication : ❶ Open System/Shared Key

Encryption : ❷ WEP RC4 64 (40)

Key Generator : ❸

WEP Key : ❹ 0000000000

Input5alphanumeric characters or10hexadecimal digits.

❹ WEP Key .... If you do not use the Key generator, enter the key directly in hexadecimal or in ASCII code. (Case distinction)

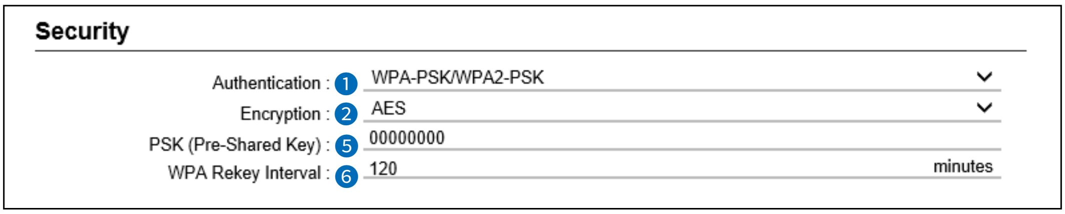
- When selecting an Encryption type in the [Encryption] item (❷), an enumeration of "0" appears in the [WEP] item (❹). This indicates the total digits of the key. Enter the key in the same number of digits. (For Example: "0000000000" is displayed, the number of key digits must be 10.)
  When you enter the key in ASCII code, the number of characters must be 1/2. (For Example: "0000000000" is displayed, the number of key characters in ASCII code must be 5.)

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Security

• Items ❺ and ❻ are displayed according to the value or option set in items ❶ and ❷. (pp. 3-74 ~ 3-76)



Security

Authentication : ❶ WPA-PSK/WPA2-PSK

Encryption : ❷ AES

PSK (Pre-Shared Key) : ❺ 00000000

WPA Rekey Interval : ❻ 120 minutes

❺ PSK (Pre-Shared Key) ………… Enter the key in the alphanumeric when "WPA-PSK," "WPA2-PSK" or "WPA-PSK/WPA2-PSK" in the [Authentication] (❶) item.

- The shared key must be matched with the network device that communicates with.
- Enter the key directly in hexadecimal (64 digits) or in ASCII code. (Case distinction)

❻ WPA Rekey Interval …………… Enter the key update interval (in minutes) when "WPA," "WPA2," "WPA/WPA2," "WPAPSK," "WPA2-PSK" or "WPA-PSK/WPA2-PSK" in the [Authentication] (❶) item. (Default: 120)

(Range: 0 ~ 1440)

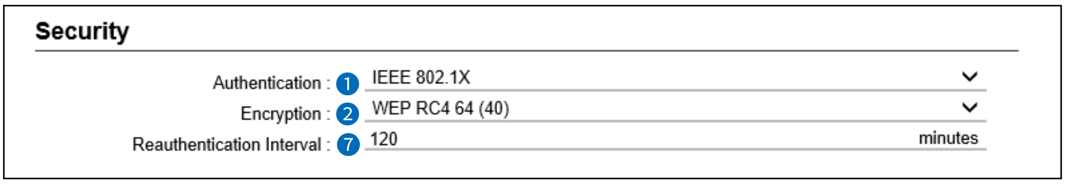
- The key is not updated when "0" is entered.

[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Security

- Items ⑦ is displayed according to the value or option set in items ① and ②. (pp. 3-74 ~ 3-76)



Security

Authentication : ① IEEE 802.1X

Encryption : ② WEP RC4 64 (40)

Reauthentication Interval : ⑦ 120 minutes

⑦ Reauthentication Interval ...... Enter the reauthentication interval when "IEEE802.1X" is selected in the [Authentication] (①) item. (Default: 120)
(Range: 0 ~ 9999)

- The reauthentication is not required when "0" is entered.

[Virtual AP] Screen

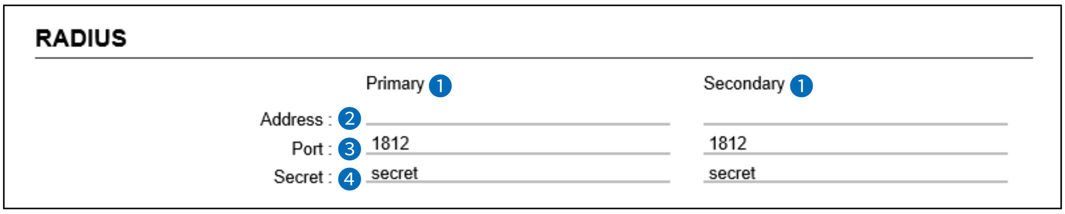
Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Setting for RADIUS

Set the RADIUS for authorizing the WPA, WPA2, or IEEE802.1X.

This screen appears when "IEEE802.1X," "WPA," "WPA2" or "WPA/WPA2" in the [Authentication] item.

• Refer to the manual that is supplied with the RADIUS server or wireless LAN station for the EAP authentication.



RADIUS

	Primary ①	Secondary ①
Address : ②		
Port : ③	1812	1812
Secret : ④	secret	secret

① **Primary/Secondary** .... When no response is received from the RADIUS server that is set in [Primary], the RADIUS server that is set in [Secondary] will be used instead.

② **Address** .... Enter the RADIUS server address.

③ **Port** .... Enter the RADIUS server's authentication port number. (Default: 1812)
(Range: 1 ~ 65535)
• The default port number may differ, depending on the presetting.

④ **Secret** .... Enter the RADIUS server key of up to 64 characters. (Default: secret)

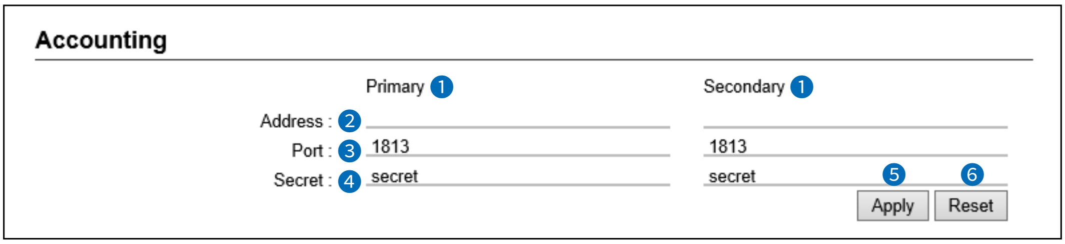
[Virtual AP] Screen

Wireless Settings > Wireless 1/Wireless 2 > Virtual AP

■ Accounting

Setting “Accounting” is required for compiling the network status information (connection, disconnection, MAC address and so on) of the wireless LAN station that you want to communicate with, and then sending it to the accounting server.

• To use this function, you must set an accounting server.



Accounting

	Primary ❶	Secondary ❶
Address : ❷		
Port : ❸	1813	1813
Secret : ❹	secret	secret

❶ **Primary/Secondary** .... When no response is received from the RADIUS server that is set in [Primary], the RADIUS server that is set in [Secondary] will be used instead.

❷ **Address** .... Enter the RADIUS server address.

❸ **Port** .... Enter the RADIUS server's authentication port number. (Default: 1813)
(Range: 1 ~ 65535)
• The default port number may differ, depending on the presetting.

❹ **Secret** .... Enter the RADIUS server key of up to 64 characters. (Default: secret)

❺ **<Apply>** .... Click to apply entries.

❻ **<Reset>** .... Click to reset the settings.
• You cannot reset after clicking <Apply>.

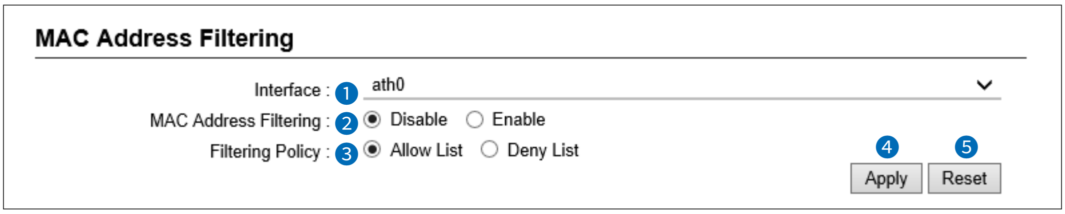
[MAC Address Filtering] Screen

Wireless Settings > Wireless 1/Wireless 2 > MAC Address Filtering

■ MAC Address Filtering

This security system is used to permit or to prohibit access to only the wireless LAN stations with the MAC address preset to the AP-95M’s Virtual AP.

- Up to 1024 MAC addresses of wireless LAN stations (clients) can be registered.
- If JavaScript is disabled in your web browser, parameters may not be correctly displayed.



MAC Address Filtering

Interface : ❶ ath0

MAC Address Filtering : ❷ ● Disable ○ Enable

Filtering Policy : ❸ ● Allow List ○ Deny List

❶ **Interface** .... Select a Virtual AP to change the setting. (Default: ath0 (Wireless 1) ath1 (Wireless 2))

- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.

❷ **MAC Address Filtering**............ Select "Enable" to allow or deny the access from wireless LAN stations. (Default: Disable)

- When "Enable" is selected, the [Filtering Policy] (❸) item and settings on the [List of MAC Address Filtering Entries] screen will be applied.
- You need to select an interface on the [Virtual AP] screen and set the [Virtual AP] item to "Enable."

❸ **Filtering Policy** .... Select the filtering option. (Default: Allow List)

Allow List: Only network devices on the [Station MAC Address] list can communicates with AP-95M.

Deny List: Network devices on the [Station MAC Address] list cannot communicates with AP-95M.

❹ **<Apply>** .... Click to apply entries.

❺ **<Reset>** .... Click to reset the settings.

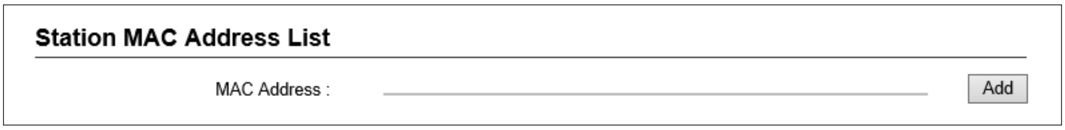
- You cannot reset after clicking <Apply>.

[MAC Address Filtering] Screen

Wireless Settings > Wireless 1/Wireless 2 > MAC Address Filtering

■ Station MAC Address List

Register the MAC address of wireless LAN stations to be filtered according to the filtering criteria.



MAC Address .... Enter the MAC address of the wireless LAN station in alphanumeric (in hexadecimal) as the filtering criteria, then click [Add].

- If you cannot select the MAC address from [List of MAC Address Filtering Entries], directly enter the address.
- Up to 1024 MAC addresses can be registered for each Virtual AP.
- The MAC address may or may not contain "-" (hyphen)
  (For example, "00-90-c7-00-00-10" and "0090c7000010" are recognized as the same address.)
- The communication with wireless LAN is filtered according to the MAC address filtering policy set in the [Filtering Policy] item.

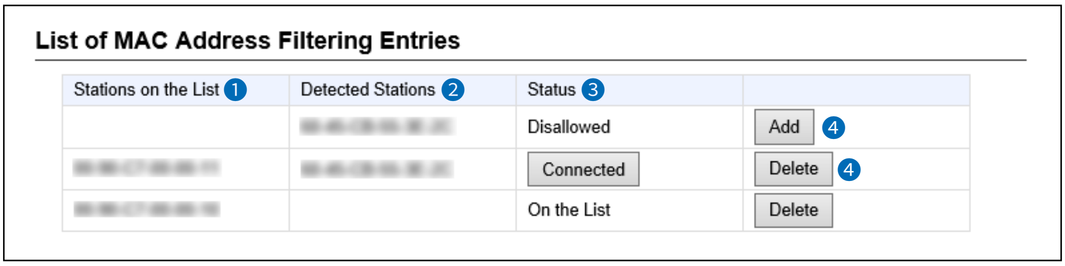
[MAC Address Filtering] Screen

Wireless Settings > Wireless 1/Wireless 2 > MAC Address Filtering

■ List of MAC Address Filtering Entries

You can set the AP-95M to allow or deny the access from wireless LAN stations, for each virtual AP.

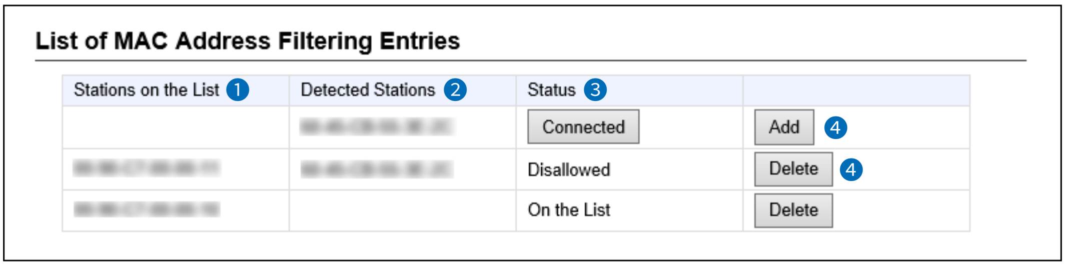
When "Allow List" is selected in the [Filtering Policy] item.



List of MAC Address Filtering Entries

Stations on the List ①	Detected Stations ②	Status ③	
	[redacted]	Disallowed	Add ④
[redacted]	[redacted]	Connected	Delete ④
[redacted]		On the List	Delete

When "Deny List" is selected in the [Filtering Policy] item.



List of MAC Address Filtering Entries

Stations on the List ①	Detected Stations ②	Status ③	
	[redacted]	Connected	Add ④
[redacted]	[redacted]	Disallowed	Delete ④
[redacted]		On the List	Delete

① **Stations on the List** .... Registered wireless LAN station's MAC address.

② **Detected Stations** .... The MAC address of wireless LAN stations in the wireless communication area.

③ **Status** .... Communication status.

<Connected>: Communication is allowed. (Connected to the AP-95M)
• Click to open the wireless communication status window.

Disallowed: Communication is not allowed.

On the List: Communication is allowed. (Not connected)

④ **<Add>/<Delete>** .... Click to add or delete the entry.

[Network Monitoring] Screen

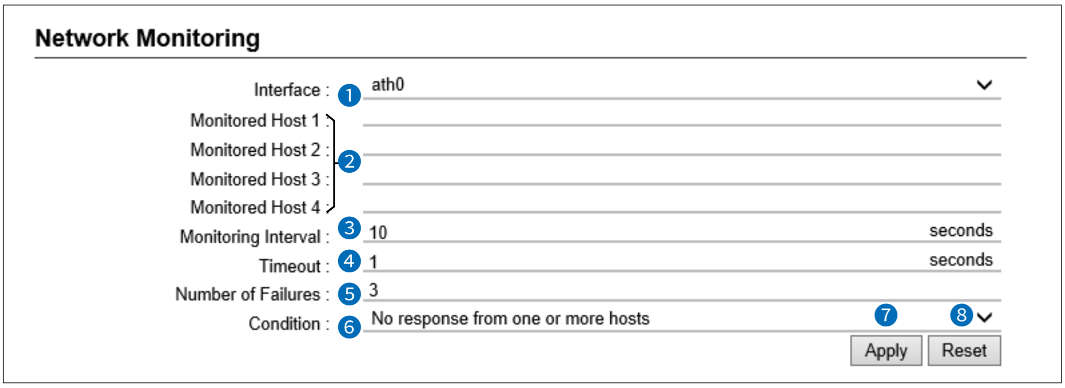
Wireless Settings > Wireless 1/Wireless 2 > Network Monitoring

■ Network Monitoring

Configure the automated network disconnect settings.

When a network error or malfunction is detected, the monitoring function automatically deactivates the Virtual AP.

- The AP-95M may fail to detect error or malfunction, depending on the security setting. Check the network environment before using the monitor function.



Network Monitoring

Interface : ❶ ath0

Monitored Host 1 :
Monitored Host 2 : ❷
Monitored Host 3 :
Monitored Host 4 :

Monitoring Interval : ❸ 10 seconds

Timeout : ❹ 1 seconds

Number of Failures : ❺ 3

Condition : ❻ No response from one or more hosts ❼ ❽

❶ **Interface** .... Select the Virtual AP to use the Monitoring function.

(Default: Wireless 1→ath0
Wireless 2→ath1)

- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.

❷ **Monitored Host 1 ~ 4** .... Enter the IP address of the host to be monitored.

- PING is periodically sent according to the set interval. (When this is left blank (default), no PING will not be sent.)

❸ **Monitoring Interval** .... Enter the PING interval in seconds. (Default: 10)
(Range: 1 ~ 120)

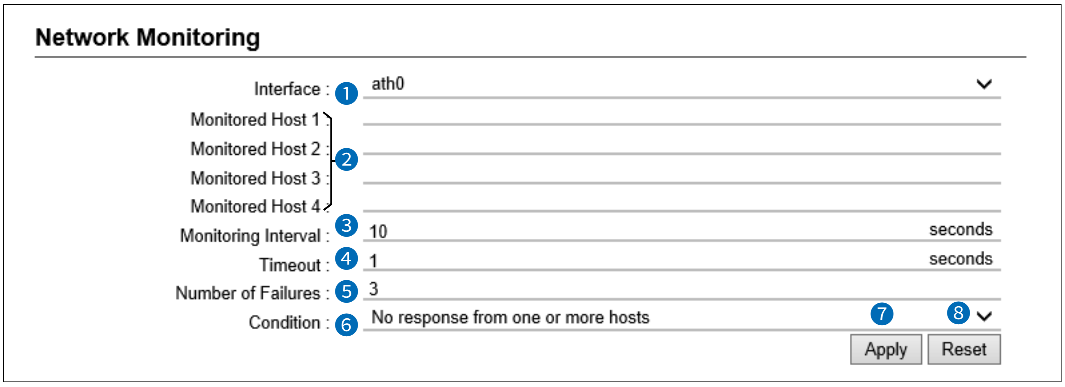
❹ **Timeout** .... Enter the PING Timeout time in seconds. (Default: 1)
(Range: 1 ~ 10)

❺ **Number of Failures** .... Enter the PING failure count. (Default: 3)
If the PING fails set times, the Monitoring function deactivates the Virtual AP.
(Range: 1 ~ 10 times)

[Network Monitoring] Screen

Wireless Settings > Wireless 1/Wireless 2 > Network Monitoring

■ Network Monitoring



Network Monitoring

Interface : ❶ ath0

Monitored Host 1 :
Monitored Host 2 : ❷
Monitored Host 3 :
Monitored Host 4 :

Monitoring Interval : ❸ 10 seconds

Timeout : ❹ 1 seconds

Number of Failures : ❺ 3

Condition : ❻ No response from one or more hosts

❻ **Condition** .... Select the condition to deactivate the Virtual AP.

(Default: No response from one or more hosts)

- **No response from one or more hosts**
  The Monitoring function deactivates when no response is received from one or more hosts.
- **No response from any of the hosts**
  The Monitoring function deactivates when no response is received from all hosts.

❼ **<Apply>** .... Click to apply entries.

❽ **<Reset>** .... Click to reset the settings.

- You cannot reset after clicking <Apply>.

