Cat. No. N153-E1-03

生産終了
DISCONTINUED

WE70-AP/CL

FA Wireless LAN Unit

OPERATION MANUAL

OMRON

Warning

(1) For PC and peripheral devices, follow instructions of its respective manual.

(2) Copyright of this manual and intellectual property of Omron's hardware and software belong to Omron Corporation.

(3) Reproduction of this document or parts of this document is not permissible unless our explicit consent.

(4) Content of this manual is subject to change without notice.

(5) If you have any questions or problems in this document, contact our branch or sales office listed at the end of this document.

Notice on Registered Trademark

Microsoft Windows is a registered trademark of Microsoft Corporation in the U.S. and other countries.
Microsoft Corporation has permitted screens in this document.
Atheros, Atheros logo, Total 802.11, Super AG, Atheros XR logo are trademarks of Atheros Communications, Inc.
Companies and products mentioned herein may be the trademarks of their respective owners.

About this Manual

This manual describes a wireless unit set conformance to IEEE802.11a and IEEE802.11b/g* wireless LAN.
Please read this manual carefully and be sure you understand the information provided before attempting to operate this product.

* IEEE802.11g is compatible with IEEE802.11b.

The Radio Law prohibits outdoor use of wireless LAN in IEEE802.11a standard (5GHz band).

Caution for the Radio Law on Wireless LAN

- The Radio Law prohibits outdoor use of wireless LAN in IEEE802.11a standard (5GHz band).
- Do not use it close to a person with a cardiac pacemaker.
  Electromagnetic interference may affect it, putting his/her life at risk.
- Do not use it close to medical equipment.
  Electromagnetic interference may affect the cardiac pacemaker to cause loss of human life.
- Do not use it close to an electric oven.
  Electromagnetic interference may affect the medical equipment to cause loss of human life.
- Radio device in this product has been certified by the Radio Law. Do not disassemble or modify this product.

Caution for Radio Interference with 2.4GHz Wireless LAN

Take the following precautions for communication by 2.4GHz (IEEE802.11b/g) wireless LAN.
Within this product's frequency range, industrial, scientific, and medical equipment, such as electric oven, as well as RFID premises radio stations (license required) and specified low power radio station and ham radio station (license not required) used in factory manufacturing lines are operated.

❍ Before using this device, confirm that no RFID premises radio station, specified low power radio station, or ham radio station is operating close to it.

❍ If this product caused radio interference with an RFID premises radio station, immediately change the product's frequency or stop radio emission, and contact OMRON representative for actions to take to prevent cross talk.

Wireless LAN Standards Supported by This Product

This product supports the following wireless LAN standards:

- IEEE802.11a :Up to 54Mbps (5GHz band)
- IEEE802.11g :Up to 54Mbps (2.4GHz band)
- IEEE802.11b :Up to 11Mbps (2.4GHz band)

* IEEE802.11g is compatible with IEEE802.11b.

Overview of This Product

- Accessory antenna of this product uses an external diversity type supporting 5GHz and 2.4GHz bands.
- This product provides DFS function that can automatically avoid radio interference by weather radar or others while using IEEE802.11a.

  * For more information on the DFS function, see "3-3 Configuring IP Address/SSID/Channel", "DFS Function" (P.3-11).
- In addition to WEP RC4 and OCB AES encryption, TKIP, AES, and WOC KEY are supported.
- AP-to-AP bridging allows wireless connection between APs (access points).
- Spanning tree function can prevent problems related to network groups.
- This product supports 10BASE-T and 100BASE-TX wired LAN types are supported (automatic switching).
- Major setup of this product can be performed through a WWW browser.
- This product received Technical Standard Conformity Certification and does not require radio station license.
- AP-to-AP bridging is not available at the channel where DFS function is provided.

Notations

This document uses the following notation conventions:

" " :A name of a window of the operating system (OS), a setup screen menu item, or a setup screen under a menu item is represented by " ".

[ ] :A name of a tab, icon, text box, check box, or setup item in a setup screen is represented by [ ].

< > : A name of a command button in a dialog box is represented by < >.

* Microsoft® Windows® Vista is indicated as Windows Vista.

  Microsoft® Windows® XP Professional and Microsoft® Windows® XP Home Edition are indicated as Windows XP.

  Microsoft® Windows® 2000 Professional is indicated as Windows 2000.

* Setup screen shown in this document may be different from those of your PC depending on your OS version and preferences.

Warranty and Limitations of Liability

1. WARRANTY

WARRANTY

OMRON's exclusive warranty is that the products are free from defects in Documents and workmanship for a period of one year (or other period if specified) from date of sale by OMRON.

OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, REGARDING NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR PARTICULAR PURPOSE OF THE PRODUCTS. ANY BUYER OR USER ACKNOWLEDGES THAT THE BUYER OR USER ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE. OMRON DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

2. LIMITATIONS OF LIABILITY

LIMITATIONS OF LIABILITY

OMRON SHALL NOT BE RESPONSIBLE FOR SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR COMMERCIAL LOSS IN ANY WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED ON CONTRACT, WARRANTY, NEGLIGENCE, OR STRICT LIABILITY.

In no event shall responsibility of OMRON for any act exceed the individual price of the product on which liability is asserted.

IN NO EVENT SHALL OMRON BE RESPONSIBLE FOR WARRANTY, REPAIR, OR OTHER CLAIMS REGARDING THE PRODUCTS UNLESS OMRON'S ANALYSIS COMFIRMS THAT THE PRODUCTS WERE PROPERLY HANDLED, STORED, INSTALLED, AND MAINTAINED AND NOT SUBJECT TO CONTAMINATION , ABUSE, MISUSE, OR INAPPROPRIATE MODIFICATION OR REPAIR.

3. Application Considerations

SUITABILITY FOR USE

OMRON shall not be responsible for conformity with any standards, codes, or regulations that apply to the combination of products in the customer's application or use of the product.

At the customer's request, OMRON will provide applicable third party certification documents identifying ratings and limitations of use that apply to the products. This information by itself is not sufficient for a complete determination of the suitability of the products in combination with the end product, machine, system, or other application or use.

The following are some examples of applications for which particular attention must be given. This is not intended to be an exhaustive list of all possible uses of the products, nor is it intended to imply that the uses listed may be suitable for the products:

- Outdoor use, uses involving potential chemical contamination or electrical interference, or conditions or uses not described in this document.

- Nuclear energy control systems, combustion systems, railroad systems, aviation systems, medical equipment, amusement machines, vehicles, safety equipment and installations subject to separate industry or government regulations.

• Systems, machines, and equipment that could present a risk to life or property.

Please know and observe all prohibitions of use applicable to the products.

NEVER USE THE PRODUCTS FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCT IS PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

4. Disclaimers

CHANGE IN SPECIFICATIONS

Product specifications and accessories may be changed at any time based on improvements and other reasons.

It is our practice to change model numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the product may be changed without any notice. When in doubt, special model numbers may be assigned to fix or establish key specifications for your application on your request. Please consult with your OMRON representative at any time to confirm actual specifications of purchased product.

Do not use IEEE802.11 outdoors.

The Radio Law in Japan prohibits outdoor use of IEEE802.11a (5.2GHz/5.3GHz band).
Within this product's frequency range, industrial, scientific, and medical equipment as well as RFID premises radio station (license required) and specified low power radio station (license not required) used in factory manufacturing lines are operated.

(1) Before using this device, confirm that no RFID premises radio station or specified low power radio station is operating close to it.

(2) If in case this product causes radio interference with an RFID premises radio station, immediately change the product's frequency or stop radio emission, and contact OMRON representative for actions to take to prevent cross talk (e.g. installation of a partition)

(3) If any other problem occurred due to this product, such as radio interference with an RFID specified low power radio station, contact OMRON representative.

Approved Standards
Conforming Wireless Standards:
Japan: ARIB STD-T66,T71
USA: FCC part 15.247,401-407
Canada: IC RSS-Gen RSS-210
Chinese domestic wireless standard [2002]353,[2002]227
Europe: EN 300 328,EN 301 893
Conforming Safety Standards:
cUL 60950-1(Listing)
EN 60950-1
Conforming EMC Standards: EN 301 489-1,EN 301 489-17
Conforming EMF Standards: EN 50371

* The WE70-AP does not comply with FCC/IC rules when it is connected with the WE70-CA5M Extension Cable. Do not use the WE70-CA5M with WE70-AP in the United States and Canada. (The WE70-CA5M can be used with the WE70-CL.)

Applicable Countries
This product has been approved for wireless standards in the countries listed below. This product cannot be used in any other countries.

WE70-AP/CL-US(United States), WE70-AP/CL-EU(Austria, Denmark, Finland, Germany, United Kingdom, Ireland, Italy, Netherlands, Norway, Sweden, Switzerland, Spain, France, Belgium, Greece, Portugal, Czech, Hungary, Poland, Slovenia, Slovakia), WE70-AP/CL-CA(Canada), WE70-AP/CL-CN(China), WE70-AP/CL(Japan)

Conformance to EN Standards
Use a DC power line less than 3 m to conform to EN standards. If a power line of 3 m or longer is required, extend the length at the Switching Power Supply's primary side (i.e., the AC power line).

Conformance to UL Standards
Always use a Listing Class 2 power supply to conform to UL standards.

Using 5.8GHz in China
Gain approval from the wireless management body of a local province, autonomous region or city under the direct jurisdiction for installing and using frequency of 5.8GHz in China.
Related body: Ministry of Information Industry (http://www.mii.gov.cn/)

We, the manufacturer (name of the manufacturer) hereby declare that this equipment (type of the equipment), model WE70-AP-EU/WE70-CL-EU is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

FCC/IC WARNING
Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
In addition, users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.
NOTICE
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules and RSS-Gen of IC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
• Reorient or relocate the receiving antenna
• Increase the separation between the equipment and receiver.
• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
• Consult the dealer or an experienced radio/TV technician for help.

STP cables must be used for connection to host computer and/or peripherals in order to meet FCC and IC emission limits.
In according with 47 CFR Part15.407(e) U-NII devices operating in 5.15-5.25GHz frequency bands are restricted to indoor operations only.
This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.
This equipment complies with FCC and IC radiation exposure limits set forth for uncontrolledequipment and meets the FCC and IC radio frequency (RF) Exposure Guidelines in Supplement C to OET65. This equipment should be installed and operated with at least 20cm and more between the radiator and person's body (excluding extremities: hands, wrists, feet and legs).
This device has been designed to operate with an antenna having a maximum gain of 7 dBi (5 GHz)/ 4.5 dBi (2.4 GHz). Antenna having a higher gain is strictly prohibited per regulations of Industry Canada.
The Required antenna impedance is 50 ohms.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

Safety Precautions

■ Indication for Safe Use

This document uses the following indication and symbols in precautions for safe use of WE70-AP/CL.
Precautions here specifies very important things related to safety and must be complied.
Indication and symbols include:

Warning Indication

⚠ **Warning**	Indicates a potentially hazardous situation which, if not avoided, will result in minor or moderate injury, or may result in serious injury or death. Additionally there may be significant property damage.
⚠ **Caution**	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury or in property damage.

■ Meanings of Alert Symbols

Symbol		Meaning
Precautions		• **General precaution** Indicates unspecified general precaution, warning, and hazard.
Prohibition		• **General prohibition** Indicates unspecified general prohibition.
		• **Do Not Disassemble** Indicates that disassembly of equipment may cause an electrical shock or injuries.
Mandatory		• **General mandatory indication** Indicates unspecified general mandatory operation.

■ **Warning Indication**

⚠ Warning	
DO NOT use this product without a protection circuit. Otherwise it may result in heavy injuries or damage on property due to malfunction. Dual or triple safety protection circuits, such as emergency stop, interlock, or limit circuit, must be configured by external control circuit so that the system should operate on safe side even if a failure of this product or an error due to an external factor occurred.	
This product uses electric wave for communication which may be broken up temporarily due to its environment or usage.Safety of the system must be maintained even in such a case.	
Do not use this product for a real-time control application.	
DO NOT use this product close to any medical equipment such as a cardiac pacemaker as it may affect operation of such medical equipment and may result in heavy injuries.	

⚠ Caution	
In rare cases, light electric shock, fire, or failure of this product may occur.Do not disassemble, modify, fix, or touch inside of this product. Disassembly and modification are prohibited by the Radio Law in each country.	

Precautions for Safe Use

Observe the following precautions when using this product.

1) Dedicated packaging must be used for transportation of this product. Take precautions to prevent excessive vibration or shock on the product or falling of the product.
2) Storage of this product must be within the specified environment. Allow the product to warm up to room temperature for at least 3 hours after it has been stored at -10 °C or lower.
3) Use the product within the specified temperature and humidity ranges.
4) Do not use the product under the following environments:
   - Locations subject to extreme temperature changes resulting in condensation
   - Locations subject to static electricity, excessive noise, or electric fields
   - Locations where the product may come into contact with water, oil, or chemicals
   - Locations where corrosive gases or flammable gases are present
   - Locations where large amounts of dust or dirt are present
   - Locations subject to spatters, iron chips, or fillings
5) Do not use it outdoors (outside a control panel).
6) Use tape, cord, or other means to hold the product while adjusting the installation position to prevent the product from damage due to failing.
7) Tighten the mounting screws to the specified torque of 4.4 to 5.3 in lb. (0.5 to 0.6 N·m)
8) Provide sufficient space around the product for heat dissipation. Install the products with a margin of 20mm or longer externally.
9) Do not reverse the power supply connection or connect the product to an AC power supply.
10) Use the correct power supply voltage.
11) Use the solid wire, 22 to 16 AWG for power supply. The exposed length of wire is 10 to 11mm(UL Listing).
12) Do not lay communications cables and antenna cables near other high-voltage cables or power lines.
13) Setup is required after the installation or replacement of this product. Set up the product correctly according to the manual, and be sure to confirm that communication is established before using it.
14) Do not apply excess vibrations or shock to this product. Do not drop this product.
15) Other wireless devices operating within the same frequency band may interfere with this product or be adversely affected by this product. Therefore, be sure to perform the test provided with the product (e.g., installation tests) before operating it.
16) Make sure that the antenna is not disconnected during operation.
17) Do not use this product near other devices that may malfunction due to the electromagnetic waves emitted by this product.
18) Turn OFF the power supply before performing any wiring or replacing devices.
19) Do not touch the product with wet hands.
20) Dispose of the product as industrial waste.

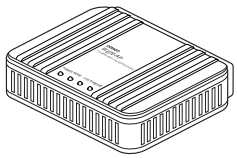
Precautions for Correct Use

Always heed these precautions to prevent faulty operation, malfunction, or adverse affect on the product's performance and functionality.

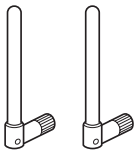
1) Communication performance may be affected by its environment. Always confirm its operation before using it.
2) Do not install its antenna where it is surrounded by metal, such as in a control panel.
3) Install the antenna so that it is as far away as possible from and not parallel to electric wires or metal plates.
4) Do not use this product in areas exposed to extremely high humidity, near televisions or radios, near motors or drills that emit sparks, near strong magnets, or near fluorescent lights.
5) Do not pull or bend cables with force.

Contents

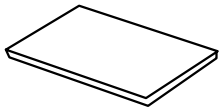
This product package includes the followings. (WE70-AP/CL-US/-EU/-CN)
Check if all of them are included in the package before using this product.



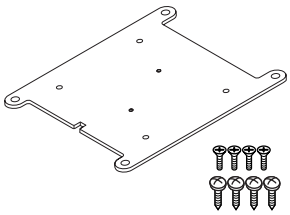
WE70-AP/WE70-CL



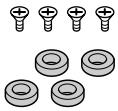
Antenna x 2



Instruction Sheet x 3



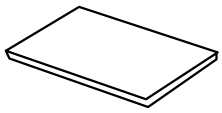
Mounting Bracket
(with 4 flat-head screws)
(with 4 tapping screws)



Magnet x 4
(with 4 flat-head screws)

Antenna Connector
Cover x 2

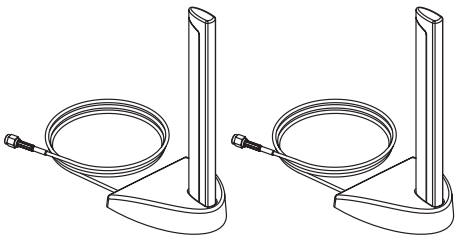
IP Address Label



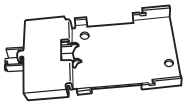
EC Declaration of Conformity

Options

(As of December 2006)



1 set with 2 antennas
High-sensitivity Magnetic-base Antenna
Common for 2.4GHz and 5GHz bands
(WE70-AT001H)



DIN Rail Adapter
(WT30-FT001, 002)
1 set with 2 antennas
Antenna Extention Cable (5M)
common for 2.4GHz and 5GHz bands
(WE70-CA5M)

* The WE70-AP does not comply with FCC/IC rules when it is connected with the WE70-CA5M Extension Cable. Do not use the WE70-CA5M with WE70-AP in the United States and Canada. (The WE70-CA5M can be used with the WE70-CL.)

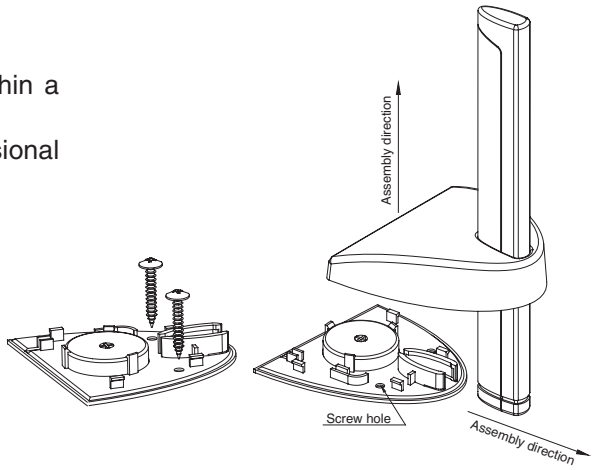
<High-sensitivity Magnetic-base Antenna>

WE70-AT001H is a non-directional antenna for 2.4/5GHz.

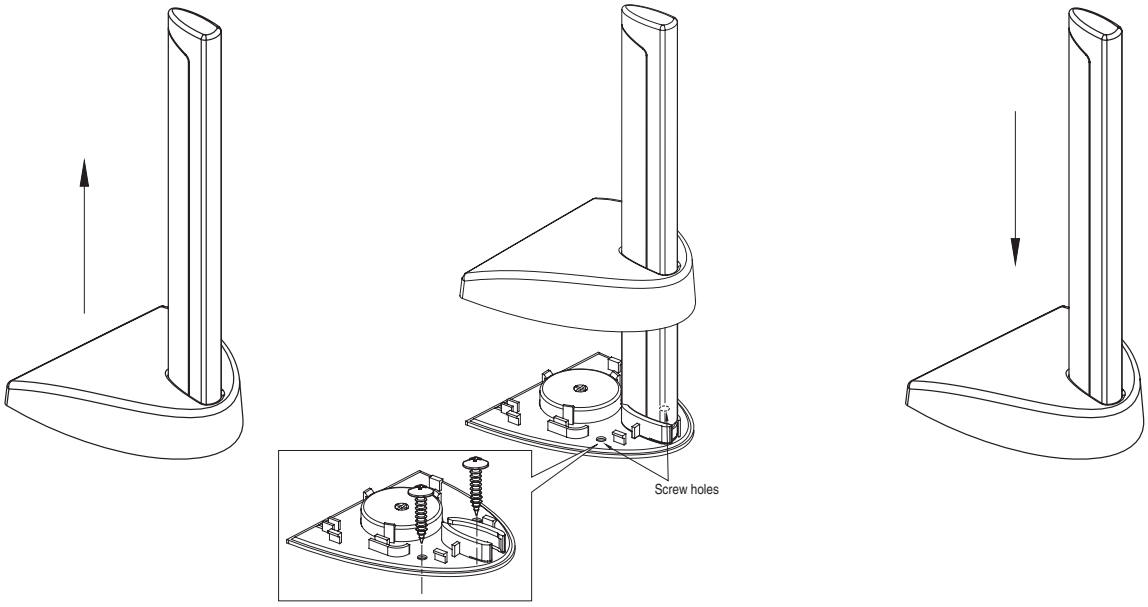
It can be installed where radio wave status is good, within a range of a given coaxial cable length (about 2m).

* Refer to page Appendices-10?? for the outline dimensional drawing.

Assembly drawing



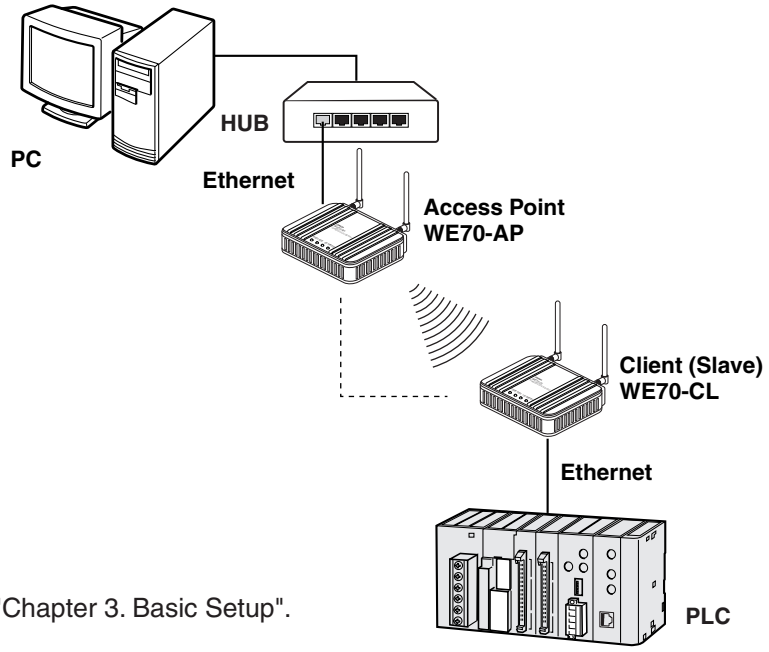
1. Hold the pole tightly and remove the cover from the main body.
2. Use screws to attach the main body to the installation location. (The pole can be removed from the body.)
3. Replace the cover, pressing down until it clicks into place.



Application Guide

Basic Function

Constructs a network through radio communication.



See P.3-1 Refer to "Chapter 3. Basic Setup".

Installation

See P.2-1 Refer to "Chapter 2. Installation & Connection".

Enhancing Security

See P.3-12 Refer to "Chapter 3-4. Configuring Encryption".

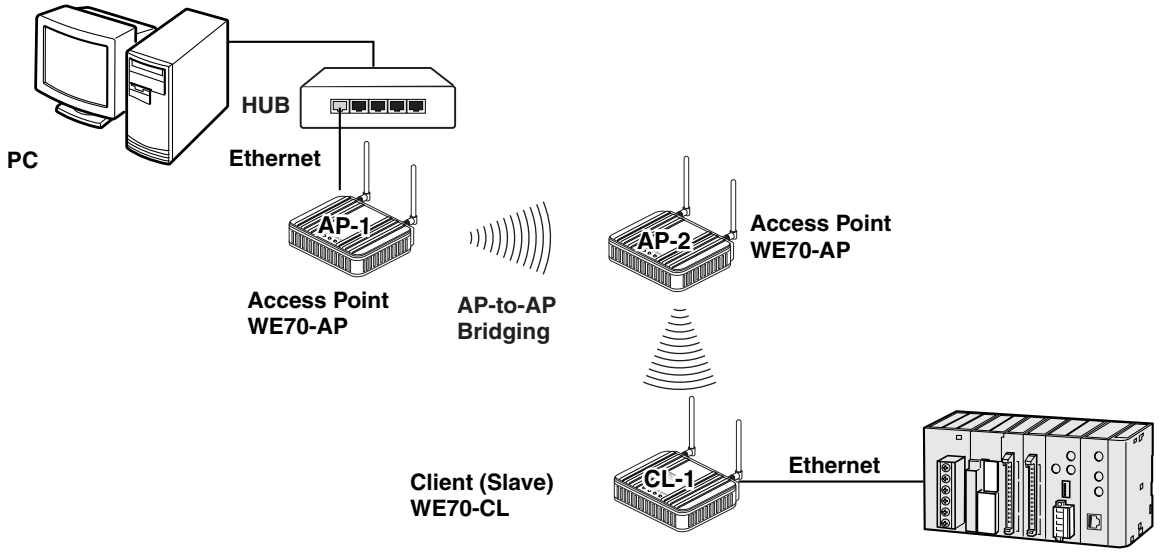
Replacing Wireless Unit

See P.6-2 Refer to "Chapter 6-1. Replacing Wireless Unit".

AP-to-AP Bridging (Relay function)

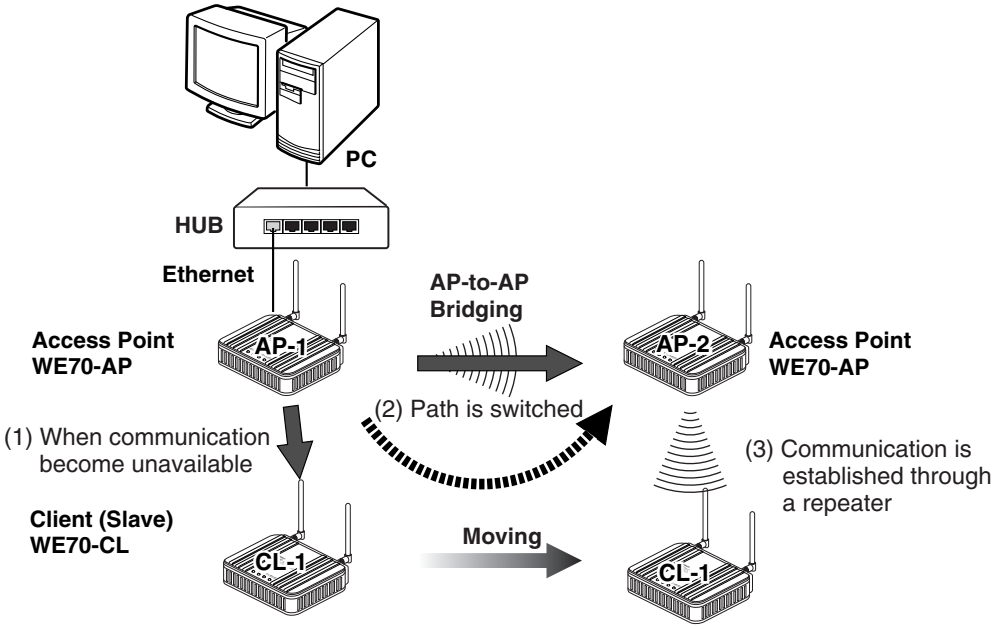
Pattern A

An access point is used as a repeater for communication with a client (slave).
Under this system configuration, a client (CL-1) as a fixed station communicates with an access point (AP-2).



Pattern B

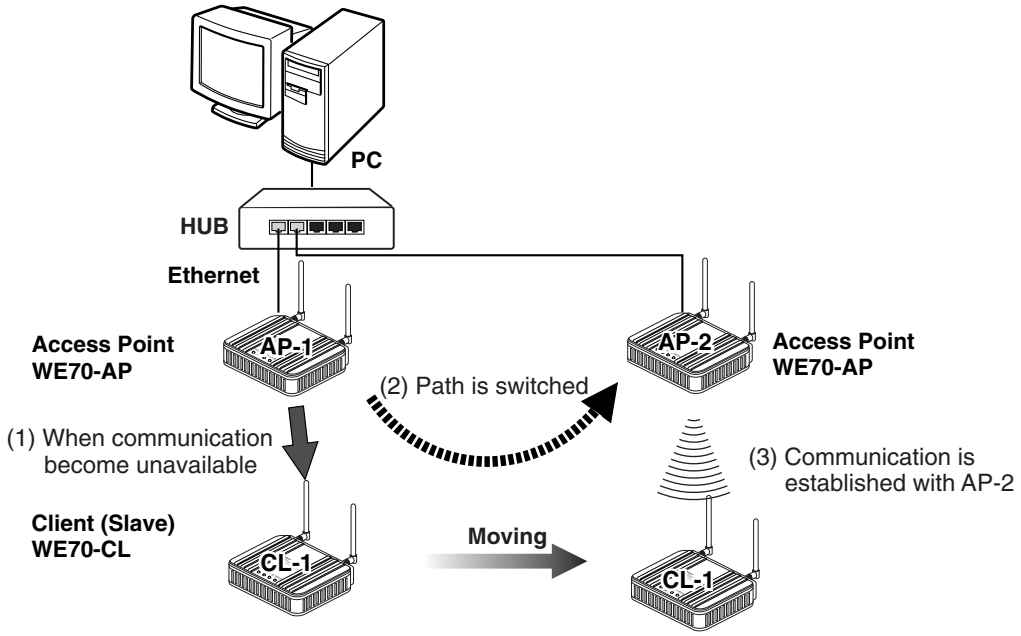
An access point is used as a repeater for communication with a moving client (slave).
A client (CL-1) moves between AP-1 and AP-2, switching communication paths.



See P.4-2 Refer to "Chapter 4-1. To Use AP-to-AP Bridging".

Roaming for Wired Connection

AP-1 and AP-2 are wired through HUB to communicate with a moving client (slave).
A client (CL-1) moves between AP-1 and AP-2, switching communication paths.



See P.4-22 Refer to "Chapter 4-9. Smart Roaming".

Manual Configuration

Chapter 1	Overview	Describes main features of this product.	1
Chapter 2	Installation & Connection	Describes cautions for wireless unit installation and how to connect the unit set.	2
Chapter 3	Basic Setup	Describes how to establish communication between an access point and a client (slave) as well as a PLC using PC.	3
Chapter 4	Advanced Setup	Describes setup for communication between access points and communication between clients through an access point,as well as setup for stable communication.	4
Chapter 5	Setup Menu	Describes setup screens available for functions of this wireless unit set.	5
Chapter 6	Replacement Procedure	Describes how to save or initialize setup data for wireless unit replacement.Read this chapter when necessary.	6
Appendices		Describes major troubleshooting, setup screen configuration, and initial setup values.	

Table of Contents

About this manual 1
Warranty and Limitations of Liability 5
Safety Precautions 8
Precautions for safe use 10
Precautions for Correct Use 11
Contents 11
Options 12
Application Guide 13
Manual Configuration 15

Chapter 1 Overview

1-1. Features 1-2
- ■ Major Features 1-2
- ■ System Configuration 1-7
- ■ Relay Function 1-9

1-2. Components and Functions 1-10
- ■ Top View 1-10
- ■ Rear View 1-11

Chapter 2 Installation & Connection

2-1. Installation 2-2
- ■ Installation Location 2-2
- ■ Installation Precautions 2-2
- ■ Precautions for Antenna Installation Location 2-3
- ■ Dimensions 2-5
- ■ Installation Method 2-5

2-2. Connection 2-7
- ■ Notice for Wiring 2-7
- ■ Main Unit Power Wiring 2-7
- ■ LAN Cabling 2-8

2-3. Connection Check 2-10
- ■ Checking Setup Screen Access 2-10

Chapter 3 Basic Setup

3-1. Setup Workflow 3-2

3-2. Opening Setup Screen 3-3
- Step 1. PC (Wired LAN) Setup 3-3
- Step 2. Connecting 3-3
- Step 3. Checking Setup Screen Access 3-4
- Step 4. Monitoring Wireless Communication Status 3-6

3-3. Configuring IP Address/SSID/Channel 3-7
- Step 1. IP Address Setup 3-7
- Step 2. Configuring Wireless Network Name (SSID) 3-8
- Step 3. Configuring Channel 3-9
- Step 4. Checking Communication 3-11
- Step 5. Other Setups 3-11

3-4. Configuring Encryption 3-12
- ■ To Enter Encryption Key Using ASCII Characters 3-12
- ■ Entering Encryption Key 3-13
- ■ Setup Example of Encryption Key 3-14
- ■ To Enter Encryption Key Using hexadecimal number 3-15

■ Conversion Table from ASCII Character to hexadecimal number 3-16
■ To Generate Encryption Key Using Key Generator 3-17
■ To Configure TKIP/AES/WOC KEY Encryption 3-18
3-5. Communicating with PLC 3-20
Step 1. Preparing PLC & PC 3-20
Step 2. MAC Address Setup.....3-21
Step 3. PLC Setup 3-21
Step 4. Checking Communication with PLC 3-22
■Precautions for Communication with PLC.....3-22

Chapter 4 Advanced Setup

4-1. To Use AP-to-AP Bridging 4-2
■ Communication with 2 or More Access Points.....4-2
■ To Register BSSID.....4-4
4-2. AP-to-AP Bridging Setup 4-5
Step 1. Configuring IP Address 4-5
Step 2. Checking Own & Partner SSIDs.....4-6
Step 3. Checking Wireless Channel 4-6
Step 4. Checking Own & Partner BSSIDs 4-6
Step 5. Checking Partner BSSID.....4-7
Step 6. Checking Receiving electric field strength.....4-8
Step 7. Checking AP-to-AP Bridging 4-9
4-3. Configuring Relay Function (Pattern A) 4-10
Step 1. Changing Access Point SSID.....4-11
Step 2. Configuring Client IP Address 4-11
Step 3. Checking Communication 4-12
Step 4. Configuring Client-PLC Communication.....4-13
Step 5. PLC Setup 4-14
Step 6. Checking PC-PLC Communication 4-14
4-4. Configuring Relay Function (Pattern B) 4-15
Step 1. Configuring Smart Roaming 4-16
Step 2. Checking Smart Roaming 4-16
Step 3. Checking PC-PLC Communication 4-17
4-5. To Set up MAC Address Filtering 4-18
4-6. Using Spanning Tree Function 4-19
■ Configuring Spanning Tree Function 4-19
4-7. Using CL-to-CL Communication via AP.....4-20
4-8. Limiting IEEE802.11b Communication 4-21
4-9. Smart Roaming.....4-22
■ Scanning Frequency 4-22
■ Smart Roaming for 802.11a 4-22
■ Smart Roaming for 802.11b/g 4-23
4-10. Configuring Smart Roaming 4-24
Step 1. Configuring IP Address 4-24
Step 2. Changing Own & Partner SSIDs 4-25
Step 3. Checking Wireless Channel 4-26
Step 4. Configuring Client-PLC Communication.....4-26
Step 5. PLC Setup 4-27
Step 6. Configuring Smart Roaming 4-28
Step 7. Checking Smart Roaming 4-28
Step 8. Checking PC-PLC Communication 4-29

Chapter 5 Setup Menu

5-1. Setup Screen & Functions 5-2
■ Setup Screen 5-2
5-2. Setup Screen (WE70-AP) 5-3
■ Network Settings 5-3
■ Wireless Settings 5-4
■ Information 5-13
■ Maintenance 5-15
5-3. Setup Screen (WE70-CL) 5-19
■ Setup 5-19
■ Information 5-26
■ Maintenance 5-27
5-4. Limiting Setup Screen Access 5-28

Chapter 6 Replacement Procedure

6-1. Replacing Wireless Unit 6-2
■ Saving Setup Data 6-2
■ Writing Saved Setup Data 6-4
6-2. Restoring to Factory Shipment Status 6-5
■ Using <INIT> Button 6-5
■ Using Setup Screen 6-6

Appendices

Troubleshooting Appendices-2
Changing Waiting Period for Scanning (from Version 1.22 of WE70-CL) Appendices-3
Options Appendices-5
■ Power Appendices-5
■ Antenna Appendices-5
■ Others Appendices-5
Initial Setup Value List Appendices-6
■ WE70-AP Appendices-6
■ WE70-CL Appendices-7
Rating Appendices-8
■ Wireless LAN Block (5GHz, 54Mbps; Common in AP/CL) Appendices-8
■ Wireless LAN Block (2.4GHz, 11Mbps/54Mbps; Common in AP/CL) Appendices-8
■ Common Spec for Wireless LAN Block (Common in AP/CL) Appendices-8
■ Wired LAN Block (Common in AP/CL) Appendices-8
■ General Specification (Common in AP/CL) Appendices-9
■ Other Functions Appendices-9
Dimensions Appendices-10
■ WE70-AP/CL Appendices-10
■ Mounting Bracket Appendices-10
■ High-sensitivity Magnetic-base Antenna (WE70-AT001H: Optional) Appendices-11
■ Extension Cable (WE70-CA5M: Optional) Appendices-12
Glossary Appendices-13
Revision History Appendices-14

Overview

Chapter 1

This chapter describes
Main features of a wireless unit set.

1-1. Features 1-2
■ Main Features 1-2
■ System Configuration 1-7
■ Relay Function 1-9
1-2. Components and Functions 1-10
■ Top View 1-10
■ Rear View 1-11

1-1. Features

WE70-AP/CL is a FA wireless LAN unit set conformance to IEEE802.11a/b/g.This section describes features of the FA wireless LAN unit set WE70-AP/CL.

Connecting this wireless unit set to a PLC Ethernet unit allows wireless monitoring of facility information through network as with wired connection.Ethernet unit functions can be used via radio communications as they are.

(e.g. FINS communication service/socket/FTP server/e-mail transmission)

■ Main Features

● FA wireless LAN units conformance to IEEE802.11a/b/g

This wireless unit set supports world-standard IEEE802.11a/b/g: both 5GHz band in IEEE 802.11a and 2.4GHz band in IEEE 802.11b/g.(Switched by setup and cannot be used simultaneously.)

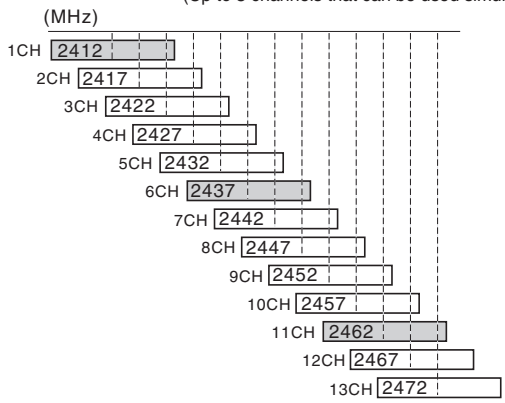
FA sites having used various types of wireless devices (such as wireless LAN, RF-ID, WD30/WT30), 2.4GHz band has been congested.If you have difficulty in installing a new wireless system due to radio interference, 5GHz band is recommended.5GHz band allow installation of additional wireless systems without influences on existing wireless systems.(Up to 24 systems)

Standards	IEEE 802.11a	IEEE802.11b	IEEE 802.11g
Maximum Speed	54Mbit/s	11Mbit/s	54Mbit/s
Frequency Band	5GHz band	2.4GHz band	2.4GHz band
Modulation	OFDM	DS-SS	OFDM
Characteristics	• 5 times higher in speed than 11b • Noise resistant • Less cross talk with other devices • All of 24 channels can be used at the same time	• Wide selection of products • Long communication distance • Can be used outdoors	• 5 times higher in speed than 11b • Less vulnerable to obstacles • Long communication distance • Compatible with 11b • Can be used outdoors

■ Channel assignment based on frequency band

2.4GHz band

802.11b/g: All of 13 channels (except 12CH and 13CH in United States and Canada)
(Up to 3 channels that can be used simultaneously)

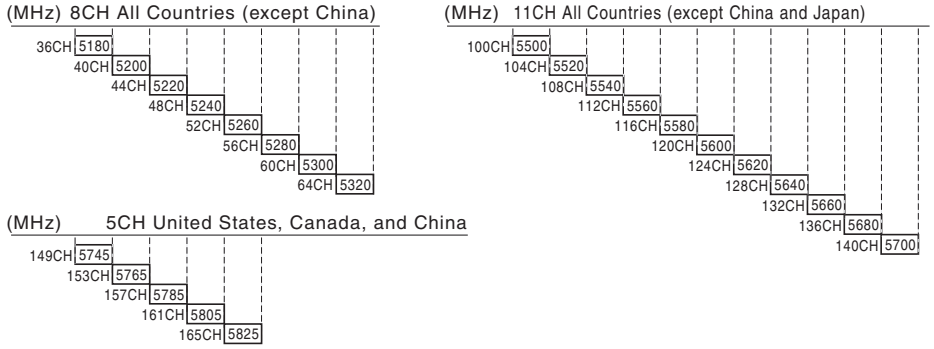


*You can chose a model for the country to use.

WE70-AP/CL	:Japan
WE70-AP/CL-US	:United States
WE70-AP/CL-CA	:Canada
WE70-AP/CL-EU	:Europe
WE70-AP/CL-CN	:China

5GHz band

802.11a: All of 24 channels (up to 24 channels that can be used simultaneously)(DFS-CH)
globally common, indoors only



● Transmission power switching function

This wireless unit set can configure 3 levels of radio field intensity for transmission.This allows easier installation of multiple wireless systems in one production site.Configuring the best transmission power for an installed system should minimize influence on other systems.

Assuming high wireless transmission power as 1.0, middle and low transmission power can be indicated as 0.5 and 0.25 respectively.

● Wireless communication distance

Wireless communication distance depends on installation environment and communication frequency. Use followings as guidelines.

- IEEE802.11a
  54Mbps communication: ca. 40m (indoors: Clear view)
- IEEE802.11b/g
  54Mbps (2.4GHz) communication: ca. 60m (indoors: Clear view)

● Receiving electric field strength monitoring function

RSSI (Receive Signal Strength Indicator) on CL shows a radio status.

A radio communication status is displayed on LEDs on the unit.

● Multiple sets of units installation is available in one zone

Using different channels (frequencies) in one zone prevents interference.

Up to 3 and 24 systems can be configured for 2.4GHz and 5GHz bands respectively.

● Noise-resistance in FA sites

Noise resistance is the same level as that for installation in control panel of Omron's FA equipment.(Equivalent to PLC)

The power supply is typical 24VDC in FA sites.Moreover, it is resistant against instantaneous power interruption in the same level as FA equipment, allowing stable operation under continuous motion.

● Optionally magnetic-base antenna can be provided.

Magnet allows easy installation of an antenna on a metallic part of a control panel

You can install a wireless unit set inside a control panel while its antenna outside the control panel.

Magnetic-base antenna contributes to cost reduction for installation.

● Easy installation & setup

This wireless unit can be easily installed on a DIN rail.

(DIN rail mounting bracket: For options (WT30-FT001/FT002))

Setting is conducted in a web browser on your PC.

● Smart roaming

When a radio wave status of current access point gets worse due to movement or relocation of WE70-CL (slave), communication can be made through other access point (WE70-AP) with better radio wave status.

● DFS (Dynamic Frequency Selection)

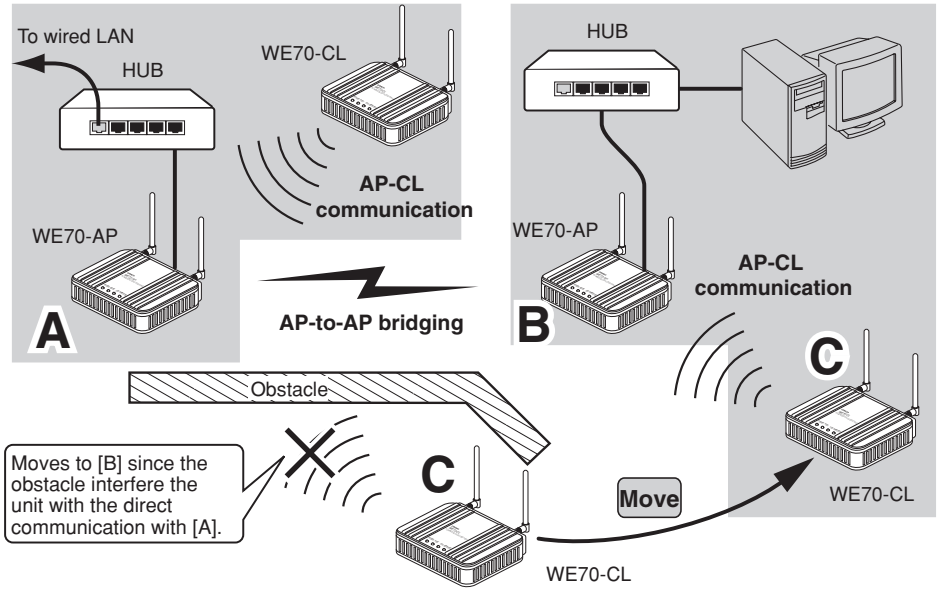
As some channels (52CH - 64CH, 100CH-140CH) have been already used by air traffic control radars and weather radars, a mechanism (DFS) is necessary to detect the radars.

When one of these channel is set, DFS scans radio waves for 1 minute after power-on of an access point and allows use of the channel only if it is not used.

If radio waves of an air traffic control radar or a weather radar is detected while wireless LAN is under operation, use of the channel is stopped within 10 seconds and switched to other channel.

● AP-to-AP (access point) bridging

In addition to communication between an access point and a client (slave), communication between access points (between A and B in the figure) is available.This function is called AP-to-AP bridging.
AP-to-AP bridging can be up to 54Mbps [IEEE802.11a /IEEE802.11g], allowing connection between access points.
Furthermore, an obstacle can be avoided that prevent direct communication between a client (slave, C in the figure) and its closest access point (A), by moving close to other access point (B) without any obstacle.
This function can be used also as a relay function (P.1.9, B) to expand a communication zone by wireless connection.



* All access points that use AP-to-AP bridging must be configured to use the same channel.
* Up to 6 units can communicate with an access point at the same time.
* To use encryption, the same encryption key must be configured for the access points.
* Only "WEP RC4" and "OCB AES" can be used as encryption for AP-to-AP bridging.
* BSSID of respective access point must be registered for those that use AP-to-AP bridging.
  In the figure above, [BSSID] of [B] must be registered to [A] and [BSSID] of [A] to [B].
* Configuring the same channel and SSID allows detection of BSSID of the others, making registration easier.
* To use roaming, the same SSID must be configured for the access points (A and B).
* AP-to-AP bridging requires the same setup of Super AG (Yes or No).
* AP-to-AP bridging is not available at the channel where DFS function is provided.

● Ample wireless LAN security function (* not configured on factory shipment status)

This wireless unit set provides the latest standardized security.It allows communication in FA wireless LAN only and rejects communication with other wireless LAN, enhancing security.

Following functions are provided for security required in wireless LAN communication.

MAC address filtering .....Access can be permitted to clients (slaves) with MAC addresses registered in an access point for communication in the same wireless network group.

WEP (RC4)/OCB AES .....Data transmitted in a wireless network is encrypted based on a set string for security.For AP-to-AP bridging, OCB AES is recommended.

* Communication will not be available if the other part of the communication uses a different encryption method or a cryptographic key.

• Others

TKIP/AES .....These encryption methods can only be used for a wireless LAN computer with Windows XP (Service Pack1) with a certain update program applied or with Windows XP (Service Pack2).

* "TKIP" is stronger than "WEP (RC4)".
* "AES" is a next-generation encryption method stronger than "TKIP".
* "TKIP" and "AES" do not support AP-to-AP bridging.

WOC KEY.....Omron's proprietary authentication method that uses a Pre-Shared Key as with TKIP/AES.

* "WOC KEY" do not support AP-to-AP bridging.

● Spanning tree

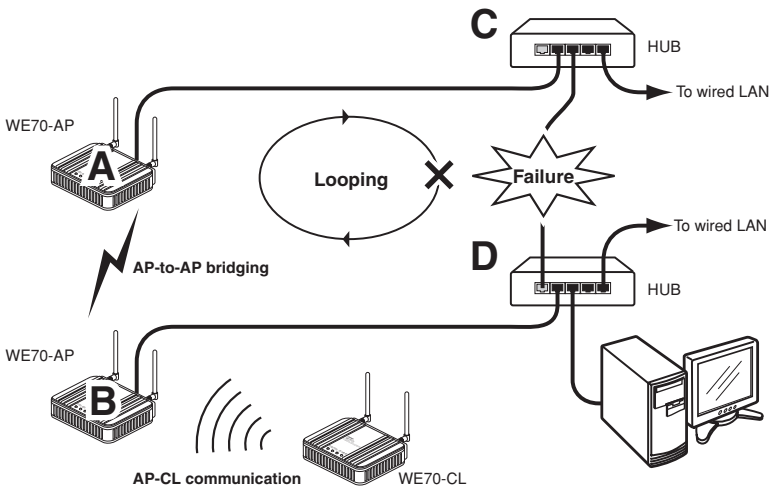
This function is used to detect a loop of communication between bridges, avoid endless looping of packets, and create an optimal route.

In a network example shown below, if spanning tree function is enabled for access points (A and B) a loop of any route is detected and a route with lower priority (route A-B) is shut off as long as no failure is occurring.If any communication failure occurs in a route between cascade-coupled hubs (route C-D), radio communication between access points (A and B) is enabled to keep normal operation of the network.

If this function is not used, communication packets on the network endlessly flow through access points (B->D->C->A->B).

If the spanning tree function is being enabled, it will take about 30 seconds after inserting a LAN cable before network communication becomes available,while its LAN indicator may be lit.

To construct a network using the spanning tree function, you must choose a switch or a hub that supports IEEE802.1d spanning tree protocol.



● Super AG technology

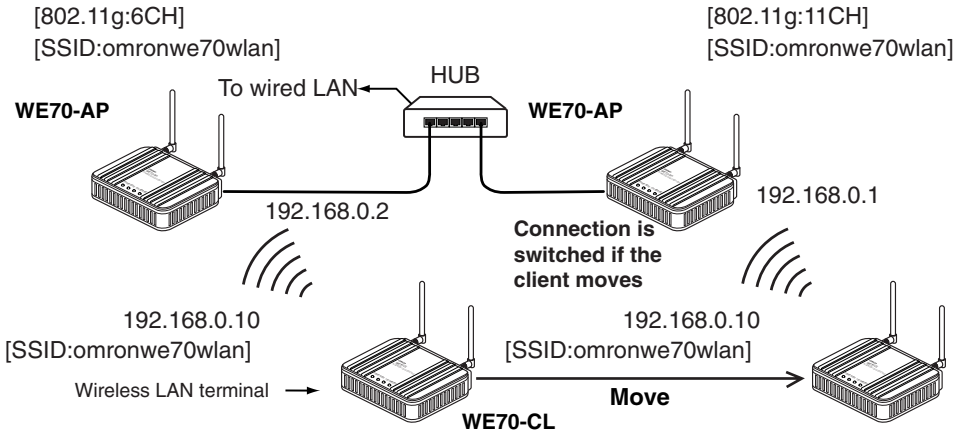
This technology was developed by Atheros Communications in the U.S. for higher speed wireless LAN.
To use the Super AG with other wireless device, other devices must support "Super AG" as well.
Super AG setup must be the same for those that use AP-to-AP bridging.

* To use AP-to-AP bridging with configuration of [Super AG] as [Yes (Compressed)], a key index to be configured for WEP (RC4)/OCB AES encryption must be configured as the same as those that use AP-to-AP bridging. Communication is unavailable if key indexes differ.

