

PCWL-0500

PCWL-0510

Version 1.03

[USERS MANUAL]

PicoCELA Corporation

1	Introduction.....	4
1.1	precautions.....	4
1.2	Warning.	5
1.3	Prohibitions.....	5
1.4	Precautions Regarding Radio Waves.....	6
1.5	Security precautions.....	7
1.6	Definition of Terms	7
2	Packaging and product appearance and name	9
2.1	PCWL-0500 Package Contents.....	9
2.2	PCWL-0500 Product appearance and name.....	9
2.3	PCWL-0510 Package Contents.....	15
2.4	PCWL-0510 Product appearance and name.....	16
3	Mounting method	21
3.1	PCWL-0500 installation method.....	21
3.2	Antenna mounting direction for PCWL-0500.....	24
3.3	How to remove PCWL-0500	27
3.4	How to install PCWL-0510	28
	Mounting on a pole.....	29
	Wall Mounting Method	29
3.5	How to remove PCWL-0510	29
4	Installation method.....	30
	ステップ 1 : Prepare the necessary equipment.....	30
	ステップ 2 : Check the Internet connection.	30
	ステップ 3 : Temporarily install PCWL (parent unit/core) to connect to the Internet	31
	ステップ 4 : Temporarily install PCWL(child/branch).....	37
	ステップ 5 : Check the link (connection) between parent and child.....	38
	ステップ 6 : Connect to the Internet with a Wi-Fi device.....	39
	ステップ 7 : Perform the main installation	40
	ステップ 8 : If you want to extend the area.....	40
5	About setting changes	41
6	How to operate PCWL's management screen	43
6.1	Screen header and footer icon operation	43
6.2	Help Screen Operation.....	44
7	Detailed settings of the monitoring system	45
7.1	Backhaul (relay line) settings	45
	Operation mode setting	45
	Wireless Setup.....	46
	Backhaul route update setting: at core setting	48
	Restoration settings in case of backhaul route failure: when core is configured	48
	Backhaul special settings.....	49
7.2	Network configuration: in router mode (parent unit/core only).....	53
	WAN-side network configuration: Eth-up port connection.....	53
	WAN-side network settings: PPPoE connection.....	54
	LAN-side network settings.....	55

DHCP Server Settings	55
7.3 Network settings: in bridge mode, in branch mode	57
LAN-side IP address setting	57
7.4 VLAN Settings	59
VLAN table settings	59
Default VLAN / Native VLAN (untagged)	59
VLAN ID and various settings	60
7.5 Router Function Configuration	66
Firewall Feature Configuration	66
Configure port forwarding functionality	67
7.6 Access Point Settings	69
5GHz/2.4GHz wireless configuration	69
SSID setting	71
SSID settings: General settings (name, security settings related, etc.)	71
SSID setting: Radius setting	73
SSID setting: VLAN setting	75
SSID setting: MAC address filtering setting	75
Common AP Settings	77
7.7 system setup	78
System Log Settings	78
Time setting	79
Account Settings	79
8 Check status (operating condition)	81
8.1 system status	81
8.2 Network Status	82
8.3 Backhaul (relay line) status	82
8.4 access point status	84
8.5 Node access method via backhaul	84
9 diagnostic function	86
9.1 Network Throughput Measurement	86
ステップ 1 : Log in to the management screen of the device to be measured.	86
ステップ 2 : Designation of iperf3 client	88
ステップ 3 : Display of network throughput measurement results	89
9.2 Internet Speed Measurement	90
9.3 access point scan function	91
9.4 Confirmation of reachability	91
10 Maintenance Functions	92
10.1 Reboot equipment	92
10.2 Firmware update	92
10.3 initialization	93
10.4 Backhaul Maintenance	94
10.5 logging	94
11 Connection settings with PicoManager	95
11.1 PicoManager account registration and license registration	95

How to register an account.....	95
Account Verification.....	95
How to register a license.....	96
11.2 PicoManager Activation.....	99
auto-activation.....	99
Manual Activation Operation	100
12 Application Usage Settings.....	101
12.1 Shared File Server Settings	101
13 Building a Wireless LAN Area with PCWL: The Basics	102
13.1 BH and AP	102
13.2 Parent (core) and child (branch).....	102
13.3 Optimal route construction and rerouting.....	103
13.4 Network partitioning	104
13.5 Prospects.....	104
13.6 Importance of temporary installation.....	105
13.7 How to check the wireless status of the access line	105
13.8 How to check the wireless status of relay lines	106
13.9 IP network partitioning	107
14 Building a Wireless LAN Area with PCWL: Applications	107
14.1 About Channels	107
14.2 About DFS	108
High-speed DFS function	109
14.3 About Wired Backhaul	110
14.4 Forgot your login password?	110
15 Interconnection with PCWL-0400 series.....	111
15.1 PCWL Series Interconnection Specifications.....	111
15.2 Interconnection Limitations.....	112
PCWL-0400 firmware version limitations	112
802.11k (proximity AP reporting) roaming restrictions	112
Prohibition of 2.4GHz backhaul operation	112
Limitations of parent unit (core) redundant operation	113
Limitations of Fast DFS Operation	113
16 salient points.....	115
16.1 PCWL-0500 main specifications	115
16.1 PCWL-0510 main specifications	118

1 Introduction.

1.1 precautions

- ❗ The copyright of this manual belongs to our company. No part of this manual may be reproduced, reprinted, or redrafted in any form or by any means without the prior written consent of our company.
- ❗ Specifications, design, and other information in this manual are subject to change without notice for improvement and may differ in part from the product you purchased.
- ❗ While every effort has been made to ensure the accuracy of the contents of this manual, please contact us if you have any questions or if there are any errors or omissions.
- ❗ The PCWL-0500 is intended for use in general commercial environments and as indoor IT equipment. We will not be liable for any damage caused by using the PCWL-0500 in any other environment.
PCWL-0500 is not dustproof or drip-proof as expected for outdoor use.
- ❗ PCWL-0510 is dustproof and drip-proof equivalent to IP67 for outdoor use, but should not be used in an environment exposed to direct sunlight. The internal temperature may become very high relative to the ambient temperature, which may interfere with operation.
- ❗ Do not use the product for purposes that require a high level of safety, such as use in medical facilities or in systems that directly or indirectly involve human life.
- ❗ When the product is used in a system environment that requires higher reliability and safety than general, please take responsibility for safety design and adequate measures against failures and other defects.
- ❗ PCWL products are manufactured for use in Japan only. Use of PCWL products outside of Japan is at your own risk. We do not provide maintenance or technical support outside of Japan.
- ❗ PCWL products should be used in accordance with the methods described in this manual. In particular, pay close attention to the cautions and warnings and do not use the product in such a manner.
- ❗ We will repair or replace PCWL products under certain conditions, but we do not guarantee the loss or corruption of stored data.
- ❗ PCWL shall not be liable for any damages arising out of the transaction of PCWL products unless we have been intentionally or grossly negligent, and the maximum liability shall be limited to an amount equal to the purchase price of the product.
- ❗ If a PCWL Product has an unknown defect and we deem it necessary, we will repair the defect free of charge or replace it with an equivalent product, but we will not be liable for any damages based on such defect.
- ❗ This manual is based on the latest firmware version at the time of preparation. Please note that some items are not supported by older versions.

In the case of PCWL-0500 Firmware version: v1.0.4

1.2 Warning.

- ❗ Do not install PCWL products in areas that are constantly hot.
- ❗ Do not install inside electrical appliances or near equipment that is expected to generate heat.
- ❗ Do not modify, disassemble, or repair PCWL products yourself.
- ❗ PCWL products are inspected for dustproof and drip-proof tightness at the time of shipment; never disassemble PCWL5 series products, as the dustproof and drip-proof performance is not guaranteed.
- ❗ If abnormal sounds, smells, or smoke are detected, immediately unplug the PCWL5 series product from the power supply, then disconnect the power supply from the surrounding equipment.
- ❗ Do not drop or shock the PCWL product. If the product is dropped or impacted, unplug it immediately.
- ❗ If a liquid or foreign object gets inside the PCWL product, immediately unplug it from the power supply.
- ❗ Regarding AC adapters for optional PCWL products
 - ① Do not process, overheat, or repair.
 - ② Install the product so that it will not get caught in walls, shelves, etc.
 - ③ Do not pull or apply weight.
 - ④ Do not heat the product, for example, by bringing it close to a hot appliance.
 - ⑤ Be sure to hold the plug when unplugging the power supply.
 - ⑥ Use the cable in such a way that the cable connections, etc. are not extremely bent.
 - ⑦ Do not move the equipment while it is connected.
 - ⑧ Make sure the AC adapter is properly and completely plugged into the outlet.
 - ⑨ The AC adapter should be plugged into the DC jack of the main unit and securely attached.
 - ⑩ Never connect an AC adapter other than the one supplied with the PCWL product.
 - ⑪ The DC input of PCWL products is $12V \pm 5\%$.
- ❗ Avoid static electricity from the human body and other equipment.
- ❗ Do not snag or pull on the cables connected to the PCWL product.
- ❗ When disposing of PCWL products, please follow the guidance of your local government authorities.

1.3 Prohibitions

Do not store or install the product in the following places. Doing so may adversely affect the product or cause a fire.

- ▶ Locations where static electricity or strong magnetic fields are generated
- ▶ Where vibration occurs
- ▶ Wall surface that may fall due to insufficient installation strength
- ▶ Low in places where people pass by
- ▶ Direct sunlight
- ▶ Around fire or equipment that emits hot air, or in places where hot air can accumulate
- ▶ Locations where there is a risk of electrical leakage or water leakage

1.4 Precautions Regarding Radio Waves

PCWL products have received technical standards conformity certification as radio equipment for low-power data communication system radio stations based on the Radio Law. Therefore, a radio station license is not required to use this product. PCWL products are intended for use in Japan. Please contact us for the technical standards conformity certification of each country in which the product is to be used overseas at your own risk.

- ❗ PCWL products have been certified for technical standards compliance, so disassembly, modification, or removal of the certification label is prohibited.
- ❗ IEEE802.11a/n/ac/ax W52 and W53 are prohibited for outdoor use by Japanese radio law.
- ❗ Application for registration station is required to use the 4.9GHz band. PCWL-0500 cannot use 4.9GHz band, please use PCWL-0510 when using 4.9GHz band.
- ❗ When using PCWL-0510 with the optional directional antenna (model name: PCAT-1115), be sure to specify "directional" as the antenna type. When connecting the directional antenna to the access side, specify the antenna type for the access side; when connecting to the backhaul side, specify the antenna type for the backhaul side. If a directional antenna is connected and used with "Standard" selected, it will not comply with the Radio Law.
- ❗ Since this product is compatible with IEEE802.11b/g/n/ax, do not use it near microwave ovens or near objects using radio waves in the vicinity of 2.4 GHz.
- ❗ The radio channels of IEEE802.11b/g/n/ax (2.4 GHz band) compatible products are used by some industrial, scientific and medical equipment, premises radio stations and specified low power radio stations.
- ❗ Note that IEEE802.11b/g/n/ax (2.4 GHz band) may cause radio interference with the aforementioned devices and radio stations, so be sure that they are not operating nearby.
- ❗ When 5GHz band (W53, W56) of IEEE802.11a/n/ac/ax is selected, communication may be temporarily interrupted by the DFS function to avoid interference from weather radar, etc. PCWL products have greatly improved the interruption time compared to previous models. However,

when radar waves are detected simultaneously on multiple channels, the interruption time may be as long as one minute.

- ❗ The communication speed nominalized in the IEEE802.11a/b/g/n/ac/ax standard is the maximum speed in the standard that connects wireless devices. Actual communication speeds will vary depending on the device (wireless terminal, etc.), environment, and usage conditions. Please note that the speeds quoted are not guaranteed.

1.5 Security precautions

Wireless LAN uses radio waves to connect PCs and other terminal devices to wireless access points (hereinafter referred to as "APs") to exchange information, making it much more convenient than a wired connection using LAN cables, and enabling network connections anywhere within range of radio waves. Network connection is possible anywhere within the range of radio waves.

On the other hand, if the network can be connected as long as the signal is within range, there is a risk of the following problems if security settings are not properly configured.

- ❗ The contents of communications may be understood. A malicious third party may intentionally intercept radio waves and view the contents of communications, including personal information and e-mail content.
- ❗ There is a risk of unauthorized intrusion. A malicious third party may access the network without authorization and steal personal or confidential information. There is also the risk of unauthorized information being transmitted through spoofing. Furthermore, intercepted data may be falsified and distributed, or viruses may be introduced.

The AP feature of PCWL products has a security system to address these issues. Security risks can be avoided by properly configuring and using security-related settings.

Since the security settings of the device may not be appropriate for your environment by default, please be sure to make the correct settings by yourself before using the device as an AP to avoid security problems. Please be aware that security settings may be broken by unknown means.

Please note that we are not responsible for any damages caused by such problems with the specifications of wireless communication, regardless of whether or not security settings have been configured.

1.6 Definition of Terms

terminology	Definition.
node	PCWL mainframe.
Parent Unit/Core	Node connected to the router using a LAN cable

Subsidiary/Branch	Core node or a node that is relay-connected to other nodes via PicoCELA Wi-Fi mesh
back hole	PicoCELA Wi-Fi mesh network/network relaying each node
rerouting	Backhaul optimal path reconstruction or its operation
STA/Station	General term for PCs, smartphones, and other terminals
PicoManager	Cloud services provided by PicoCELA Service that allows remote operation and management of node monitoring, diagnostics, configuration, etc.

2 Packaging and product appearance and name

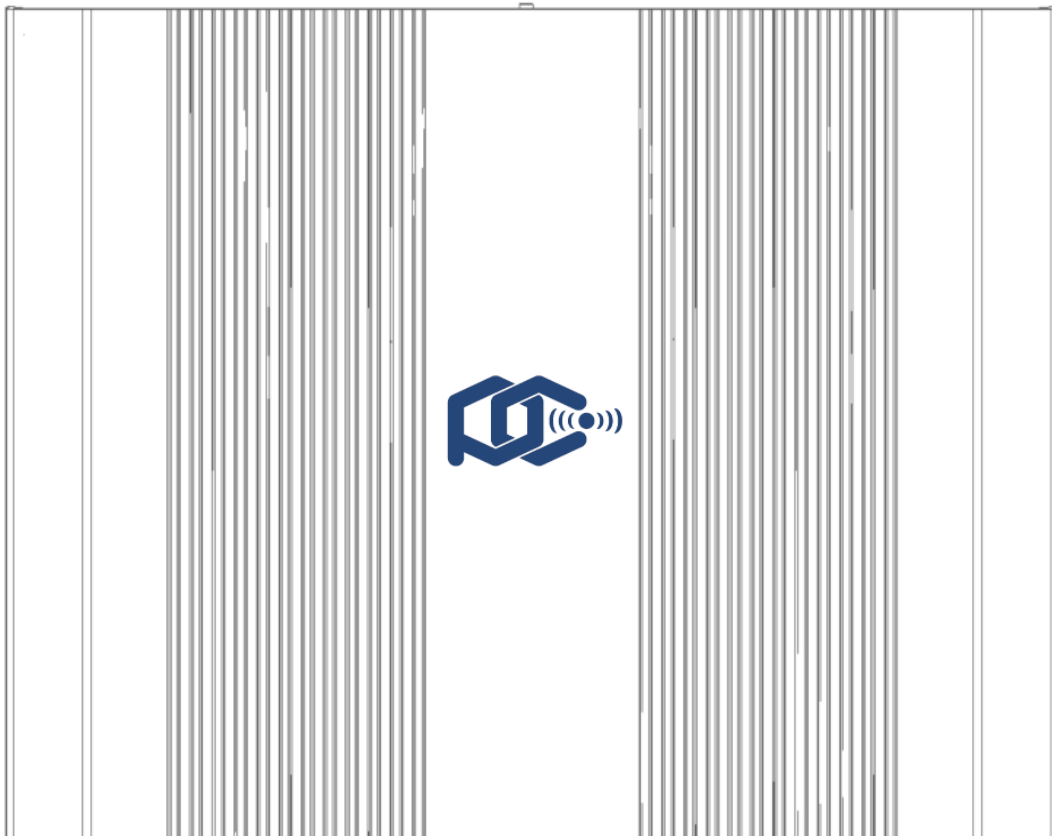
Thank you for purchasing this product. Before using this product, please check the package contents. If any item is missing, please contact your dealer or us.