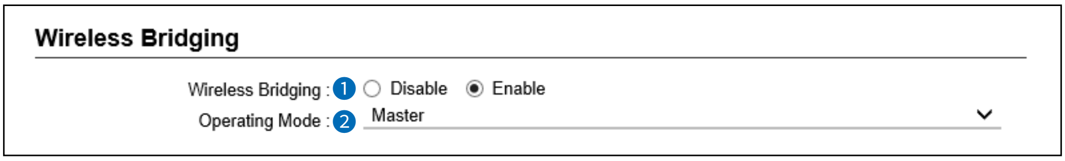
[Wireless Bridging] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging

■ Wireless Bridging

Setting screen for the Wireless Bridging.

• This screen is an example of when [Wireless Bridging] (❶) item is set to "Enable."



Wireless Bridging

Wireless Bridging : ❶ ○ Disable ● Enable

Operating Mode : ❷ Master

❶ **Wireless Bridging** .... Set whether or not to use the Wireless Bridging function enable.

(Default: Disable)

❷ **Operating Mode** .... Select the function mode form Master or Client.

• The SSID and security settings that are set to the Master's Virtual AP [ath0] (Wireless 1) and [ath1] (Wireless 2) are used for the Wireless Bridging communication.

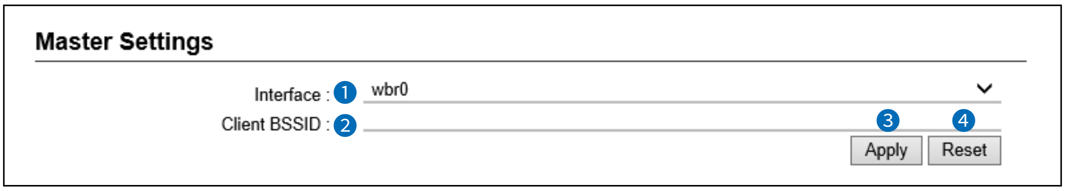
[Wireless Bridging] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging

■ Master Settings

The setting screen of when the AP-95M is used as the Master unit.

- This item appears when "Master" is selected in the [Wireless Bridging] item. Refer to page 3-91 for the screen of when the AP-95M is used as the Client unit.



Master Settings

Interface : ① wbr0

Client BSSID : ②

① **Interface** .... Select the bridge communication interface to register.

(Default: Wireless 1→wbr0
Wireless 2→wbr8)

- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.
- Up to 8 clients can be registered.
- You cannot change the interface name.

② **Client BSSID** .... Enter the client's BSSID in 12 digits (hexadecimal).

③ **<Apply>** .... Click to apply entries.

④ **<Reset>** .... Click to reset the settings.

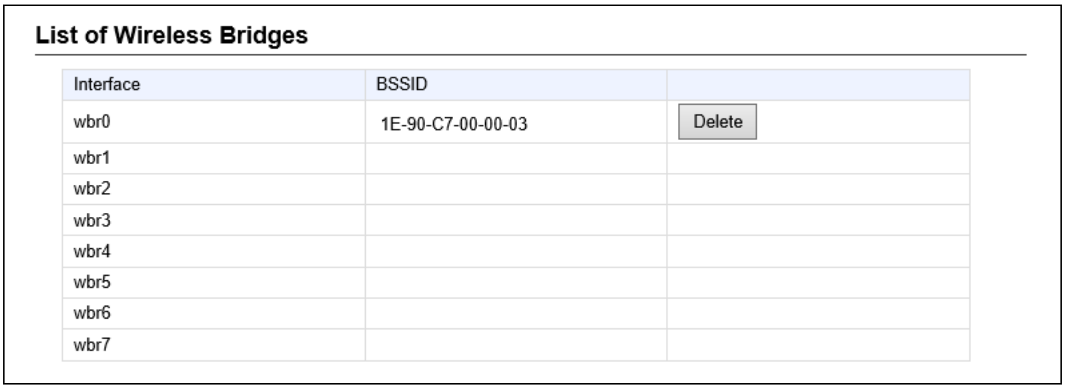
- You cannot reset after clicking <Apply>.

[Wireless Bridging] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging

■ List of Wireless Bridges

Displays the Wireless Bridge entries.



List of Wireless Bridges

Interface	BSSID	
wbr0	1E-90-C7-00-00-03	Delete
wbr1		
wbr2		
wbr3		
wbr4		
wbr5		
wbr6		
wbr7		

(This is an example.)

Click <Delete> to cancel the entry.

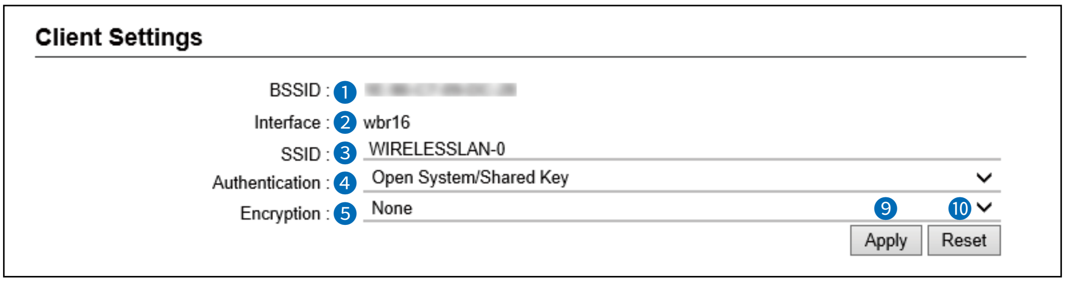
[Wireless Bridging] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging

■ Client Settings

The setting screen of when the AP-95M is used as the Client unit.

- This item appears when "Client" is selected in the [Wireless Bridging] item.
  Refer to page 3-89 for the screen of when the AP-95M is used as the Client unit.
- Items (❻, ❼, ❽) appear, depending on the content that is set to items (❹ and ❺). (pp. 3-91 and 3-92)



Client Settings

BSSID : ①

Interface : ② wbr16

SSID : ③ WIRELESSLAN-0

Authentication : ④ Open System/Shared Key

Encryption : ⑤ None ⑨ ⑩

① BSSID .... The Host's BSSID is displayed.
This BSSID is registered to the host station in the Bridging communication.

② Interface .... The bridge communication interface by name
- You cannot change the interface name. (Default: Wireless 1→wbr16
  Wireless 2→wbr17)

③ SSID .... Enter the host's SSID (Default: WIRELESSLAN-0)

④ Authentication .... Select the authentication method that is registered to the host.
(Default: Opne System/Shared Key)

About the Authentication method:

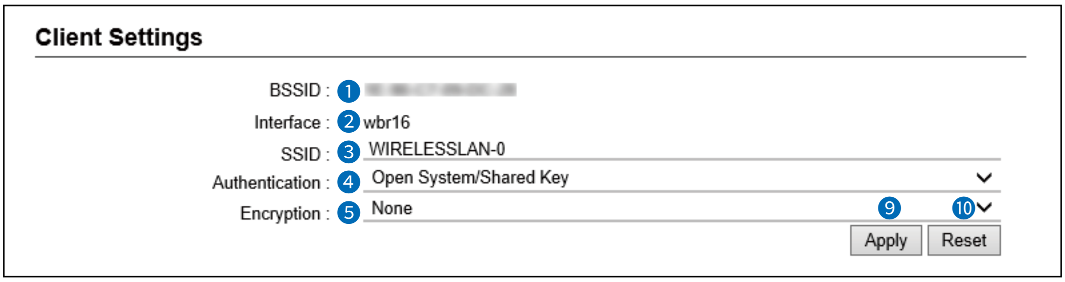
- **Open System/Shared key**
  The authentication method (Open System/Shared Key) is automatically applied to the access that is in "WEP RC4."
- **Open System**
  No authentication method is automatically applied to the access that is in "WEP RC4."
- **Shared Key**
  Shared key is used for the authentication.
- **WPA2-PSK**
  Shared key is used for the authentication. This is a simple authentication method without using the RADIUS server. The client connection is authenticated on the shared key.
- **WPA-PSK/WPA2-PSK**
  An automatic authentication method (WPA-PSK/WPA2-PSK).
- **WPA-PSK (Pre-Shared Key)**
  Shared key is used for the authentication.
  A simple authentication method without a RADIUS server.

[Wireless Bridging] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging

■ Client Settings

- Items (⑥, ⑦, ⑧) appear, depending on the content that is set to items (④, ⑤). (pp. 3-91 and 3-92)



Client Settings

BSSID : ① [redacted]
Interface : ② wbr16
SSID : ③ WIRELESSLAN-0
Authentication : ④ Open System/Shared Key
Encryption : ⑤ None ⑨ ⑩

⑤ **Encryption** .... Select the encryption type from "WEP RC4," "TKIP," and "AES."

(Default: None)

About the encryption method:

- **None**

  Communication is not encrypted.

  - You can select this option when "Open System/Shared Key" or "Open System" is selected in the [Authentication] (④) item.
  - Selecting other encryption option is recommended.

- **WEP RC4**

  Communication is encrypted using the encryption key.

  - Select he bit length from 64 (40)/128 (104)/152 (128) bits.
  - You can select this option when "Open System/Shared Key," "Open System" or "Shared Key" is selected in the [Authentication] (④) item.

- **AES (Advanced Encryption Standard)**

  The encryption key is periodically updated. More securer encryption method than "TKIP."

  - You can select this option when "WPA-PSK" or "WPA2-PSK" is selected in the [Authentication] (④) item.

- **TKIP/AES**

  "TKIP/AES" is automatically applied to the access from a wireless LAN station.

  Only when "AES" is detected, the communication rate exceeds 54 Mbps.

  - You can select this option when "WPA-PSK" or "WPA2-PSK" is selected in the [Authentication] (④) item.

- **TKIP (Temporal Key Integrity Protocol)**

  The encryption key is periodically updated. More securer encryption method than "WEP RC4."

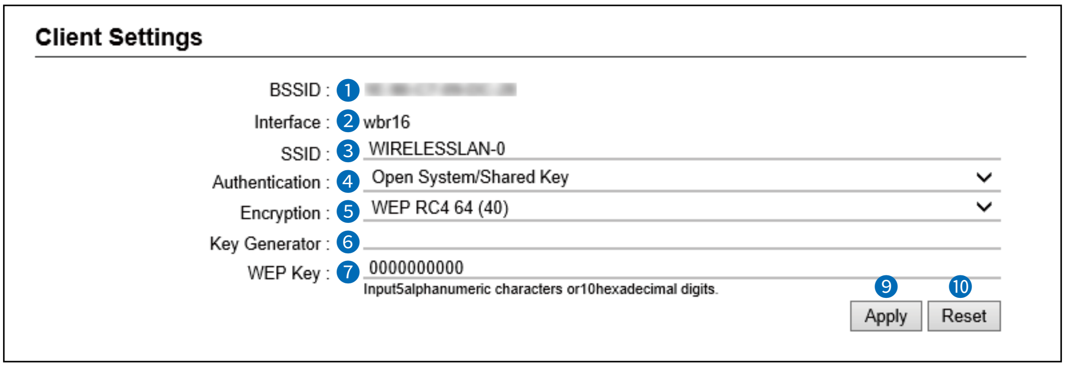
  - You can select this option when "WPA-PSK" or "WPA2-PSK" is selected in the [Authentication] (④) item.

[Wireless Bridging] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging

■ Client Settings

- Items (❻, ❼, ❽) appear, depending on the content that is set to items (❹, ❺). (pp. 3-91 and 3-92)



Client Settings

BSSID : ❶

Interface : ❷ wbr16

SSID : ❸ WIRELESSLAN-0

Authentication : ❹ Open System/Shared Key

Encryption : ❺ WEP RC4 64 (40)

Key Generator : ❻

WEP Key : ❼ 0000000000

Input5alphanumeric characters or10hexadecimal digits.

❻ **Key Generator** .... Displayed when "WEP RC4" is selected in the [Encryption] (❺) item. Enter the string to generate the key in hexadecimal. (Default: (blank))

❼ **WEP Key** .... If you do not use the Key Generator, enter the key directly in hexadecimal or in ASCII code. (Case distinction) (Default: 0000000000)

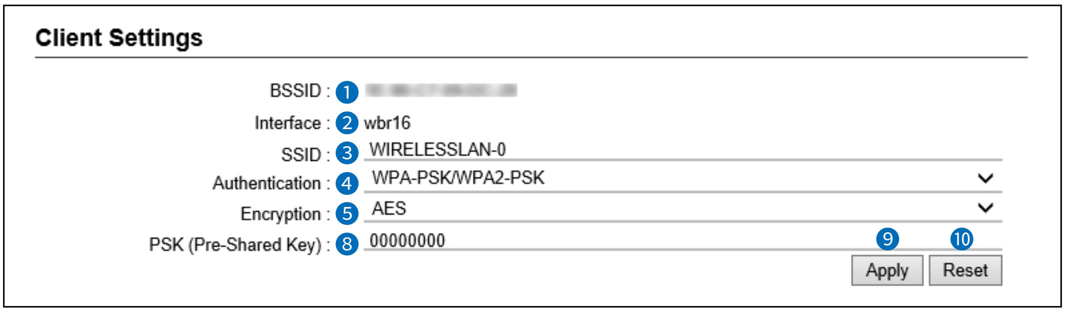
- WEP64(40): 10 digits in hexadecimal, 5 characters in ASCII
- WEP128(104): 26 digits in hexadecimal, 13 characters in ASCII

[Wireless Bridging] Screen

Wireless Settings > Wireless 1/Wireless 2 > Wireless Bridging

■ Client Settings

- Items (⑥, ⑦, ⑧) appear, depending on the content that is set to items (④, ⑤). (pp. 3-91 and 3-92)



Client Settings

BSSID : [redacted]

Interface : wbr16

SSID : WIRELESSLAN-0

Authentication : WPA-PSK/WPA2-PSK

Encryption : AES

PSK (Pre-Shared Key) : 00000000

⑧ PSK (Pre-Shared Key) .... [Enter the key in the alphanumeric when "WPA-PSK," "WPA2-PSK" or "WPA-PSK/WPA2-PSK" in the [Authentication] (④) item. (Default: 00000000)
- The shared key must be matched with the network device that communicates with.
- Enter the key directly in hexadecimal (64 digits) or in ASCII code. (Case distinction)

⑨ <Apply> .... Click to apply entries.

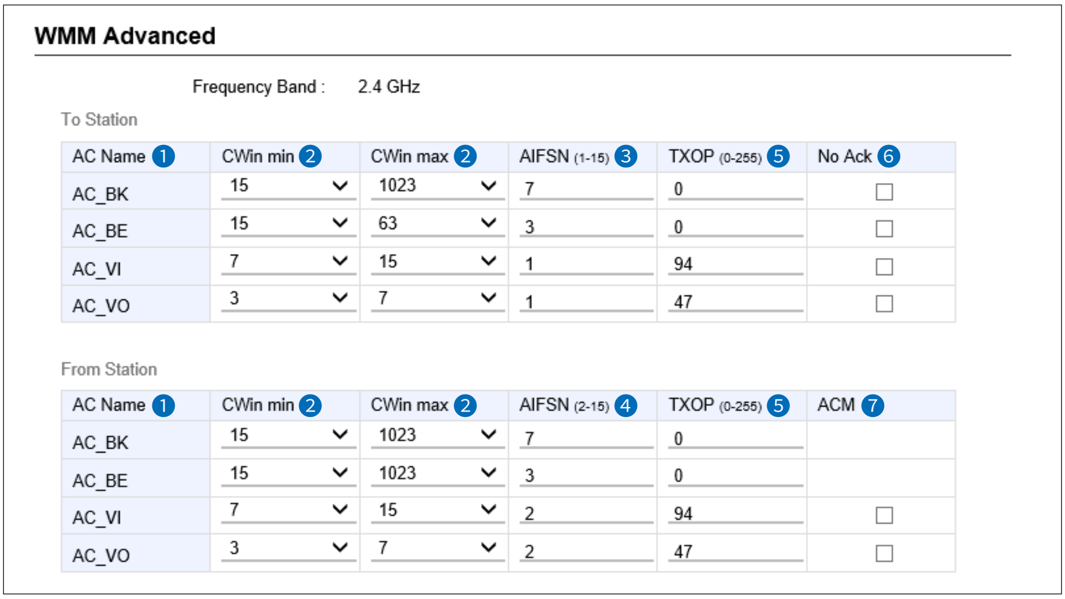
⑩ <Reset> .... Click to reset the settings.
- You cannot reset after clicking <Apply>.

[WMM Advanced] Screen

Wireless Settings > Wireless 1/Wireless 2 > WMM Advanced

■ WMM Advanced

To use the WMM (Wi-Fi Multimedia) function, set the EDCA (Enhanced Distributed Channel Access) parameter to [To Station] and [From Station] items.
Priorize the packets from AP-95M to wireless LAN stations by setting the EDCA parameter to the [To Station] item.



WMM Advanced

Frequency Band : 2.4 GHz

To Station

AC Name ❶	CWin min ❷	CWin max ❷	AIFSN (1-15) ❸	TXOP (0-255) ❺	No Ack ❻
AC_BK	15	1023	7	0	□
AC_BE	15	63	3	0	□
AC_VI	7	15	1	94	□
AC_VO	3	7	1	47	□

From Station

AC Name ❶	CWin min ❷	CWin max ❷	AIFSN (2-15) ❹	TXOP (0-255) ❺	ACM ❼
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	□
AC_VO	3	7	2	47	□

❶ **AC Name ....** Set the EDCA parameter to each access category (AC_BK, AC_BE, AC_VI, AC_VO).
Priority (These values are set accordance with the Wi-Fi alliance principal.):

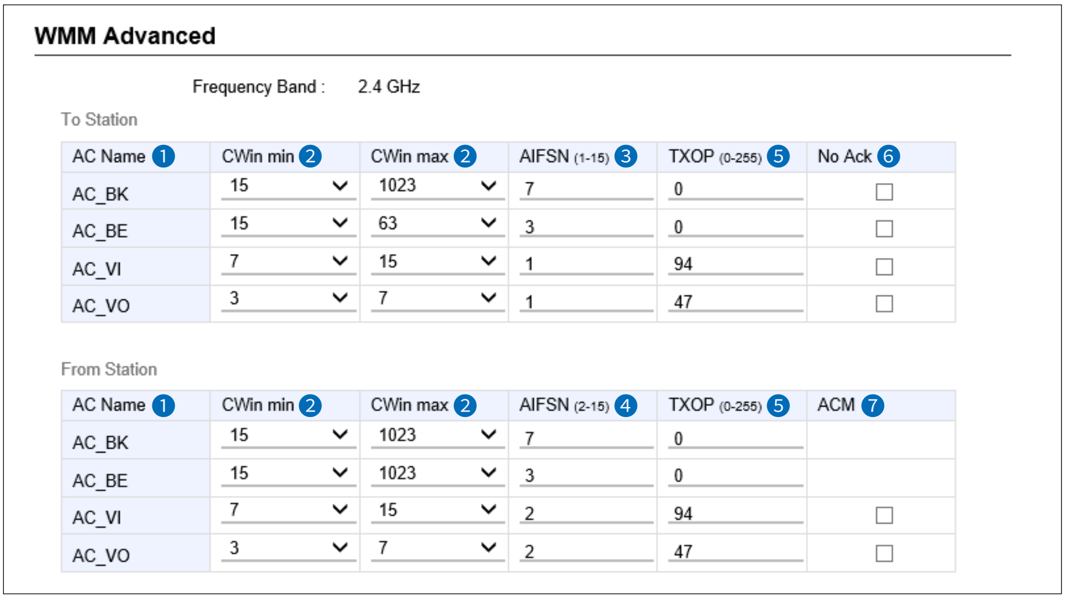
"AC_BK":	Low
"AC_BE":	Normal
"AC_VI":	Priorized
"AC_VO":	Most priorized

NOTE:
Generally, the EDCA parameters are not needed to be changed.
If you change the parameter, keep the priority according to the access category that is established by the Wi-Fi alliance.
If you change the priority, some controls such as ACM (❼) may not work properly.

