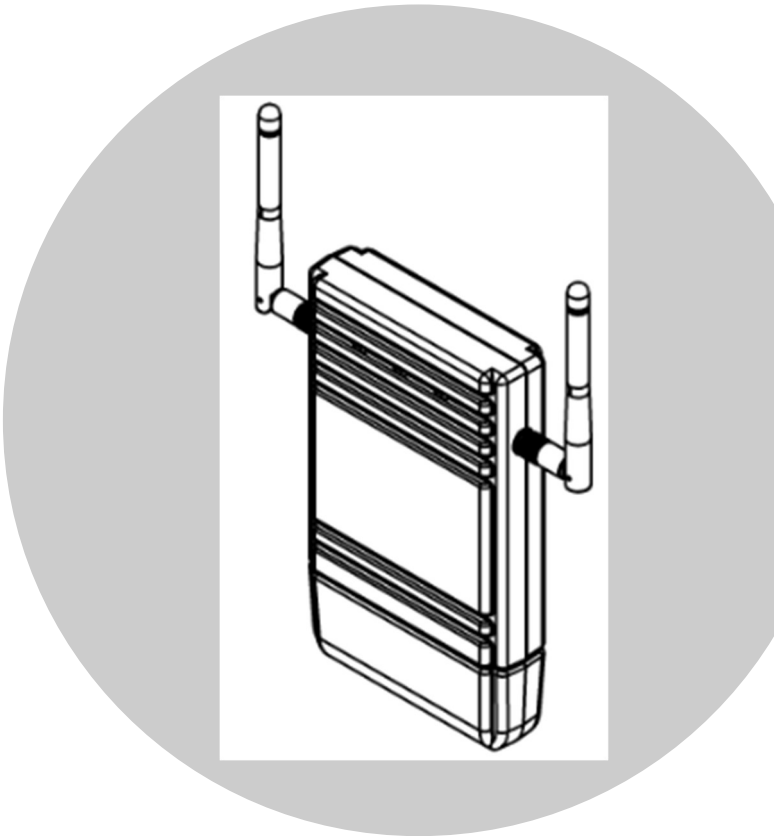
CONTEC

リファレンスマニュアル

IEEE802.11n/a/b/g
Wireless LAN Accesspoint
USA(Access Point / Station)

FXA3020-US



目 次

株式会社コンテック

目次

目次

目次

Introduction

This section provides necessary information of the product such as the outline, bundled items and manuals before actual use.

1. Related Manuals

The manuals related to the product are listed below.

Read them as necessary along with this document.

◆ Must Read the Following.

Name	Purpose	Contents	How to get
Please read the following	Must read this after opening the package.	This introduces related materials that are made available on the CONTEC website, such as those for the included items, manuals, and software.	Included in the package (Printed matter)
Reference Manual (This document)	Read this when operating the product.	This describes the hardware aspects such as functions and settings.	 Download from the Contec website (PDF)

◆ Download Manuals

Download the manuals accordingly from the following URL.

Download https://www.contec.com/jp/download/

2. Features

■ Supports a various power supply

This product supports an AC adapter (sold separately), DC power supplies from 5 to 30 VDC, and power supplied from the LAN connector.

■ This product can be switched between access point, station (client), and repeater operation modes

By switching the operation mode, you can use this product as not only an access point but also as a station (client) and a repeater. You can use this product as a wireless LAN converter for a wired LAN device.

■ The proprietary encryption technology "WSL" that is available along with WPA3/WPA2/WPA and WEP.

In addition to the certifications for advanced security standards WPA3/WPA2/WPA and IEEE802.1X, this product is also equipped with our proprietary encryption technology "WSL", which can be used at the same time as these certifications. MAC address filtering and ESSID hiding are also supported.

■ Features variety of functions, including VLAN and a virtual AP function

This product is equipped with a VLAN function for constructing virtual networks and a virtual AP function for operating one AP as multiple virtual APs with different security settings. Also, large capacity event logs can be saved.

*VLAN function will be supported by firmware upgrade.

■ Light weight and compact design for installation setting and sophisticated appearance

Compatible with PoE and include an antenna inside chassis considering installation setting and sophisticated appearance. This product can be used at variety of setting using included magnets and tapping screws.

■ Supported with a connector protection cover and security wire connection configuration

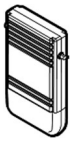
This product can be protected from theft by protecting connectors with included connector cover and attaching a security wire to security slot.

3. Included Items

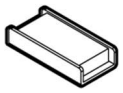
The product consists of the items listed below.

Check, with the following list, that your package is complete.

If you discover damaged or missing items, contact your retailer.

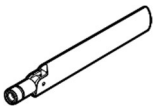


Main unit…1※1

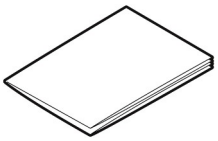


Magnet…2

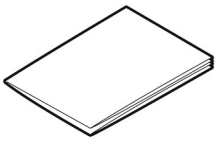
Tapping screws…2



Antenna…2



Please read the following…1



Setup Guide…1

※1 Connector cover (Installed in unit)

4. Support Software

You can use CONTEC support software according to your purpose and development environment.

For more details on the supported OS, applicable languages, or to download the latest version of software, visit the CONTEC Web site.

Download https://www.contec.com/jp/download/

Safety Precautions

Understand the following definitions and precautions
to use the product safely.
Never fail to read them before using the product.

1. Safety Information

This document provides safety information using the following symbols to prevent accidents resulting in injury or death and the destruction of equipment and resources.

Understand the meanings of these labels to operate the equipment safely.

⚠ **DANGER**	Signal word used to indicate an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ **WARNING**	Signal word used to indicate a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ **CAUTION**	Signal word used to indicate a potentially hazardous situation which, if not avoided, could result in minor or moderate injury.

2. Handling Precautions

⚠ DANGER

Do not use the product where it is exposed to flammable or corrosive gas. Doing so may result in an explosion, fire, electric shock, or failure.

⚠ CAUTION

- Do not touch this product directly with your hands.
- Doing so may cause the board to malfunction, overheat, cause a failure, or be damaged. To prevent damage caused by static electricity, implement measures to prevent static electric discharges when handling the product.
- Do not use or store this device in high temperature or low temperature surroundings, or do not expose it to extreme temperature changes. Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device where it is exposed to direct sunlight or near stoves or other sources of heat. Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device near strong magnetic fields or devices emitting electromagnetic radiation. Otherwise, the board may malfunction, overheat, or cause a failure.
- If an unusual smell or overheating is noticed, unplug the power cable immediately In the event of an abnormal condition or malfunction, please contact your retailer.
- The specifications of this product are subject to change without notice for enhancement and quality improvement. Even when using the product continuously, be sure to read the manual and understand the contents.
- Do not attempt to modify this device. The manufacturer will bear no responsibility whatsoever for the device if it has been modified.
- The product must always be associated with the instruction manual.
- Regardless of the foregoing statements, CONTEC is not liable for any damages whatsoever (including damages for loss of business profits) arising out of the use or inability to use this CONTEC product or the information contained herein.
- Do not use the product where it is exposed to flammable or corrosive gas. Doing so may result in an explosion, fire, electric shock, or failure.
- This product contains precision electronic elements and must not be used in locations subject to physical shock or strong vibration. Otherwise, the board may malfunction, overheat, or cause a failure.
- This product is intended for installation by trained personnel. Ensure compliance with local electrical and safety regulations.
- Use only PoE injectors or switches that meet IEEE standards. Do not be exposed to moisture or extreme environmental conditions.
- Use only with UL Listed PoE network equipment.

- This equipment power cord must be connected to a socket-outlet with earthing connection.
- This product is intended to be supplied by a UL certified power supply. If you need further assistance, please contact CONTEC for further information.

1. Federal Communication Commission Interference Statement

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CAUTION

Any changes or modifications not expressly approved by the party responsible for compliance could void the electromagnetic compatibility (EMC) and wireless compliance and negate your authority to operate the product.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

Radiation Exposure Warning

The equipment complies with the FCC radiation exposure limits set forth for an uncontrolled environment.

The equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

3. Precaution on use

It is prohibited to modify the inside of this product. The product cannot be used in any country other than those authorized for use.

4. Usage limitation

This product has not been developed or manufactured to be used in systems including the equipment which is directly related to human lives *1 or the equipment which involves human safety and may significantly affect the maintenance of public functions *2. Therefore, do not use the product for such purposes. In addition, do not use the product within 20cm from a human body on a regular basis.

*1: Medical devices such as life-support equipment and devices used in an operating theater.

*2: Main control systems at nuclear power stations, safety maintenance systems at nuclear facilities, other important safety-related systems, operation control systems within group transport systems, air-traffic control systems, etc.

5. Precautions Related to Service

Clean this product by wiping lightly with a soft cloth moistened with water or a cleaning solution.

Take care to avoid the use of benzene, thinners or other volatile solutions which may cause deformation or discoloration.

6. Security Precautions

Wireless LAN uses radio waves instead of LAN cables to send and receive data between a computer and a wireless access point, making it possible to freely establish a LAN connection within a range of the radio waves. However, radio waves can be received through obstacles, such as walls, when within the range. Therefore, if security settings are not made, the following problems may occur.

Unauthorized viewing of data

An unauthorized third party can intercept the radio waves and view e-mail messages and personal information, such as user ID and password or your credit card information.

Unauthorized access

An unauthorized third party can access a personal or corporate network and cause the following damage:

- Intercepting personal information and confidential information (information leak)
- Using a false identity to communicate and disclose information illegally (identity theft)
- Changing and transmitting intercepted data (tampering)
- Damaging data and systems by spreading a computer virus (destruction)

The wireless LAN card and wireless access point have security features to counter these problems. Using the security settings of the wireless LAN equipment can help prevent these problems from occurring. The security settings of the wireless LAN equipment are not configured at the time of purchase.

To reduce security problems, configure all security settings of the wireless LAN equipment according to the manual before using the wireless LAN card and wireless access point. Please be aware that the security settings do not provide complete security protection due to wireless LAN specifications. If you are unable to configure the security settings yourself, please contact your local authorized dealer. The customer is responsible for configuring the security settings and understanding the risks inherent in using the product without the security settings configured.

7. Environment

Use this product in the following environment. If used in an unauthorized environment, the board may overheat, malfunction, or cause a failure.

Operating temperature

0 - +40℃

Humidity

10 - 90%RH(No condensation)

Corrosive gases

None

Floating dust particles

Not to be excessive

8. Inspection

Inspect the product periodically to use it safely.