2.1 PCWL-0500 Package Contents

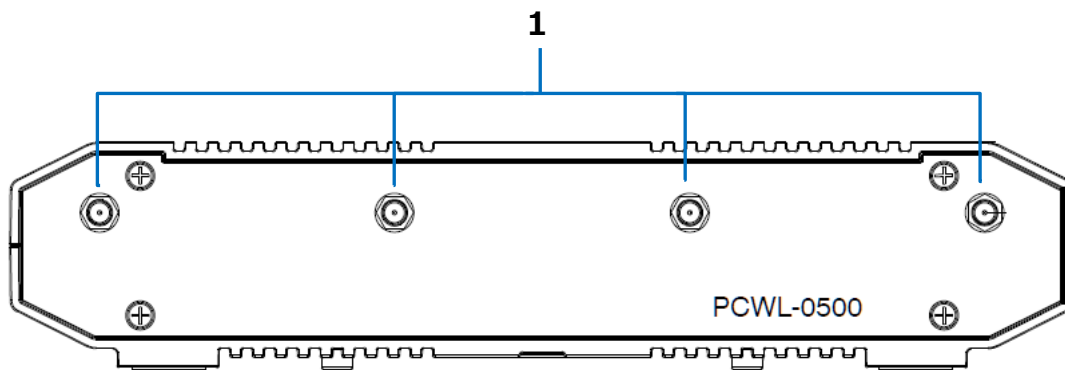
	name of product	volume
1	PCWL-0500 main unit	1
2	Antenna for backhaul line/access line	8
4	Antenna for Bluetooth (antenna with BT notation)	1
5	Antenna for Radar Scanning (antenna with RDR notation)	1
6	Attachment for mounting	1
7	safety precautions	1
8	PCWL-0500 Welcome Card	1

2.2 PCWL-0500 Product appearance and name

<Top case

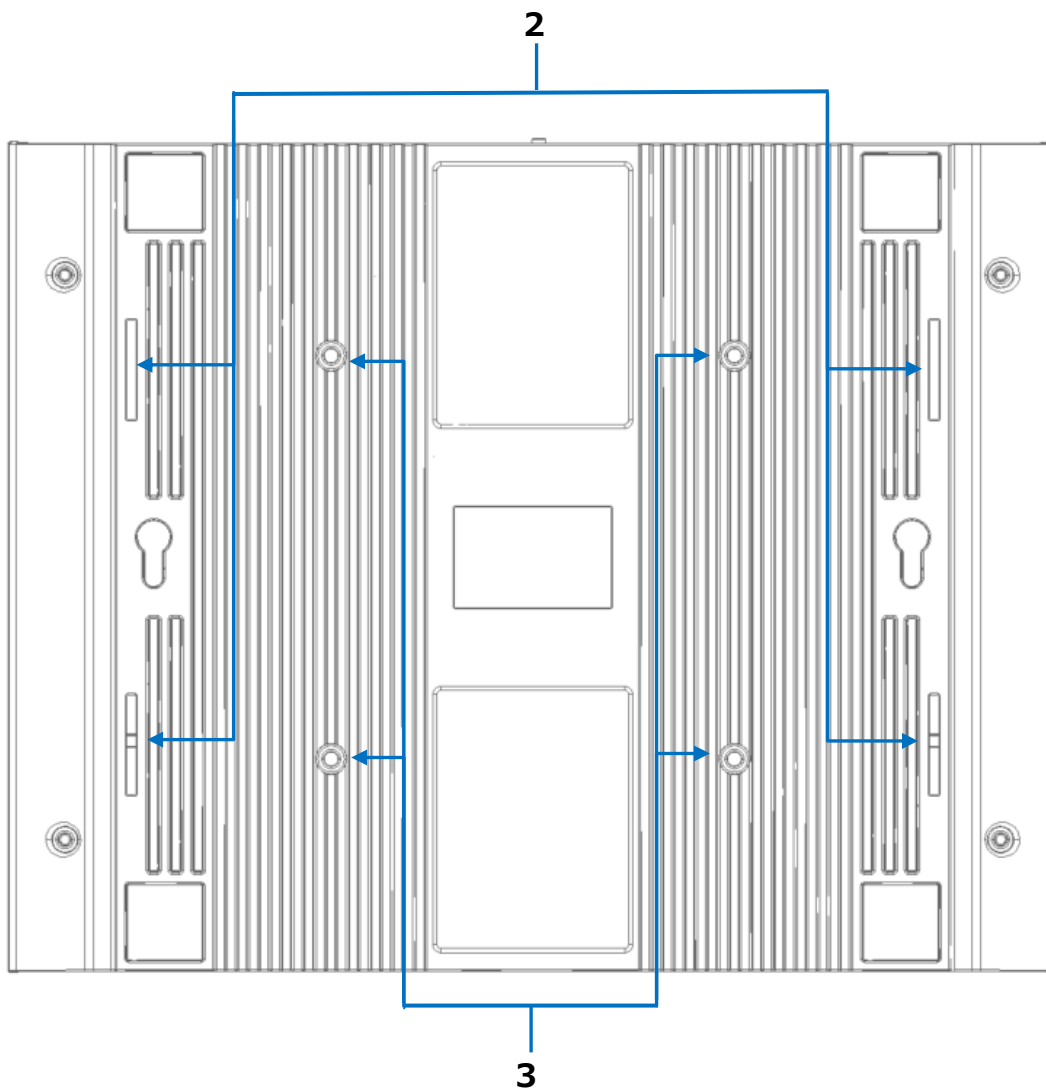


<Front panel

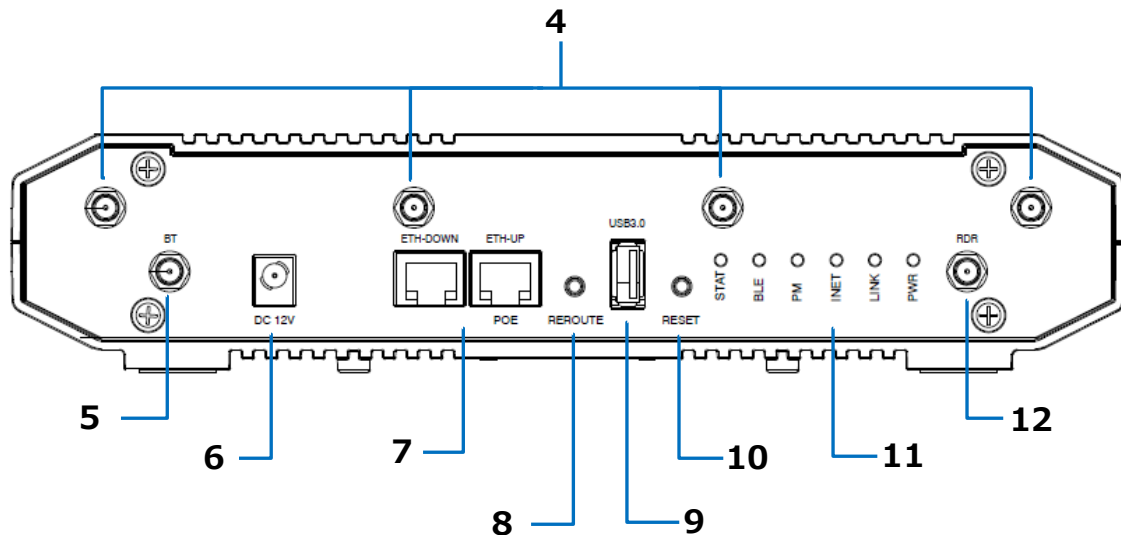


- ① Back hole side antenna terminal. Attach the supplied Wi-Fi antenna. Attaching an antenna other than the supplied one or the one specified by us may violate the Radio Law.

<Bottom case



- ② Slit for mounting panel
③ Mounting screw holes for VESA mount



④ Access side antenna terminal

Antenna terminal on the access line side. Use the supplied antenna or the antenna specified by us. Attaching an antenna other than the one specified by our company may violate the Radio Law.

⑤ Antenna terminal for Bluetooth

This is the antenna terminal for Bluetooth. Do not install any antenna other than the supplied one as it may violate the Radio Law.

⑥ DC input

Power supply terminal using AC adapter; use our optional AC adapter.

DC input: 12V±5

⑦ LAN terminal (RJ45)

Eth-up terminal : The parent unit is connected to the upper-level Internet line with a LAN cable.

The child unit is connected to the upper node with a LAN cable during wired backhaul construction.

To feed power to the main unit via POE, connect to the Eth-up terminal.

Eth-down terminal: Connects to a PC for accessing the monitoring system's management screen.

Connects to lower-side nodes with a LAN cable when constructing a wired backhaul.

When connecting an external device such as a network camera to this unit via LAN cable, connect it to the Eth-down terminal.

I will do so.

⑧ Reroute Switch

When the Reroute switch is pressed, the backhaul route is constructed. It is also used to check the signal strength of the backhaul line at the location where the equipment is installed or to intentionally reconstruct the route.

⑨ USB 3.0 terminal

USB3.0 compatible devices such as USB memory sticks and surveillance cameras can be connected.

⑩ Reset switch

This switch is used to reset the unit.

Please note that a long press for more than 10 seconds will return all settings to factory defaults. If you have forgotten your login ID or password or wish to return to the default settings, press and hold for more than 10 seconds.

⑪ Status indicator lamp

PWR PWR: Displays power supply status and source of power supply

LINK LINK: Displays backhaul connection status and connection radio wave strength

INET INET: Displays the status of the connection to the Internet

PM: PicoManager Activation Status and Connection Status PicoManager: Displays

PicoManager activation status and connection status

BLE BLE: Display the status of the BLE scan function.

STAT STAT: Displays the backhaul operation mode of the monitoring system

(core/branch/wired backhaul)

name	lighting conditions	Operational status of the monitoring system
PWR	switching off the light	No power supply
	Orange light	When powered by DC12V *When powered by AC adapter of optional product
	Red light	When POE is supplied *When operating by receiving PoE power from the Eth-up port
LINK	switching off the light	In branch mode: When backhaul route construction is not completed
	Flashing for 2 seconds (each color)	At device startup In branch mode: After constructing a backhaul route during rerouting, the backhaul route blinks for 2 seconds in a color corresponding to the RSSI level.
	High-speed flashing (each color)	Fast flashing RSSI level color while the branch node is searching for backhaul channels
	Slow blinking (each color)	When CAC is required due to radar wave detection, it blinks at low speed in a color corresponding to the RSSI level
	Red light	In branch mode: When backhaul is connected and RSSI level is less than -65 dBm
	Yellow light	In branch mode: Backhaul connected and RSSI levels below -55 dBm and above -65 dBm
	Green light	In branch mode: Backhaul is connected and RSSI level is less than -45 dBm and greater than 55 dBm
	Blue light	In core mode

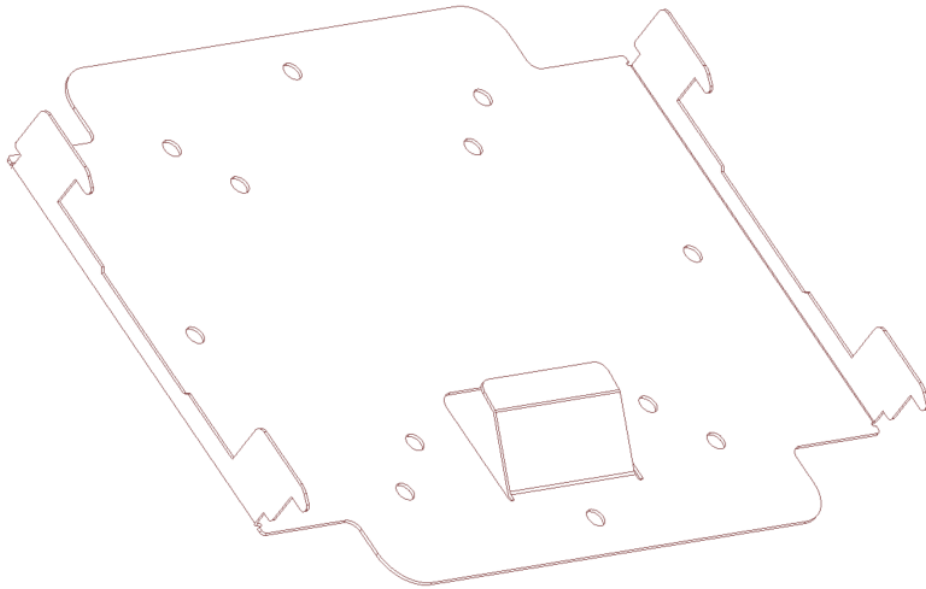
		In branch mode: when backhaul is connected and RSSI level is above -45 dBm or when wired backhaul is connected
INET	switching off the light	When communication with the external Internet is not possible
	Orange light	If communication with the external Internet is possible
afternoon	switching off the light	Before activation
	Orange high-speed blinking	When auto-activation is performed
	Slow blinking orange	Activation completed, PicoManager connection process in progress (unconnected)
	Orange light	Communication with PicoManager is established.
BLE	switching off the light	When BLE data collection of the monitoring system is disabled
	Green light	When the monitoring system's BLE data collection is enabled
STAT	switching off the light	-
	Yellow light	When the operation mode of the monitoring system is the parent unit (core)
	Green light	When the operation mode of the monitoring system is child (branch)
	Light blue light	Operating in wired backhaul (branch only)

⑫ Antenna terminal for radar scan

Antenna terminal for radar scanning for high-speed DFS; install the supplied antenna labeled RDR.

Do not install any antenna other than the supplied one as it may violate the Radio Law.

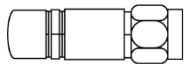
<Mounting plate



<Backhaul/Access side antenna



<Antenna for BT/Radar Scan



The antenna for BT is compatible with 2.4 GHz and the antenna for Radar Scan is compatible with 5 GHz. Be sure to use the specified antenna(s) as antenna(s).

Connect the antenna to the antenna terminal. Performance cannot be guaranteed if the wrong antenna is connected.

BT" and "RDR" are printed on the antenna, so please check when installing.

2.3 PCWL-0510 Package Contents

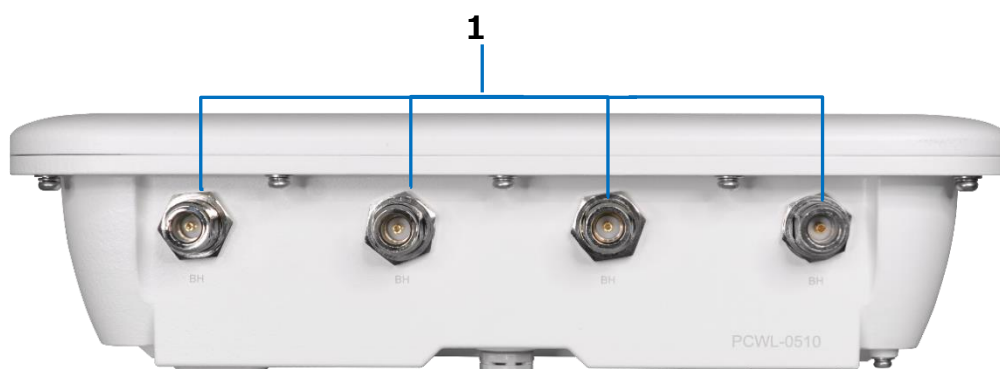
	name of product	volume
1	PCWL-0510 main unit	1
2	Backhaul line antenna	4
3	Antenna for access line	4
4	Antenna for Bluetooth (antenna with BT notation)	1
5	Antenna for Radar Scanning (antenna with RDR notation)	1
6	safety precautions	1
7	PCWL-0510 Welcome Card	1
8	Attachments for wall mounting: quantity in parentheses RJ45 waterproof connector (2) M8 x 100 screws (2) M8 x 35 screws (4) M8 spring washer - (4) M8 washer - (4) M8 nuts (4) M6 x 14 screws (4) Mounting brackets (1) Anchor screws (4) Plastic anchors (4)	

2.4 PCWL-0510 Product appearance and name

<Top panel

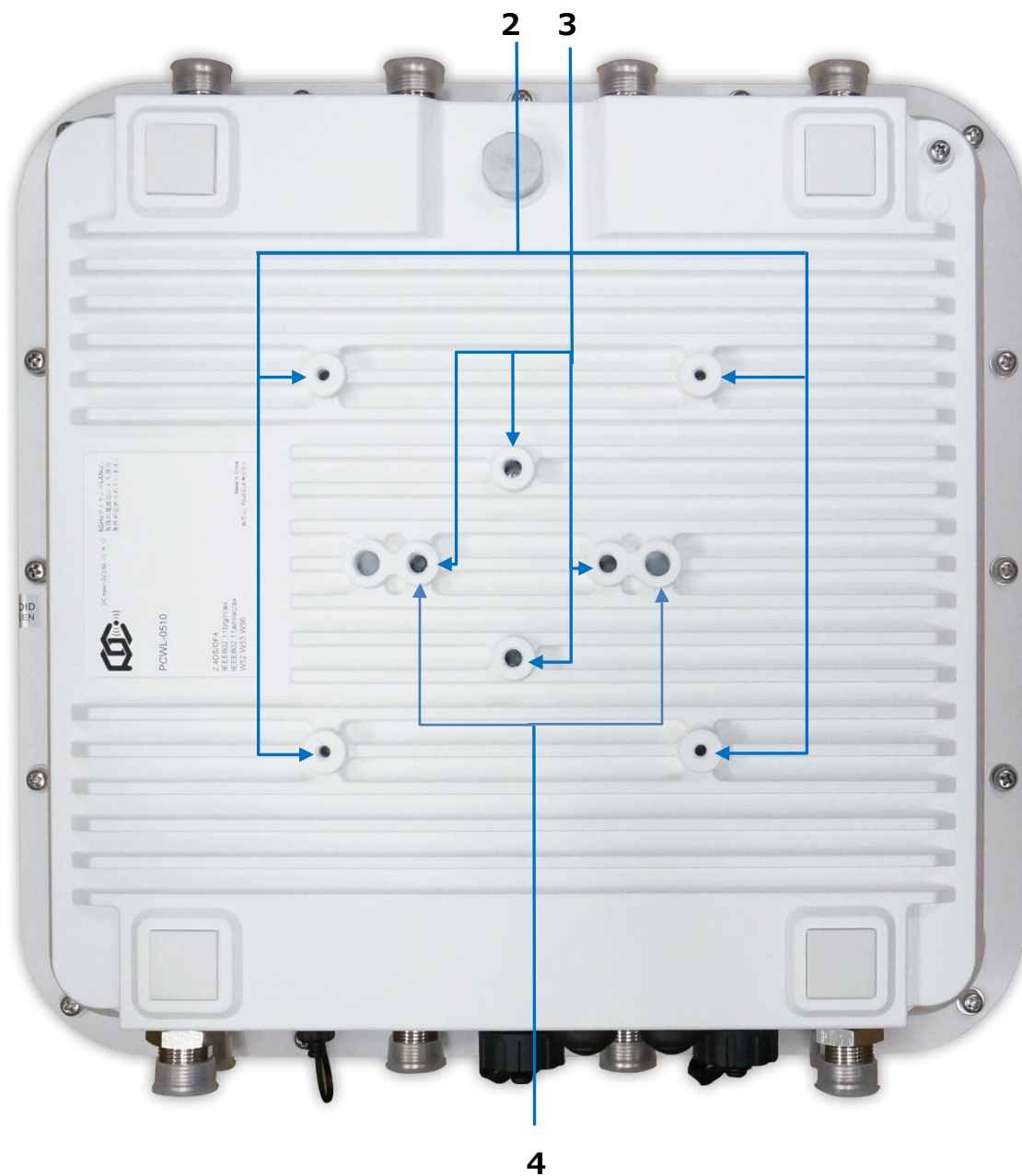


<Front panel



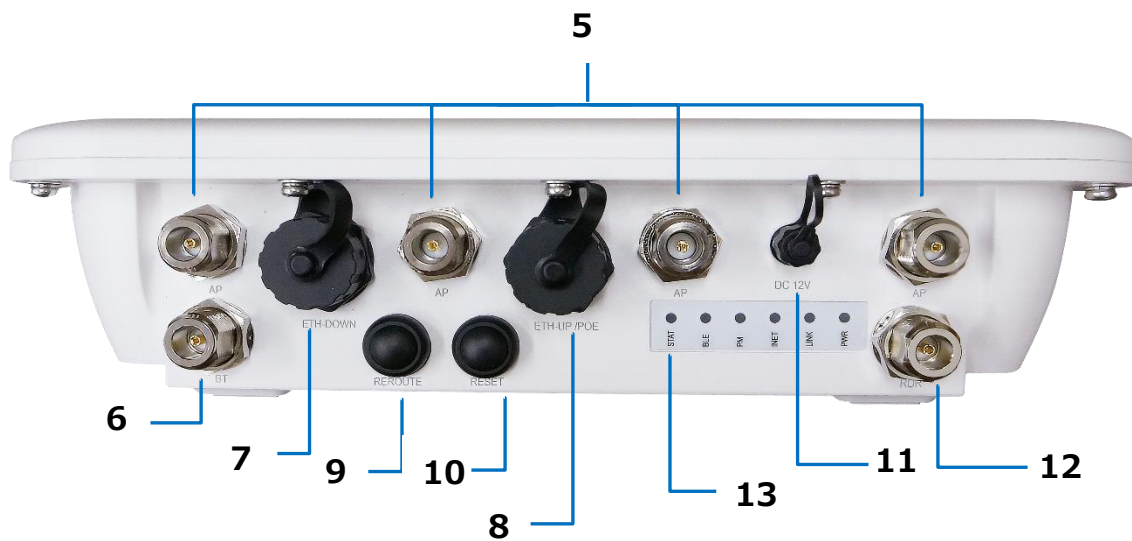
- ① Antenna terminal for backhaul side. Attach the supplied antenna for the backhaul (BH). Attaching an antenna other than the supplied one or the one specified by us may violate the Radio Law.