[WMM Advanced] Screen

Wireless Settings > Wireless 1/Wireless 2 > WMM Advanced

■ WMM Advanced



WMM Advanced

Frequency Band : 2.4 GHz

To Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (1-15) ③	TXOP (0-255) ⑤	No Ack ⑥
AC_BK	15	1023	7	0	□
AC_BE	15	63	3	0	□
AC_VI	7	15	1	94	□
AC_VO	3	7	1	47	□

From Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (2-15) ④	TXOP (0-255) ⑤	ACM ⑦
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	□
AC_VO	3	7	2	47	□

❷ **CWin min/CWin max**...............

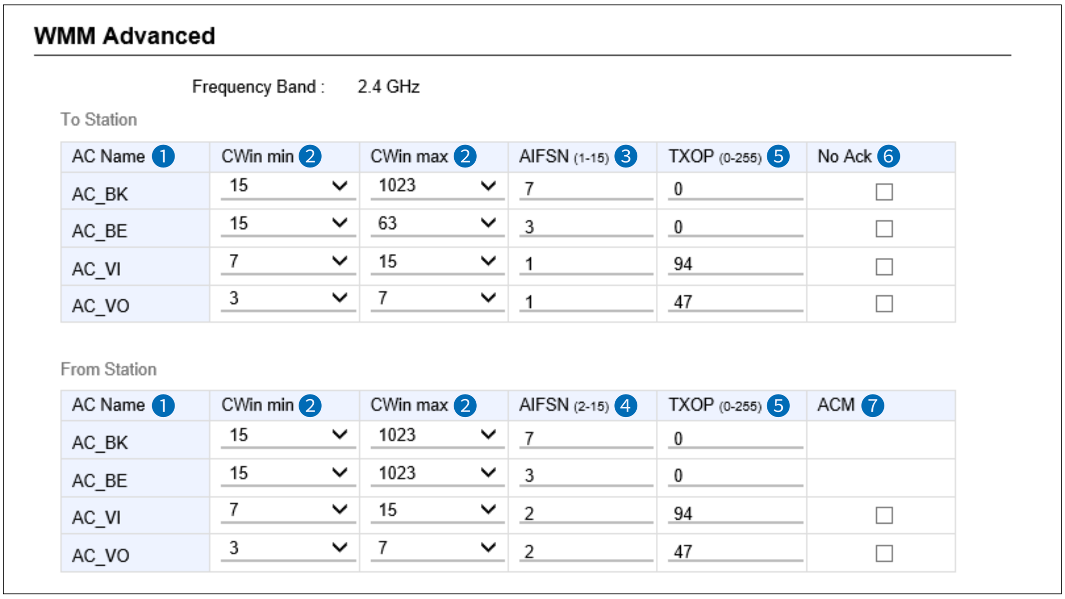
Select the minimum value and maximum value of CWin (Contention Window). This setting prevents the frame collision.

Lower value makes the priority level higher, and higher value makes the priority level lower. (Default: [To Station]/[From Station]
CWin min→ AC_BK (15)
AC_BE (15)
AC_VI (7)
AC_VO (3)
[To Station]
CWin max→ AC_BK (1023)
AC_BE (63)
AC_VI (15)
AC_VO (7)
[From Station]
CWin max→ AC_BK (1023)
AC_BE (1023)
AC_VI (15)
AC_VO (7))

[WMM Advanced] Screen

Wireless Settings > Wireless 1/Wireless 2 > WMM Advanced

■ WMM Advanced



WMM Advanced

Frequency Band : 2.4 GHz

To Station

AC Name ❶	CWin min ❷	CWin max ❷	AIFSN (1-15) ❸	TXOP (0-255) ❺	No Ack ❻
AC_BK	15	1023	7	0	□
AC_BE	15	63	3	0	□
AC_VI	7	15	1	94	□
AC_VO	3	7	1	47	□

From Station

AC Name ❶	CWin min ❷	CWin max ❷	AIFSN (2-15) ❹	TXOP (0-255) ❺	ACM ❼
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	□
AC_VO	3	7	2	47	□

❸ AIFSN (1-15) .... Enter the Arbitration Interframe Space Number.
Lower value makes the priority higher.
(Range: 1 ~ 15) (Default: [To Station]→ AC_BK (7)
AC_BE (3)
AC_VI (1)
AC_VO (1))

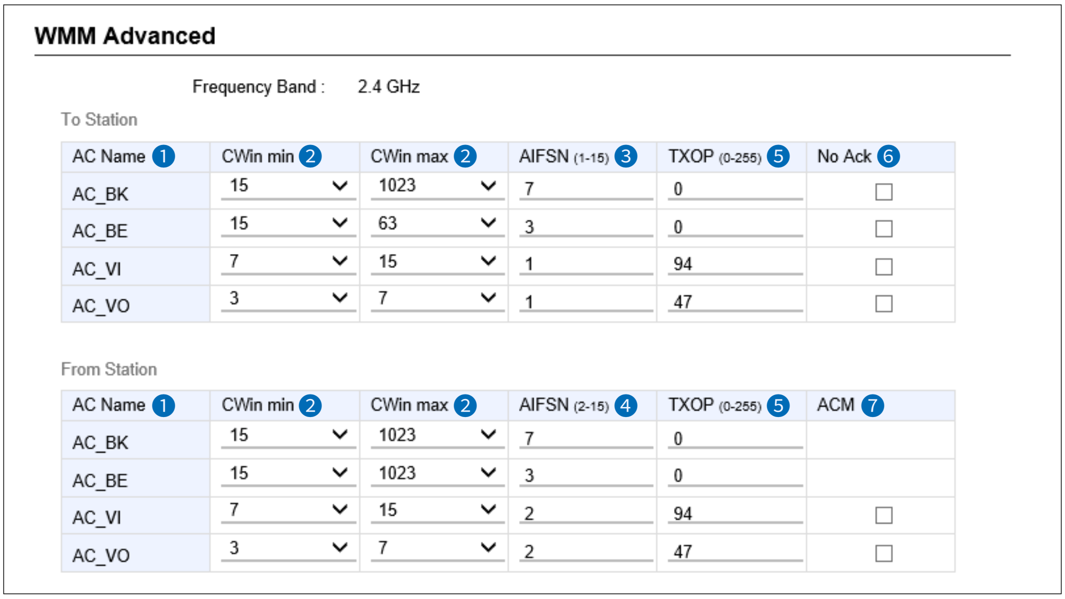
❹ AIFSN (2-15) .... Enter the Arbitration Interframe Space Number.
Lower value makes the priority higher.
(Range: 2 ~ 15) (Default: [From Station]→ AC_BK (7)
AC_BE (3)
AC_VI (2)
AC_VO (2))

❺ TXOP (0-255) .... Enter the transmission opportunity limit.
When "0" is entered, only one frame can be transmitted.
(Default: [To Station]/[From Station]
AC_BK (0)
AC_BE (0)
AC_VI (94)
AC_VO (47))

[WMM Advanced] Screen

Wireless Settings > Wireless 1/Wireless 2 > WMM Advanced

■ WMM Advanced



WMM Advanced

Frequency Band : 2.4 GHz

To Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (1-15) ③	TXOP (0-255) ⑤	No Ack ⑥
AC_BK	15	1023	7	0	□
AC_BE	15	63	3	0	□
AC_VI	7	15	1	94	□
AC_VO	3	7	1	47	□

From Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (2-15) ④	TXOP (0-255) ⑤	ACM ⑦
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	□
AC_VO	3	7	2	47	□

⑥ **No Ack** .... Select whether or not to resend the packet according to the received ACK (Acknowledgment), by entering a check mark into the box.

(Default: [To Station]→ AC_BK □
AC_BE □
AC_VI □
AC_VO □)

⑦ **ACM** .... Select whether or not to apply the ACM (Admission Control Mandatory), by entering a check mark into the box. (Default: [From Station]→ AC_VI □
AC_VO □)

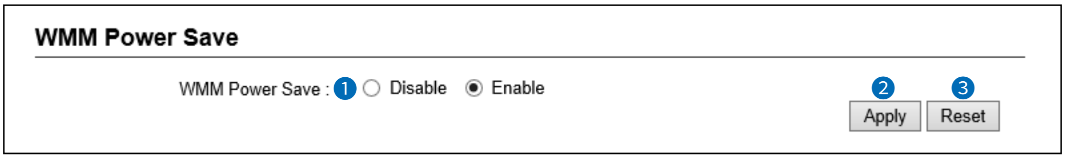
• To apply this setting, the client also must support this setting.

[WMM Advanced] Screen

Wireless Settings > Wireless 1/Wireless 2 > WMM Advanced

■ WMM Power Save

Configure the power save setting for the Unscheduled Automatic Power Save Delivery function. (IEEE802.11e U-APSD)



WMM Power Save

WMM Power Save : ① ○ Disable ● Enable

① **WMM Power Save** .... Select "Enable" to use the WMM Power Save function. (Default: Enable)
The client wireless LAN station automatically enters to the Power Save mode according to the necessity.

② **<Apply>** .... Click to apply entries.

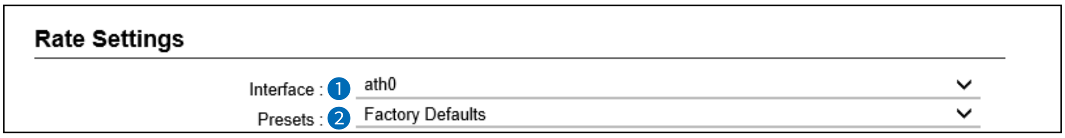
③ **<Reset>** .... Click to reset the settings.
- You cannot reset after clicking <Apply>.

[Rate] Screen

Wireless Settings > Wireless 1/Wireless 2 > Rate

■ Rate Settings

You can restrict the wireless LAN stations that communicate with Virtual AP by establishing the lowest communication rate.



Rate Settings

Interface : ① ath0

Presets : ② Factory Defaults

① Interface .... Select the AP to change the setting. (Default: Wireless 1→ath0
Wireless 2→ath1)

You can independently set the [Legacy] and [HT-MCS] items.

- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.

② Presets .... You can configure the settings based on a preset. (Default: Factory Defaults)

- This item is not displayed when Wireless 2 (5 GHz) is used.
- The network connection may be unstable, depending on the setting. Not to change this setting is recommended.
- If the network connection is unstable, try other presets.
- A "–" is displayed at the preset that has been changed from its default.

- **Reject IEEE802.11b Stations***
  Basic rate is fixed to 6 Mbps, 12 Mbps and 24 Mbps.
  IEEE802.11g stations can still communicate using the IEEE802.11b rates.
- **Disable IEEE802.11b Rates***
  Prevents the decrease of communication in quality.
- **Optimized for Voice Stations**
  Disables the IEEE802.11b and some other rates to stabilizes the voice communication.
- **Optimized for Stable Communication 1**
  Priories the communication stability than communication rate.
  Disables some IEEE802.11ac rates and IEEE802.11n rates, to stabilizes the communication.
- **Optimized for Stable Communication 2**
  More stable setting than "Optimized for Stable Communication 1."

* These items are not displayed for Wireless 2 (5 GHz).

[Rate] Screen

Wireless Settings > Wireless 1/Wireless 2 > Rate

■ List of the preset rate

Default	
1Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
2Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
5.5Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
6Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
9Mbps	Enable
11Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
12Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
18Mbps	Enable
24Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
36Mbps	Enable
48Mbps	Enable
54Mbps	Enable
MCS0 ~ MCS15	Enable
VHT-MCS 1 ~ 2 stream	(Only for IEEE802.11ac) MCS0-9
Multicast rate	1Mbps (2.4 GHz) 6Mbps (5 GHz)

Reject IEEE802.11b Stations	
1Mbps	Enable
2Mbps	Enable
5.5Mbps	Enable
6Mbps	Basic rate
9Mbps	Enable
11Mbps	Enable
12Mbps	Basic rate
18Mbps	Enable
24Mbps	Basic rate
36Mbps	Enable
48Mbps	Enable
54Mbps	Enable
MCS0 ~ MCS15	Enable
Multicast rate	1Mbps

Disable IEEE802.11b Rates	
1Mbps	Disable
2Mbps	Disable
5.5Mbps	Disable
6Mbps	Basic rate
9Mbps	Enable
11Mbps	Disable
12Mbps	Basic rate
18Mbps	Enable
24Mbps	Basic rate
36Mbps	Enable
48Mbps	Enable
54Mbps	Enable
MCS0 ~ MCS15	Enable
Multicast rate	6Mbps

[Rate] Screen

Wireless Settings > Wireless 1/Wireless 2 > Rate

■ List of the preset rate

Optimized for Voice Stations	
1Mbps	Disable (2.4 GHz) Not displayed (5 GHz)
2Mbps	Disable (2.4 GHz) Not displayed (5 GHz)
5.5Mbps	Disable (2.4 GHz) Not displayed (5 GHz)
6Mbps	Basic rate
9Mbps	Disable
11Mbps	Disable (2.4 GHz) Not displayed (5 GHz)
12Mbps	Basic rate
18Mbps	Disable
24Mbps	Basic rate
36Mbps	Disable
48Mbps	Disable
54Mbps	Enable
MCS0	Enable
MCS1	Disable
MCS2	Disable
MCS3	Disable
MCS4	Enable
MCS5	Disable
MCS6	Disable
MCS7	Enable
MCS8	Enable
MCS9	Disable
MCS10	Disable
MCS11	Disable
MCS12	Enable
MCS13	Disable
MCS14	Disable
MCS15	Enable
VHT-MCS 1 ~ 2 stream	(Only for IEEE802.11ac) MCS0-9
Multicast rate	6Mbps

Optimized for Stable Communication 1	
1Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
2Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
5.5Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
6Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
9Mbps	Enable
11Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
12Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
18Mbps	Enable
24Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
36Mbps	Enable
48Mbps	Enable
54Mbps	Enable
MCS0 ~ MCS11	Enable
MCS12 ~ MCS15	Disable
VHT-MCS 1 ~ 2 stream	(Only for IEEE802.11ac) MCS0-8
Multicast rate	1Mbps (2.4 GHz) 6Mbps (5 GHz)

Optimized for Stable Communication 2	
1Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
2Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
5.5Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
6Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
9Mbps	Enable
11Mbps	Basic rate (2.4 GHz) Not displayed (5 GHz)
12Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
18Mbps	Enable
24Mbps	Enable (2.4 GHz) Basic rate (5 GHz)
36Mbps	Enable
48Mbps	Enable
54Mbps	Enable
MCS0 ~ MCS7	Enable
MCS8 ~ MCS15	Disable
VHT-MCS 1 ~ 2 stream	(Only for IEEE802.11ac) MCS0-7
Multicast rate	1Mbps (2.4 GHz) 6Mbps (5 GHz)

[Rate] Screen

Wireless Settings > Wireless 1/Wireless 2 > Rate

About the communication rate

Set the Virtual AP's communication rate on the Rate Settings screen.

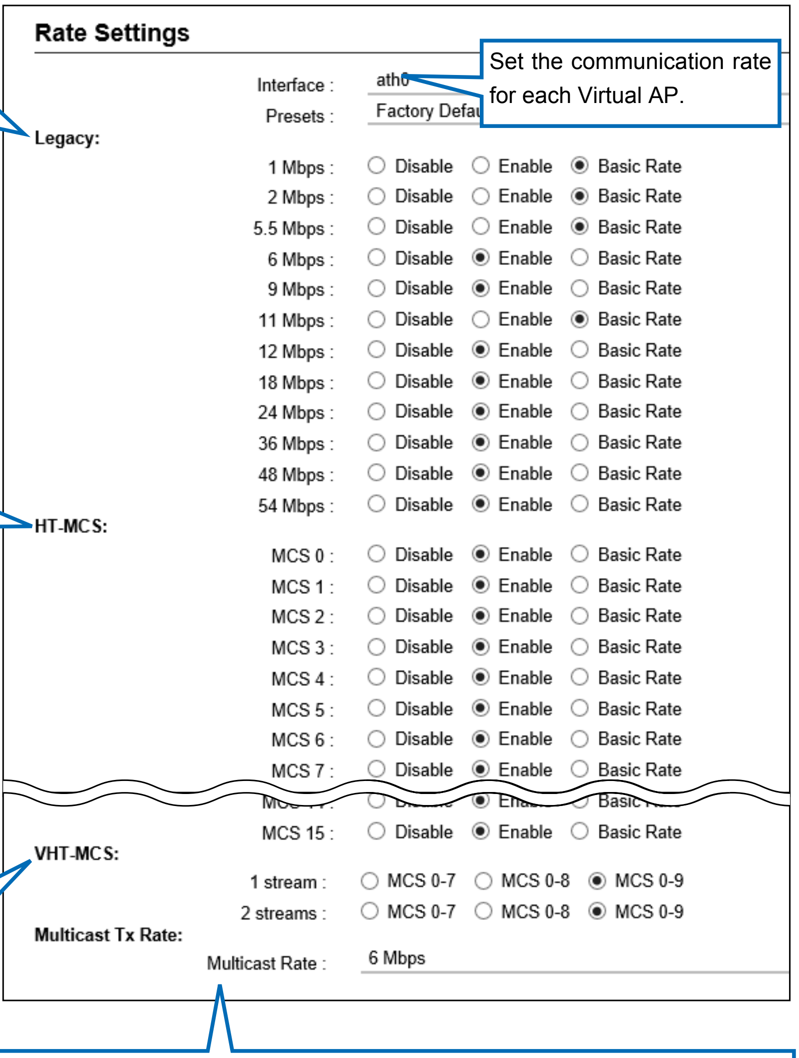
You can limit the connection from wireless LAN stations or specify the communication rate in the multicast packet mode.

Note: This setting may affect the system performance when a huge amount of packets is processed. Using this only for the testing purpose is recommended.

- Disable: Inhibits the communication in the selected rate.
- Enable: The communication rate is fixed to the selected rate.
- Basic rate: Inhibits the connection from the wireless LAN station if the communication in the set rate is not enabled.

- Disable: Inhibits the communication in the selected MCS value.
- Enable: The communication rate is fixed to the selected MCS value.
- Basic rate: Inhibits the connection from the wireless LAN station if the communication in the set MCS value is not enabled.

Only for Wireless 2 (5 GHz): Set the MCS value for each number of stream (1 stream and 2 streams).



Rate Settings

Interface : ath0

Presets : Factory Defau

Set the communication rate for each Virtual AP.