Check the ventilation slit and make sure that it is not blocked by dust or foreign matter.

9. Storage

When storing this product, keep it in its original packing form.

- Put this product in the storage bag.
- Wrap it in the packing material, and then put it in the box.
- Store the package at room temperature at a place free from direct sunlight, moisture, shock, vibration, magnetism, and static electricity.

10. Disposal

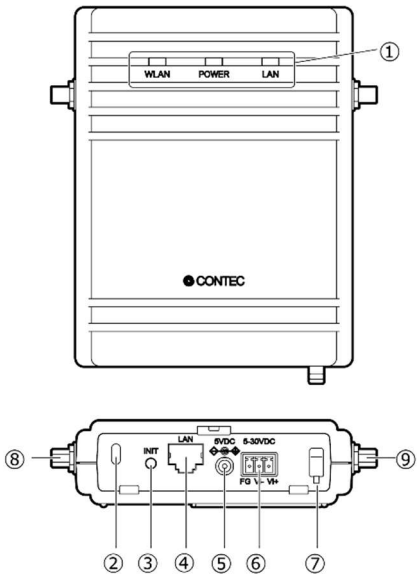
When disposing of the product, follow the disposal procedures stipulated under the relevant laws and municipal ordinances.

Product Nomenclature and Function

This section describes product component names and their functions, pin assignment of each connector.

1. Nomenclature of Product Components

Component names of the product are shown in the figure below.



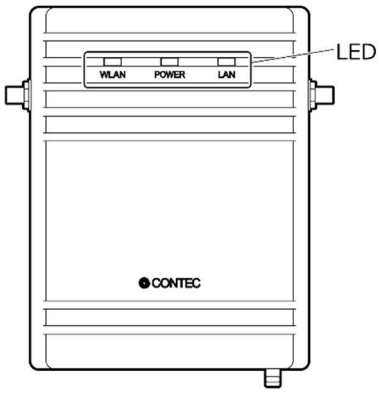
No.	Title	Function
①	LED disply	This is an LED that indicates the status of the unit.
②	Security slot	A commercially available security wire can be attached.
③	INIT Switch	This switch is used to initialize the unit.
④	LAN port	Connect the LAN cable to the PC.
⑤	DC JACK	This is the jack for DC power.
⑥	Power connector	Connect this to the power connector when supplying power from an external source.
⑦	Power disconnection prevention hook	This is the hook for preventing the power cable from coming off.
⑧	Antenna connector	This is the connector for antenna connection.
⑨		

2. Description of Product Components

Components such as connectors, switches are described.

2. LED Indicator

Status of the product is indicated by ON/OFF and flashing of LED.

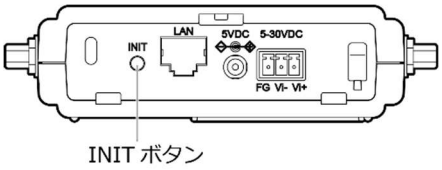


表示色とその意味

LED name	Color	Status	Indicator
POWER	Blue	ON	Indicates that the device is operating.
		Flashing (Interval)	Indicates that the device is being started (This device turned on)
		OFF	Power has not been supplied.
LAN	Green	ON	Indicates that a wired LAN connection.
		Flashing	Indicates data is being transmitted and received over a wired LAN.
		OFF	Indicates that a wired LAN is not connected.
WLAN	Green	ON	Indicates that wireless LAN is connected.
		Flashing	Indicates data is being transmitted to or received from the device connected through wireless LAN.
		OFF	Indicates that wireless LAN is not connected.
POWER/ LAN/ WLAN	Blue/Green/ Green	Flashing (simultaneously)	Indicates that a file is being written.
POWER/LAN	Blue/Green	Blinking twice /On	DHCP error

3. INIT switches

This button initializes the machine.

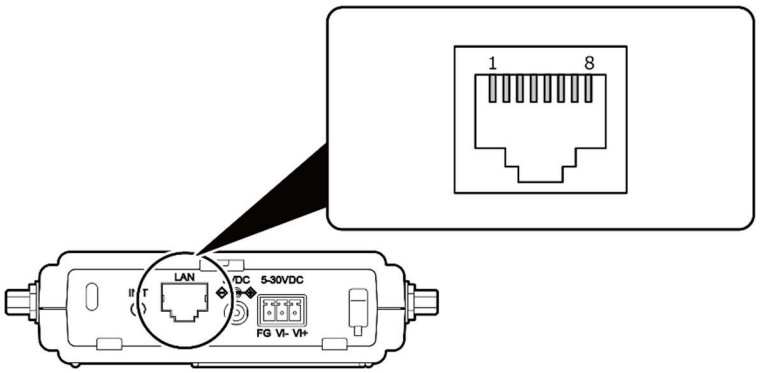


Title	Function
INIT	Used to initialize this product (reset to factory default settings). When this switch is pressed, the POWER, WLAN, and LAN LEDs start to flash. If this switch is released during the period from when the LEDs start to flash and until they turn on (approximately 3 seconds), all of this products settings will be reset to the factory default when next started.

※When initializing the product by turning the INIT signal on and off, the LEDs will continue flashing for a short time after the signal is turned off. This indicates the internal memory files are being deleted. If the power is turned off while the LEDs are flashing, the internal memory files may be damaged and the product may no longer be able to start properly. Always restart the product after the LEDs stop flashing.

4. LAN port

This product has 1 Ethernet ports.

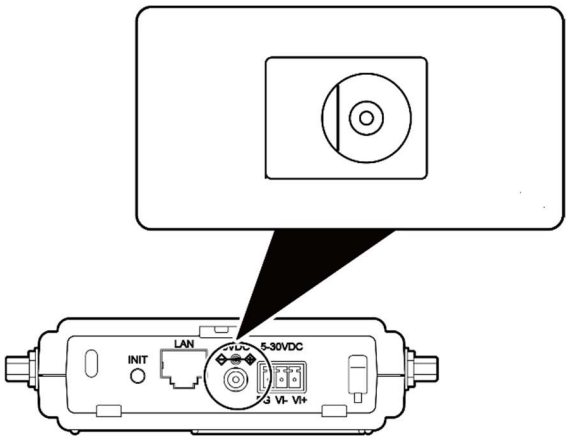


ピンアサイン

No.	Sign	Contents
1	TRD+(0)	Positive side of data pair 0 / Alternative A type positive PoE supply
2	TRD-(0)	Negative side of data pair 0 / Alternative A type positive PoE supply
3	TRD+(1)	Positive side of data pair 1 / Alternative A type negative PoE supply
4	TRD+(2)	Positive side of data pair 2 / Alternative B type positive PoE supply
5	TRD-(2)	Negative side of data pair 2 / Alternative B type positive PoE supply
6	TRD-(1)	Negative side of data pair 1 / Alternative A type negative PoE supply
7	TRD+(3)	Positive side of data pair 3 / Alternative B type negative PoE supply
8	TRD-(3)	Negative side of data pair 3 / Alternative B type negative PoE supply

5. DC JACK

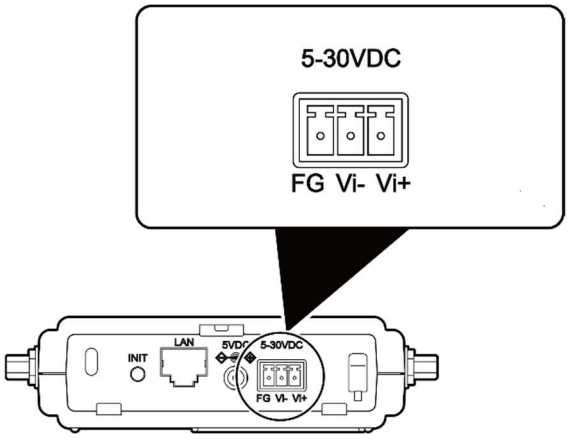
DC power jack. Use this jack with an optional AC adaptor.



Pin	Sign
Center	Input power
Periphery	GND

6. Power connector

Connect to an external power source using a 3-pin connector.



Pin assignment

Pin No.	Signal name	Operation / Function
1	Vi+	5-30VDC±5%
2	Vi-	GND
3	FG	Frame Ground

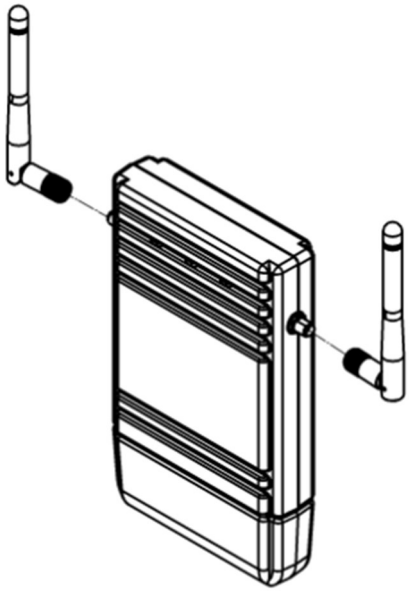
7. Antenna connector

◆ Connecting the Antenna

The MIMO antenna system used by this product uses two antennas simultaneously. When connecting the antennas, please connect both antennas for use. The following shows how to attach the attached antenna.

1 Straighten the antenna, then rotate it and attach it to the antenna connector on the main unit.

2 Bend the antenna to any angle you like.



⚠ CAUTION

- Using the product with the antenna disconnected from the antenna connector or with the antenna loosened may result in a breakdown of the product. Always use the product with the antenna connected.
- Do not touch the antenna connector when the power is on. If you need to touch the connector to remove the antenna connector, be sure to turn off the power to the product.
- Be careful not to touch the antenna connector with your bare hands, as static electricity may cause the product to malfunction.

3. DFS function

When set to DFS-supported channels (5 GHz only), if radar waves are detected, the channel must be changed in order to avoid radio wave interference with weather radars and other radars, so note the following.

DFS-enabled channel (frequency: 5 GHz)

Channel	DFS capability
W52 : 36, 40, 44, 48	Disabled
W53 : 52, 56, 60, 64	Enabled
W56 : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Enabled
W58 : 149, 153, 157, 161, 165	Disabled

* The DFS function applies to W53 and W56. The DFS function does not apply to W52 and W58 because the DFS function is not required.