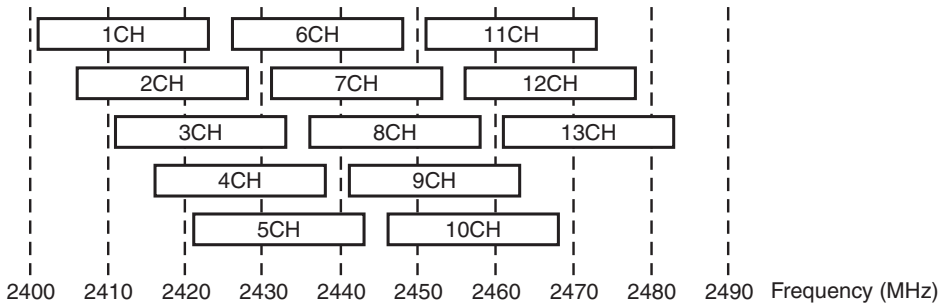
● Roaming

Providing more than one access point connected with wired LAN expands its wireless communication zone by automatically switching to an access point with better radio wave status when a client (slave) is moved, allowing use of wireless LAN while moving in a wide space such as a plant or a warehouse.
(Example: IEEE802.11g wireless LAN)

* To use roaming, the same wireless network name (SSID) and encryption must be configured for all access points and clients (slaves).(Communication is unavailable if setup differs)



* For communication using 2.4GHz band (IEEE802.11b/g), "channels" of access points must be configured with blank channels of 4 or more between them to avoid radio interference.
Otherwise a part of a band may overlap and cause cross talk.



* For communication using 5GHz band [IEEE802.11a], radio interference will not occur as long as configured channels are different for each other.

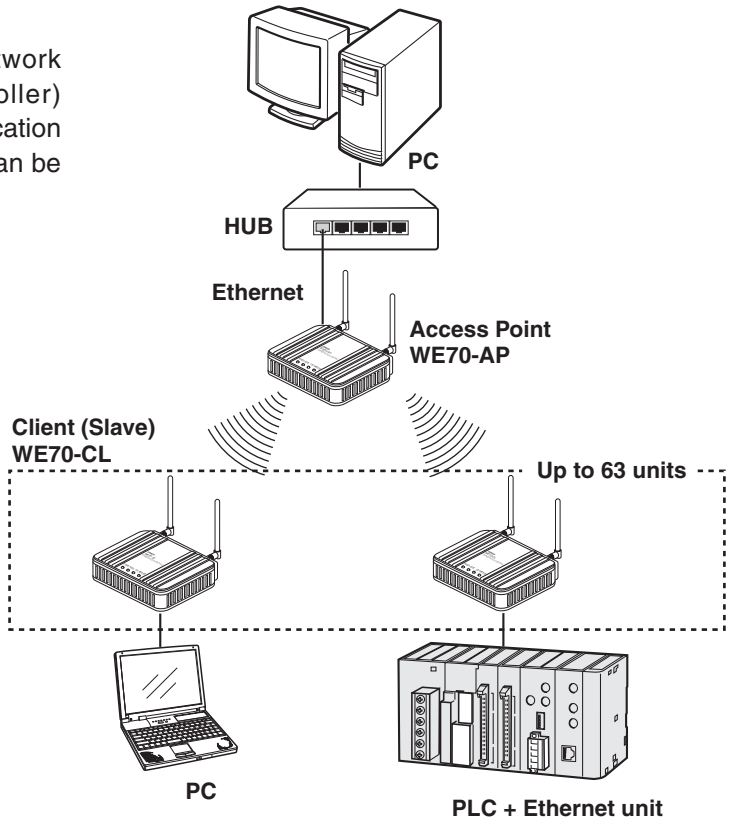
● Connection terminal limiting function

This function the limits the number of clients (slaves) that can be connected to an access point at the same time to prevent decrease in communication speed due to jammed connection.

* The value is 63 on factory shipment status.

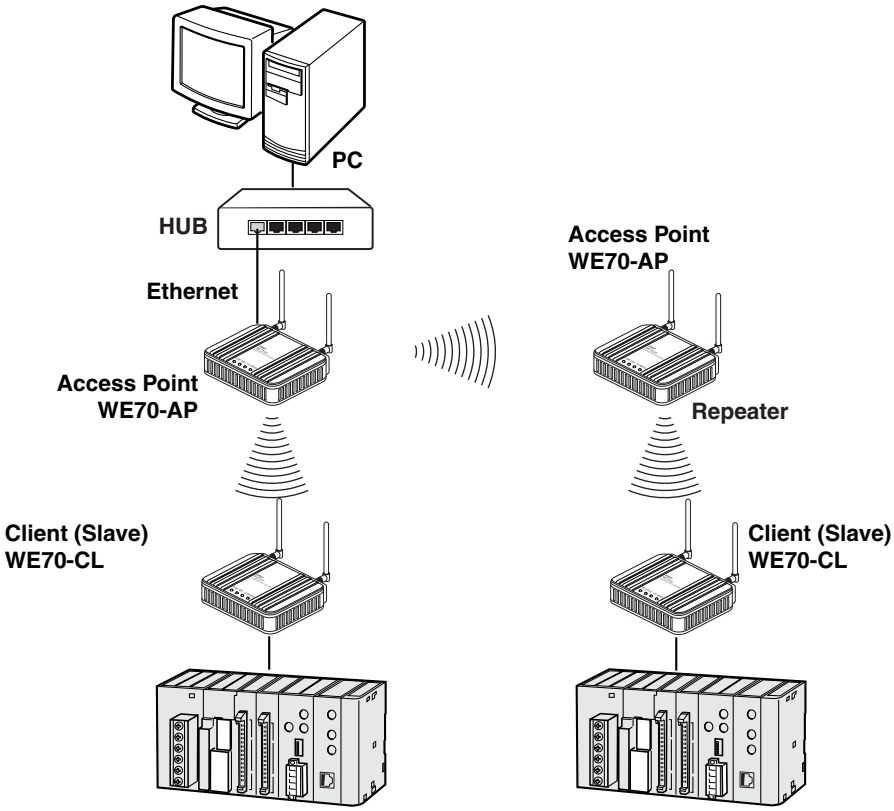
■ System Configuration

Connect an access point to the same network (Ethernet) as PLC (programmable controller) and/or PC (personal computer) for communication with clients (slaves),through which PC data can be shared and PLC data can be acquired.



● AP-to-AP bridging

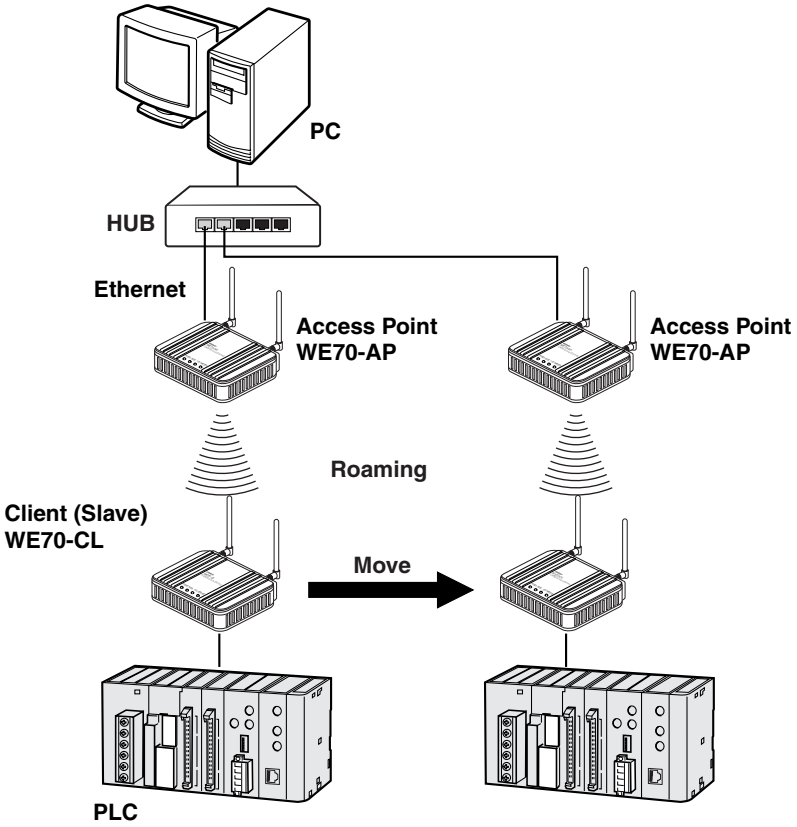
An access point is used as a repeater for communication with a client (slave).Access points used for this function must register the others' BSSIDs.



* AP-to-AP bridging is not available at the channel where DFS function is provided.

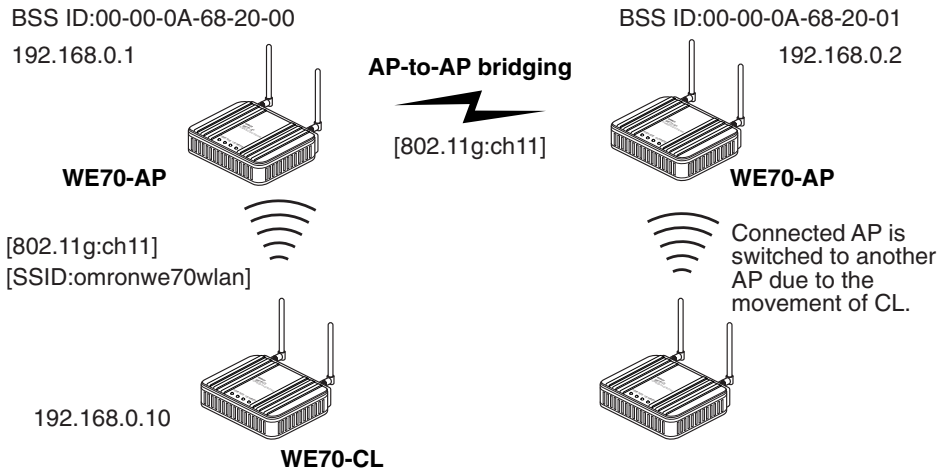
● **Roaming**

Connect 2 or more access points to the same network (Ethernet) for communication with a client (slave). Communication will be available with an access point closest to a client (slave) even if it is moved.



■ Relay Function

This function extends communication distance using other access point of AP-to-AP bridging as a wireless repeater.
BSSID of respective access point must be registered for those that use AP-to-AP bridging.
Communication will be available between a distant access point and a client (slave) via a repeater.



* Up to 7 access points (including own unit) can be used for communication at the same time.
  When one path is busy, other paths suspend communication. Because of this, all throughput is 1/6(1/ access number) by AP-to-AP Bridging.
  For the diagram of the maximum connection structure of communication AP-to-AP Bridging, see Ex 1 – 3 in “4-1 To Use AP-to-AP Bridging” (P.4-2 and 4-3).
* All access points that use AP-to-AP bridging must be configured to use the same channel.
* For more information on AP-to-AP bridging, see "To Use AP-to-AP Bridging" (P.4-2).
  Configuring the same SSID (3-3 Step 2. Configuring Wireless Network Name (SSID)(P.3-8)) allows detection of BSSID of the others, making registration easier.
* If connection described below is made in addition to the example above, spanning tree function must be configured to avoid looping of packets.(See P.1-5)
  •A network has 3 or more wireless units using AP-to-AP bridging.
  •Connecting access points (between A and B) using AP-to-AP bridging through a LAN cable
* AP-to-AP bridging is not available at the channel where DFS function is provided.

1-2. Components and Functions

■ Top View

[POWER] Indicator (Green)

Displays a power source status and a wireless unit operation mode.

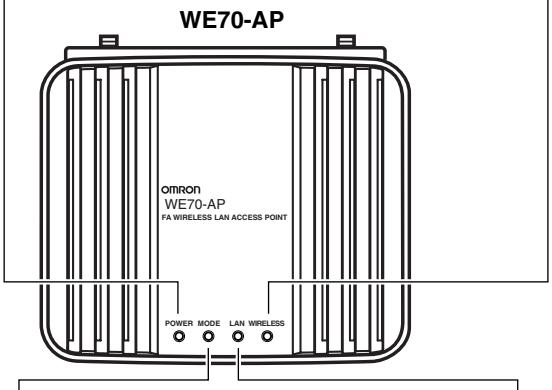
On: The wireless unit is turned on.
Flashing: Simultaneous flashing of [POWER] and [MODE]*1 indicates setup initialization.
Alternate flashing of [POWER] and [MODE] indicates startup.

[WIRELESS] Indicator (Orange)

Displays a status of the wireless LAN.

On: Radio communication is being established with the wireless unit.
Off: Absence of wireless LAN terminal which is communicating with the wireless unit, or no radio communication has been made for more than 5 minutes (10 seconds for WE70-CL).

*1 [RSSI] indicator for WE70-CL



[MODE] Indicator (Orange)(WE70-AP)

Displays an operation mode of the wireless unit.

Flashing: Simultaneous flashing of [MODE] and [POWER] indicates setup initialization.
Using 802.11a: On
Using 802.11b/g: Off

[LAN] Indicator (Orange)

Displays a status of the wired LAN.

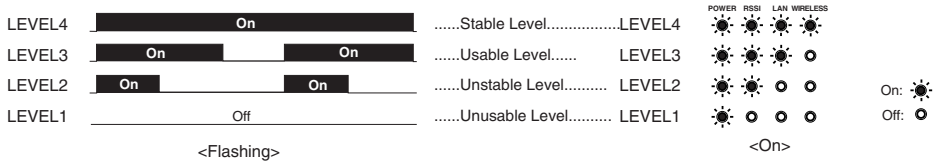
On: LAN connection is normal
Off: LAN is not being connected
Flashing: Data is being transmitted

RSSI

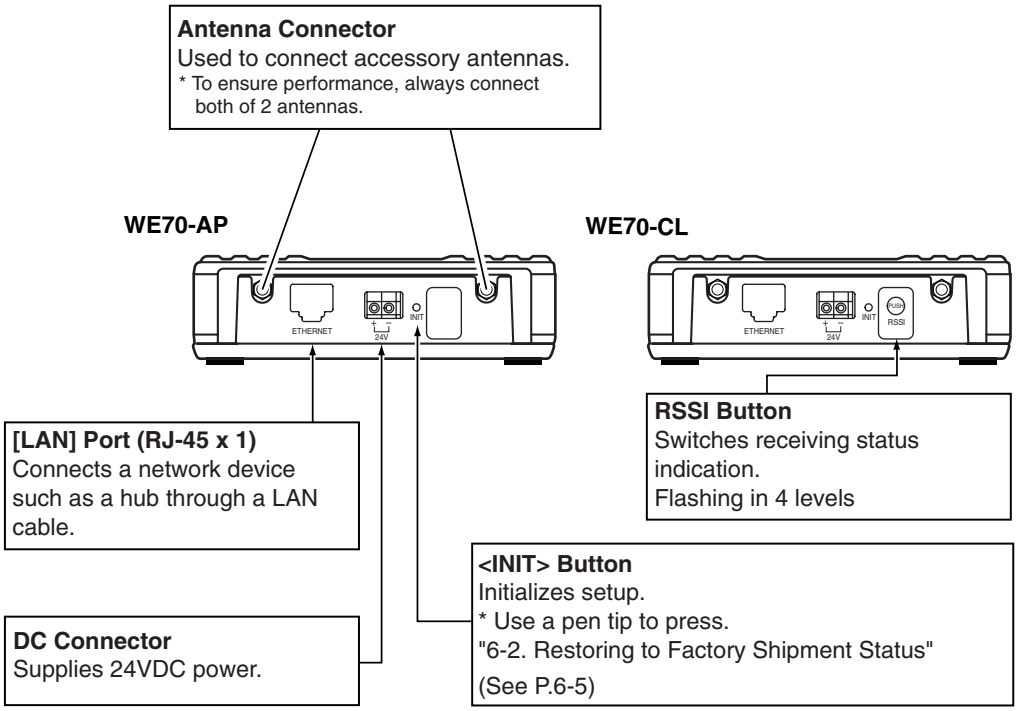
[RSSI] Indicator (Orange)(WE70-CL)

Displays receiving electric field intensity by flashing.

When the RSSI button on top of the unit is pressed, receiving electric field intensity is displayed on [RSSI], [LAN], and [WIRELESS] indicators in 4 levels. The [POWER] indicator flashes at the same time.Indication returns to its original status when 10 minutes passes or the button is pressed again.



■ Rear View



[For Reference]

- Use a Crossed LAN cable for a connection between a wireless unit and a hub.
- The [LAN] port of a wireless unit does not support automatic detection of straight LAN cable or cross LAN cable. Be careful for polarity to connect to a hub that does not support the automatic detection. [LAN] indicator will not be lit if polarity is wrong.
- For 100BASE-TX communication, STP LAN cable of category 5 or higher must be used. If a cable with lower category is used for the same LAN, total cable characteristics will be degraded to the lowest level of such a cable.

Installation & Connection

Chapter 2

This chapter describes
cautions for wireless unit installation and how to connect the unit set.

2-1. Installation 2-2
- ■ Installation Location 2-2
- ■ Installation Precautions 2-2
- ■ Precautions for Antenna Installation Location 2-3
- ■ Dimensions.....2-5
- ■ Installation Method 2-5

2-2. Connection 2-7
- ■ Wiring Precautions 2-7
- ■ Main Unit Power Wiring 2-7
- ■ LAN Cabling 2-8

2-3. Connection Check 2-10
- ■ Checking Setup Screen Access 2-10

2-1. Installation

Make sure that the radio wave conditions at the installation location are favorable before actually installing the WE70 wireless unit.

■ Installation Location

Install this product as high as possible.
Do not install it to the following places:

- Where it is exposed to direct sunlight
- Where with extremely high humidity
- Near devices such as televisions, radios, and computers
- Near devices such as motor, drill, and welder
- Near strong magnets
- Near fluorescent lights
- Inside a metal panels or locations surrounded by metal or concrete

If WE70 is installed in a metal panel, be sure to mount the magnetic-base antenna outside the panel where there are no obstacles.

■ Installation Precautions

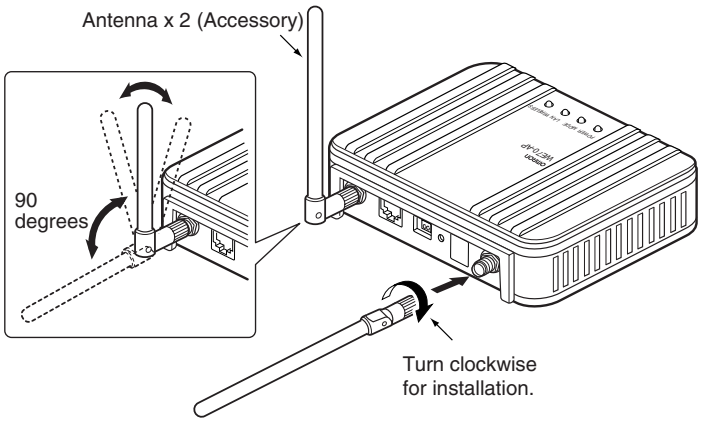
● Mounting Antenna

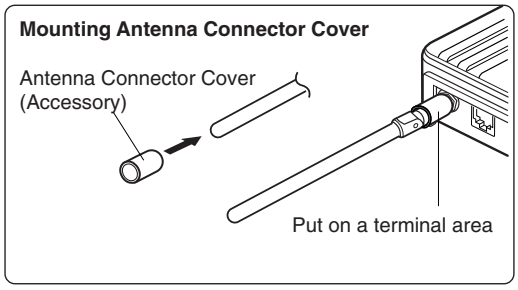
A set of 2 antennas function as diversity and is good at multi-path, allowing communication under stable radio wave status.To install, hold the connection point of antenna and turn the antenna clockwise.

Antennas can be bent to an angle ranging from 0 to 90 degrees. They can be turned right and left while being bent.

To uninstall, hold the connection point of antenna and turn the antenna counterclockwise.

* To ensure performance, always connect both of 2 antennas.
* If radio wave status is bad, change a direction or an installation location of an antenna.
* Use antenna connector cover to dust prevention.(See right)





> ⚠ Caution: Do not grasp or pull the antenna itself which is mounted to the wireless unit.
> Otherwise it may be damaged.

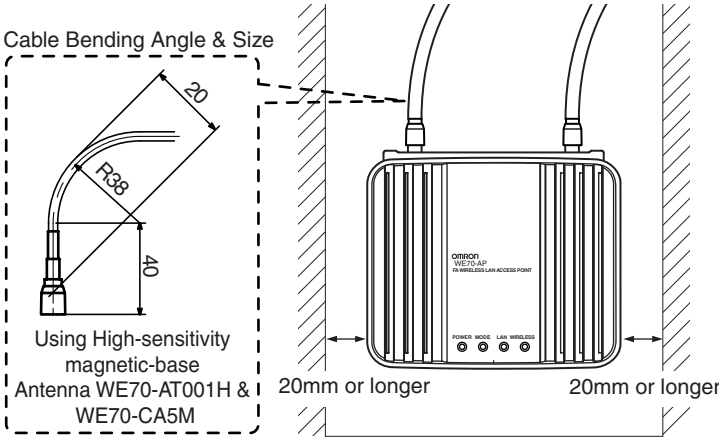
● Installing the magnet base antenna and antenna extension cable

Use the connector cover when connecting a cable.

● Margin and Spacing

For heat release, ensure space between a wireless unit and a control panel or other equipment as shown in the right.

> ⚠ Caution: Antennas manufactured by other manufacturer cannot be used because of the conflict with Technical Standard Conformity Certification.



● **Connecting the antenna extension cable (WE70-CA5M)**

The cable length of the magnet base antenna is 2m. If longer length is required, use the antenna extension cable (WE70-CA5M) 5m. Pay attention to attenuation of the cable when using the antenna extension cable.

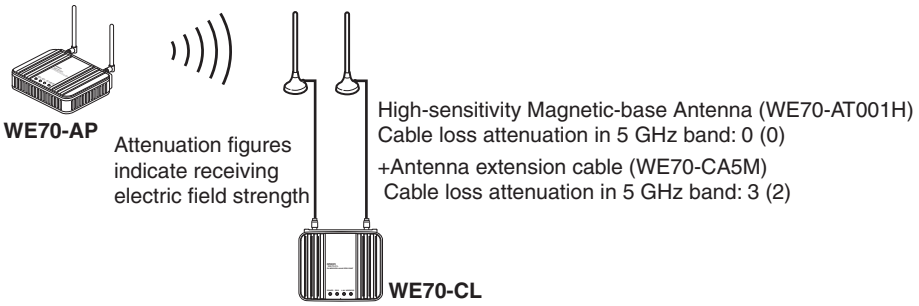
* The WE70-AP does not comply with FCC/IC rules when it is connected with the WE70-CA5M Extension Cable. Do not use the WE70-CA5M with WE70-AP in the United States and Canada. (The WE70-CA5M can be used with the WE70-CL.)
Due to the technical standard conformity certification, only one Extension cable can be used per Magnetic-base Antenna.

● **Precautions on Using Magnetic-base Antenna & Antenna extension cable**

Using a magnetic-base antenna causes signal attenuation due to its cable, reducing communication range compared with a standard pencil antenna.

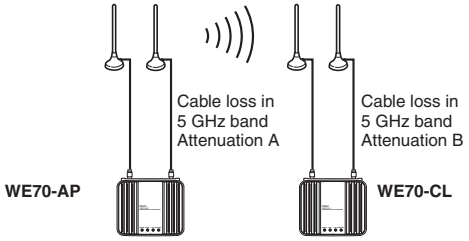
Using Magnetic-base Antenna on Client

In an example below, receiving electric field strength decreases in the 5GHz band by up to 8 levels.Degree of decrease is larger in the 5GHz band that uses higher frequency than the 2.4GHz band.To use a magnetic-base antenna, a communication range should take cable attenuation into account for actual receiving electric field strength of a pencil antenna.



Using Magnetic-base Antenna on Access Point & Client

Using magnetic-base antennas & Antenna extension cable causes signal attenuation by up to 6 levels in the 5GHz band, compared with a pencil antenna (accessory).If magnetic pedestal antennas are used for both of an access point and a client in the 5GHz band, it is necessary to ensure additional 6 levels of received field intensity to gain the same level of received field intensity as that of a pencil antenna.



Attenuation A+B = 0(0) High-sensitivity Magnetic-base Antenna(WE70-AT001H)
6(4) High-sensitivity Magnetic-base Antenna(WE70-AT001H)+Antenna extension cable(WE70-CA5M)

Figures in ( ) are for 2.4 GHz:IEEE802.11b/g
Attenuation figures indicate receiving electric field strength

For receiving electric field strength, see "5-3. Setup Screen (WE70-CL)" (P.5-19).

⚠ **Caution**

- Holding or pulling an antenna while uninstalling may damage it.
- Always hold the base part for handling.
- Avoid cable twisting as much as possible.
- Before attaching it to a wireless unit, check if the plug and the jack are properly coupled, and tighten a ring nut.For installation, turn the ring nut only while keeping a cable unturned.
- Take precautions so that a cable should not be damaged by a hole edge while putting it into the hole.
- Using a magnetic base antenna causes signal attenuation due to its cable, reducing communication range compared with a standard pencil antenna.

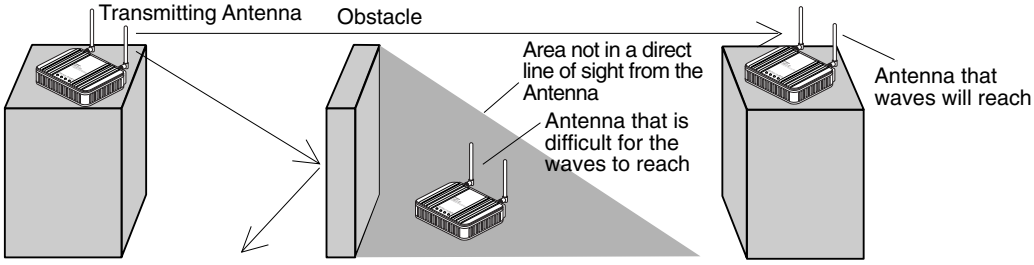
■ Precautions for Antenna Installation Location

This wireless unit set uses very high radio frequencies of 2.4/5GHz.High frequency radio wave is progressive and reflective.
To ensure wireless performance, it is necessary to choose an appropriate location for antenna installation.
For co-polarization of each antenna, see "Appendices-3 Antenna".

(1) Install antennas so that there is a direct line of sight between them

WE70 uses radio waves with a frequency of 2.4GHz and 5GHz, which are very high. High-frequency waves, which exhibit strong rectilinear propagation and are reflected easily. For this reason, much consideration is required for the Antenna installation location to achieve optimal wireless performance.

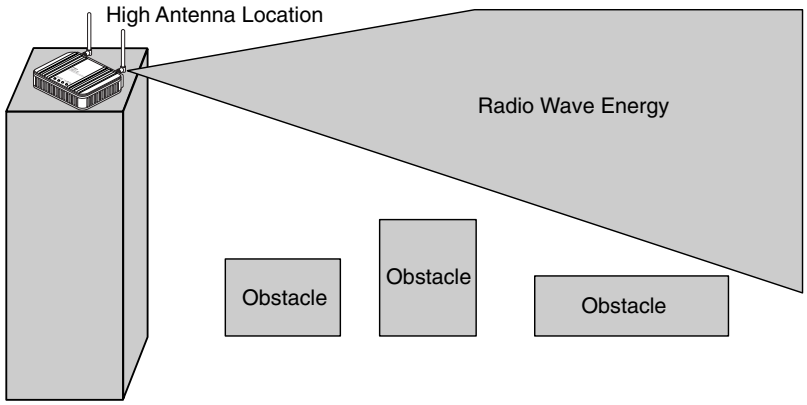
This is particularly important point for long distance communication over 50 to 60m.



If the Antennas are installed in locations with relatively high ceilings and a lot of open space, even if there is no direct line of sight between the Antennas, if one of the Antennas is installed in a high location, communications may still be possible via radio waves that are reflected off the ceiling.

(2) Install in as high location as possible

As mentioned in the preceding paragraph, if the Antennas are installed in high locations, since the space surroundings the Antennas will be more open, there will be less influence from obstacles, and the radio waves will propagate more easily.

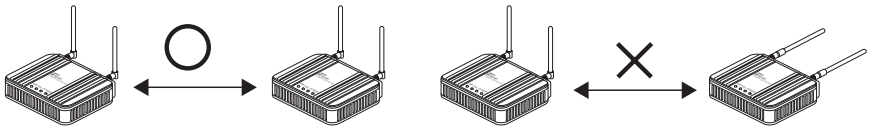


(3) Do not put any obstacle (especially a metal object) near the Antennas

If there are obstacles near the Antennas (in particular, in the direction of radio wave propagation), the radio waves may not be propagated due to the influence of the objects. Metal objects have the greatest influence as they reflect radio waves, whereas glass and plastic objects allow the waves to pass through and so have the least influence. Be sure to install Antennas at least 30 cm away from any obstables.

(4) Install the Antennas with the same orientation

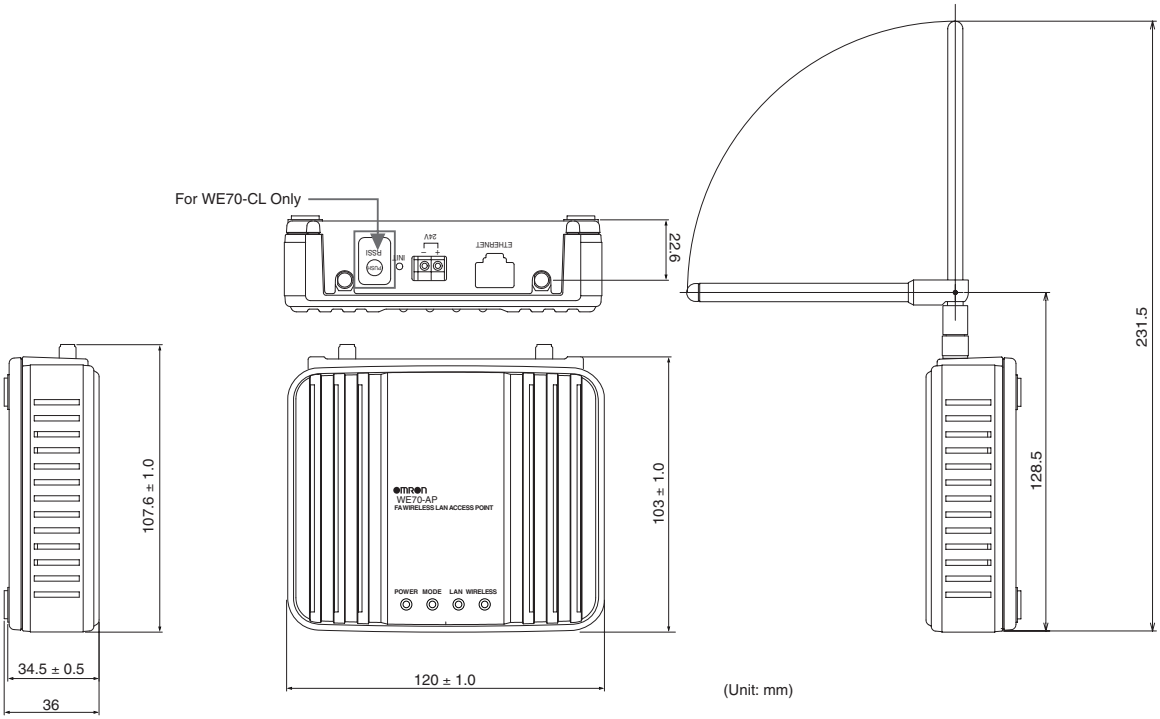
Install Antennas that are performing communications with the same orientation, as shown in the following diagram. If they are installed at an angle of 90 degrees to each other, the possible communications distance will be shortened.



(5) Do not subject the Antenna to shock

Do not install an antenna which it may be hit by other objects.Take preventive measures for installation in such a place.Subjecting the Antenna to strong shock may cause either external or internal damage to the Antenna. Internal damage that is not necessarily visible may prevent communications, such as broken wires.

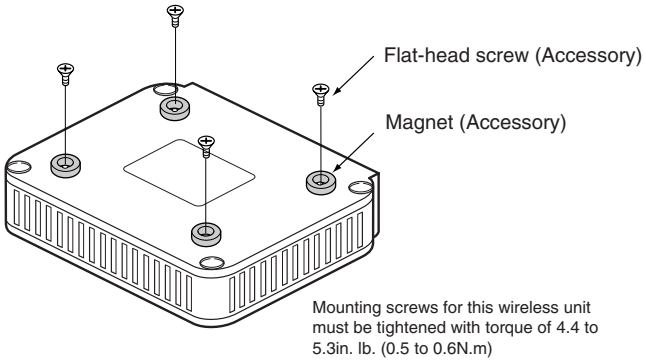
■ Dimensions (Common with WE70-AP/CL)



■ Installation Method

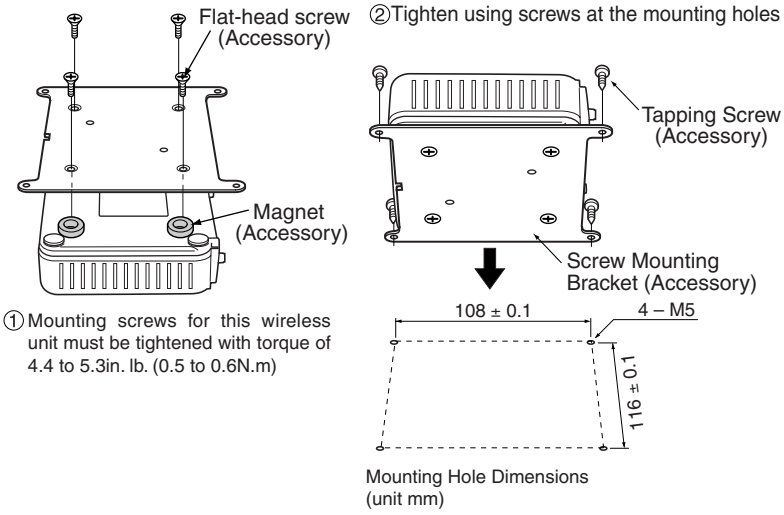
● Mounting Magnets

Mounting magnets allows temporary installation and easy move for setup and testing before actual operation.
Mount magnets using screws as shown in the right.



● To Mount Using Mounting Bracket

Attach the mounting bracket on accessory magnets which are installed on a wireless unit. Installation on a control panel requires screw hole drilling.



> ⚠ **Caution**
> - Installation with magnets cannot be used at the location with excessive vibration. Use the mounting bracket or DIN rail adapter in that case.
> - Make sure to insert the enclosed magnets between the mounting braket and the wireless unit.

● To Mount on a DIN Rail

Do not install a product with a pencil-type antenna in a metal panel as it may result in degradation of radio performance.To install this product in a panel, use and install a magnetic-base antenna outside the panel.See "Options" of "Appendices", "Antenna" (P.Appendix-5).

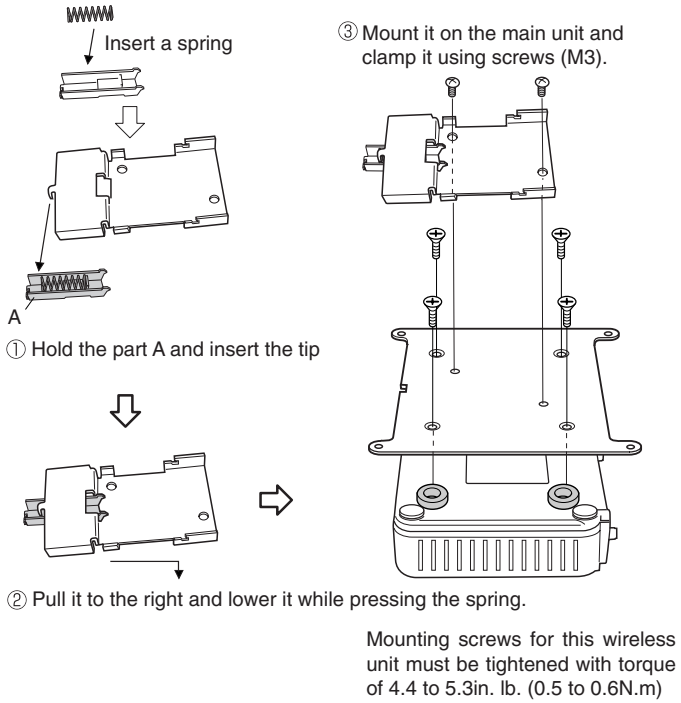
Applicable Rail

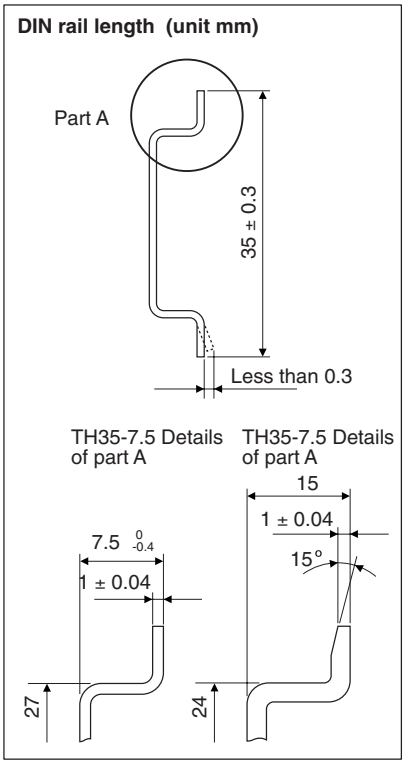
There are 2 types of rails with a width of 35mm, height of 7.5mm or 15mm.

(Conformance to DIN, EN, IEC, and JIS C2812 standards)

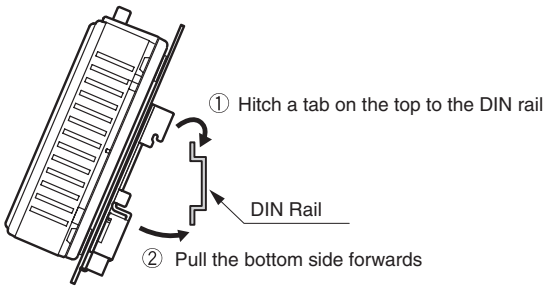
Model	Rail	Specification
WT30-FT001	TH35-7.5	Rail width 35mm and height 7.5mm
WT30-FT002	TH35-15	Rail width 35mm and height 15mm

Mounting DIN Rail Adapter

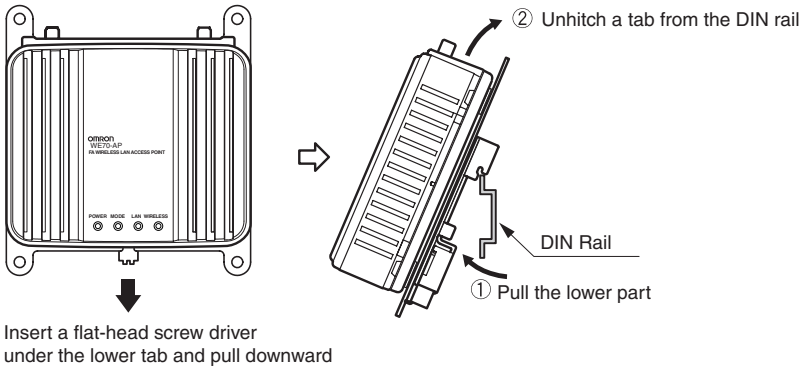




<Mounting>



<Demounting>



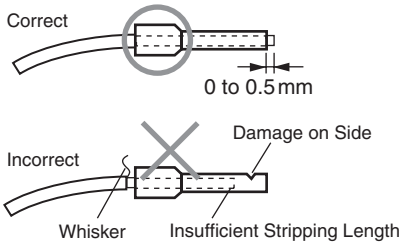
2-2. Connection

For connecting the antenna and the antenna extension cable, see “2-1 Installation” (P 2-1).

■ Wiring Precautions

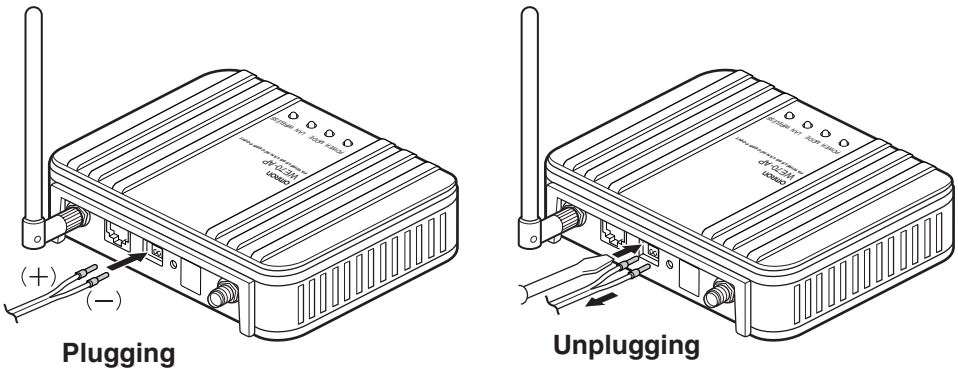
- Signal lines and power lines must be separated to avoid influence of noise.
- Do not lay cables close to antennas.
- Wiring must be done while power is off.
- Use a pin terminal or a cable for connection as shown below.

A pin terminal must be clamped with an appropriate tool based on its size.The tip of a wire must be cut in the same length as the pin terminal or 0.5mm longer.A whisker must not exist, and a pin terminal must not be broken.



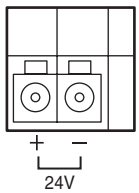
Phoenix Contact Inc.*	
Pin terminal	AWG18 AI 0.75-10
Clamping Tool	CRIMPFOX ZA3

- Plug the pin terminal into the power terminal block to the end.Fix wiring close to its connector so that a cable should not apply load to the connector due to its twisting or weight.
- A pin terminal must be unplugged while inserting a flat-head screw driver as shown below.



■ Main Unit Power Wiring

Power of the wireless unit is 24VDC.



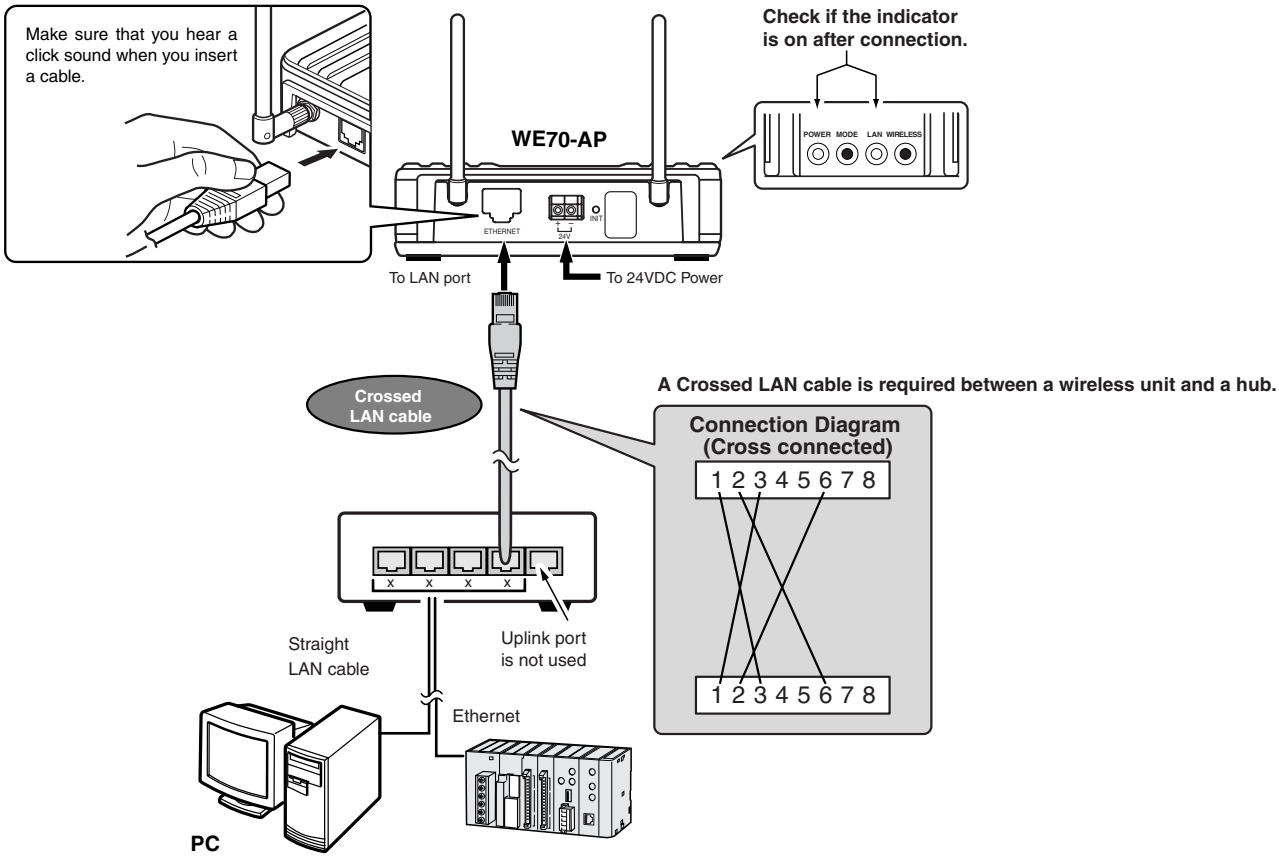
A wireless unit requires 24VDC power supply.
Use a power source of 30W or higher, taking inrush current on startup into account.
Omron's switching power supply is recommended.
See "Option" of "Appendix", "Power Supply" (P.Appendix-5).
And, it power is supplied from the battery supply via the DC-DC converter.

Line Voltage	24VDC
Allowable Voltage Range	20.4 to 26.4VDC

- This unit needs to be installed under local regulations.
- This unit is intended to be supplied by a "Listing Class 2" or "L.P.S." and rated from 24V, 250mA.

■ LAN Cabling

⚠ **Caution** Turn off power of a wireless unit and connected devices before cabling.

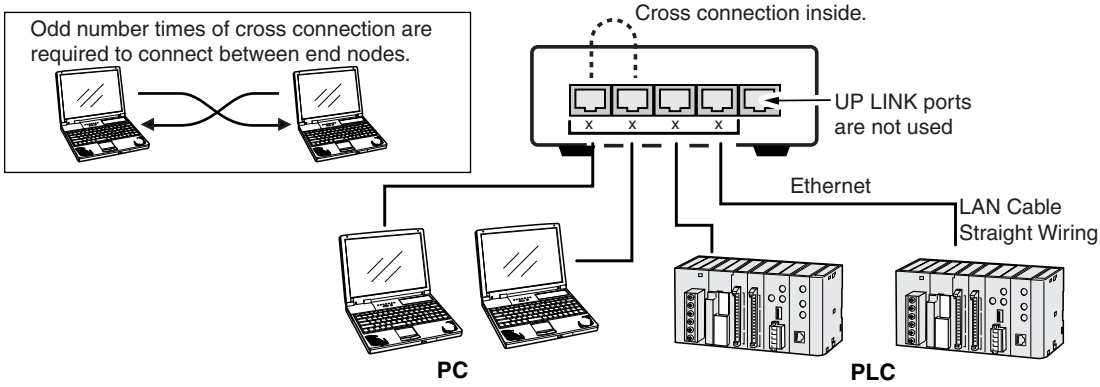


* A straight LAN cable can be used for direct connection of PLC or PC to a wireless unit for setup. Use a crossed LAN cable for a connection between a wireless unit and a hub.

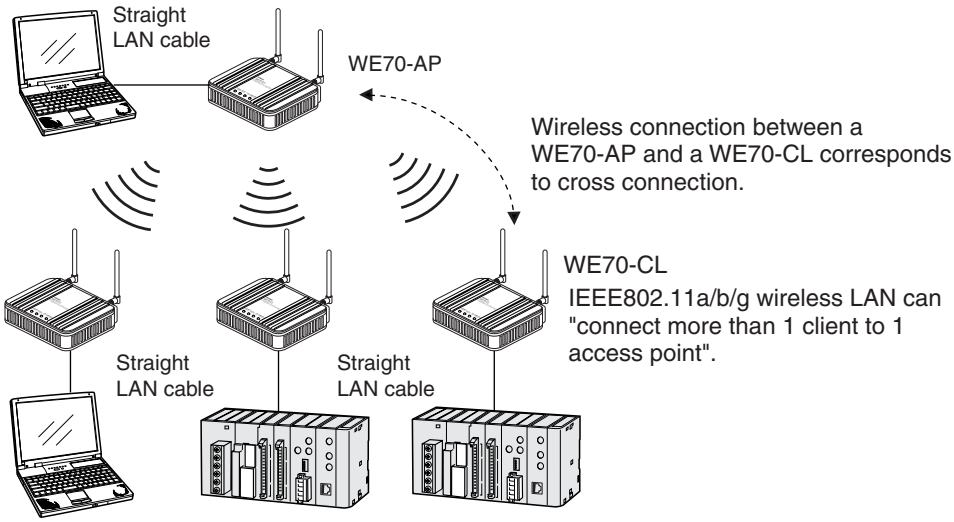
* STP LAN Cable must be used.

● Using Switching Hub (1:N Connection)

Ports other than UPLINK have no difference such as master/slave or upper/lower (all other ports other than UPLINK are equal)



● Using WE70 (1:N Connection)



2-3. Connection Check

■ Checking Setup Screen Access

This section describes how to make access to a setup screen for a wireless unit via a WWW browser of a wired computer on LAN.

* Use Microsoft Internet Explorer 6.0 or 7.0 as the WWW browser of your PC.
* In this document Internet Explorer 6.0 is used.

* A screen shown below indicates a factory shipment status or all-initialized status of a wireless unit.

● IP Address Setup

This section describes how to configure a fixed PC IP address (ex.: 192.168.0.100) on Windows XP.

IP addresses of a wireless unit set are "192.168.0.1" for an access point and "192.168.0.254" for a client (slave).

<To Configure>

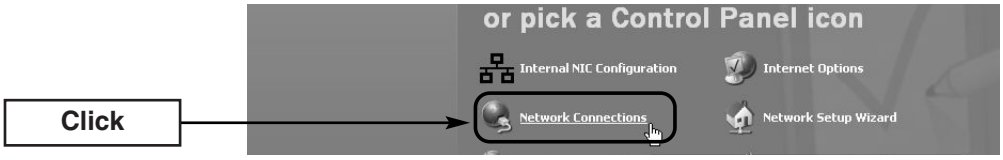
(1) Start your PC.

(2) In the Logon screen, log on using administrator's user name.

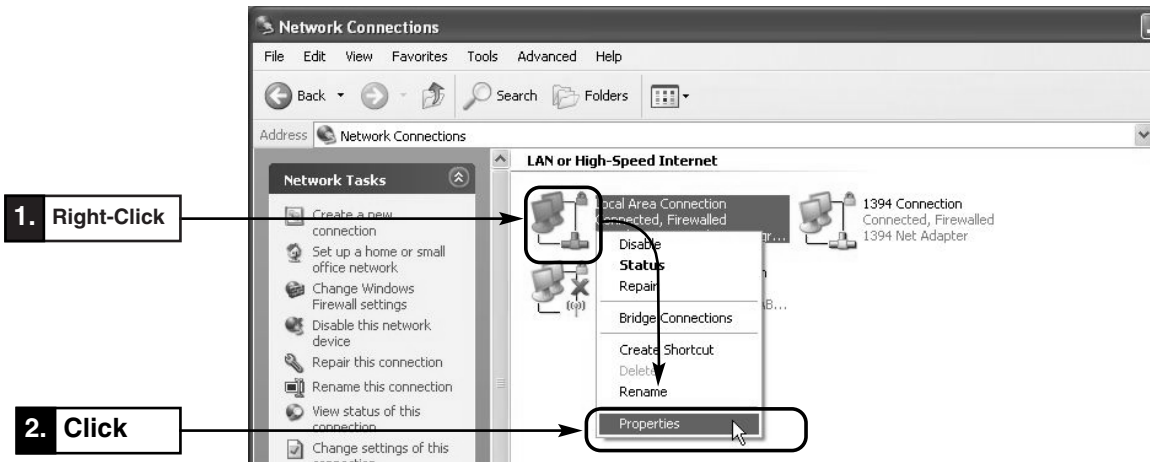
(3) Select <Start>, [Control Panel].