Legacy:

1 Mbps :	○ Disable	○ Enable	● Basic Rate
2 Mbps :	○ Disable	○ Enable	● Basic Rate
5.5 Mbps :	○ Disable	○ Enable	● Basic Rate
6 Mbps :	○ Disable	● Enable	○ Basic Rate
9 Mbps :	○ Disable	● Enable	○ Basic Rate
11 Mbps :	○ Disable	○ Enable	● Basic Rate
12 Mbps :	○ Disable	● Enable	○ Basic Rate
18 Mbps :	○ Disable	● Enable	○ Basic Rate
24 Mbps :	○ Disable	● Enable	○ Basic Rate
36 Mbps :	○ Disable	● Enable	○ Basic Rate
48 Mbps :	○ Disable	● Enable	○ Basic Rate
54 Mbps :	○ Disable	● Enable	○ Basic Rate

HT-MCS:

MCS 0 :	○ Disable	● Enable	○ Basic Rate
MCS 1 :	○ Disable	● Enable	○ Basic Rate
MCS 2 :	○ Disable	● Enable	○ Basic Rate
MCS 3 :	○ Disable	● Enable	○ Basic Rate
MCS 4 :	○ Disable	● Enable	○ Basic Rate
MCS 5 :	○ Disable	● Enable	○ Basic Rate
MCS 6 :	○ Disable	● Enable	○ Basic Rate
MCS 7 :	○ Disable	● Enable	○ Basic Rate
MCS 15 :	○ Disable	● Enable	○ Basic Rate

VHT-MCS:

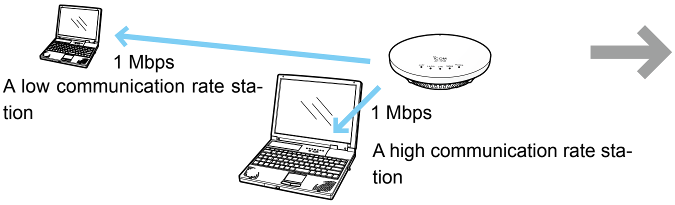
1 stream :	○ MCS 0-7	○ MCS 0-8	● MCS 0-9
2 streams :	○ MCS 0-7	○ MCS 0-8	● MCS 0-9

Multicast Tx Rate:

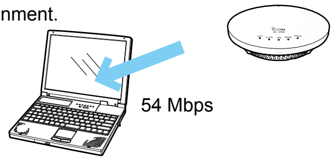
Multicast Rate : 6 Mbps

Setting the multicast transmission rate

When several wireless stations are connected to the AP-95M in the multicast mode, and the communication rate is different among them, the communication rate is fixed to the lowest. (In this situation, you cannot set the communication rate higher.)


1 Mbps
A low communication rate station
1 Mbps
A high communication rate station

When the communication rate in the multicast packet mode, the communication rate may get higher, depending on the signal strength or area environment.



•The transmission rate in the multicast mode is set to the lowest as the default.

[Rate] Screen

Wireless Settings > Wireless 1/Wireless 2 > Rate

■ About the communication rate for each MCS value

Refer to the table below for setting the HT-MCS value.

HT-MCS	Number of stream	Communication rate (Mbps)			
		Bandwidth 20MHz (HT20)		Bandwidth 40MHz (HT40)	
		800ns GI	400ns GI	800ns GI	400ns GI
0	1	6.5	7.2	13.5	15
1		13	14.4	27	30
2		19.5	21.7	40.5	45
3		26	28.9	54	60
4		39	43.3	81	90
5		52	57.8	108	120
6		58.5	65	121.5	135
7		65	72.2	135	150
8	2	13	14.4	27	30
9		26	28.9	54	60
10		39	43.3	81	90
11		52	57.8	108	120
12		78	86.7	162	180
13		104	115.6	216	240
14		117	130	243	270
15		130	144.4	270	300

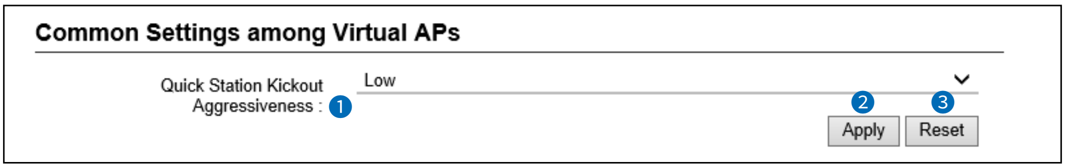
VHT-MCS	Number of stream	Communication rate (Mbps)					
		Bandwidth 20MHz (VHT20)		Bandwidth 40MHz (VHT40)		Bandwidth 80MHz (VHT80)	
		800ns GI	400ns GI	800ns GI	400ns GI	800ns GI	400ns GI
0	1	6.5	7.2	13.5	15	29.3	32.5
1		13	14.4	27	30	58.5	65
2		19.5	21.7	40.5	45	87.8	97.5
3		26	28.9	54	60	117	130
4		39	43.3	81	90	175.5	195
5		52	57.8	108	120	234	260
6		58.5	65	121.5	135	263.3	292.5
7		65	72.2	135	150	292.5	325
8		78	86.7	162	180	351	390
9		–	–	180	200	390	433.3
0	2	13	14.4	27	30	58.5	65
1		26	28.9	54	60	117	130
2		39	43.3	81	90	175.5	195
3		52	57.8	108	120	234	260
4		78	86.7	162	180	351	390
5		104	115.6	216	240	468	520
6		117	130	243	270	526.5	585
7		130	144.4	270	300	585	650
8		156	173.3	324	360	702	780
9		–	–	360	400	780	866.7

[Rate] Screen

Wireless Settings > Wireless 1/Wireless 2 > Rate

■ Common Settings among Virtual APs

You can restrict the wireless LAN stations to improve the communication quality.



Common Settings among Virtual APs

Quick Station Kickout Aggressiveness : ① Low

② Apply ③ Reset

① Quick Station Kickout Aggressiveness

.... Select the aggressiveness of kicking out the station with a low communication quality, to prevent the influence to other stations. (Default: Low)

By kicking out low communication quality wireless stations, improves the communication in the communication area.

Select the Kickout level from "High," "Medium," "Low" or "Disable."

A Higher option kicks out more low quality communication stations.

② <Apply> .... Click to apply entries.

③ <Reset> .... Click to reset the settings.

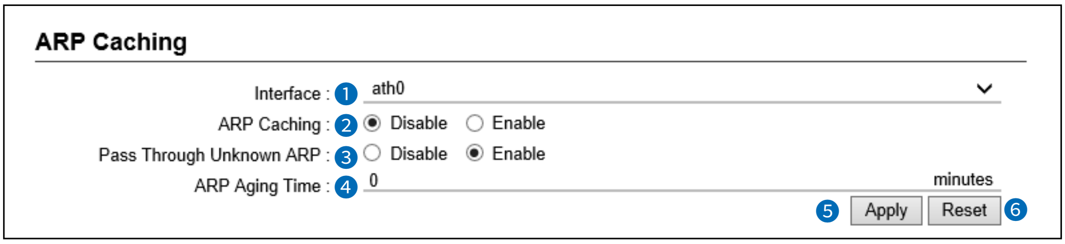
- You cannot reset after clicking <Apply>.

[ARP Caching] Screen

Wireless Settings > Wireless 1/Wireless 2 > ARP Caching

■ ARP Caching

The ARP Caching saves the power consumption of wireless LAN stations.



ARP Caching

Interface : ❶ ath0

ARP Caching : ❷ ● Disable ○ Enable

Pass Through Unknown ARP : ❸ ○ Disable ● Enable

ARP Aging Time : ❹ 0 minutes

❶ **Interface** .... Select a Virtual AP to change setting. (Default: Wireless 1→ath0 Wireless 2→ath1)

- You can change the settings on the [Virtual AP] or [Security] screen.
- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.
- When you use "ath01" ~ "ath07" or "ath11" ~ "ath17," set "Enable"in the [Virtual AP] item.
- If JavaScript is disabled in your web browser, parameters may not be correctly displayed.

❷ **ARP Caching** .... Select "Enable" to use the ARP Caching function. (Default: Disable)

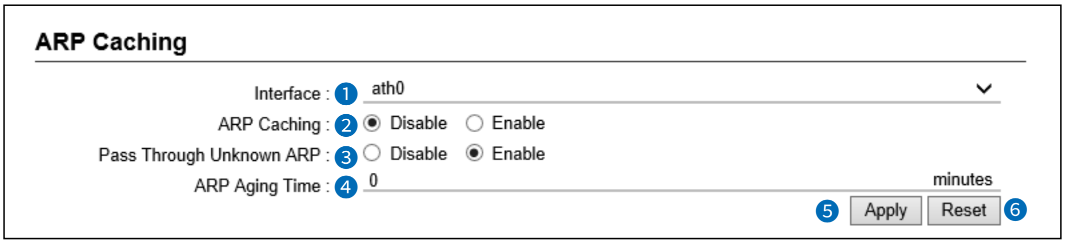
❸ **Pass Through Unknown ARP**... Select "Disable" to block Unknown ARP. (Default: Enable)
When receiving a ARP request, the AP-95M handles the packet, according to the IP address.

- **Wireless LAN stations with known IP address**
  If the TargetIP of received ARP request is known, the AP-95M responds to the request instead of the wireless LAN station.
  If the TargetIP is unknown and "Disable" is selected, the packet is discarded.
- **At least one Wireless LAN station with known IP address**
  If the TargetIP of received ARP request is known, the AP-95M responds to the request instead of the wireless LAN station.
  If the TargetIP is unknown and "Disable" is selected, the packet is passed, regardless of the setting.

[ARP Caching] Screen

Wireless Settings > Wireless 1/Wireless 2 > ARP Caching

■ ARP Caching



ARP Caching

Interface : ① ath0

ARP Caching : ② ● Disable ○ Enable

Pass Through Unknown ARP : ③ ○ Disable ● Enable

ARP Aging Time : ④ 0 minutes

④ **ARP Aging Time**..................... Enter the period of time in minutes before/until the obtained ARP information is automatically deleted. (Default: 0)
 (Range: 0 ~ 1440)

- After the ARP information is obtained and set time is expired, the ARP information is automatically deleted.
- If the connected wireless LAN station is a DHCP client, lease time that is determined by the DHCP server will take priority.
- If "0" is entered, the ARP information is NOT automatically deleted.
- When the wireless LAN station is disconnected from the AP-95M, the ARP information will be deleted regardless of the remaining time.

⑤ **<Apply>** .... Click to apply entries.

⑥ **<Reset>** .... Click to reset the settings.

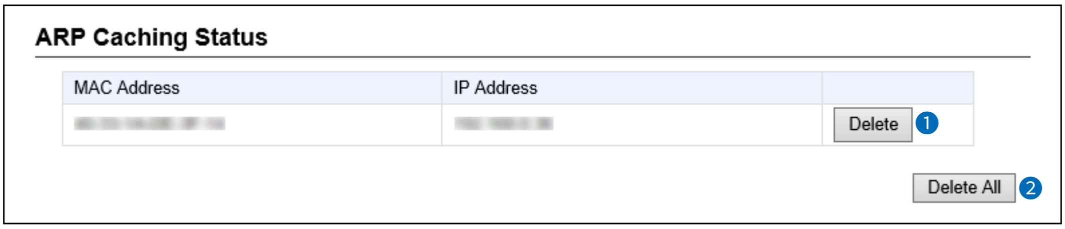
- You cannot reset after clicking <Apply>.

[ARP Caching] Screen

Wireless Settings > Wireless 1/Wireless 2 > ARP Chaching

■ ARP Caching Status

You can delete the ARP information that is indicated by the combination of MAC address and IP address, according to the necessity.



ARP Caching Status

MAC Address	IP Address	
[illegible]	[illegible]	Delete

❶ **<Delete>** .... Click to delete the ARP cache.

❷ **<Delete All>**........................... Click to delete all ARP cache.

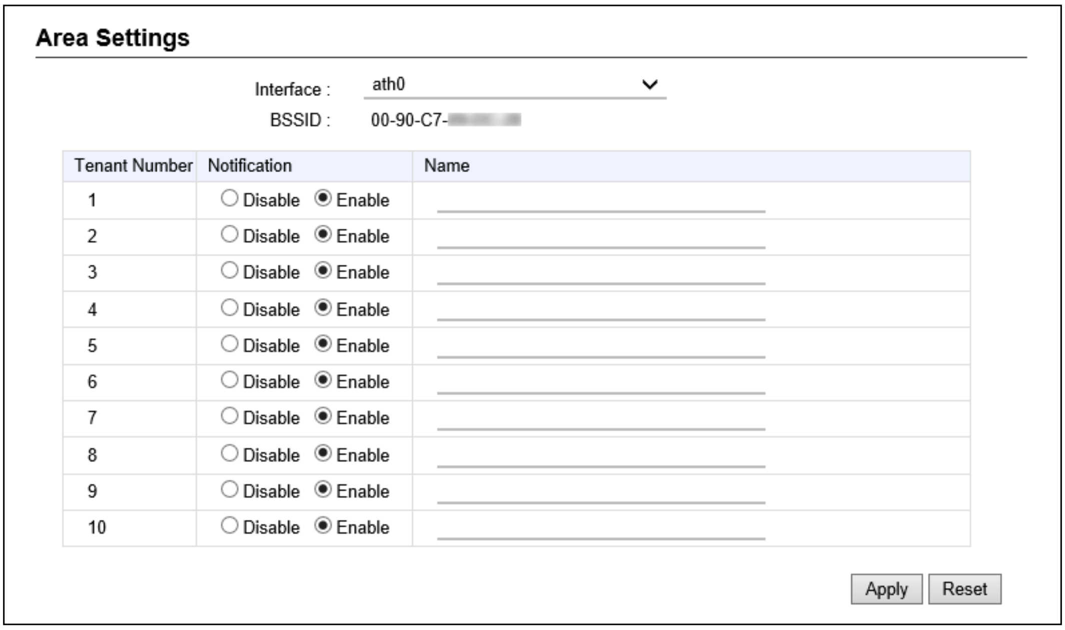
[IP Advanced Radio System] Screen

Wireless Settings > Wireless 1/Wireless 2 > IP Advanced Radio System

■ About the IP Advanced Radio System

Configure to use the AP-95M with the controller (example: IP1000C) area call function.
Select "Enable" in the [Notification] item and enter the tenant name to search an access point on the network to register the AP's BSSID and name.

- Select a Virtual AP in the [Interface] item, and configure the tenant settings.
- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.
- Enter a name (Example: Ground floor) of up to 31 characters to each tenant.



Area Settings

Interface : ath0

BSSID : 00-90-C7-[redacted]

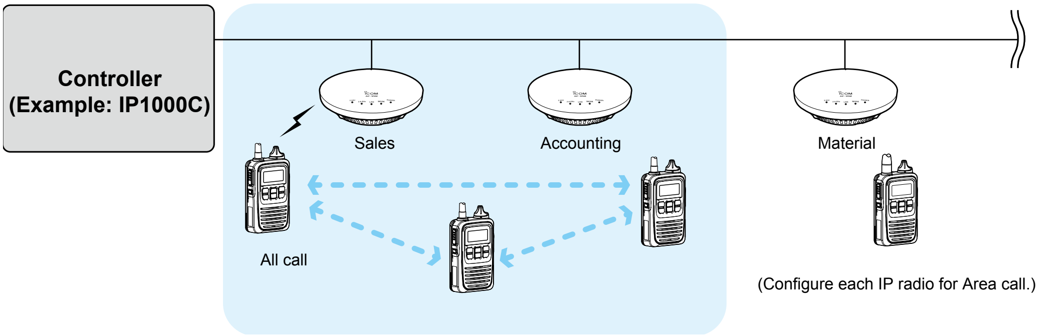
Tenant Number	Notification	Name
1	○ Disable ● Enable	
2	○ Disable ● Enable	
3	○ Disable ● Enable	
4	○ Disable ● Enable	
5	○ Disable ● Enable	
6	○ Disable ● Enable	
7	○ Disable ● Enable	
8	○ Disable ● Enable	
9	○ Disable ● Enable	
10	○ Disable ● Enable	

About the Area call

Area call is a communication of IP radios in a limited area (For example: Ground floor).

- You have to configure APs in the area ("Sales" and "Accounting" in the example shown below.)

An example of All Call

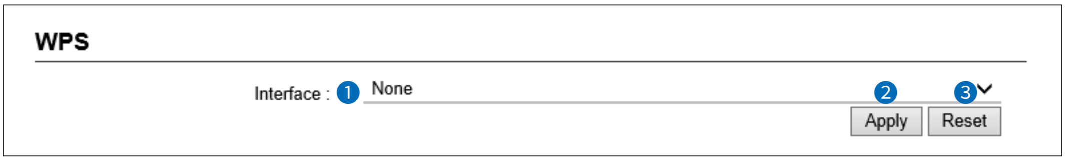


[WPS] Screen

Wireless Settings > WPS

■ WPS

With the function that the “Wi-Fi Alliance” proposed, SSID and Security (WPA-PSK/WPA2-PSK) can automatically be set to the AP-95M and the wireless LAN station that supports the WPS (Wi-Fi Protected Setup) function.



❶ **Interface** .... Select the interface (example: ath0) that use the WPS function with. (Default: None)

- Select "ath0," "ath01" ~ "ath07" for Wireless 1, select "ath1," "ath11" ~ "ath17" for Wireless 2.
- Wireless LAN station must support the WPS function.
- You cannot use this function while the Hide SSID (p. 3-70) is enabled.
- The supported authentication methods are "WPA-PSK" and "WPA2-PSK."
- The supported encryption type is only TKIP/AES.

❷ **<Apply>** .... Click to apply entries.

❸ **<Reset>** .... Click to reset the settings.

- You cannot reset after clicking <Apply>.

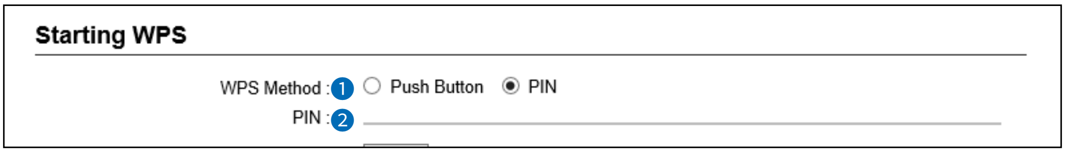
[WPS] Screen

Wireless Settings > WPS

■ Starting WPS

Configure the automatic SSID and PSK (Pre-Shared Key) that are set to the Virtual AP for the WPS (Wi-Fi Protected Setup) function on a wireless LAN station.

When "Push Button" is selected:

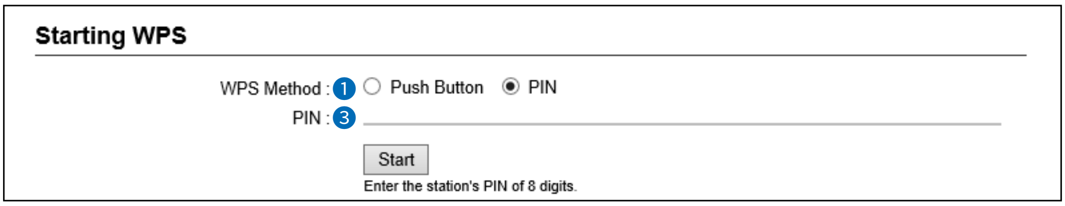


Starting WPS

WPS Method : ❶ ○ Push Button ● PIN

PIN : ❷

When "PIN" is selected:



Starting WPS

WPS Method : ❶ ○ Push Button ● PIN

PIN : ❸

Enter the station's PIN of 8 digits.