⚠ CAUTION

- After starting, the channel is checked for radar waves for one minute, so at a minimum, one minute or longer is required.
- If radar waves are detected during startup or while started, the access point may start on another channel since it must use a channel different from the set channel.
- Even after starting with the set DFS-supported channel, the channel may change while running.
- If radar waves are detected, the radio waves must stop for 30 minutes, so the detected channel cannot be used for 30 minutes.

Setting Up

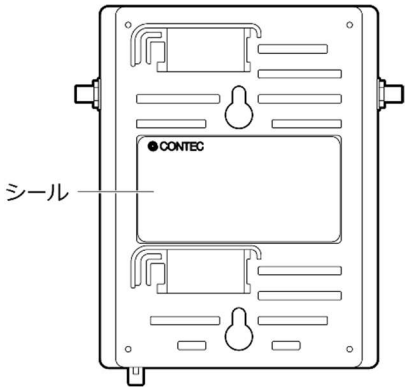
This section describes how to set up the product.

1. Checking the Network Addresses

The Ethernet (wired LAN), wireless LAN MAC address and IP address are defined on the housing sticker on the side of this product. Write down the MAC addresses for Ethernet and wireless LAN in the following table as they are device-individual values and may be required for future setup.

Network Address

Description on the housing sticker	Explanation	Address
IP:	Default IP Address	192.168.0.1
LAN MAC:	LAN MAC Address	
WLAN MAC:	Wireless LAN MAC Address	



2. Power Supply

This product is powered by the following methods.

1. Using the DC JACK

The power plug to be used must conform to EIAJ voltage classification 2.

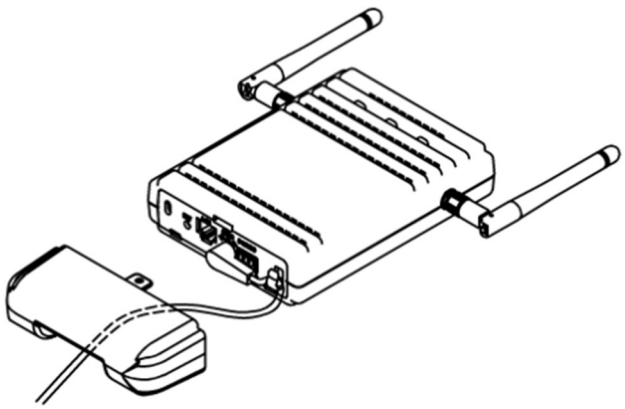
⚠ CAUTION

When supplying power through the DC jack, do not use it together with supplying power from the power connector.

2. When using the AC adapter (FX-AC053)

Connect the DC plug of the AC adaptor to the DC jack of the machine.

Pass the DC plug through the connector cover opening and connect the AC adapter's DC plug to the product's DC jack. You can prevent the DC plug from being pulled out by hooking the cord on the power disconnection prevention hook located on the connector section.



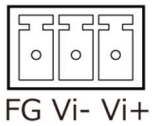
*Since FX-AC053 is a product for Japan, it may not be usable outside of Japan.

⚠ CAUTION

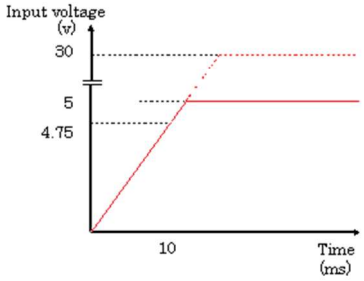
When supplying power through the AC adaptor, do not use it together with supplying power from the power connector.

3. Using the Power connector

ower can be externally supplied using the power connector. Use the components indicated to the followings for the power cable or use equivalent components.

Function			
Power connector: MC1,5/3-ST-3,5(PHOENIX CONTACT), Cable: AWG28-16(on the condition that the cable length satisfies the power specifications)			
Pin No.	Signal name	Meaning	
1	Vi+	Power supply (5 to 30 VDC ±5%)	
2	Vi-	Power supply (GND)	
3	FG	Frame ground	

Power Supply Time



⚠ CAUTION

- Carefully manufacture the power cable taking care not to mistake the wiring. In particular, if the power cable is used with mistaken housing pin numbers, there is a risk of malfunction or accidents.
- Input voltage range: 5 to 30 VDC ± 5%. Use a power supply that rises to 4.75 VDC or higher in the input voltage range within 10 ms. There is a risk of damage to the device or accident if a power supply outside this range is used.

Connecting to ground

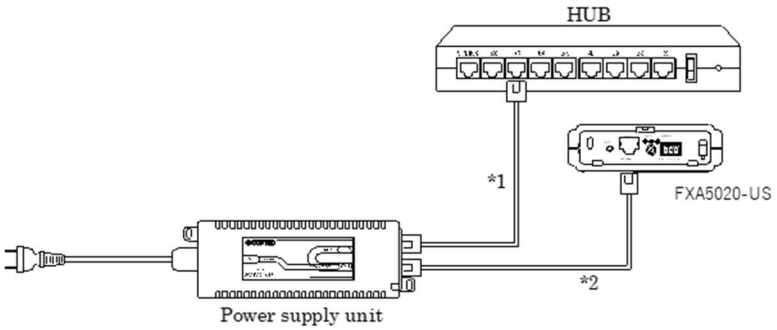
When you connect this product to ground, connect the power cable to the power connector. Process the cable in an appropriate manner to connect the cable to ground.

4. When supplying power from the LAN cable

This product can be power-supplied through a LAN cable from an IEEE802.3af-compliant power supply unit.

For details, refer to the power supply unit.

The following gives an example of connection.



⚠ CAUTION

- The overall length of the LAN cable between the power supply destination and the hub must be up to 100 m.Route the cabling such that *1 + *2 is 100 (m) or less.
- Do not connect the output LAN cable to any IEEE802.3af non-compliant device as doing so can cause device faults or accidents.

*Since POW-CB50AF, POW-CB60AT, and POW-CB70AT is a product for Japan, it may not be usable outside of Japan.

3. Installation

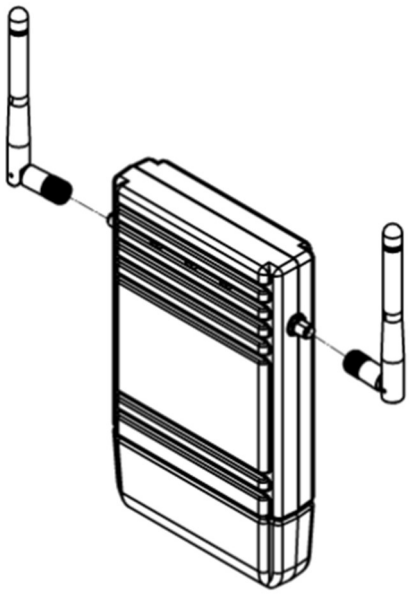
1. Prepare for installation

◆ Connecting the Antenna

The MIMO antenna system used by this product uses two antennas simultaneously. When connecting the antennas, please connect both antennas for use. The following shows how to attach the attached antenna.

3 Straighten the antenna, then rotate it and attach it to the antenna connector on the main unit.

4 Bend the antenna to any angle you like.

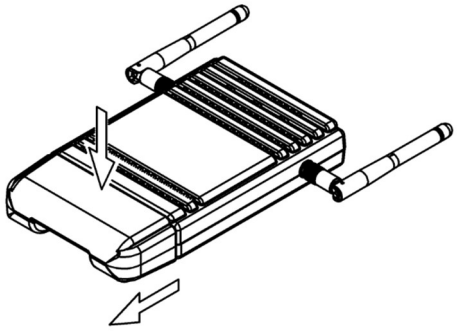


⚠ CAUTION

- Using the product with the antenna disconnected from the antenna connector or with the antenna loosened may result in a breakdown of the product. Always use the product with the antenna connected.
- Do not touch the antenna connector when the power is on. If you need to touch the connector to remove the antenna connector, be sure to turn off the power to the product.
- Be careful not to touch the antenna connector with your bare hands, as static electricity may cause the product to malfunction.

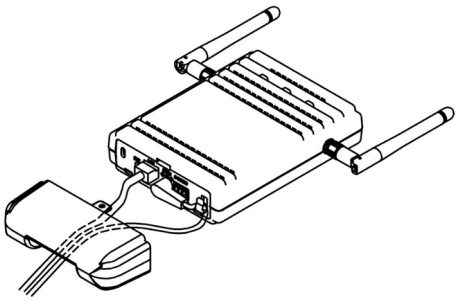
◆ Removing the connector cover

While lightly pushing vertically on the center of the connector cover [(1) in the diagram], slide the entire cover [(2) in the diagram], and remove the connector cover.



◆ LAN Port

Connect a LAN cable to this product's LAN port.



⚠ CAUTION

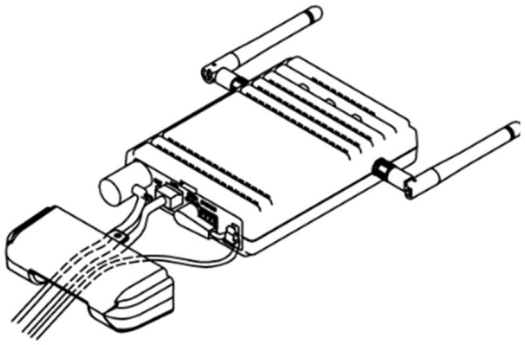
- Ensure that the cable length between this product and a PC or hub is 100 m or shorter.
- When supplying power via PoE or when using 100BASE-TX, use a Category 5 or better cable. When using 10BASE-T, use a Category 3 or better cable.

◆ Attaching the security wire

A commercially available security wire can be attached to the security slot located on the connector section.

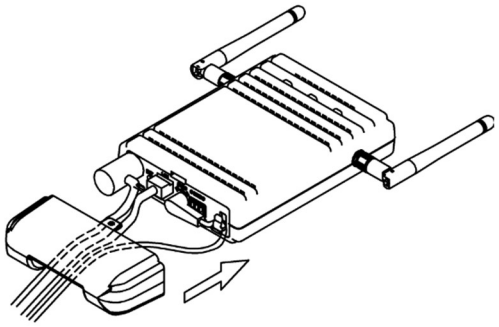
Recommended security wires :

- KOKUYO EAS-L41
- SANWA SUPPLY SL-31S



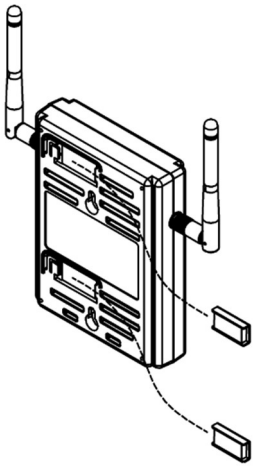
◆ Attaching the connector cover

Attach the connector cover to the product.