<Bottom panel



- ② Mounting screw holes for VESA mount
These are screw holes for mounting VESA (100x100) brackets.
- ③ Screw holes for included mounting hardware
These are screw holes for attaching the included mounting hardware to the main unit.
- ④ Screw holes for general mounting hardware
These are screw holes for attaching the mounting bracket of the Pole Clamp/PCWL-0410.

<Bottom panel



⑤ Access side antenna terminal

Antenna terminal on the access line side. Use the supplied antenna or our specified antenna. Attaching antennas other than those specified by us may violate the Radio Law.

⑥ Antenna terminal for Bluetooth

Antenna terminal for Bluetooth. Do not install any antenna other than the supplied one as it may violate the Radio Law.

⑦ Eth-up terminal (RJ45)

The parent unit is connected to the upper-level Internet connection with a LAN cable. The child unit is connected to the upper node with a LAN cable during wired backhaul construction.

When supplying power to the main unit via POE, connect to the Eth-up terminal

⑧ Eth-down terminal (RJ45)

Connects to a PC when accessing the monitoring system's management screen.

Connects to lower-side nodes with a LAN cable when constructing a wired backhaul.

When connecting an external device such as a network camera to this unit with a LAN cable, etc., also connect it to the Eth-down terminal.

⑨ Reroute Switch

When the Reroute switch is pressed, a backhaul route is constructed. Also, the location of the equipment

Used to check the signal strength of the backhaul line or to intentionally reconfigure the route.

⑩ Reset switch

This switch is used to reset the unit.

Note that a long press for more than 10 seconds will return all settings to factory defaults.

If you forget your login ID or password or want to return to the initial state, press and hold for more than 10 seconds.

Please do so.

⑪ DC input

Power supply terminal using AC adapter; use our optional AC adapter.

DC input: 12V±5

⑫ Antenna terminal for radar scan

Antenna terminal for radar scanning for high-speed DFS; install the supplied antenna labeled RDR.

Do not install any antenna other than the supplied one as it may violate the Radio Law.

⑬ Status indicator lamp

PWR PWR: Displays power supply status and source of power supply

LINK LINK: Displays backhaul connection status and connection radio wave strength

INET INET: Displays the status of the connection to the Internet

PM: PicoManager Activation Status and Connection Status PicoManager: Displays

PicoManager activation status and connection status

BLE BLE: Display the status of the BLE scan function.

STAT STAT: Displays the backhaul operation mode of the monitoring system

(core/branch/wired backhaul)

name	lighting conditions	Operational status of the monitoring system
PWR	switching off the light	No power supply
	Orange light	When powered by DC12V *When powered by AC adapter of optional product
	Red light	When POE is supplied *When operating by receiving PoE power from the Eth-up port
LINK	switching off the light	In branch mode: When backhaul route construction is not completed
	Flashing for 2 seconds (each color)	At device startup In branch mode: After constructing a backhaul route when rerouting is executed, the backhaul route is displayed blinking in a color corresponding to the RSSI level for 2 seconds.
	High-speed flashing (each color)	Fast flashing RSSI level color while the branch node is searching for backhaul channels
	Slow blinking (each color)	When CAC is required due to radar wave detection, it blinks at low speed in a color corresponding to the RSSI level
	Red light	In branch mode: When backhaul is connected and RSSI level is less than -65 dBm
	Yellow light	In branch mode: Backhaul is connected and RSSI level is below -55 dBm and above -65 dBm

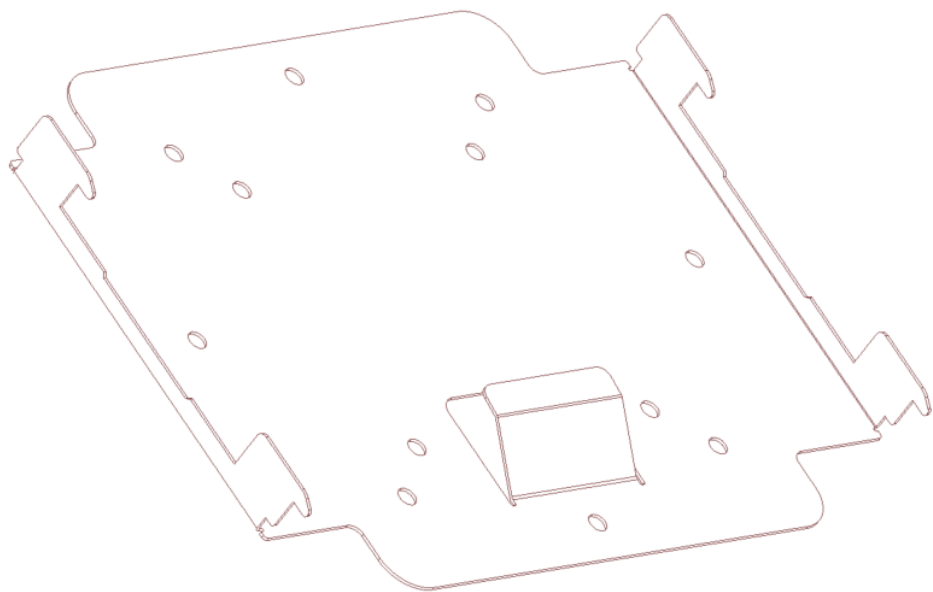
	Green light	In branch mode: Backhaul is connected and RSSI level is less than -45 dBm and greater than 55 dBm
	Blue light	In core mode In branch mode: when backhaul is connected and RSSI level is less than -45 dBm or when wired backhaul is connected
INET	switching off the light	When communication with the external Internet is not possible
	Orange light	If communication with the external Internet is possible
afternoon	switching off the light	Before activation
	Orange high-speed blinking	When auto-activation is performed
	Slow blinking orange	Activation completed, PicoManager connection process in progress (not connected)
	Orange light	Communication with PicoManager is established.
BLE	switching off the light	When BLE data collection of the monitoring system is disabled
	Green light	When the monitoring system's BLE data collection is enabled
STAT	switching off the light	-
	Yellow light	When the operation mode of the monitoring system is the parent unit (core)
	Green light	When the operation mode of the monitoring system is child (branch)
	Light blue light	Operating in wired backhaul (branch only)

⑫ Antenna terminal for radar scan

Antenna terminal for radar scanning for high-speed DFS; install the supplied antenna labeled RDR.

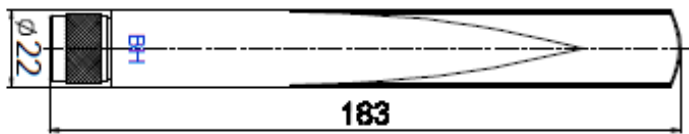
Do not install any antenna other than the supplied one as it may violate the Radio Law.

<Mounting bracket



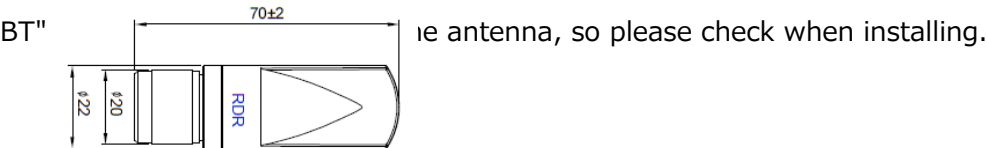
<Backhaul/Antenna for access

Backhaul antennas support 4.9 GHz and 5 GHz, and access antennas support 2.4 GHz.
Be sure to connect the specified antenna to the antenna terminal. If the wrong antenna is connected Performance cannot be guaranteed.
BH" (for backhaul) and "AP" (for access) are printed on the antenna.



<Antenna for BT/Radar Scan

The antenna for BT is compatible with 2.4 GHz and the antenna for Radar Scan is compatible with 5 GHz. Be sure to use the specified antenna(s) as antenna(s).
Connect the antenna to the antenna terminal. Performance cannot be guaranteed if the wrong antenna is connected.

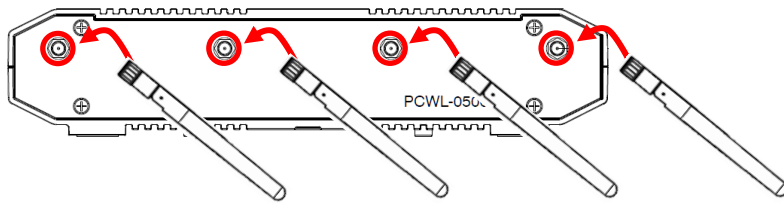


3 Mounting method

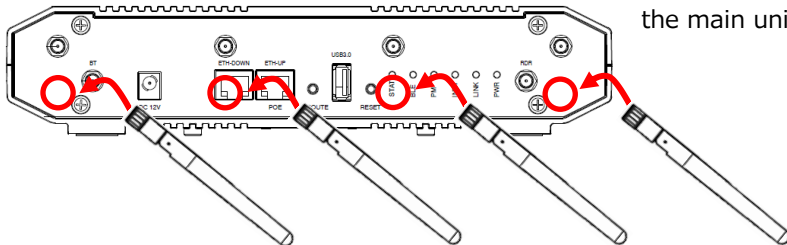
3.1 PCWL-0500 installation method

PCWL-0500 installation instructions are described.

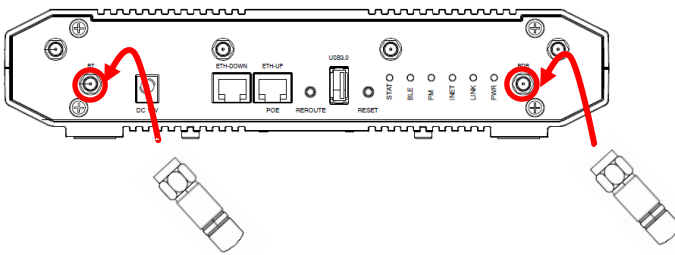
- ① Attach the antenna for the relay line. Attach it to the antenna connection terminal on the upper front panel of the main unit.



- ② Attach the antenna for the access line. Attach it to the antenna connection terminal at the top of the side of the main unit.



- ③ Attach the antennas for Bluetooth (BT terminal) and for radar scan (RDR terminal). Attach the antenna marked "BT" to the BT terminal and the antenna marked "RDR" to the RDR terminal.

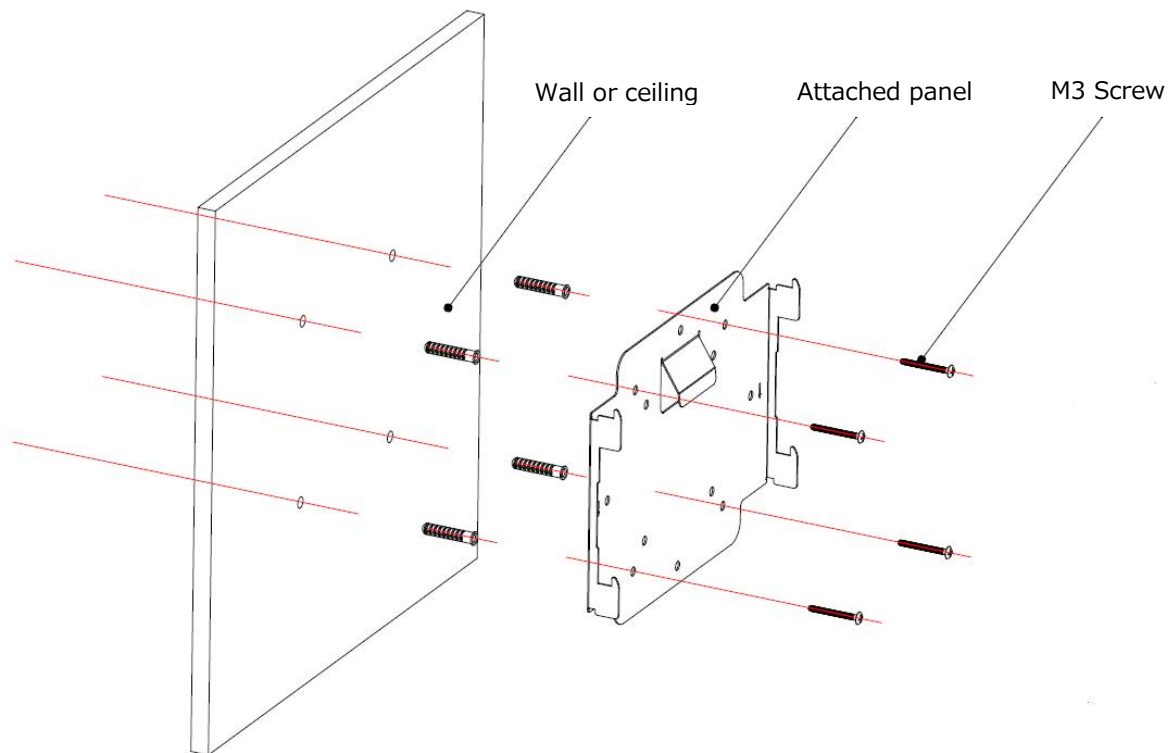


- ④ Attach the supplied panel to the wall or ceiling, then install the main unit on the panel.

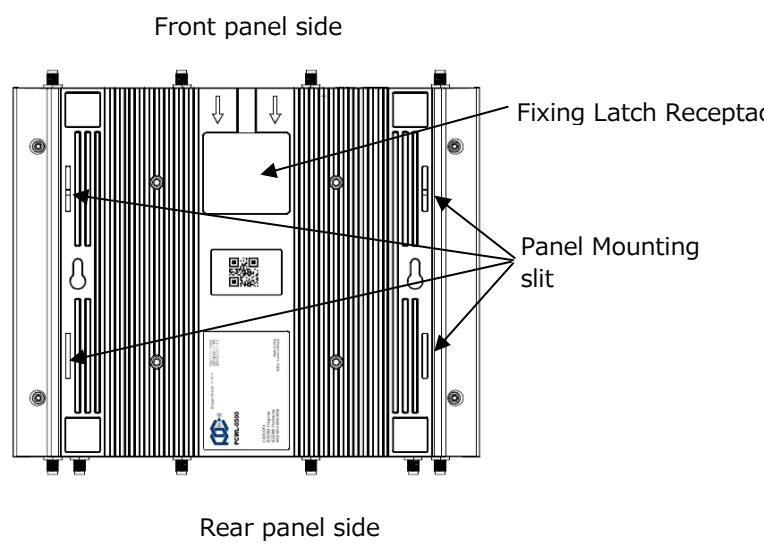
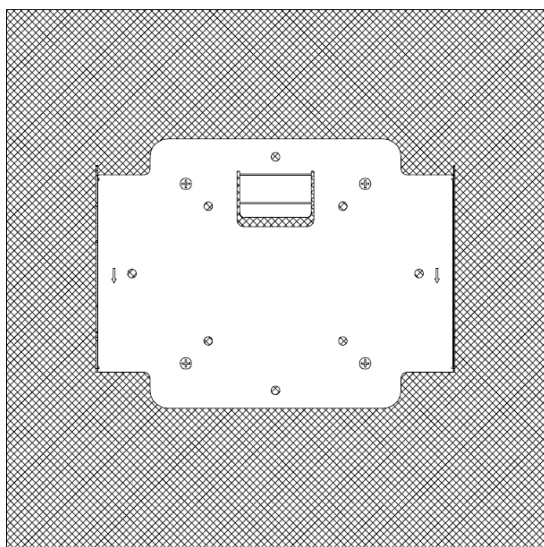
Install the supplied panels on the wall or ceiling.

*Please prepare anchors and screws of the appropriate standard for the material of the walls and ceilings where they will be installed.

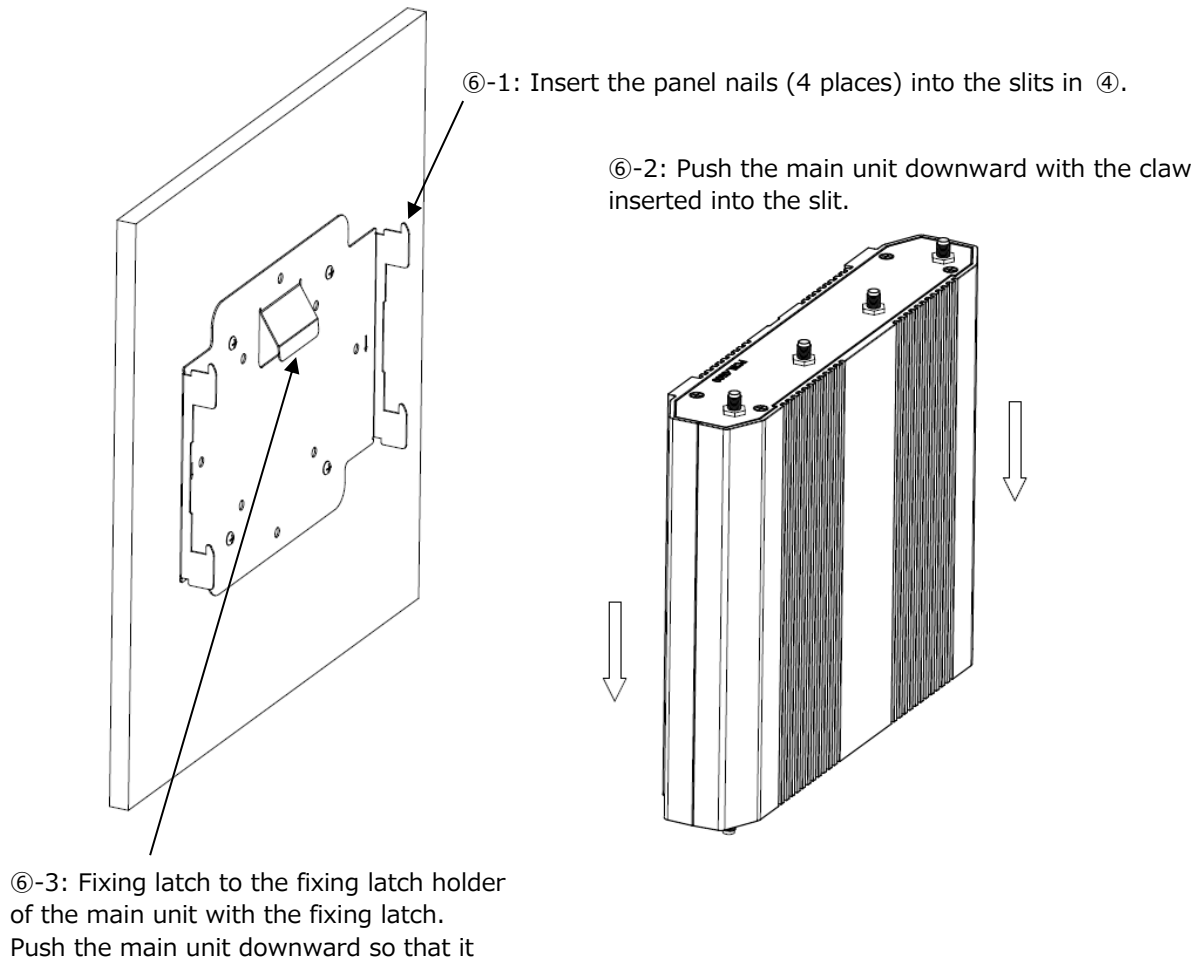
The weight of the main unit with the antenna attached is approximately 2.0 kg.