(4) Click [Network and Internet Connections].

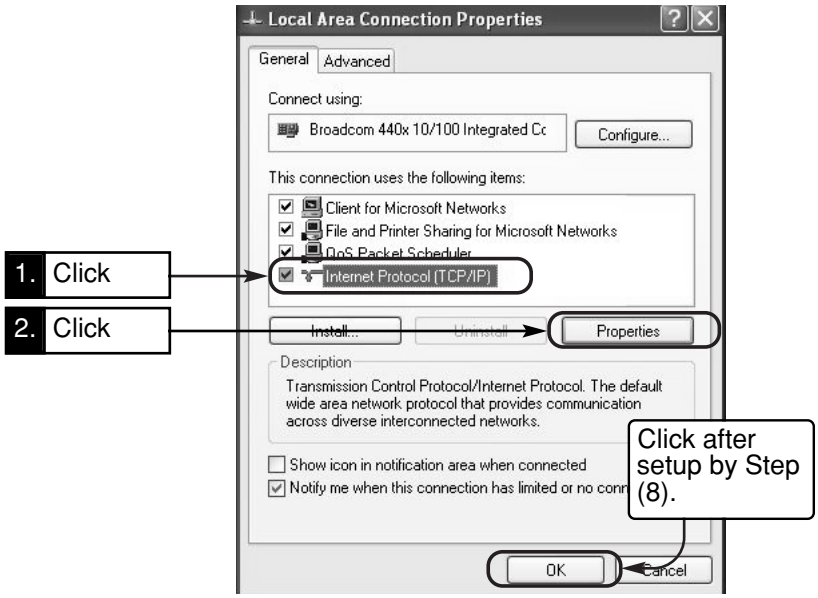
(5) Click [Network Connections].



(6) Right-click on [Local Area Connection] icon with your Ethernet card name, then select [Properties] from the context menu.

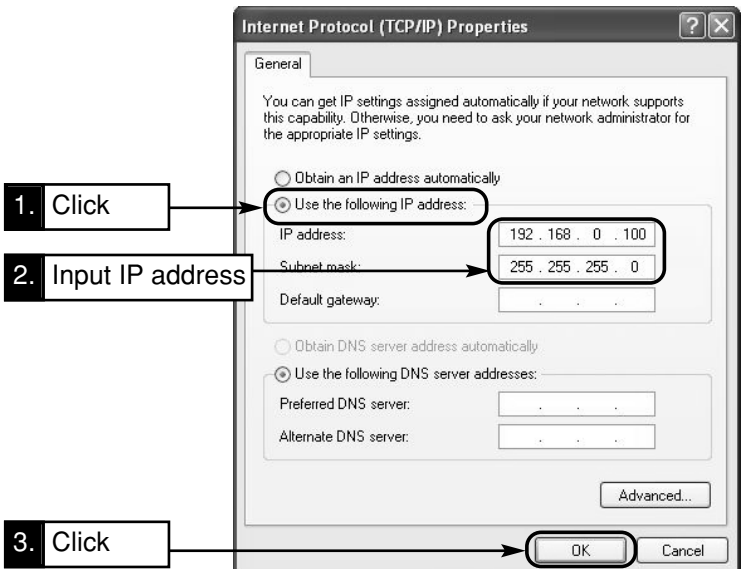


(7) Check the box of "Internet Protocol (TCP/IP)" and click <Properties>.



Before changing an IP address, record the current value.

(8) Select [Use the following IP address] radio button.Enter [IP address](192.168.0.100) and [Subnet mask](255.255.255.0), then click <OK>.(* Close a screen shown in Step (7))



● IP Address Assignment

An IP address consists of 2 fields; a network block and a host block.
Take a default IP address "192.168.0.254"(class C) of a wireless unit. "192.168.0." represents a network block and the remaining "254" represents a host block.Network devices (e.g. PC) with the same "network block" of IP addresses are identified as those on the same network.
A "host block" identifies each network device on the same network.
The followings must be taken into account for assignment of IP addresses:

- Assign the same "network block" for network devices that should be on the same network
- Do not assign the same "host block" for network devices on the same network
- Do not assign a network address (one that has "0" as its host block, in case of subnet mask of "255.255.255.0")
- Do not assign a broadcast address (one that has "255" as its host block, in case of subnet mask of "255.255.255.0")

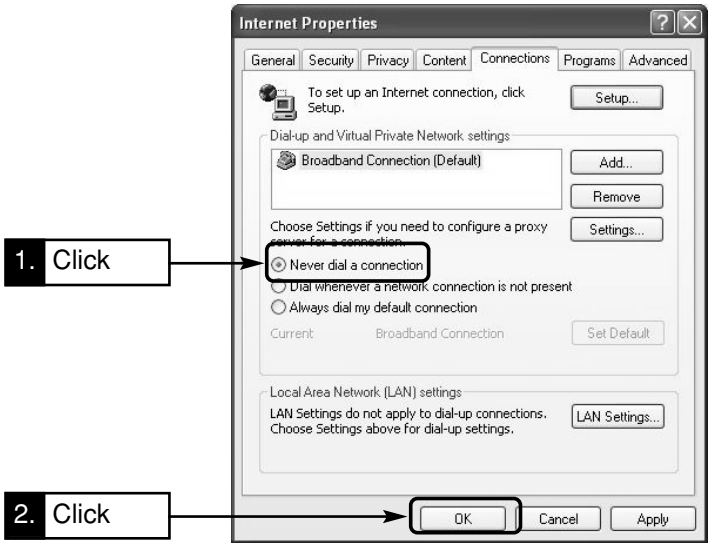
● **WWW Browser (IE) Setup**

Configuration must be made so that dial-up access should not be made when a WWW browser is started.

<To Configure>

(1) Select [Tool], [Internet Options], then select [Connections] tab.

(2) Select [Never dial a connection] and click <OK>.

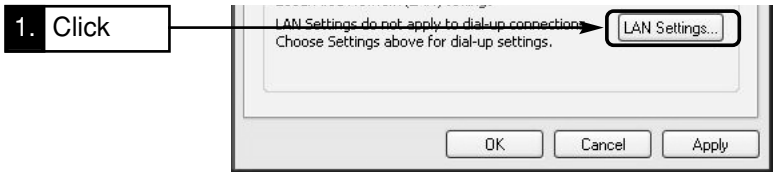


● **Proxy Setup**

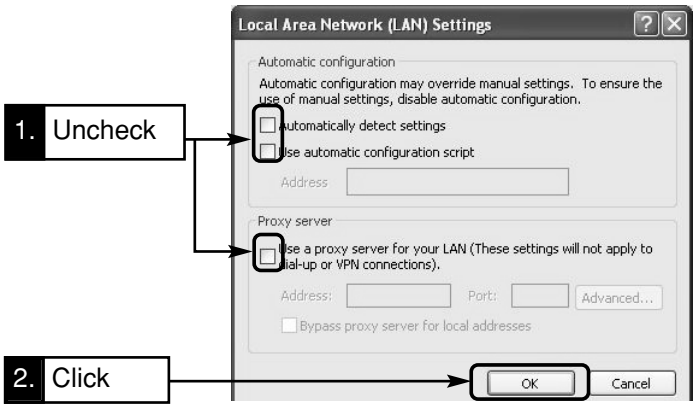
Configuration must be made not to use a proxy server.

<To Configure>

(1) From the above screen, click [LAN Settings].



(2) Uncheck all boxes, then click <OK>.



● Initiating Setup Screen

(1) Start a WWW browser.

(2) Enter the IP address specified for the wireless unit in the address bar of the WWW browser.
Enter "http://192.168.0.1/" (factory shipment status) for WE70-AP and "http://192.168.0.254/" (factory shipment status) for WE70-CL, and press [Enter] key.

(3) In case of an access point, a user name input is admin and a password input is requested. Press [Enter] key while leaving the password field blank.Initial value (User name: admin, Password: Blank)

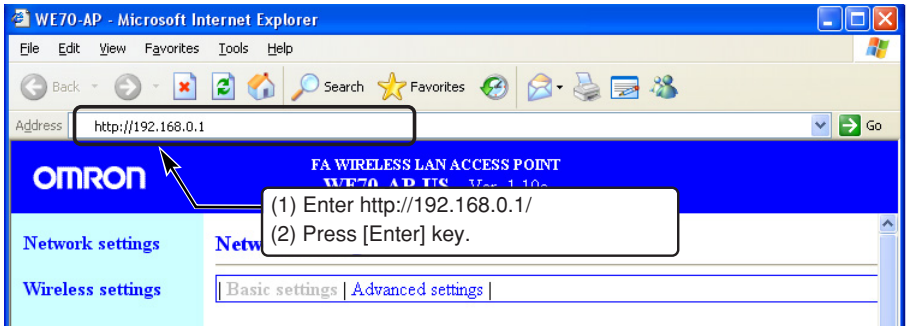
• A Basic Setup screen of Network Setup menu is displayed.

* To configure SSID and encryption of wireless LAN from PC connected to a wired LAN, see sections "3-4. Configuring Encryption" (P.3-12) to "3-5. Communicating with PLC" (P.3-21).

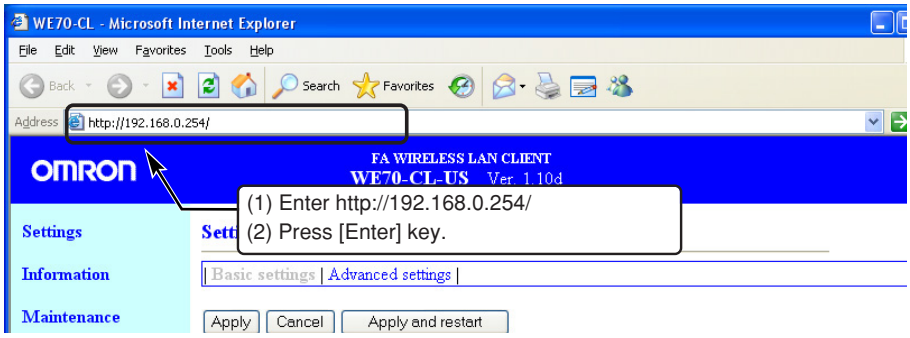
* For more information on the screen, see "5-1. Setup Screen & Functions" (P.5-2).

Setup Screen

Screen of WE70-AP



Screen of WE70-CL



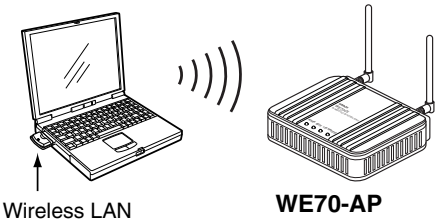
● **Access Point Communication Speed**

WE70-AP works as an access point in IEEE802.11a /b/g standards.

If clients (slaves) of IEEE802.11b and IEEE802.11g make access to an access point at the same time, communication speed may remarkably decrease.

Although up to 63 clients (slaves) can be used for the same wireless LAN standard* at the same time, it is recommended that number of clients should be limited to 10 or less.

In an environment where clients (slaves) of IEEE802.11b and IEEE802.11g exist, use 11g protection mode.(See "4-8. Limiting IEEE802.11b Communication" (P.4-21))



* An IEEE802.11b client (slave) is assumed to be included in access point "IEEE802.11g" standard.

Basic Setup

Chapter 3

This chapter describes
how to establish communication between an access point and a client (slave) as well as a PLC using PC.

3-1. Setup Workflow 3-2
3-2. Opening Setup Screen 3-3
Step 1. PC (Wired LAN) Setup.....3-3
Step 2. Connecting.....3-3
Step 3. Checking Setup Screen Access.....3-4
Step 4. Monitoring Wireless Communication Status 3-5
■ To display the setup screen in Japanese 3-6
3-3. Configuring IP Address/SSID/Channel.....3-7
Step 1. IP Address Setup.....3-7
Step 2. Configuring Wireless Network Name (SSID) 3-8
Step 3. Configuring Channel 3-9
Step 4. Checking Communication 3-11
Step 5. Other Setups 3-11
3-4. Configuring Encryption.....3-12
■ To Enter Encryption Key Using ASCII Characters 3-12
■ Entering Encryption Key.....3-13
■ Setup Example of Encryption Key 3-14
■ To Enter Encryption Key Using hexadecimal number 3-15
■ Conversion Table from ASCII Character to hexadecimal number..3-16
■ To Generate Encryption Key Using Key Generator 3-17
■ To Configure TKIP/AES/WOC KEY Encryption 3-18
3-5. Communicating with PLC.....3-20
Step 1. Preparing PLC & PC 3-20
Step 2. MAC Address Setup 3-21
Step 3. PLC Setup 3-21
Step 4. Checking Communication with PLC.....3-22
■ Precautions for Communication with PLC 3-22

3-1. Setup Workflow

Read steps described below to introduce a wireless unit set.
Steps are compiled so that basic setup can be made in their order.
Numbers indicated in the right of these steps indicate pages to refer to in this document.

Step 1 3-2. Opening Setup Screen ——— 3-2

▼

Step 2 3-3. Configuring IP Address/SSID/Channel ——— 3-7

▼

Step 3 3-4. Configuring Encryption ——— 3-12

▼

Step 4 3-5. Communicating with PLC ——— 3-20

3-2. Opening Setup Screen

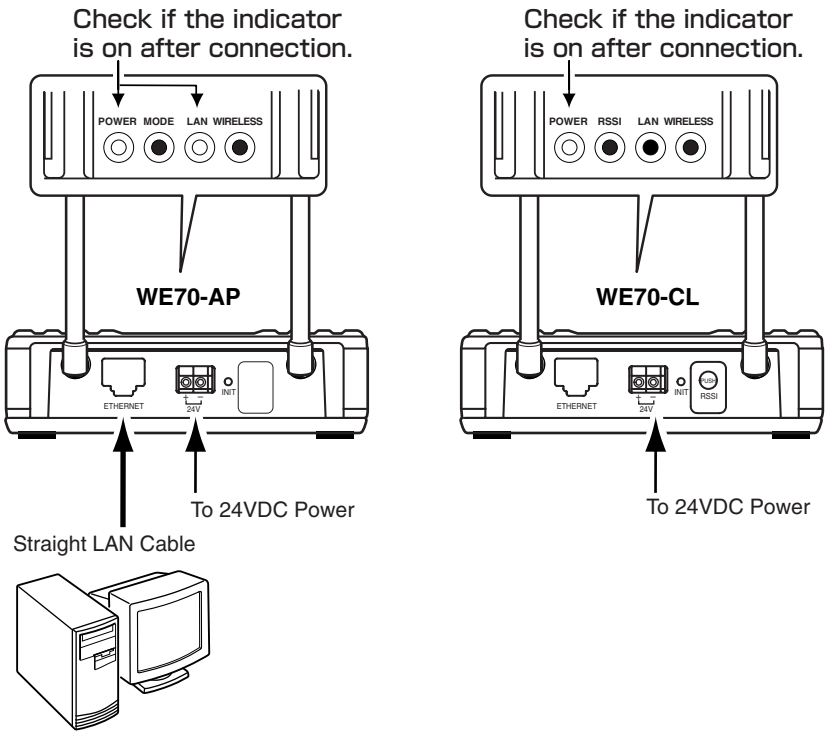
This section describes steps from opening a setup screen for an access point and a client (slave) to checking communication.

Step 1. PC (Wired LAN) Setup

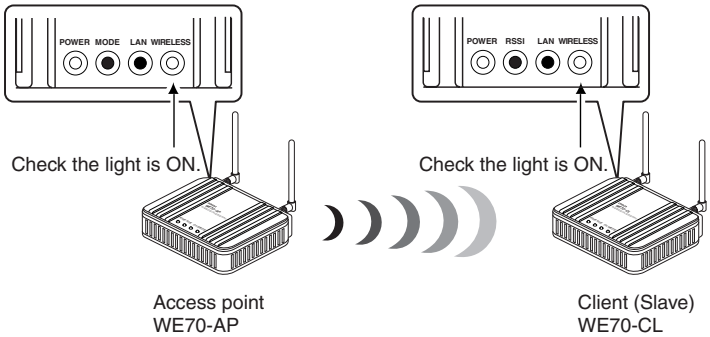
Configure an IP address through Chapter 2-3. Connection Check, IP Address Setup (P.2-10).

Step 2. Connecting

(1) Connect an access point and PC using a LAN cable.
Always use a straight cable.
(2) Connect power cables of an access point and a client (slave).
(3) Turn their power on and check indication of each POWER indicator as shown below.
Check the LAN indicator of the access point because it is connected to PC.



(4) Check if each WIRELESS indicator of the access point and the client (slave) is on in several seconds (about 8 seconds).Communication will be started as they have the same SSID and channel in their factory shipment status.



Step 3. Checking Setup Screen Access

This section describes procedures for setup screen access of a client (slave) through a WWW browser.

<Initiating Setup Screen>

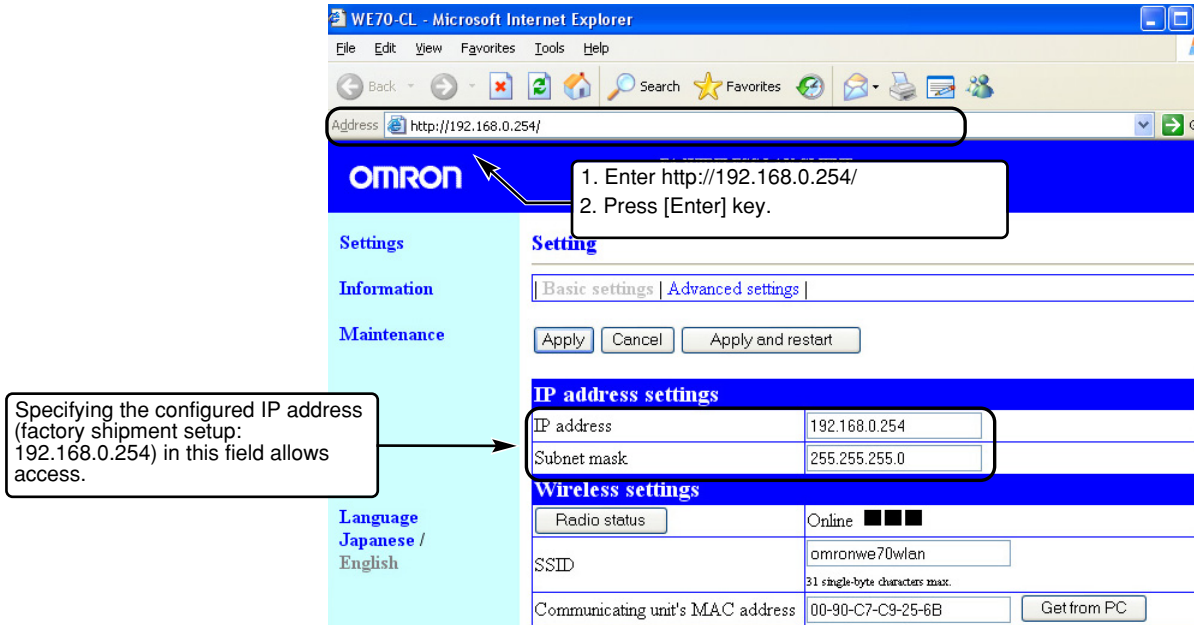
(1) Start a WWW browser.

* In this document Internet Explorer 6.0 is used.

(2) Enter the IP address specified for the client (slave) in the address bar of the WWW browser.
Enter "http://192.168.0.254/" (factory shipment status) and press [Enter] key.

• A screen in Settings menu is first displayed.

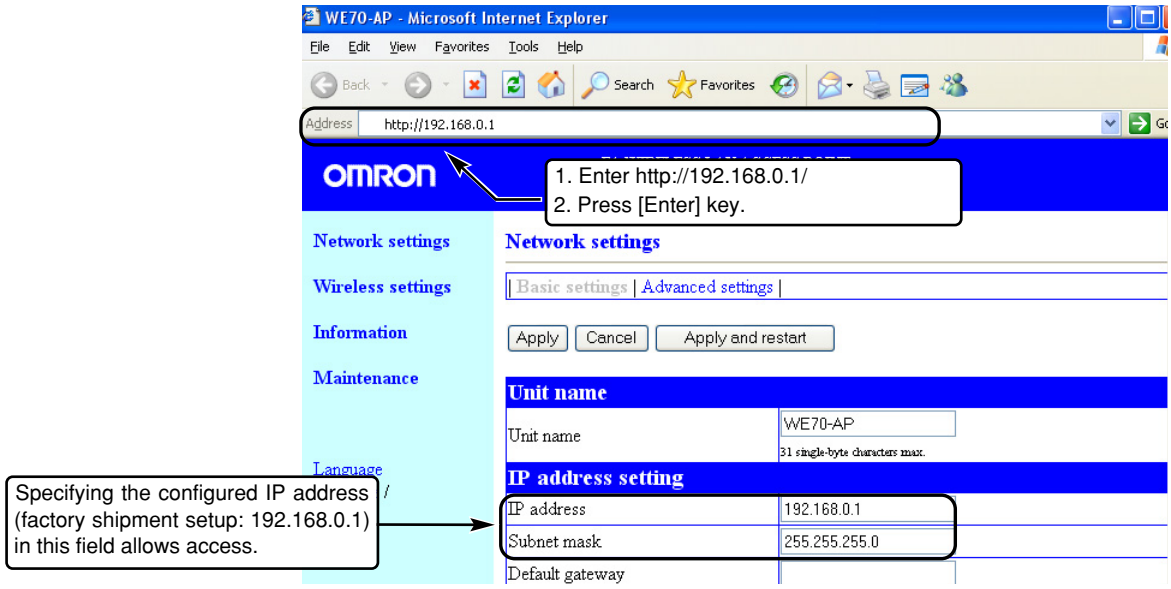
* A screen shown below indicates a factory shipment status or all-initialized status of a wireless unit.



For WE70-AP

(1) Enter the IP address specified for the access point in the address bar of the WWW browser.
Enter "http://192.168.0.1/" (factory shipment status) and press [Enter] key.Enter [admin] to user-name. and press [Enter] key ignoring a password request.

* A screen shown below indicates a factory shipment status or all-initialized status of a wireless unit.



Step 4. Monitoring Wireless Communication Status

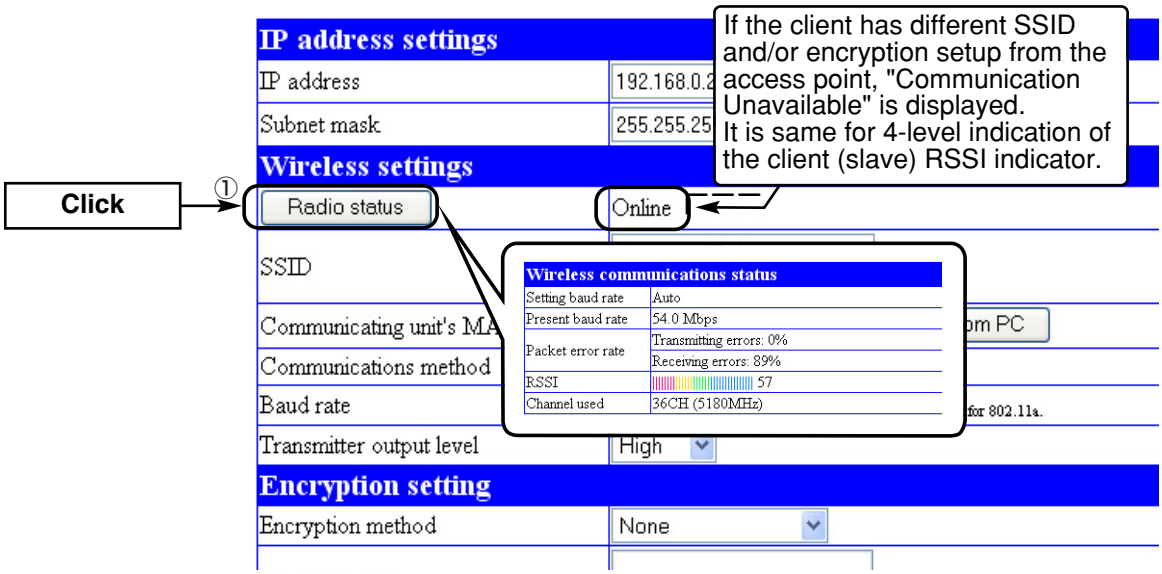
If the client is under communication with the access point, the screen displays "Online ■■■".
If not, "Communication Unavailable" is displayed.Verify a channel through which communication should be made.

* "Communication Unavailable" may be displayed until the WWW browser screen is updated in a case such as after setup change.

(1) To monitor detailed status, click <Radio status>.

• An independent screen displays Wireless communication status information.

* Information on the independent screen is updated every 0.5 seconds, while continuous monitoring increases network load.Close the screen after verification.



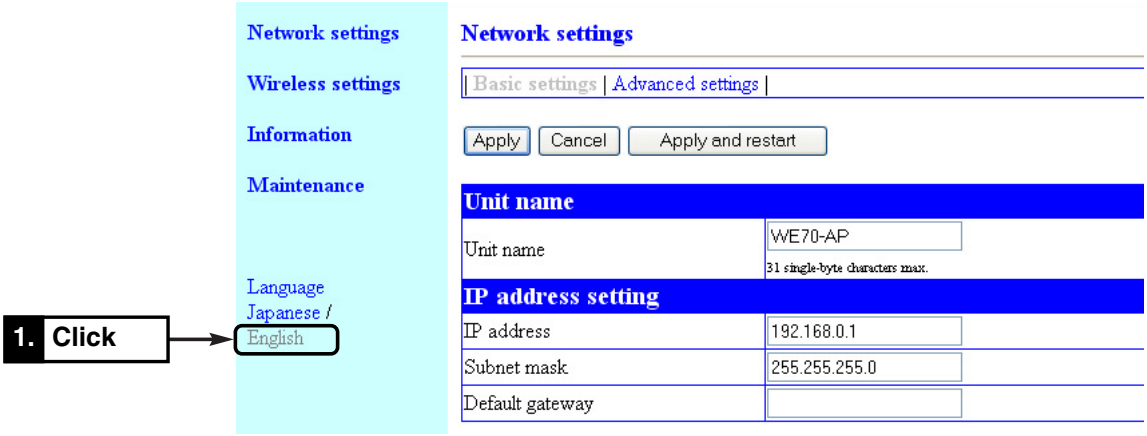
(1) <Radio Status> Button ..... Radio wave intensity that an access point can receive is displayed in the right of this button. If the client has different SSID and/or encryption setup from the access point, "Communication Unavailable" is displayed. Radio wave intensity is displayed in 4 levels as shown below.
Levels may differ depending on a communication type.

● Level: □□□ ■□□ ■■□ ■■■

0-8	9-14	15-20	21 or higher (in case of 802.11a)
0-13	14-19	20-25	26 or higher (in case of 802.11b/g)

Clicking <Radio status> allows monitoring of statuses of radio communication such as channels and communication speed in the [Wireless communication status].

■ **To display the setup screen in English.**



When the power of the wireless unit is turned ON again after turning OFF, the setup screen will be displayed in English (Default Setting).

[For Reference]

- Some wireless LAN devices may use a name ESS ID for a wireless network name, which is same as SSID.
- To check access to an access point, specify LAN-end IP address (such as 192.168.0.1) of the access point based on a procedure in 2-3. Connection Check, IP Address Setup (P.2-10).
  A setup screen of the access point is displayed.

* In case of an access point, a password input is requested.

3-3. Configuring IP Address/SSID/Channel

This section describes steps from changing setup values of an access point and a client (slave) to establishing communication.

Step 1. IP Address Setup

This section describes how to change IP address setup.

<To Configure>

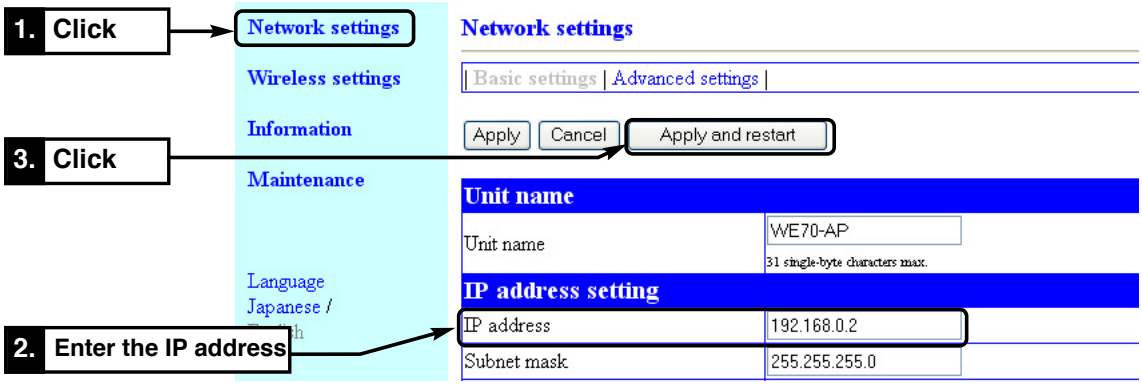
(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Network Settings menu.

(2) Change the LAN-end IP address to "192.168.0.2".

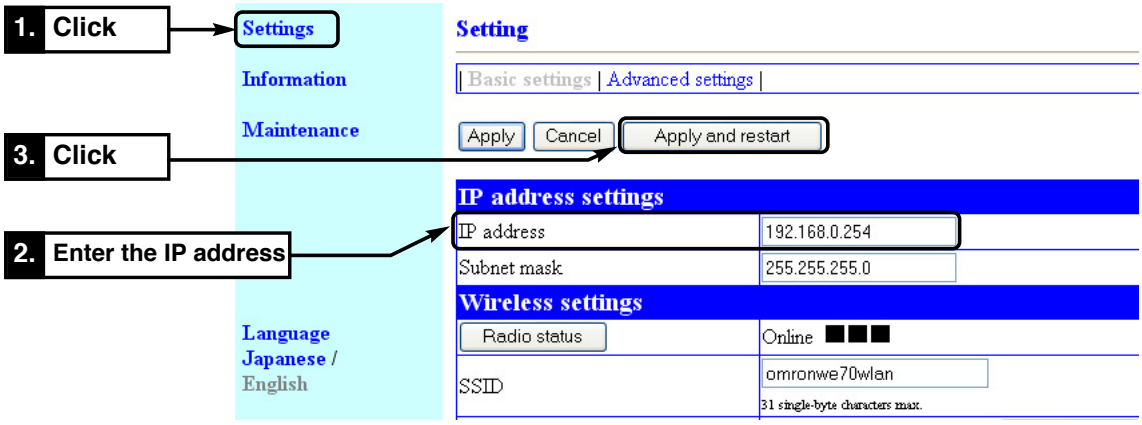
(3) Click <Apply and restart>.

After restart AP or CL, input registered IP adress to URL of IE, and open the setup screen.

Screen of WE70-AP



Screen of WE70-CL



Step 2. Configuring Wireless Network Name (SSID)

This section describes how to change a wireless network name (SSID).

● **Wireless Network Name (SSID)**

An access point and a client (slaves) have SSID (or ESS ID) as wireless network names to identify each other for communication.

If more than one wireless routers or access points exist in one wireless communication zone, cross talk with other wireless network group can be prevented by identification using different SSID (wireless network name) for each wireless network group.

A wireless LAN terminal with a SSID different from a wireless unit cannot communicate.

* If ANY-connection refusal setup is being disabled for an access point, and if a SSID of a client (slave) is blank, the client (slave) can communicate with the access point regardless of access point SSID setup.

<To Configure>

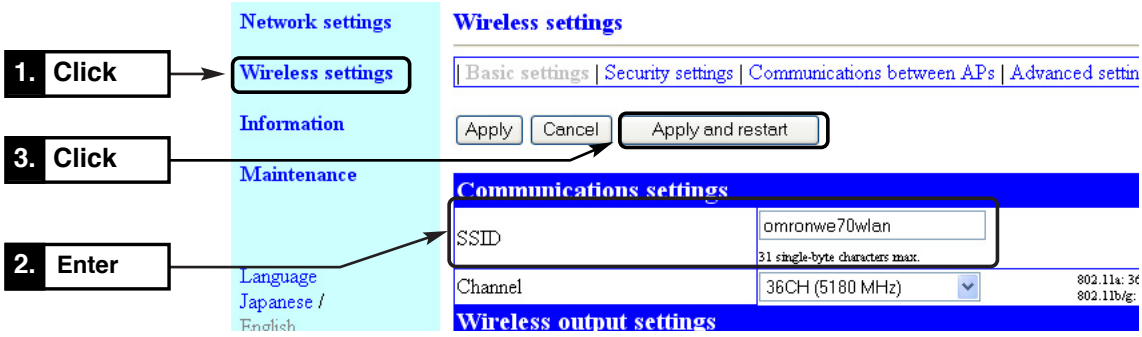
(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Wireless settings menu.
• A Wireless settings screen is displayed.

(2) Enter the desired alphanumeric characters in SSID (within 31 characters) with the attention for capitalization.
(Initial value: omronwe70wlan)

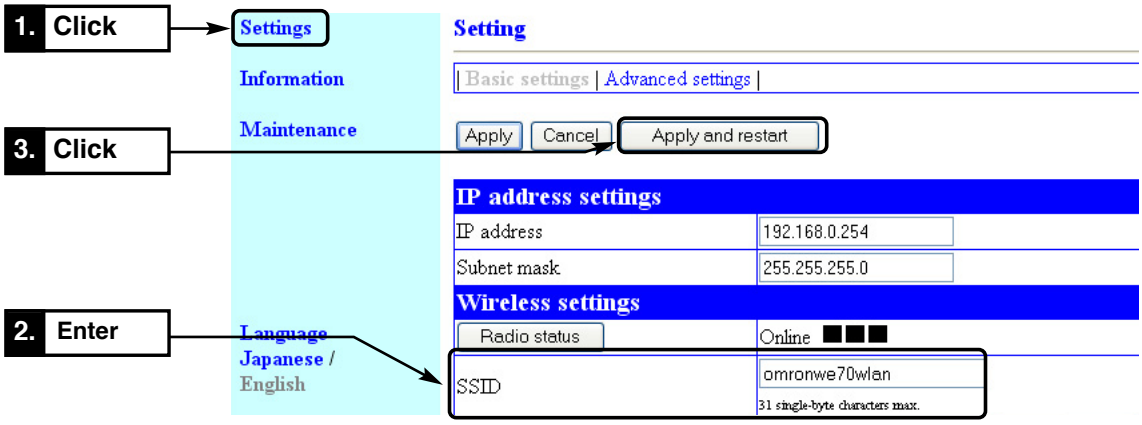
(3) Click <Apply and restart>.

* If a wireless LAN terminal is used for setup, switch the connection to the SSID configured here.

Screen of WE70-AP



Screen of WE70-CL



⚠SSID: Illegal access using "blank"

* If ANY-connection refusal setup is being disabled, and if a SSID (or ESS ID) of a client (slave) is blank, the client (slave) can communicate with the access point regardless of access point SSID setup.
* To refuse access, enable ANY-connection refusal from Wireless Setup > Detailed Communication Setup of the access point.The wireless unit's SSID will not appear on a standard wireless network connection screen of Windows XP then.

Step 3. Configuring Channel

This section describes how to change a wireless channel.
Wireless channel setup must be made on an access point.A client (slave) has no such setup, but it must be configured as the same communication type as that of the access point.The channel setup is IEEE802.11a and 36CH (5180MHz) for factory shipment status.

● Channel (frequency)

Following 24 channels can be used in 5GHz.

Except China

Channel	Frequency (MHz)	Channel	Frequency (MHz)
36CH	5180	52CH	5260
40CH	5200	56CH	5280
44CH	5220	60CH	5300
48CH	5240	64CH	5320

Except China and Japan

Channel	Frequency (MHz)	Channel	Frequency (MHz)
100CH	5500	124CH	5620
104CH	5520	128CH	5640
108CH	5540	132CH	5660
112CH	5560	136CH	5680
116CH	5580	140CH	5700
120CH	5600		

United States, Canada and China

Channel	Frequency (MHz)
149CH	5745
153CH	5765
157CH	5785
161CH	5805
165CH	5825

Following 13 channels can be used in 2.4GHz. **(Except 12CH and 13CH in United States and Canada)**

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1CH	2412	6CH	2437	11CH	2462
2CH	2417	7CH	2442	12CH	2467
3CH	2422	8CH	2447	13CH	2472
4CH	2427	9CH	2452		
5CH	2432	10CH	2457		

This is an example for connecting a PC wired LAN to a client (slave) and setup must be made from an access point to communicate.To change the setup from a client (slave), it is necessary to switch the LAN cable to the access point end.In this case, the setup screen may not be available due to specification, which can be solved by entering a command "arp -d" at command prompt of PC.

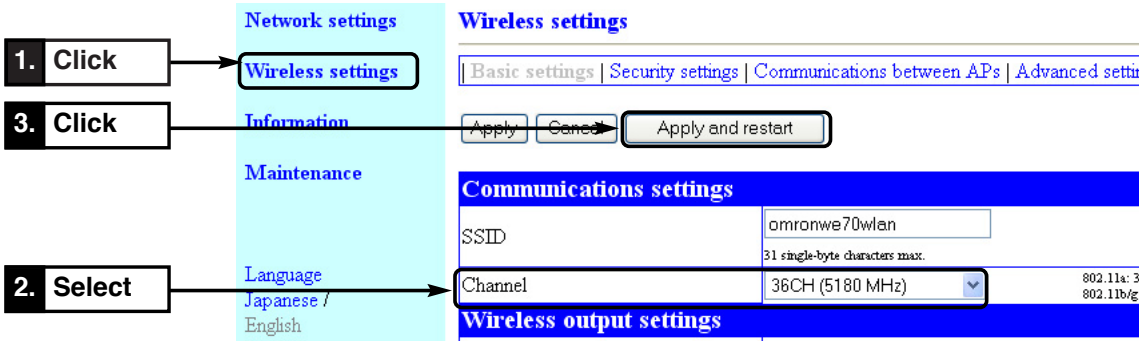
↑
Space

● **Access point setup**

(1) Open a setup screen of the access point (see Chapter 2-3. Checking Connection, Opening Setup Screen (P.2-13)) and click Wireless settings menu.
- A Wireless settings screen is displayed.

(2) Select a channel.
Example: 36CH

(3) Click <Apply and restart>.
- Communication becomes available through IEEE802.11a standard with a client (slave).

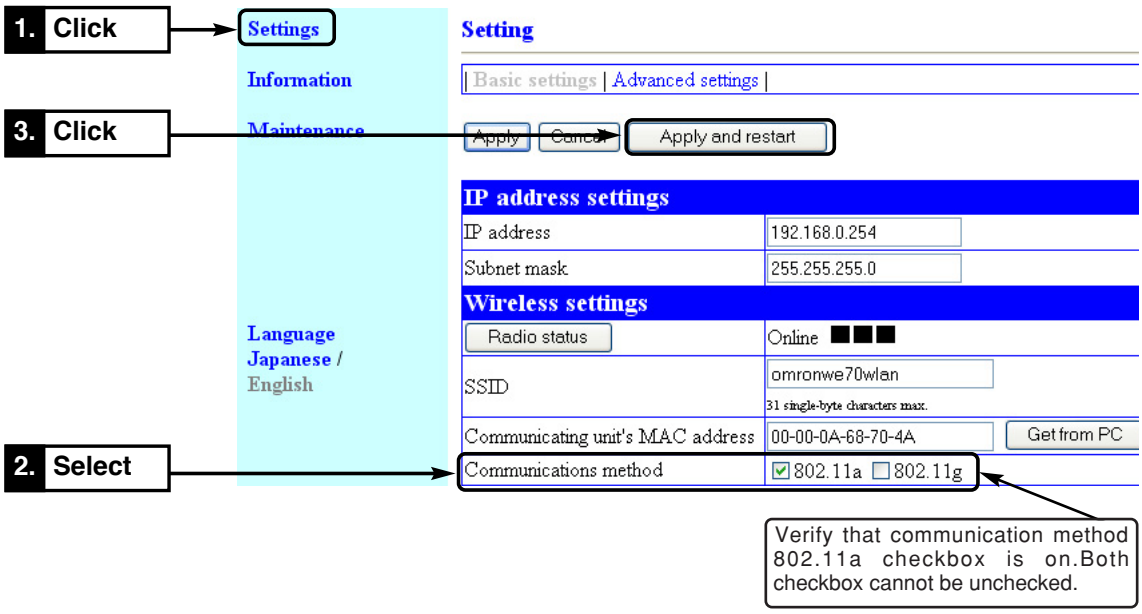


● **Client (Slave) Setup**

(1) Open a setup screen of the client (slave) (see Chapter 2-3. Checking Connection, Opening Setup Screen (P.2-13)) and click Settings menu.
- A Settings screen is displayed.

(2) Select a communication method.
Example 802.11a

(3) Click <Apply and restart>.
- Communication becomes available through IEEE802.11a standard with an access point.



⚠**Caution** The Radio Law prohibits outdoor use of wireless LAN in IEEE802.11a standard (5GHz band).

[DFS Function]

DFS function can be enabled only when an IEEE802.11a (52CH-64CH, 100CH-140CH) standard channel is set in Channel field of Communication setting. If DFS function is being enabled, detection of interfering radio waves such as a weather radar automatically changes the channel to a non-interfering IEEE802.11a standard wireless channel.
If a selected channel on startup is DFS, the [WIRELESS] indicator of a wireless unit flashes (for about 1 minute) and wireless access is inhibited before restart of the wireless unit is completed.
Any response to a client stops and access to the unit is inhibited as well.

* DFS function will not be activated if the channel is changed to non-interfering IEEE802.11a (52CH-64CH, 100CH-140CH) standard one.

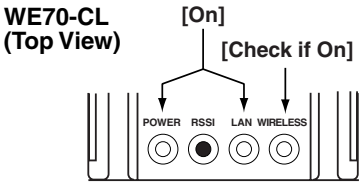
Step 4. Checking Communication

Verify that PC connected to a client (slave) can connect to an access point.

<To Verify>

Check if the [WIRELESS] indicator is on.

* If the indicator is not on as shown in the right, communication is not being established with an access point.
  If the [WIRELESS] indicator does not turn on, check wireless LAN setup of the access point and wireless unit set to be used and network setup of PC, then restart them.



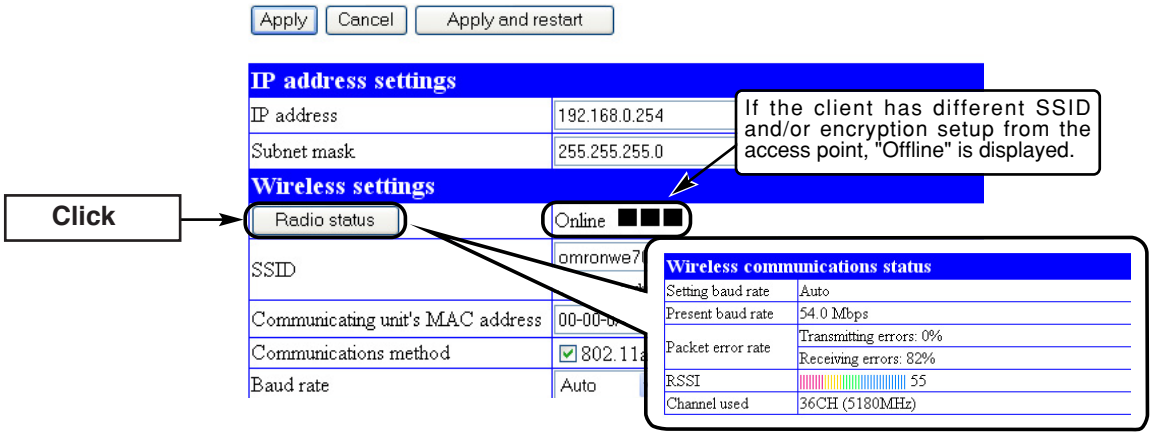
● **To monitor radio status**

(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check (P.2-13)).
- The screen displays "Online ■■■".

* "Communication Unavailable" may be displayed until the WWW browser screen is updated in a case such as after setup change.

(2) To monitor detailed status, click <Radio status>.
- An independent screen displays Wireless communication status information.

* Information on the independent screen is updated every 0.5 seconds, while continuous monitoring increases network load.Close the screen after verification.



[For Reference]

- To check access to an access point, specify LAN-end IP address (such as 192.168.0.1) of the access point based on a procedure Checking Connection, Opening Setup Screen (P.2-13).
- A setup screen of the access point is displayed.

* If access is controlled by a password, a message is displayed that requires password input.

Step 5. Other Setups

For details of setup, see Chapter 5 Setup Menu.

3-4. Configuring Encryption

WEP (RC4)/OCB AES encryption key setup can be configured by directly entering hexadecimal number or ASCII characters in the WEP key text box or entering any alphanumeric characters or symbols in the Key generator text box.The key generator automatically generates 4 encryption keys, one of which to be used can be specified in the Key index.

* For encryption setup of TKIP, AES, and WOC KEY, see P.3-18.

■ To Enter Encryption Key Using ASCII Characters

Suppose following conditions to configure.

◎ Encryption method: WEP RC4, 128 (104) bits
◎ Key index: 1 (Factory Shipment Setting)
◎ Input Mode: ASCII character 13 character, hexadecimal number.

* Some wireless LAN devices may use names authentication mode and key ID, which are same as network authentication and key index.

<To Configure>

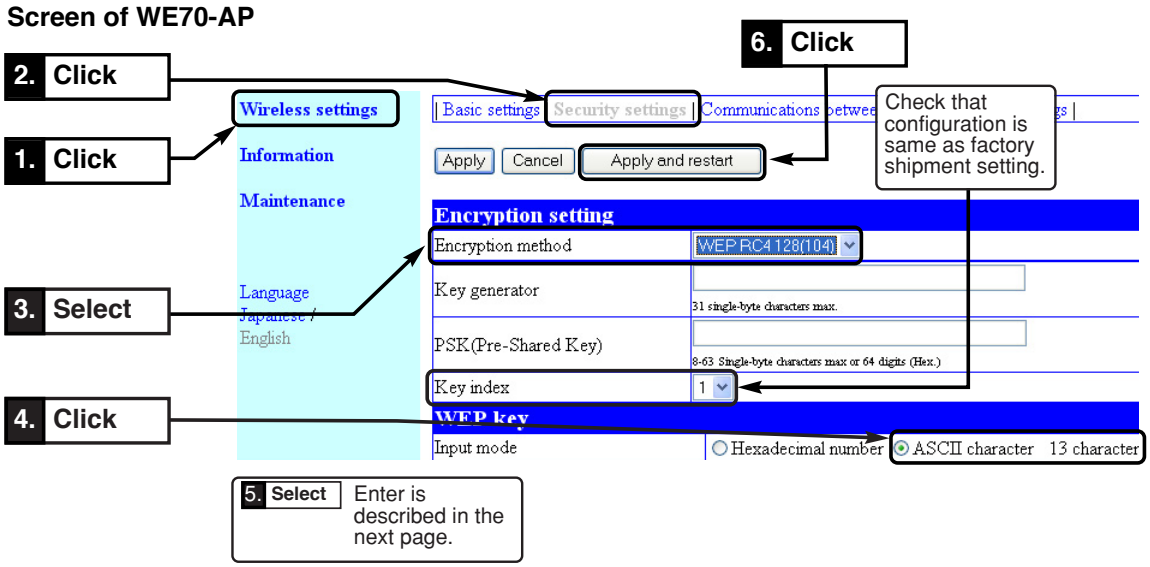
The same setup must be applied to a client (slave) for communication.

(1) Open a setup screen of the access point (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Wireless setting menu > Security settings.
• A Security setting screen is displayed.

(2) Set Encryption method as WEP RC4 128 (104).
* If None (Factory Shipment Setting) is set, data will not be encrypted.

(3) In Input mode field of WEP key, click ASCII character 13 character radio button.

Screen of WE70-AP



[Key Index Setup]

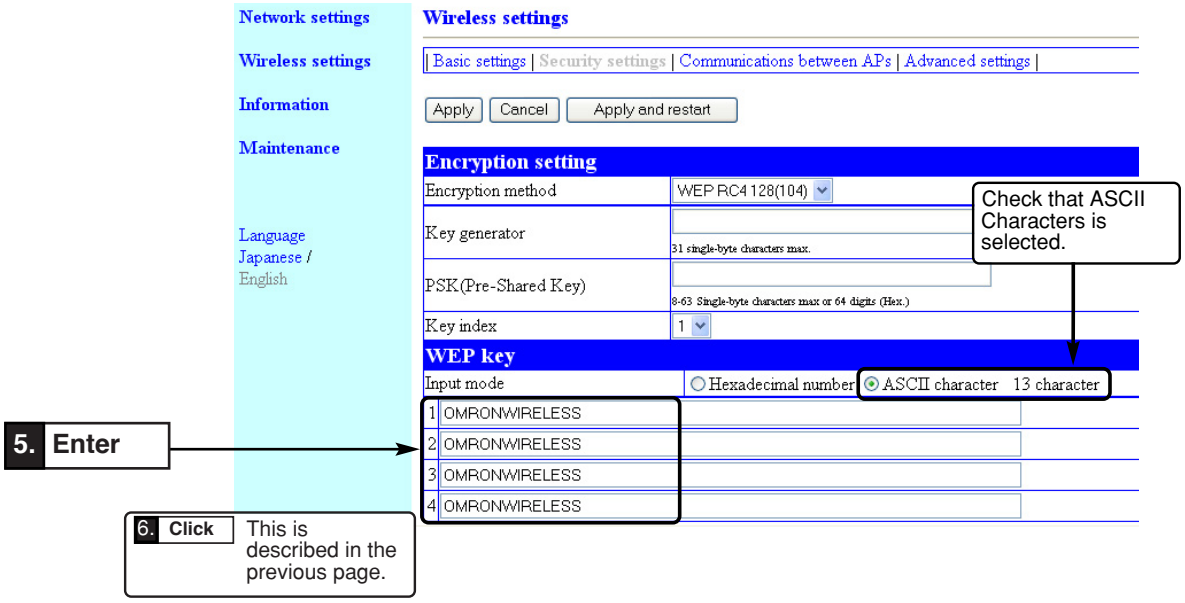
(Excluding Windows XP with Service Pack Applied)
A range of Key index (key IDs) is from 1 to 4 for Omron's wireless devices, while that for standard wireless network connection in Windows XP is from 0 to 3.
Selecting "1" for a wireless unit is same as specifying "0" in Key index (advanced) in Windows XP.

(4) Enter WEP key in text boxes from 1 to 4 of Key Index using ASCII characters.(Example: OMRONWIRELESS)

* A WEP key must be configured as the same for communication in a text box of the same number even if key indexes are different for those that communicate.

(5) Click <Apply and restart>.

• Setup is now being enabled.