2. Using magnets for installation

Attach the included magnets to the two magnet attachment locations on the back of the access point. To attach the magnets, push them in the direction of the arrow to insert them entirely into the attachment holes.



⚠ CAUTION

- When using magnetic installation, please ensure the equipment is installed at a height of 2 meters or less.
- Do not place the magnets near items that are susceptible to magnetic fields.
- If the product is moved while attached to a steel desk or other object, it may damage the painted surface.

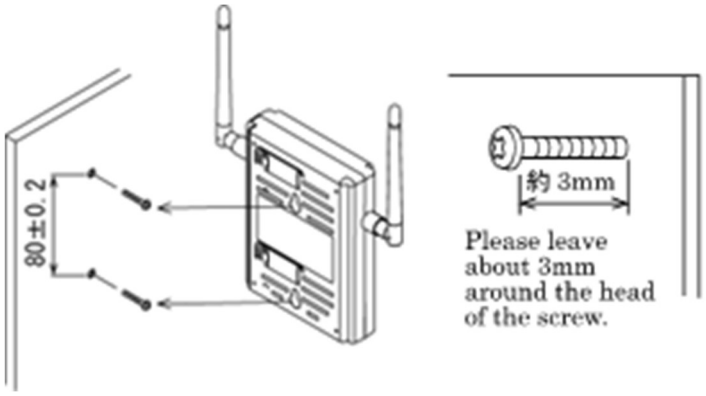
3. Using the included screws for installation

Referring to the diagram to the right, drive the two included screws into a sturdy, vertical wall surface while leaving around 3 mm of the screws sticking out from the wall surface.

Hook the attachment holes on the back of the access point to the heads of the screws to attach it.

Due to the characteristics of wireless networks, the signal will spread in a wider area when the access point is installed in a highly-visible location, so we recommend you install it in a location as high as possible.

Note that the placing the product near metal or concrete walls (including steel beams) may cause the signal quality to degrade.

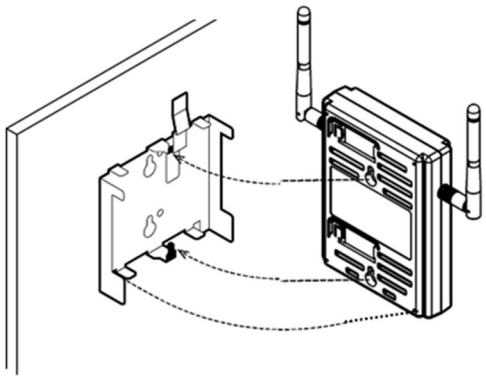


⚠ CAUTION

- The access point cannot be installed on the ceiling using the screws due to the danger of falling. If a ceiling installation is required, use the optional installation bracket.
- If the product's ventilation holes are blocked, the product may malfunction due to a rise in internal temperature.

4. Installing the product with an installation bracket (sold separately)

You can use the FX-BRA20 installation bracket (sold separately) to install this product on a wall or ceiling. For details, see the user's manual of the installation bracket (sold separately).



Connection to Devices and Setup Methods

This product is set up via a network using a Web browser. Follow the setup procedure below once the product is set up.

1. Preparation before Setup

You must use a PC which can be connected to a network as the product is set up via the network. The setup is performed by connecting a PC for setup purposes and then using a Web browser.

5. Connecting for the first time

1 Connect this product to PC on a wired LAN.

2 Select an IP address 192.168.0.XXX (e.g. 192.168.0.10) for the PC, which is not the same address as for this product. And then set the subnet mask to 255.255.255.0

*** The default setting IP address is 192.168.0.1.**

The following example settings are for Windows 11 or Windows 10 using Microsoft Edge.

◆ Windows 11 / Windows 10

1 Click [Start] (the Windows logo button), and then click [Control Panel], [Network and Internet], [Network and Sharing Center], then [Change adapter settings]. Then, right-click the Ethernet icon, and then click [Properties].

2 If a User Account Control window appears, click "Yes" or "Continue".

3 Select the "Internet Protocol Version 4 (TCP/IPv4)" check box, and click "Properties".

4 In the "Use the following IP address" field, type an IP address 192.168.0.XXX, which is not the same address as this product (e.g. 192.168.0.10), and then set the subnet mask to 255.255.255.0.

5 Click "OK", and then click "OK" or "Close" to enable the settings.

6. Changing the settings

1 Connect this product to PC on a wired LAN.

2 Set the network address of the PC to the same network address as for this product.

2. Setup Using a Web Browser

Start up a Web browser and enter the IP address of this product after “http://” in the address bar. If connecting for the first time, enter the default IP address. When the default setting IP address is 192.168.0.1, enter as follows.

http://192.168.0.1/

Enable the JavaScript function in the browser setting as it is used.

Recommended web browsers

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

1. Setting the Browser

You may have to change the browser settings as well as the IP address and subnet mask for the PC to be connected to this product via the network.

◆ Changing browser settings

(1) Proxy Settings

Networks at companies and schools may use browsers with proxy settings. Proxy is not required as a PC is used to set up the product, which is on a local network. Disable the proxy settings temporarily when setting up this product on a Web browser.
The following example settings are for Microsoft Edge, Google Chrome, or Mozilla Firefox.
Actual settings will depend upon the environment you are using. For details, see your web browser's help information or contact the software manufacturer.

Microsoft Edge or Google Chrome

1 Right-click [Start] (the Windows logo button), and then click [Network & Internet].

2 Click [Proxy], and then turn off "Use a proxy server".

Mozilla Firefox

1 Launch Mozilla Firefox.

2 From the menu bar, click [Tools] - [Options].

3 Click [Advanced], open the [Network] tab, and then click [Settings].

4 Select "No proxy", and then click "OK".

5 Click "OK" button.

(2) Enable JavaScript.

The following example settings are for Microsoft Edge, Google Chrome, or Mozilla Firefox.
Actual settings will depend upon the environment you are using. For details, see your web browser's help information or contact the software manufacturer.

Microsoft Edge

1 Launch Microsoft Edge.

2 Click [···] in the upper right corner of the screen to access the Menu tab, and then click [Settings].

3 Click [Site permissions], and then click [JavaScript].

4 Turn on "Allow (recommended)".

Google Chrome

1 Launch Google Chrome.

2 Click [···] in the upper right corner of the screen to access the Menu tab, and then click [Settings].

3 Click [Security and Privacy], and then click [Site settings].

4 Click [JavaScript], and then Turn on "Allow (recommended)".

Mozilla Firefox

1 Launch Mozilla Firefox.

2 From the menu bar, click [Tools] - [Options].

3 Click [Contents], and then select "Enable JavaScript" to turn on JavaScript.

4 Click [OK] to enable the settings.

⚠ CAUTION

When the Web browser settings have been changed, restore the original browser settings upon the completion of setup of this product.

2. Connecting to This Product Using Web Browser

The following login screen is displayed when connected to this product using web browser.

If the login screen is not displayed, the IP address setting for PC, browser settings, or the URL entered in the address bar of the browser may be incorrect.

When connecting for the first time, enter the default user name (admin) and password (pass) and click [OK].

⚠ CAUTION

Please change the password from the factory defaults to avoid possible security issues.

For details on how to change the password, please refer to " **Setup and Status Display** " > "**4. Maintenance** " > " **Password** ".

3. Configuring Settings from a Web Browser

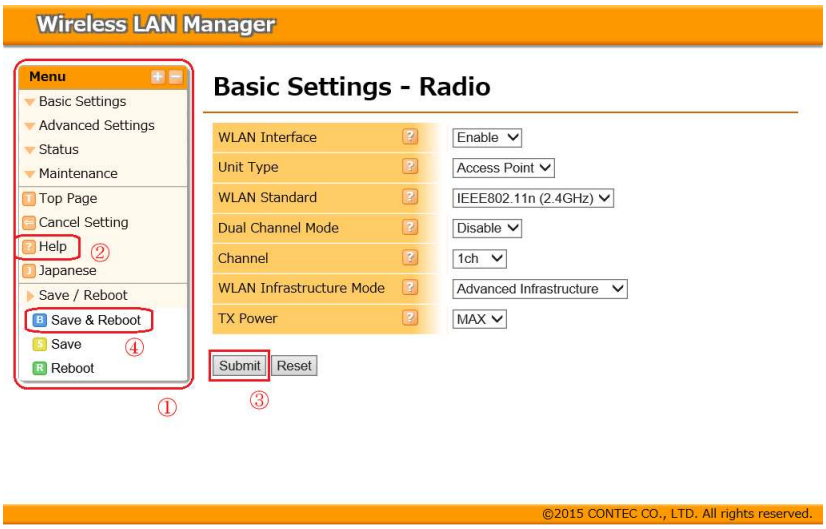
Select [Basic Settings] on the menu on the left side of the screen ((1) in the following figure), and then select the setting item in the menu that opens.

For details on the setting items, refer to the [Help] ((2) in the following figure).

The settings must be temporarily recorded on this product, so, after changing the settings on each page, be sure to click [Submit] ((3) in the following figure).

After you have configured all the settings, save them and restart this product to enable the settings.

Click [Save & Reboot] ((4) in the following figure) on the menu on the left side of the screen.



There will be no problem if you just save the settings now but reboot the product later when necessary. In this case, saving the settings does not actually change the settings of the product. Therefore, make sure to reboot the product later.

* For explanations of functions and setting instructions, see the manual available from the CONTEC website or see help information.

⚠ CAUTION

Saving the settings takes about 5 to 10 seconds. During this time, all LEDs flash. Do not restart or turn off the power until "Save complete" appears on the display. If you restart or turn off the power while the settings are being saved, the settings files and firmware may be corrupted, resulting in the inability to start up normally.

Do not turn off the power to the machine during startup, restart, or initialization. Doing so may cause the machine to stop operating normally.

Wireless Link Mode and Wireless LAN Function

This chapter describes the major functions of the FLEXLAN series as a wireless LAN system and the wireless link modes of the product along with configuration examples of networks available in the wireless link modes.