- ⑤ The mounting orientation of the panel and main unit is as follows



- ⑥ Insert the panel's pawl into the slit in the body, push the body downward, and secure it firmly with the fixing latch.

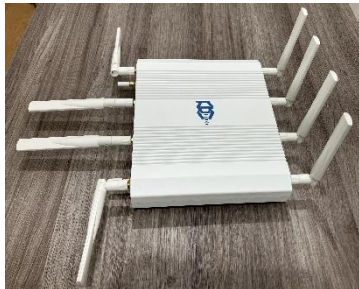
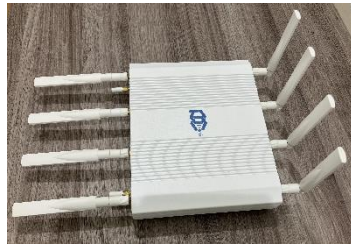


3.2 Antenna mounting direction for PCWL-0500

The PCWL-0500 attached antenna is an omni antenna. The HPBW (Half Power Beam Width) of the attached antenna radiates radio waves horizontally in all directions of 360 degrees, vertically in 50 degrees for 2.4 GHz and 25 degrees for 5 GHz. Depending on the mounting direction of the backhaul antenna and the access antenna, radio interference may occur, resulting in significant degradation of communication quality and performance. When installing the antennas, use the backhaul antenna and the access antenna in a non-opposing relationship.

Recommended Antenna Orientation

Refer to the following pictures to ensure that the antennas on the backhaul side and the access side do not face each other.



The antennas are installed in a direction where none of the antennas on the backhaul side and the access side are opposite each other.

Deprecated antenna installation orientation

Do not install the antenna in the direction shown in the photo below, as this will cause radio interference and significantly degrade communication quality.



8 antennas facing each other



Four antennas facing each other



Four antennas facing each other

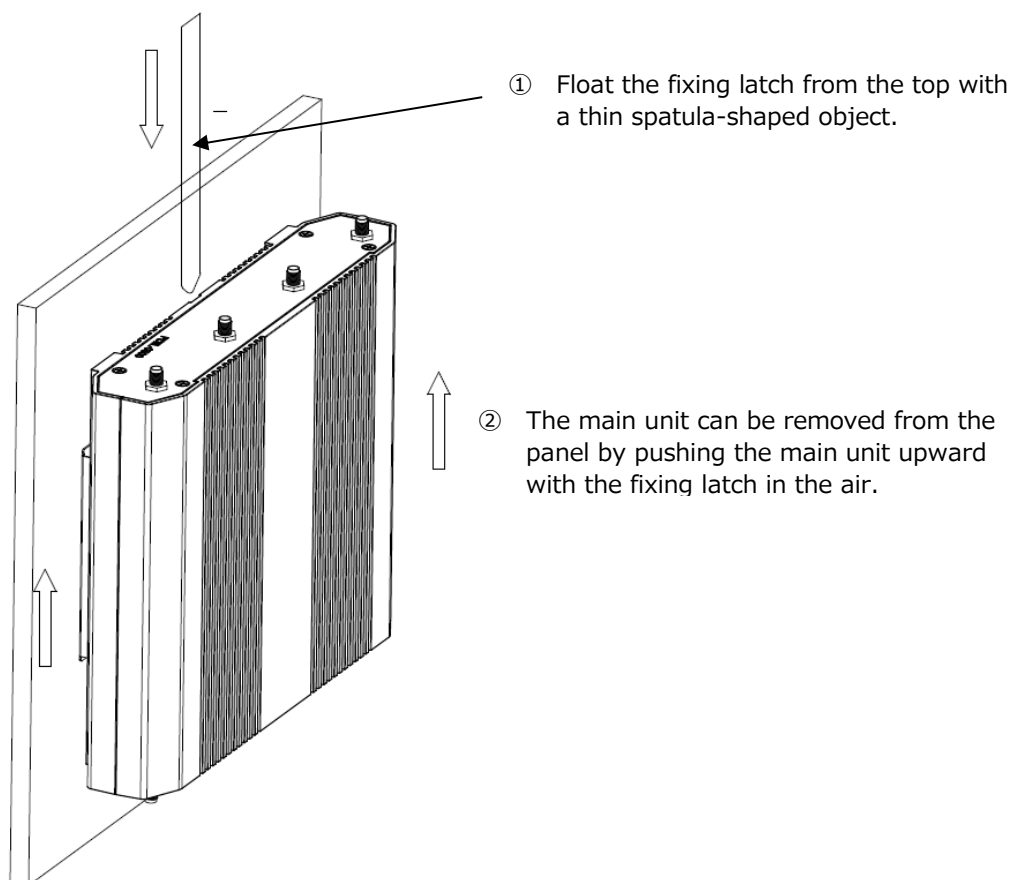


8 antennas facing each other

An installation where any of the antennas on the backhaul side and the access side are opposite each other.

3.3 How to remove PCWL-0500

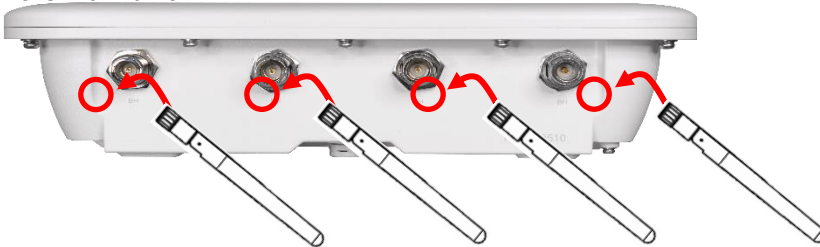
PCWL-0500 removal instructions are provided.



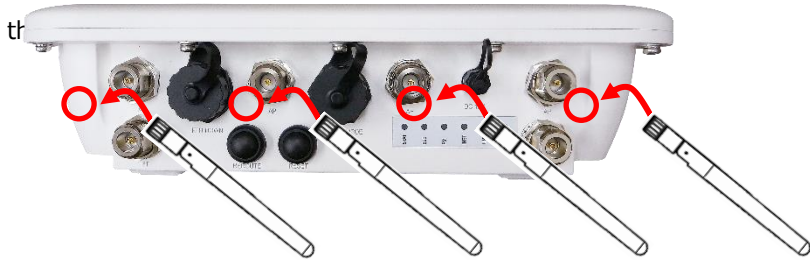
3.4 How to install PCWL-0510

PCWL-0500 installation instructions are described.

- ③ Attach the antenna for the relay line. Attach it to the antenna connection terminal on the upper front panel of the main unit.



- ④ Attach the antenna for the access line. Attach it to the antenna connection terminal at the top of the side of the main unit.



- ⑦ Attach the antennas for Bluetooth (BT terminal) and for radar scan (RDR terminal). Attach the antenna marked "BT" to the BT terminal and the antenna marked "RDR" to the RDR terminal.



- ⑧ Assemble the included mounting hardware.

- ⑨ Attach the supplied mounting brackets to the main unit, then install the mounting brackets on the wall or pole.

Install the supplied mounting brackets on the wall or pole.

*Please prepare anchors and screws of the appropriate standard for the material of the walls and ceilings where they will be installed.

The weight of the main unit with the antenna attached is approximately 3.6Kg.

This section describes how to mount the PCWL-0410 to a pole, wall, or camera tripod. Also described is how to install the RJ45 waterproof connector. The mounting bracket is made of steel, which may rust, but this will not affect the strength of the mounting (period of about 10 years) or the operation or performance of the equipment or antenna.

Mounting on a pole

Wall Mounting Method

3.5 How to remove PCWL-0510

PCWL-0510 removal instructions are provided.

4 Installation method

This section describes the installation procedure when the installation is performed with the factory default settings. If you wish to change the settings, please refer to "5 Changing Settings" below before installation.

ステップ 1 : Prepare the necessary equipment

☐ Internet connection environment

One LAN port for PCWL is required on the device connected to the Internet (router, hub, etc.).

☐ LAN cable 1 pc

A cable is required to connect PCWL to the Internet.

☐ PoE powered equipment or our optional AC adapter

When PCWL is powered by PoE power supply, a PoE power supply compatible device is required. Not required when powered by AC adapter (sold separately).

☐ PC with built-in wired LAN port

*If your PC

does not have a wired LAN port, use a USB-to-wired LAN adapter.

☐ PCs with built-in wireless LAN port or Wi-Fi enabled devices such as iPhone

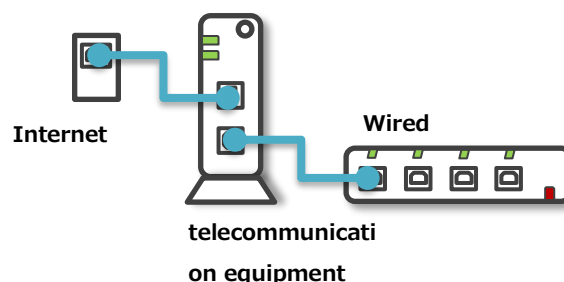
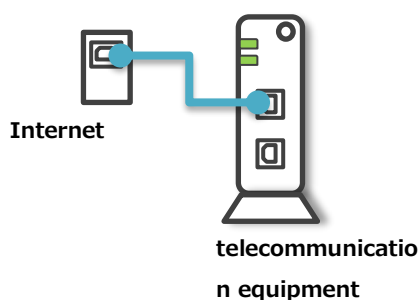
☐ Packing set

Device, 8 antennas for BH/AP, 2 antennas for BLE/Radar Scanning, attachment for installation

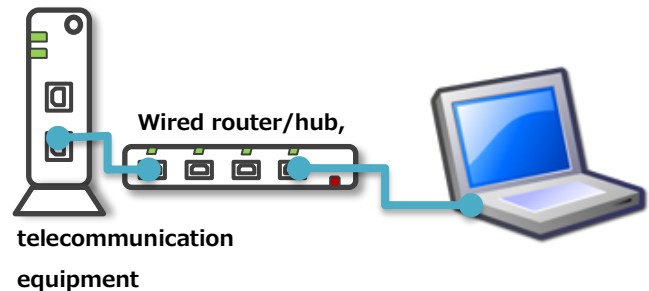
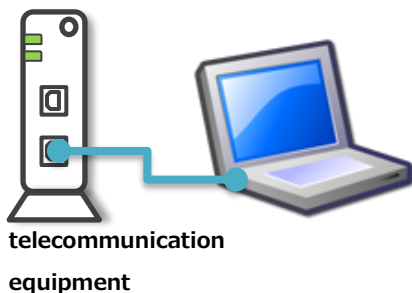
ステップ 2 : Check the Internet connection.

Beforehand, check to see if Internet access is available.

- ① Check to see if there is any communication equipment (e.g., modem) purchased or rented from the provider or line provider at the time of the Internet contract.



- ② Connect the communication device or wired router, etc. to the PC with a LAN cable.



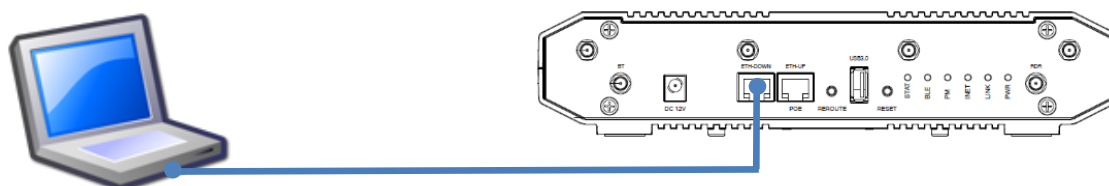
③ Check if you can connect to the Internet in this state.

Ex) For Windows PCs, check that the IP address is correct in "Local Area Connection" under "Network Connection" and that the Internet site can be displayed by launching a browser or other device.

④ Once the connection is confirmed, disconnect the LAN cable and proceed to the next step.

ステップ 3 : Temporarily install PCWL (parent unit/core) to connect to the Internet

1. If you have purchased only one PCWL, please use that PCWL as the parent unit (core); if you have purchased two or more PCWLs, please select any one PCWL as the parent unit (core).
2. Since the factory default setting is set to the child unit (branch), connect the main unit to a PC and change the setting to the parent unit (core) on the WEB UI screen by following the procedure from step 3 onward.
3. Connect the LAN terminal of the PC to the **Eth-down terminal of** PCWL (PCWL-0500 is used as an example) with a LAN cable, and connect the power supply to DC IN.



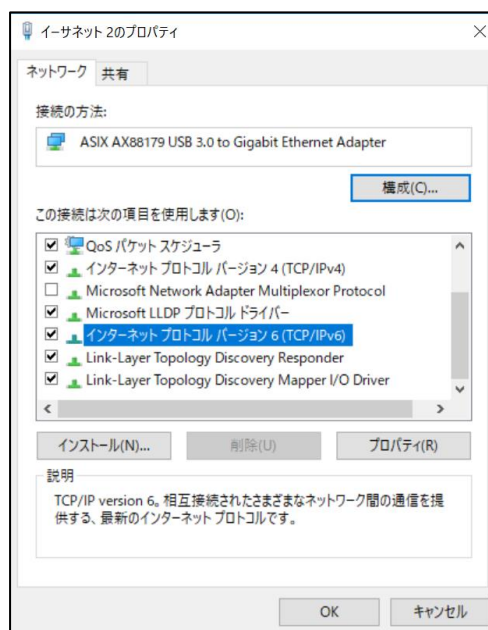
4. Set the IPv6 address of the PC to the following address
IPv6 address on PC side = FD00:5043::062B:BBFF:FEF0:XXXX
XXXX is an arbitrary value in hexadecimal (0 to F)
Subnet prefix length: 64

<Example of Window 10

- ① Open "Control Panel" ← "Network and Sharing Center" and select (click) the target "Ethernet". The following screen will appear and select "Properties".



- ② Select "Internet Protocol Version 6 (TCP/IPv6)" on the following screen and click "Properties".

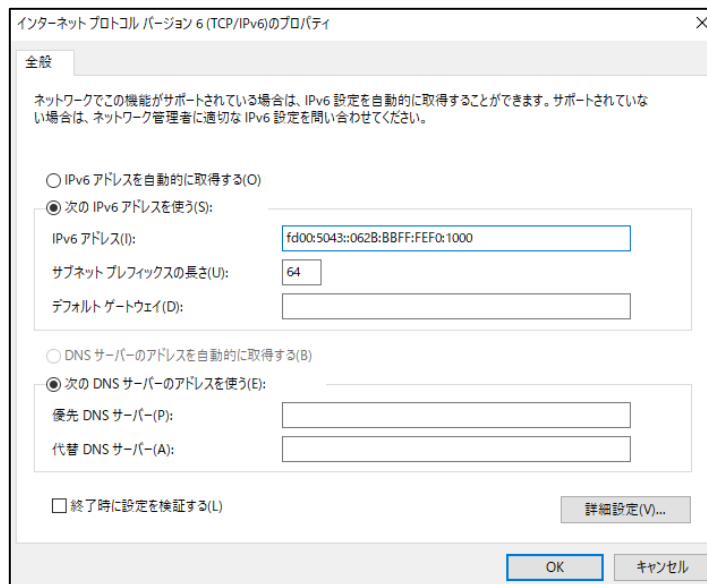


- ③ On the following screen, enter the PC's "IPv6 address" and "subnet prefix" and click "OK".

IPv6 address on PC side = FD00:5043::062B:BBFF:FEF0:XXXXX

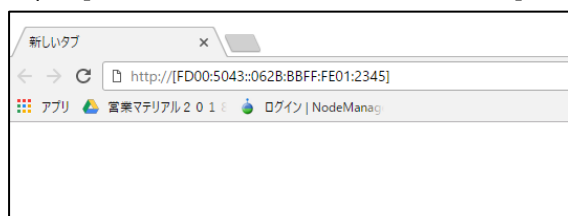
XXXX is an arbitrary value in hexadecimal (0-F) (1000 in the example below)

Length of subnet prefix: 64



- ④ Calculate the IPv6 address of PCWL according to the following rules.
- I. Check the MAC address affixed on the rear panel.
(Example.)
PCWL MAC address = 042BBB012345
 - II. Split the upper 3 bytes and lower 3 bytes of the MAC address.
042BBB (fixed) + 012345
 - III. Change the split upper "042BBB" to "062BBB" and insert "FFFE" between the upper and lower levels.
062BBB+FFFE+012345 = 062BBBFFFE012345
 - IV. Separate the above by ":" every 16 bits according to IPv6 address notation.
"062B:BBFF:FE01:2345" is the lower 64-bit address.
The upper 64 bits are fixed "FD00:5043:0000:0000".
These upper 64 bits + lower 64 bits are the IPv6 address (128 bits) of the PCWL-0500.
- (For example.)
PCWL IPv6 address = FD00:5043::062B:BBFF:FE01:2345
- ⑤ Start a PC browser (Google Chrome recommended), enter the PCWL IPv6 address converted in http://の後に
④, and access the PCWL WEB UI screen.

http://[FD00:5043::062B:BBFF:FE01:2345]



Recommended browsers: Google Chrome, Microsoft Edge, Firefox

- ⑥ When you access PCWL, you will see the following login screen.

Access will be available approximately 2 minutes after power-on.



The factory default user name is "admin" and the password is "picocela".