■ Entering Encryption Key

Number of encryption key digits depends on encryption method and input mode setting:

[Wireless LAN standard: IEEE802.11a /b/g]

Network Authentication		Input Mode / Encryption method	(HEX.)	ASCII Character
Open System	Shared Key	WEP RC4, 64 (40) bits	10 digits	5 characters
		WEP RC4, 128 (104) bits	26 digits	13 characters
		WEP RC4, 152 (128) bits	32 digits	16 characters
		OCB AES, 128 (128) bits	32 digits	16 characters

* Number of digits available for input is indicated in ( ).

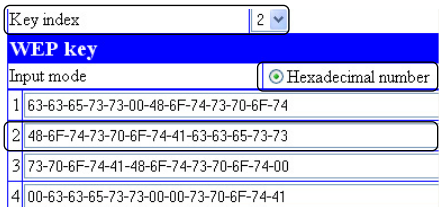
■ Setup Example of Encryption Key

This section describes how to configure encryption keys for an access point and a client (slave) by directly entering hexadecimal number (26 digits) in case of RC4, 128 (104) bits.。

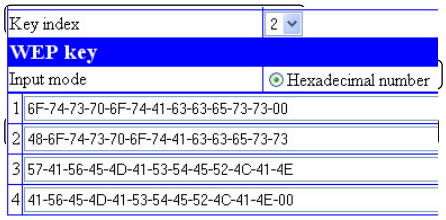
[Ex.] Enter "48-6f-74-73-70-6f-74-41-63-63-65-73-73" and "57-41-56-45-4d-41-53-54-45-52-4c-41-4e" to key IDs 2 and 3 as shown below.

◎ WEP key values in key index 2 are same and communication is available.

WE70-AP End

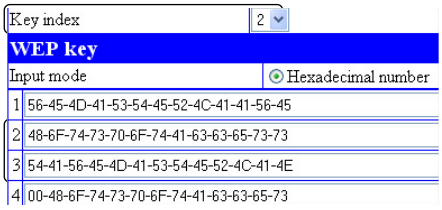


WE70-CL End

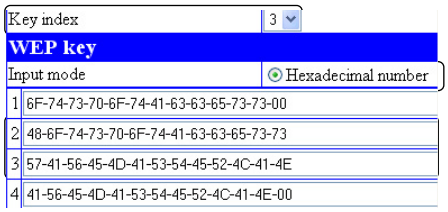


◎ WEP key values in key indexes 2 and 3 are same and communication is available.

WE70-AP End

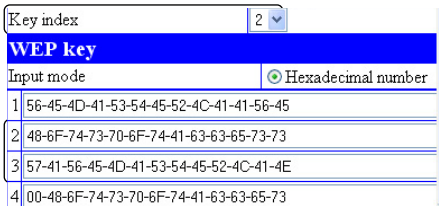


WE70-CL End

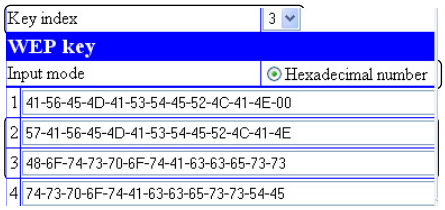


◎ WEP key values in key indexes 2 and 3 are different and communication is unavailable.

WE70-AP End



WE70-CL End



■ To Enter Encryption Key Using hexadecimal number

Suppose following conditions to configure.

◎ Encryption Method: WEP RC4, 128 (104) bits
◎ Key Index: 1 (Factory Shipment Setting)
◎ Input Mode: Hexadecimal number (Factory Shipment Setting)

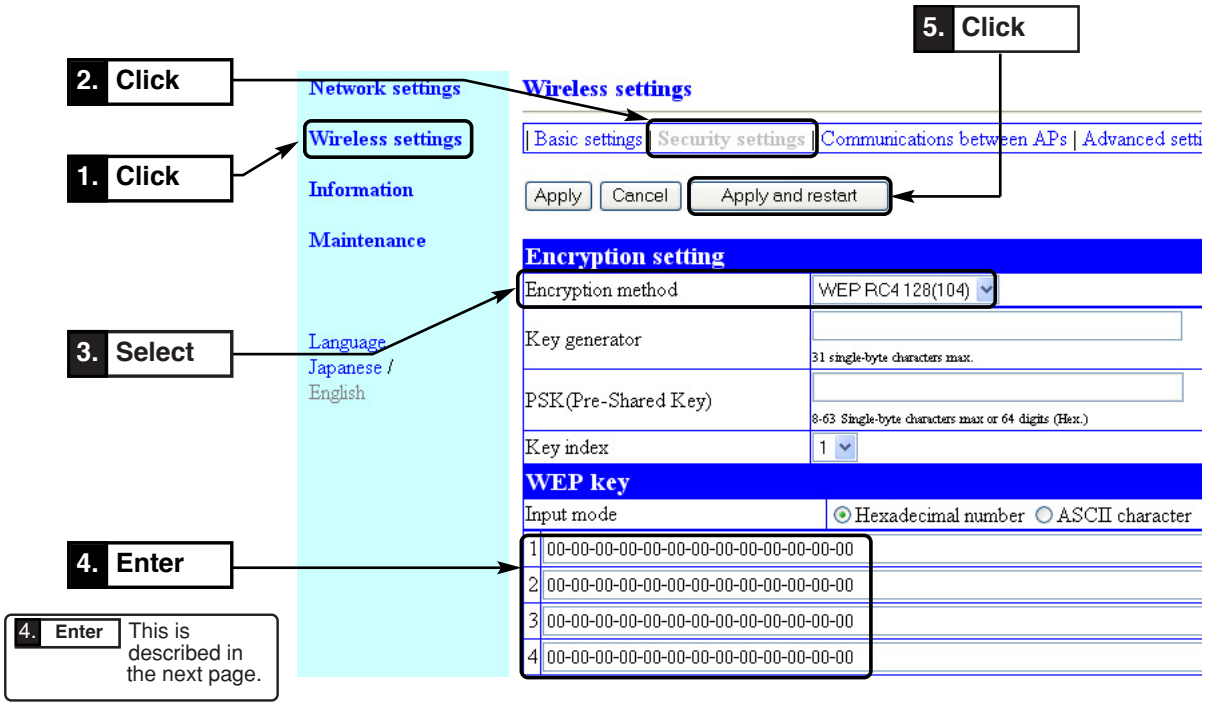
* Some wireless LAN devices may use names authentication mode and key ID, which are same as network authentication and key index.

<To Configure>

The same setup must be applied to a client (slave) for communication.

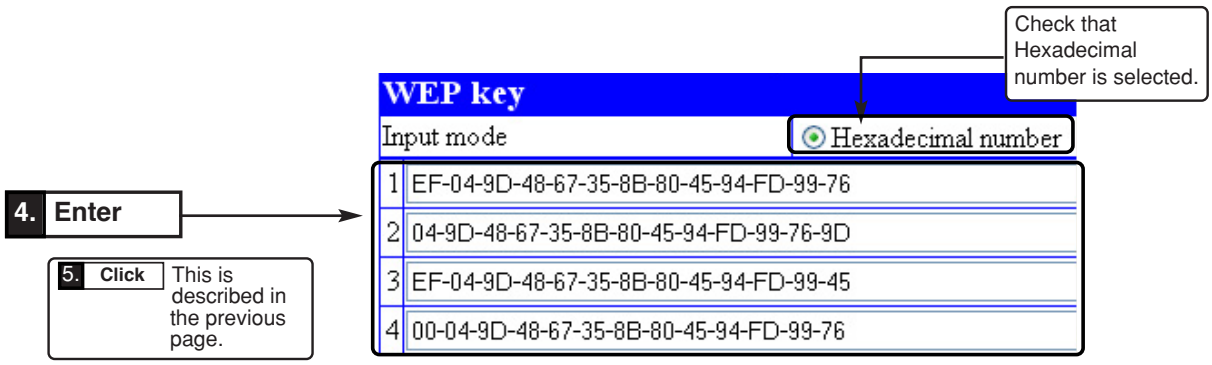
(1) Open a setup screen of the access point (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Wireless setting menu > Security settings.
• A Security settings screen is displayed.

(2) Set Encryption method as WEP RC4 128 (104).
* If None (Factory Shipment Setting) is set, data will not be encrypted.



(3) Enter WEP key in text boxes from 1 to 4 of Key index using hexadecimal numbers.
(Input Example 1: EF-04-9D-48-67-35-8B-80-45-94-FD-99-76)
(Input Example 2: EF049D4867358B804594FD9976)
* Results are the same for either examples.
* Communication is available when the same WEP key is set in a text box of the same number even if key indexes are different from a client (slave).

(4) Click <Apply and restart>.
• Setup is now being enabled.



■ Conversion Table from ASCII Character to hexadecimal number

If your PC supporting wireless LAN does not support both modes, use the following conversion table to specify a key to set.

[Ex.] "4f4d524f4e574952454c455353" (26 digits) in hexadecimal number is "OMRONWIRELESS" (13 characters) ASCII characters.

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

■ To Generate Encryption Key Using Key Generator

This function can be used to set "Hexadecimal number" (factory shipment setting) to Input Mode field of WEP Key.

* Entering any character string into the key generator automatically generates encryption keys in WEP Key text boxes.
* The key generator is incompatible with other manufacturers' products than Omron's.

Suppose following conditions to configure.

◎ Encryption method: WEP RC4, 128 (104) bits
◎ Key generator: OMRON
◎ Input Mode: Hexadecimal number (Factory Shipment Setting) * ASCII characters cannot be used.

* Some wireless LAN devices may use names authentication mode, which is same as network authentication.

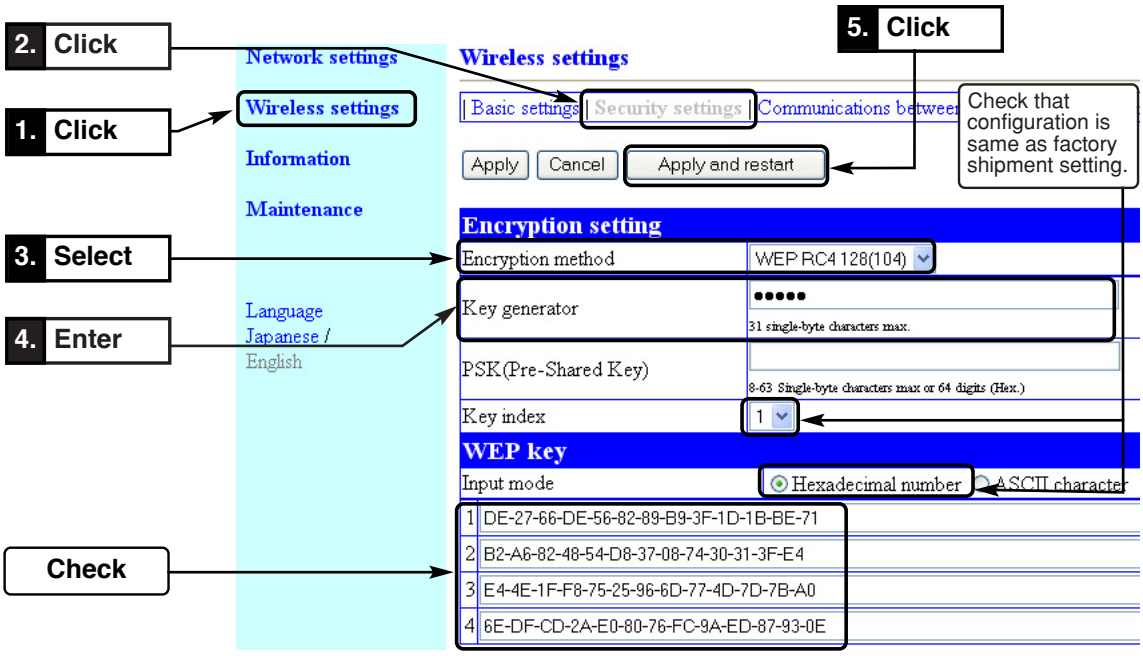
<To Configure>

(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Wireless settings menu > Security settings.
• An Encryption method screen is displayed.

(2) Set Encryption method as WEP RC4 128 (104).
* If None (Factory Shipment Setting) is set, encryption security is disabled.

(3) Enter an alphanumeric numbers or symbols (within 31 characters) in Key generator field.

(4) Click <Apply and restart>.



■ To Configure TKIP/AES/WOC KEY Encryption

TKIP and AES encryption key setup can be configured by entering 64-digit hexadecimal number or 8 to 63 ASCII characters.For WOC KEY, only 8 to 63 alphanumeric characters can be used, while 64-digit hexadecimal number cannot.

* For encryption setup for WEP (RC4)/OCB AES, see Chapter 3-4. Configuring Encryption (P.3-12).

Suppose following conditions to configure.

◎ Encryption method: TKIP

◎ PSK (Pre-Shared Key): OMRONWE70 (Use 8 to 63 ASCII characters)

<To Configure>

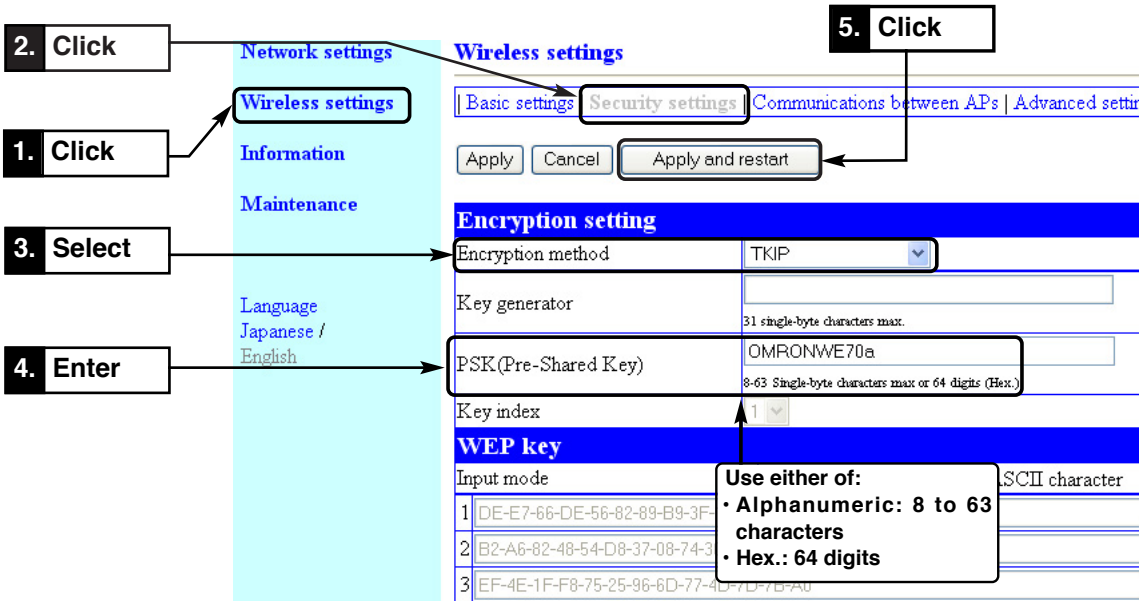
The same setup must be applied to a client (slave) for communication.

(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Wireless settings menu > Security settings.

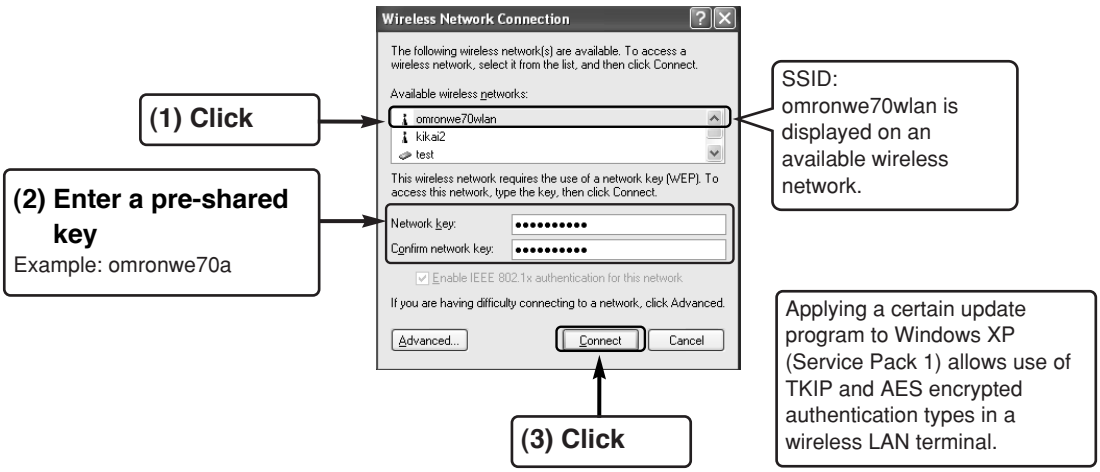
(2) Set Encryption method as TKIP.
* If None (Factory Shipment Setting) is set, data will not be encrypted.

(3) Enter OMRONWE70a in PSK (Pre-Shared Key).

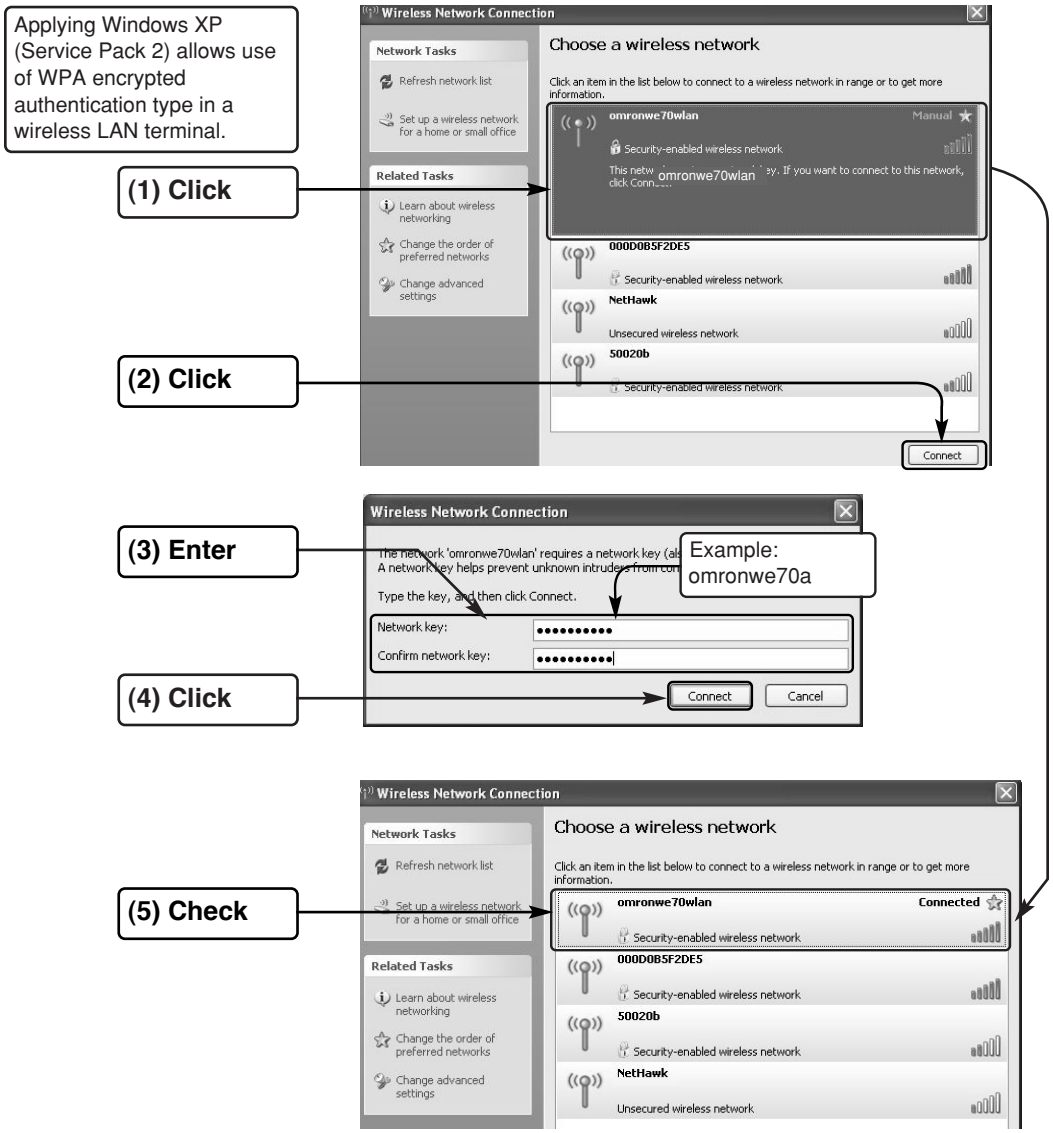
(4) Click <Apply and restart>.Setup is now being enabled.



<Wireless LAN Terminal End: Connection Example for Windows XP (Service Pack 1)>



<Wireless LAN Terminal End: Connection Example for Windows XP (Service Pack 2)>

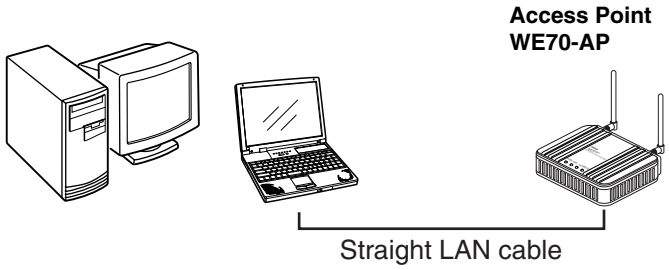


3-5. Communicating with PLC

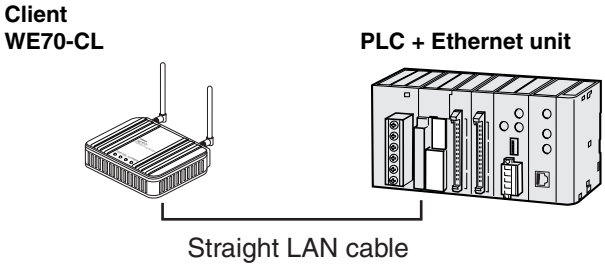
This section describes how to set communication between an access point (WE70-AP) and a client (WE70-CL).A PLC + Ethernet unit must be connected to an access point using a LAN cable.PC with Ethernet card must be connected to a client (WE70-CL).

Step 1. Preparing PLC & PC

PLC is connected to Access point using straight LAN cable.

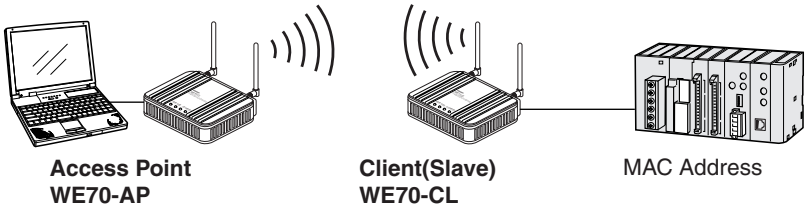


A client (slave) can be configured by direct connection of a LAN cable or wireless connection by entering "192.168.0.254" (factory shipment setting) to PC connected to an access point.
To connect a PLC to an Ethernet network, 100BASE-TX type Ethernet unit CS1W-ETN21 or CJ1W-ETN21 is required.



Network Device	Description
CS series Ethernet unit (CS1W-ETN21) CJ series Ethernet unit (CJ1W-ETN21)	A communication unit to connect a CS series or CJ series PLC to a 100BASE-TX type Ethernet network.
LAN Cable	A LAN cable with RJ45 modular connectors on both ends,used to connect a 100BASE-TX type Ethernet unit and an access point. An STP (shielded twisted pair) cable of category 3, 4, 5, or 5e must be used.

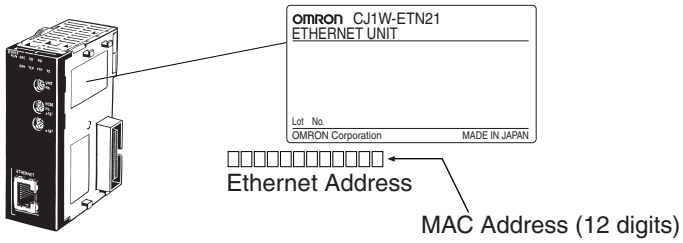
Step 2. MAC Address Setup



To attach PLC connected to WE70-CL to network, a client (slave) needs a setup as follows. Specifying a MAC address (Ethernet address) of PLC's Ethernet unit to Terminal MAC Address field for WE70-CL.

> ⚠ **Caution** Only 1 model connected to WE70-CL can be registered to Terminal MAC Address.If more than one model is connected, it is necessary for PLC2 to issue a ping to PLC1 provided as an FINS command.

Ex. For Ethernet unit CJ1W-ETN21, Ethernet address is indicated at the right side.



Step 3. PLC Setup

To connect a PLC to a network, Ethernet unit's IP address must be configured.A unique IP address must be allocated for each communication node,using either of the followings:

1. Specifying with a default IP address

A rotary SW in the Ethernet unit can specify a FINS node address (1 to 254), which is used as a host block of the IP address. A FINS node address and an IP address to be specified for an Ethernet unit have the following relationship:
192.168.250.FINS_Node_Address
That is, specifying a node number 10 to a network of 192.168.250.* sets an IP address of 192.168.250.10 by default.

2. Specifying by Unit Setup of CX-Programmer

From I/O Table window of online CX-Programmer, select an Ethernet unit and specify an IP address from Unit Setup.

3. Specifying by CPU advanced function unit assignment DM area

Under a status of an IP address unconfigured for Unit Setup, specify an IP address to IP Address Display/Setup Area of CPU advanced function unit assignment DM area.

By default, IP addresses of an access point and a client are:
Access Point (WE70-AP): 192.168.0.1
Client (WE70-CL): 192.168.0.254
For details, see CS1W-ETN21/CJ1W-ETN21 Ethernet Units Construction of Networks Operation Manual(W420-E1), Section 5-2. IP Address in FINS Communications.

Step 4. Checking Communication with PLC

Check if communication is available between WE70 and PLC.

Execute a ping command from your PC at command prompt.

Example: Ping 192.168.0.10 (PLC's IP addresses)

```
C:\>ping  192.168.0.10

Pinging  192.168.0.10  with  32  bytes  of  data:

Reply  from  192.168.0.10:  bytes=32  time<1ms  TTL=250
```


■ Precautions for Communication with PLC

● High Load in FINS Communication

Constructing an application using the FINS communication service function may lead to a communication failure (frequent response timeout) due to high load depending on a system configuration and an application program.

For details, see CS1W-ETN21/CJ1W-ETN21 Ethernet Units Construction of Networks Operation Manual(W420-E1), Section 5-2. IP Address in FINS Communications.

● Using FL-NET

It is not recommended to use the WE70 to make FL-NET communication wireless. Communication errors may occur due to lost frames.

Advanced Setup

Chapter 4

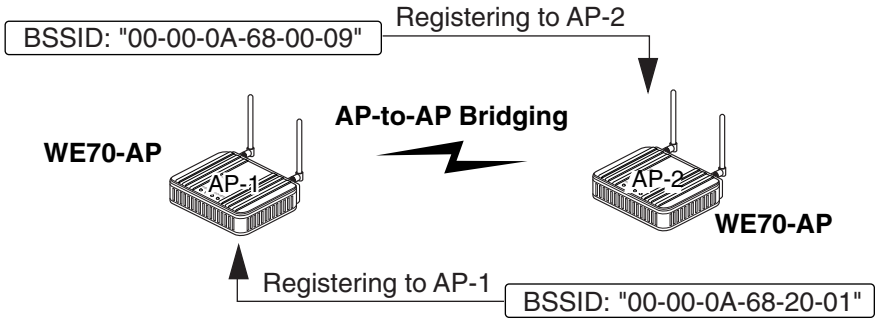
This chapter describes
setup for communication between access points or communication between clients through an access point, as well as setup for stable communication.

4-1. To Use AP-to-AP Bridging.....4-2
■ Communication with 2 or More Access Points 4-2
■ To Register BSSID 4-4
4-2. AP-to-AP Bridging Setup.....4-5
Step1. Configuring IP Address 4-5
Step2. Checking Own & Partner SSIDs 4-6
Step3. Checking Wireless Channel.....4-6
Step4. Checking Own & Partner BSSIDs 4-6
Step5. Checking Partner BSSID 4-7
Step6. Checking Receiving electric field strength 4-8
Step7. Checking AP-to-AP Bridging 4-9
4-3. Configuring Relay Function (Pattern A).....4-10
Step1. Changing Access Point SSID 4-11
Step2. Configuring Client IP Address 4-11
Step3. Checking Communication 4-12
Step4. Configuring Client-PLC Communication 4-13
Step5. PLC Setup 4-14
Step6. Checking PC-PLC Communication 4-14
4-4. Configuring Relay Function (Pattern B).....4-15
Step1. Configuring Smart Roaming.....4-16
Step2. Checking Smart Roaming 4-16
Step3. Checking PC-PLC Communication 4-17
4-5. To Set up MAC Address Filtering 4-18
4-6. Using Spanning Tree Function 4-19
■ Configuring Spanning Tree Function.....4-19
4-7. Using CL-to-CL Communication via AP 4-20
4-8. Limiting IEEE802.11b Communication 4-21
4-9. Smart Roaming 4-22
■ Scanning Frequency 4-22
■ Smart Roaming for 802.11a 4-22
■ Smart Roaming for 802.11b/g 4-23
4-10. Configuring Smart Roaming 4-24
Step1. Configuring IP Address 4-24
Step2. Changing Own & Partner SSIDs 4-25
Step3. Checking Wireless Channel.....4-26
Step4. Configuring Client-PLC Communication 4-26
Step5. PLC Setup 4-27
Step6. Configuring Smart Roaming.....4-28
Step7. Checking Smart Roaming 4-28
Step8. Checking PC-PLC Communication 4-29

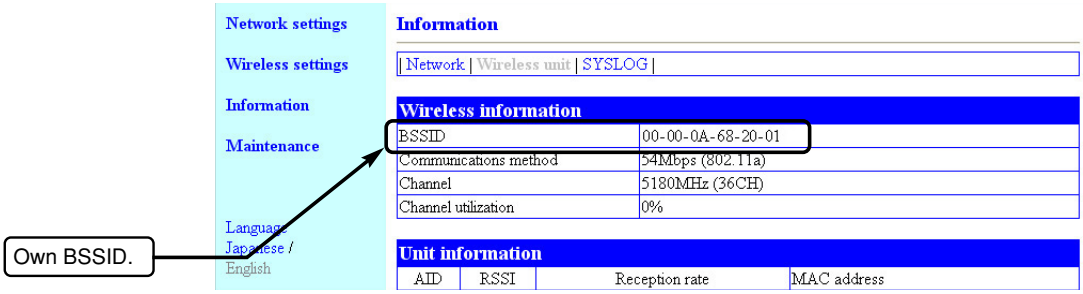
4-1. To Use AP-to-AP Bridging

Communication through AP-to-AP bridging can be made by registering partner access point's BSSID.
It is not necessary to use the same SSID, but using the same SSID as an initial value (factory shipment status) allows automatic detection and registration of partner access point's BSSID.

* AP-to-AP bridging cannot work until partner's BSSID is registered.
* All access points that use AP-to-AP bridging must be configured to use the same channel.
* Do not connect access points to the same wired network after configuring AP-to-AP bridging.
  It may lead to looping, resulting in a network failure.



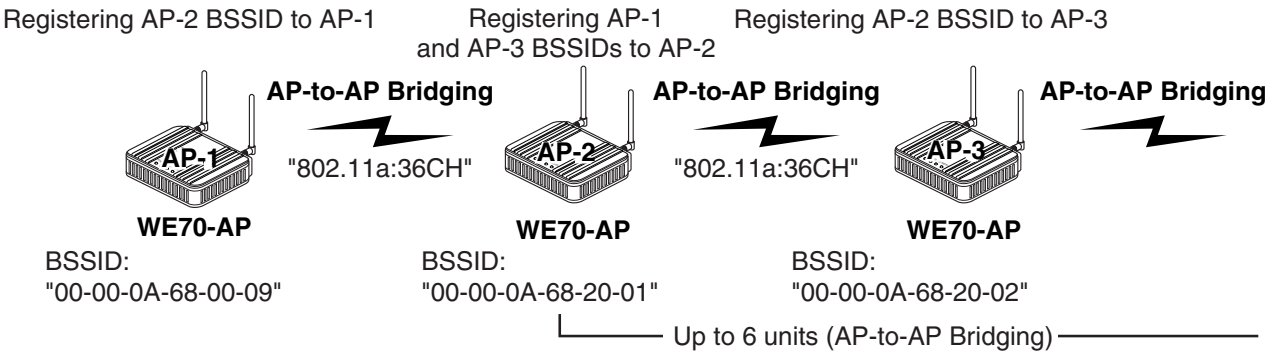
Setup screen by "Information" menu, "Wireless unit"



■ Communication with 2 or More Access Points

Register access point BSSIDs of the other part of communication. In an example below, BSSIDs of AP-1 and AP-3 are to be registered to AP-2. A channel of all access points must be configured as the same.
The maximum number of access points which simultaneous AP-to-AP bridging is available is 7 (including your own PC. The maximum number of relays: 6).

Example1. Communication via Repeater

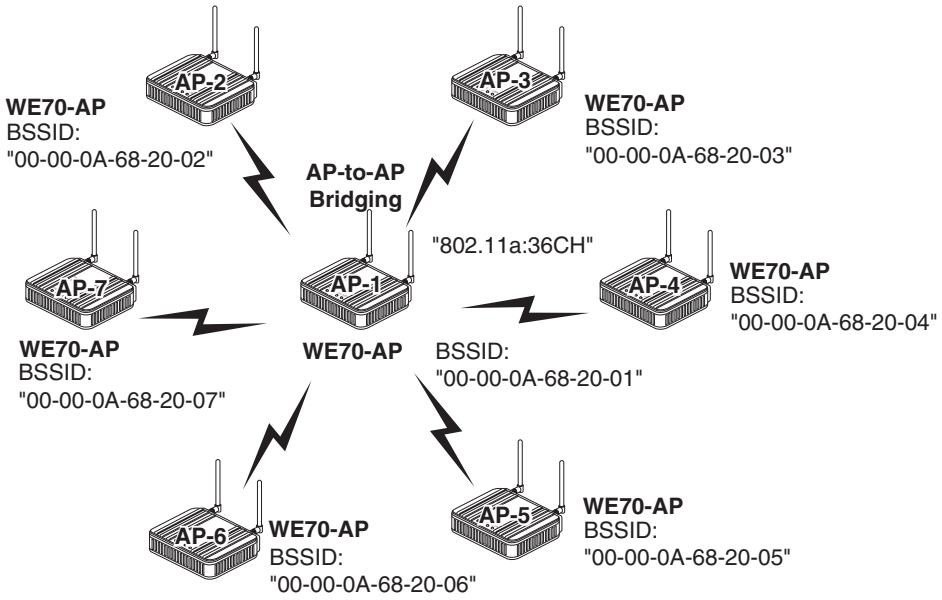


All throughput is 1/6(1/ access number) by AP-to-AP Bridging.

Example 2. Communication with 2 or More Access Points

Register all partner access point BSSIDs. In an example below, BSSIDs from AP-2 to AP-7 are to be registered to AP-1. Channels of all access points must be configured as the same. Up to 6 BSSIDs can be registered to 1 access point.

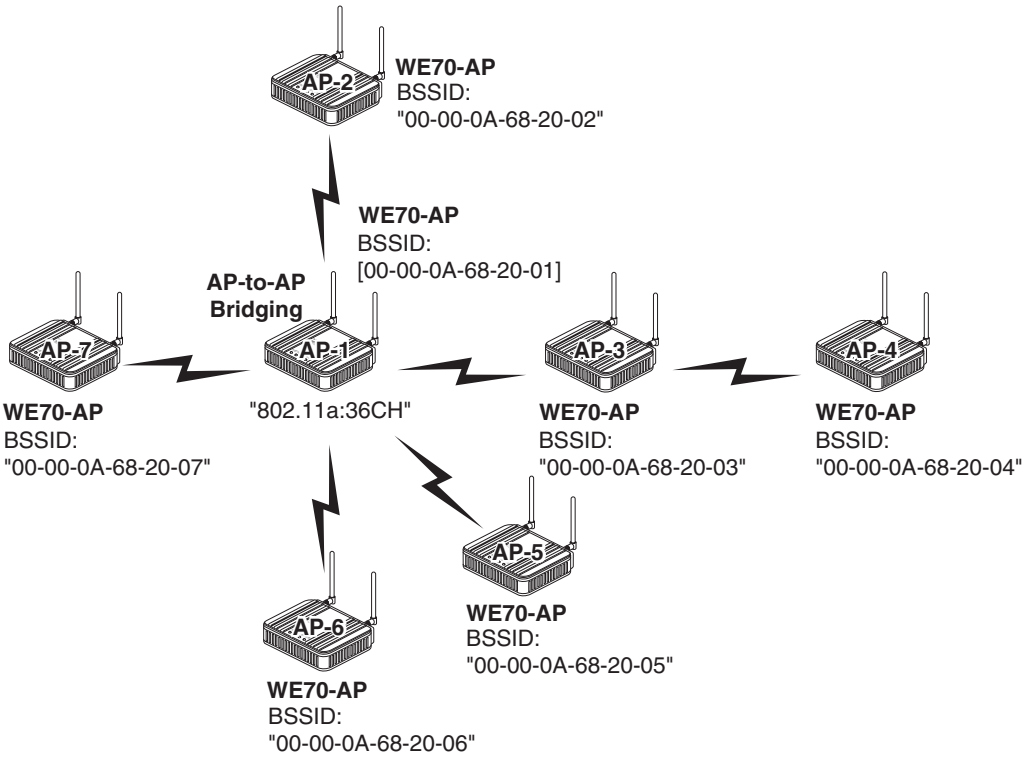
The maximum number of access points which simultaneous AP-to-AP bridging is available is 7 (including your own PC).



Example 3. Communication with 2 or More Access Points via Repeater

Register access point BSSIDs of the other part (partner) of communication. This is a combination of the examples 1 and 2.

The maximum number of access points which simultaneous AP-to-AP bridging is available is 7 (including your own PC).



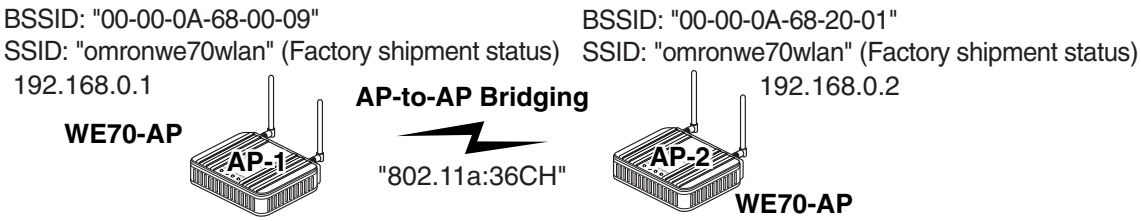
All throughput is 1/6(1/ access number) by AP-to-AP Bridging.

■ To Register BSSID

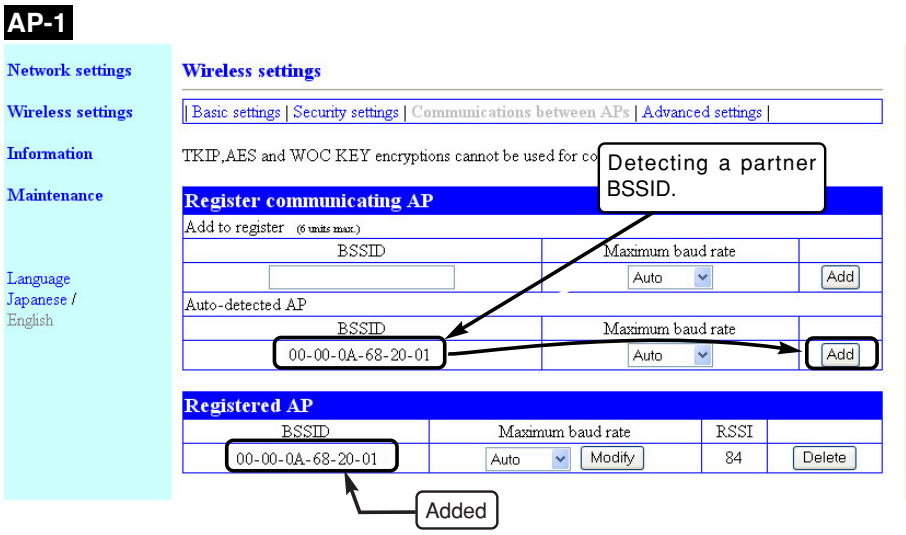
A BSSID can be registered in two ways; automatic detection and manual input.

●Automatic Detection

Configuring the same channel and SSID for AP-1 and AP-2 allows automatic detection of BSSID of partner, making registration easier. Register AP-1 BSSID to AP-2 as well.

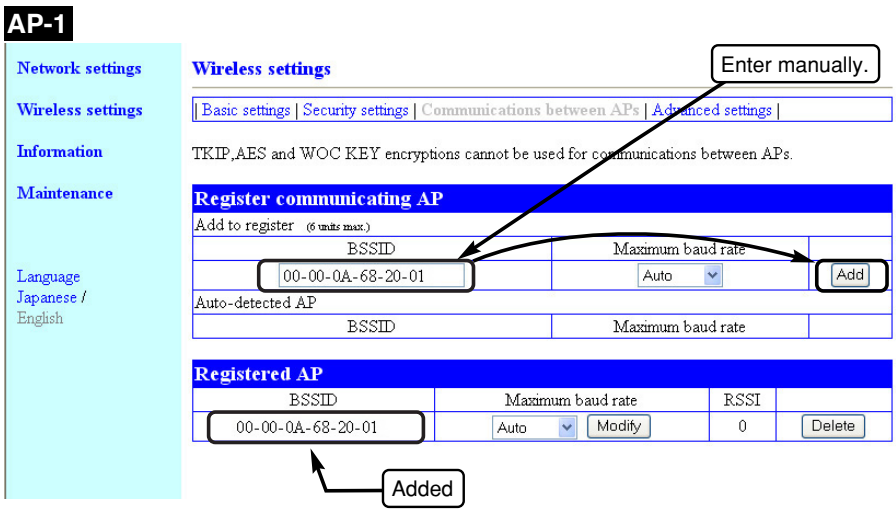


"Wireless Settings" Menu > "Communications between Aps" Setup Screen
If SSIDs and channels are the same, the screen displays a BSSID, which can be registered by clicking "Add".



● Manual Input

Verify BSSIDs for AP-to-AP bridging from "Information" menu, "Wireless settings" setup screen, and configure AP-2 BSSID by manual input. If SSIDs of access points AP-1 and AP-2 are unmatched, enter it manually for registration.



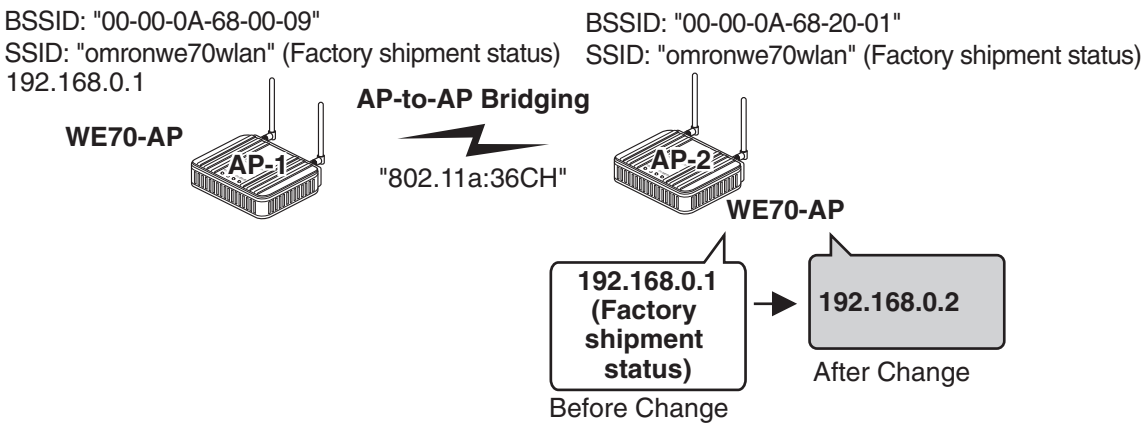
[For Reference] Detection of BSSID

Configuring the same SSID (factory shipment status: omronwe70wlan) and channel with a partner allows detection of partner BSSID.

This makes registration of partner BSSID easier for new registration and switching.
* Enter the desired alphanumeric characters in SSID (within 31 characters) with the attention for capitalization.
* As this configuration of the same SSID is for detection of BSSID only, it does not affect AP-to-AP bridging for those with a different SSID value.
* To use encryption, the same encryption key must be configured for the wireless units.
* "TKIP", "AES", and "WOC KEY" encryption methods cannot be used at the same time with AP-to-AP bridging.
* To use AP-to-AP bridging with configuration of [WEP (RC4), OCB AES] and [Super AG] as [Yes (Compressed)], a key index must be configured as same as those that use AP-to-AP bridging. Communication is unavailable if different key indexes are configured.

4-2. AP-to-AP Bridging Setup

This section describes how to configure and verify basic AP-to-AP bridging setup in steps from 1 to 7 below:

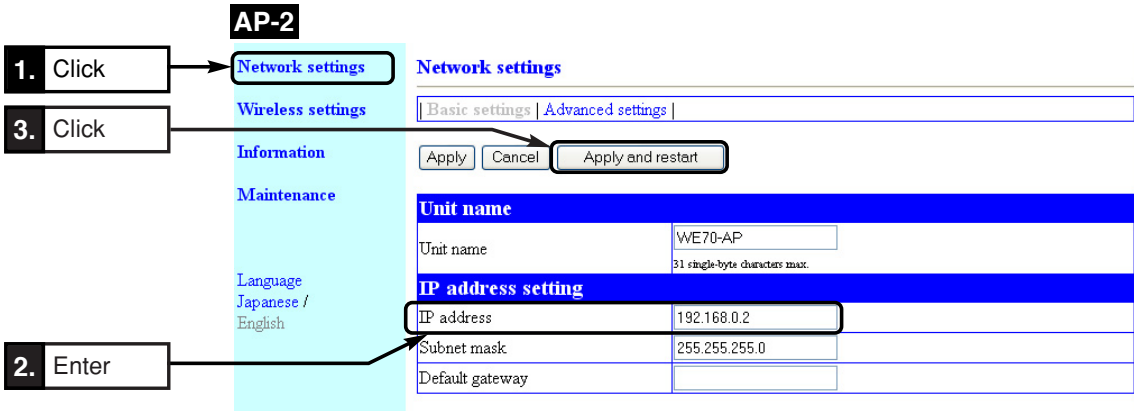


Step 1. Configuring IP Address

Change access point AP-2 IP address.
Leave AP-1 as 192.168.0.1.

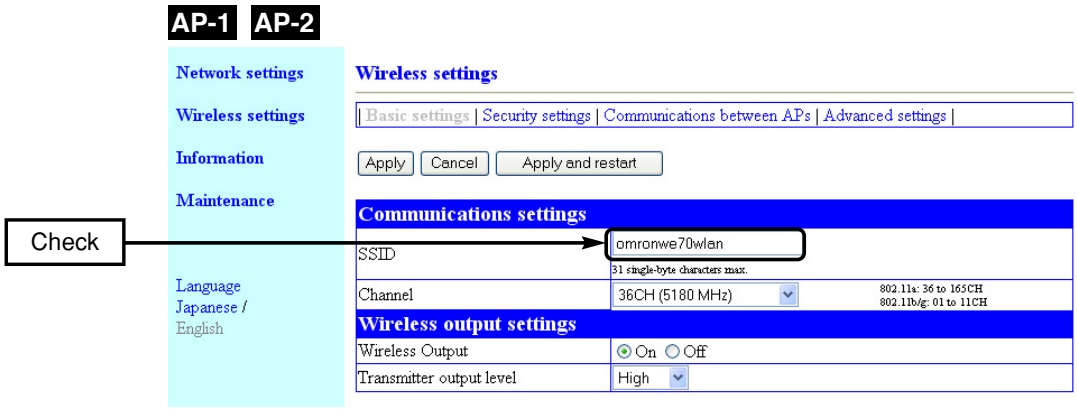
<To Configure>

(1) Open a setup screen of AP-2 (see Chapter 2-3. Connection check, Opening Setup Screen (P.2-13)) and click Network settings menu.
(2) Change the IP address to "192.168.0.2".
(3) Click <Apply and restart>.



Step 2. Checking Own & Partner SSIDs

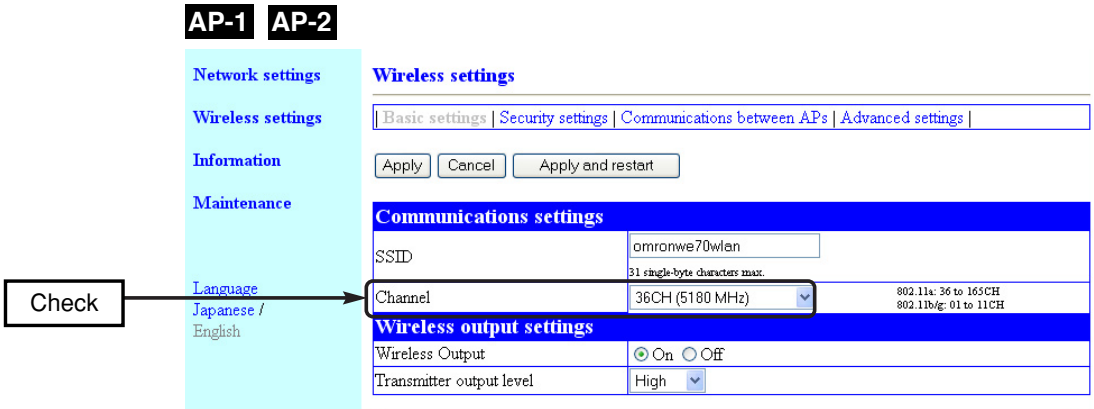
(1) On "Wireless settings" screen, verify that SSIDs of AP-1 and AP-2 are the same.
(Factory shipment status:"omronwe70wlan")



Step 3. Checking Wireless Channel

Verify a channel for AP-to-AP bridging.(Factory shipment status:36CH (5180MHz))

(1) On "Wireless settings" screen, verify that channels of AP-1 and AP-2 are the same.
(Factory shipment status:36CH)



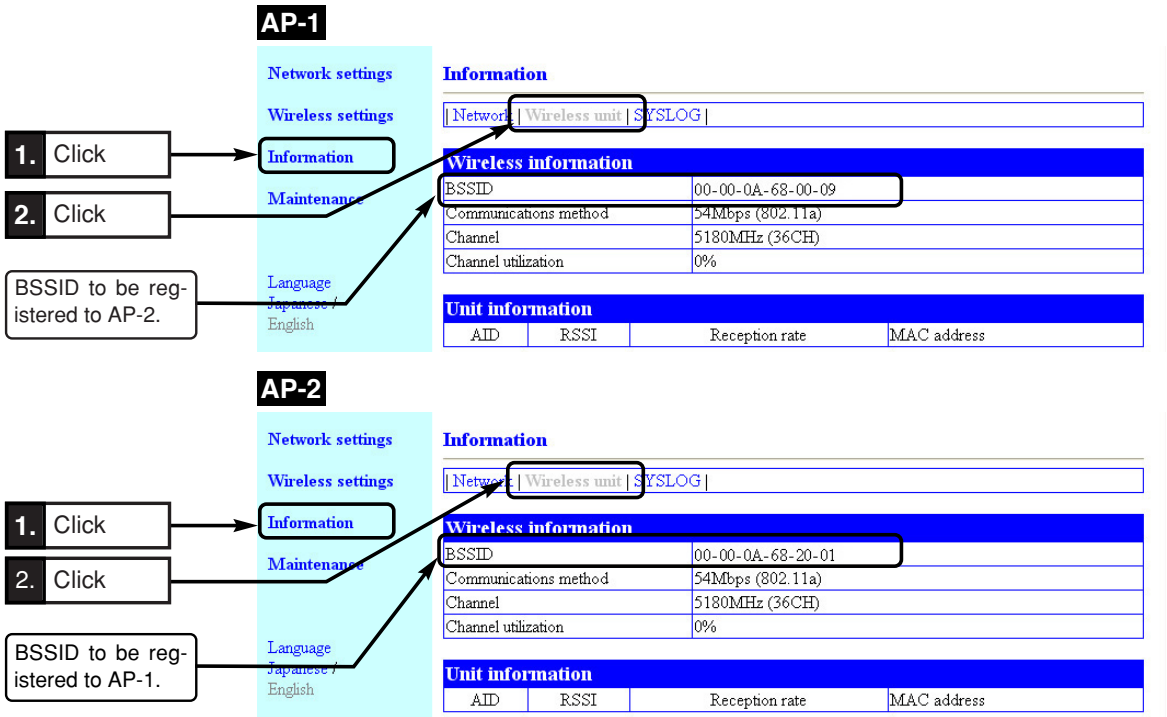
Step 4. Checking Own & Partner BSSIDs

(1) Select "Information" menu, "Wireless unit".