❶ **WPS Method** .... Select the WPS configuration method. (Default: Push Button)

- **Push Button**
  The SSID and the security configuration are automatically applied to the wireless LAN station, by pushing the WPS button on the station.
- **PIN**
  The SSID and the security configuration are automatically applied to the wireless LAN station, according to the PIN code that is set to the station.

❷ **Push Button** .... Click "Start" to start the automatically appliy the SSID and security configuration.

- This button will appear after the WPS function is enabled.
- During the configuration, [MODE] blinks green (☀).
  [2.4GHz] or [5GHz] will light green (●) when the configuration has finished.

❸ **PIN**...................................... Enter the station's PIN of 8 digits, then click "Start" to start the automatically appliy the SSID and security configuration.

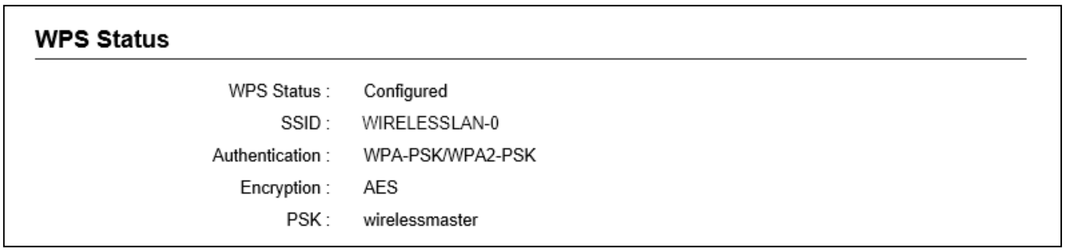
- Refer to the instruction manual supplied with the wireless LAN station for the PIN code.
- During the configuration, [MODE] blinks green (☀).
  [2.4GHz] or [5GHz] will light green (●) when the configuration has finished.

[WPS] Screen

Wireless Settings > WPS

■ WPS Status

The set Virtual AP settings are displayed.



WPS Status

WPS Status : Configured

SSID : WIRELESSLAN-0

Authentication : WPA-PSK/WPA2-PSK

Encryption : AES

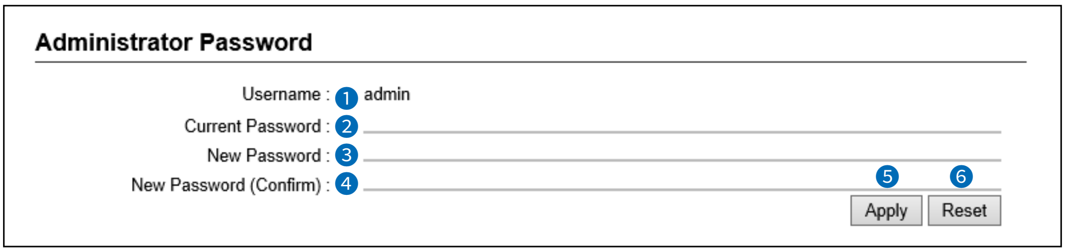
PSK : wirelessmaster

[Administrator] Screen

Management > Administrator

■ Administrator Password

As the default, you can access the setting screen with the User ID “admin” and Password “admin.”
You can prevent unauthorized access and setting modification by setting a password.



Administrator Password

Username : ❶ admin
Current Password : ❷
New Password : ❸
New Password (Confirm) : ❹

❶ **Username** .... Displays the administrator login ID (“admin”).
• This item cannot be changed.

❷ **Current Password** .... Carefully enter the current password. Use both lower and upper case letters. (Default: admin)
• The passwords are displayed in dots or asterisks.

❸ **New Password** .... Enter the desired new password of up to 31 characters. Use both lower and upper case letters.

❹ **New Password (Confirm)** ...... Enter the new password again.

❺ **<Apply>** .... Click to apply entries.

❻ **<Reset>** .... Click to restore the settings.
• You cannot restore after clicking <Apply>.

To prevent unauthorized access
You must carefully chose your password, and change it occasionally. See “Changing the administrator password” on the supplied leaflet for password setting details.
• Choose one that is not easy to guess.
• Use numbers, characters and both lower and upper case letters.

NOTE:
If you have forgotten your password, you cannot access the AP-95M’s setting screen.

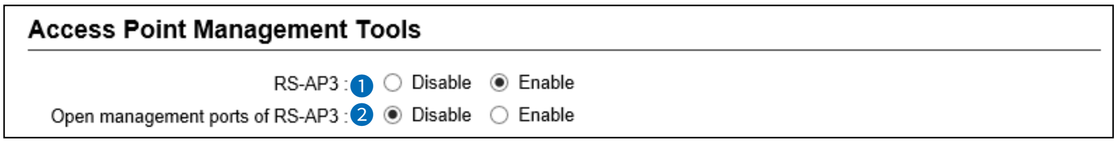
If you forget your password:
Hold down the [MODE] button by following the instructions described in the supplied leaflet.
The AP-95M will have to be reset to its default values.

[Management Tools] Screen

Management > Management Tools

■ Access Point Management Tools

You cancontrol the AP-95M using the RS-AP3 by a centrized management.



Access Point Management Tools

RS-AP3 : ① ○ Disable ● Enable

Open management ports of RS-AP3 : ② ● Disable ○ Enable

① **RS-AP3** .... Select "Enable" to control the AP-95M by the RS-AP3. (Default: Disable)

- While the AP-95M is controlled by the RS-AP3, you cannot change the settings on the AP-95M setting screen.

② **Open management ports of RS-AP3** Select "Enable" to allow the WAN access from the RS-AP3. (Default: Disable) When "Enable" is selected, the IP filter is automatically configured so that the RS-AP3 accesses the AP-95M through the WAN port.

- Even "Disable" is selected, you can allow the access by appropriately configuring the IP filter.

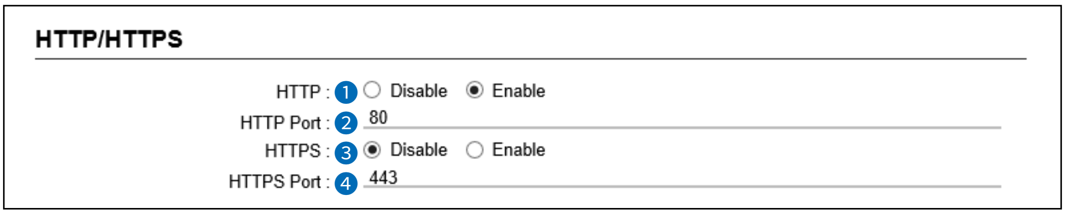
[Management Tools] Screen

Management > Management Tools

■ HTTP/HTTPS

HTTP and HTTPS are protocols to access the setting screen using internet browsers.

• If “Disable” is selected for both “HTTP” and “HTTPS,” the AP-95M’s setting screen cannot be accessed.



HTTP/HTTPS

HTTP : ① ○ Disable ● Enable

HTTP Port : ② 80

HTTPS : ③ ● Disable ○ Enable

HTTPS Port : ④ 443

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

② **HTTP Port** .... Enter the access port number. (Default: 80)
(Range: 80, 1024 ~ 65535)
• Some port numbers may not usable.
• Do not duplicate port numbers when using HTTPS, Telnet or SSH.

③ **HTTPS** .... Select “Enable” to accept the HTTPS protocol. (Default: Disable)
• HTTPS is a more secure protocol than HTTP.

④ **HTTPS Port** .... Enter the access port number. (Default: 443)
(Range: 443, 1024 ~ 65535)
• Some port may not be used.
• Do not duplicate port numbers when using HTTPS, Telnet or SSH.

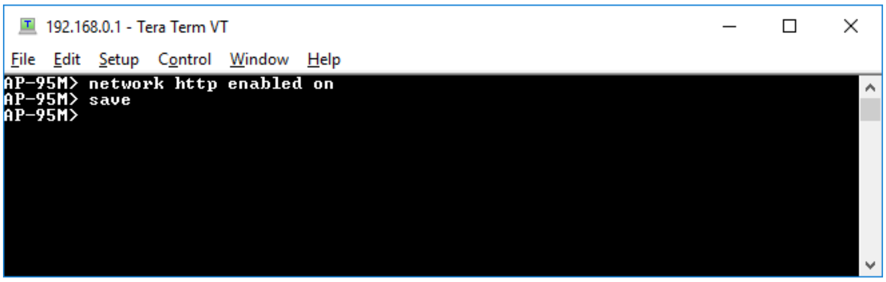
[Management Tools] Screen

Management > Management Tools

■ If you cannot access the setting screen

Access the AP-95M using SSH or Telnet (Teletype network) (example: 192.168.0.1).
Following “AP-95M>,” enter the letters written in bold as follows, and then push [Enter].
• When you use Telnet, you have to set the [Telnet] item to "Enable." (p. 3-117)

1. Enter “AP-95M> **network http enabled on**” and push [Enter].
2. Enter “AP-95M> **save**” and push [Enter].
3. Check if you can access the setting screen.

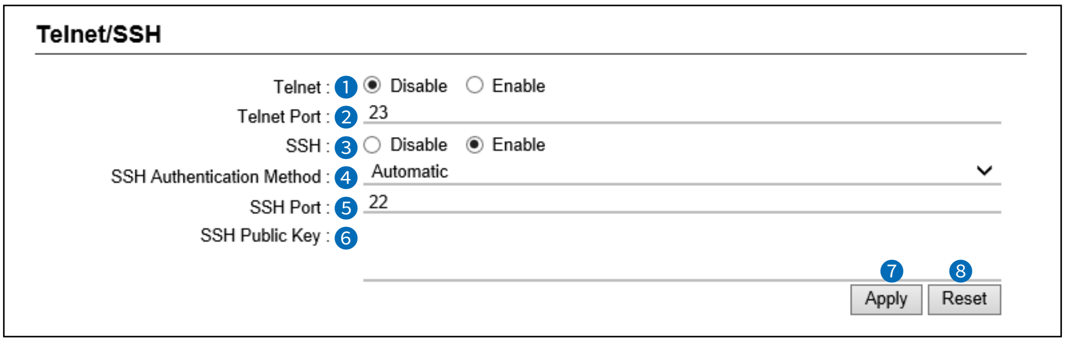

192.168.0.1 - Tera Term VT
File Edit Setup Control Window Help

```
AP-95M> network http enabled on
AP-95M> save
AP-95M>
```

[Management Tools] Screen

Management > Management Tools

■ Telnet/SSH



Telnet/SSH

Telnet : ① ● Disable ○ Enable

Telnet Port : ② 23

SSH : ③ ○ Disable ● Enable

SSH Authentication Method : ④ Automatic

SSH Port : ⑤ 22

SSH Public Key : ⑥

① **Telnet** .... Select “Disable” to block the Telnet protocol. (Default: Disable)

② **Telnet Port** .... Enter the access port number. (Default: 23)
(Range: 23, 1024 ~ 65535)
- Some port numbers may not usable.
- Do not duplicate port numbers when using HTTPS, Telnet or SSH.

③ **SSH** .... Select “Enable” to accept the SSH protocol. (Default: Enable)
- The SSH protocol encrypts the communication between the AP-95M and SSH client.

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.

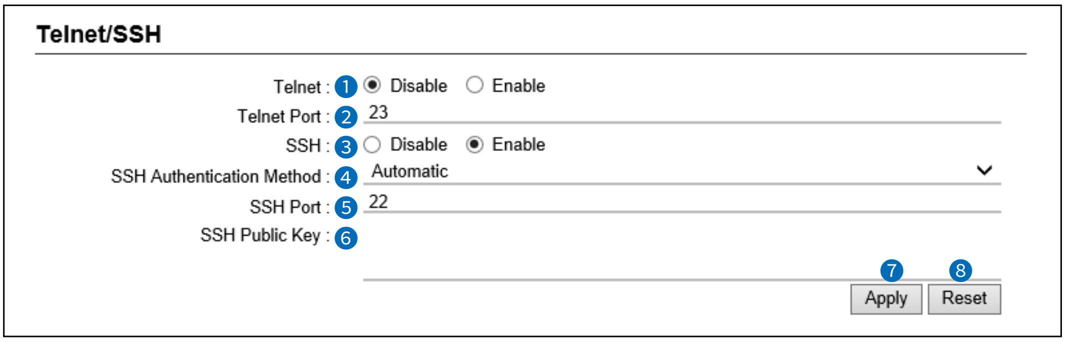
⑤ **SSH Port** .... Enter the access port number. (Default: 22)
(Range: 22, 1024 ~ 65535)
- Some port numbers may not usable.
- Do not duplicate port numbers when using HTTPS, Telnet or SSH.

⑥ **SSH Public Key** .... Enter the public key for communication between the AP-95M and SSH client.
- Open the public key file using a text editor appication, copy and paste it all to this item.

[Management Tools] Screen

Management > Management Tools

■ Telnet/SSH



Telnet/SSH

Telnet : ① ● Disable ○ Enable

Telnet Port : ② 23

SSH : ③ ○ Disable ● Enable

SSH Authentication Method : ④ Automatic

SSH Port : ⑤ 22

SSH Public Key : ⑥

⑦ **<Apply>** .... Click to apply entries.

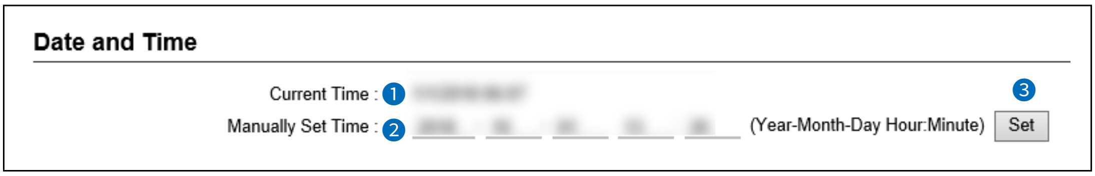
⑧ **<Reset>** .... Click to restore the settings.
- You cannot restore after clicking <Apply>.

[Date and Time] Screen

Management > Date and Time

■ Date and Time

You can set the AP-95M’s internal clock time.



Date and Time

Current Time : ①

Manually Set Time : ② (Year-Month-Day Hour:Minute) Set ③

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

② **Manually Set Time**.................. Displays the time when you have opened this screen.

- Refresh the browser screen to obtain the current time from the PC.

③ **<Set>**.................................... Click to set the internal clock to the time displayed in the [Manually Set Time] (②) item.

- Before clicking <Set>, refresh the browser screen.

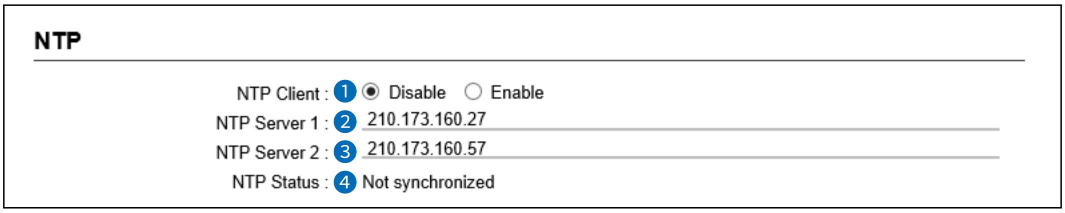
[Date and Time] Screen

Management > NTP

■ 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.



NTP

NTP Client : ❶ ● Disable ○ Enable

NTP Server 1 : ❷ 210.173.160.27

NTP Server 2 : ❸ 210.173.160.57

NTP Status : ❹ Not synchronized

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

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

- If the AP-95M cannot access this address, then the address set in the [NTP Server 2] (❸) item is used.
- The default NTP servers are provided by INTERNET MULTIFEED Co.

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

❹ **NTP Status** .... Displays the NTP synchronizing status.

NOTE:

The Automatic clock synchronize function synchronizes the internal clock with the time management server (NTP), and you need to set the “Static Routing” menu to the NTP server.

If you have not set the “Routing Table,” the automatic clock synchronize function cannot be used.

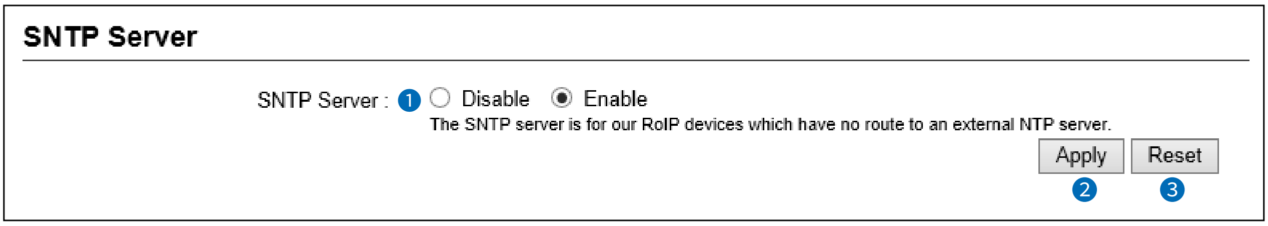
Enter “Static Routing” to set the “Routing Table” in one of the following menus.

- Network Settings > IP Address > IP Address > Default Gateway
- Network Settings > Static Routing > Static Routing

[Date and Time] Screen

Management > Date and Time

■ SNTP Server



SNTP Server

SNTP Server : ① ○ Disable ● Enable

The SNTP server is for our RoIP devices which have no route to an external NTP server.

① SNTP Server .... Select "Enable" to use the AP-95M as an SNTP server. (Default: Enable)
- When the AP-95M is used as its SNTP Server, this entry is not necessary.
- This function is for only Icom's RoIP devices.
  Use this function when you use an Icom RoIP device that cannot establish the route to an external NTP server.
- Before using this function, set the current time on the [Date and Time] screen.

② <Apply> .... Click to apply entries.

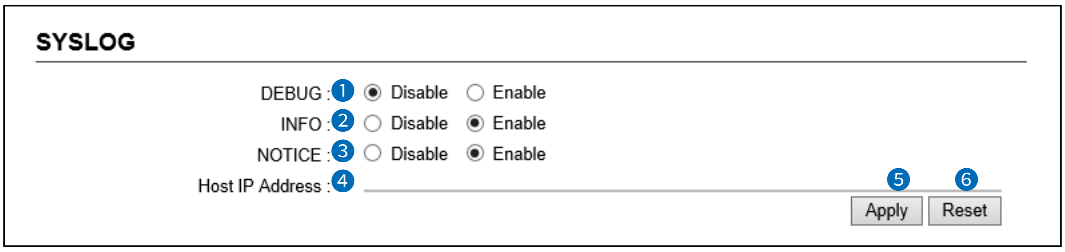
③ <Reset> .... Click to restore the settings.
- You cannot restore after clicking <Apply>.