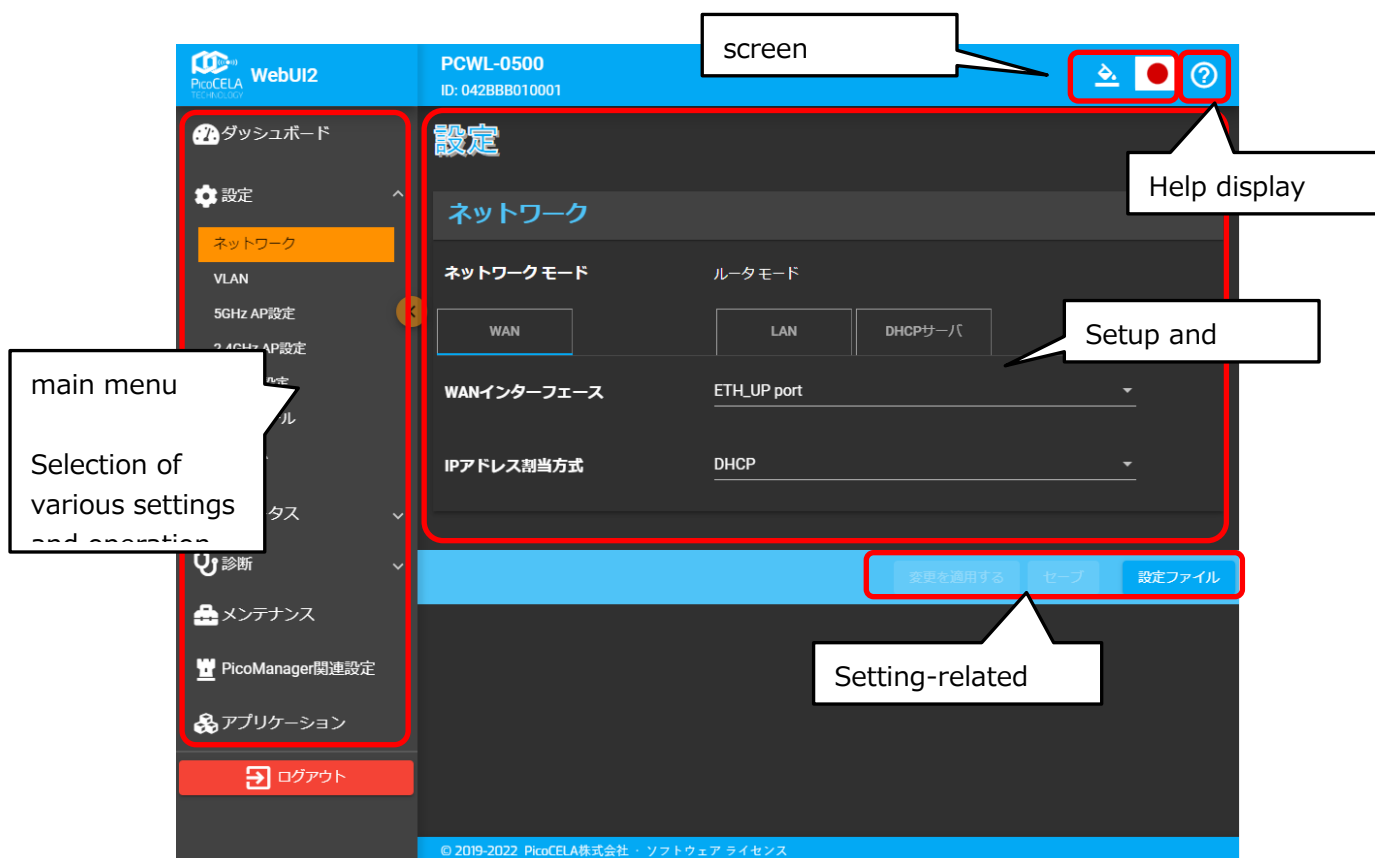
Enter the information as shown in the screen above and click the "Login" button.

*If the login screen does not appear, please check the connection status of the LAN cable, the IPv6 address setting of the PC, or the PCWL

Please check your IPv6 address settings.

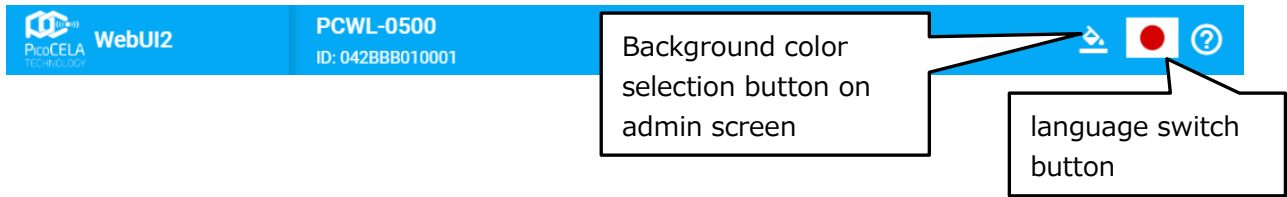
After successful login, you will be redirected to the top screen. You can choose a white or black background color for the administration screen.

This manual is explained on a black background screen.



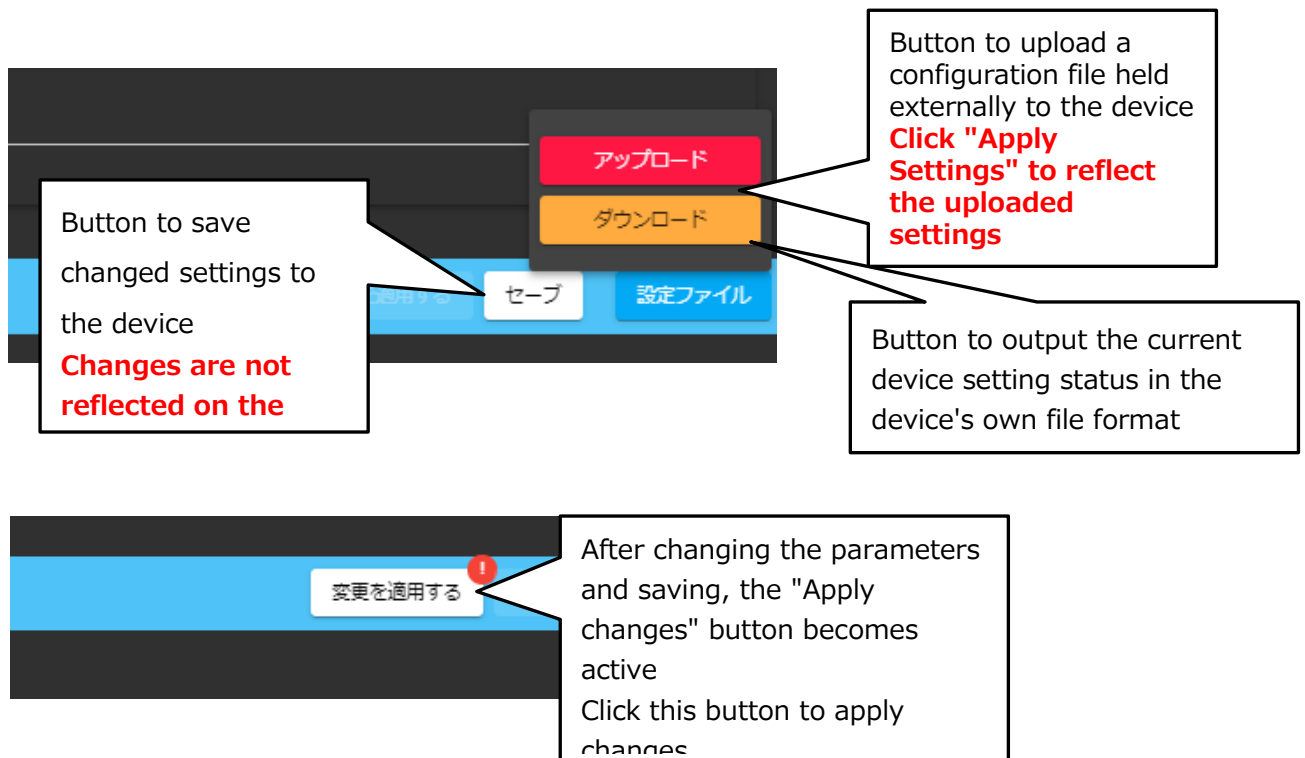
Each icon in the screen is explained below.

The icons in the header are placed with a button for switching the screen background color and language.

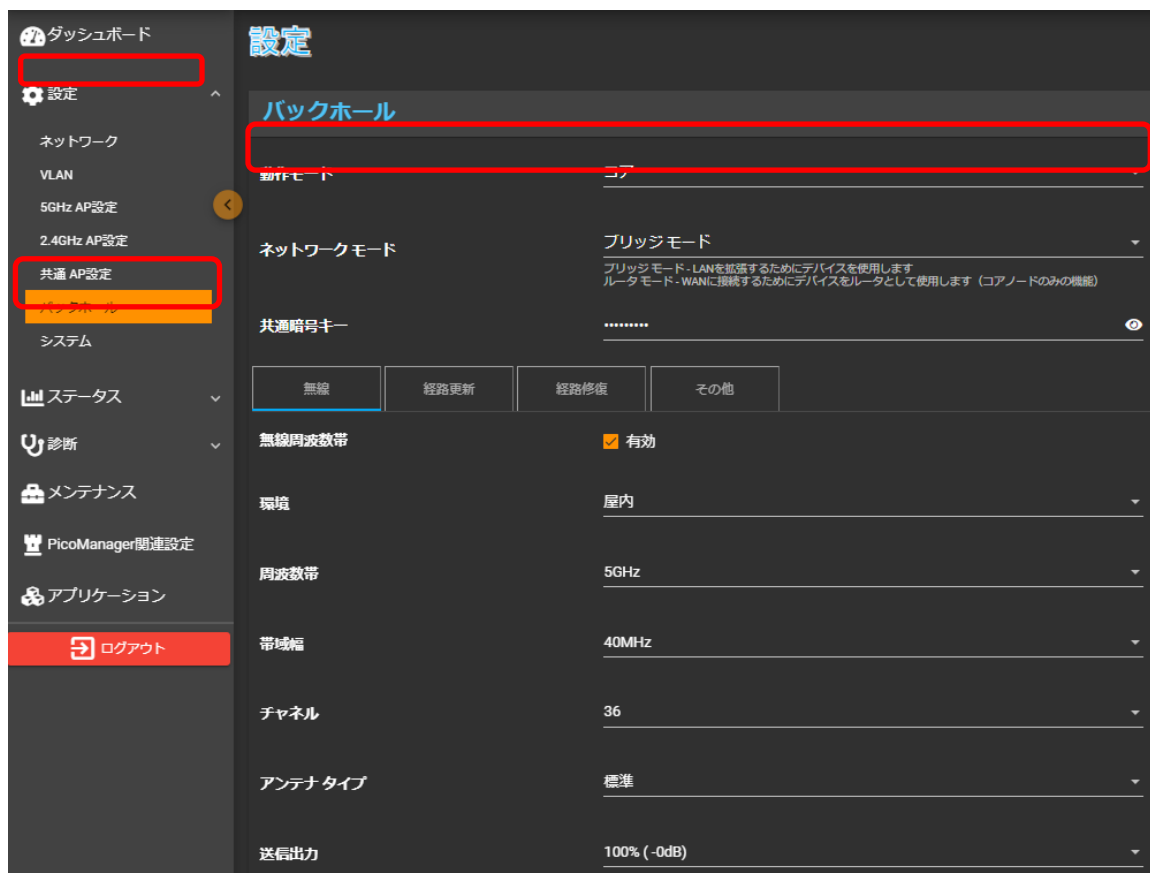


The footer contains buttons for "Save" and "Apply changes" of the configuration data, as well as buttons for uploading and downloading the configuration files.

Click on the Configuration File button to display the Upload Diagram and Download button.



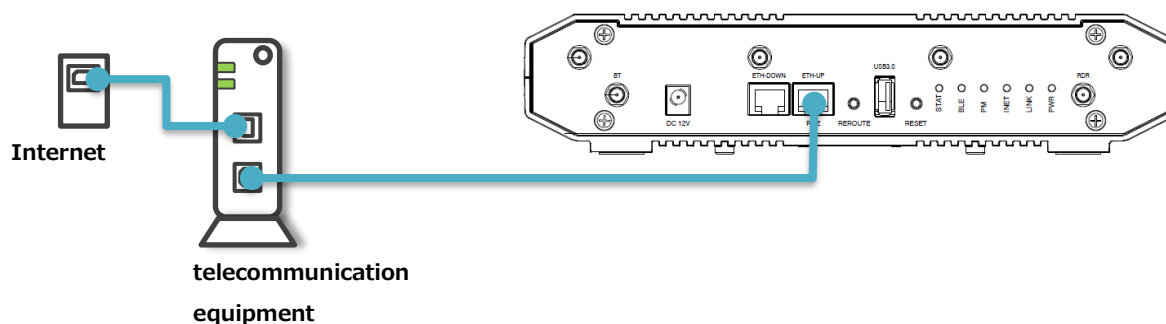
- ⑦ Change to parent unit (core) configuration
Select (click) "Settings→Backhaul" from the main menu on the left side of the screen to move to the following screen.



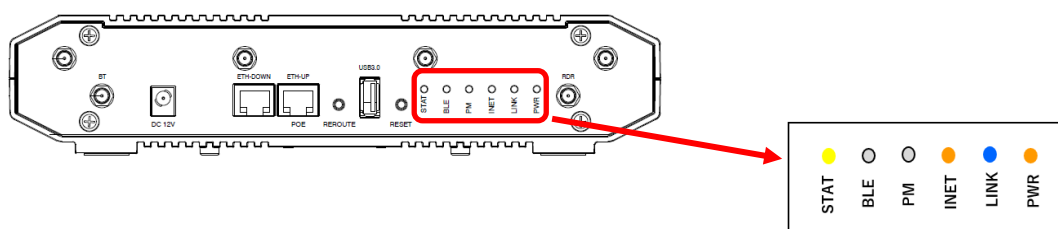
Change the operation mode to "core".

Click "Save" at the bottom of the screen to save settings and apply changes.

- ⑧ Connect the **Eth-up terminal of the PCWL** configured as the parent unit (core) to the upper network with a LAN cable.



After turning on the PCWL, the startup is complete when the device lamps light up as shown below (it takes about 2 minutes to start up).



PWR Lit orange (when DC power is supplied) or lit red (when PoE power is received)

STAT Yellow light on (core display)

LINK LINK : Blue light (core display)

INET Lit orange (Internet connection status); unlit indicates no Internet connection is available.

PM, BLE : Lighting status is irrelevant.

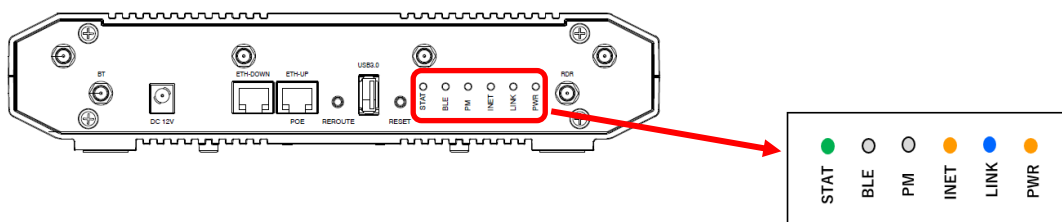
*The startup operation behavior (LED display) changes depending on the channel (W52, W53, or W56) used for the relay line.

For details, please refer to "14.2 About DFS" below.

ステップ 4 : Temporarily install PCWL(child/branch)

If you have purchased only one PCWL, skip this step; use one unit as the parent (core) unit.

1. The factory default state is the child (branch) setting; if set to the parent (core) setting on the WEB UI screen, change to the "branch" setting in the General: Operation Mode on the Backhaul Settings screen in Step 4.
2. Place the PCWL configured as the parent unit (core) in close proximity (power ON), connect power to the child unit (branch), and confirm that the Power light turns on. The Link light blinks and then lights up depending on the signal strength of the BH connection.



PWR Lit orange (when DC power is supplied) or lit red (when PoE power is received)

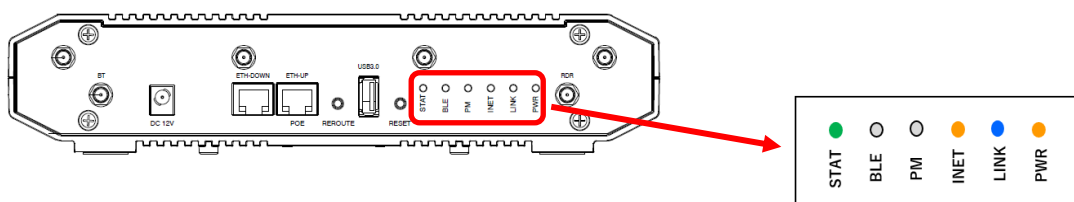
STAT STAT: Lit green (branch indication)

LINK Lit according to the signal strength of the BH line
 Blue (RSSI = -45 dBm or higher), green (RSSI = -45 to -55 dBm), yellow (RSSI = -55 to -65 dBm)
 Red (RSSI=-65dBm or less)

INET Lit orange (Internet connection status); unlit indicates no Internet connection is available.

PM, BLE : Lighting status is irrelevant.

3. After startup, press the Reroute button on the front panel for about 1 second, and when the Link lamp blinks 3 to 4 times and then lights up, the connection with the parent unit (core) is complete.



Use the LINK lamp with the following lighting colors.

Lit blue RSSI is above -45dBm (good signal condition)
 Lit green RSSI is -45 to -55 dBm (good signal condition)
 Yellow light on : RSSI is -55 to -65 dBm (available radio wave condition)
 Lit red : Below -65dBm (radio wave condition not suitable for use)

*The red light can still be used, but the transmission speed will be reduced and the communication quality will be worse.

If the Link LED does not blink or light up, press the reroute button again and confirm that the Link LED lights up.

Perform operations 1 through 3 for the number of child units (branches).

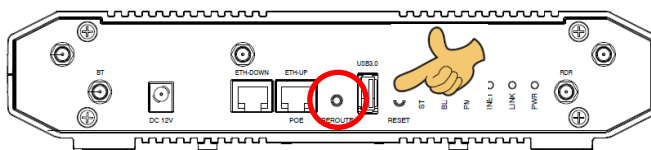
*Operating behavior (LED display) at startup varies depending on the channel (W52, W53, W56) used for the relay line.

For details, please refer to "14.2 About DFS" below.

4. Determine the installation location. Be sure to check the signal and communication status with a temporary installation.

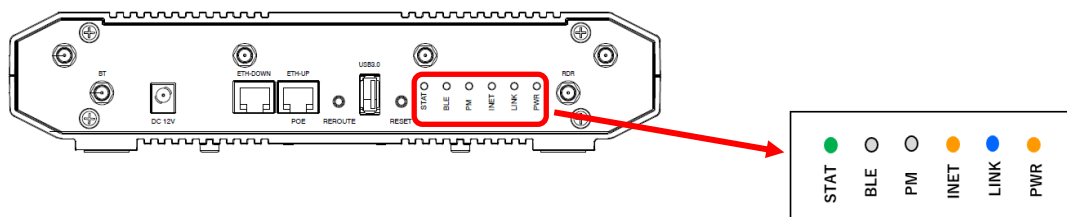
ステップ 5 : Check the link (connection) between parent and child

1. Press the reroute button on the PCWL farthest from the parent unit (core).



※ In fact, it does not matter which PCWL reroute button is pressed; all devices communicate with each other simply by pressing one, even if there are multiple PCWLs.

2. After pressing the reroute button for a while, the LINK lamp will blink several times and then light up.



If the light is lit, that PCWL is available. The color of the light indicates the signal strength.

- ❗ If red is displayed, communication quality (including speed) may be low due to weak connection strength.
- ❗ Use an RSSI value of yellow lighted (recommended is green or blue lighted) or higher.
- ❗ If it does not light up, the PCWL interconnection (link) has failed.
- ❗ Check the connection strength (lighted color) on all installed child units.

In either case, reexamine the location of the PCWL and install it in a location where the signal strength from the reroute button is stable.

3. Make sure that the Link lamp is lit on all the children (branches) of the installed PCWL.
4. Check that the INET lamp is lit (orange). If the light is off, Internet connection is disabled. Check that the INET light on the parent unit (core) is lit. If the INET light on the parent unit (core) is off, check the connection to the upper network.

ステップ 6 : Connect to the Internet with a Wi-Fi device

Actually connect to the Internet wirelessly using a Wi-Fi device. Follow the connection instructions for the appropriate device.