* Note that a BSSID is different from [Unit's MAC Address] in the "Network information" screen of "Information" menu.

<To Verify>

A 12-digit number displayed as [BSSID] in the next page is a BSSID to be registered to a communication partner.



Step 5. Checking Partner BSSID

Communication through AP-to-AP bridging can be made by registering each other's BSSID to a wireless unit.

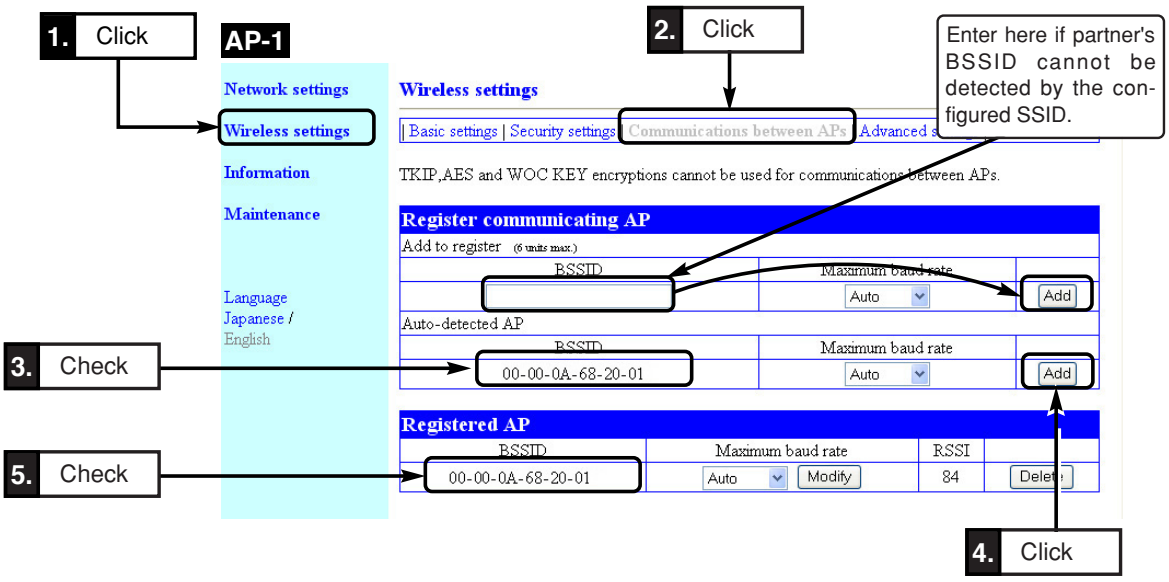
Register AP-to-AP bridging partner's BSSID to [Registered AP].

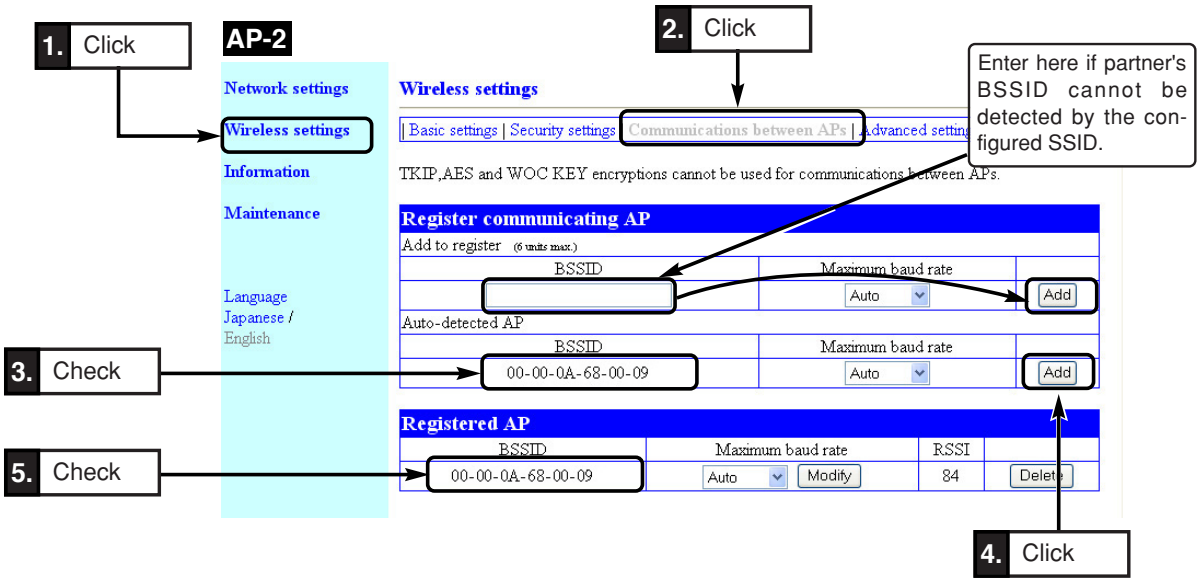
<To Register>

(1) Select "Wireless settings" menu, "Communications between APs".
- A "Communications between APs" screen is displayed.

(2) If a BSSID is displayed in the [Auto-detected AP] field in [Register communicating AP] (e.g. 00-00-0A-**-**-**), click <Add> in the right of the field.

(3) If partner's BSSID is not displayed, enter a BSSID to be registered and click <Add>.
- The BSSID is registered and displayed in the [Registered AP] field.





Step 6. Checking Received Signal Strength Indication

Verify AP-to-AP bridging through access point received signal strength indication (RSSI).

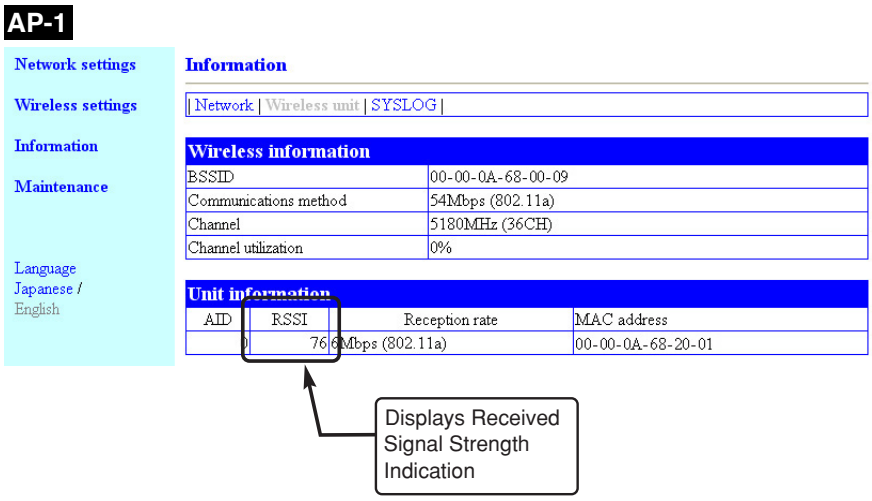
(1) Select "Information" menu, "Wireless unit".

- A "Wireless unit" screen is displayed.

(2) Received Signal Strength Indication is displayed in the [RSSI] field of [Unit Information] (e.g. 76).

* To update the value, refresh your browser window.

* AIDs of APs using AP-to-AP bridging are all 0s.



Step 7. Checking AP-to-AP Bridging

Execute the Ping command to AP-2 from PC connected to AP-1 and verify its response.

(1) Execute a ping command from your PC at command prompt.

Example:Ping 192.168.0.2 (Partner's IP address)

```
C:¥>ping  192.168.0.2

Pinging  192.168.0.2  with  32  bytes  of  data:

Reply  from  192.168.0.2:  bytes=32  time<1ms  TTL=250
```

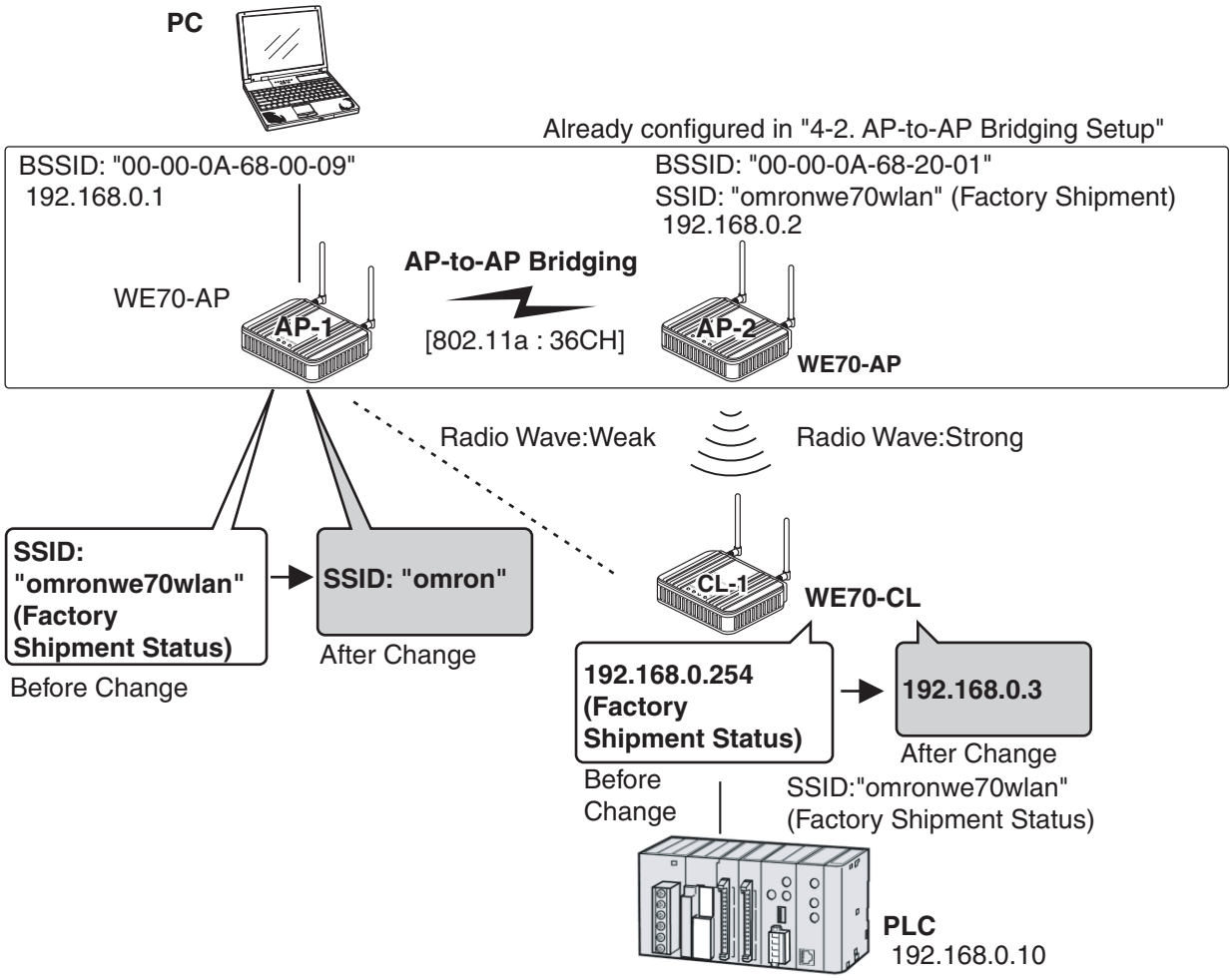
* If no response is returned, follow the steps below:
• Execute "arp -d" command.
• Verify if security settings are the same.

* AP-to-AP bridging is not available at the channel where DFS function is provided.

* All access points that use AP-to-AP bridging must be configured to use the same channel.
* Up to 6 units can communicate with an access point at the same time.
* To use encryption, the same encryption key must be configured for the access points.
* Only "WEP RC4" and "OCB AES" can be used as encryption for AP-to-AP bridging.
* BSSID of respective access point must be registered for those that use AP-to-AP bridging.
  In the figure above, [BSSID] of [B] must be registered to [A] and [BSSID] of [A] to [B].
* Configuring the same channel and SSID allows detection of BSSID of the others, making registration easier.
* To use roaming, the same SSID must be configured for the access points (A and B).
* AP-to-AP bridging requires the same setup of Super AG (Yes or No).
* AP-to-AP bridging is not available at the channel where DFS function is provided.

4-3. Configuring Relay Function (Pattern A)

The pattern A is a mechanism of communication with a client CL-1 via an access point AP-2 as a repeater. CL-1 always communicates with AP-2, not with AP-1, allowing stable operation. Through the steps from 1 to 7 in "4-2. Configuring AP-to-AP Bridging", communication setup must be completed for AP-1 and AP-2 beforehand. From the next page, setup and verification steps are described for the pattern A (P.13) of AP-to-AP bridging (Relay function).



In this example, AP-1 communicates with CL-1 via AP-2 as a repeater. As configuring the same SSID for AP-1 and CL-1 may use an unstable communication pathway between AP-1 and CL-1 with weak radio wave, AP-1's SSID is changed so that AP-1 and CL-1 cannot directly communicate with each other. In addition, even if power of AP-2 is lost and thus communication becomes unavailable, CL-1 would not communicate with AP-1. Communication will be restarted when AP-2 is recovered.

⚠ **Caution**	Configuring the same SSID for AP-1 and AP-2 can result in endless communication between CL-1 and AP-1 unless the communication is completely lost. To configure the same SSID for AP-1 and AP-2, it is recommended to enable smart roaming as in the pattern B. If smart roaming is being enabled, communication will be switched to an access point with better radio wave status. Do not make wired connection between AP-1 and AP-2 after AP-to-AP bridging was established between them. If such a case is required, enable the spanning tree function for AP-1 and AP-2.See "4-6. Using Spanning Tree Function".

Step 1. Changing Access Point SSID

Change AP-1's SSID. In the pattern A, SSIDs of AP-2 and CL-1 are left as their initial values and CL-1 communicates AP-2 only. Matching the SSIDs allows AP-CL communication.

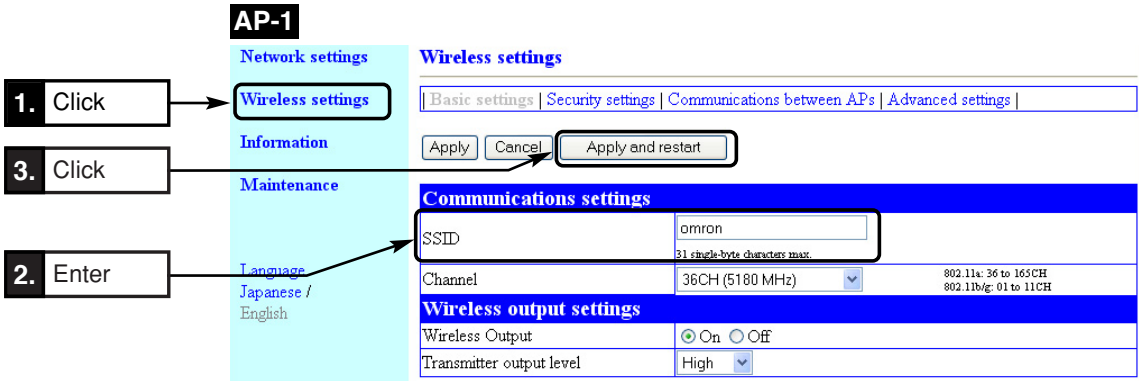
<To Configure>

(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Wireless settings menu.

(2) In the "Wireless settings" screen, enter the desired alphanumeric characters in SSID (within 31 characters) with the attention for capitalization. Example:omron (Initial value:omronwe70wlan)

(3) Click <Apply and restart>.

* If a wireless LAN terminal is used for setup, switch the connection to the SSID configured here.



Step 2. Configuring Client IP Address

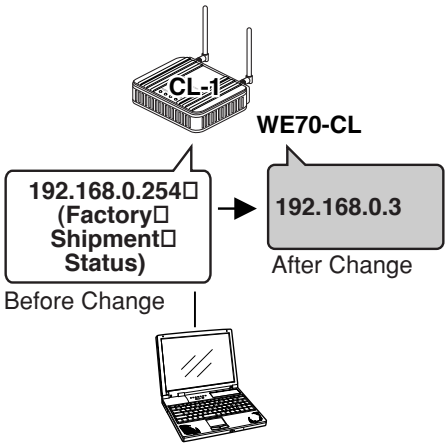
This section describes how to change IP address setup.
Connect a client and PC using a LAN cable (straight).

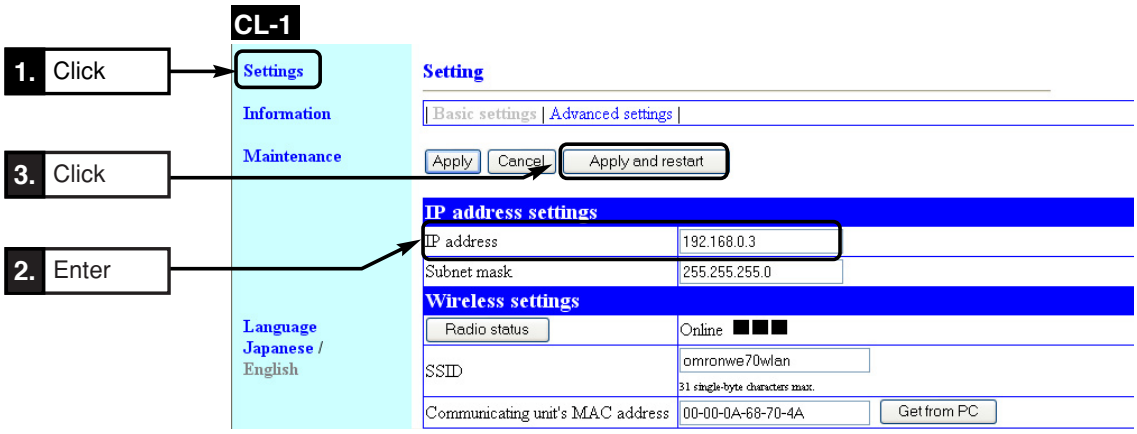
<To Configure>

(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click settings menu.

(2) Change the LAN-end IP address to "192.168.0.3".

(3) Click <Apply and restart>.





Step 3. Checking Communication

Verify that PC connected to a client (slave) can connect to an access point.

● **To monitor radio status**

(1) Select "settings" menu, "Basic settings".

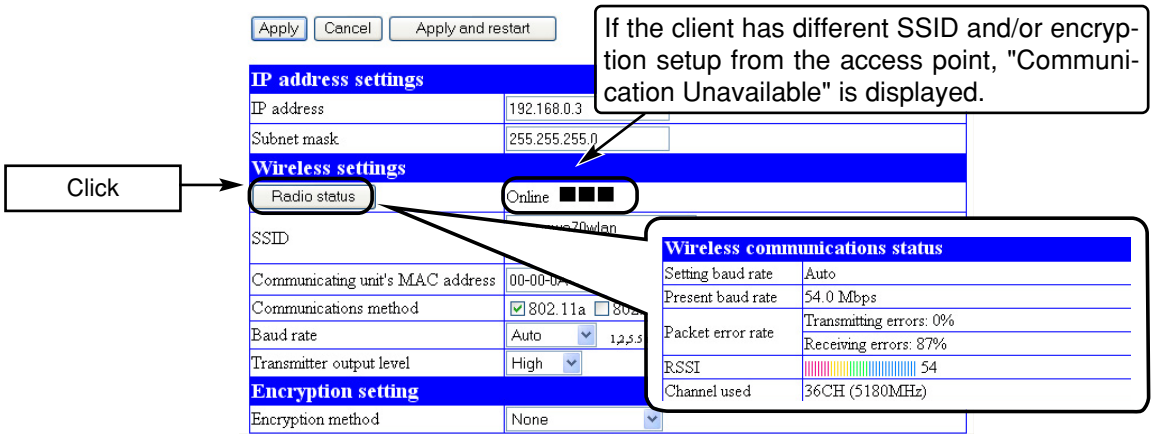
- "Basic settings" screen is displayed.
- The screen displays "Online ■■■".

* "Communication Unavailable" may be displayed until the WWW browser screen is updated in a case such as after setup change.

(2) To monitor detailed status, click <Radio status>.

- An independent screen displays Wireless communications status information.

* Information on the independent screen is updated every 0.5 seconds, while continuous monitoring increases network load. Close the screen after verification.



<Radio Status> Button..... Radio wave intensity that an access point can receive is displayed in the right of this button. If the client has different SSID and/or encryption setup from the access point, "Communication Unavailable" is displayed.
Radio wave intensity is displayed in 4 levels as shown below.
Levels may differ depending on a communication type.

- Level: □□□ ■□□ ■■□ ■■■

0-8	9-14	15-20	21 or higher (in case of 802.11a)
0-13	14-19	20-25	26 or higher (in case of 802.11b/g)

Clicking <Radio status> allows monitoring of statuses of radio communication such as channels and communication speed in the [Wireless communications status].

[For Reference]
To check access to an access point, specify LAN-end IP address (such as 192.168.0.1) of the access point based on a procedure Connection Check, Opening Setup Screen (P.2-13).
- A setup screen of the access point is displayed.
  * If access is controlled by a password, a password input is requested.

Step 4. Configuring Client-PLC Communication

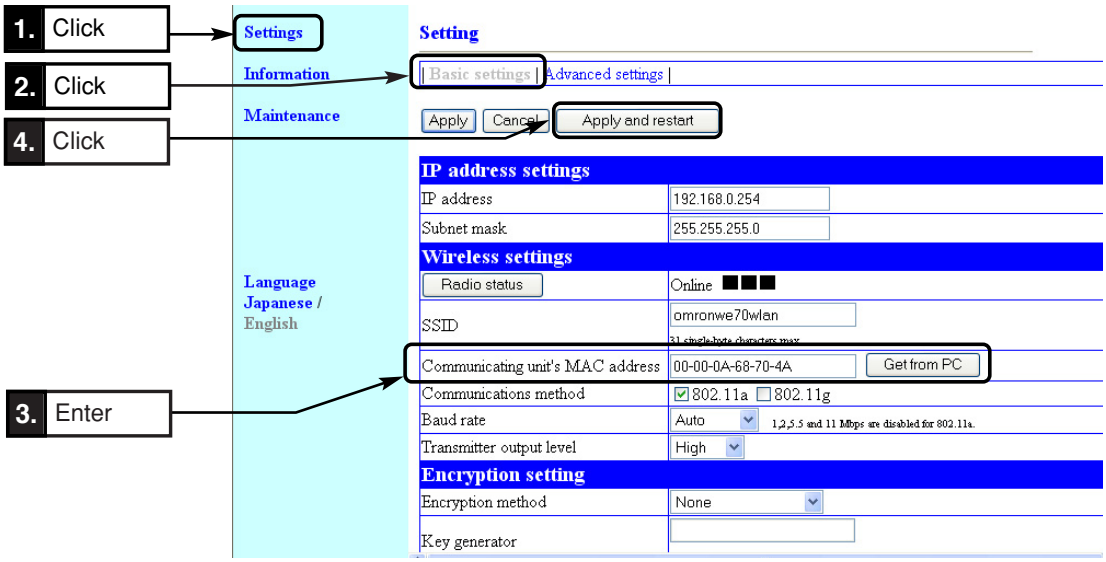
Configure a terminal MAC address. A MAC address of PLC Ethernet unit must be set to a client CL-1.

<To Configure>

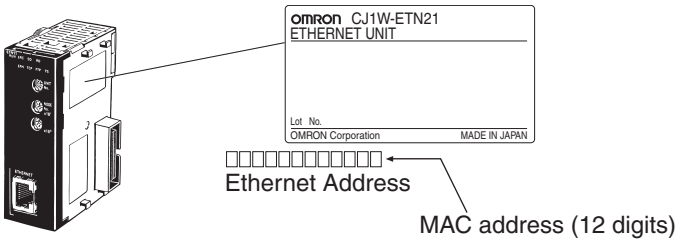
(1) Select "settings" menu, "Basic settings".
  * A "Basic settings" screen is displayed.

(2) Enter a MAC address of PLC Ethernet unit in the [Communicating unit's MAC address]. (Example:00-00-0A-68-70-4A)

(3) Click <Apply and restart>.



Example. The Ethernet unit CJ1W-ETN21 has a label of Ethernet address (MAC address) on its right side.



Step 5. PLC Setup

To connect a PLC to a network, Ethernet unit's IP address must be configured. A unique IP address must be allocated for each communication node, using either of the followings:

1. Specifying with a default IP address

A rotary SW in the Ethernet unit can specify a FINS node address (1 to 254), which is used as a host block of the IP address. A FINS node address and an IP address to be specified for an Ethernet unit have the following relationship:

192.168.250.FINS_Node_Address

That is, specifying a node number 10 to a network of 192.168.250.* sets an IP address of 192.168.250.10 by default.

2. Specifying by Unit Setup of CX-Programmer

From I/O Table window of online CX-Programmer, select an Ethernet unit and specify an IP address from Unit Setup.

3. Specifying by CPU advanced function unit assignment DM area

Under a status of an IP address unconfigured for Unit Setup, specify an IP address to IP Address Display/Setup Area of CPU advanced function unit assignment DM area.

FINS node addresses and IP addresses must not overlap in a network.

By default, IP addresses of an access point and a client are:

Access Point (WE70-AP) :192.168.0.1

Client (WE70-CL) :192.168.0.254

For details, see CS1W-ETN21/CJ1W-ETN21 Ethernet Units Construction of Networks Operation Manual(W420-E1), Section 5-2. IP Address in FINS Communications.

Step 6. Checking PC-PLC Communication

Execute the Ping command to PLC from PC connected to AP-1 and verify its response.

(1) Execute a ping command from your PC at command prompt.
Example:Ping 192.168.0.10 (Partner's IP address)

```
C:¥>ping  192.168.0.10
Pinging  192.168.0.10  with  32  bytes  of  data:
Reply  from  192.168.0.10:  bytes=32  time<1ms  TTL=250
```

* If no response is returned, follow the steps below:

• Execute "arp -d" command.

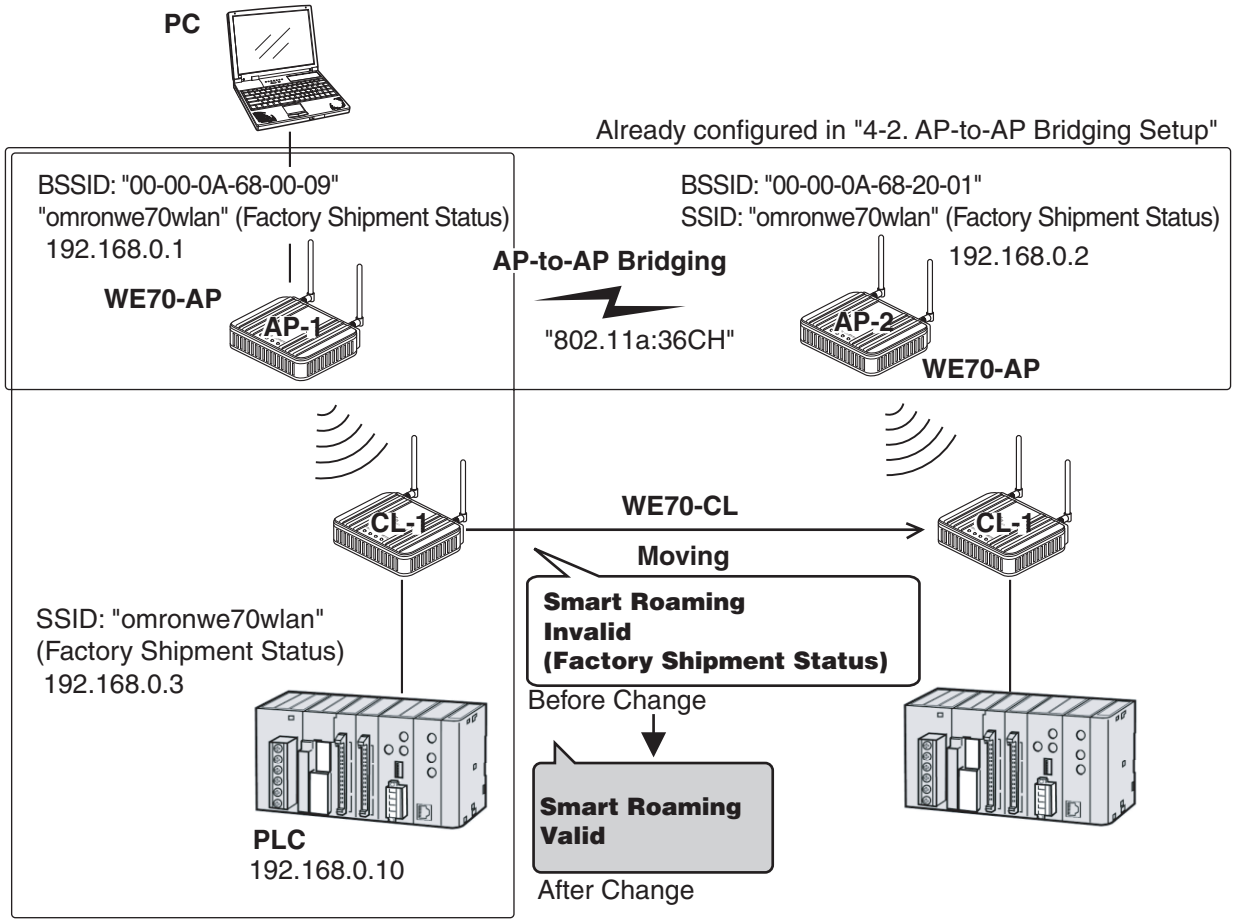
• Verify if security settings are the same.

4-4. Configuring Relay Function (Pattern B)

Pattern B is a mechanism of communication for a moving client (slave) switching paths with 2 access points. Difference from the Pattern A lies in availability of communication with any access point, with the same SSID for AP-1 and AP-2. In the pattern B for smooth connection to an access point after moving, "Smart Roaming" must be enabled.

Through steps in "4-2. Configuring AP-to-AP Bridging" and the steps from 2 to 6 in "4-3. Configuring Repeater Function (Pattern A)", communication setup must be completed for AP-1 and CL-1 beforehand.

Using an example below, setup and verification steps are described for the pattern B (P.14) of AP-to-AP bridging (Relay function).



Already configured in "4-3. Configuring Relay Function (Pattern A)", steps from 2 to 6

Step 1. Configuring Smart Roaming

If communications get worse after a client (slave) is moved to another access point, the client starts detecting another access point that may provide better communications.

When the client finds a good access point, it switches its wireless connection to the good point to maintain stable communications. This function is called smart roaming.

See "4-9. Smart Roaming" for details. When you use smart roaming, set "Smart Roaming" mode of the client CL-1 to "Valid". (Default setting: Invalid)

* All of SSID and Encryption setup must be the same.

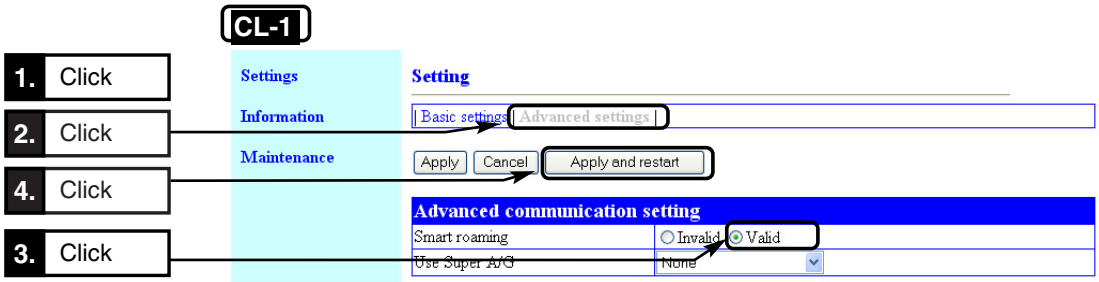
<To Configure>

(1) Open a setup screen of the CL-1 (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click settings menu.

(2) Click "Advanced settings".
- An "Advanced settings" screen is displayed.

(3) Select [Valid] radio button in the [Smart roaming] field.

(4) Click <Apply and restart>.



Step 2. Checking Smart Roaming

Display a BSSID of Settings currently communicating with, to verify which access point is communicating with the client.

<To Verify>

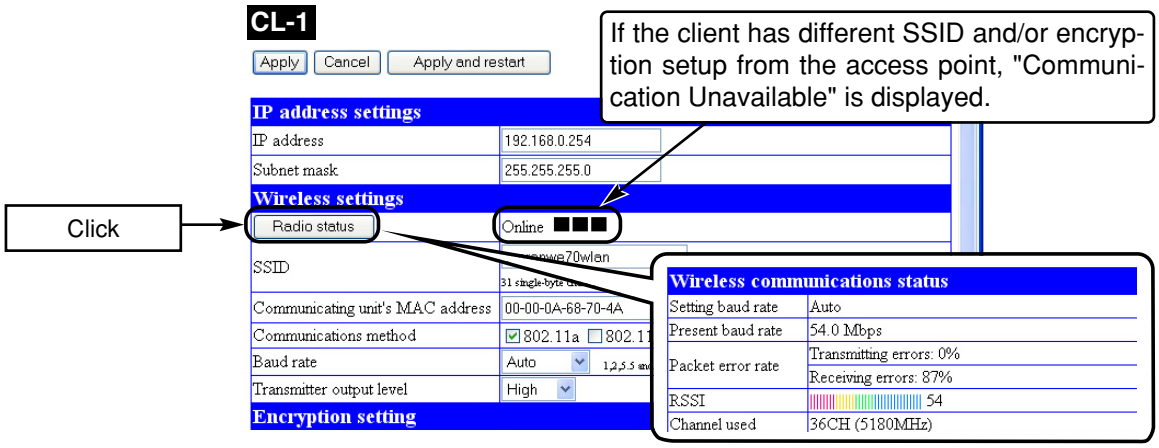
(1) From "Information" menu, "Wireless Information", "BSSID", verify which access point is communicating with CL-1. Assume that it is AP-1 in this example.

(2) Select "Settings" menu, "Basic settings".

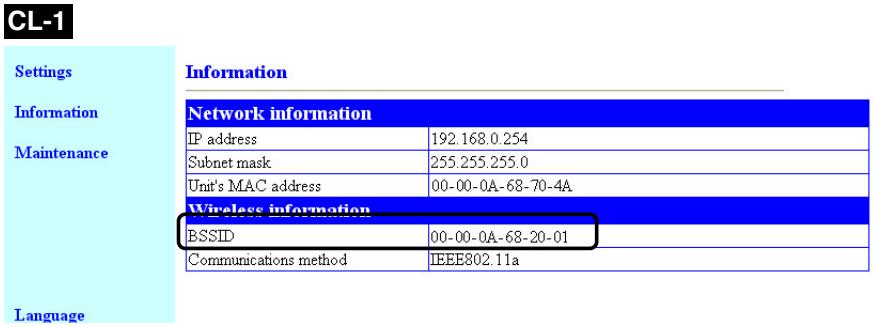
(3) Click <Radio Status>.
- An independent screen displays Wireless communications status.
- * Information on the independent screen is updated every 0.5 seconds, while continuous monitoring increases network load. Close the screen after verification.

(4) While checking received electric field strength, move CL-1 away from AP-1 and closer to AP-2. As it moves away from AP-1, a received electric field strength decreases, then the level suddenly should rise momentarily. In case of 802.11a, move a client so that a received electric field strength should be 14 or less from AP-1 and 21 or more from AP-2. In case of 802.11b/g, move it so that a received electric field strength should be 19 or less from AP-1 and 26 or more from AP-2.

* These values are for reference only and may depend on your environment.



(5) From CL-1 Setup screen "Information" menu, "Wireless Information", "BSSID", verify that BSSID should be AP-2 value.



(6) Check if communication is available between PC and PLC.Test the roaming in the opposite direction and verify that access points should be switched from AP-2 to AP-1 and that communication should be available between PC and PLC.

Step 3. Checking PC-PLC Communication

Execute the Ping command to PLC from PC connected to AP-1 and verify its response.

(1) Execute a ping command from your PC at command prompt.

Example:Ping 192.168.0.10 (Partner's IP address)

```
C:¥>ping 192.168.0.10
Pinging 192.168.0.10 with 32 bytes of data:
Reply from 192.168.0.10: bytes=32 time<1ms TTL=250
```

* If no response is returned, follow the steps below:

• Execute "arp -d" command.

• Verify if security settings are the same.

⚠ Caution

- Set CL-1's SSID as the same one as that of an access point to communicate. (In this example those of AP-1 and AP-2)
- When performance of smart roaming switching time is required, combine WE70-AP and WE70-CL.
- For mobile operation of CL-1, make sure that CL-1 should not go into an area where radio wave cannot reach from neither AP1 and AP-2.
- When smart roaming is being valid, and if CL-1's received electric field strength levels from AP-1 and AP-2 are not very much different, roaming may not be available or may take a long time.
- Repeating is available for 6 segments.
- As larger number of segments decreases throughput, take precautions for an application that requires high speed. Always perform testing before actual operation.

4-5. To Set up MAC Address Filtering

MAC address filtering is a function to communicate with a specified partner using a MAC address. An access point communicates with a client (slave) only with a registered terminal MAC address. This section describes steps to register a terminal MAC address of a client (slave) to an access point.

* Some wireless LAN devices may calls this function as "MAC address security", which is same as MAC address filtering.

<To Configure>

(1) Open a setup screen of the access point (see Chapter 2-3. Checking Connection, Opening Setup Screen (P.2-13)) and click Wireless settings menu > Advanced settings.
- An "Advanced settings" screen is displayed.

(2) Select [Valid] radio button in the [MAC address filtering] field.

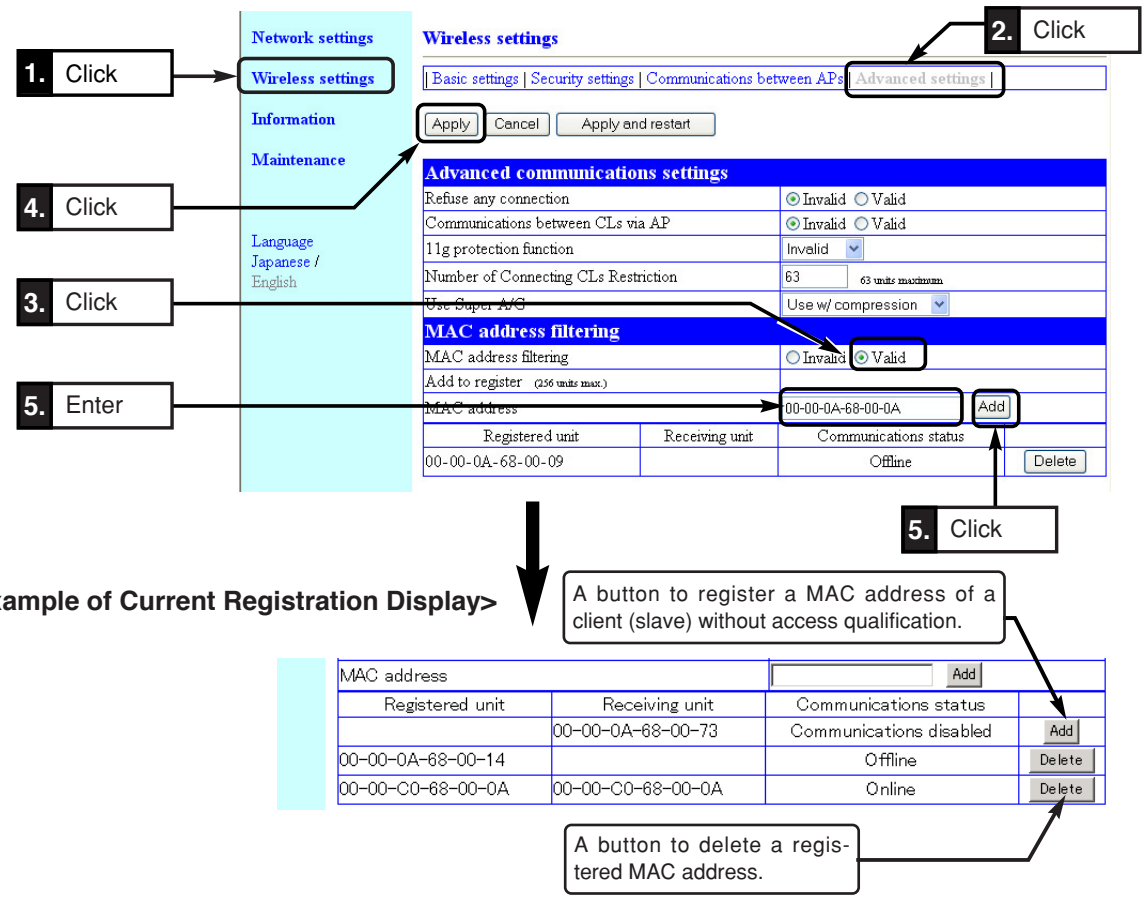
(3) Click <Apply>.

(4) Enter a terminal MAC address of a client to communicate with an access point in [Add to register (MAC address)] using alphanumeric characters. (Example:00-00-0A-68-00-0A)
To connect to PLC, enter a terminal MAC address of PLC.

(5) Click <Add> in the right of [Add to register] field.
- Verify that entered terminal MAC address is displayed in [Registered unit] field.

* Clicking <Add> in the right of [Registered unit] field allows communication with the client (slave).

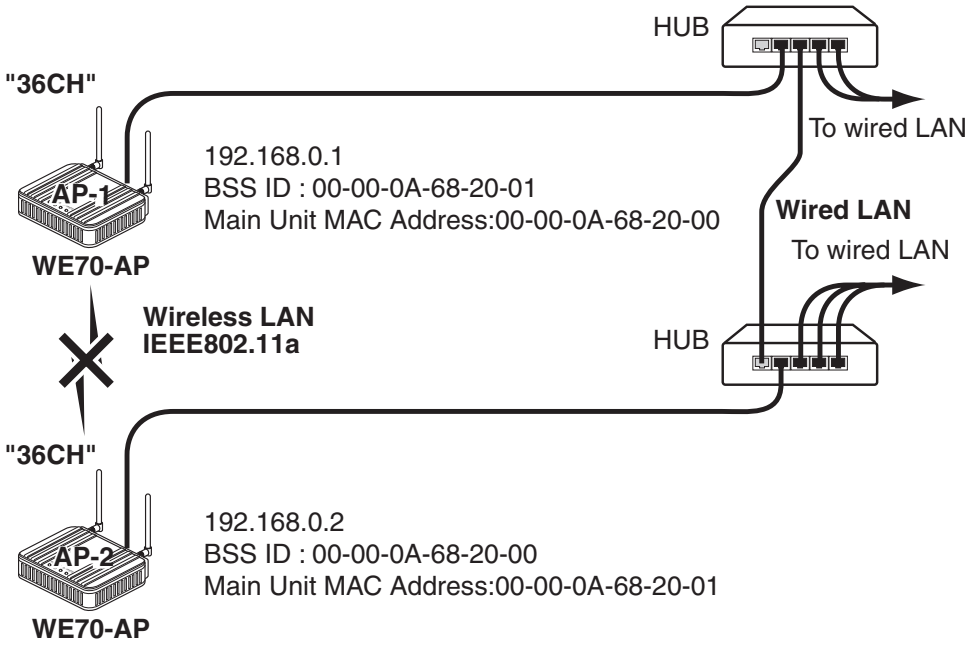
* When MAC address is displayed in [Receiving unit], clicking <Add> in the right of [Receiving unit] field allows communication with the client (slave).



4-6. Using Spanning Tree Function

Configuring the spanning tree function prevents endless looping of packets in a looped communication path. In an example shown below, a wireless LAN port with low priority is being stopped if no obstacle exists in wired LAN paths. To construct a network using the spanning tree function, you must choose a switch or a hub that supports IEEE802.1d spanning tree protocol.

* This section describes how to configure for communication using the spanning tree function,assuming wireless units of AP-1 and AP-2.



■ Configuring Spanning Tree Function

Set the spanning tree function in access points AP-1 and AP-2.

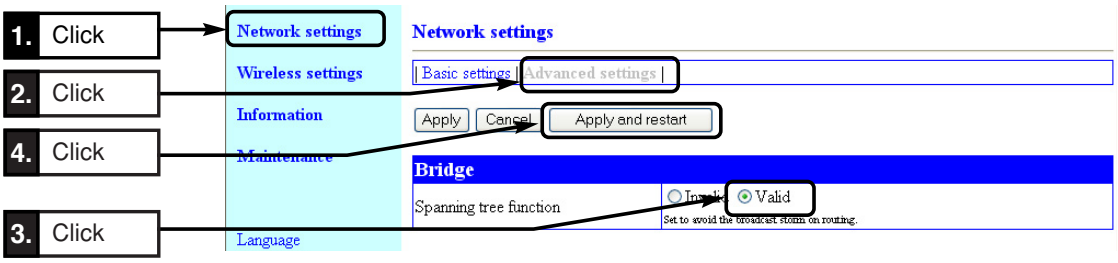
<To Configure>

(1) Open a setup screen of the access point (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Network settings menu, Advanced settings .

- A "Bridge" screen is displayed.

(2) Select [Valid] radio button in the [Spanning tree function] field.

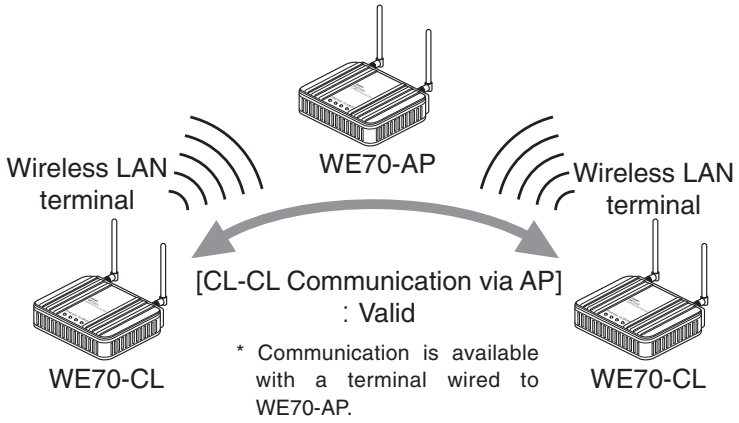
(3) Click <Apply and restart>.



4-7. Using CL-to-CL Communication via AP

Configuration can be made so that wireless LAN terminals can communicate with each other via an access point or not.

* This function is valid for terminals connected to an access point via wireless LAN.
* The terminals can communicate with a wired LAN terminal connected to the access point.

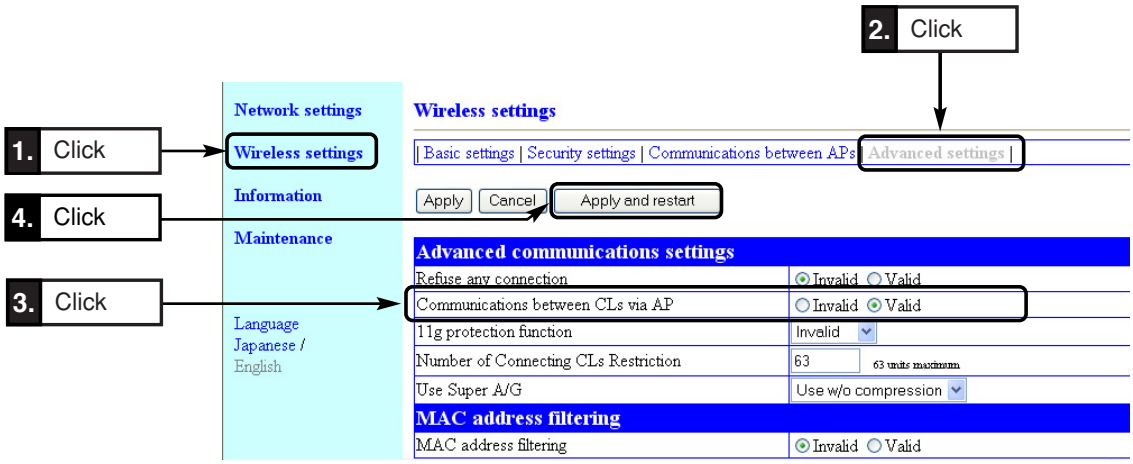


<To Configure>

(1) Open a setup screen of the access point (see Chapter 2-3. Checking Connection, Opening Setup Screen (P.2-13)) and click Wireless settings menu, then Advanced settings.
- An "Advanced settings" screen is displayed.

(2) Select [Valid] radio button in the [Communications between CLs via AP] field.

(3) Click <Apply and restart>.



4-8. Limiting IEEE802.11b Communication

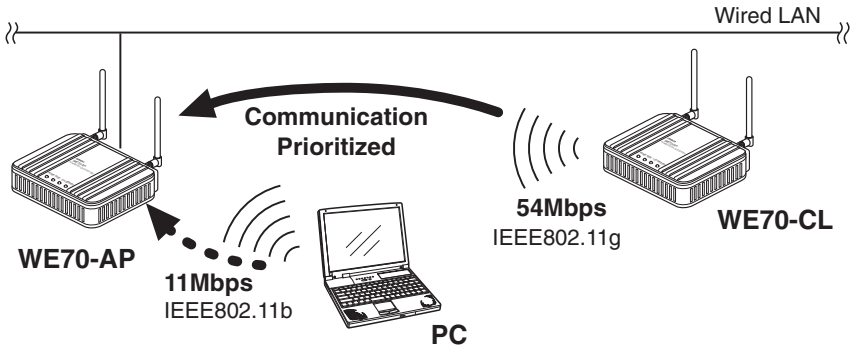
In an environment using both of IEEE802.11g and IEEE802.11b standards, communication with IEEE802.11g can be prioritized or restricted based on access point setup. This can prevent or mitigate decrease of communication speed due to cross talk.