[SYSLOG] Screen

Management > SYSLOG

■ SYSLOG

Select the information to be sent to the SYSLOG host.



SYSLOG

DEBUG : ● Disable ○ Enable

INFO : ○ Disable ● Enable

NOTICE : ○ Disable ● Enable

Host IP Address :

Apply Reset

❶ DEBUG .... Select "Enable" to send the DEBUG messages to the host that is set in the [Host IP Address] (❹) item. (Default: Disable)

❷ INFO................................ ... Select "Enable" to send the INFO messages to the host that is set in the [Host IP Address] (❹) item. (Default: Enable)

❸ NOTICE................................ Select "Enable" to send the NOTICE messages to the host that is set in the [Host IP Address] (❹) item. (Default: Enable)

❹ Host IP Address .... Enter the SYSLOG host's address.

❺ <Apply> .... Click to apply entries.

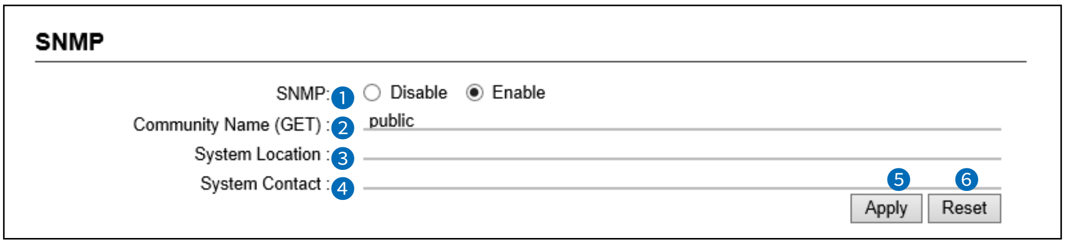
❻ <Reset> .... Click to restore the settings.
- You cannot restore after clicking <Apply>.

[SNMP] screen

Management > SNMP

■ SNMP

Configure the SNMP function.



SNMP

SNMP: ❶ ○ Disable ● Enable

Community Name (GET) : ❷ public

System Location : ❸

System Contact : ❹

❶ **SNMP** .... Select “Enable” to use the SNMP function. (Default: Enable)

❷ **Community Name (GET)...... ...** Enter the Community name to get the SNMP community string of up to 31 characters. (Default: public)

❸ **System Location** .... Enter the SNMP system location of up to 127 characters.

❹ **System Contact.................. ...** Enter the SNMP system contact of up to 127 characters.

❺ **<Apply>** .... Click to apply entries.

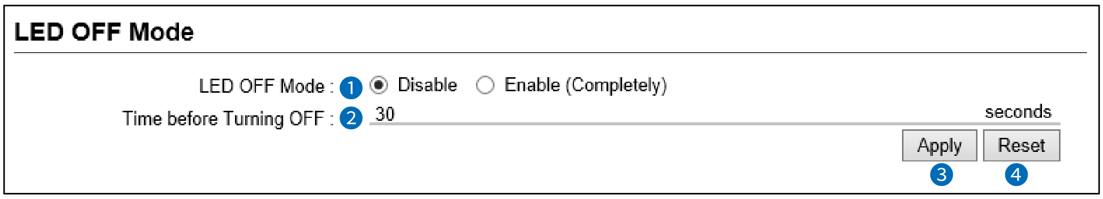
❻ **<Reset>** .... Click to restore the settings.
- You cannot restore after clicking <Apply>.

[LED] screen

Management > LED

■ LED OFF Mode

The LED function turns OFF LED indicators.



LED OFF Mode

LED OFF Mode : ❶ ● Disable ○ Enable (Completely)

Time before Turning OFF : ❷ 30 seconds

❶ **LED OFF Mode** .... Select "Enable" to use the LED function. (Default: Disable)
- Disable: LED indicators are ON.
- Enable (Completely): All LED indicators are OFF. When <MODE> is pushed, the LED indicator lights regardless of this setting.

❷ **Time before Turning OFF......** If "Enable" is selected in the [LED OFF Mode] (❶) item, enter the time before LED indicators turn OFF. (Default: 30 seconds) (Range: 0 ~ 3600 seconds)

❸ **<Apply>** .... Click to apply entries.

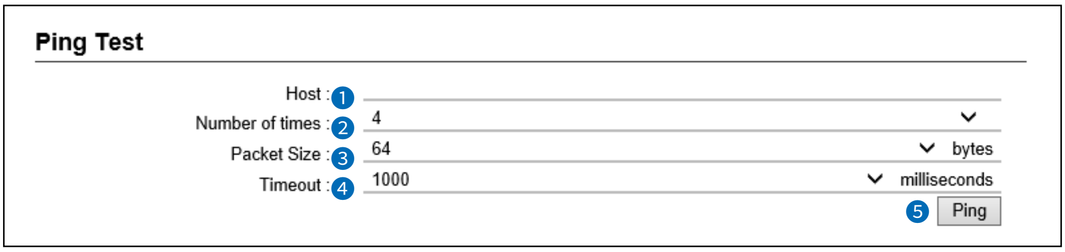
❹ **<Reset>** .... Click to restore the settings.
- You cannot restore after clicking <Apply>.

[Network Test] Screen

Management > Network Test

■ Ping Test

Run the Ping test.



Ping Test

Host : ①
Number of times : ② 4
Packet Size : ③ 64 bytes
Timeout : ④ 1000 milliseconds
⑤ Ping

① **Host** .... Enter the IP address or host name of up 64 characters to send the Ping packets to.

② **Number of times** .... Select the number of times to send from "1," "2," "4" and "8." (Default: 4)

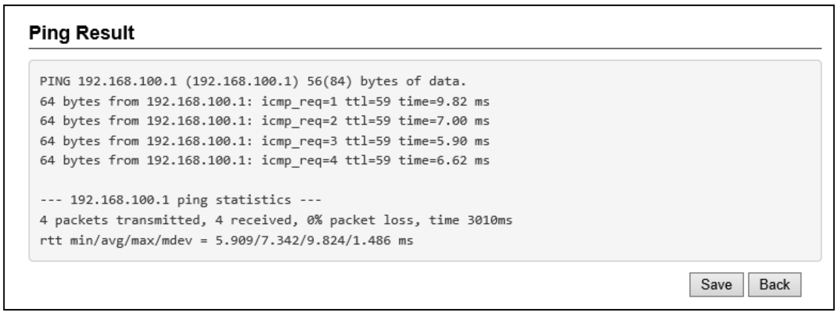
③ **Packet Size**........................ ... Select the data packet size from "32," "64," "128," "256," "512," "1024," "1448," "1500" and "2048" (Byte). (Default: 64)

④ **Timeout** .... Select the Ping response time from "500," "1000" and "5000" (milliseconds). (Default: 1000)

- 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.



Ping Result

```
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_req=1 ttl=59 time=9.82 ms
64 bytes from 192.168.100.1: icmp_req=2 ttl=59 time=7.00 ms
64 bytes from 192.168.100.1: icmp_req=3 ttl=59 time=5.90 ms
64 bytes from 192.168.100.1: icmp_req=4 ttl=59 time=6.62 ms

--- 192.168.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 5.909/7.342/9.824/1.486 ms
```

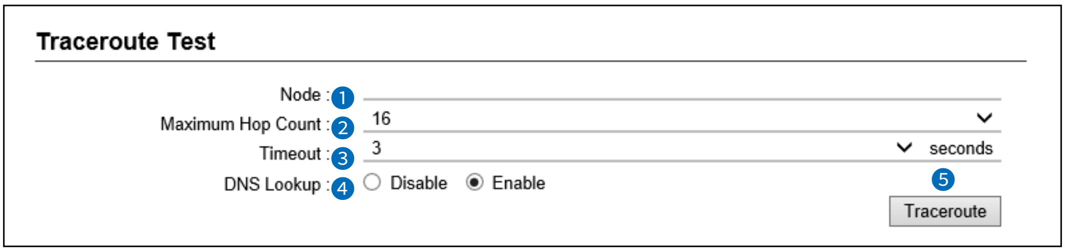
- Click <Save> to save the result to a PC as a text file (extension: “txt”).
  (The file is saved as “ping_host’s address.txt.”)
- Click <Back> to return to the Ping Test screen.

[Network Test] Screen

Management > Network Test

■ Traceroute Test

Run the Traceroute test.



Traceroute Test

Node :

Maximum Hop Count : 16

Timeout : 3 seconds

DNS Lookup : ○ Disable ● Enable

❶ **Node ....** Enter the node's (device's) IP address or domain name in 64 characters.

❷ **Maximum Hop Count ....** Select the maximum hop number from "4," "8," "16" and "32." (Default: 16)

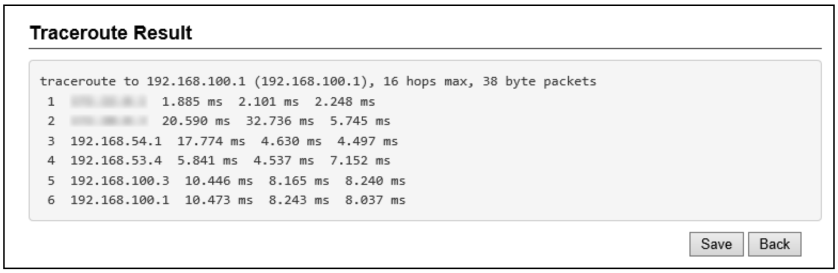
❸ **Timeout ....** Select the response time from "1," "3" and "5" (seconds). (Default: 3)

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

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

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

- The test result is displayed as shown below.



Traceroute Result

```
traceroute to 192.168.100.1 (192.168.100.1), 16 hops max, 38 byte packets
 1  [redacted]  1.885 ms  2.101 ms  2.248 ms
 2  [redacted]  20.590 ms  32.736 ms  5.745 ms
 3  192.168.54.1  17.774 ms  4.630 ms  4.497 ms
 4  192.168.53.4  5.841 ms  4.537 ms  7.152 ms
 5  192.168.100.3  10.446 ms  8.165 ms  8.240 ms
 6  192.168.100.1  10.473 ms  8.243 ms  8.037 ms
```

(This is only 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.

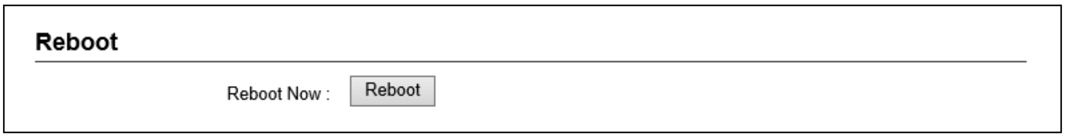
[Reboot] Screen

Management > Reboot

■ Reboot

Click <Reboot> to reboot the AP-95M.

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



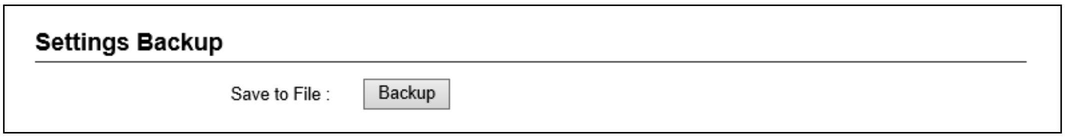
[Settings Backup/Restore] Screen

Management > Settings Backup/Restore

■ Settings Backup

Save the AP-95M's settings to a PC as a backup.

- DO NOT write the saved file to any other devices.



Settings Backup

Save to File : Backup

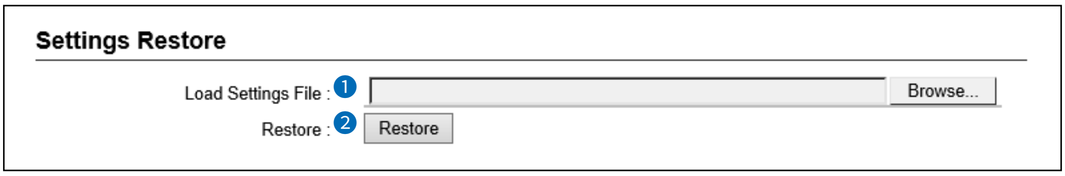
Save to File .... Click <Backup> to save the settings to a PC as a backup file (Extension: sav). See the topic below to load the saved file into the AP-95M.

Management > Settings Backup/Restore

■ Settings Restore

Load the setting file (Extension: "sav") to the AP-95M.

- Loading takes a few minutes.



Settings Restore

Load Settings File : ❶ Browse...

Restore : ❷ Restore

❶ **Load Settings File** .... Click <Browse...> to select the setting file.

❷ **Restore**................................ Click to load the setting into the AP-95M.

- The AP-95M's setting is overwritten.
- After loading, the AP-95M automatically reboots.
- A modified setting file will damage the AP-95M.

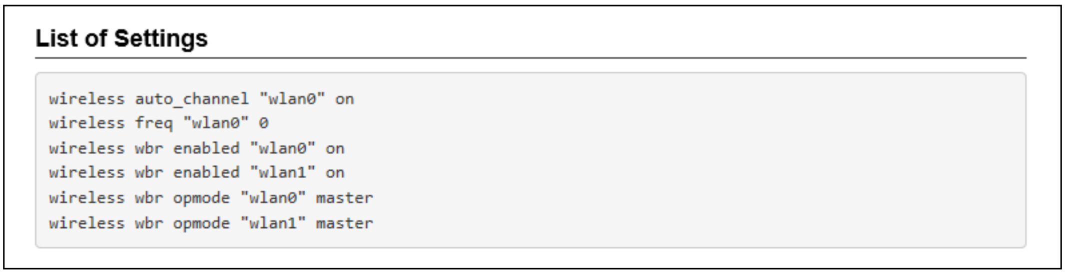
[Settings Backup/Restore] Screen

Management > Settings Backup/Restore

■ List of Settings

List of settings that have been changed from their default.

- The list will be cleared when the AP-95M is initialized.
- The screen is an example.



List of Settings

```
wireless auto_channel "wlan0" on
wireless freq "wlan0" 0
wireless wbr enabled "wlan0" on
wireless wbr enabled "wlan1" on
wireless wbr opmode "wlan0" master
wireless wbr opmode "wlan1" master
```

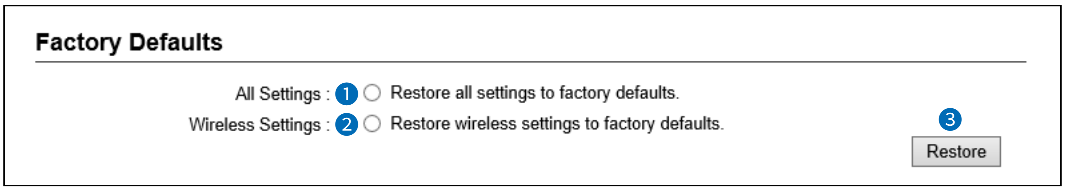
[Factory Defaults] Screen

Management > Factory Defaults

■ Factory Defaults

You can return AP-95M's settings to their factory defaults.

- If you cannot access the AP-95M’s setting screen, initialize the AP-95M.
  See the CONNECTION GUIDE leaflet for details.



Factory Defaults

All Settings : ① ○ Restore all settings to factory defaults.

Wireless Settings : ② ○ Restore wireless settings to factory defaults.

① **All Settings** .... Returns all settings to their factory defaults.
- After the AP-95M is initialized, the IP address is returned to the default (192.168.0.1), and you must configure the country (only in Europe) and Time Zone. See the supplied leaflet for details.
- If the network part of the PC IP address is different from that of the AP-95M, you cannot access the AP-95M setting screen. In such case, change the PC IP address according to your network environment,

② **Wireless Settings** .... Returns settings in the [Wireless Settings] menu to factory defaults.

③ **<Restore>** .... Returns settings according to the selected restore option.

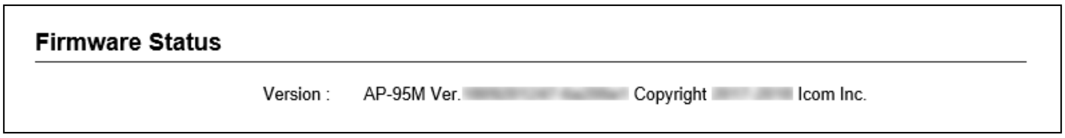
[Firmware Update] Screen

NOTE:
- Never turn OFF the AP-95M during a firmware update. This will cause the data to be lost or corrupted.
- While updating the firmware, the AP-95M is disconnected from the network.
- Firmware update may be failed, depending on the network or server condition.

Management > Firmware Update

■ Firmware Status

Displays the firmware version.



Firmware Status

Version : AP-95M Ver.[redacted] Copyright [redacted] Icom Inc.

(The screen is an example.)

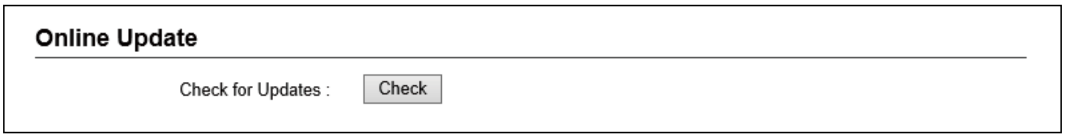
[Firmware Update] Screen

Management > Firmware Update

■ Online Update

Downloads the firmware through the internet, and automatically updates it.

- To use this function, an internet connection is necessary.

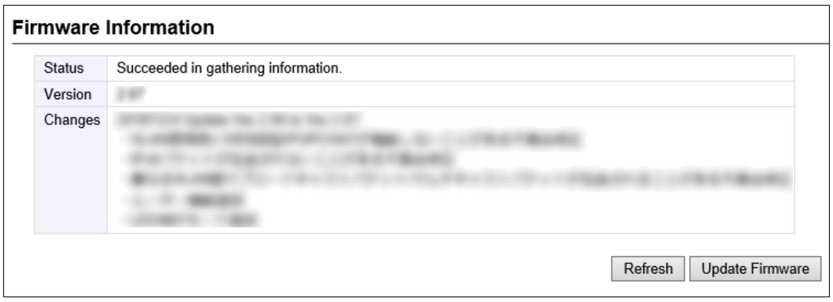


Online Update

Check for Updates :

Check for Updates .... Click <Check> to access the update management server.

When the AP-95M has successfully accessed the server, the latest firmware version is displayed as shown below.



Firmware Information

Status	Succeeded in gathering information.
Version	[illegible]
Changes	[illegible]

About the firmware information:

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

NOTE

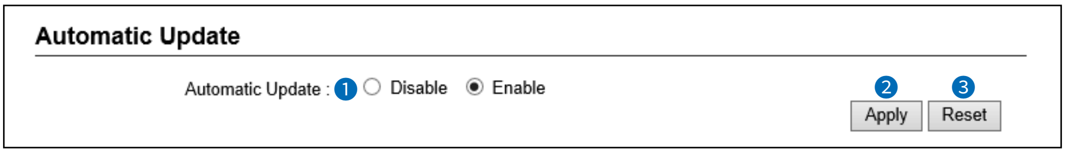
- NEVER turn OFF the power until the updating has been completed. Otherwise, the AP-95M may be damaged.
- Ask your dealer for updated function or specification details.

[Firmware Update] Screen

Management > Firmware Update

■ Automatic Update

The firmware can be automatically downloaded and updated.