1. Wireless Link Mode

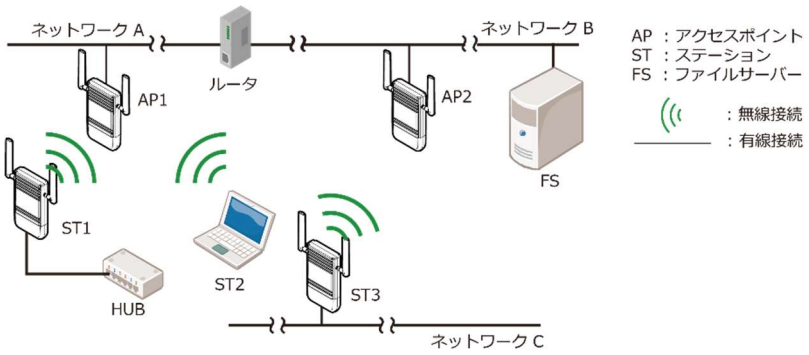
This product has three wireless link modes. The available functions and network configurations differ depending on the mode. Use the wireless link mode most suitable to the type of network you are constructing.

The factory default setting is “Advanced Infrastructure Mode”.

“**Connection to Devices and Setup Method(P37)** “ and “錯誤! 找不到參照來源。**(P**錯誤! 尚未定義書籤。**)** “ describe the software setting procedures for the wireless link modes and related items.

1. Standard Infrastructure Mode

In this mode, each access point (AP) can accommodate stations (ST) to make up a network.
This mode allows the use of multiple APs to configure a wide-area wireless LAN. All communication between wireless terminals must go through an AP.



In the Standard Infrastructure mode above, all wireless terminals communicate via AP. Roaming functions are supported, allowing login to any AP within range of radio waves.
For the IP tunneling function to work properly, one of the APs must be setup as a master AP.

・Advantages

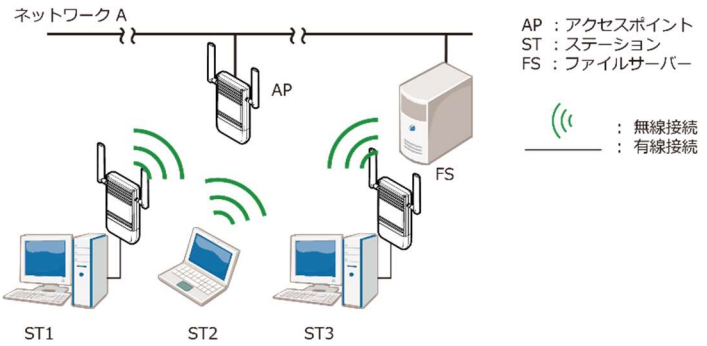
(1) Allows log-in restrictions (security function).
(2) Improves security using the WSL (Wireless Security Link).
(3) When connecting a CONTEC station to this product using a wired connection, there is no limit to protocols and the number of devices that can be connected.

2. Compatible Infrastructure Mode

This mode allows the product to be networked with other manufacturers' Wi-Fi certified wireless terminals other than the FLEXLAN series. Communications between the wireless terminals are always made via the APs.

⚠ CAUTION

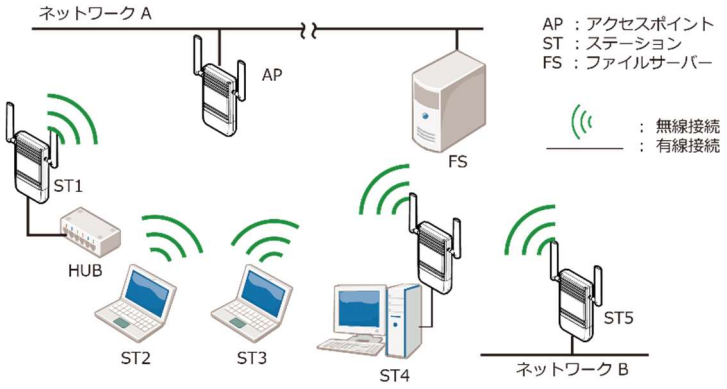
The Compatible Infrastructure mode does not guarantee interconnection with Wi-Fi compliant products of other manufacturers.



In the Compatible Infrastructure mode, each wireless terminal performs communication via the AP as in the Standard Infrastructure mode. Roaming functions are supported, allowing login to any AP within range of radio waves.

3. Advanced Infrastructure Mode

The Advanced Infrastructure mode is a mixture of the Standard Infrastructure and Compatible Infrastructure modes. The Advanced Infrastructure mode can be used only when the product is configured as an access point.



On the terminal set to the Standard Infrastructure mode, the FLEXLAN series' unique functions can be used.

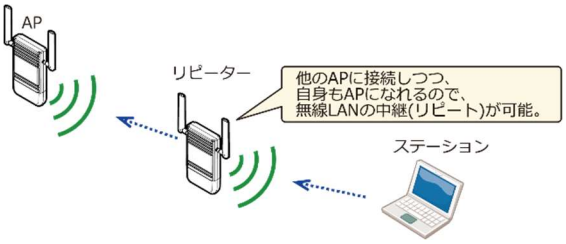
The terminal set to the Compatible Infrastructure mode serves as a simple bridge and thus the FLEXLAN series' unique functions cannot be used on this terminal.

2. Repeater

1. What's Repeater?

The repeater used with the wireless LAN is a function that operates the wireless LAN equipment as a pair of virtual wireless LAN devices (VAP). One of these devices is set as the access point and the other is set as the station.

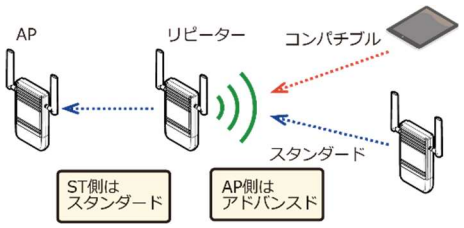
It is possible to connect to other access points from the station and to log in to the access point from other stations.



2. Specification for Repeater and Wireless Connection Mode

When a piece of equipment is set as a repeater, its VAP2 becomes an access point and its VAP1 becomes a station. In this situation, if you set "Wireless Connection Mode" to "Advanced Infrastructure", the repeater's access point side will operate in "Advanced Infrastructure" mode and the repeater's station side will operate in "Standard Infrastructure" mode.

If you set "Wireless Connection Mode" to "Compatible Infrastructure", both the access point and the station will operate in "Compatible Infrastructure" mode. In this situation, the multi-client function of VAP1 (the station) will be forcibly enabled.



Wireless connection mode of repeater	VAP2 of repeater (AP side)	VAP1 of repeater (ST side)
Standard Infrastructure	Standard Infrastructure	Standard Infrastructure
Compatible Infrastructure	Compatible Infrastructure	Compatible Infrastructure
Advanced Infrastructure	Advanced Infrastructure	Standard Infrastructure

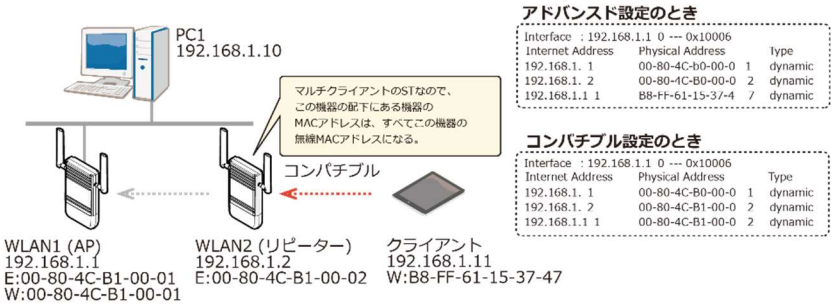
If you set "Wireless Connection Mode" to "Advanced Infrastructure", you will be able to connect to stations in "Standard Infrastructure" mode and to stations in "Compatible Infrastructure" mode.

3. Recommended Setting

When "Wireless Connection Mode" is set to "Compatible Infrastructure", the VAP2 (station side) of each repeater located under this device is also set to "Compatible Infrastructure" mode. As such, all terminals under the repeater have the same MAC address in the PC1 ARP table.

In this situation, clients roam from WLAN2 to WLAN1, and communication cannot be performed from PC1 to 192.168.1.11. The reason for this is that if a client connects to WLAN1, its MAC address will be changed.

To have PC1 perform communication, you have to delete the PC1 ARP table, and have PC1 learn the 192.168.1.11 MAC address again.



PC1 is linked to the client roaming, so the PC1 ARP table cannot be deleted. When you use repeaters to construct your system, we recommend that you operate the repeaters in "Advanced Infrastructure" mode.

⚠ CAUTION

If APs without "Standard Infrastructure" mode made by other companies exist within your system, you will not be able to use "Advanced Infrastructure" mode.

For example, if WLAN1 in the above figure is an access point made by another company and you set WLAN2 to "Advanced Infrastructure" mode, WLAN1 and WLAN2 will not be able to communicate with each other.

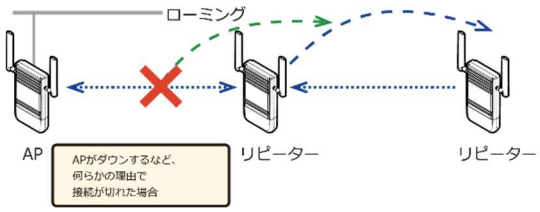
4. Notes

When you configure the device to operate as a repeater, regardless of whether the network configuration is chain or star, use the "Preferred AP" function to specify the connection destination access point.

Also, you have to set the "Connections to Non-Preferred APs" function to "Disable" in order to prevent loops between repeaters with unauthorized connections to unexpected access points.

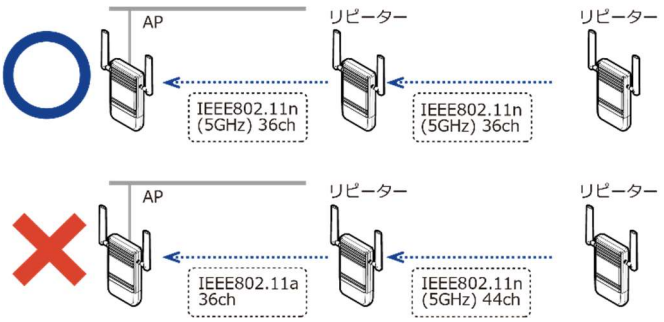
(1) Use the preferred access points to specify the connection destinations to establish an arbitrary connection structure.

(2) If you do not fix the connection destinations, loops may occur between repeaters.



If you set a device as a repeater, set all parts of the wireless network to the same channels and the same wireless LAN standard.