For Windows (Windows 10)

※ This is the connection method when your environment is a PC with built-in wireless LAN in Windows 10.

1. Open the control panel
2. [Click on "Network and Internet" and then on "Connect to Network" in the Network and Sharing Center.
3. Select the factory-set SSID "PicoCELA_A" or "PicoCELA_G" in Wireless Network Connections and click the Connect button. The factory default security setting is WPA2-Personal and the passphrase is "picocela"; enter "picocela" as the passphrase when connecting to Wi-Fi. To change the security settings, follow the procedure described in "7.6 Access Point Settings" in "7 Advanced Settings for the Device" below.
Please be sure to change the passphrase when actually using the device.
4. Verify that you are connected. Click the wireless network connection icon in the system tray at the bottom right of the screen and confirm that "PicoCELA_A" or "PicoCELA_G" is displayed as "connected".
5. Check the connection by launching a browser or other device and displaying a page on the Internet.


For iPhone, iPad, etc.

※ This is how to connect with an iPhone, but others can be connected in much the same way.

1. Tap [Settings
2. Tap [Wi-Fi
3. Select the factory-set SSID "PicoCELA_A" or "PicoCELA_G" in the Wireless Network Connection and click the Connect button. The factory default security setting is WPA2-Personal and the passphrase is "picocela"; enter "picocela" as the passphrase when connecting to Wi-Fi. To change the security settings, follow the procedure described in "7.6 Access Point Settings" in "7 Advanced Settings for the Device" below.
Please be sure to change the passphrase when actually using the device.
4. Go back to the top page, tap [safari], view a page on the Internet, etc. to check the connection.

For Android Smartphone, etc.

※ Please refer to the operation manual of your Smartphone for details as the menu differs depending on the device.

1. Touch [Settings
2. Select a menu item such as "Network and  Internet" or "Wi-Fi".
3. Select "PicoCELA_A" or "PicoCELA_G" from the displayed SSIDs and tap "Connect". The factory default security setting is WPA2-Personal and the passphrase is "picocela." Enter "picocela" as the passphrase when connecting to Wi-Fi. To change the security setting, follow the procedure described in "7.6 Access Point Settings" in "7 Advanced Settings for the Device" below.
Please be sure to change the passphrase when actually using the device.
4. Confirm that the selected "PicoCELA_A" or "PicoCELA_G" is displayed as "Connected" by the operation in step 2.
5. Go back to the top page, tap "Google Chrome" or other browser, and check the connection by viewing the page on the Internet, for example.

ステップ 7 : Perform the main installation

Once the connection is confirmed, perform the main installation of PCWL.

Since the location and height of the temporary installation site and the main installation site may change slightly, press the reroute button at the main installation site just to be sure that the link can be established.

ステップ 8 : If you want to extend the area

If you wish to extend the wireless LAN area, purchase an additional PCWL. Perform steps 3 and 5-8 of this step for the purchased PCWL.

5 About setting changes

Although you can easily build or expand your wireless LAN area with the factory default settings, you can change the settings to improve convenience, security, operability, and performance in the following cases.

- ▶ I want to set communication security (change from factory settings)
- ▶ I want to use the SSID that matches the name of the store or service. (The factory default settings are fixed to "PicoCELA_A" (5GHz band) and "PicoCELA_G" (2.4GHz band).)
- ▶ Separate SSID for each access point (ex. separate SSID for conference room and office)
- ▶ I want to add SSIDs (I want to change security settings for each SSID)
- ▶ There are other wireless LAN access points or wireless LAN routers in the building or on the floor (performance is degraded due to interference)
- ▶ Separate networks (e.g., for employees and for visitors)

etc., the settings can be easily changed using PCWL's web configuration screen.

If you want to set up security,

Access the web configuration screen and set the SSID security-related settings.

See "7.6 Access Point Settings" in "7 Detailed Settings of the IF1-WF01" below for details on setting items and methods.

If you want to use an SSID that matches the name of the store or service,

Access the web setup screen, select "SSID", and set any character string. See "SSID Settings" in "7.6 Access Point Settings" below for setting items and methods.

If you wish to have separate SSIDs for each access point,

On each PCWL, access the web screen, select "SSID", and set a different arbitrary character string as the "SSID". Refer to "SSID Settings" in "7.6 Access Point Settings" below for setting items and methods.

You want to set up VLANs and separate networks,

Assign a VLAN ID to each SSID and configure the office network, guest network, etc. The setting items and methods include

For details, please refer to "VLAN Table" in "7.2 VLAN" and "SSID Settings" in "7.6 Access Point Settings" below.

It's not.

Performance is degraded due to interference caused by other wireless LAN access points or wireless LAN routers,

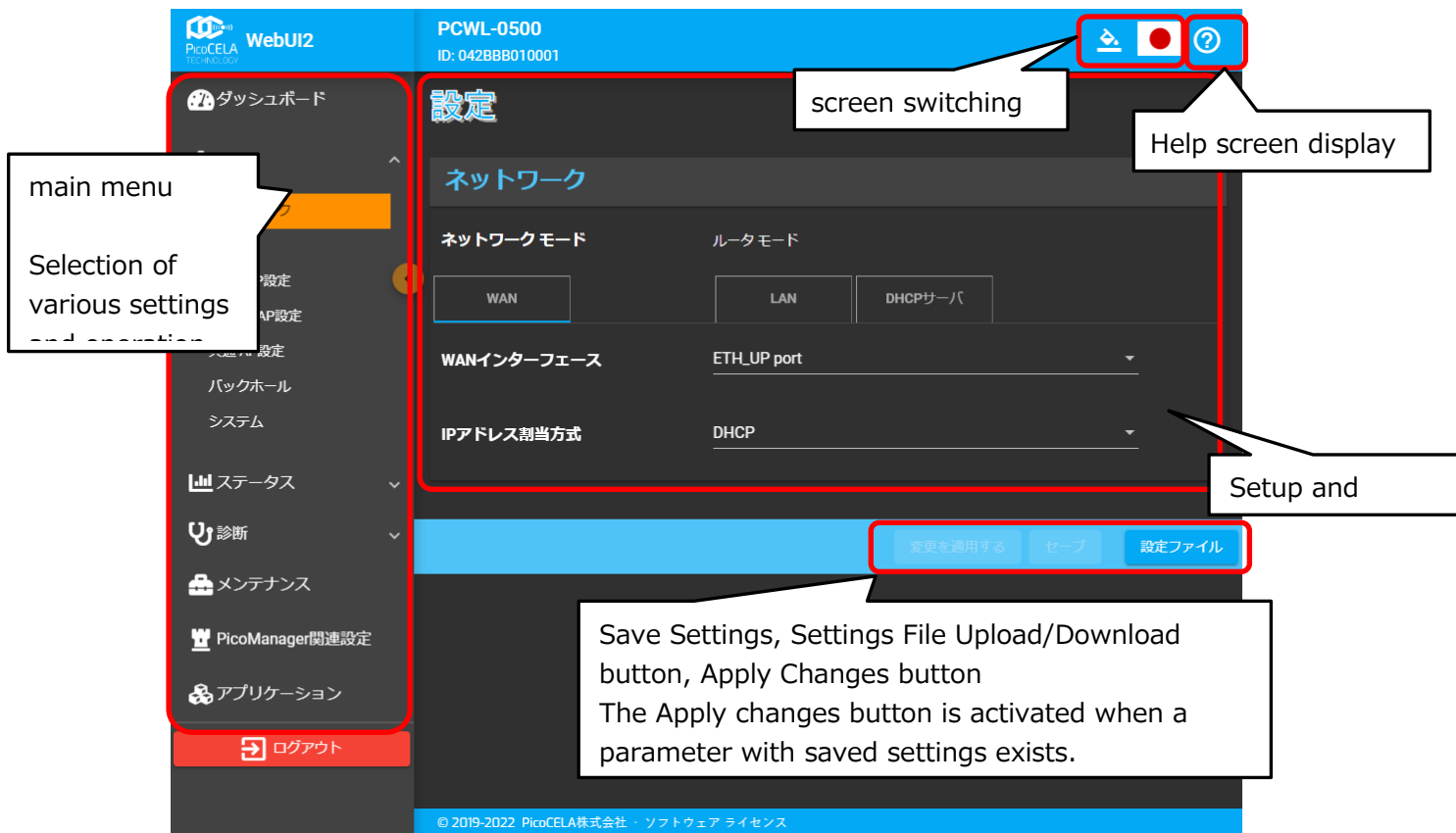
Access the web setup screen, select "5GHz/2.4GHz Radio Settings" and change the channel. Channels are described in detail in "14.1 About Channels" below. Refer to "5GHz/2.4GHz Wireless Settings" in "7.6 Access Point Settings" below for setting items and methods.

If you want to separate networks,

In each PCWL, access the web screen, select "Backhaul Settings," and specify "Channel" and "Common Encryption Key" to separate the networks. For details on setting items and methods, refer to "7.1 Backhaul (relay line) Settings" in "7 Detailed Settings of the IF1-WF01" below.

6 How to operate PCWL's management screen

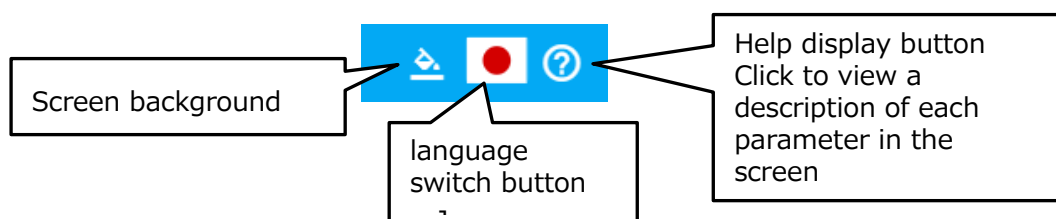
After successful login, you will be taken to the top screen. The administration screen consists of a header section, footer section, main menu, and settings/operation area as shown below.



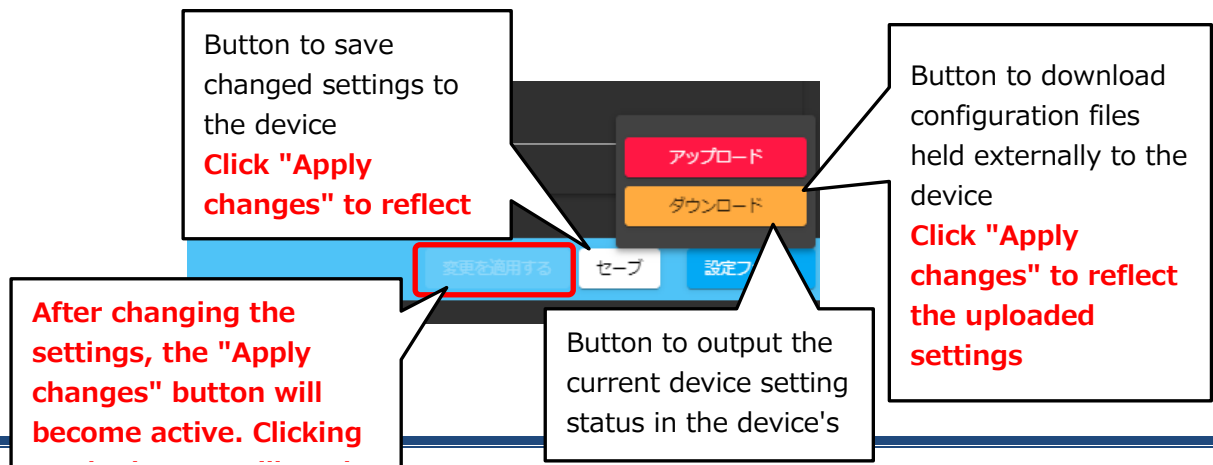
6.1 Screen header and footer icon operation

Each icon in the screen is explained below.

Header icons include a button for switching screen background color, a button for switching language, and a button for displaying help.



The footer has buttons for saving configuration data, uploading and downloading configuration files.



6.2 Help Screen Operation

Clicking on the Help button displays an explanation of each parameter that can be set within that screen.

Please set each parameter in conjunction with Chapter 7, "Detailed Settings of the IF1-WF01.

The screenshot shows the PCWL-0500 settings interface. The main screen has a blue header with the model name and ID. Below it, the '設定' (Settings) title is displayed. The 'ネットワーク' (Network) section is active, showing 'ネットワークモード' (Network Mode) with options for WAN, LAN, and DHCPサーバ. The 'WANインターフェース' (WAN Interface) section shows 'ETH_UP port' and 'IPアドレス割当方式' (IP Address Assignment Method) set to 'DHCP'. A red-bordered help overlay is positioned on the right side of the screen. It contains the title '設定' and a detailed explanation of the settings process, including instructions on saving and applying changes. Below this, it lists 'ネットワーク' (Network) and 'ブリッジモード' (Bridge Mode) with their respective descriptions. At the bottom of the overlay, the 'LAN' section is visible, stating 'LAN側関連の設定ができます' (You can set LAN-related settings). A callout box points to the top right of the overlay with the text '?\" Click to view'. Another callout box at the bottom left of the main screen provides instructions on scrolling and clearing the help screen.

PCWL-0500
ID: 042888010001

設定

ネットワーク

ネットワークモード

ルータモード

WAN

LAN

DHCPサーバ

WANインターフェース

ETH_UP port

IPアドレス割当方式

DHCP

設定

各設定の変更が実施できます。設定変更後「セーブ」ボタンをクリックすれば、変更を一時的に保存できます。この時、変更した設定はまだ機器に反映していません。もしその状態で機器の電源オフまたは再起動を実施したら、一時的に保存した変更が消えてしまいますので、ご注意ください。変更を適用するためには、必要な設定変更を全てセーブし、「変更を適用する」ボタンをクリックすれば設定が機器に反映されます。

「設定ファイル」メニューにある「アップロード」と「ダウンロード」機能を利用すれば、機器にある設定をファイル形式で管理可能です。機器のバックアップとリストアに役立ちます。

ネットワーク

設置場所のオフィス等のネットワーク環境に合わせて、より詳細な設定を行うことができます。

端末間通信禁止

ブリッジモード

本体をブリッジモードとして使用します。本機をブリッジモードで動作させる場合は、上位側ネットワークにルータを設置し、本機と接続してください。

LAN

LAN側関連の設定ができます

?\" Click to view

Help Display Screen
Scrolling operation allows you to scroll the display in the screen
Click the Help button to clear the screen

7 Detailed settings of the monitoring system

More detailed settings can be configured according to the network environment of the office or other location where the system is installed. After logging in, the "Settings" screen will appear.

To set up the monitoring system, first determine and set the operating mode of the backhaul (relay line) of the monitoring system.

7.1 Backhaul (relay line) settings

Select "Settings" from the main menu. Select "Backhaul" from the submenu. This chapter describes the settings for the parent unit (core). For the child unit (branch), only the items that can be configured are displayed.

After changing the settings, click the "Save" button. To apply the saved settings to the device, click the "Apply changes" button. All settings saved in each screen will be applied to the device.

Operation mode setting

Specifies the operating mode of the IF1-WF01. Core (parent unit) is an operation mode in which the unit is connected to the Internet connection via a LAN cable. Branch (child unit) is a mode in which the core (parent unit) or branches (child units) wirelessly build a backhaul (mesh network) with each other and relay (communicate) via a Wi-Fi connection.

When a core (parent unit) is specified, the network mode can be specified. Specify whether the unit is to be used as a router to connect directly to the WAN line or in bridge mode to connect to a higher-level router.

The screenshot shows the 'バックホール' (Backhaul) settings screen. It has three main sections: '動作モード' (Operation Mode), 'ネットワークモード' (Network Mode), and '共通暗号キー' (Common Encryption Key). The '動作モード' section has a dropdown menu currently set to 'コア' (Core). A callout points to this dropdown with the text: 'Specify backhaul operation mode Set core (parent machine)/ branch'. The 'ネットワークモード' section has a dropdown menu currently set to 'ブリッジモード' (Bridge Mode). A callout points to this dropdown with the text: 'Specifies the operating mode of the core (parent unit)'. Below this, there is explanatory text: 'ブリッジモード - LANを拡張するためにデバイスを使用します' and 'ルーターモード - WANに接続するためにデバイスをルータとして使用します (コアノードのみの機能)'. The '共通暗号キー' section shows a field with asterisks. A callout points to this field with the text: 'Specify backhaul common encryption key' and 'Mesh networks are built between devices that share a common key. *Be sure to change the key to any'.

For more information on common encryption keys, please refer to Chapter 13.4, "Dividing the Network".

(data) item	Contents	Possible values	Factory setting
[BACKHOLE]. Operation Mode	Specifies the backhaul operation mode of the monitoring system (PCWL).	Core (parent unit) Branch (Child)	Branch (Child)

	Designates the core (parent unit) and branch (child unit)		
[BACKHOLE] network mode	Specifies the network mode of the device. When the above operation mode is specified as core, you can specify either router mode, which connects directly to the WAN line, or bridge mode, which connects to an upper-level router. If the operation mode is specified as branch, it operates in bridge mode.	router mode bridge mode	bridge mode
[BACKHOLE] symmetric encryption key	Network identifier can be specified Mesh networks are constructed between devices with the same common encryption key. If this common encryption key is different, the same mesh network will not be created When dividing a mesh network, set a separate key for each mesh network for the common encryption key *If the common encryption key is used with the factory default settings, it may connect to devices that are not expected.	half-width alphanumeric character 6 to 255 characters	PCWL-05xx

Wireless Setup

Select the "Wireless" tab to display the Wireless Settings screen.