Configuring [11g Protection] allows communication as shown below.

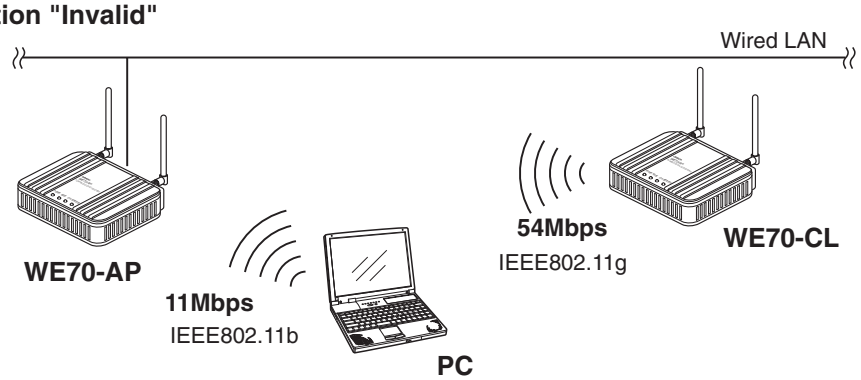
* The 11g protection can be configured in a screen displayed by clicking "Wireless Setup", "Advanced Setup" menu.

11g Protection "Valid" (Factory Shipment Status)

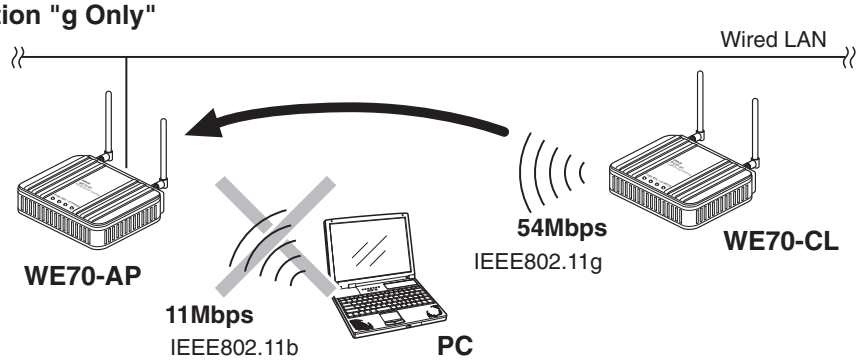
* This can be effective only if communication speed is extremely low due to mixed environment with IEEE802.11b and if decrease of IEEE802.11g speed can be prevented.



11g Protection "Invalid"



11g Protection "g Only"



4-9. Smart Roaming

If communications get worse after a client (slave) is moved to another access point, the client starts detecting another access point that may provide better communications.
When the client finds a good access point, it switches its wireless connection to the good point to maintain stable communications. This function is called smart roaming.

Note	When performance of smart roaming switching time is required, combine WE70-AP and WE70-CL.

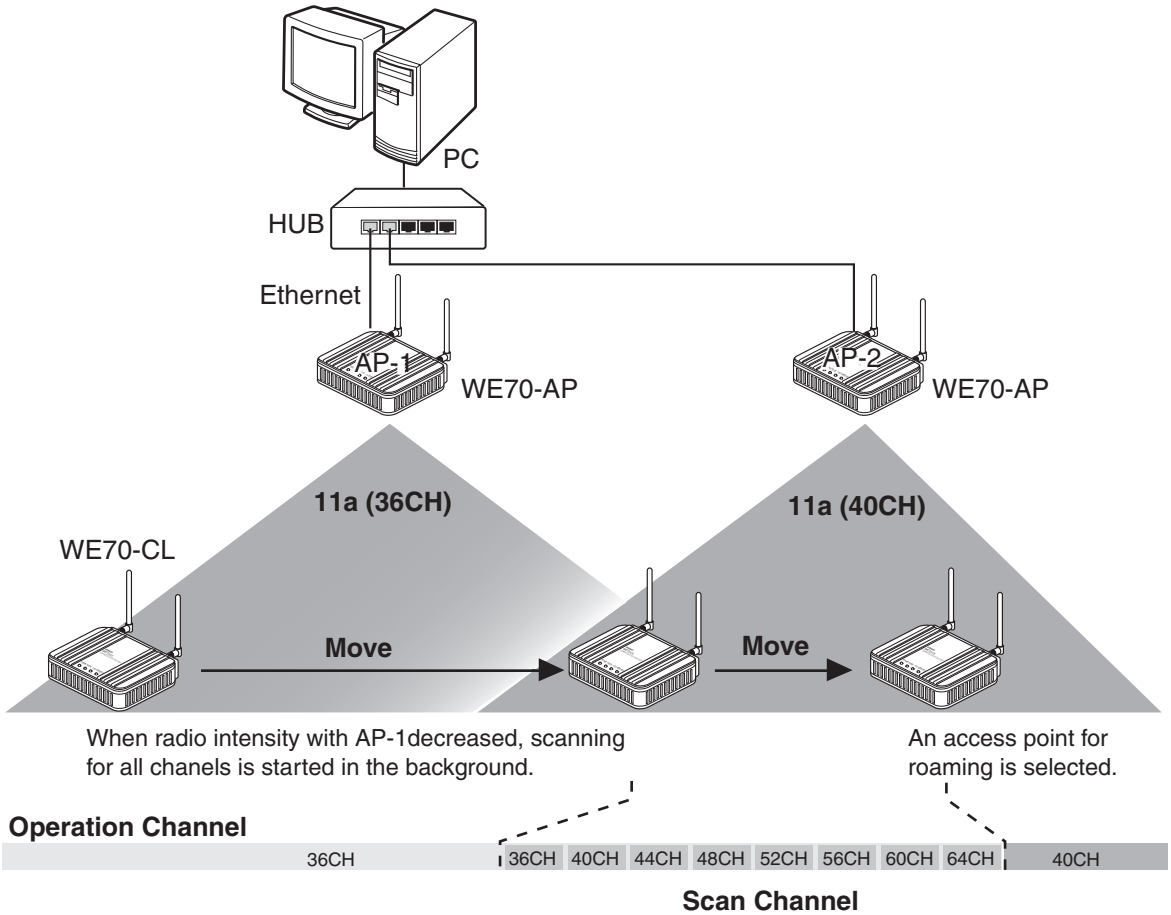
■ Scanning Channel

As WE70 can use 802.11a/b/g, frequency to be scanned depends on WE70-CL setup. ("802.11a":24CH max., "802.11b/g":13CH max. (Refer to Section 1-1))
Scanning is started when communication quality with WE70-AP gets worsened.

⚠ **Caution**	If both of "802.11a" and "802.11b/g" are selected, scanning is made for total 802.11a/b/g.

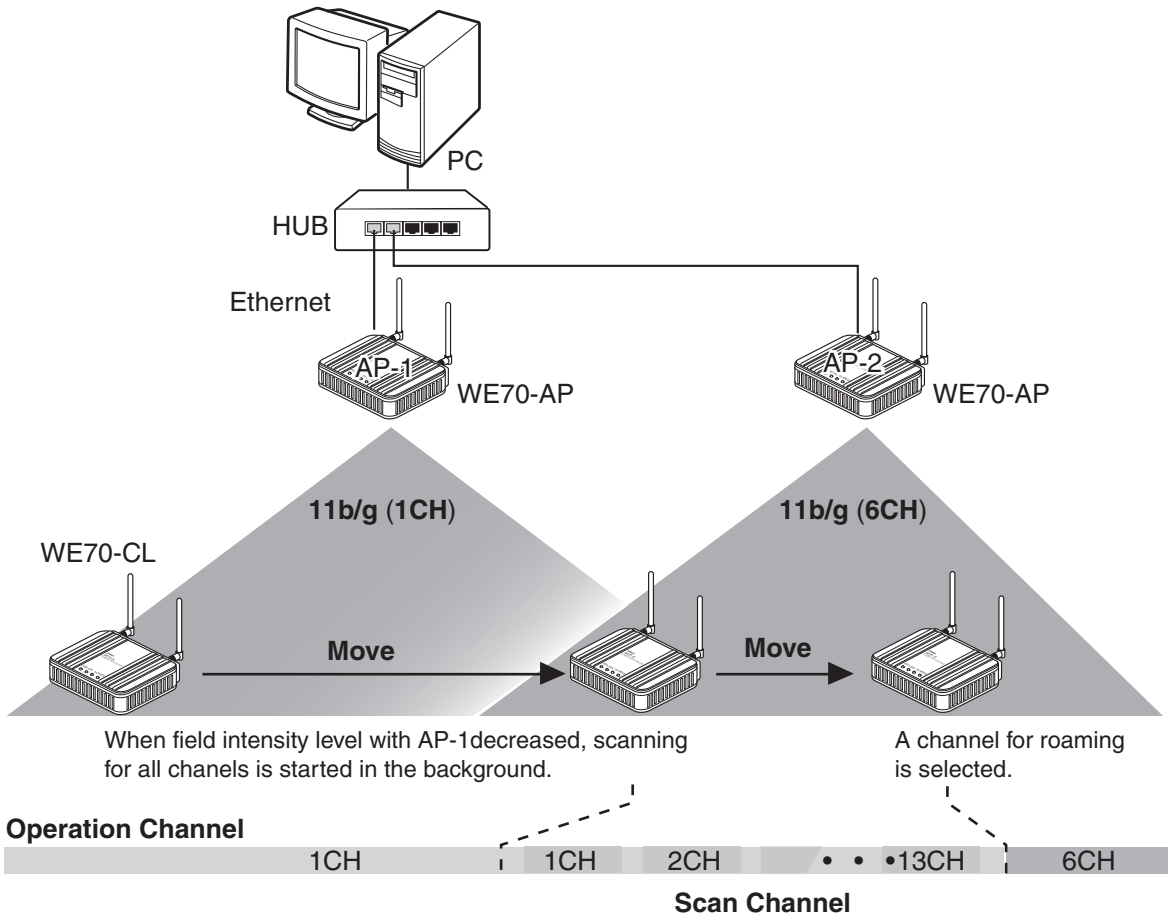
■ Smart Roaming for 802.11a

When a client (slave) moves from an area of an access point AP-1 to that of AP-2 and the received electric field strength decreases (to about 14 or less), scanning of wireless channels is automatically started and an access point for roaming is selected.



■ **Smart Roaming for 802.11b/g**

When a client (slave) moves from an area of an access point AP-1 to that of AP-2 and the received electric field strength decreases (to about 19 or less), scanning of wireless channels is automatically started and an access point for roaming is selected.



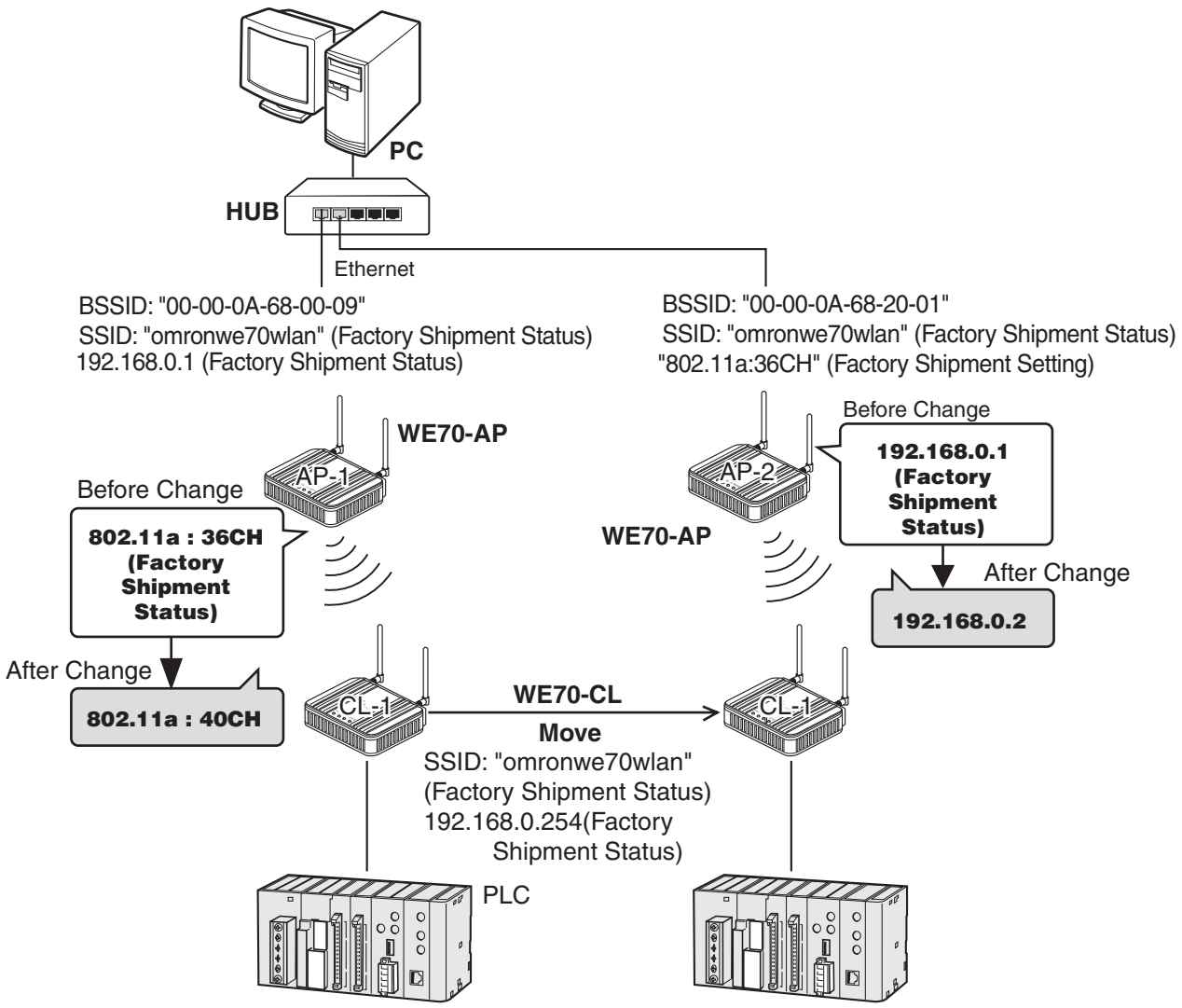
Follow instructions below for stable communication:

- Operate under a clean environment without cross talk as much as possible.
- Install antennas so that there is a direct line of sight between them.
- Install communication ranges of access points so that they should overlap as much as possible.
  Install access points with an interval of about 30 to 40m, as a guideline.

⚠ **Caution**	After scanning of the all channels is completed in the background, a 60-second waiting period is imposed before the next scanning. This waiting period can be changed on the clients (slaves) of version 1.22 or later. See "Changing the waiting period for scanning" in the appendices for details.

4-10. Configuring Smart Roaming

If there are 2 access points, connect PC, hub, wireless units, and PLC as shown below.



Step 1. Configuring IP Address

Change access point AP-2 IP address.

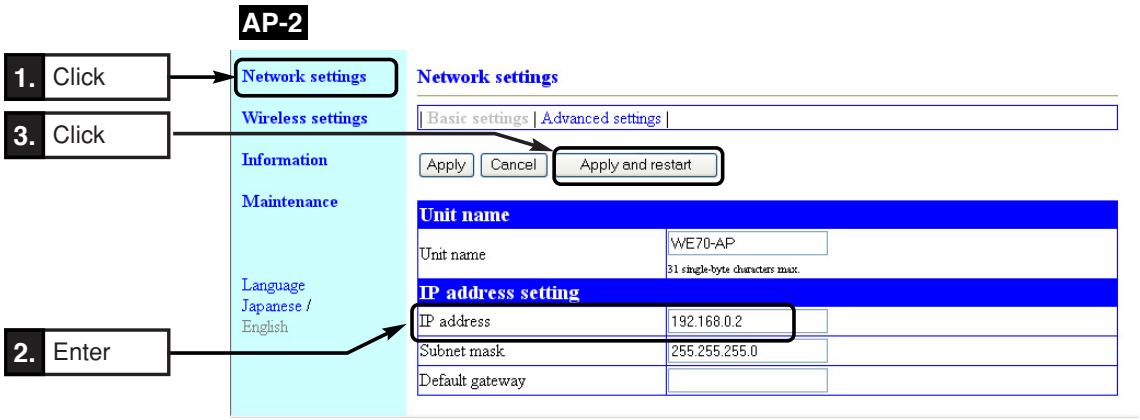
Leave AP-1 [192.168.0.1] and CL-1 [192.168.0.254] as they are.

<To Configure>

(1) Open a setup screen of AP-2 (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Network settings menu.

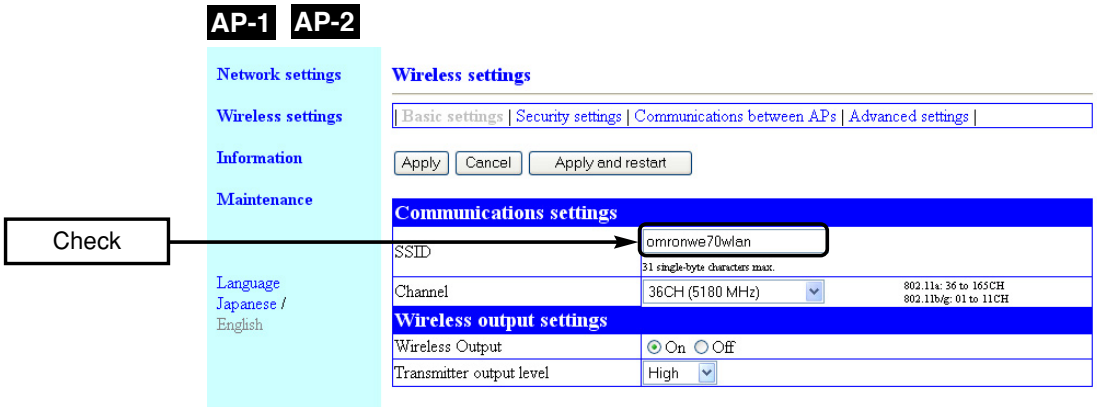
(2) Change the IP address to "192.168.0.2".

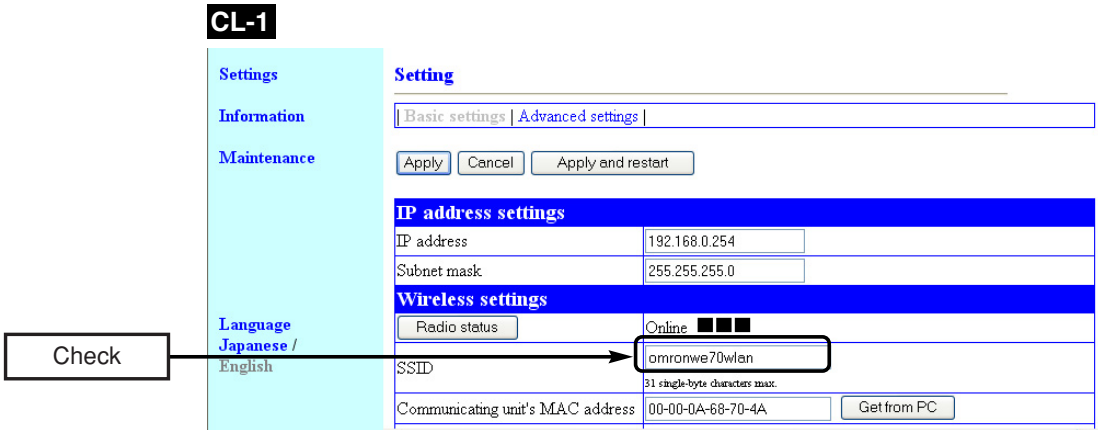
(3) Click <Apply and restart>.



Step 2. Checking Own & Partner SSIDs

(1) On "Wireless settings" screen, verify that SSIDs of AP-1, AP-2, and CL-1 are the same.
(Factory Shipment Status:"omronwe70wlan")

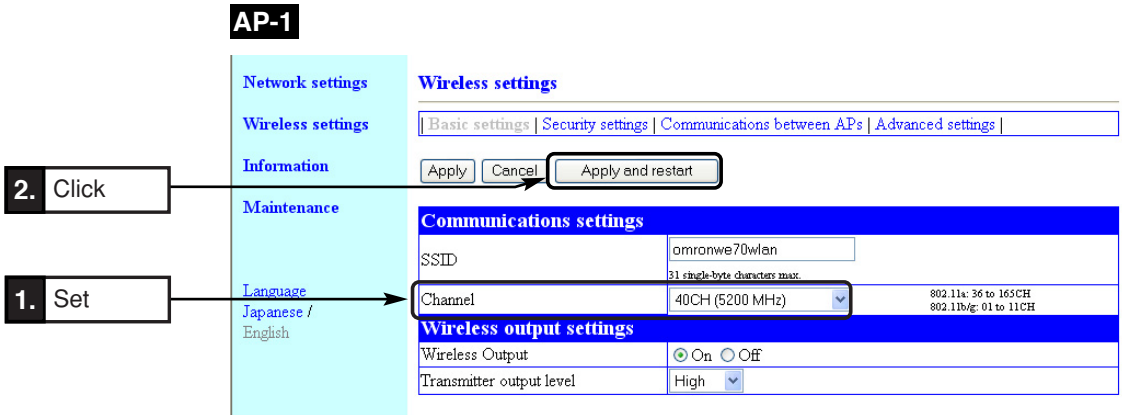




Step 3. Checking Wireless Channel

Change access point AP-1 channel. (Factory Shipment Status:36CH (5180MHz))

(1) On "Wireless settings" screen, change AP-1's [Channel] to 40CH. (Factory Shipment Status:36CH)



Step 4. Configuring Client-PLC Communication

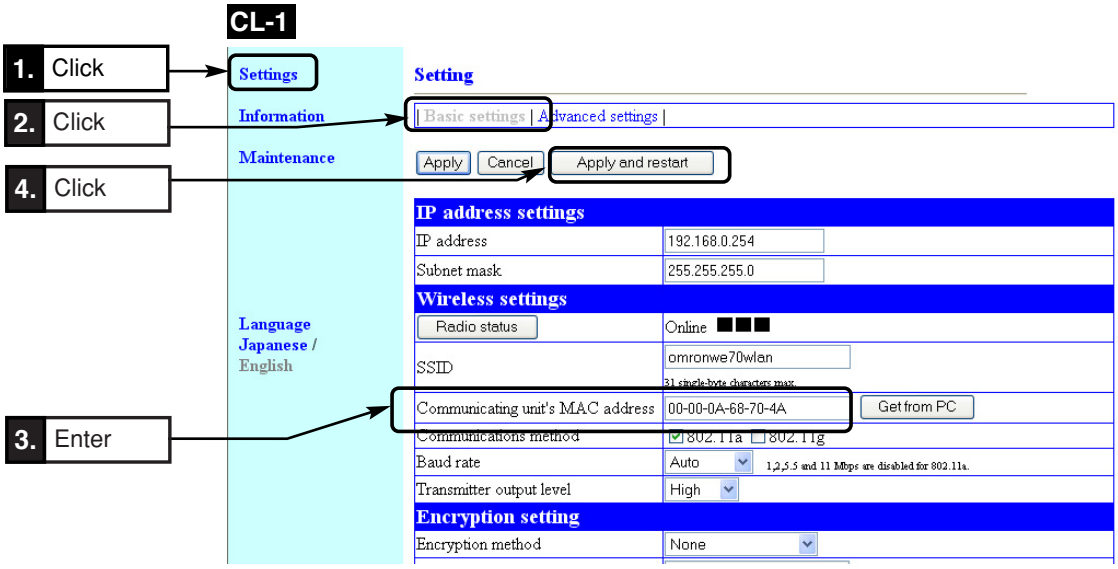
Configure a terminal MAC address. A MAC address of PLC Ethernet unit must be set to a client CL-1.

<To Configure>

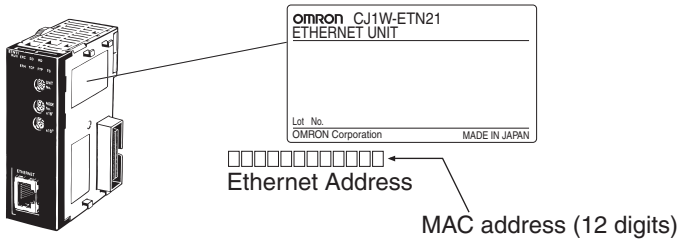
(1) Select "Settings" menu, "Basic settings".
- "Basic settings" screen is displayed.

(2) Enter a MAC address of PLC Ethernet unit in the [Communicating unit's MAC address]. (Example:00-00-0A-68-70-4A)

(3) Click <Apply and restart>.



Example. The Ethernet unit CJ1W-ETN21 has a label of Ethernet address (MAC address) on its right side.



Step 5. PLC Setup

To connect a PLC to a network, Ethernet unit's IP address must be configured.A unique IP address must be allocated for each communication node, using either of the followings:

1. Specifying with a default IP address

A rotary SW in the Ethernet unit can specify an FINS node address (1 to 254), which is used as a host block of the IP address. An FINS node address and an IP address to be specified for an Ethernet unit have the following relationship:

192.168.250.FINS_Node_Address

That is, specifying a node number 10 to a network of 192.168.250.* sets an IP address of 192.168.250.10 by default.

2. Specifying by Unit Setup of CX-Programmer

From I/O Table window of online CX-Programmer, select an Ethernet unit and specify an IP address from Unit Setup.

3. Specifying by CPU advanced function unit assignment DM area

Under a status of an IP address unconfigured for Unit Setup, specify an IP address to IP Address Display/Setup Area of CPU advanced function unit assignment DM area.

FINS node addresses and IP addresses must not overlap in a network. By default, IP addresses of an access point and a client are:

Access Point (WE70-AP) : 192.168.0.1

Client (WE70-CL) : 192.168.0.254

For details, see CS1W-ETN21/CJ1W-ETN21 Ethernet Units Construction of Networks Operation Manual(W420-E1), Section 5-2. IP Address in FINS Communications.

Step 6. Configuring Smart Roaming

Configure [Smart roaming] of the client (CL-1) as [Valid].(Factory Shipment Status:Invalid)

* SSID and Encryption setup must be the same for all of AP-1, AP-2, and CL-1.

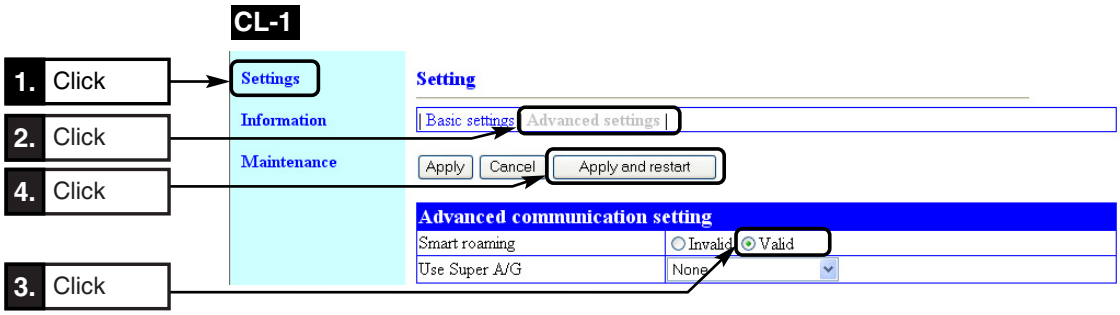
<To Configure>

(1) Open a setup screen of the client (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click "Settings" menu.

(2) Click "Advanced settings".
- An "Advanced settings" screen is displayed.

(3) Select [Valid] radio button in the [Smart roaming] field.

(4) Click <Apply and restart>.



Step 7. Checking Smart Roaming

Display a BSSID of an access point currently communicating with, to verify which access point is communicating with CL-1.

<To Verify>

(1) From "Information" menu, "Wireless information", "BSSID", verify which access point is communicating with CL-1. Assume that it is AP-1 in this example.

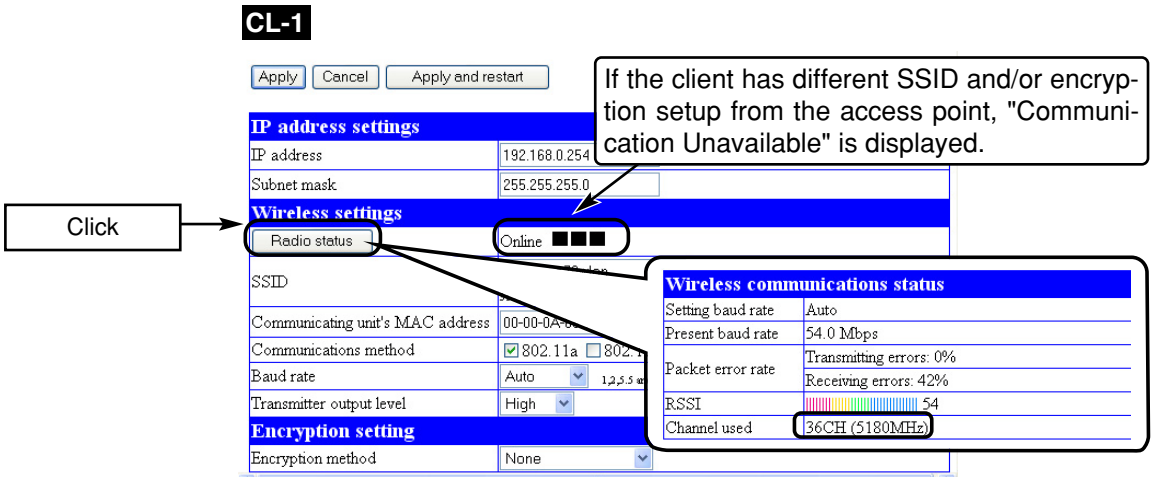
(2) Select "Settings" menu, "Basic settings".

(3) Click <Radio status>.
- An independent screen displays Wireless communications status information.

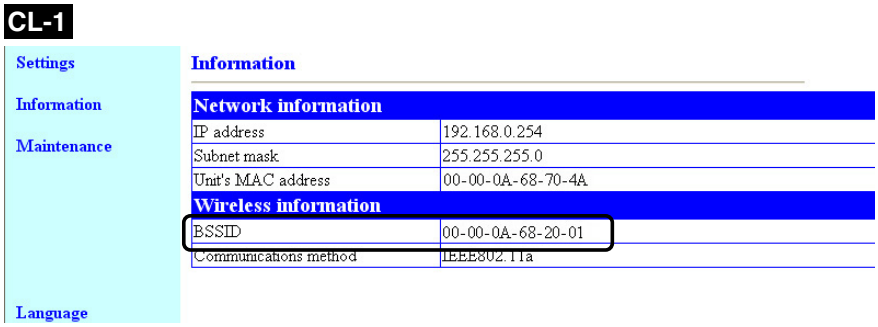
  * Information on the independent screen is updated every 0.5 seconds, while continuous monitoring increases network load. Close the screen after verification.

(4) While checking radio intensity, move CL-1 away from AP-1 and closer to AP-2. As it moves away from AP-1, radio intensity decreases, then the level suddenly should rise momentarily and the channel should change from 40CH to 36CH.In case of 802.11a, move a client so that a radio intensity should be 14 or less from AP-1 and 21 or more from AP-2. In case of 802.11b/g, move it so that a received field intensity level should be 19 or less from AP-1 and 26 or more from AP-2.

* These values are for reference only and may depend on your environment.



(5) From CL-1 Setup screen "Information" menu, "Wireless information", "BSSID", verify that BSSID should be AP-2 value.



(6) Check if communication is available between PC and PLC.Test the roaming in the opposite direction and verify that access points should be switched from AP-2 to AP-1 and that communication should be available between PC and PLC.

Step 8. Checking PC-PLC Communication

Execute the Ping command to PLC from PC connected to AP-1 and verify its response.

(1) Execute a ping command from your PC at command prompt.

Example:Ping 192.168.0.10 (Partner's IP address)

```
C:¥>ping 192.168.0.10
Pinging 192.168.0.10 with 32 bytes of data:
Reply from 192.168.0.10: bytes=32 time<1ms TTL=250
```

* If no response is returned, follow the steps below:

- Execute "arp -d" command.
- Verify if security settings are the same.

Setup Menu

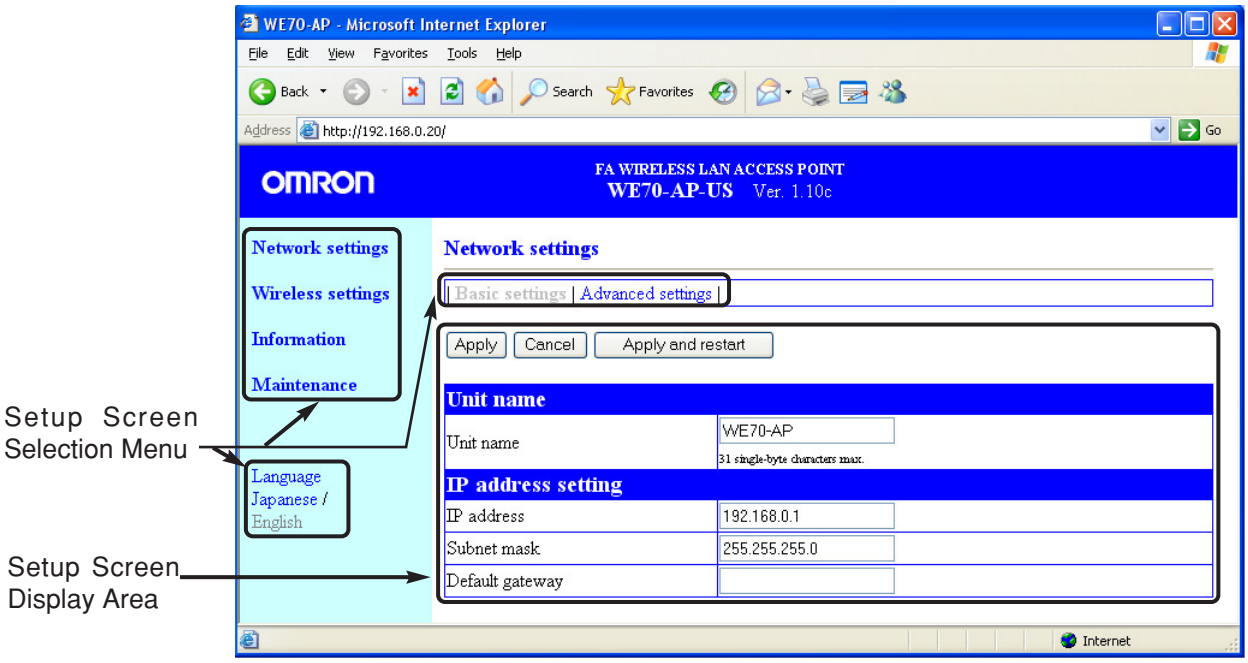
Chapter 5

This chapter describes
setup screens available for functions of this wireless unit set.

5-1. Setup Screen & Functions.....5-2
■ Setup Screen.....5-2
5-2. Setup Screen (WE70-AP) 5-3
■ Network Settings 5-3
■ Wireless Settings.....5-4
■ Information.....5-13
■ Maintenance 5-15
5-3. Setup Screen (WE70-CL) 5-19
■ Setup 5-19
■ Information.....5-26
■ Maintenance 5-27
5-4. Limiting Setup Screen Access.....5-28

5-1. Setup Screen & Functions

This section describes setup screens and items.



■ Setup Screen

Setup Screen Selection Menu

You can select any setup screen from this menu.

Clicking a menu item displays a link to a setup screen.

You can select language English or Japanese.

Setup Screen Display Area

This area displays a screen selected by the setup screen selection menu.

To change setting in a setup screen, click <Apply> to transition to a next screen.

If you move to a next screen without clicking <Apply>, changes will be discarded.

<Apply>/<Cancel>/<Apply and restart> Button

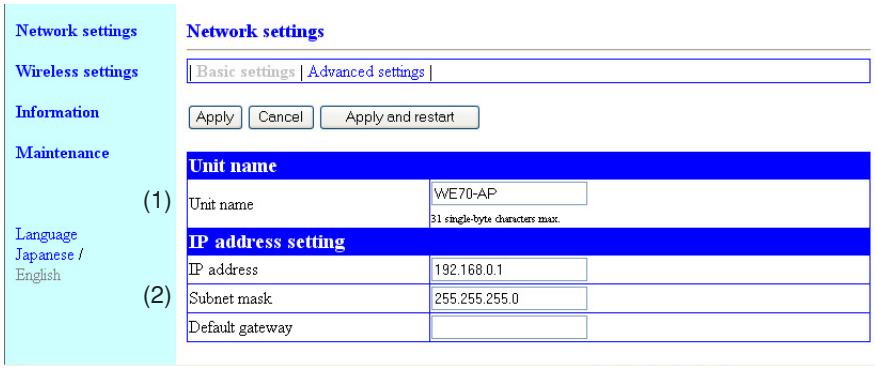
Setup item in a displayed menu screen can be registered or canceled.

For some items that require restart of a wireless unit to be enabled, Click <Apply and restart>.

5-2. Setup Screen (WE70-AP)

■ Network Settings

<Basic settings> Screen



● Unit Name/IP Address Setup

You can configure a name and an IP address of an access point.

<Apply> Button..... After a setup item in a setup screen is changed, pressing this button enables items in [Unit Name/IP address settings], other than [IP address] and [Subnet mask] fields.

* Changing an IP address and a subnet mask are reflected on a screen in respective fields, but they will not be enabled unless <Apply and restart> is clicked.

<Cancel> Button..... This button resets changed setup items in a setup screen to original settings before change. Note that the original setting cannot be recovered after <Apply> or <Apply and restart> button is clicked.

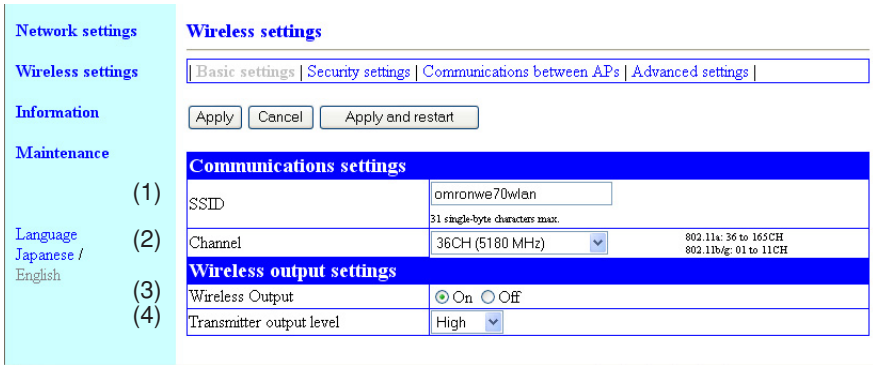
<Apply and restart> Button
..... Clicking this button restarts an access point and enables all setup items changed in the setup screen.

(1) Unit name..... You can enter an alphanumeric character string (within 31 characters) as a unit name. You cannot use symbols #, %, ¥, @, :, and ?.
(Factory Shipment Status:WE70-AP)

(2) IP address..... You can enter an IP address of an access point.
(Factory Shipment Status:192.168.0.1)
To connect a wireless unit to an operating network, this address must be changed to a proper network address of the LAN.

■ Wireless settings

<Basic settings> Screen



● Communications settings

This is a setup item for a wireless LAN card in a wireless unit.

<Apply> Button..... This button fixes a changed setup item in the "Wireless settings" screen. The changed item cannot be enabled unless <Apply and restart> is clicked.

<Cancel> Button..... This button resets changed setup items in the "Wireless settings" screen to original settings before the change.
Note that the original setting cannot be recovered after <Apply> or <Apply and restart> button is clicked.

<Apply and restart> Button
..... Clicking this button restarts an access point and enables all setup items changed in the "Wireless settings" screen.

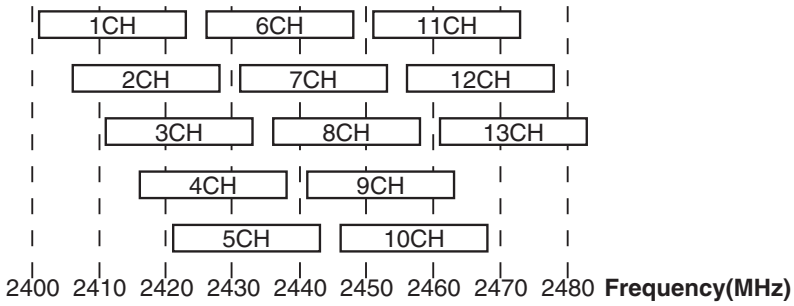
(1) SSID..... This is used for grouping of wireless networks.
If more than one wireless routers or access points exist in one wireless communication zone, cross talk with other wireless network group can be prevented by identification using different SSID (wireless network name) for each wireless network group.
Communication is not available with a wireless LAN terminal with a different SSID.
You can enter the desired alphanumeric characters in SSID (within 31 characters) with the attention for capitalization.
(Factory Shipment Status:omronwe70wlan)

* SSID and ESSID have the same meaning.
Some wireless LAN devices other than a wireless unit may call this ESS ID.

(2) Channel..... This is used to set a radio communication channel of a wireless unit.
(Factory Shipment Status:36CH (5180MHz))
A wireless LAN terminal automatically detects a channel of a wireless unit.

◎For communication by 2.4GHz (IEEE802.11b/g), select a channel from 1 to 13. (11 in United States)

* If other wireless network group exists that uses IEEE802.11b/g, "channels" of a wireless unit must be configured with blank channels of 4 or more between them to avoid radio interference.
  Otherwise a part of a band may overlap and cause cross talk as shown below.
  For example, channel configuration of 1, 6, and 11 channels for each other will not cause cross talk.



◎For communication by 5GHz (IEEE802.11a, select a channel from 36-64 (except China), 100-140 (except China, Japan), 149-165 (United States, Canada and China)

* DFS (Dynamic Frequency Selection) function will be activated if a channel of IEEE802.11a (52CH-64CH, 100CH-140CH) is selected. Detection of interfering radio waves such as weather radar automatically changes to a non-interfering IEEE802.11a wireless channel.
  Until a channel is changed after detection (for about 1 minute), wireless access to an access point is stopped. The DFS function is activated on startup and thus startup takes about 1 minute (WIRELESS lamp flashes).

* DFS function is stopped if a channel is changed to an IEEE802.11a (36CH-48CH, 149CH-165CH) channel.
* **For communication using 5GHz band [IEEE802.11a], radio interference will not occur as long as configured channels are different for each other.**

● **Wireless output settings**

(3) Wireless output ..... This item is used to temporarily stop emission of radio wave. It On or off wireless communication function.

(4) Transmitter output Level ..... You can configure transmission power of an access point.
Selection is available from high/middle/low (3 levels).(Factory Shipment Status:High)
Maximum transmission range of an access point can be achieved by the level "High".
Lower power level decreases a transmission range.
Assuming high wireless transmission power as 1.0, middle and low transmission power can be indicated as 0.5 and 0.25 respectively.

[Use Low Power Level When]
◎You want to reduce radio wave leak from wireless unit out of a room
◎You want to enhance security by limiting a communication area
◎You want to alleviate communication speed reduction by eliminating radio interference with a close client (slave) or an access point in an environment where more than one access point is installed in a comparatively small area

<Security settings> Screen

● **Encryption setting**

You can configure encryption for data protection of wireless LAN communication.

(1) Encryption method .....
* "WEP (RC4)", "OCB AES", "TKIP", "AES", and "WOC KEY" are not compatible with each other.

You can select an encryption method for wireless data.(Factory Shipment Status:None)Supported encryption types include "WEP (RC4)", "OCB AES", "TKIP", "AES", and "WOC KEY".
Communication partners with different encryption methods have no compatibility. Set the same configuration for encryption method and bit count between communication partners.

WEP (RC4)	This security setup is typically used for wireless LAN communication. It is based on WEP (RC4) (Rivest's Cipher 4) algorithm. This type uses a data block length of 8 bits and provides selection of an encryption key length. * You can select an encryption key length from 64(40)/128(104)/152(128) bits. * "WEP (RC4) 152(128)" type cannot be connected to a wireless unit using wireless network connection that comes with Windows XP.
OCB AES	This is a next-generation encryption method being standardized and is stronger than "WEP (RC4)". This type uses 128-bit data block and encryption key. As any encryption key can be configured for the 128 bits, it is stronger than WEP (RC4).
TKIP (Temporal Key Integrity Protocol)	This type automatically updates its encryption key in a given interval and is stronger than "WEP (RC4)". It can be used for a Windows XP (modification program applied to Service Pack 1) or Windows XP (Service Pack2) terminal.
AES (Advanced Encryption Standard)	It can be used for a Windows XP (modification program applied to Service Pack 1) or Windows XP (Service Pack2) terminal. * This type is enhanced in encryption and automatically updates its encryption key in a given interval, and is stronger than "WEP (RC4)".
WOC KEY (OC Security)	This is Omron's proprietary encryption.

(2) Key generator..... You can configure a character string to generate an encryption key for encryption and decryption if an encryption method of "WEP RC4 64(40)", "WEP RC4 128(104)", "WEP RC4 152(128)", or "OCB AES 128(128)" is selected in [Encryption method] field (1).
Enter the same alphanumeric characters (within 31 characters) with the attention for capitalization for communication partners.
Entered character is displayed as "*(asterisk)" or "•(black circle)". (Example: **)
Selecting an encryption key and clicking <Apply> displays a key, generated by a character string entered in the [Key generator] field, in a text box of the [WEP key] field.
Number of encryption key digits and characters in the [WEP key] text boxes depends on a selected encryption method.

* If the [Input mode] field of [WEP key] is configured as ASCII Characters, a key generator cannot be used.
* If None is selected in the [Encryption method], keys are not generated in the [WEP Key] text boxes.
* If configured character strings are different between communication partners, encrypted data cannot be decrypted.
* If they are directly set from [WEP key], the [Key generator] field shows nothing.
* As the 1st 24 bits of WEP (RC4) is automatically updated in a given interval, it is not displayed in WEP key text boxes.
* It is not compatible with other manufacturers' wireless LAN devices.

(3) PSK (Pre-Shared Key) .... You can enter an encryption key in alphanumeric characters.
This setup can be specified if "TKIP", "AES", or "WOC KEY" is selected in the [Encryption method] (1).

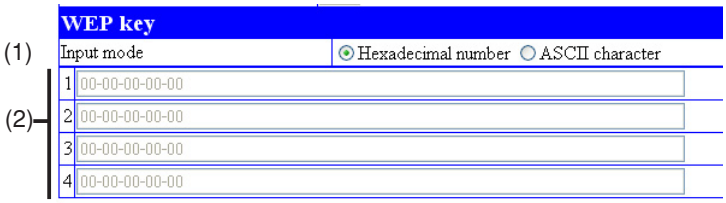
* The same encryption key must be configured for communication partners using the same encryption method.
* Enter 64-digit number if you want to use hexadecimal number.
* To use WOC KEY (OC security)", enter an 8 to 63 alphanumeric characters. You cannot enter 64-digit hexadecimal number. Enter an ASCII character string.
* Enter an 8 to 63 character string if you want to use an ASCII character string.

(4) Key index ..... You can specify a text box number for a key to encrypt send data, from 1 to 4 in the [WEP key] if an encryption method of "WEP RC4 64(40)", "WEP RC4 128(104)", "WEP RC4 152(128)", or "OCB AES 128(128)" is selected in [Encryption method] field (1). (Factory Shipment Status: 1)
If encryption keys specified in boxes from 1 to 4 are the same as those of a communication partner, communication is available even if different numbers are set between communication partners.

* If you want to specify a key index of a wireless LAN terminal for a wireless unit and use Windows XP (except for Service Pack applied) standard wireless network connection, a range of selection becomes from 0 to 3, which is different from a wireless unit.
  Selecting "1" for a wireless unit is same as specifying "0" in Key index (advanced) in Windows XP.

● **WEP key**

This item specifies an encryption key to be used for "WEP (RC4)" or "OCB AES" encryption type.



(1) Input mode..... You can select a mode for entering an encryption key. (Factory Shipment Status: Hex.)

* If an ASCII character is specified, [Key generator] in [Encryption method] cannot be used.

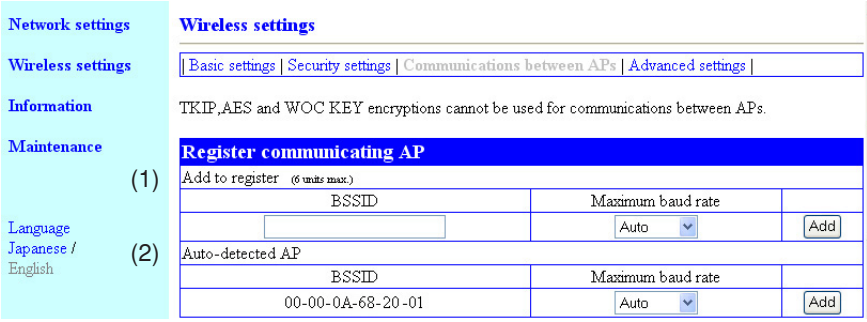
(2) Key Input Box..... If you do not use the key generator, directly enter a key for encryption and decryption with a specified mode in the [Input mode](1) field. (Factory Shipment Status: 00-00-00-00-00)
If [ASCII character] is specified in the [Input mode](1) field, entering other characters than hexadecimal number is invalid. (Alphanumeric character only)

* It is recommended to specify the same encryption key values for communication partners in respective key index (1 to 4).
  Communication will not be available if the other part of the communication uses a different value.

<AP-to-AP Bridging> Screen

● Register Communicating AP

You can register an AP-to-AP bridging partner's BSSID.



(1) Add to Register ..... You can enter a BSSID of an AP-to-AP bridging partner (access point).

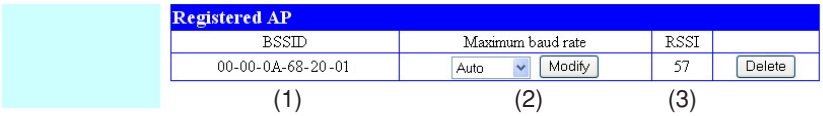
* Specify IP addresses of access points so that they should not be duplicate.
* Clicking <Add> registers the entered BSSID to [Registered AP].
* Up to 6 units' BSSIDs can be registered.
* Use 12-digit (hex.) alphanumeric characters for BSSID.
* Entering BSSIDs as shown below is handled as the same BSSID.
  (Example: 00-00-0A-68-20-01, 00000A682001)

(2) Auto-Detected AP ..... If an access point with the same channel and SSID as those of current access point is detected, its BSSID is displayed here.
For AP-to-AP bridging with the detected device, clicking <Add> in the right of this field registers the detected BSSID to [Registered AP].

* Up to 32 devices can be indicated if detected.

This is different from [Unit's MAC Address] in the "Network information" screen of "Information" menu.