For example, if you construct a network with one access point and two repeaters for a total of three pieces of wireless equipment, configure all the equipment so that the same wireless LAN standard and the same channels are used.



3. Installation in a Network

This section describes how to install this product to construct a network with improved performance and discusses the general features and radio characteristics of the wireless LAN as well as the guidelines for constructing the network.

1. Features of the Wireless Network

In general, the operation of a wireless network is the same as for most other types of LAN. The most prominent feature of the wireless network is that it uses radio waves as its medium, eliminating the need for cabling. The wireless network thus requires no cabling cost and has other advantages as listed below :

- Quick construction of a LAN
- Temporary installation of a LAN
- Higher flexibility in layout of connected PCs (terminals)
- Assured mobility of connected PCs (terminals)

On the other hand, the wireless network has the following drawbacks from the operational point of view due to the nature of radio waves :

- Signal attenuation
- Signal interference

Also, although this unit does not require a radio license, it is subject to radio regulations.

2. Operating Environment and Radio Waves

When using this product to construct a network, install and operate it considering the radio environment to optimize the performance.

◆ Is allowed to use radio equipment at the installation location?

In some medical institutions and laboratories, radio-sensitive precision instruments are used and it may be prohibited to use radio equipment.

◆ Radio waves are attenuated.

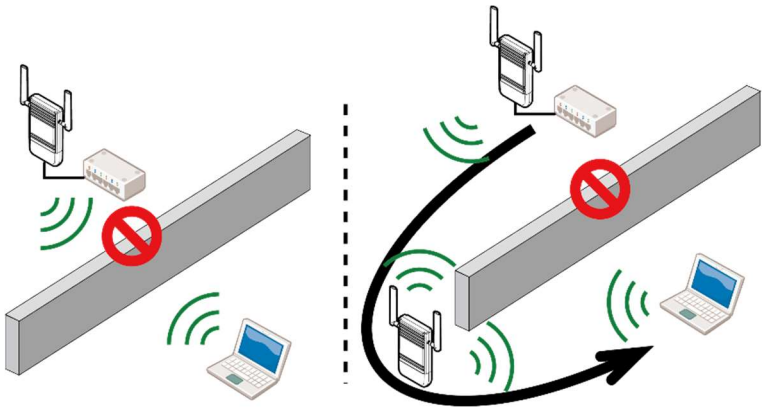
Although a radio wave is attenuated naturally as it travels from its transmission source, it may also be attenuated by an object existing in its way. Major obstacles that attenuate radio waves are as follows :

- Concrete wall
- Metal surfaces in the vicinity of the antenna

Obstacles blocking radio waves include metal walls and walls containing a metal firewall.

Strictly speaking, nearly all objects in the path of the radio waves (such as partitions or people) cause some attenuation but these do not have a significant impact on network performance.

RSSI (Receive Signal Strength Indication) utility is available as a means of knowing the signal strength of an incoming radio wave. Placing this product for a greater RSSI value makes the communication state more stable. If the RSSI value is small and slightly moving the position of the product does not increase the RSSI value, it indicates radio wave attenuation either to the distance or by an obstacle.



◆ Pay attention to radio interference.

Radio interference means the reception of radio waves in the frequency band used by this network that are generated by equipment that is not part of the network to which this product belongs. Listed below are major examples of sources of interfering radio waves generated in general environments excluding plants and factories：

- 5GHz (if using this product in the 11ax/ac/n/a 5 GHz band) or 2.4GHz (if using this product in the 11ax/n/b/g 2.4 GHz band) band wireless networks that do not comply with IEEE802.11.
- If using IEEE 802.11ax/n/b/g standard in the 2.4GHz band. Ex. microwave ovens, security gates (installed near the entrances of some department stores and rental shops), copiers which give off the 2.4GHz electric waves.

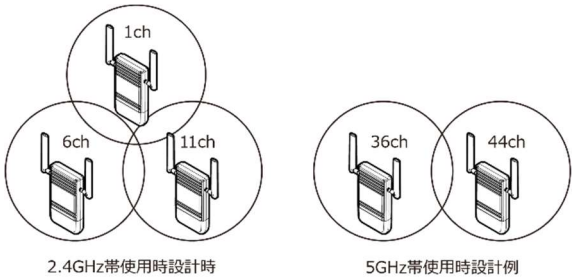
Where there is a large metal wall such as in a warehouse, the radio wave generated from the sender is reflected, resulting in those radio waves reaching the receiver which have taken different routes (thereby phase-shifted). This has the similar effect as the generation of interfering radio waves, possibly slowing down data transfer.

Most of the interfering radio wave sources other than wireless networks have local and/or temporary effects, not so affecting network performance. Rarely, however, the date rate is reduced and, in the worst case, communication is disabled temporarily. In such cases, change the location of this product and the channel used for communication. This may solve the problem.

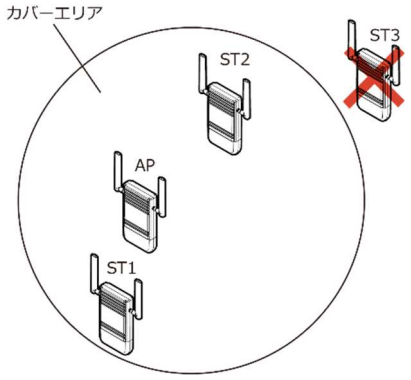
◆ Constructing a Network

This section gives some pointers and cautions relating to constructing a network using the AP and station, and provides some practical examples.

- Wireless communication is possible with the station corresponding to the channel. Wireless communication is possible with stations that support the above channels. Using different channels for wireless networks adjacent to each other (In 5GHz band, set it to 36.44, 8ch or more apart and in 2.4GHz, 1, 6, 11 5ch or more apart) prevents radio interference and improves the throughput of either network.



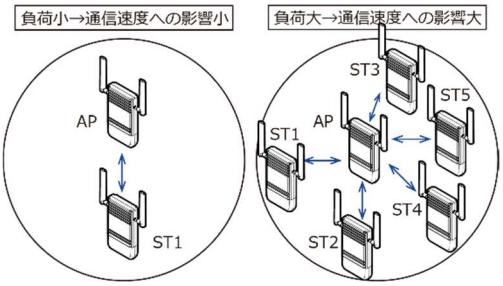
- Check the coverage (cover area) of the AP. To use the AP with two or more station logged in AP, all the station must be installed within the cover area. The AP's coverage varies with obstacles (concrete walls, iron doors, elevator halls, etc.). Note also that the number of transmission/reception errors increases beyond a certain transmission distance.



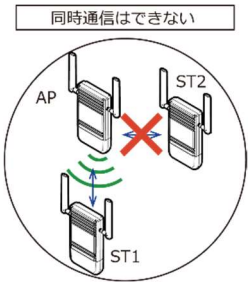
When setting up the network, check the RSSI level then confirm that communication works correctly with the application you plan to use. For a TCP/IP system, for example, you can use the Windows PING command. To use PING, start the command prompt (MS-DOS) and enter the following command. The example command is for an AP with an IP address of 192.168.0.2.

```
ping 192.168.0.2
```

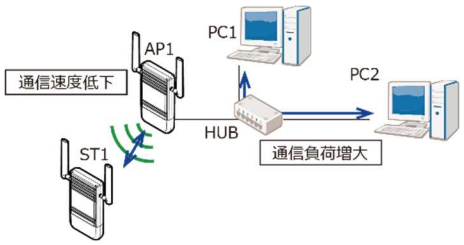
- Two or more stations can log in the AP at the same time　However, remember that the communication speed slows due to the increased loading as the number of user units for a particular AP increases.



- If a pair of wireless terminals are communicating via a particular channel, no other communications can use that channel within the range of the radio signal (the exception is broadcasting which transmits to all terminals).　As a result, communication speed tends to drop as the density of wireless terminals increases although this depends to a large extent on how frequently the network is used.

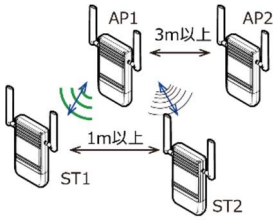


- If the AP is connected to an Ethernet hub or similar, an unexpectedly large load can occur on the AP if the Ethernet traffic is heavy and this may reduce the performance of the wireless network.　This can be solved by changing the hub connected to the AP to a switching hub (bridge).



- Setup the software in accordance with how the network will be used.

- The communication speed may also drop due to interference if two wireless terminals are located close to each other.　In general, maintain a gap of about 1m between station, 3m between APs and station, and 3m between APs.



- The best performance is achieved from antennas if they are located in an open space free from obstructions. Avoid locating antennas where they will be hidden. In particular, when communication distance is an important consideration, it is recommended that you install antennas in a high location with a clear view.
- Floors often contain steel beams or metal firewalls and therefore communication between floors is often not possible.

Maintenance

This chapter describes how to perform maintenance on the AP and explains the tools to be used. Here, “maintenance” means the following : log file collection, firmware upgrades, and saving and restoring the software settings.

1. Maintenance Tool

This maintenance tool is available for the FTP, Web browser and FLEX HELPER. This section describes how to use the tool by the FTP. or details about downloading using a Web browser, see the section titled "錯誤! 找不到參照來源。**(P**錯誤! 尚未定義書籤。**)**".

For details and applications of FLEX HELPER, contact your dealer.

2. Log File Collection

To collect the log file, you collect it by using Web browser or FTP via the LAN.

The log file is in text format and can be displayed in the Notepad or WordPad programs that come with Windows.

The collected log file is stored the AP memory with the following file name.

File name : LOGFILE

⚠ CAUTION

To collect the log file, log collection must be enabled. Note also that the contents of the log file differ depending on the operating mode and software settings.

1. Using FTP to Get the Log File

To collect log files using FTP, follow step 1~6.

1 Move to the folder in which you wish to save the file.

2 Run FTP to log in to the AP.

3 Run FTP to log in to the AP. (Enter FTP user's name)

4 Run FTP to log in to the AP. (Enter FTP password)

5 Transfer the log file.

6 Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the saving folder D : ¥tmp and LOGFILE will be collected after connecting to this product via FTP. The example assumes the User as admin (blank is OK), Password as Pass (initial setting) and the IP address as 192.168.0.1.

```
C:¥>cd D:¥tmp                          ····· 1
D:¥tmp>ftp 192.168.0.1                 ····· 2
User (192.168.0.1:none):admin          ····· 3
Password:pass                          ····· 4
ftp>get LOGFILE                        ····· 5
ftp>bye                                ····· 6
```

*For details about downloading using a Web browser, see the section titled "錯誤! 找不到參照來源。 **(P**錯誤! 尚未定義書籤。**)**" .