Automatic Update

Automatic Update : ① ○ Disable ● Enable

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

About the new firmware indication

When [MODE] lights orange ●, a firmware update is ready. (p. 4-6)

- Firmware will not be automatically updated.
- Firmware update may be executed by the update management server, depending on the update contents.
- Select "Disable" if you don't desire to automatically update the firmware.

② **<Apply>** .... Click to apply entries.

③ **<Reset>** .... Click to restore the settings.

- You cannot restore after clicking <Apply>.

NOTE

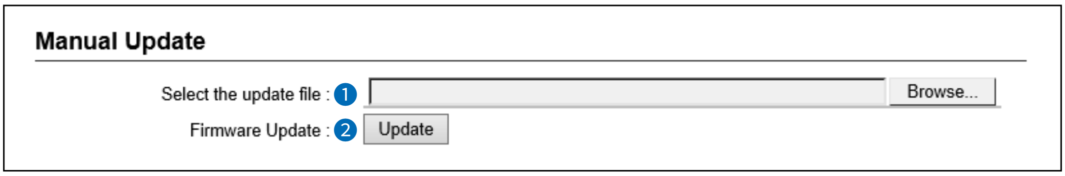
- NEVER turn OFF the power until the updating has been completed. Otherwise, the AP-95M may be damaged.
- Ask your dealer for updated function or specification details.

[Firmware Update] Screen

Management > Firmware Update

■ Manual Update

The firmware can be updated using the firmware file that is saved in a PC.



Manual Update

Select the update file : ①

Firmware Update : ②

① **Select the update 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.
• After updating, the AP-95M automatically reboots.

NOTE
• NEVER turn OFF the power until the updating has been completed. Otherwise, the AP-95M may be damaged.
• Ask your dealer for updated function or specification details.

MAINTENANCE

Section 4

1. Checking and saving the settings

Management > Settings Backup/Restore

You can check the settings changed on the setting screen, and then save them as a setting file (format: sav) on your PC.

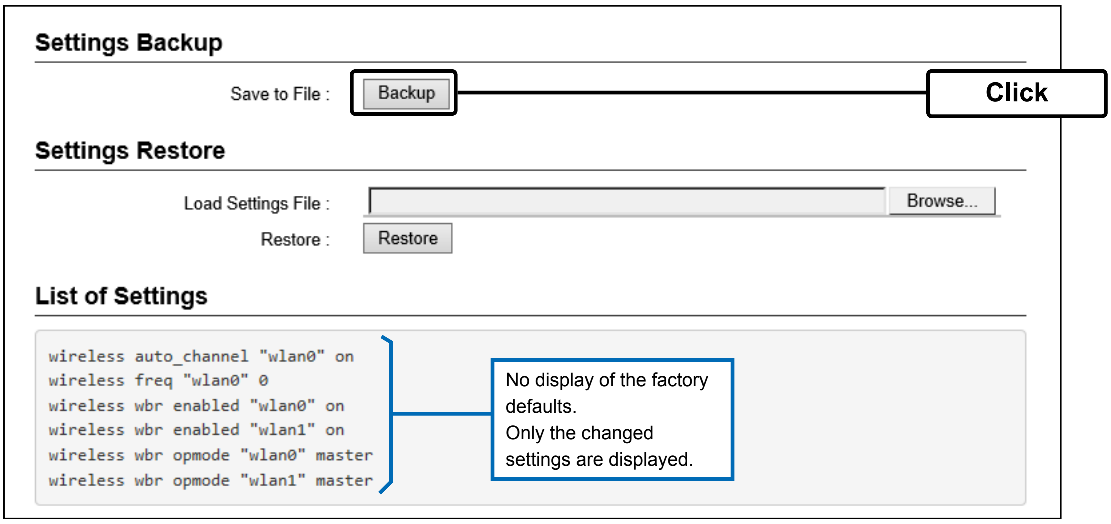
You can use the saved file as a backup if the settings are lost or damaged.

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

- The “Settings Backup/Restore” screen is displayed.

2 In the “Settings Backup” menu, click [Backup].

- The file confirmation screen is displayed.

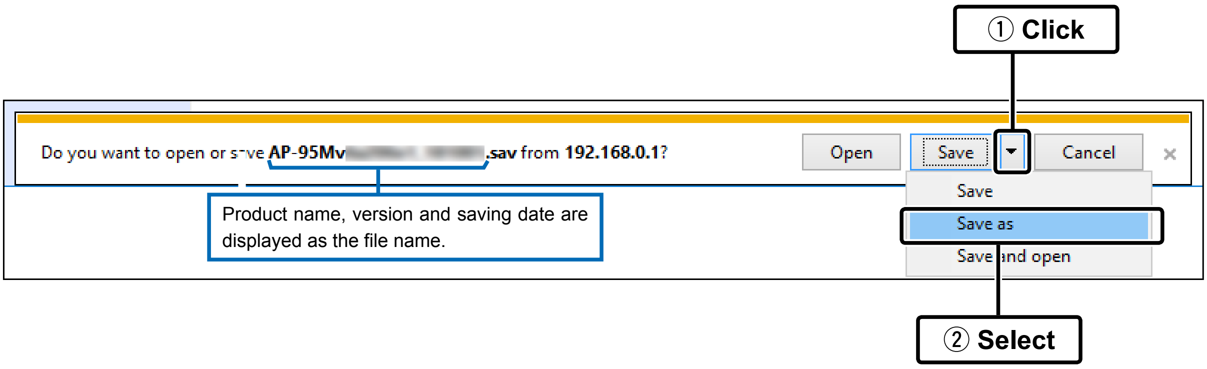


```
wireless auto_channel "wlan0" on
wireless freq "wlan0" 0
wireless wbr enabled "wlan0" on
wireless wbr enabled "wlan1" on
wireless wbr opmode "wlan0" master
wireless wbr opmode "wlan1" master
```

No display of the factory defaults.
Only the changed settings are displayed.

3 Click [▼] by the [Save] button, and then select [Save as].

- The “Save as” window appears.



Do you want to open or save **AP-95Mv**[redacted]**.sav** from **192.168.0.1**?

Product name, version and saving date are displayed as the file name.

4 Select the location to save and click [Save].

- The setting file is saved in the selected location.

2. Uploading the saved settings

Management > Settings Backup/Restore

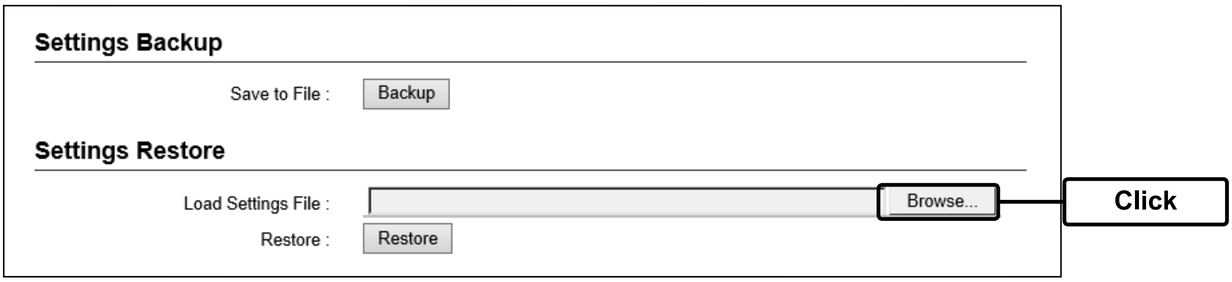
This page explains how to upload a setting file saved on your PC to the AP-95M.

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

- The “Settings Backup/Restore” screen is displayed.

2 To select the setting file, click [Browse].

- The “Choose File to Upload” window appears.



Settings Backup

Save to File : Backup

Settings Restore

Load Settings File : Browse...

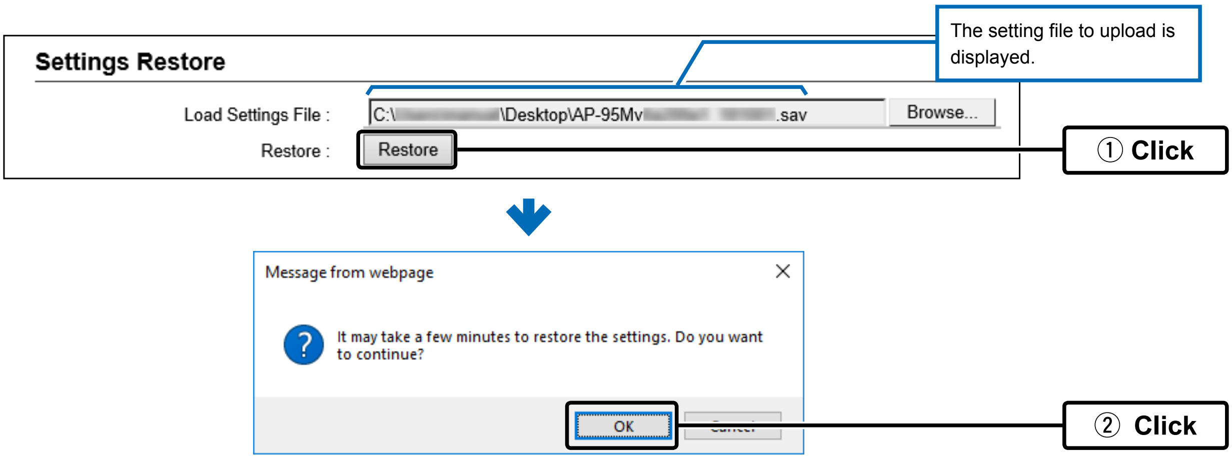
Restore : Restore

3 In the “Choose File to Upload” window, select the setting file (format: sav), and then click [Open].

- The setting file to upload will be displayed in the “Load Settings File” text box.

4 Click [Restore].

- The AP-95M restarts to restore the settings.



Settings Restore

Load Settings File : C:\[redacted]\Desktop\AP-95Mv[redacted].sav Browse...

Restore : Restore

The setting file to upload is displayed.

Message from webpage

It may take a few minutes to restore the settings. Do you want to continue?

3. Restoring the factory defaults

If you cannot access the AP-95M setting screen, you can reset the AP-95M.

- This resets all settings to the factory defaults.

Ⓐ Pushing [MODE]:

When the setting screen cannot be accessed because the IP address or the password set to the AP-95M is unknown.

Ⓑ Using the setting screen:

(See the next page.)

Ⓐ Pushing <MODE>

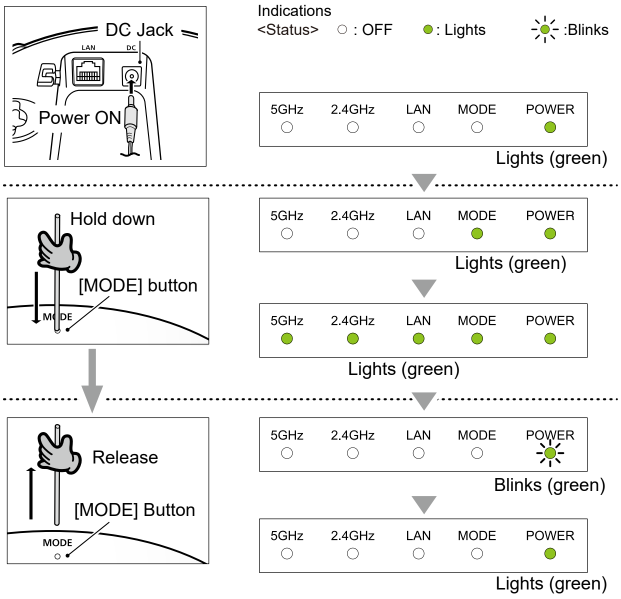
1 Disconnect all cables from the AP-95M, and then connect the power adapter.

- Confirm that the [POWER] indicator is lit in green ●.
- The other indicators status may differ, depending on the operation status.

2 Hold down [MODE] with a pin on the top panel until all indicators light green ●.

3 Confirm that all indicators are lit in green ●, and then release [MODE].

- When the initialization has been completed, the [POWER] indicator lights green ●.



NOTE:
After resetting, the AP-95M IP address is returned to “192.168.0.1(default)."
If you cannot access the AP-95M setting screen after the reset, change the PC’s IP address.

3. Restoring the factory defaults (Continued)

Management > Factory Defaults

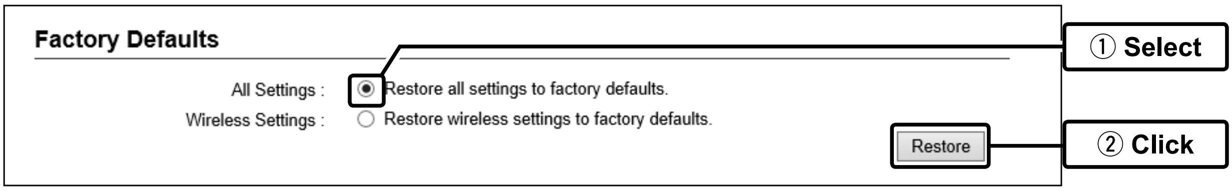
If you can access the setting screen with the IP address and the administrator’s password, you can restore all the default settings from the setting screen.
If the IP address and the password are unknown, see the previous page.

Ⓑ Using the setting screen

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

• The “Factory Defaults” screen is displayed.

2 Select the restore button, and then click [Restore]. (Default: Restore All Settings)



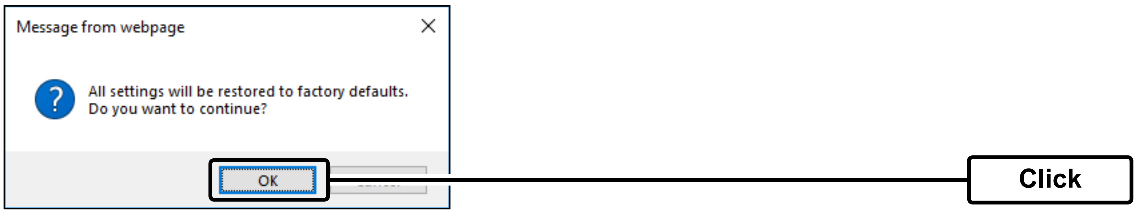
Factory Defaults

All Settings : ● Restore all settings to factory defaults.

Wireless Settings : ○ Restore wireless settings to factory defaults.

3 Click [OK].

• The AP-95M restarts to restore the default settings.



Message from webpage

All settings will be restored to factory defaults.
Do you want to continue?

4 After the restart is complete, click [Back].

NOTE: About “Factory Defaults”

• Restore All Settings

Restores all the set values to their defaults, including the IP address. (http://192.168.0.1/)
If you cannot access the AP-95M, change the PC’s IP address.

• Restore Wireless Settings

Restores only the settings set on the “Wireless Settings” screen to their default values.
After the restoring is complete, “SSID” is set to “WIRELESSLAN-0,” and “Encryption” is set to “None.”
If the SSID or security settings set by restoring the factory defaults differ from those set in the AP-95M, you will not be able to access the setting screen. In such a case, change the settings in the “Wireless Settings”menu and the wireless LAN station settings.

4. Firmware Update

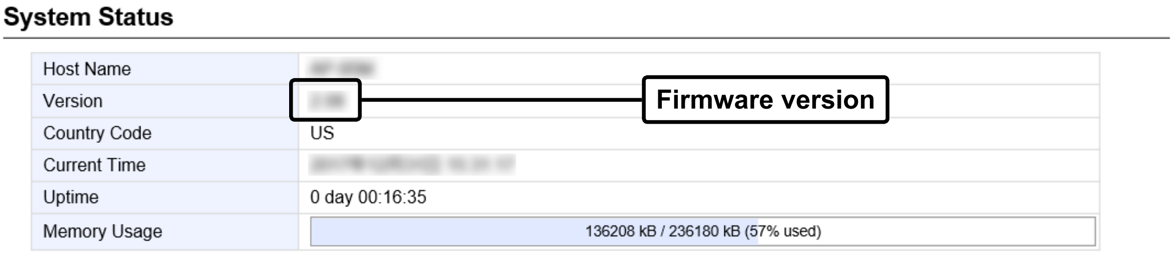
The AP-95M’s firmware can be updated on the setting screen.

Ⓐ **Manually updating the firmware:**
If you cannot update the firmware online, select the firmware downloaded from the Icom website, and then manually update.
Ⓑ **Updating the firmware online (p. 4-8):**
The firmware can be updated to the latest version using the Internet.

TOP

■ About the firmware

The firmware is a system programmed into the flash memory to enable the AP-95M to operate.
This system can be updated to a newer version in order to have more functions, or to improve the firmware.
Before updating, access the setting screen and check the firmware version information on the “TOP” screen.



System Status

Host Name	[redacted]
Version	[redacted]
Country Code	US
Current Time	[redacted]
Uptime	0 day 00:16:35
Memory Usage	136208 kB / 236180 kB (57% used)

Firmware version

■ Firmware update note

- Firmware update takes approximately 10 minutes.
  Never turn OFF the AP-95M during a firmware update.
  This will cause the data to be lost or corrupted.
- If you have a firewall security system enabled, and the firmware cannot be updated, so turn OFF the system.
- Updating the firmware is your responsibility.
  Read the following information carefully, and then access the Icom website (http://www.icom.co.jp/world/) to download the AP-95M’s firmware update file.
  Icom is not responsible on the consequences of updating the firmware.

4. Firmware Update

Management > Firmware Update

A Manually updating the firmware:

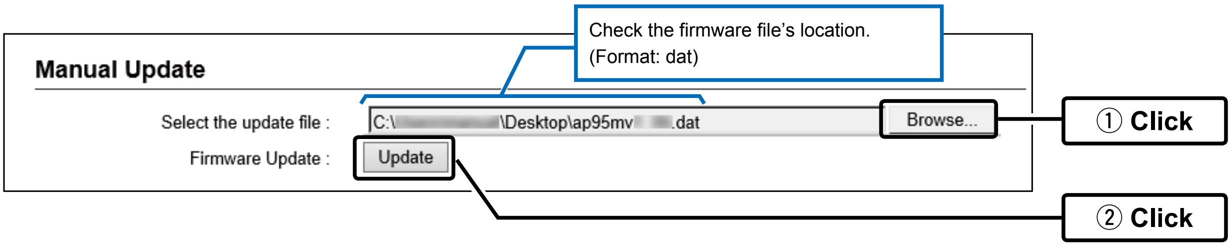
We recommend that you save all the settings before updating the firmware. (p. 4-2)

- There are firmware files that reset the defaults. Therefore, check the firmware update information on the Icom web site before downloading the firmware file.
- You can limit the setting screen access so only the administrator can update the firmware.

1 Click [Management], and then click “Firmware Update.”

- The “Firmware Update” screen is displayed.

2 Select the saving location for the firmware file that you downloaded and decompressed from the Icom web site, as shown below.



Manual Update

Select the update file : C:\[redacted]\Desktop\ap95mv[redacted].dat Browse...