Core mode screen]

In case of core setting, specify backhaul line radio output ON/OFF for

無線周波数帯 ☒ 有効

環境 屋内

周波数帯 5GHz

帯域幅 40MHz

チャンネル 36

アンテナタイプ 標準

送信出力 100% (-0dB)

Specify indoor or outdoor installation environment

Specify the frequency band of the

Specify bandwidth for backhaul

Specify backhaul line channel

Specify antenna for backhaul line

Specifies the transmission output

Branch mode screen]

無線

その他

スレーブはコアの帯域幅とチャネルを自動検出します。

環境

屋内

アンテナタイプ

標準

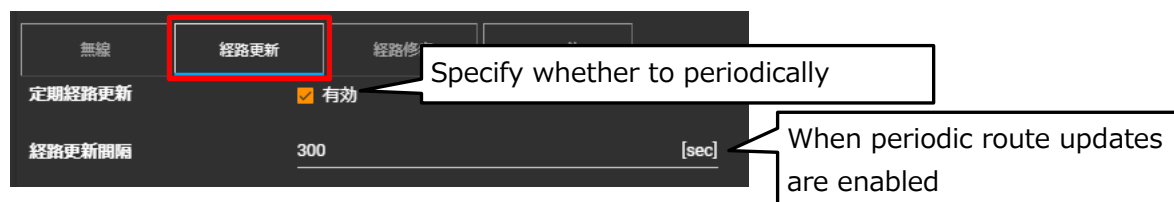
送信出力

100% (-0dB)

(data) item	Contents	Possible values	Factory setting
Wireless] radio frequency band	In case of core setting, radio output ON/OFF setting of backhaul line is available Be sure to enable it for wireless connection to the branch machine. When operating the core alone, the radio output of the backhaul line can be deactivated	Check: Enable (output ON) Unchecked: Disabled (output OFF)	Check: Enabled
Wireless] environment	Specify the installation environment When indoor is selected, W52, W53, and W56 CH can be set. When outdoor is selected, only W56 CH can be set. (When used outdoors, the use of W52 and W53 CH is prohibited by the Radio Law.	indoor (court, pool, etc.) outdoors	indoor (court, pool, etc.)
Wireless / core setting frequency band	Sets the frequency band for the wireless backhaul line This unit can only be specified for 5 GHz	5GHz	5GHz
Wireless / core setting bandwidth	Sets the bandwidth of the communication channel used by the wireless backhaul line	20MHz 40MHz 80MHz 160MHz	40MHz
Wireless / core setting channel	Sets the communication channel to be used for wireless backhaul	The environment, frequency band, and bandwidth define the channels that can be specified.	36
Wireless] Antenna Type	Specifies the antenna to be connected to the backhaul side of the unit Select "Standard" if you wish to use the antenna supplied as a standard accessory *Directional antennas can be used with the PCWL-0510 outdoor unit *Operation with a directional antenna connected while the standard is selected may violate radio laws.	standard directivity	standard
Wireless] Transmission output	Sets the transmit output Controlling the output can reduce the radio coverage area Transmission output level of 100% depends on antenna type	10% (%) 25%. 50% of 100%.	100%.

Backhaul route update setting: at core setting

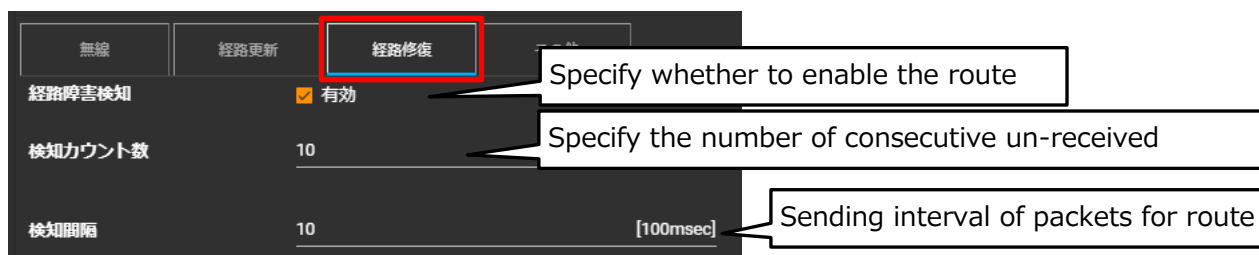
You can configure how to update the route construction of the wireless backhaul. Select the "Route Update" tab to display the Route Update Settings screen.



(data) item	Contents	Possible values	Factory setting
[Pathway update]. periodic route update	You can specify whether to perform periodic backhaul route updates	Unchecked: Invalid Check: Enabled	Check: Enabled
[Pathway update]. routing update interval	Allows you to set the cycle settings for route updates Unit is specified in seconds.	1-65535	300 sec.

Restoration settings in case of backhaul route failure: when core is configured

You can configure the repair method when the wireless backhaul line fails due to equipment failure, etc. and the route is disconnected. Select the "Route Repair" tab to display the Route Repair Settings screen.



(data) item	Contents	Possible values	Factory setting
[Path repair]. Path Failure Detection	You can specify whether to enable route failure detection If enabled, route updates are performed immediately after failure detection Even if disabled, when the above-mentioned periodic route update is enabled, the periodic route update reconstructs the routes except for the failed devices.	Unchecked: Invalid Check: Enabled	Check: Enabled
[Path repair]. Number of detection counts	Allows you to set the detection counter value for route failure detection Specifies how many consecutive packets for route failure detection cannot be received to determine that a route failure has occurred.	1 to 255	10
[Path repair]. detection interval	Specifies the sending interval of packets for route failure detection	1 or more	10 (1 second)

	The specified unit is 100msec.		
--	--------------------------------	--	--

Backhaul special settings

You can specify restrictions on the construction of backhaul lines and on the operation of access points in the event of route failures. Other."

tab to display the settings screen.

Setting screen when selecting a core].

無線	経路更新	経路修復	その他
ブロードキャスト制御パケット最大 3 送信回数			
Specify the maximum number of times to			
RSSI移動平均係数 3 初期値は3です			
Specify local RSSI moving average			
ルーティングメトリック係数 通常			
Specify routing matrix coefficients			
移動グループ <input type="checkbox"/> 有効			
Specify activation of move			
移動グループID 1			
Specify mobile group ID			
コア冗長化モード <input checked="" type="checkbox"/> 有効			
Designation for redundant			
Eth-upリンク確認 <input type="checkbox"/> 有効			
Specify whether or not to detect abnormalities on the			
有線バックホールVLANタグID 0			
Specify VLAN ID for wired backhaul			

The setting screen when a branch is selected.

The screenshot shows the 'その他' (Other) settings screen for a branch. The 'その他' tab is selected and highlighted with a red box. The settings are as follows:

- リーフモード** (Leaf mode): ☐ 有効 (Leaf mode enable)
- 経路障害時APオフ** (AP off in case of path failure): ☐ 有効 (Specify to stop AP output in)
- ブロードキャスト制御パケット最大送信回数** (Broadcast control packet maximum transmission count): 3
- ローカルのRSSI移動平均係数** (Local RSSI moving average coefficient): ☐ 有効
- RSSI移動平均係数** (RSSI moving average coefficient): 3 (初期値は3です)
- ルーティングメトリック係数** (Routing metric coefficient): 通常
- 移動グループ** (Mobile group): ☐ 有効
- 移動グループID** (Mobile group ID): 1
- 上流ノードMACアドレス** (Upstream node designation for): FF:FF:FF:FF:FF:FF
- 有線バックホールVLANタグID** (Wired backhaul VLAN tag ID): 0

(data) item	Contents	Possible values	Factory setting
Other/Branch settings leaf mode	Can be specified to prohibit the construction of routes under itself When leaf mode is specified, no backhaul route will be constructed under the specified child The child specified as valid will be the end of the route	Unchecked: Possible to construct a route under the control of Check: Prohibits construction of subordinate routes	Unchecked: Possible to construct a route under the control of
Other/Branch settings AP off in case of path failure	If a device fails and the route is disconnected, the communication of the child APs that cannot connect to the host can be stopped for each device.	Unchecked: Continued AP communication Check: Stop AP communication	Unchecked: Continued AP communication
Other Maximum number of broadcast control packet transmissions	You can specify the maximum number of broadcast packets to be sent for backhaul construction Normally, three times is recommended, but if there are many nodes that are isolated from the route, increasing the number of transmissions may solve the problem.	1~	3
Other/Branch settings	Only branches can be set	Unchecked: Not used Check: Use	Unchecked: Not used

Use local RSSI moving average coefficients	Individual RSSI moving average coefficients can be used instead of RSSI moving average coefficients sent from the core		Operation with factory settings is recommended
Other RSSI moving average coefficient	You can specify the weighting of RSSI values to be referenced in the optimal route construction Increasing the RSSI value increases the weight of the past history value	0 to	3 Operation with factory settings is recommended
Others routing metric factor	You can specify whether to prioritize the route construction type by reducing the number of hops or by RSSI value.	Specified in 5 steps	usual
Other movement group enable	When the monitoring system is mounted on a mobile device, the nodes in the mobile device can be grouped together Only one node in a grouped node county is configured to communicate with the outside (outside the mobile unit)	Unchecked: Invalid Check: Enabled	Unchecked: Invalid
Other IMG-ID	A group ID can be assigned to each mobile unit Groups can be divided by separating IDs for adjacent mobile units, etc.	1~	1
Other / When core mode is set core redundancy mode	When this mode is enabled during core redundancy operation, connection to the existing route is made at core startup Search backhaul routes for a certain period of time, and if no route with the same backhaul key exists, start with the configured backhaul channel and bandwidth	Unchecked: Invalid Check: Enabled	Unchecked: Invalid
Other / When core mode is set Confirmation of Eth-up link	When core redundancy mode is enabled, the system detects failures on the Eth-up port. If a failure is detected, the backhaul and access-side radio waves are shut down. Branch machines with backhaul connections to this core automatically transition to the backhaul route configured by the other core.	Unchecked: Invalid Check: Enabled	Unchecked: Invalid
Other/Branch settings upstream node MAC address Valid only in branch mode.	Only branches can be set When constructing a route, the upper node to be connected can be specified regardless of the radio wave status. Specify the upper node MAC address to be connected If FF:FF:FF:FF:FF:FF:FF:FF:FF is specified, the optimal route is determined and an automatic route is constructed (Note) If a MAC address that does not exist in the route is specified, it will not be connected to the upper node.	MAC address	FF:FF:FF:FF:FF:FF:FF:FF
Other cable backhaul	Specifies the VLAN ID for wired backhaul connections between nodes via network devices	0 to 409	0

VLAN ID tag	such as HUBs, when VLAN ID=0 tags are not allowed All nodes connected by wired backhaul must have the same ID and an ID that does not duplicate other VLAN IDs		
-------------	---	--	--

7.2 Network configuration: in router mode (parent unit/core only)

Display the main menu and select "Settings→Network". Router mode can only be configured for "Parent/Core". The "Subscriber/Branch" operating mode is only available in Bridge mode.

After changing the settings, click the "Save" button. To apply the saved settings to the device, click the "Apply changes" button. All settings saved in each screen will be applied to the device.

WAN-side network configuration: Eth-up port connection

This section describes how to set up this unit when it is used by connecting its Eth-up port to the upper network with a LAN cable.

Select the "WAN" tab to display the WAN Settings screen.

The screenshot shows the 'ネットワーク' (Network) settings page. At the top, 'ネットワークモード' (Network Mode) is set to 'ルータモード' (Router Mode). Below this, the 'WAN' tab is selected and highlighted with a red box. The 'WANインターフェース' (WAN Interface) is set to 'ETH_UP port'. The 'IPアドレス割当方式' (IP Address Assignment Method) is set to '静的IPアドレス' (Static IP Address). The 'IPアドレス' (IP Address) is '10.0.0.3', 'サブネットマスク' (Subnet Mask) is '255.255.255.0', 'ゲートウェイ' (Gateway) is '10.0.0.1', and 'DNS' is '8.8.8.8'. The 'セカンダリDNS' (Secondary DNS) is 'e.g. 8.8.8.8'. Callouts point to the 'ルータモード' label, the 'WAN' tab, the 'ETH_UP port' selection, the '静的IPアドレス' selection, and the IP address fields.

Display of the network mode

Designation of WAN-side interface

Designation of WAN-side IP address allocation method

When static IP address is selected for WAN IP address assignment, specify IP address, subnet mask, default gateway, and DNS

(data) item	Contents	Factory setting
network mode	The mode specified in the network mode of the backhaul configuration is displayed To change this mode, change it on the backhaul setting screen	
Settings in router mode	Contents	Factory setting
[WAN]. WAN Interface ETH_UP port PPPoE	Specifies the WAN-side interface ETH_UP port: When connecting this unit's ETH_UP port to a host router with a LAN cable PPPoE: When connecting to ONU via PPPoE protocol	ETH_UP port
[WAN]. IP address allocation scheme	Select the IP address allocation method for the WAN side DHCP: When an IP address is automatically assigned by the upper router via DHCP	DHCP

DHCP static IP address	Static IP address: To assign a static IP address	
[WAN]. IP address	When "Static IP address" is specified as the IP address allocation method, specify a fixed IP address on the WAN side IP address: Specify the fixed IP address of the monitoring system on the WAN side	IP address: 10.0.0.3
[WAN]. subnet mask	Specifies the subnet mask on the WAN side Subnet mask: Specify the subnet mask on the WAN side	255.255.255.0
[WAN]. gateway	Specify the address of the WAN-side gateway	gateway 10.0.0.1
[WAN]. Domain Name System secondary DNS	Specify the IP address of the DNS server on the WAN side DNS: Specify the IP address of the primary DNS server Secondary DNS: Specify a secondary DNS server if needed	Domain Name System 8.8.8.8 secondary DNS unspecified

WAN-side network settings: PPPoE connection

This section describes the case in which the device is connected directly to the ONU with a LAN cable and connected using PPPoE settings.

The screenshot shows the WAN interface configuration page. The 'WAN' tab is selected, and 'PPPoE' is chosen from the dropdown menu. The form includes the following fields:

- ユーザーID (User ID):** e.g. picotaro@picocela.com
- パスワード (Password):** (masked)
- MTU:** 1454
- サービス名 (オプション) (Service Name):** e.g. pppoe-service
- ローカルIP (オプション) (Local IP):** e.g. 8.8.8.8
- リモートIP (オプション) (Remote IP):** e.g. 8.8.8.8

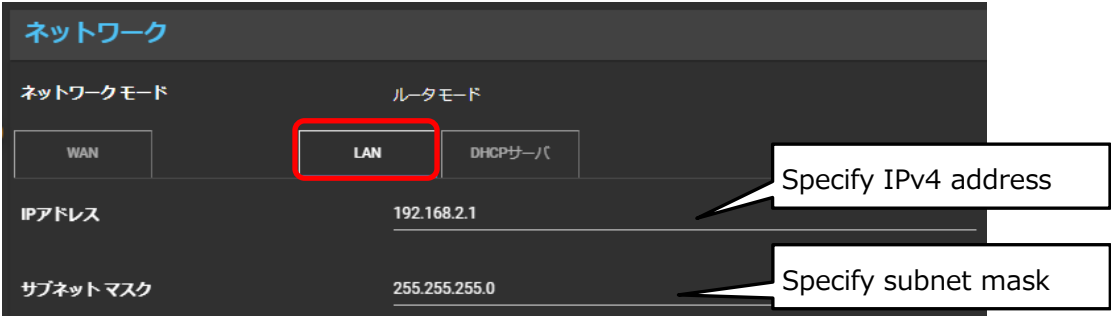
Callouts indicate: 'Select PPPoE' and 'Please refer to the connection setting information from your provider and set it up.' (pointing to the MTU field).

When PPPoE is selected for WLAN connection	Contents	Factory setting
[WAN]. user ID	Specify the authentication ID (user name) for the Internet connection provided by your provider. (Example) picocela1234@●●●●.●●.jp	blank space
[WAN]. (computer) password	Specify the password for Internet access provided with your authentication ID by your contracted provider.	blank space
[WAN]. MTU	Set the optimal MTU size according to your network line. Please check with your provider for details.	1454

	Standard PPPoE: 1492 B Flets: 1454	
[WAN]. Service name (option)	Specify the name of the service for Internet access provided by your provider along with your authentication ID. Operation without specification is also possible.	blank space
[WAN]. Local IP (optional)	If a global fixed IP address is assigned by the provider, set the local fixed IP address for the PPPoE link	blank space
[WAN]. Remote IP (optional)	If a global static IP address has been assigned by the provider, set the remote side static IP address for the PPPoE link	blank space

LAN-side network settings

This section describes the settings for the LAN side of the device. Select the "LAN" tab for the settings. Check with your network administrator for the IP address to be set.



LAN-side setting	Contents	Factory setting
[LAN] IP address	Specifies the IP address of the LAN side	192.168.2.1
[LAN] subnet mask	Specifies the subnet mask on the LAN side	255.255.255.0

DHCP Server Settings

When using the device in router mode, the DHCP server of the device can be used. This section describes how to set that up. Click on the "DHCP Server" tab to configure the settings.

ネットワーク

ネットワークモード

ルータモード

WAN

LAN

DHCPサーバ

DHCPサーバ

☒ 有効

開始IPアドレス

192.168.2.50

終了IPアドレス
IPアドレス数 : 205

192.168.2.254

アドレスリース期間

120

Specify DHCP server as

Specify starting IP address for

Specify the IP address of the end

Specify IP address lease period

(data) item	Contents	Factory setting
DHCP server DHCP Server	Specify whether to enable the DHCP server function. Unchecked: Invalid Check: Enabled	Check: Enabled
DHCP server starting IP address	Specifies the starting address of the IPv4 address range to be distributed when the DHCP server is enabled.	192.168.2.20
DHCP server terminating IP address	Specifies the end address of the IPv4 address range to be distributed when the DHCP server is enabled.	192.168.2.100
DHCP server address lease period	Specifies the lease period of IPv4 addresses to be distributed when the DHCP server is enabled. Specified unit is minutes	120 min.

7.3 Network settings: in bridge mode, in branch mode

This section explains how to configure the backhaul settings when the bridge mode is selected as the network mode and the branch mode is selected as the backhaul operation mode. When operating the parent unit (core) in bridge mode, install a router in the upper network and connect it to this unit.

LAN-side IP address setting

Click the " LAN" tab and set the LAN-side IP address.

ネットワーク

ネットワークモード ブリッジモード

LAN

IPアドレス割当方式 静的IPアドレス

IPアドレス 192.168.1.254

サブネットマスク 255.255.255.0

ゲートウェイ 192.168.1.1

DNS 8.8.8.8

セカンダリDNS e.g. 8.8.8.8

Select IP address allocation method

When DHCP is selected, the IP address obtained from the upper router (DHCP server) is set.
When a static IP address is selected, the left column is displayed and the IP address is set.

(data) item	Contents	Factory setting
LAN] IP address allocation scheme	Specify DHCP or static IP address as the LAN-side IP address allocation method	DHCP
LAN] When static IP address is selected IP address subnet mask	Specify the fixed IP address and subnet mask for the LAN side IP address: Specify the fixed IP address of the device on the LAN side Subnet mask: Specifies the subnet mask on the LAN side	IP address: 192.168.1.254 subnet mask 255.255.255.0
LAN] gateway	Specify the IP address of the LAN-side default gateway	gateway 192.168.1.1
LAN] Domain Name System secondary DNS	Specify the IP address of the DNS server on the LAN side DNS: Specify the IP address of the primary DNS server Secondary DNS: Specify a secondary DNS server if needed	Domain Name System 8.8.8.8 secondary DNS unspecified

7.4 VLAN Settings

If VLANs are to be established in the network construction, configure the VLAN settings in advance and assign the configured VLAN ID to each SSID.

Display the main menu and select "Settings". Select "VLAN" from the submenu.

After changing the settings, click the "Save" button. To apply the saved settings to the device, click the "Apply changes" button. All settings saved in each screen will be applied to the device.