3. Saving the Settings File

Making a backup of the AP software settings file has the following benefits :

- If you have more than one AP and all APs have the same settings, you just need to setup one AP then use the resulting settings file for the other APs. (However, as this sets the same IP address for all APs, you need to change the IP address separately.)
- The old settings can be restored easily if a fault causes the settings file to be erased.

The settings file is stored the AP memory with the following file name.

File name ··· CONFIG

If the MAC address filtering is used, its setting file should also be saved. The setting file is stored in memory on the AP with the following file name :

MAC address filtering ··· MACFIL

The file is in the memory even when the MAC address filtering function is not in use it, however, does not have to be saved.

1. Using FTP to Backup the Settings File

To collect configuration files using FTP, follow step 1~6 below.

1 Move to the folder in which you wish to save the file.

2 Run FTP to log in to the AP.

3 Run FTP to log in to the AP. (Enter FTP user's name)

4 Run FTP to log in to the AP. (Enter FTP password)

5 Transfer the settings file (CONFIG).
MACFIL is also transferred if necessary.

6 Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the saving folder D：¥tmp and CONFIG and MACFIL will be collected after connecting to the product via FTP. The example assumes the IP address as 192.168.0.1。

C:¥>cd D:¥tmp	····· 1
D:¥tmp>ftp 192.168.0.1	····· 2
User (192.168.0.1:none):admin	····· 3
Password:pass	····· 4
ftp>get CONFIG	····· 5
ftp>get MACFIL	····· 5
ftp>bye	····· 6

*For details about downloading using a Web browser, see the section titled "錯誤! 找不到參照來源。**(P**錯誤! 尚未定義書籤。**)**" .

4. Restoring the Software Settings

The software settings of this product can be recovered by using the saved setup file.

1. Using FTP to Restore the Settings

Follow the procedure below to recover the software settings using FTP.

1 Move to the folder with file.

2 Run FTP to log in to the AP.

3 Run FTP to log in to the AP. (Enter FTP user's name)

4 Run FTP to log in to the AP. (Enter FTP password)

5 Transfer the settings file(config).
MACFIL is also transferred if necessary.

6 Issue the reset request command(command ： quote rst).

7 Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.
In this example, the file will be moved to the folder with file D : ¥tmp and CONFIG and MACFIL will be transferred after connecting to the product via FTP. The example assumes the IP address as 192.168.0.1.

```
C:¥>cd D:¥tmp                          ····· 1
D:¥tmp>ftp 192.168.0.1                 ····· 2
User (192.168.0.1:none):admin          ····· 3
Password:pass                          ····· 4
ftp>put CONFIG                         ····· 5
ftp>put MACFIL                         ····· 5
ftp>quote rst                          ····· 6
ftp>bye                                ····· 7
```

The reset request command shown in (6) is a command used to reboot the product. There is no problem to skip (6), stop FTP in (7) and reboot the product later.

5. Upgrading the Firmware

The AP firmware may be upgraded to resolve any bugs found in the software or to add new functions. Contact CONTEC via our web site for details of the latest firmware.

There are two ways to upgrade the version of the firmware : FTP; and Access Point Manager with a Web setup screen.

1. Performing an Upgrade Using FTP

Follow the procedure below for the firmware version up settings using FTP.

1 Move to the folder with file.

2 Run FTP to log in to the AP.

3 Run FTP to log in to the AP. (Enter FTP user's name)

4 Run FTP to log in to the AP. (Enter FTP password)

5 Change the transfer mode to binary.

6 Transfer the firmware file FIRMWARE.BIN.

7 Issue the reset request command (quote rst).

8 Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the firmware file for version up will be moved to the folder with file D : ¥tmp and FIRMWARE.BIN will be transferred after connecting to the product via FTP. The example assumes the IP address as 192.168.0.1.

```
C:¥> cd D:¥tmp                          ····· 1
D:¥tmp>ftp 192.168.0.1                  ····· 2
User (192.168.0.1:none):admin           ····· 3
Password:pass                           ····· 4
ftp>bin                                 ····· 5
ftp>put FIRMWARE.BIN                    ····· 6
ftp>quote rst                           ····· 7
ftp>bye                                 ····· 8
```

*For details about downloading using a Web browser, see the section titled "錯誤! 找不到參照來源。**(P**錯誤! 尚未定義書籤。**)**" .

⚠ CAUTION

The setup file data and firmware data may be damaged and the product may not operate properly if it is rebooted or switched off while the firmware is still being updated (data being written).

6. Initialization

There are two ways to initialize this product (recovering the factory settings).

- Using a Web browser
- Using the INIT switch of the main unit

Each initialization method is described below.

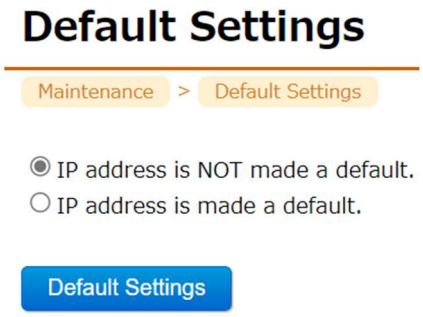
1. Using a Web Browser

Follow the procedure below when using Web browser to initialize the product.

1 Follow the procedure below when using Web browser to initialize the product.

2 Select “Maintenance” - “Default setting” from the menu.

1 To leave the IP address of the product unchanged without initialization, tick “Do not set IP address to default”. To initialize the IP address, tick “Set IP address to default” and then click “Default Settings”.



2 Click “Save/Reboot” on the menu to save the default setting and reboot the product.

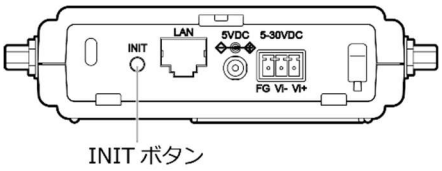
⚠ CAUTION

Even when the default settings are restored, they are not saved to the device's configuration file, so you must save and restart to reflect the settings.

Do not turn off the machine during startup, restart, or initialization. Doing so may cause the machine to stop operating normally.

2. Using the INIT Switch of the Main Unit

Follow the procedure below when using the INIT Switch of the Main Unit to initialize the product. There is an INIT button on the side of the machine. Use a thin, non-conductive rod to initialize the settings as described below.



1 The LEDs of POWER, LAN and WLAN continue to blink for a little while after INIT switch is pushed.

2 Release this button after the LED starts flashing but before it reverts to an ON state (an interval of approx. 3 seconds).

1 All the settings are restored to the default settings after the product is started next time.

⚠ CAUTION

The flashing continues for a little while after the product is released during initialization by pushing the INIT switch. This indicates internal memory files are being deleted. The internal memory files may be damaged and the product may not start up properly if the power is switched off before the flashing stops. Always reboot the product after the flashing stops.

When you're in trouble

It explains the causes of faults and problems, how to handle them, and how to check them.

1. Troubleshooting

If any problem occurs during use, follow the procedure below.

1. When Communication Fails

◆ Check wired LAN communication

Check the wired LAN communication between this product and the connected PC.

- Check that the LAN cable is connected correctly.
- Check if the IP addresses and subnet masks of the product and PC are set correctly.
- The communication with this product is not possible unless the TCP/IP protocol is installed in the PC.

◆ Check wireless LAN communication

If no problem is detected in the wired LAN communication between the product and PC, check the wireless LAN communication between the product and access point.

- The FLEXLAN series is designed to handle a variety of operating formats, and requires software setting for each type of operation. Check that the settings are appropriate for the type of operation, and check the format in which communication is being attempted.
- The terminals that cannot communicate with each other may have the same ESSID. Two terminals with the same ESSID cannot communicate with each other.
- Check whether the wireless link mode has been set correctly. The wireless link mode of the station (slave station) must support the wireless link mode set on this product.
- Check whether communication is restricted by security functions such as the MAC address filtering.
- Check whether the data encryption setting is the same as that of the recipient. Communication cannot be performed while data encryption is being switched between ON (enabled) and OFF (disabled).

◆ Check the peripheral environment and place of installation

A nearby source of electromagnetic interference can prevent communication. In general locations (excluding factories) the following may be sources of electromagnetic emissions.

- Wireless network not conforming to wireless LAN.
- When using by 2.4GHz band, electric devices which give off 2.4GHz band electric wave - microwave oven, security gate (it is an antitheft gate in the shop), copy machine and so on.

Most electromagnetic sources other than wireless networks are local and not continuous, and therefore by moving the location of the unit and waiting briefly, communication may be possible.

- Sometimes communication is hindered by attenuation of electric waves. Attenuation occurs naturally as distance from the source of transmission increases, but may also be caused by objects in the path of the transmission. The objects primarily responsible for attenuation are the following.
  - ・ Concrete walls
  - ・ Metallic surfaces around this product

2. Setup Screen Unavailable on Web Browser

- Check if communication is possible between the product and PC.
- If no problem is detected in the communication between the product and PC, it may be related to the browser settings. For the browser settings, see "**Connection** to Devices and Setup Method**(P37)**".

3. Does not start

◆ Check the LED

- Check whether the "POWER" LED is illuminated. If it is not illuminated, check the power cable and make sure that it is connected correctly to the power jack and the socket.
- Check whether the Power LED is flashing. If the power LED is still flashing more than 5 minutes after the power is switched on, the problem may be an AP firmware failure.
  In this case, the problem may be a startup error caused by corrupt data in the memory of this product.
  If you cannot restore it, contact your retailer.

◆ Check the power

- If using an AC adapter, check that the adapter is an optional accessory of a type specified by CONTEC. Only use AC adapters specified by CONTEC with this product.

- If supplying power from the power connector, check the power supply connection, supply voltage, etc., and make sure that there are no problems. For details about connecting the power supply, see "**Power** Suppl**(P28)**".

Appendix

This section lists the specifications and the physical dimensions of the product, and the details of model name.