Firmware Update : Update

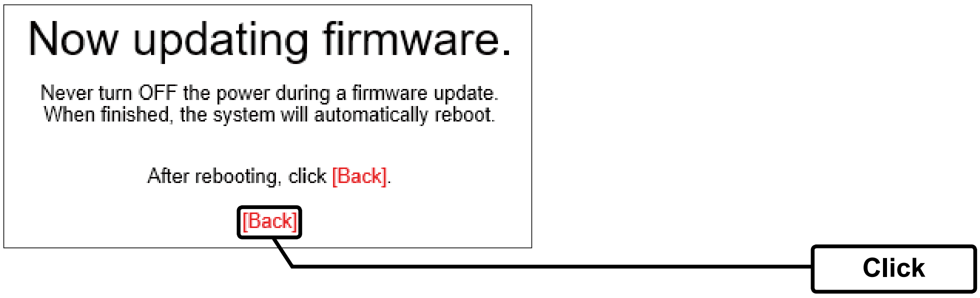
Check the firmware file’s location.
(Format: dat)

① Click

② Click

3 After the restart is complete, click [Back] to return to the setting screen.
If the setting screen does not return, the firmware is still updating. In such a case, wait a while and click again.
(Do not turn OFF the AP-95M or the PC during the update.)

- Updating the firmware takes approximately 10 minutes.



Now updating firmware.

Never turn OFF the power during a firmware update.
When finished, the system will automatically reboot.

After rebooting, click [Back].

[Back]

Click

NOTE:
After resetting, the AP-95M IP address is returned to “192.168.0.1 (default)," depending on the firmware.
If you cannot access the AP-95M setting screen after the reset, change the PC’s IP address.

4. Firmware Update

Management > Firmware Update

B Updating the firmware online

When the [POWER] indicator lights orange ●, check the firmware update as described below. The AP-95M's firmware can be updated online.

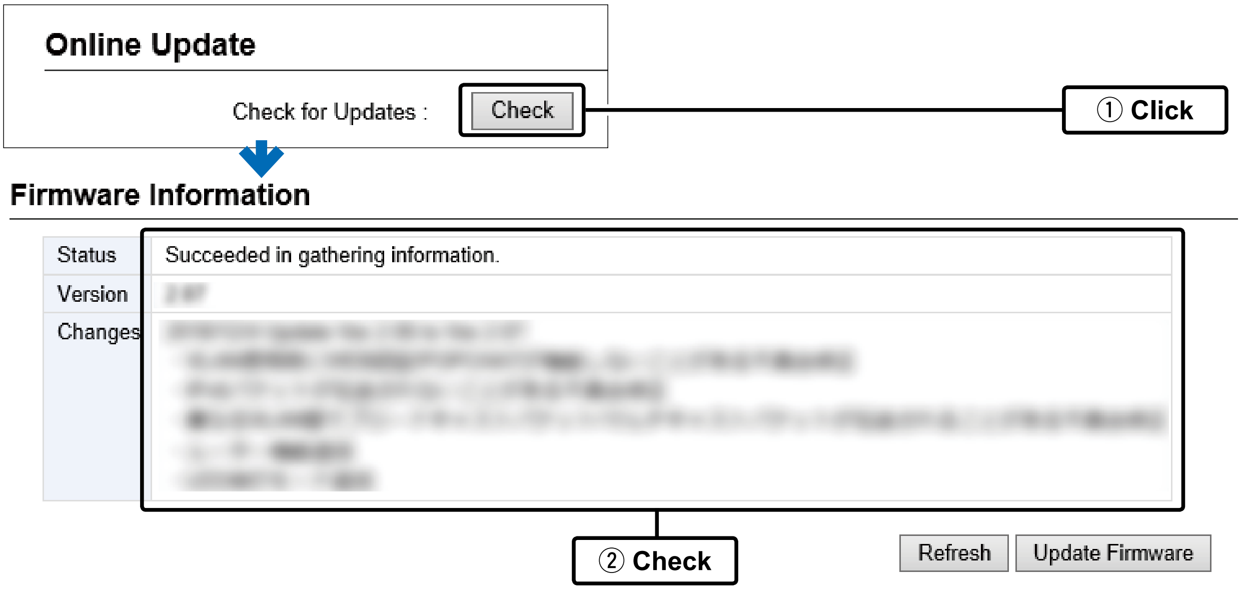
- When the "Automatic Update" item is set to "Enable," the AP-95M automatically checks for a firmware update. (p. 3-133)
- To check for a firmware update, an internet connection, DNS settings to the AP-95M, and the default gateway settings are required.
- Before updating the firmware, we recommend that you save the settings. (p. 3-133)

1 Click [Management], and then click [Firmware Update].

- The "Firmware Update" screen is displayed.

2 Check for the firmware update information by clicking [Check] for "Check for Updates."

- If "Firmware already up-to-date." is displayed and no indication lights, there is no firmware update available.



Online Update

Check for Updates : Check

① Click

Firmware Information

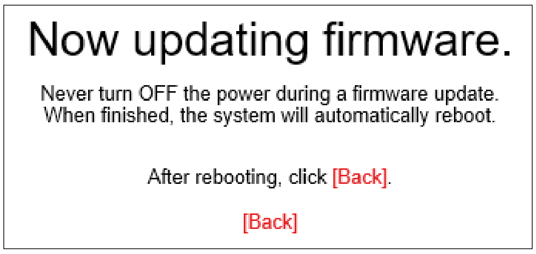
Status	Succeeded in gathering information.
Version	[illegible]
Changes	[illegible]

② Check

3 Click [Firmware Update].

- Starts to access the Icom's update management server.
- There are firmware files that reset the defaults when updated. Therefore, check the firmware update information on the setting screen before downloading the file.

4 Wait approximately 10 minutes until the update is complete.
If you connect to Icom's update management server, the AP-95M automatically restarts when the update is complete.



Now updating firmware.

Never turn OFF the power during a firmware update.
When finished, the system will automatically reboot.

After rebooting, click [Back].

[Back]

INFORMATION

Section 5

1. Troubleshooting

The following conditions are not due to a malfunction. Check before sending a request for repair.

The [POWER] indicator does not light

- The power adapter is not connected.
  - Check the adapter or DC jack connection.
- The power adapter is connected to the power outlet interlocked with a PC.
  - Connect the power adapter to a different power outlet.

The [LAN] indicator does not light

- The Ethernet cable is not properly connected to the AP-95M.
  - Make sure the Ethernet cable is securely connected.
- The Switch or PC is turned OFF.
  - Turn ON the Switch or PC.

The [2.4GHz]/[5GHz] indicator does not light green

- The PC is not working properly.
  - Refer to the instruction manual of the PC or the wireless LAN adapter.
- The wireless LAN standards do not match between the wireless LAN station and the AP-95M.
  - Check the wireless LAN station’s wireless LAN standards.
- No radio communication is made for more than 4 minutes after the last communication.
  - Access the AP-95M again, and then make sure the indicators light.
- The wireless LAN station’s communication mode is set to “Ad hoc.”
  - Set to “Infrastructure.”
- SSID is set incorrectly.
  - Check the SSID on both the AP-95M and the wireless LAN station.
- The security mode is set incorrectly.
  - Set the same authentication mode to both the AP-95M and the wireless LAN station.
- MAC address filtering is used.
  - Register the wireless LAN station’s MAC address to the AP-95M.
- The “Hide SSID” setting is enabled.
  - Disable the “Hide SSID” settings.

The [2.4GHz]/[5GHz] indicator lights green but cannot communicate

- The security settings are set incorrectly.
  - Check the security settings for both the AP-95M and wireless LAN station.

Cannot communicate with the [IEEE802.11n] or [IEEE802.11ac] standard

- The wireless LAN station does not comply with the [IEEE802.11n] or [IEEE802.11ac] standard.
  - Use a wireless LAN station that complies with the standards.
- Encryption is not set to “AES.”
  - When communicating with the [IEEE802.11n] or [IEEE802.11ac] standards, set the encryption to “AES” or disable the encryption.

The setting screen does not open properly

- The JavaScript or Cookie functions are turned OFF.
  - Turn the functions ON.
- Your Microsoft Internet Explorer version is 8 or earlier, or your browser is other than Internet Explorer.
  - Use Microsoft Internet Explorer 9 or later.

Cannot access the AP-95M’s setting screen

- The IP address is not set.
  - Set the PC’s IP address as a static IP address when accessing for the first time, or after a reset. (p.1-12)
- The wireless LAN settings for the PC and the AP-95M are different.
  - Set the same “Authentication” and “Encryption” to both the PC and the AP-95M.
- A proxy server is used for the web browser setting.
  - Set the web browser’s proxy server setting to OFF.
    Click the “Tools” in the web browser menu, and then click “Internet option.”
    Click the “Connections” tab, and click [LAN settings], and then confirm there is no check mark in “Automatically detect settings” and “Use a proxy server for your LAN (These settings will not apply to dial-up on a VPN connection).

1. Troubleshooting

The [WPS] button does not work (Wireless LAN is not automatically set)

- **WPS is set to “Disable.”**
  - The WPS interface (ath0 to ath7) is not set, or the interface number is set incorrectly.
- **The wireless station does not support WPS.**
  - Use the wireless station that supports WPS.
- **The automatic setting with other wireless LAN station is in process.**
  - Wait until the automatic setting is complete.
- **The Automatic Setting procedure was not performed within 2 minutes after the [WPS] button was pushed.**
  - Perform the Automatic Setting procedure within 2 minutes after [WPS] is pushed.
- **The automatic setting would not start after trying several times.**
  - Disable the WPS function, and then set it manually.

Cannot change the settings on the AP-95M’s setting screen

- **The “Management Tools” is enabled, and the RS-AP3 is used.**
  - Change the settings in the RS-AP3.
  - Complete the RS-AP3 settings, and then change the settings on the AP-95M.

Cannot operate the AP-95M using the RS-AP3

- **The “Management Tools” is disabled.**
  - Select “Enable” for the “Management Tools.”
- **The AP-95M’s IP address is not correctly set to the RS-AP3.**
  - Check the IP address, and correctly set it.
- **The LAN cable is not properly connected.**
  - Check the [LAN] port or the LAN cable connections.

Cannot use the wireless bridging function (WBR)

- **The client's security settings do not match the AP-95M.**
  - Check the security settings.
- **The client's SSID is does not match the Virtual AP's SSID.**
  - Check the SSID setting.
- **The peer unit’s BSSID is not correctly registered correctly for the wireless bridging function.**
  - Check the BSSID registered to the peer unit.

2. Connecting using Telnet/SSH

This topic explains how to connect using Telnet/SSH.

- Settings differ, depending on the OS or Telnet/SSH client
- Telnet is set to "Disable" as the default. (p. 3-117)
- The supported character code is UTF-8.

How to set

1. Enter as follows, and then push [Enter] to log in.

   login: admin (Fixed)

   password: admin

   - Enter the administrator's password set on the setting screen.
   - "admin" is set as the default.

2. If Telnet can access the AP-95M, "AP-95M #" is displayed on the Telnet screen.

Saving settings:

After changes have been made, enter "save" and then push [Enter] to save.

- If you quit without saving, all changes will be lost after rebooting.

Logging out

Enter "quit," "exit" or "logout" then push [Enter] to log out.

■ About the Telnet/SSH 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] -> **n**etwork
Suggested commands are displayed.
(Example) "res" + [Tab] -> **res**et or **res**tart

3. About the setting screen

The following items are displayed on the setting screen, when all items are their defaults.

Menu	Setting screen	Setting
TOP	TOP	System Status
		MAC Address
		WAN Status
Information	Network Status	Interface List
		Ethernet Port Connection Status
		Wireless LAN
		Wireless Bridging (WBR)
		DHCP Lease Status
	SYSLOG	SYSLOG
	Wireless Status	AP Status
		Station Status
		Wireless Bridging Status
Network Settings	IP Address	Host Name
		VLAN
		IP Address
	DHCP Server	DHCP Server
		Static DHCP
		List of Static DHCP Settings
	Static Routing	Routing Table
		Static Routing
		List of Static Routing Entries
	Policy Routing	Source Address Routing
		List of Source Address Routing Entries
	Packet Filter	Packet Filter Settings
		List of Packet Filter Entries
	Web Authentication — Basic	Web Authentication
		Custom Page
	Web Authentication — Advanced	Web Authentication Method
		RADIUS
Router Settings	WAN	Connection Status
		Connection Type
	NAT	NAT
		DMZ Host
		Port Forwarding
		List of Port Forwarding Entries
	IP Filter	General Settings
		IP Filter
		List of IP Filter Entries
	Simple DNS	Simple DNS Server Settings
		List of Simple DNS Server Settings

3. About the setting screen

Menu	Setting screen	Setting
Wireless Settings	Wireless 1 — Wireless LAN	Wireless LAN
	Wireless 1 — Virtual AP	Virtual AP
		Security
	Wireless 1 — MAC Address Filtering	MAC Address Filtering
		Station MAC Address List
		List of MAC Address Filtering Entries
	Wireless 1 — Network Monitoring	Network Monitoring
	Wireless 1 — Wireless Bridging (WBR)	Wireless Bridging
	Wireless 1 — WMM Advanced	WMM Advanced
		WMM Power Save
	Wireless 1 — Rate	Rate Settings
		Common Settings among Virtual APs
	Wireless 1 — ARP Caching	ARP Caching
		ARP Caching Status
	Wireless 1 — IP Advanced Radio System	Area Settings
	Wireless 2 — Wireless LAN	Wireless LAN
	Wireless 2 — Virtual AP	Virtual AP
		Security
	Wireless 2 — MAC Address Filtering	MAC Address Filtering
		Station MAC Address List
		List of MAC Address Filtering Entries
	Wireless 2 — Network Monitoring	Network Monitoring
	Wireless 2 — Wireless Bridging (WBR)	Wireless Bridging
	Wireless 2 — WMM Advanced	WMM Advanced
		WMM Power Save
	Wireless 2 — Rate	Rate Settings
		Common Settings among Virtual APs
	Wireless 2 — ARP Caching	ARP Caching
		ARP Caching Status
	Wireless 2 — IP Advanced Radio System	Area Settings
	WPS	WPS
		Starting WPS
		WPS Status

3. About the setting screen

Menu	Setting screen	Setting
Management	Administrator	Administrator Password
	Management Tools	Access Point Management Tools
		HTTP/HTTPS
		Telnet/SSH
	Date and Time	Date and Time
		Time Zone
		NTP
		SNTP Server
	SYSLOG	SYSLOG
	SNMP	SNMP
	LED	LED OFF Mode
	Network Test	Ping Test
		Traceroute Test
	Reboot	Reboot
	Settings Backup/Restore	Settings Backup
		Settings Restore
		List of Settings
	Factory Defaults	Factory Defaults
	Firmware Update	Firmware Status
		Online Update
		Automatic Update
		Manual Update

4. Feature functions

■ Wireless LAN

- [IEEE802.11ac] standard*[1]
- [IEEE802.11n] standard*[1]
- [IEEE802.11a/b/g] standard
- Security (WEP RC4, TKIP, AES)
- Authentication
  (Open System, Shared Key, IEEE802.1X, WPA, WPA2, WPA-PSK, WPA2-PSK)
- MAC Authentication (RADIUS)
- SSID (Service Set IDentifier)
- Access point
- Roaming
- Hide SSID (Rejects ANY connection)
- Virtual AP
- MAC address filtering
- Protection
- Power level adjustment
- Limit of station connection
- Wireless Bridging (WBR)
- WMM*[2] (Wi-Fi Multimedia)
- WPS*[2]
- ARP caching
- WMM power save
- Authentication server (RADIUS/Accounting)
- Network monitoring
- Automatic channel

■ Network Management

- SYSLOG
- SNMP (MIB-II)
- RS-AP3

■ Router Management

- PPPoE connection
- DHCP client
- Static IP
- DMZ
- IP masquerade
- Port forwarding
- DHCP server
- Static DHCP server
- Static routing
- Policy routing
- IP filter
- DNS proxy

■ Other features

- VLAN Tagging function
- Packet filter
- Limit of administrators
  (Administrator ID/Password)
- Built-in clock settings
- Web authentication (RADIUS/Local List)
- PoE
- Firmware updates
- Browser maintenance (HTTP/HTTPS)
- Telnet maintenance (Telnet/SSH)

*[1] The [IEEE802.11ac] and [IEEE802.11n] standards can be used when “None” or “AES” are selected for the “Encryption” setting.

*[2] This device is not certified by the Wi-Fi alliance. (As of Jan. 2019)

5. About the characters

The usable character strings differ, depending on the setting item.

- To display the setting item by using the online help, place the cursor on the item, and then when the "?" icon is displayed, click on it.

■ Network Settings

Setting screen	Setting	Setting item	Character strings	Number of characters
IP Address	Host Name	Host Name	Characters and symbols	31 (maximum)
DHCP Server	DHCP Server	Domain Name	Characters and symbols	253 (maximum)
Web Authentication (Advanced)	Local List	Username	ASCII	128 (maximum)
		Password	ASCII	128 (maximum)

■ Wireless Settings

Setting screen	Setting	Setting item	Character strings	Number of characters
Virtual AP	Security	WEP Key	ASCII/Hexadecimal	See page 2-4
		PSK (Pre-Shared Key)	ASCII/Hexadecimal	See page 2-3
Wireless Bridging (WBR)	Client Settings	WEP Key	ASCII/Hexadecimal	See page 2-4
		PSK (Pre-Shared Key)	ASCII/Hexadecimal	See page 2-3

■ Management

Setting screen	Setting	Setting item	Character strings	Number of characters
Administrator	Administrator Password	Password	Characters and symbols	31 (Maximum)
SNMP	SNMP	Community Name (GET)	Characters and symbols	31 (Maximum)
Network Test	Ping Test	Host	Characters and symbols	64 (Maximum)
	Traceroute Test	Node	Characters and symbols	64 (Maximum)

- There are symbols that you cannot use, depending on the setting item.

6. Specofications

■ General

Power supply:	12 V DC ±10% (2 A) [Polarity ⊖–●–⊕] (The PoE specification is in accordance with IEEE802.3af.)
Usable condition:	Temperature –10 ~ +55˚C, +14 ~ +131˚F Humidity 5–95% (At no condensation)
Dimension:	Approximately 162 (W) x 42 (H) x 162 (D) mm, 6.4 (W) x 1.7 (H) x 6.4 (D) inch (Projections not included)
Weight:	Approximately 520 g, 1.1 Ib (Accessories not included)
Regularity Compliance:	FCC (Part 15 Class B/Part 68) Canada RSS-210
Interface:	Indicators (5GHz, 2.4GHz, LAN, MODE and POWER) Button (MODE)

■ Cable LAN

Communication rate:	10/100/1000 Mbps (Automatic switching/Full duplex)
Interface:	[LAN] port (RJ-45 type) x1 (Auto MDI/MDI-X) Based on: IEEE802.3/10BASE-T IEEE802.3u/100BASE-TX IEEE802.3ab/1000BASE-T IEEE802.3af

■ Wireless LAN

International standard:	Based on: IEEE802.11ac IEEE802.11n IEEE802.11a IEEE802.11b/g
Frequency:	5180 ~ 5825 MHz 2412 ~ 2472 MHz (May differ depending on the country of use.)

All specifications are subject to change without notice or obligation.

Count on us!

A7493-3EX

© 2019 Icom Inc.

Icom Inc.
1-1-32 Kamiminami, Hirano-ku, Osaka 547-0003, Japan