● Registered AP



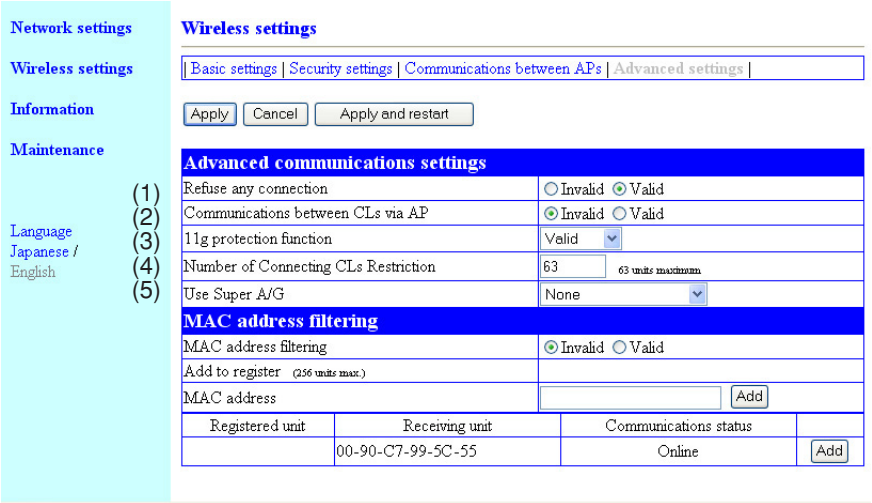
(1) BSSID ..... A BSSID registered in [Register communicating AP] is displayed here.
AP-to-AP bridging is available with Omron's wireless router or Omron's access point, with BSSID displayed in this list, supporting AP-to-AP bridging.

* To deregister, click <Delete> in the right of the field.
* Register AP-to-AP bridging partner's BSSID only.
  Registering more than one BSSID of other partners may result in decrease in communication speed.

(2) Maximum baud Rate ..... Indicates maximum speed between registered access points.

(3) RSSI..... Indicates a radio intensity received from a registered access point.

<Advanced settings> Screen



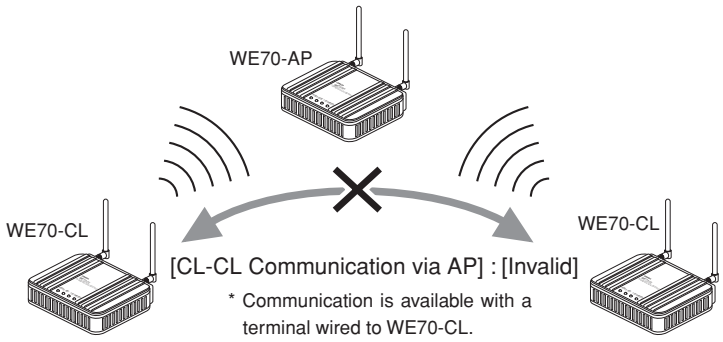
● **Advanced communications settings**

This setup item allows communication between wireless LAN terminals via an access point.

(1) Refuse any connection... This item specifies whether search and/or connection should be enabled or disabled from a wireless LAN terminal using [ANY] mode (automatic access point search & connection).
(Factory Shipment Status:Valid)
Setting "Valid" this function interfere communication with a client (slave) with a blank SSID. Also, SSID of an access point cannot be seen.
If this setup item is being valid, a device cannot be searched by a wireless LAN terminal under ANY mode using Windows XP standard wireless network connection or setup utility of a wireless LAN card supporting wireless network display.
Setting "Invalid" this function allows communication with a client (slave) with a blank SSID, and an access point SSID can be seen by a communication partner.

(2) Communications between CLs via AP
..... This setup item allows communication with a client (slave) via an access point. Setting "Valid" this setup item allows communication.

* This function is valid for a wireless LAN terminal supporting wireless LAN standards of a wireless channel specified in the access point.



(3) 11g protection function ..

* This function is invalid if a channel of IEEE802.11a is specified.

This function can prevent decrease of communication speed due to an environment mixed with IEEE802.11b by prioritizing IEEE802.11g. (Factory Shipment Status: Valid)

◎Invalid : Communication speed may decrease if an environment includes a wireless LAN device using IEEE802.11b.

◎Valid : Prioritizes IEEE802.11g wireless communication to ensure throughput if an environment includes IEEE802.11g and IEEE802.11b terminals.

◎11g Only : Inhibits communication with an adjacent IEEE802.11b wireless device.

(4) Number of Connecting CLs Restriction

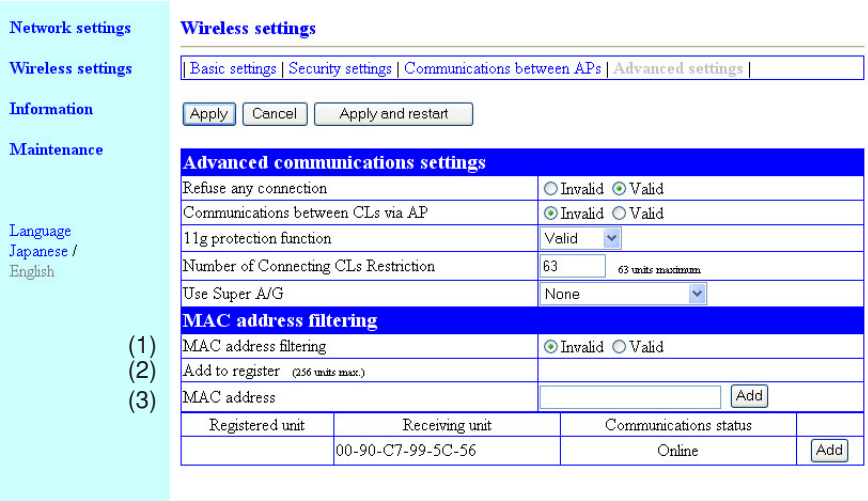
..... Specifies number of clients (slaves) that can be connected to an access point at the same time.
An available range is from 1 to 63. (Factory Shipment Status: 63)
If this limitation is specified, concentration of connections to only 1 access point can be prevented (wireless unit load can be distributed), thus decrease of communication speed can be prevented.

(5) Use Super A/G ..... This technology was developed by Atheros Communications in the U.S. for higher speed wireless LAN.(Factory Shipment Status:None)
Selection is available from "None", "Use w/o compression" and "Use w/ compression". Specifying "Use w/ compression" can further increase communication speed.
For AP-to-AP bridging, "Super A/G" setup must be matched.

* If compressed data is often handled, specifying "Use w/ compression" may decrease the speed during transmission of compressed data.
  In such a case specify "Use w/o compression".
* If a wireless LAN card of a terminal does not support "Super A/G", its operation is the same as that for specifying "None" in [Use Super A/G].

● **MAC address filtering**

This setup item allows communication with a wireless unit (MAC address) registered in an access point.



(1) MAC address filtering

..... This function specifies whether wireless connection for a client (slave) with a registered MAC address only or not
(Factory Shipment Status:Invalid)

* If "Valid" is specified, access cannot be made from a wireless LAN terminal with a MAC address not registered in [Current Registration] to a wireless unit.

(2) Add to register ..... You can enter a MAC address of a wireless unit for which access should be permitted and click <Add>.

* The registered MAC address is displayed in the [Registered unit] field. If the MAC address filtering is being enabled, communication is available with a wireless LAN terminal only with the MAC address.
* It cannot be specified for an access point using AP-to-AP bridging.
* Up to 256 units' MAC addresses can be registered.
* Use 12-digit (hex.) alphanumeric characters.
* The following character strings are the same MAC address.

(Example:00-00-0A-68-20-01, 00000A682001)

(3) Registered unit..... Displays statuses of wireless unit registration and communication.
A MAC address can be displayed in the [Receiving unit] field for a wireless unit with an unregistered MAC address, which can be additionally registered by clicking <Add>.

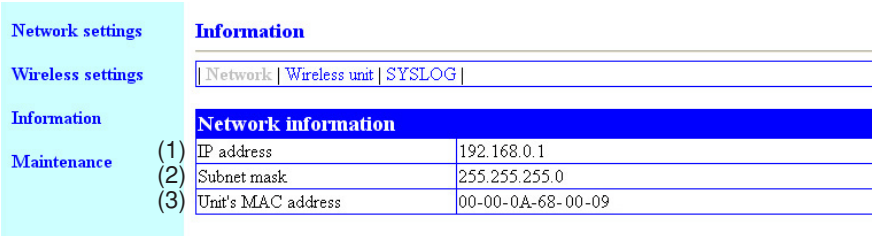
* To deregister, click <Delete> in the right of the field.

■ Information

<Network> Screen

● Network Information

This screen displays network information.



(1) IP address ..... Displays an IP address of an access point.

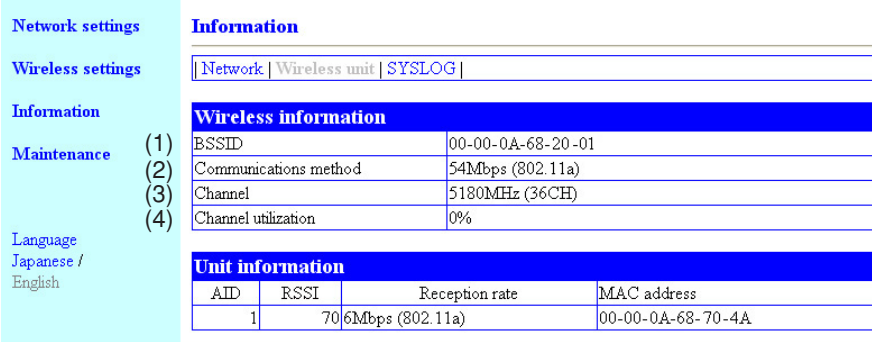
(2) Subnet mask ..... Displays a subnet mask of an access point.

(3) Unit's MAC address
..... Displays a MAC address (wired end) of an access point.

<Wireless unit> Screen

● Wireless information

This screen displays a communication status of a wireless unit.
Indication of RSSI and Receiving rate are not updated unless data communication is being performed.



(1) BSSID ..... Indicates a MAC address (wired end) of an access point. To use AP-to-AP bridging, register a BSSID in the screen to a partner access point.

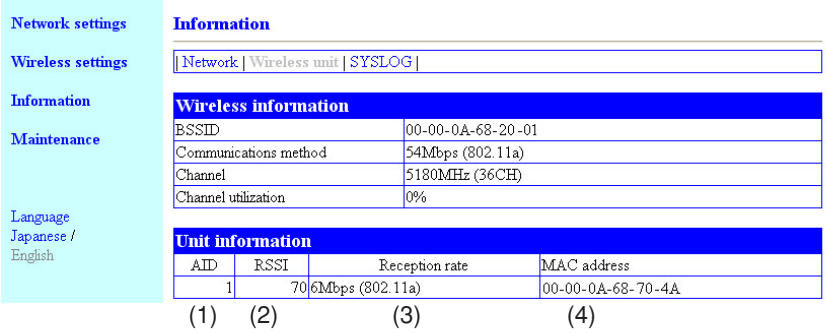
(2) Communications method Indicates a type of communication being used.

(3) Channel ..... Indicates a communication channel being used.

(4) Channel utilization ..... Indicates a percentage of busy status when search is made if a channel is free before data transmission.

● Unit information

This screen displays radio intensity and communication speed during data communication.



(1) AID ..... Indicates an access point as "0" and clients as 1 to 63.

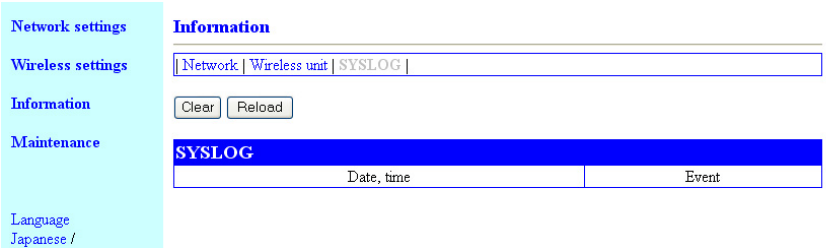
(2) RSSI ..... Indicates a Received Signal Strength Intensity from a terminal.

(3) Reception rate ..... Indicates a received data speed from a terminal.
As an access point sends a beacon signal every 100ms, the beacon signal is sent in an interval of communication even while data communication is being performed. Momentary receiving rate is displayed as 6Mbps or 1Mbps. Beacon transmission speed is 6Mbps for 11a and 1Mbps for 11b/g.

(4) MAC address ..... Indicates a terminal MAC address (wireless end) of a client (slave) and a BSSID of an access point.

● SYSLOG

This screen displays history of startup and connection.



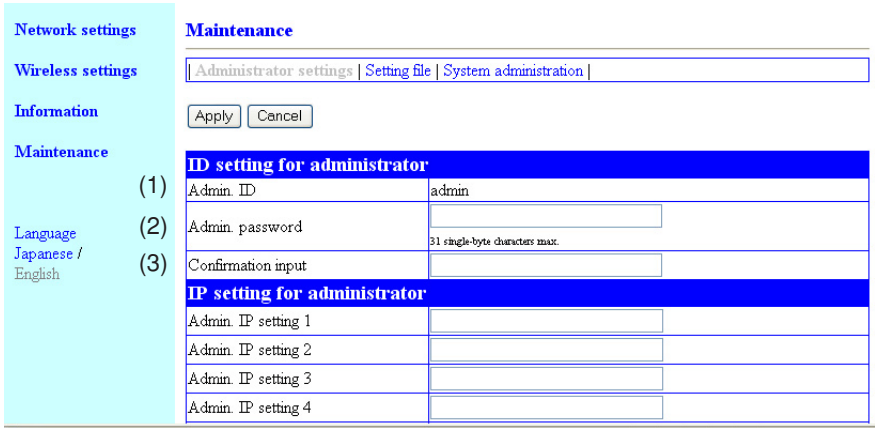
Trigger Conditions Displayed in SYSLOG (Categorized)		Message in SYSLOG	Remarks
Wireless LAN			
	Wireless Terminal Connected	join wireless terminal (XX:XX:XX:XX:XX:XX)	XX:XX:XX:XX:XX:XX indicates a MAC address
	Wireless Terminal Disconnected	remove wireless terminal (XX:XX:XX:XX:XX:XX)	
Administrator IP Limitation			
	Connection Refusal	refused connect from XXX.XXX.XXX.XXX	XXX.XXX.XXX.XXX indicates an IP address
On Start-Up			
	Version	root : WE70-AP Ver. x.xx	x.xx indicates version information
	HTTP Server Startup	httpd : thttpd starting on port 80	
	Startup Completed	root : System is ready	

■ Maintenance

<Administrator settings> Screen

● ID Setting for administrator

You can configure access control to a setup screen of an access point.



<Apply> Button..... Clicking this button enables all setup items changed in the "Administrator settings" screen.

<Cancel> Button..... This button resets changed setup items in the "Administrator settings" screen to original settings before the change.
Note that the original setting cannot be recovered after <Apply> button is clicked.

(1) Admin. ID ..... Fixed to "admin".

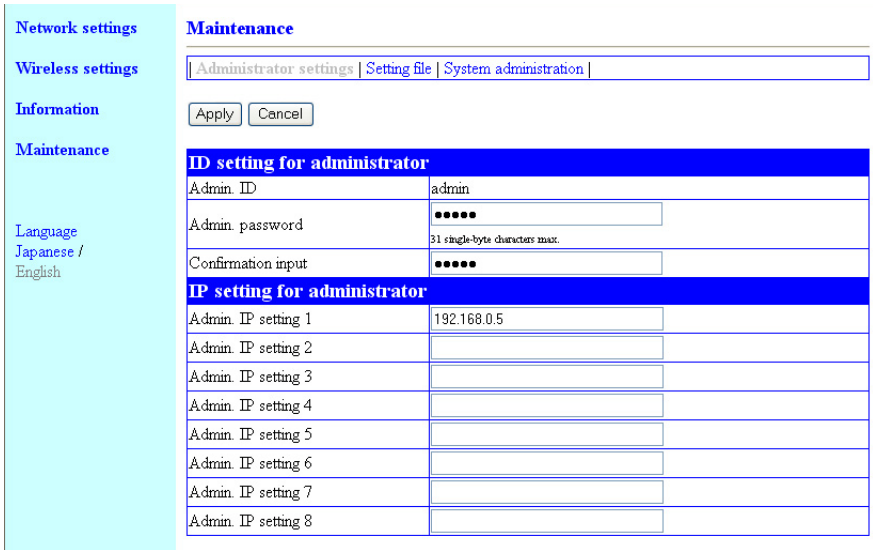
(2) Admin. Password
..... To set a password for an administrator ID, enter the desired alphanumeric characters (within 31 characters) with the attention for capitalization. Entered character is displayed as "*(asterisk)" or "•(black circle)". (Example: ****)
If an administrator password is being specified, a user is asked to enter the password for access. Enter this administrator password.

(3) Confirmation Input..... Enter new password again for confirmation.(Example: ****)

> ⚠ **Caution** If you forget the administrator password, you will not be able to check the settings.
> In such a case you must reset the unit to its factory shipment status.

● IP setting for administrator

This item is used to specify restriction on access to a setup screen by an IP address.

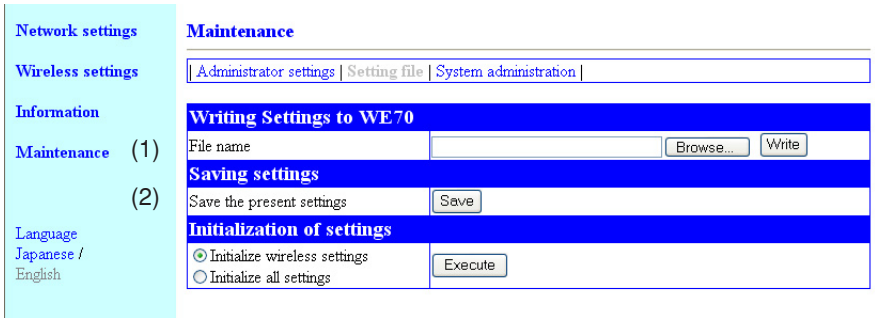


To limit access to a setup screen of an access point, the administrator can register up to 8 terminal IP addresses that make wired or wireless access to the access point.
IP setting for administrator cannot include its own IP address.
Example of Unavailable Setup:192.168.0.1 (Initial value)

* If an administrator IP address is specified, only terminals with registered IP addresses can make access to a setup screen of an access point.
* If it is blank, any terminal connected to the access point can make access to a setup screen.

<Setting file> Screen

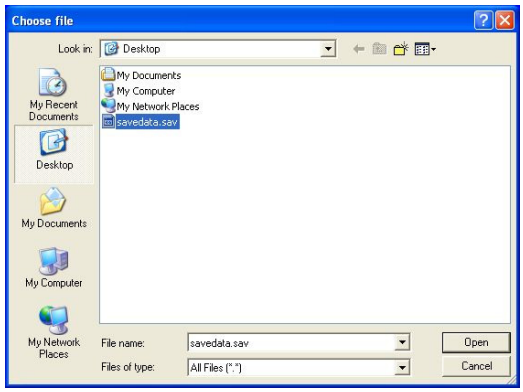
This screen allows a user to save access point setup details and write saved setup file to an access point.



● **Writing of settings**

(1) File Name ..... This item is used to write setup data into a wireless unit by opening a saved setting file (file extension .sav).

Directly enter a location of the saved setup file into the text box, or click <Browse>.
Click a setting file you want in the top right of the screen, then click <Open>.
Specify a saved location. Clicking <Write> writes the setup data to the access point.
Note that setup data will be overwritten.



* Setup data edited by off-the-shelf software may cause malfunction and must not be written to an access point.

● **Saving settings**

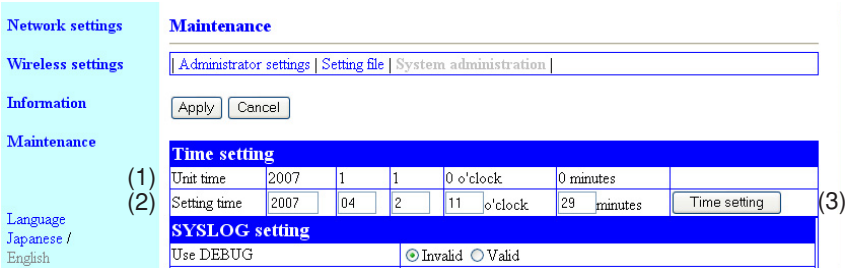
(2) Save the present settings .. Saving setup data of all access points to PC allows backup of access point setup.

Clicking [Save] in the [Save the present settings] displays a screen (right).
Clicking <Save> saves the setup file.
A setup file type (file extension) is ".sav".
The saved setup file can be written to a wireless unit itself or other device using a wireless unit by operation in [File Name] (1).

<System administration> Screen

● Time setting

You can configure the internal clock of an access point. An access point records history in SYSLOG. To record its date and time, configure the clock.



<Apply> Button..... Clicking this button enables all setup items changed in the "Time setting".

<Cancel> Button..... This button resets changed setup items in the "Time setting" screen to original settings before the change.
Note that the original setting cannot be recovered after <Apply> button is clicked.

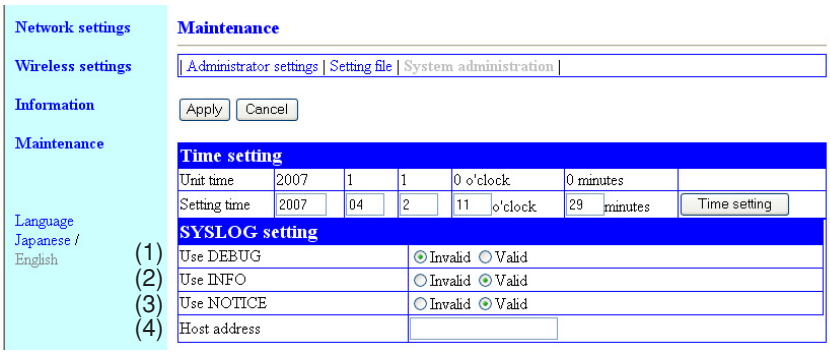
(1) Unit Time..... Displays time set in an access point.

(2) Setting time ..... Indicates time when access to a setup screen of the access point is made.
* Clicking <Refresh> of a WWW browser acquires and displays time of the terminal.

(3) <Time setting> Button .... This button is used to set time displayed in [Time to Set](2) to the access point.
To set correct time, make access to access point setup screen again, or click WWW browser <Refresh> and <Set Time>.

● SYSLOG setting

This item specifies output of log information to a specified host address.



(1) Use DEBUG ..... You can specify whether debug information output should be made to SYSLOG or not. (Factory Shipment Status: Invalid)

(2) Use INFO..... You can specify whether INFO type message output should be made to SYSLOG or not. (Factory Shipment Status: Valid)

(3) Use NOTICE..... You can specify whether NOTICE type message output should be made to SYSLOG or not. (Factory Shipment Status: Valid)

(4) Host Address..... To use the SYSLOG function, enter a host address to receive SYSLOG. The host must support SYSLOG server function.

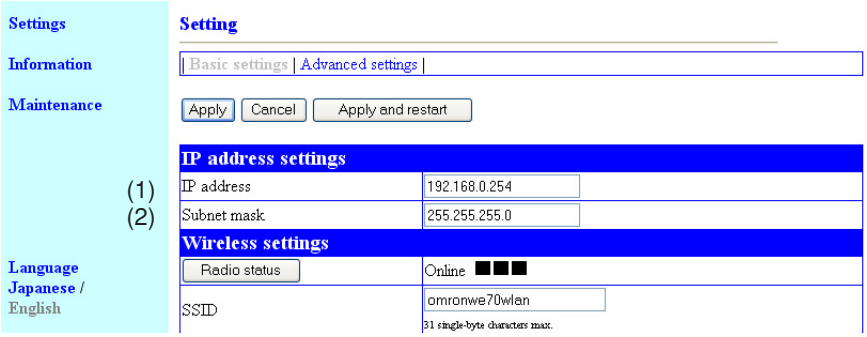
5-3. Setup Screen (WE70-CL)

■ Settings

<Basic settings> Screen

● IP address settings

You can specify a client IP address.



(1) IP address..... You can enter an IP address of a client.
(Factory Shipment Status:192.168.0.254)

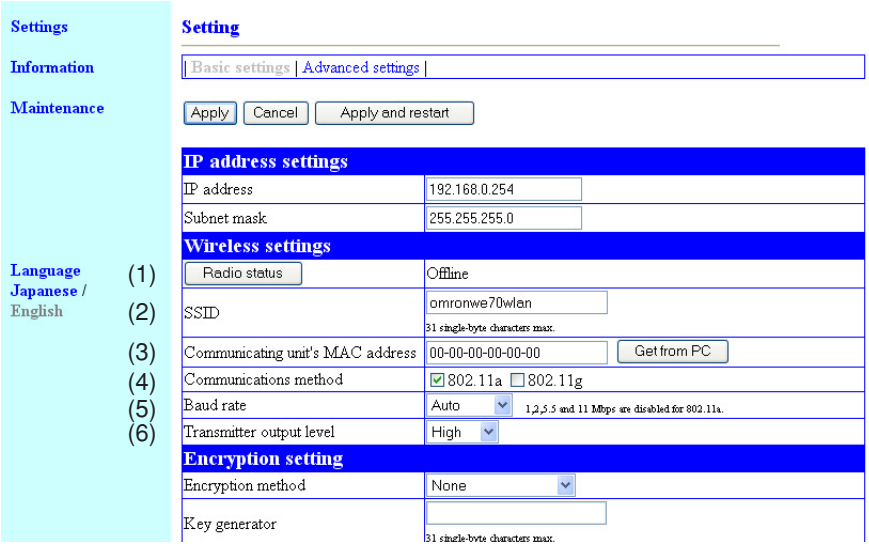
* Specify a value that does not overlap that of other network devices.

* To make access to client setup screen, specify an IP address set in this field.

(2) Subnet mask..... You can specify a client subnet mask (a range of IP addresses used for the same network group).
(Factory Shipment Status: 255.255.255.0)

● Wireless settings

You can specify basic wireless communication setup for a client (slave).



(1) <Radio status> Button.... Radio intensity that an access point can receive is displayed in the right of this button. If the client has different SSID and/or encryption setup from the access point, "Communication Unavailable" is displayed.
Radio intensity is displayed in 4 levels as shown below.
Levels may differ depending on a communication method.

* Level : □□□ ■□□ ■■□ ■■■

0-8	9-14	15-20	21 or higher (in case of 802.11a)
0-13	14-19	20-25	26 or higher (in case of 802.11b/g)

Clicking <Radio status> allows monitoring of statuses of wireless communication such as channels and communication speed in the [Wireless communication status].

(2) SSID..... An access point and a client (slave) have an SSID as a wireless network name to identify a communication partner (Factory Shipment Status: omronwe70wlan).
Wireless LAN devices with different SSIDs in the same group cannot communicate with each other.
You can enter the desired alphanumeric characters in SSID (within 31 characters) with the attention for capitalization.

* SSID and ESSID have the same meaning.
  Some wireless LAN devices other than a wireless unit may call this ESSID.

(3) Communicating unit's MAC Address
..... Indicates a wireless module MAC address of a client (slave).
Clicking <Get from PC> automatically acquires and displays PC's MAC address. To get an address from PC, you must open a setup screen on PC wired to a client (slave). If you open a client (slave) setup screen on PC connected to an access point, communication becomes unavailable.
If it is connected to PLC, PLC's MAC address is acquired.
(Factory shipment setting: Wireless module MAC address)

(4) Communications method

* If an access point supports 802.11b only, specify 802.11g.

You can specify wireless LAN standard (802.11a/802.11g) for a wireless unit. (Factory Shipment Status: 802.11a)

* 802.11a and 802.11g (including 802.11b) can be specified at the same time.
* If 802.11a and 802.11g are configured and "Auto" is specified for [Baud Rate], connection will be made to an access point with better radio wave status where 802.11a/b/g are used at the same time.

(5) Baud rate ..... Use the minimum speed for a specified communication method in a system design phase. (6M for 802.11a and 1M for 11 b/g)
Even if communication is available in system verification while peripheral equipment is not operating, a timeout error may occur when a communication environment get worsened. Specify "Auto" for actual operation. Specifying "Auto" automatically switches communication speed to one specified in [Communication method] even when communication becomes unstable due to environment changes.
(Factory Shipment Status: Auto)
Baud rate depends on a mode specified in [Communication method].
If an unavailable baud rate is set, operation will be made with "Auto" (Factory Shipment Status).

* If "802.11g" or "802.11a" is specified, 54/48/36/24/18/12/9/6Mbps are the rate supported when other setting than "Auto" (Factory Shipment Status) is set.
* If "802.11b" is specified, 11/5.5/2/1Mbps are the rate supported when other setting than "Auto" (Factory Shipment Status) is set.
* If "802.11a" is specified and [Baud rate] is set to either of 11/5.5/2/1Mbps, operation will be made with transmission rate as "Auto" (Factory Shipment Status) because the baud rate setting is unmatched with "802.11a".
* To communicate with an access point dedicated to "802.11b", specify either of Auto (Factory Shipment Status)/11/5.5/2/1Mbps.

(6) Transmitter output level .... You can specify wireless transmission power for a wireless unit.
Selection is available from high/middle/low (3 levels). (Factory Shipment Status: High)
A wireless communication range of a wireless unit (see "1-1. Features", "Wireless communication distance" (P.1-3)) can be achieved when the transmission power level is "High".

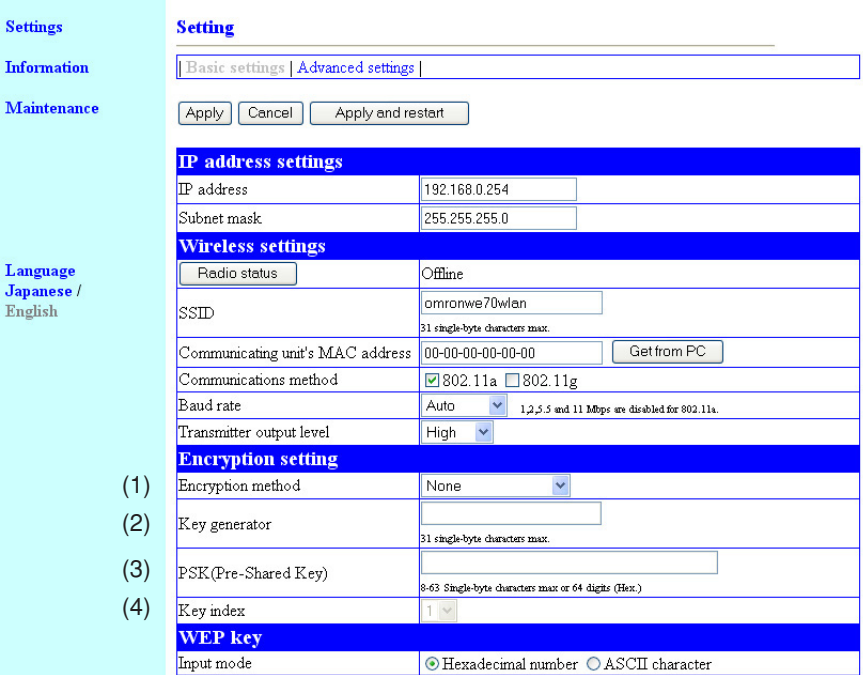
Lower transmission power level decreases a transmission range.

[Use Low Transmission Power Level When]

◎You want to reduce radio wave leak from wireless unit out of a room
◎You want to enhance security by limiting a communication area
◎You want to alleviate communication speed reduction by eliminating radio interference with a close client or an access point in an environment where more than one access point is installed in a comparatively small area

● Encryption setting

You can configure encryption for data protection of wireless LAN communication.



(1) Encryption method .....

* "WEP (RC4)", "OCB AES", "TKIP", "AES", and "WOC KEY" are not compatible with each other.

You can select an encryption method for wireless data. (Factory Shipment Status: None) Supported encryption method includes "WEP (RC4)", "OCB AES", "TKIP", "AES", and "WOC KEY".
Communication partners with different encryption types have no compatibility. Set the same configuration for encryption method and bit count between communication partners.

WEP (RC4)	This security setup is typically used for wireless LAN communication. It is based on WEP (RC4) (Rivest's Cipher 4) algorithm. This type uses a data block length of 8 bits and provides selection of an encryption key length. * You can select an encryption key length from 64(40)/128(104)/152(128) bits. * "WEP RC4 152(128)" type cannot be connected to a wireless unit using wireless network connection that comes with Windows XP.
OCB AES	This is a next-generation encryption method being standardized and is stronger than "WEP (RC4)". This type uses 128-bit data block and encryption key. As any encryption key can be configured for the 128 bits, it is stronger than WEP (RC4).
TKIP (Temporal Key Integrity Protocol)	This type automatically updates its encryption key in a given interval and is stronger than "WEP (RC4)". It can be used for a Windows XP (modification program applied to Service Pack 1) or Windows XP (Service Pack2) terminal.
AES (Advanced Encryption Standard)	It can be used for a Windows XP (modification program applied to Service Pack 1) or Windows XP (Service Pack2) terminal. * This type is enhanced in encryption and automatically updates its encryption key in a given interval, and is stronger than "WEP (RC4)".
WOC KEY (OC Security)	This is Omron's proprietary encryption.

(2) Key generator.....

* Some of Omron's wireless LAN devices use "Key ID" for this purpose.

You can configure a character string to generate an encryption key for encryption and decryption if an encryption type of "WEP RC4 64(40)", "WEP RC4 128(104)", "WEP RC4 152(128)", or "OCB AES 128(128)" is selected in [Encryption method] field (1).
Enter the same alphanumeric characters (within 31 characters) with the attention for capitalization for communication partners.
Entered character is displayed as "*(asterisk)" or "•(black circle)". (Example: ••••)
Selecting an encryption key and clicking <Apply> displays a key, generated by a character string entered in the [Key generator] field, in a text box of the [WEP key] field.
Number of encryption key digits in the [WEP key] text boxes depends on a selected encryption type.

* If the [Input mode] field of [WEP key] is configured as ASCII Characters, a key generator cannot be used.
* If None is selected in the [Encryption method], keys are not generated in the [WEP key] text boxes.
* Communication will not be available if the generated encryption key is different from that of the access point.
* If they are directly set from [WEP key], the [Key generator] field shows nothing.
* As the 1st 24 bits of WEP (RC4) is automatically updated in a given interval, it is not displayed in WEP key text boxes.

(3) PSK (Pre-Shared Key) .... Enter a PSK (Pre-Shared Key) in alphanumeric characters.
This setup can be specified if "TKIP", "AES", or "WOC KEY" is selected in the [Encryption method] (1).

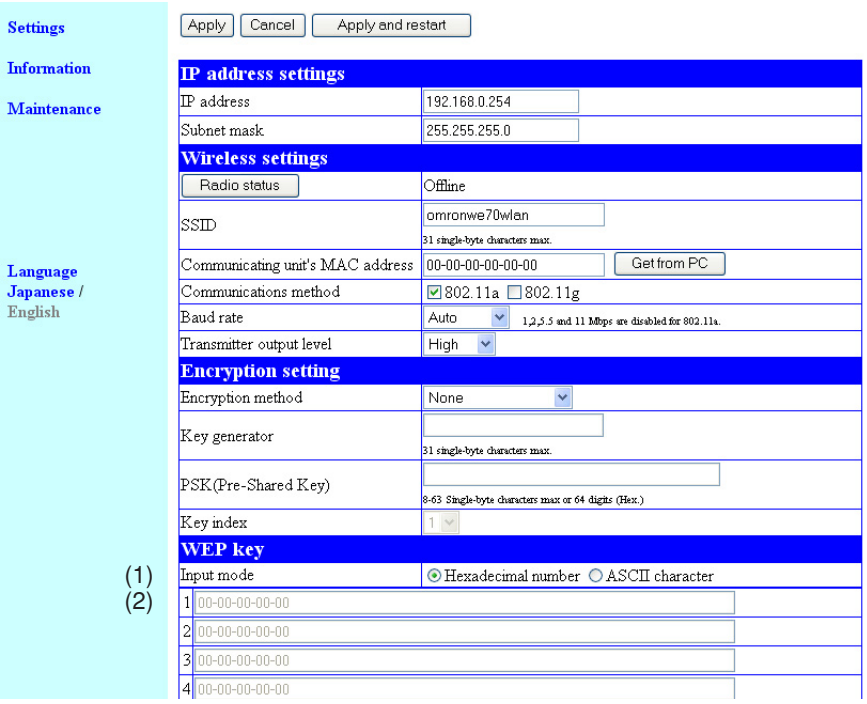
* The same encryption key must be configured for an access point using the same encryption method.
* Enter 64-digit number if you want to use hexadecimal number.
* Enter an 8 to 63 character string if you wan to use an ASCII character string.

(4) Key index ..... You can specify a text box number for a key to encrypt send data, from 1 to 4 in the [WEP key] if an encryption type of "WEP RC4 64(40)", "WEP RC4 128(104)", "WEP RC4 152(128)", or "OCB AES 128(128)" is selected in [Encryption method] field (1). (Factory shipment setting: 1)

* If encryption keys specified in boxes from 1 to 4 are the same as those of an access point, communication is available even if different numbers are set between communication partners.

● **WEP key**

This item specifies an encryption key to be used for other than "TKIP" or "AES" encryption type.



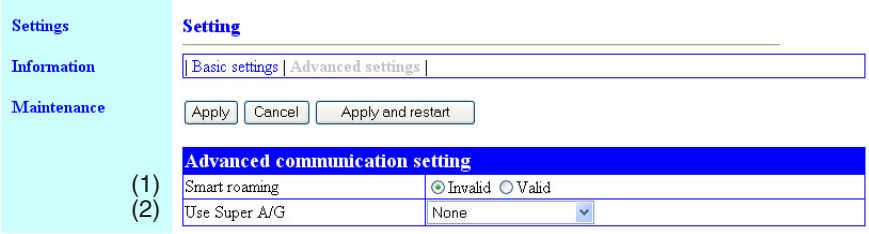
(1) Input mode..... You can select a mode for entering an encryption key.(Factory Shipment Status: Hex.)

* If an ASCII character is specified, the key generator cannot be used.

(2) Key Input Box..... Directly enter a key for encryption and decryption with a specified mode in the [Input mode](1) field.(Factory Shipment Status: 00-00-00-00-00)

* Other characters than those used for hexadecimal number are invalid.
* Specify the same WEP keys for communication partners; encryption keys for key index to be used.
  Communication will not be available if encryption keys are different for a key index to be used.

<Advanced settings> Screen

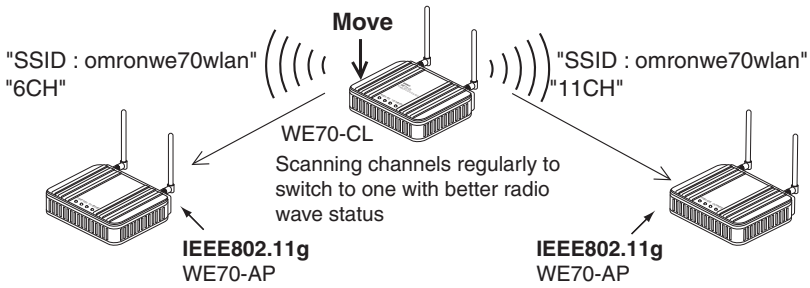


● Advanced communication setting

(1) Smart roaming.....

* All of SSID and Encryption setup must be the same.

If communications get worse after a client (slave) is moved to another access point, the client starts detecting another access point that may provide better communications.
When the client finds a good access point, it switches its wireless connection to the good point to maintain stable communications (see below).
When performance of smart roaming switching time is required, it is recommended that WE70-AP and WE70-CL should be combined.
(Factory Shipment Status: Invalid)



* If spanning tree is being enabled, switching will take several seconds even if smart roaming is being enabled.

(2) Use Super A/G.....

This technology was developed by Atheros Communications in the U.S. for higher speed wireless LAN. (Factory Shipment Status: None)
Selection is available from "None", "Use w/ compression" and "Use w/o compression".

* Specifying "Use w/ compression" can further increase communication speed.
* If compressed data is often handled, specifying "Use w/ compression" may decrease the speed during transmission of compressed data.
In such a case specify "Use w/ compression".
* Different settings between communication partners result in the same operation as that with this function disabled.

■ Information

● Network information

Settings
Information
Maintenance

Information

	Network information	
(1)	IP address	192.168.0.254
(2)	Subnet mask	255.255.255.0
(3)	Unit's MAC address	00-90-C7-B0-02-11
	Wireless information	
	BSSID	00-90-C7-99-5C-52
	Communications method	IEEE802.11a

(1) IP address..... Displays an IP address of a client (slave).

(2) Subnet mask..... Displays a subnet mask of a client (slave).

(3) Unit's MAC address
..... Displays a MAC address (wired end) of a client (slave).

● Wireless information

Settings
Information
Maintenance

Information

	Network information	
	IP address	192.168.0.254
	Subnet mask	255.255.255.0
	Unit's MAC address	00-90-C7-B0-02-11
	Wireless information	
(1)	BSSID	00-90-C7-99-5C-52
(2)	Communications method	IEEE802.11a

(1) BSSID ..... Register communicating access point BSSIDs.

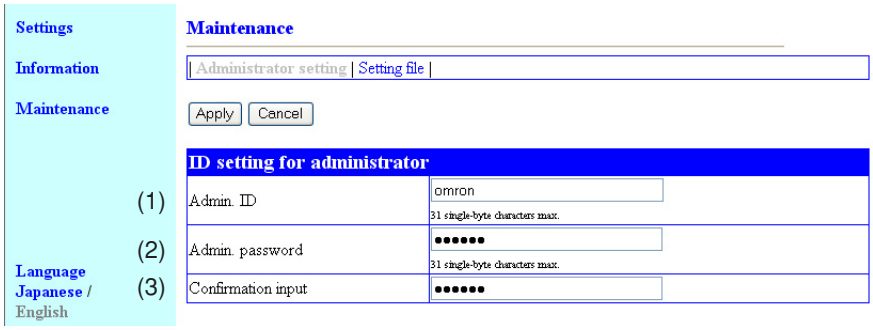
(2) Communication method... Indicates a type of communication being used.
IEEE802.11a or IEEE802.11b/g

■ Maintenance

<Administrator settings> Screen

● **ID setting for administrator**

You can configure access control to a setup screen of a client (slave).



(1) Admin. ID ..... To limit access to a setup screen of a client (slave), enter the desired alphanumeric characters (within 31 characters) with the attention for capitalization. (Example: omron)

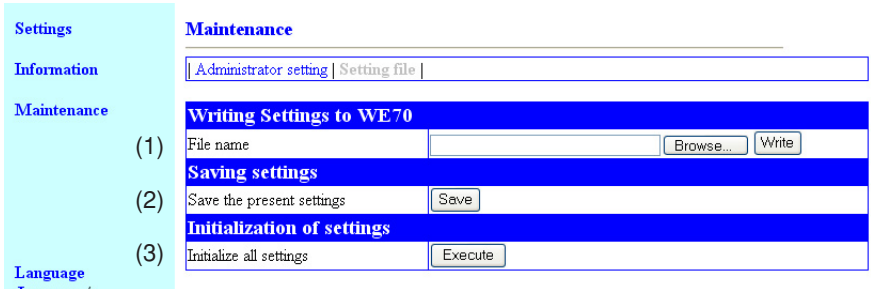
* If an administrator ID is being specified, a user is asked to enter the user name for access. Enter this administrator ID.

(2) Admin. Password ..... To set a password for an administrator ID, enter the desired alphanumeric characters (within 31 characters) with the attention for capitalization. Entered character is displayed as "*(asterisk)" or "•(black circle)". (Example: ••••••)

* If an administrator password is being specified, a user is asked to enter the password for access. Enter this administrator password.

(3) Confirmation input..... Enter new administrator password again for confirmation. (Example: ••••••)

<Settings file> Screen



● **Writing settings**

(1) File name ..... This item is used to write setup data into a wireless unit by opening a saved setup file (file extension .sav).

● **Saving settings**

(2) Save the present settings.. Saving all setup data of a client to PC allows backup of client setup.

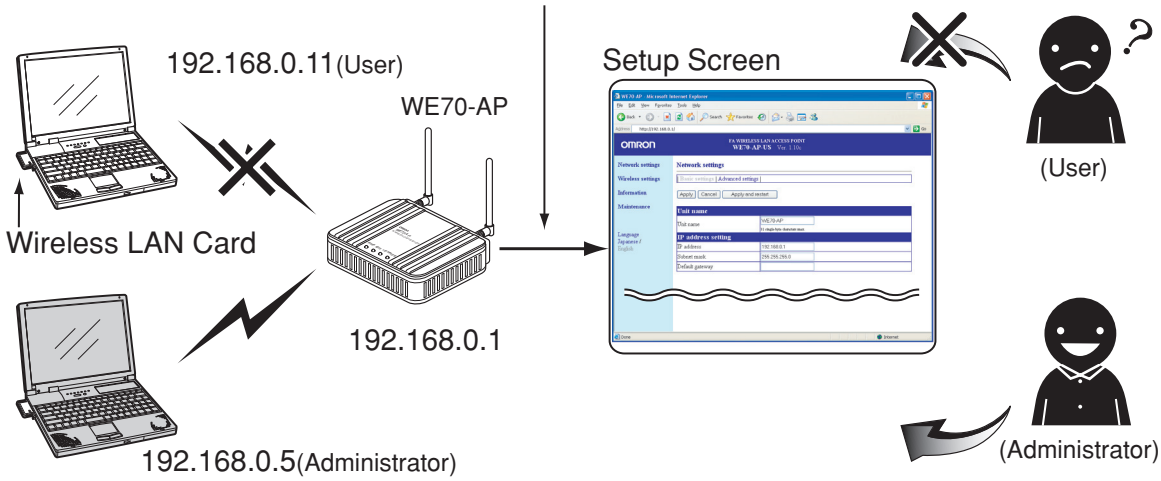
● **Initialization of setings**

(3) Initialize all settings..... All of wireless unit setup items are restored to factory shipment status.

5-4. Limiting Setup Screen Access

Specifying administrator's ID, password, and IP address can inhibit any change for wireless unit setup via a WWW browser by others than the administrator.
If an administrator IP address is specified, only terminals with registered IP addresses can make access to a setup screen of an access point.
Specify a fixed IP address to an access point to be used by the administrator.
Specifying administrator ID and password to a client (slave) can inhibit easy access to a setup screen by others than the administrator.

The administrator of the registered IP Address makes an access using [ID] or [Password]



<To Configure>

Setup on WE70-AP

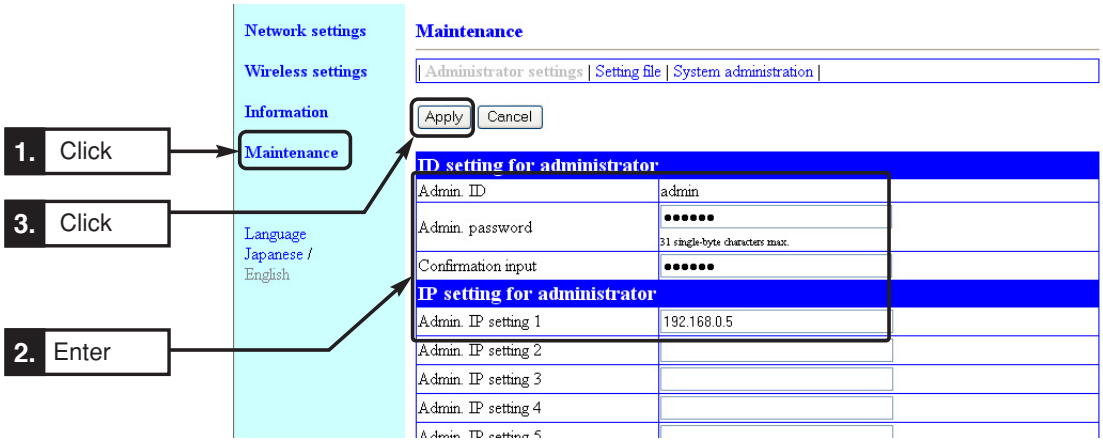
(1) Click "Maintenance" menu.
- An "Administrator Setup" screen is displayed.

(2) Enter an IP address of PC used for the administrator to [Admin. IP setting 1] in the [IP setting for administrator].
(Example: 192.168.0.5)

(3) To set an administrator password at the same time, enter an administrator password with any alphanumeric character string (within 31 characters) in [Admin. password] and [Confirmation input] fields of [ID setting for administrator].
(Input Example: uspass, Display Example: ••••••)
Entered character is displayed as "•(black circle)".

(4) Click <Apply>.
- Setup is now being enabled.

A screen asking user name and password will be displayed. Enter these administrator ID and password.



<To Configure>

Setup on WE70-CL

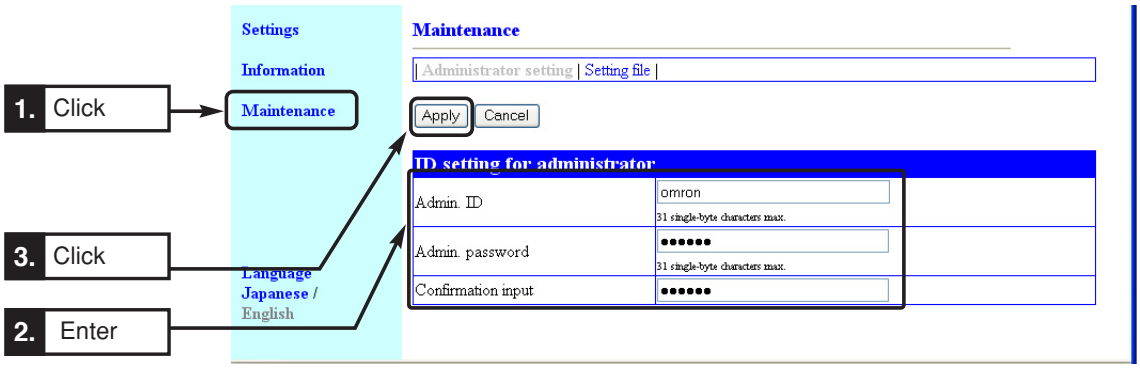
(1) Click "Maintenance" menu.
- An "Administrator settings" screen is displayed.

(2) Enter an administrator ID with any alphanumeric character string (within 31 characters) in [Admin. ID] of the [ID setting for administrator]. (Example: omron)

(3) Enter an administrator ID with any alphanumeric character string (within 31 characters) in [Admin. password] and [Confirmation input] fields of the [ID setting for administrator].
(Example: uspass, Display Example: ••••••)
Entered character is displayed as "•(black circle)".

(4) Click <Apply>.
- Setup is now being enabled.

A screen asking user name and password will be displayed. Enter these administrator ID and password.



Replacement Procedure

Chapter 6

This chapter describes
how to save or initialize setup data for wireless unit replacement. Read this chapter when necessary.

6-1. Replacing Wireless Unit 6-2
■ Saving Setup Data.....6-2
■ Writing Saved Setup Data 6-4
6-2. Restoring to Factory Shipment Status.....6-5
■ Using <INIT> Button 6-5
■ Using Setup Screen.....6-6

6-1. Replacing Wireless Unit

■ Saving Setup Data

This section describes how to save setup data changed in the setup screen of a wireless unit into PC as a setup file.

Setup file save must be made independently for an access point and a client (slave).

Setup files are required for wireless unit replacement.

* Saving setup data can help restore data when it is lost by an accident.