1. Hardware Specifications

1. Hardware Specifications

Function Specifications

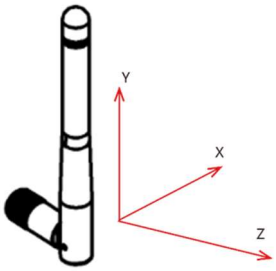
Item			Description
Unit Type			Single Station/Access point/Repeater/
Wired LAN			
	Ethernet standard		IEEE802.3 (10BASE-T), IEEE802.3u (100BASE-TX), IEEE802.3af
	Port Speed/Type/Port Number		10/100Mbps / Half Duplex、Full Duplex / 1
Wireless LAN			
	Wireless Standard		IEEE802.11n, IEEE802.11a, IEEE802.11b, IEEE802.11g
	Band Width		20/40MHz
	Channel	HT20	5180-5320 MHz: 36, 40, 44, 48, 52, 56, 60, 64 5500-5700 MHz: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 5745-5825 MHz: 149, 153, 157, 161, 165
		HT40	5180-5320 MHz: 38, 46, 54, 62 5500-5700 MHz: 102, 110, 118, 126, 134 5745-5825 MHz: 151, 159
	Data transmission speed *1	IEEE802.11n	300 - 6.5Mbps [MSC0 - 15, Short/Long GI]
		IEEE802.11a	54, 48, 36, 24, 18, 12, 9, 6Mbps
		IEEE802.11g	54, 48, 36, 24, 18, 12, 9, 6Mbps
		IEEE802.11b	11, 5.5, 2, 1Mbps
	Security		
		IEEE802.11n	WPA(AES), WPA2(AES), WPA-PSK(AES), WPA2-PSK(AES), WSL (Combination with mentioned above is possible)
		IEEE802.11a/b/g	WEP(Open/ Shared Key /Auto), WPA(AES, TKIP), WPA-PSK(AES,TKIP), WPA2(AES, TKIP), WPA2-PSK(AES,TKIP), IEEE802.1X(EAP-TLS, PEAP), WSL (Combination with mentioned above is possible)
Antenna			Dipole Antenna ×2 MIMO
External Dimensions (mm)			Unit only: 136.2(W)×117.4(D)×31.0(H) including power cable disconnection prevention hook With connector cover and Antenna attached is referred to the external dimensions diagram.
Weight			300g

*1 These are theoretical values based on their respective wireless LAN standards; they do not indicate actual data transfer rates.

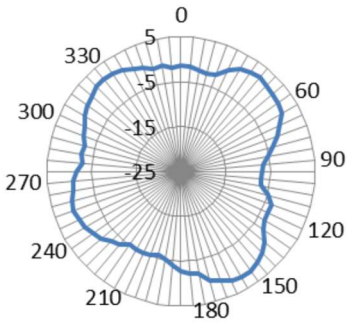
Environmental Specifications

Item	Description
Input voltage range	5VDC ± 5% (DC Jack), 5 - 30VDC ± 5% (power connector), 36 - 57VDC (PoE)
Rating input current	0.83A (5VDC input), 0.15A (30VDC input) (Max.), 0.13A (PoE input 48V)
Operating ambient temperature	0 – 40℃(without wind)
Operating ambient humidity	10 - 90%RH (No condensation)
Floating dust particles	Not extreme
Corrosive gases	None
Permitted transient power failure	17ms or less (100VAC@25°C) An automatic reset is performed when low voltage is detected.
Standard	FCC, RoHS Compliant

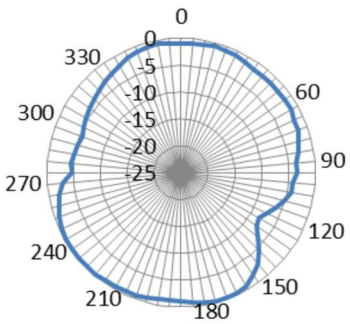
2. Antenna



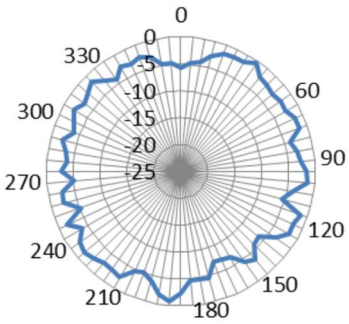
■5.5GHzXY



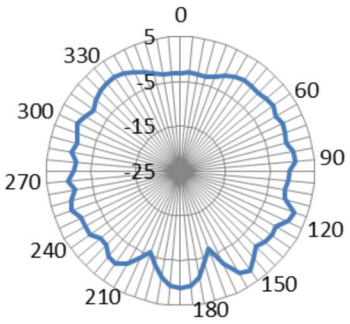
■2.4GHzXY



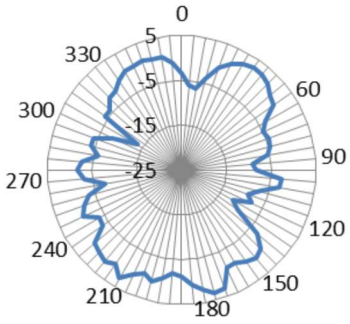
■5.5GHzXZ



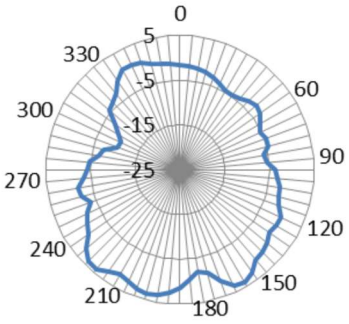
■2.4GHzXZ



■5.5GHzYZ

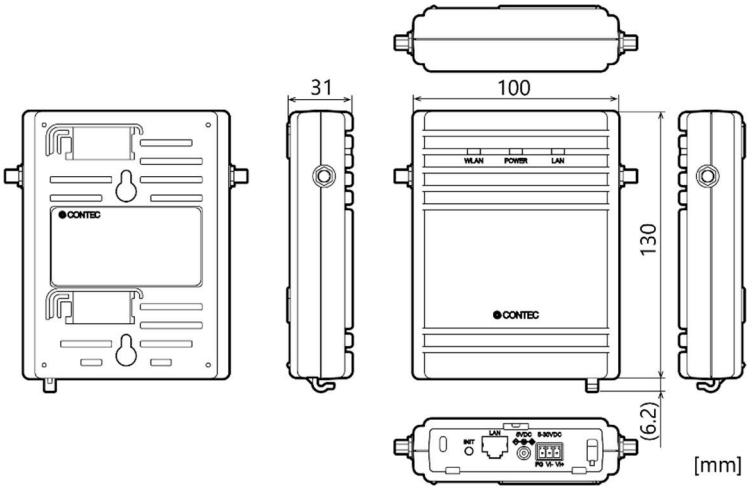


■2.4GHzYZ

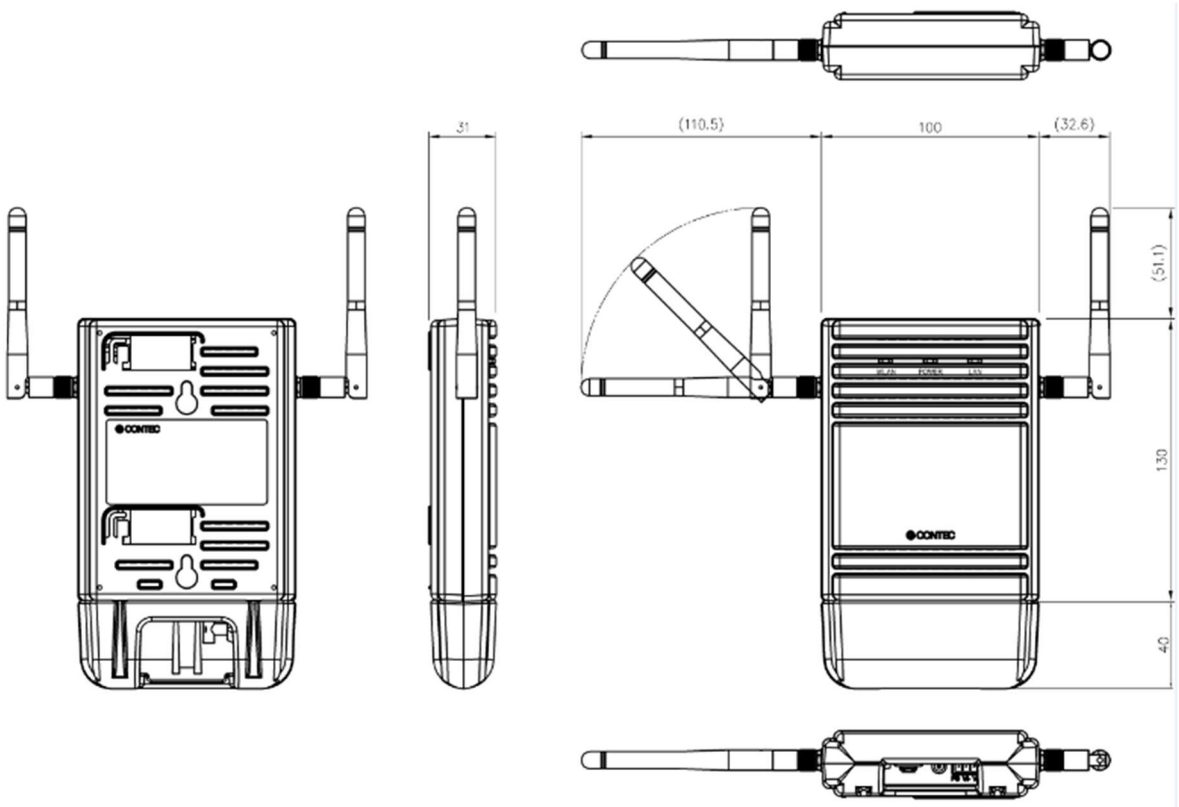


2. Physical Dimensions

1. External dimensions (Unit only)



2. External dimensions (Antenna Connected)



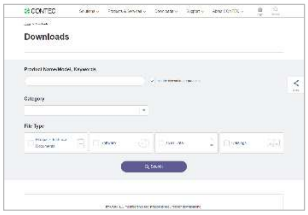
Customer Support and Inquiry

CONTEC provides the following support services for you to use CONTEC products more efficiently and comfortably.

1. Services

CONTEC offers the useful information including product manuals that can be downloaded through the CONTEC website.

Download



https://www.contec.com/download/

You can download updated device driver, firmware, and differential manuals in several languages. Membership registration (myCONTEC) is required to use the services.

Revision History

MONTH YEAR	Summary of Changes
January 2025	The First Edition

CONTEC CO., LTD. 3-9-31, Himesato, Nishiyodogawa-ku, Osaka 555-0025, Japan

https://www.contec.com/

FXA3020-US Reference Manual

NAXXXX (LXXX) [01172025] January 2025 Edition