<To Save>

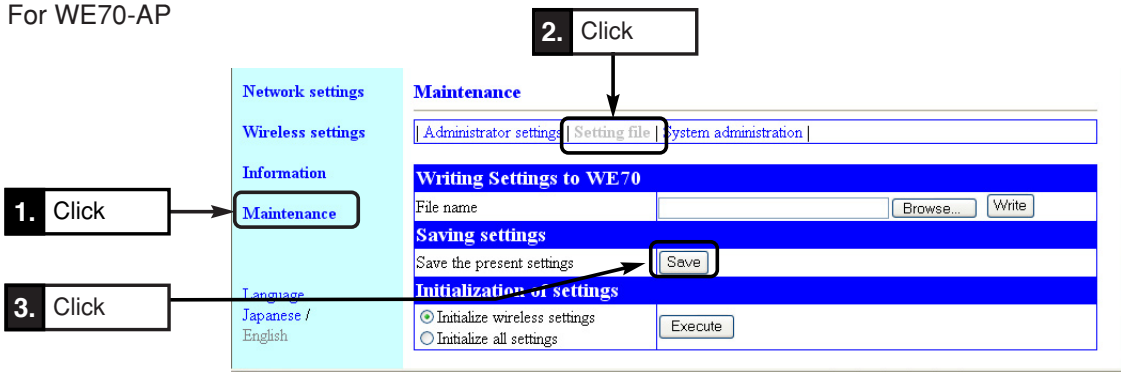
(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Maintenance menu > Setting file.

(2) Click Save in save the current configuration field of Saving settings.
A "Downloading files" screen is displayed.

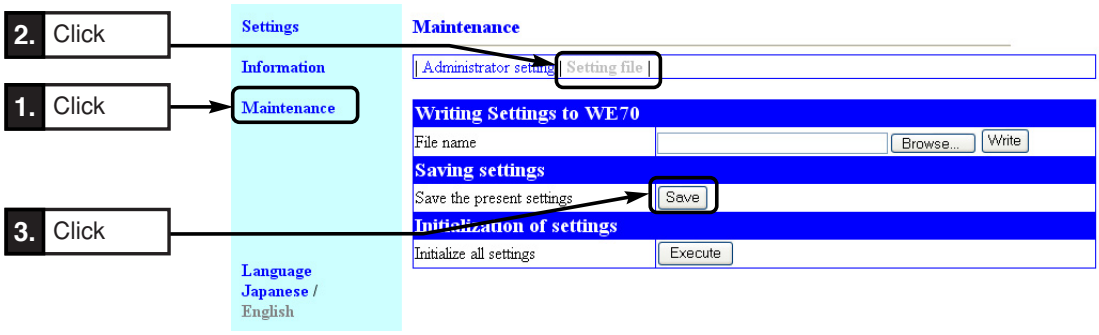
(3) Click <Save>.
- A "Rename" screen is displayed.

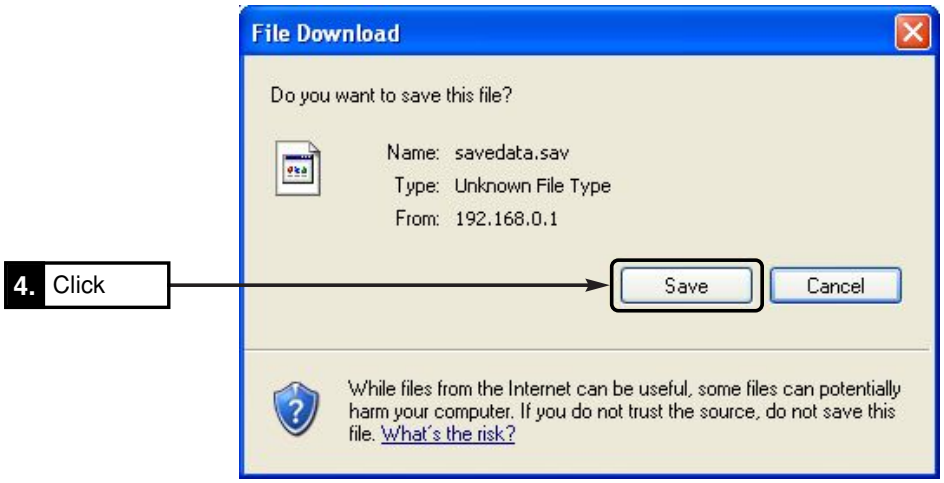
(4) Specify a location to save from Save in and Click <Save>.
- A setup file (file extension: .sav) is now saved in the specified location.

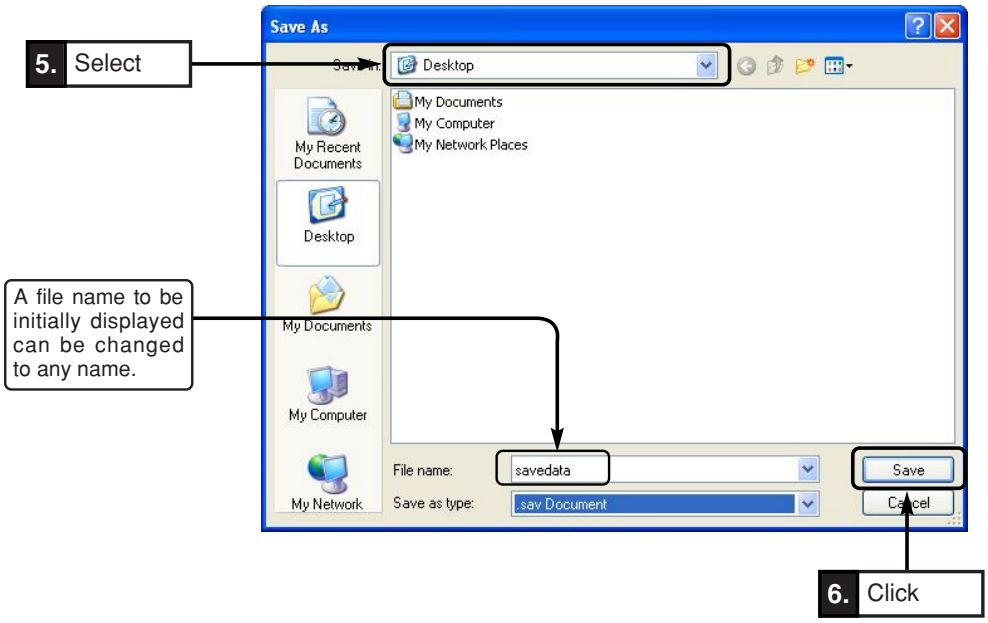
For WE70-AP



For WE70-CL







⚠ Caution

If a cable connecting PC and WE70 is unplugged and plugged again while an AP and a CL are communicating, communication may become unavailable. This cannot be recovered by power cycling.
Execute "arp -d" command from your PC at command prompt to solve this problem.
↑
Space

■ Writing Saved Setup Data

This section describes how to write a setup file saved by "Saving Setup Data" to a wireless unit.
Writing a setup file can help reducing setup work for wireless unit replacement.
Key generator, WEP key, and SSID data cannot be written for client (slave) replacement only.

* These must be set again.

Writing to a client (slave) after initialization instead of replacement, however, allows all setup data to be written.

* Before starting the following steps, make sure that other terminals on the wireless unit network that are used to write data are not communicating.

<How to Write>

(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Maintenance menu > Setting file.
- A Save Setup screen is displayed.

(2) To specify a link to a saved setup file, click <Browse> in Writing of settings.

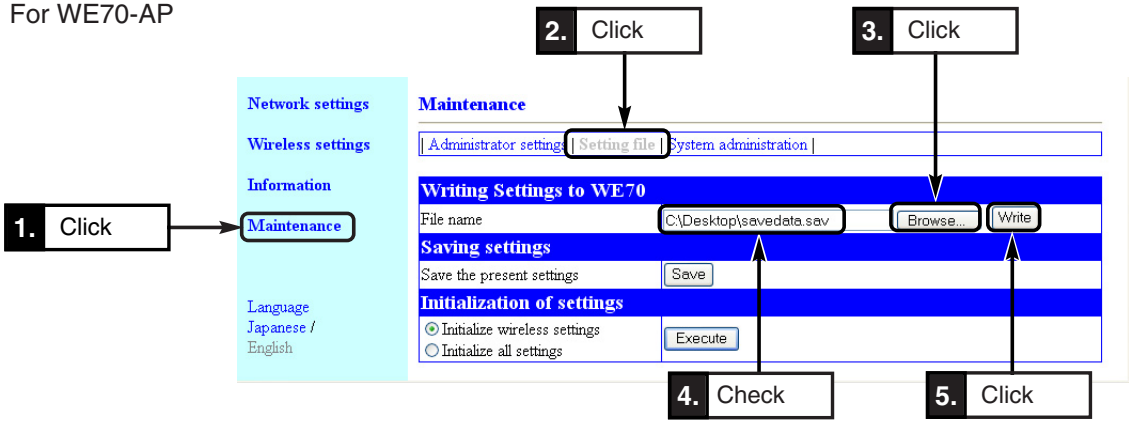
(3) Specifying a saved setup file and clicking <Open> in the screen displays its file name in the File Name text box.

(4) Click <Write>.
- Setting file data is now written to the wireless unit.

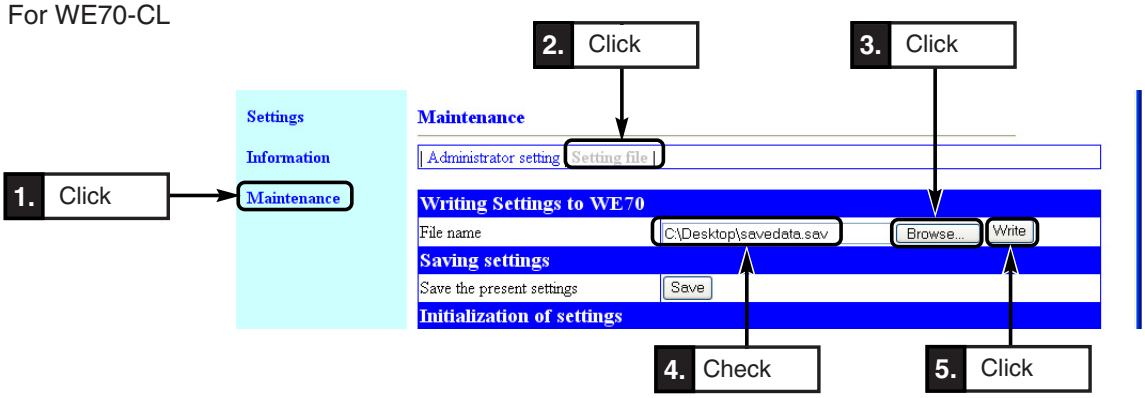
(5) After data is written, close the setup screen and open a new Setup screen.

* Current Setup screen cannot reflect written setup file data.

For WE70-AP



For WE70-CL



6-2. Restoring to Factory Shipment Status

When a network configuration is changed, a wireless unit may be reconfigured in the first place or all of the existing setup data may be deleted. Setup data can be restored (initialized) to Factory Shipment Status by 2 methods:

1. Using <INIT> Button

2. Using Setup Screen

If initialized, an access point and a client (slave) operate under "192.168.0.1" (Factory Shipment Status) and "192.168.0.254" respectively.
If the network part of an IP address becomes different from that of a wireless unit due to initialization, access will not be available. Change PC's IP address if necessary.

■ Using <INIT> Button

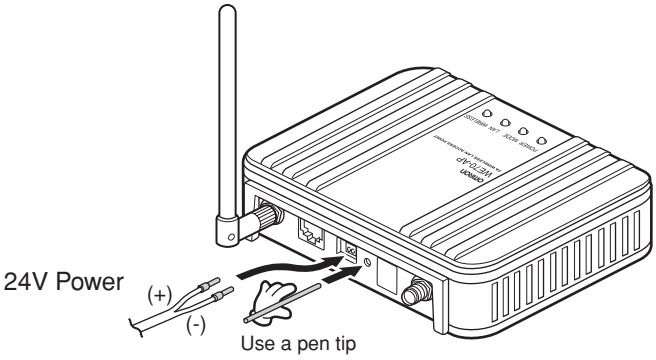
This initialization method resets all setup data to its factory shipment status.
Use the following steps to initialize if a setup screen of a wireless unit cannot be opened because an IP address configured for a wireless unit is unknown or due to other reasons.
If, however, an IEEE802.11a (52CH-64CH, 100CH-140CH) channel is being specified, a unit waits for 60 seconds by the DFS function. Within 5 seconds after the POWER indicator stops flashing in 60 seconds, press the <INIT> button for several seconds.

<To Initialize>

(1) Turn off power of a wireless unit.

(2) Detach all network devices connected to the wireless unit.

(3) Turn its power on while pressing the <INIT> button.(See below)
* Use a pen tip to press the <INIT> button.



Activate 24V power while pressing the <INIT> button

(4) After [POWER] and [MODE] indicators started flashing at the same time then [POWER], [MODE], [LAN], and [WIRELESS] indicators turned on, release the <INIT> button.
* In case of a client (slave), the [RSSI] indicator turns on instead of [MODE].

(5) Connect the wireless unit and PC then start Windows.
• [LAN] indicator turns on.

(6) Activate a WWW browser and specify a wireless unit IP address at factory shipment, which is "192.168.0.1" for an access point and "192.168.0.254" for a client (slave).

■ Using Setup Screen

If an IP address specified for a wireless unit is known and a setup screen can be opened with the IP address, all setup data can be restored to its factory shipment status from wireless unit setup screen.

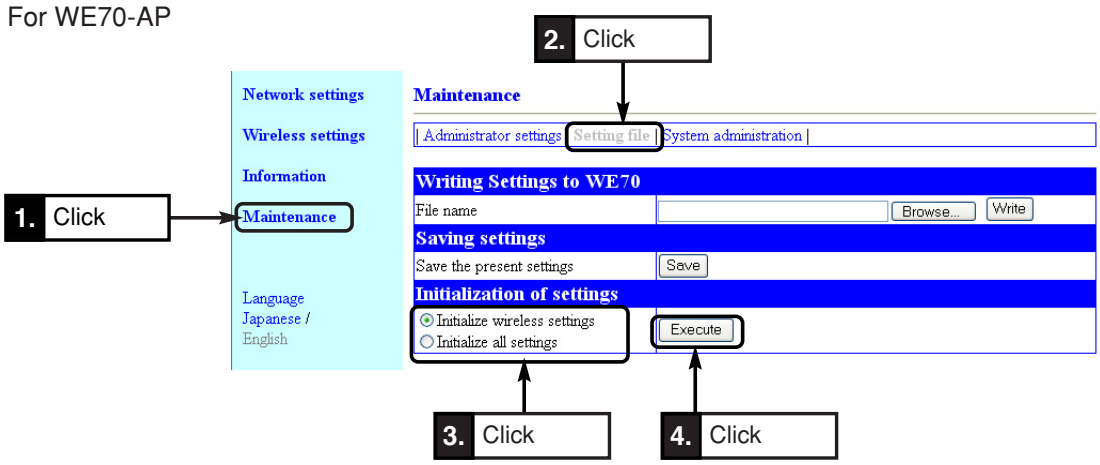
<To Initialize>

(1) Open a setup screen of the wireless unit (see Chapter 2-3. Connection Check, Opening Setup Screen (P.2-13)) and click Maintenance menu > Setting file.
- An Initialization of settings screen is displayed.

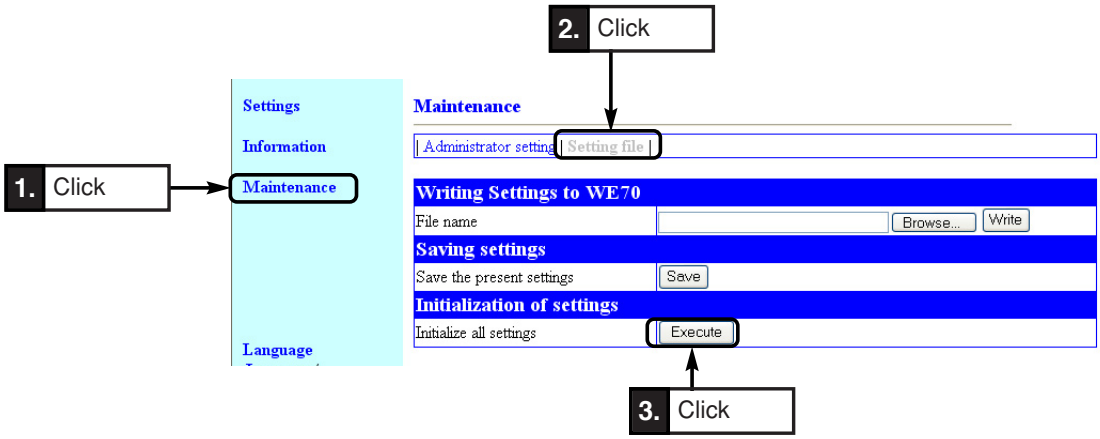
(2) Click a radio button in Initialization of settings field.
Initialize wireless settings: All of setup items in Wireless settings menu are restored to factory shipment status.
Initialize all settings : All of wireless unit setup items are restored to factory shipment status.

(3) Click <Execute>.

For WE70-AP



For WE70-CL



(4) When a next screen is displayed, initialization of the wireless unit is completed.
The unit is being restarted.

(5) If you want to configure setup right after initialization, close the current screen, reconfigure an IP address of PC, and open a new Setup screen.

Appendices

This chapter describes
major troubleshooting, setup screen configuration, and initial setup values.

Troubleshooting Appendices-2
Changing Waiting Period for Scanning (from Version 1.22 of WE70-CL) Appendices-3
Options Appendices-5
■ Power Supply Appendices-5
■ Antenna Appendices-5
■ Others Appendices-5
Initial Setup Value List Appendices-6
■ WE70-AP Appendices-6
■ WE70-CL Appendices-7
Rating Appendices-8
■ Wireless LAN Block (5GHz, 54Mbps; Common with Client) Appendices-8
■ Wireless LAN Block (2.4GHz, 11Mbps/54Mbps; Common with Client) Appendices-8
■ Common Spec for Wireless LAN Block (Common with Client) Appendices-8
■ Wired LAN Block (Common with Client) Appendices-8
■ General Specification (Common with Client) Appendices-9
■ Other Functions Appendices-9
Dimensions Appendices-10
■ WE70-AP/CL Appendices-10
■ Mounting Bracket Appendices-10
■ High-sensitivity Magnetic-base Antenna Can (WE70-AT001H: Optional).....Appendices-11
■ Antenna Extension Cable 5M (WE70-CA5M) Appendices-11
Glossary.....Appendices-12
Revision History.....Appendices-14

Troubleshooting

A wireless unit has LEDs that indicate unit statuses. Checking these LEDs can help identify details and cause of a problem.

Off: ◎ , On: ☀, Flashing: ☀, Indefinite: ☀/◎

AP: Access Point, CL: Client

LED Indication			Estimated Cause	Action
POWER	LAN	WIRELESS		
◎	◎	◎	The power is not supplied.	Supply 24VDC to the DC connector.
			Line voltage is low.	Supply 24VDC power.
◎	◎	☀	AP's DFS function is working.	Please wait for 1 minute before starting.
☀	☀/◎	☀/◎	Indefinite	Press the RSSI button and check LED indication again (CL only)
☀	◎	☀/◎	A LAN cable is not connected.	Connect a LAN cable.
			A LAN cable is inappropriate (straight or cross).	Replace between a straight cable and a cross cable.
☀	☀	◎	SSIDs are unmatched between an AP and a CL.	Match SSIDs.
			Encryption types are unmatched.	Match encryption types.
			CL's SSID of AP's Any Access Denial is configured as blank.	Configure AP's Any Access Denial as No, or specify CL's SSID as AP's.
			AP's 11g protective function is configured as dedicated to g while communication is being tried by a 11b terminal.	Enable or disable 11g protection.
			Clients exceeding the client count limitation are trying to connect.	Reduce number of clients to the specified value or less.
			MAC address filtering is working.	Register the CL to MAC address filtering, or disable AP's MAC address filtering.
			Other BSSID is not being registered for AP-to-AP bridging.	Register BSSID of the other part of communication.
			TKIP, AES, or WOC KEY is configured as an encryption type for AP-to-AP bridging.	Change the encryption method to WEP or OCB AES.
			Receiving electric field intensity is low.	Reduce a wireless distance or use the repeater function to ensure sufficient electric field intensity.
☀	☀	☀	Encryption method are unmatched.	Match encryption method.
			Encryption keys (WEP keys or PSKs) are unmatched.	Match encryption keys.
			An IP address is inappropriate.	Set an appropriate IP address and a subnet mask.
			CL-to-CL communication is being tried while CL-to-CL communication via an AP is being disabled.	Enable Communications between CLs via an AP.
			Super A/G setup is wrong for AP-to-AP bridging.	Match Super A/G setups.
			Key index setups of WEP key are unmatched when Super A/G is used for AP-to-AP bridging.	Match key indexes of WEP key.

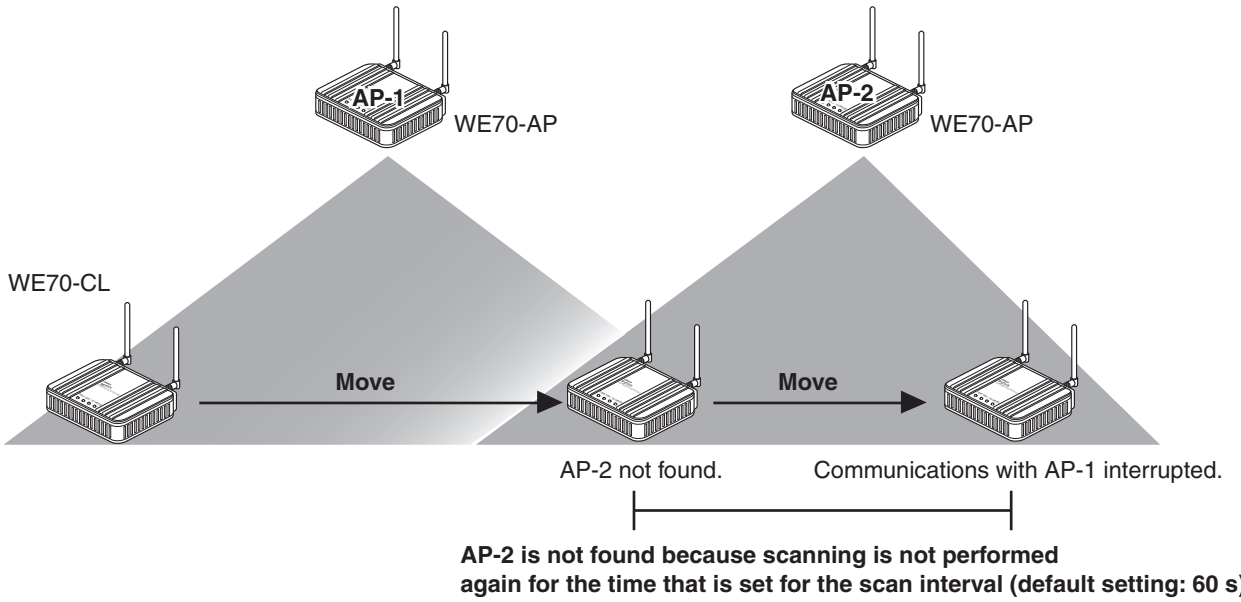
If communication is still unavailable after taking actions shown above, perform the followings:

- Delete the ARP table in PC connected to WE70 (execute "arp -d" command at command prompt).
- Restart devices connected to WE70 such as PLC, PT, or hub.
- Review settings of devices connected to WE70.
- Review the network configuration.

Space

Changing Waiting Period for Scanning (from Version 1.22 of WE70-CL)

When scanning of all channels is completed in the background, the client (slave) does not restart scanning until the set waiting period elapses (default setting: 60 seconds). If any interruptions occur in communications due to access point switching, try setting a shorter waiting period. This may eliminate the interruptions.



How to Change the Setting

Step 1. Log into a client (slave) using a Telnet command from the command prompt on a computer that is connected to the client (slave). Press the Enter Key, leaving the user password blank.

e.g.: C:.¥telnet 192.168.0.254 (IP address of the client (slave))

Step 2. Enter "System wireless wl2 scaninterval [parameter]" and press the Enter Key.

[parameter]: 1 through 225 (seconds)

If the command is not entered correctly, a warning message ("Bad command") is displayed. "Bad parameter" is displayed if the parameter is outside the range (i.e., not 1 through 225).

Step 3. Enter "Save" and press the Enter Key.

Step 4. Restart the client (slave). Repeat step 1 to log into the client.

Step 5. Enter "System wireless wl2 scaninterval".

The set value is displayed on the screen.

Example of Command Execution

Set to C:¥> telnet 192.168.0.254.

```
User:

Password:

Welcome to WE70-CL!

You are administrator!

WE70-CL # system wireless wl2 scaninterval
60
WE70-CL # system wireless wl2 scaninterval 10
WE70-CL # save
```

Restart the client.

Confirm that the setting is C:¥> telnet 192.168.0.254.

```
User:

Password:

Welcome to WE70-CL!

You are administrator!

WE70-CL # system wireless wl2 scaninterval
10
```

⚠ Caution

- Do not forget to execute the Save command after you change the setting. If the Save command is not executed in step 3, the setting is not saved after the power is turned off.
- If the waiting period is too short, scanning is carried out frequently and it may reduce the throughput.
- The setting of the waiting period is saved in the setting file of the client (slave). (For information on the setting file, refer to "6-1. Replacing Wireless Unit.")
- The waiting period cannot be changed on clients (slaves) with a version that is lower than 1.22
- If the setting file of a client (slave) with a version lower than 1.22 is written in a client (slave) with version 1.22 or higher, the parameter for the waiting period will return to the default setting (60 seconds).

Options

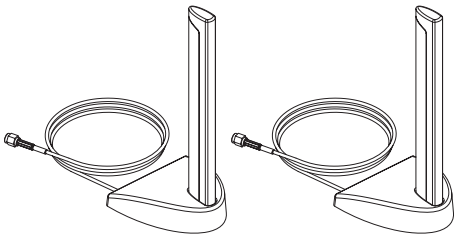
■ Power Supply

Switching Power Supply

A wireless unit requires 24VDC power supply. Use S8VM/VS (UL listing Class 2) series power source of 30W or higher, taking inrush current on startup into account. Omron's switching power supply is recommended. And, it power is supplied from the battery supply via the DC-DC converter.

■ Antenna

Magnetic Pedestal Antenna



1 set with 2 antennas

High-sensitivity Magnetic-base Antenna
Common for 2.4GHz and 5GHz bands
(WE70-AT001H)

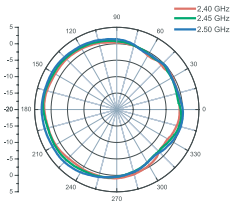
Antenna Extension Cable 5M
(WE70-CA5M)

Co-polarization pattern
High-sensitivity Magnetic-base Antenna : Model WE70-AT001H

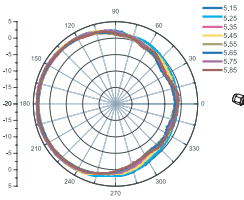
■ Others

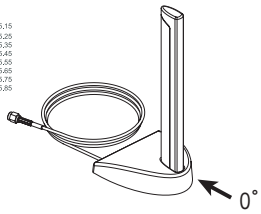
●H-plane Co-polarization pattern

2.4GHz-band



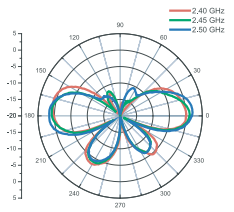
5GHz-band



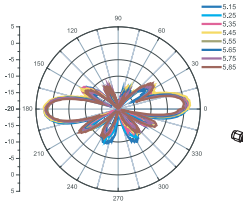


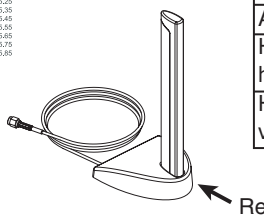
●V-plane Co-polarization pattern (View from rear side)

2.4GHz-band



5GHz-band





Frequency range（MHz）	2400-2483.5	5150-5875	
Peak gain	2.2	3.2	include cable loss
Average gain	0.2	1.2	include cable loss
HPBW/ horizontal(°)	360	360	
HPBW/ vertical(°)	30	15	

Model	Type
WT30-FT001	DIN rail mounting bracket (for TH35-7.5)
WT30-FT002	DIN rail mounting bracket (for TH35-15)
WE70-CA5M	Antenna Extension Cable (5M) 2.4GHz/5GHz, 1set with 2 Antennas

* The WE70-AP does not comply with FCC/IC rules when it is connected with the WE70-CA5M Extension Cable. Do not use the WE70-CA5M with WE70-AP in the United States and Canada. (The WE70-CA5M can be used with the WE70-CL.)

Initial Setup Value List

Shown below are initial setup values in a setup screen of a wireless unit.

■ WE70-AP

Menu			Item	Initial Value
Network settings	Basic settings	Unit name	Unit name	WE70-AP
		IP address setting	IP address	192.168.0.1
			Subnet mask	255.255.255.0
			Default gateway	Blank
	Advanced settings	Bridge	Spanning tree function	Invalid
Wireless settings	Basic settings	Communications settings	SSID	omronwe70wlan
			Channel	36CH(5180MHz)
		Wireless output settings	Wireless output	On
			Trasmitter output level	High
	Secturity settings	Encryption setting	Encryption method	None
			Key generator	Blank
			PSK (Pre-Shared Key)	Blank
			Key index	1
		WEP Key	Input mode	Hexadecimal number
			1	00-00-00-00-00
			2	00-00-00-00-00
			3	00-00-00-00-00
			4	00-00-00-00-00
	Communications between Aps	Register communicating AP	BSSID	Blank
			Maximum baud rate	Auto
	Advanced settings	Advanced communications settings	Refuse any connection	Valid
			Communications between CLs via AP	Invalid
			11g protection function	Valid
			Number of Connecting Cls Restriction	63
			Use Superr A/G	None
		MAC address filtering	MAC address filtering	Invalid
			MAC address	Blank
Maintenance	Administrator settings	ID setting for administrator	Admin. ID	admin
			Admin. password	Blank
			Confirmation input	Blank
		IP setting for administrator	Admin. IP setting 1 to 8	Blank
	Setting file	Writing Settings to WE70	File name	Blank
	System administration	Time setting	Unit time	January 1, 2007
			Setting time	PC Time
		SYSLOG setting	Use DEBUG	Invalid
			Use INFO	Valid
			Use NOTICE	Valid
			Host address	Blank

■ WE70-CL

Menu			Item	Initial Value
Settings	Basic settings	IP address settings	IP address	192.168.0.254
			Subnet mask	255.255.255.0
		Wireless settings	SSID	omronwe70wlan
			Communicating unit's MAC address	Wired MAC address
			Communications method	802.11a
			Baud rate	Auto
			Transmitter output level	High
		Encryption setting	Encryption method	None
			Key generator	Blank
			PSK (Pre-Shared Key)	Blank
			Key index	1
		WEP Key	Input mode	Hexadecimal number
			1	00-00-00-00-00
			2	00-00-00-00-00
			3	00-00-00-00-00
			4	00-00-00-00-00
	Advanced settings	Advanced communication setting	Smart roaming	Invalid
			Use Superr A/G	None
Maintenance	Administrator settings	IP setting for administrator	Admin. ID	Blank
			Admin. password	Blank
			Confirmation input	Blank
	Setting file	Writing Settings to WE70	File name	Blank

Rating

■ Wireless LAN Block (5GHz, 54Mbps; Common in AP/CL)

Item	Specification
Standards	IEEE802.11a
Transmission Method	Orthogonal Frequency Division Multiplexing (OFDM), Simplex
Frequency Range	5170 to 5330MHz (8 channels), 5470 to 5725MHz (11 channels), 5725 to 5825MHz (5 channels)
Communication Rate	Auto/54/48/36/24/18/12/9/6Mbps (theoretical)
Maximum Transmission Distance (Clear View)	Indoors:About 40m (Depending on an installed environment.Cannot be used outdoors)

■ Wireless LAN Block (2.4GHz, 11Mbps/54Mbps; Common in AP/CL)

Item	Specification
Standards	IEEE802.11b/IEEE802.11g
Transmission Method	(Using 802.11b) Direct Sequence Spectrum Spread, Simplex
	(Using 802.11g) Orthogonal Frequency Division Multiplexing (OFDM), Simplex
Frequency Range	2400 to 2483.5MHz (13 channels or 11 channels)
Communication Rate	(Using 802.11b) Auto/11/5.5/2/1Mbps (theoretical)
	(Using 802.11g) Auto/54/48/36/24/18/12/9/6Mbps (theoretical)
Maximum Transmission Distance (Clear View)	Indoors:About 60m (Depending on an installed environment)

■ Common Spec for Wireless LAN Block (Common in AP/CL)

Item	Specification
Security	OCB AES <128-bit>, WEP (RC4) <64/128/152-bit>, WPA-PSK (with encryption type of AES <128-bit>/TKIP <128-bit>), WOC KEY
Group Communication	SSID (Supporting ANY-connection Refusal)
Transmission Power	10mW/MHz or less
Antenna	Dual Band Diversity Antenna SMA Reverse Connector

■ Wired LAN Block (Common in AP/CL)

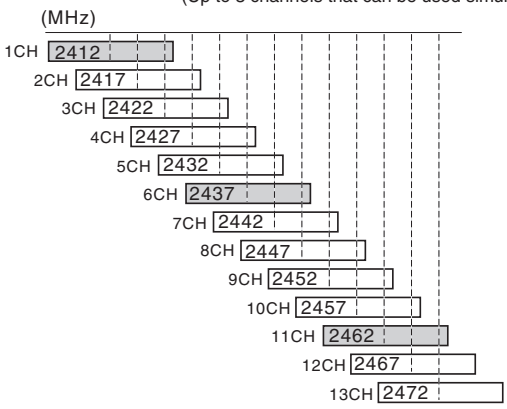
Item	Specification
Standards	IEEE802.3 (10BASE-T), IEEE802.3u (100BASE-TX)
Interface	RJ-45 x 1

* Connection to PLC and PC uses straight cables.
* Use STP LAN cable.

■ Channel assignment based on frequency band

2.4GHz band

802.11b/g: All of 13 channels (except 12CH and 13CH in United States and Canada)
(Up to 3 channels that can be used simultaneously)

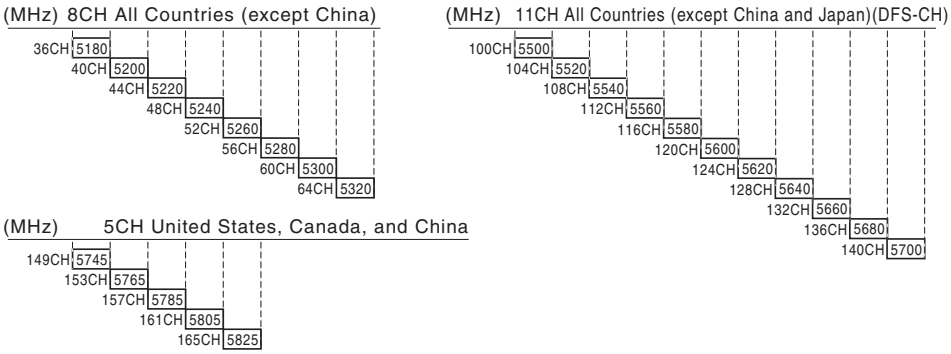


*You can chose a model for the country to use.

WE70-AP/CL	:Japan
WE70-AP/CL-US	:United States
WE70-AP/CL-CA	:Canada
WE70-AP/CL-EU	:Europe
WE70-AP/CL-CN	:China

5GHz band

802.11a: All of 24 channels (up to 24 channels that can be used simultaneously)
globally common, indoors only



■ General Specification (Common in AP/CL)

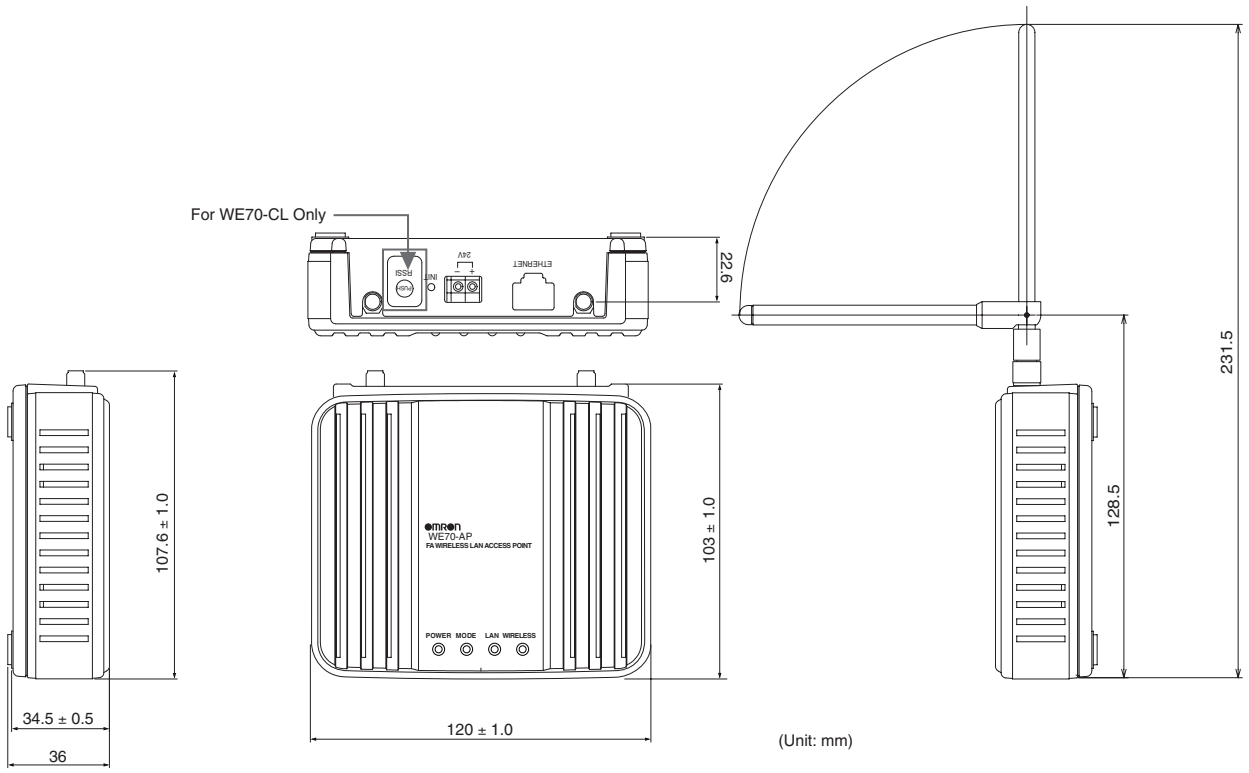
Item	Specification
Main Unit Setup	Web Browser: Microsoft Internet Explorer 6.0, 7.0 OS: Windows Vista, Windows XP with Service Pack 1 or higher, or Windows 2000 with Service Pack 4
Power	DC20.4 to 26.4 V (Screwless Terminal Block)
Current Consumption	250mA max.
Vibration resistance	JIS C0040 Frequency: 10 to 55 Hz; Single amplitude of 0.35 mm 10 sweeps of 8 min each (i.e., 80 min in total) in X, Y, Z directions
Shock resistance	Conforms to JIS C0041: 300 m/s^2 3 times each in X, Y, and Z directions
Ambient Operating Temperature	0 to +50 °C (No condensing)
Ambient Operating	25 to 85%RH (No condensing or freezing)
Humidity Dimensions	120(W) x 103(D) x 34.5(H)mm (excluding projection)
Weight	About 360g (Main Unit Only)

■ Other Functions

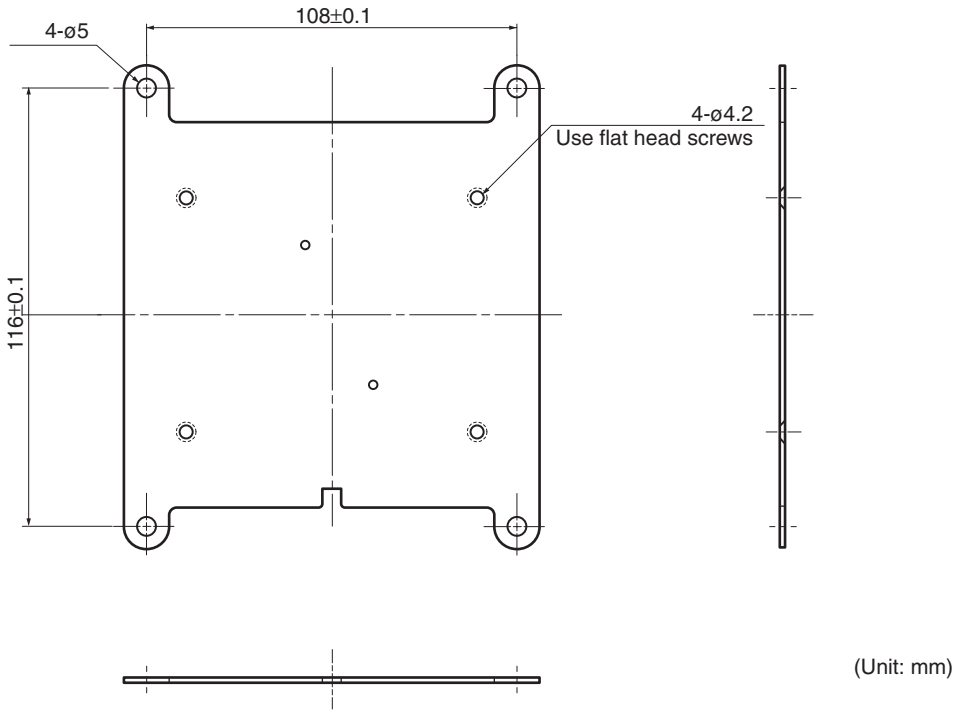
Item	Specification
Wireless LAN	Supporting Communication Rate Enhancement Technology Atheros Super AG, Variable Transmission Power (3 Levels: High/Mid/Low),Transmission Load Distribution (Connection Terminal Limiting), 11g Protection, Client-To-Client Wireless Communication Inhibition, Roaming, AP-to-AP Bridging, MAC Address Registration Security, SSID Setup ANY-connection refusal
Others	Supporting SYSLOG, Web Browser Setup, Administrator ID Setup, Administrator IP Registration

Dimensions

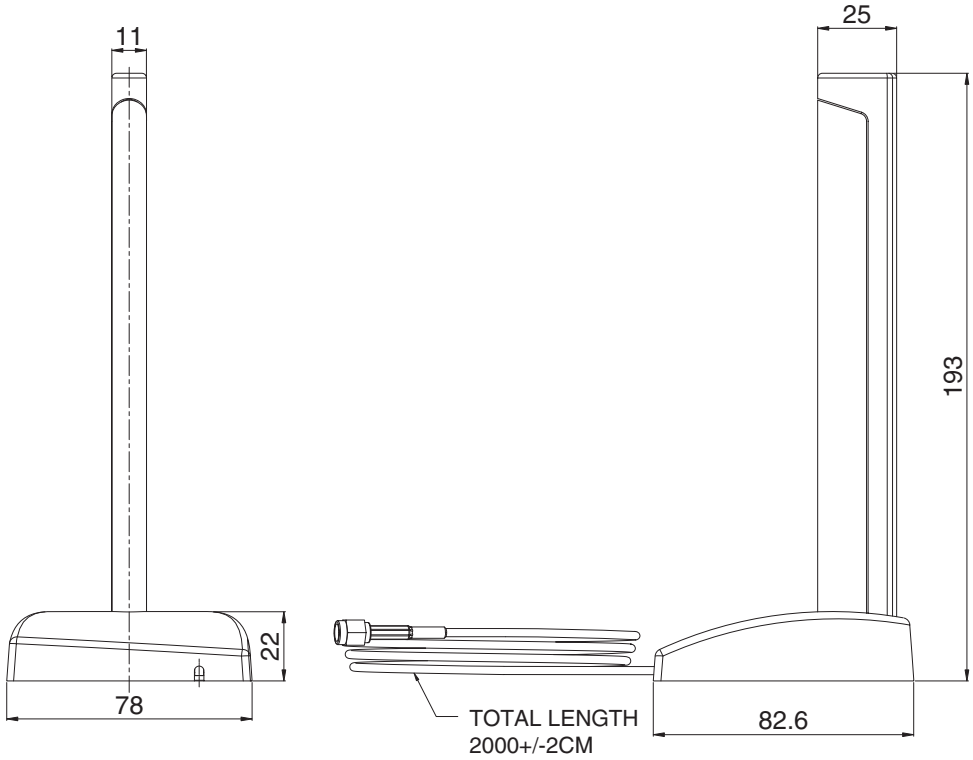
■ WE70-AP/CL (Common)



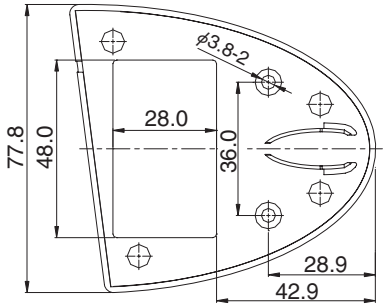
■ Mounting Bracket



■ High-sensitivity Magnetic-base Antenna Can (WE70-AT001H: Optional)



(Unit:mm)



Antenna Stand Bottom View

Glossary

Access Point

A generic name for a site through which access to the Internet is made via a provider.
Also, it is a generic name of a device that works as a bridge connecting a wired LAN and a wireless LAN.

Authentication

Validating if a user making access to a network through the Internet or others has proper permission for access by asking his/her password and user ID.

Browser

See WWW Browser.

BSSID (Basic Service Set-IDentifier)

An identification to designate a wireless LAN in the MAC layer.
It is used for AP-to-AP bridging of a wireless unit.

Client

A generic name for a terminal or an application that sends a request of information and receive a response to/from a server in a network.

DFS (Dynamic Frequency Selection)

This function is used to prevent radio interference by automatically switching to a detected unused channel before starting wireless LAN communication of IEEE802.11a (5470MHz-5725MHz) standard.-EU,-US,-CA is W53,100-140CH.

Domain Name

As an IP address is difficult for people to recognize, a domain name is assigned to a domain that is a group to which the IP address belongs.
Example) In case of an e-mail address omron@example.co.jp, example.co.jp is a domain.

ESS ID (Extended Service Set-IDentifier)

See SSID.

Ethernet

Standard LAN technology to connect PCs.
There are various types depending on cabling; 10BASE-T, 100BASE-TX, 10BASE-5, 10BASE-2, etc.

Flash Memory

A storage device in a wireless unit, to which data can be written.
Information stored in this device will not be lost even after power is turned off.

Global IP Address

A unique address that does not overlap with any other address of any device on the Internet.

HTML (Hyper Text Markup Language)

A language to describe a document on a WWW server, using tags in a document
to create a WWW page.

HTTP (Hyper Text Transfer Protocol)

A protocol to be used to transfer HTML documents. Entering URL in a WWW browser transfers an HTML document from a WWW server to the WWW browser on PC. Transferred document is interpreted and displayed on a screen by the WWW browser.

HUB

A device required to construct a network.
It is connected using 10BASE-T or 100BASE-TX cables.
To communicate under 100Mbps, it is necessary to use twisted-pair cables of category 5 or higher, and the hub itself must support 100BASE-TX.

Internet

A generic name for networks connecting computers all over the world using the IP.

Internet Explorer

Standard Web browser software that comes with Windows and Mac OS.

IP (Internet Protocol)

See TCP/IP.

IP (Internet Protocol) Address

A 32-bit address assigned to identify a device connected to a network using the TCP/IP protocol.
Typically it is grouped by every 8 bits into 4 decimal numbers. (Example:192.168.0.1)
A private IP address indicates an IP address uniquely specified by a network administrator.
It is not necessary to report this address to address management authorities or providers but it must be assigned based on the following rules.

To connect to an external network, the address must be converted to a global IP address.
Following IP addresses can be used as private IP addresses:
Class A:10.0.0.0-10.255.255.225
Class B:172.16.0.0-172.31.255.225
Class C:192.168.0.0-192.168.255.225

LAN (Local Area Network)
A small-scale network in an office floor or a campus.

MAC address (Media Access Control Address)
A physical address set to every Ethernet and wireless LAN card.
This address is managed by LAN card manufacturers so that it should be unique in the world.
Ethernet and wireless LAN cards transmit a frame based on this address.

Network
A communication system connecting devices such as servers, workstations, and PCs through cables and broadband lines to transfer data.

Password
A character string that is required for a user to enter for network access, to ensure network security. Access becomes available when a user enters a correct string registered beforehand.

Shared Key Authentication
A type of authentication that confirms that a common encryption key is shared by those that communicate using a configured encryption key for encrypted communication with an access point in a wireless LAN.
A system that does not authenticate is called an "open system".**SSID (Service Set-IDentifier)**
A name to identify a network group when more than one network group is configured in one communication zone of a wireless LAN.

Subnet Mask
A bit mask used to identify network address and host address blocks of an IP address.
Suppose an IP address of a host is "192.168.0.1" and its subnet mask is "255.255.255.0". Multiplying the IP address and the subnet mask as base 2 numbers generates its network address as "192.168.0" and the remainder "1" is its host address.

TCP/IP
A basic and most widely used protocol of the Internet, supported by major OSs such as Windows.
Some protocols such as SMTP and FTP use this protocol.

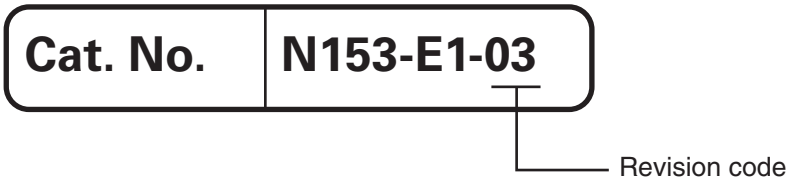
URL (Uniform Resource Locator)
is specified for access to a site on the Internet.
Omron's URL is http://www.fa.omron.co.jp/.

WEP (Wired Equivalent Privacy)
A typical function to transmit data in a wireless LAN using encryption.
It can prevent tapping of wireless LAN communication.

WWW Browser
An application to be used to view a WWW site and search a WWW server.
Such applications include Internet Explorer and Netscape Navigator.

Revision History

A manual revision code appears as a suffix to the catalog number on the back cover of the manual.



Revision	Revised on:	Revision Detail
01	June.2007	1st edition
01A	October.2007	**Page 2-7 and A-3 :** Changed "15W" to "30W".
02	February.2012	Changes and corrections
03	November.2019	Changes and corrections

OMRON Corporation **Industrial Automation Company**
Tokyo, JAPAN
Contact: www.ia.omron.com

Regional Headquarters
OMRON EUROPE B.V.
Wegalaan 67-69-2132 JD Hoofddorp
The Netherlands
Tel: (31)2356-81-300/Fax: (31)2356-81-388

OMRON ELECTRONICS LLC
One Commerce Drive Schaumburg,
IL 60173-5302 U.S.A.
Tel: (1) 847-843-7900/Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.
No. 438A Alexandra Road # 05-05/08 (Lobby 2),
Alexandra Technopark,
Singapore 119967
Tel: (65) 6835-3011/Fax: (65) 6835-2711

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-5037-2222/Fax: (86) 21-5037-2200

Authorized Distributor:

© OMRON Corporation 2007-2019 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. N153-E1-03 1119(0607)