VLAN table settings

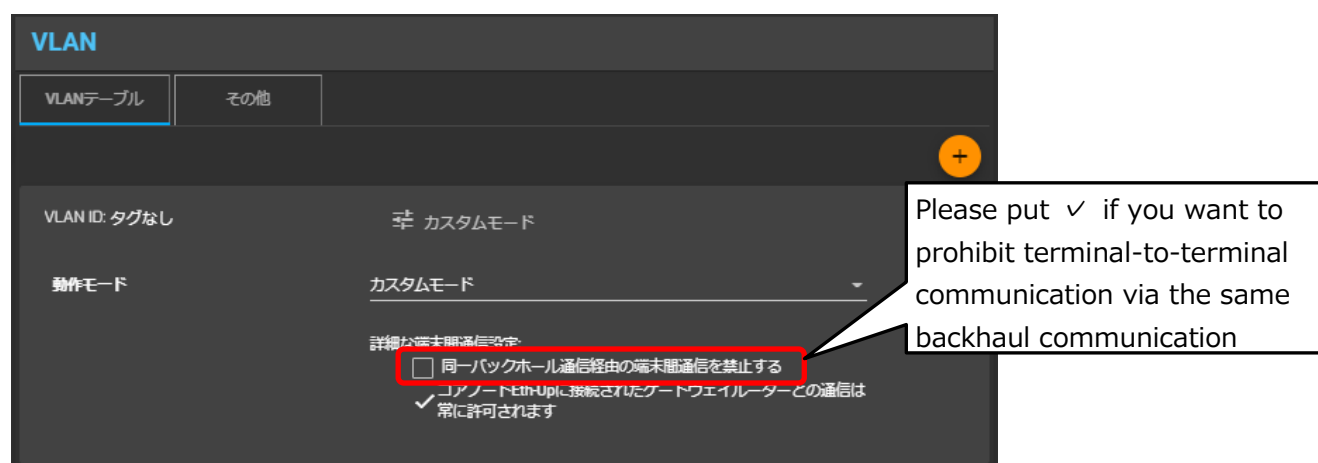
Click on the "VLAN Table" tab to configure settings related to terminal-to-terminal communications for each VLAN ID assigned in the network.

Default VLAN / Native VLAN (untagged)

Select the "VLAN Table" tab to display the following screen and configure the default VLAN settings. The default setting is to allow all communication between terminals in the same backhaul.

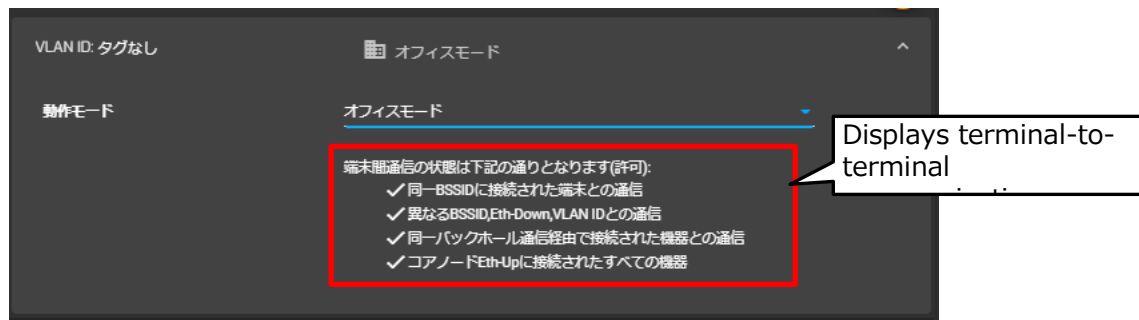


To change the terminal-to-terminal communication settings, click "V" on the far right to display the following screen.

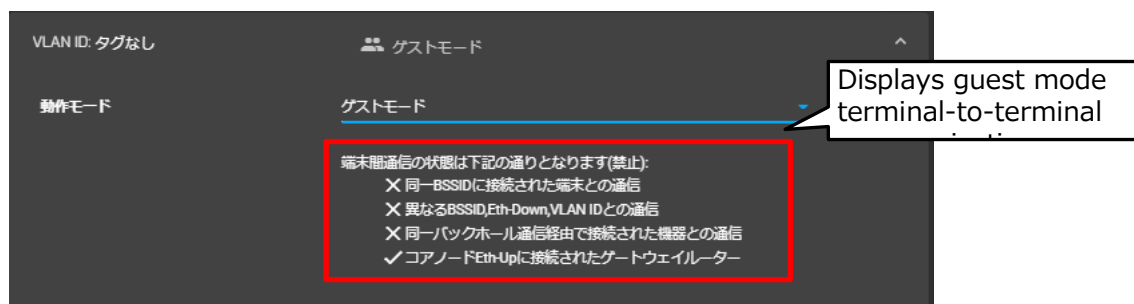


In addition to "Custom Mode," users can select either "Office Mode," which allows all terminals to communicate with each other, or "Guest Mode," which prohibits all terminals from communicating with each other and only allows Internet connection (with a gateway router).

Office mode selection screen]



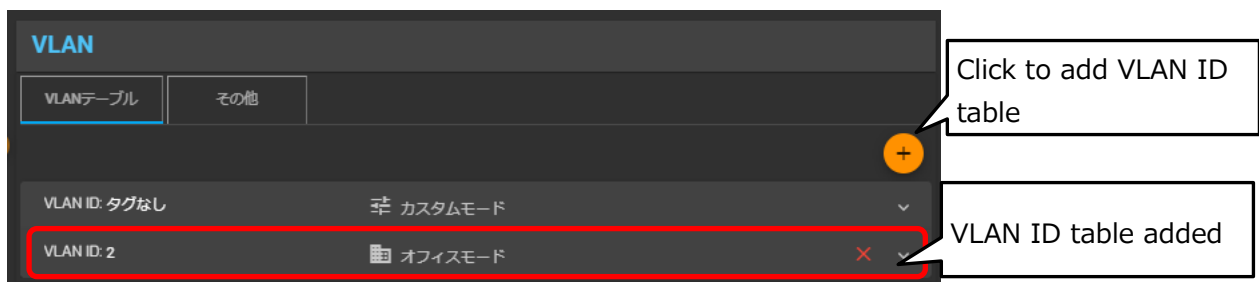
Guest mode selection screen]



✓" indicates permission, "X" indicates prohibition.

VLAN ID and various settings

To assign a VLAN ID, click the "+" button to display the following screen.

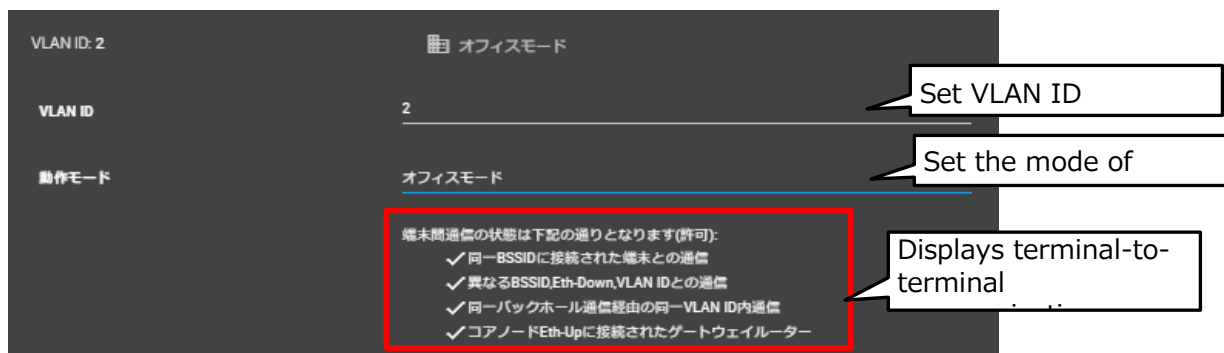


A new VLAN ID table will be added. Click on the added VLAN ID table to display the Advanced Settings screen.

When the unit is in core configuration or router mode

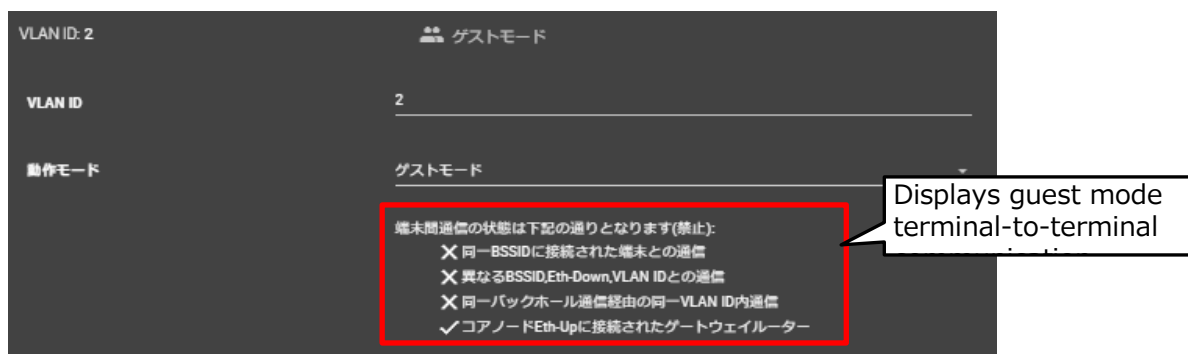
The following is the configuration when the backhaul setting of the device is the core setting and in router mode. First, specify the VLAN ID and operating mode.

The "office mode" permits all communications between terminals connected to the device.



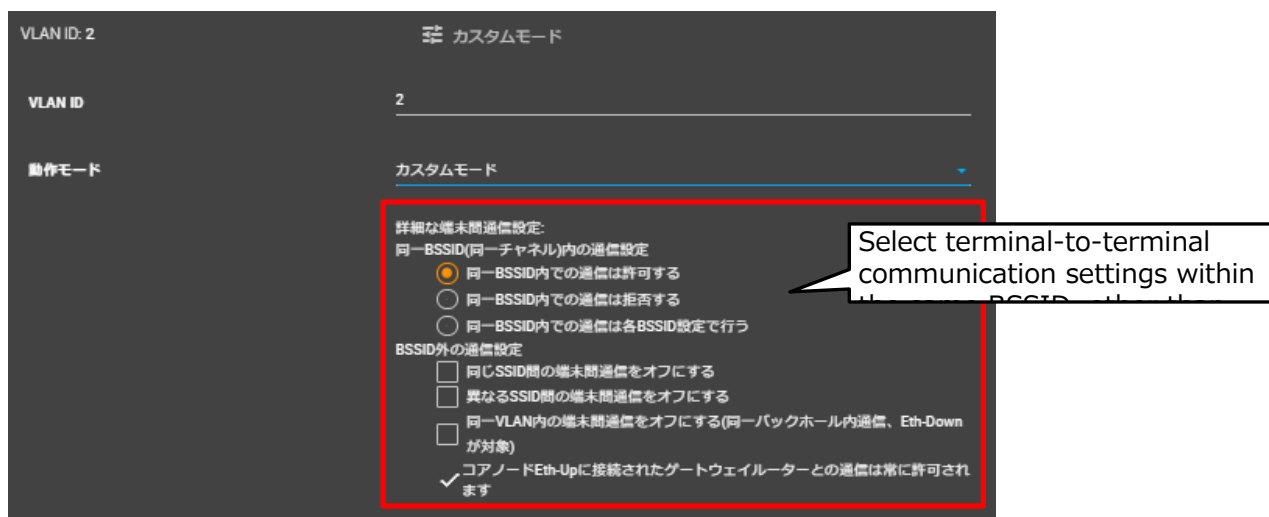
The "✓" indication indicates permission.

Guest mode" prohibits all communication between terminals connected to the unit. Each terminal is only allowed to communicate with the gateway router and is allowed to connect to the external Internet through the router.



The "X" symbol indicates prohibition.

Selecting "Custom Mode" allows you to configure each communication setting individually.



The following table describes the operation when each item is specified.

- Communication settings within the same BSSID (same channel)

choice	action when specified
Communication within the same BSSID is permitted	Specified to allow communication between terminals connected to 2.4GHz and 5GHz channels of the same device.
Communication within the same BSSID is denied	Specified to prohibit communication between terminals connected to 2.4GHz and 5GHz channels of the same device.
Communication within the same BSSID is done by each BSSID setting	7.X Refer to the SSID setting of the access point and specify after each SSID

- Communication settings outside BSSID

choice	action when specified
Turn off inter-device communication between devices with the same SSID	Specified to prohibit communication between terminals connected to 2.4GHz and 5GHz when the same SSID is specified for both 2.4GHz and 5GHz for the same device (node)
Turn off terminal-to-terminal communication between different SSIDs	Specified to prohibit communication between terminals connected to different SSIDs when multiple SSIDs are specified for the same device (node).
Turn off communication between terminals in the same VLAN (communication in the same backhaul, subject to Eth-down)	Specified to prohibit communication between terminals connected to the same VLAN (same VLAN ID) with multiple devices (multiple nodes) and multiple SSIDs.

When in router mode, be sure to make the following settings

The screenshot shows the 'VLAN IPv4' configuration page. Key settings and their explanations are as follows:

- VLAN IPv4:** ☐ 有効 (Enabled). Callout: "To assign the IP address of the device to the".
- IPアドレス割当方式 (IP Address Allocation Method):** 静的IPアドレス (Static IP Address). Callout: "Specify IP address allocation method, IP address, and subnet".
- IPアドレス (IP Address):** e.g. 192.168.1.254
- サブネット マスク (Subnet Mask):** e.g. 255.255.255.0
- DHCPサーバ (DHCP Server):** ☐ 有効 (Enabled). Callout: "Enable DHCP server to distribute IP addresses to terminals connected to the".
- 開始IPアドレス (Start IP Address):** e.g. 192.168.1.50
- 終了IPアドレス (End IP Address):** e.g. 192.168.1.200. Callout: "DHCP server related settings".
- アドレスリース期間 (Address Lease Period):** e.g. 120 minute
- DNSサーバ (DNS Server):** 自分のIPアドレス(DNSリレー) (My IP Address (DNS Relay))
- WebUIアクセス禁止 (IPv4) (WebUI Access Prohibition (IPv4)):** ☐ 有効 (Enabled). Callout: "Permission setting for WEB UI screen connection from terminals with IPv4".
- WebUIアクセス禁止 (IPv6) (WebUI Access Prohibition (IPv6)):** ☐ 有効 (Enabled). Callout: "Permission setting for WEB UI screen connection from terminals with IPv6".

(data) item	Contents
VLAN IPv4	In router mode, enables the assignment of the device's IP address within the relevant VLAN interface
IP address allocation scheme	Assigns the IP address of the device within the VLAN interface When the backhaul setting is in router mode, allocation by DHCP is not possible.
IP address	Specifies the IP address to be assigned to the relevant VLAN interface
subnet mask	Specifies the subnet mask of the IP address to be assigned
DHCP Server	Enables IP address assignment from the DHCP server of the IF1-WF01 to the terminal connected to the VLAN ID.
starting IP address	Specifies the starting address of the allocated IP address
terminating IP address	Specifies the end address of the allocated IP address
address lease period	Specifies the lease period of the allocated IP address
DNS Server	Select whether to specify the DNS server with the DNS relay function or the IP address of the DNS server; if you select IP address specification, specify the IP address of the DNS server.
WebUI access prohibited (IPv4)	Enable to prohibit access to the WebUI (management screen) from terminals connected to the relevant VLAN ID with an IPv4 address
WebUI access prohibited (IPv6)	Enable to prohibit access to the WebUI (management screen) from terminals connected to the relevant VLAN ID with an IPv6 address

When the unit is in branch setting or bridge mode

This section describes the settings when the backhaul setting of the device is set to branch or bridge mode. First, specify the VLAN ID and operating mode.

The settings for Office mode, Guest mode, and Custom mode are the same as those in the previous section. Please refer to the previous section for the settings.

The following table describes the VLAN interface configuration conditions depending on the operating mode setting.

1. When office mode is selected
VLAN IPv4 and beyond need not be configured.
Only the WebUI access prohibition setting should be specified according to the operation.
2. When guest mode is selected
Configure VLAN IPv4 and beyond according to the following table.

3. When "Turn off communication between terminals in the same VLAN" is selected in custom mode
Configure VLAN IPv4 and beyond according to the following table.
4. In the case of a configuration with Radius servers in a specific VLAN
For the VLAN in which the Radius server is located, configure VLAN IPv4 or later according to the following table.

VLAN IPv4 ☐ 有効 To assign the IP address of the device to the

IPアドレス割当方式 静的IPアドレス

IPアドレス e.g. 192.168.1.254

サブネットマスク e.g. 255.255.255.0

IPv4ゲートウェイ ☐ 有効

ゲートウェイIPアドレス e.g. 192.168.1.1

複数IPv4ゲートウェイ ☐ 有効

ゲートウェイIPアドレスリスト e.g. 192.168.1.2, 192.168.1.3
複数IPアドレスを入力する場合、「」で分けてください

MACでゲートウェイ設定 ☐ 有効

ゲートウェイMACアドレスリスト e.g. 11-22-33-AA-BB-CC, 44-55-66-DD-EE-FF
複数MACアドレスを入力する場合、「」で分けてください

WebUIアクセス禁止(IPv4) ☐ 有効

WebUIアクセス禁止(IPv6) ☐ 有効

(data) item	Contents
VLAN IPv4 Address	Enable to assign the IP address of the device to the relevant VLAN interface.
IP address allocation scheme	Specifies the IP address assignment method of the device to the VLAN interface Select whether to obtain an IP address from a DHCP server or set a static IP address
IP address	If a static IP address is selected, specify the IP address to be assigned
subnet mask	Specifies the subnet mask of the IP address to be assigned
IPv4 Gateway	Specifies activation of communication with the gateway
gateway IP address	Specify the IP address of the gateway
Multiple IPv4 address lists	In the case of a network environment with multiple gateways (e.g., redundant), enable it and specify the IP address in the next section.
gateway IP address list	If the previous section is enabled, specify the gateway IP address

	When specifying multiple IP addresses, separate them with ",".
MAC Gateway Settings	If the VLAN interface in question cannot be assigned an IPv4 address, the gateway setting can be specified by MAC address. Enable to specify by MAC address
Gateway MAC Address List	If the previous section is enabled, specify the MAC address of the gateway MAC address must be specified in the format 11:22:33:AA:BB:CC When specifying multiple MAC addresses, separate them with ",".
WebUI access prohibited (IPv4)	Enable to prohibit access to the WebUI (management screen) from terminals connected to the relevant VLAN ID with an IPv4 address
WebUI access prohibited (IPv6)	Enable to prohibit access to the WebUI (management screen) from terminals connected to the relevant VLAN ID with an IPv6 address

Configure Eth-down port, management VLAN, and VLAN for PicoManager connection

The user can configure the Eth-down port, the management VLAN and the VLAN for PicoManager connection of the device.

Please refer to the following table for setting.

PicoManager


(data) item	Contents
Eth-down VLAN mode	Specifies the VLAN mode of the communication interface connected to the eth-down port with a LAN cable Trunk mode sends packets with tags Access mode sends only the specified VLAN ID without tags
Management VLAN ID	Specify the VLAN for management of WEB UI, etc.
For PicoManager connection VLAN ID	You can set individual VLAN IDs to connect to PicoManager. VLAN IDs for individual configuration must be set in the VLAN table in advance.

7.5 Router Function Configuration


The PCWL5 series products can use the firewall and port forwarding functions newly added to the PCWL5 series products. To use PicoManager, please refer to Chapter 11 "PicoManager Connection Settings" for pre-registration and activation.

A separate contract is required to use PicoManager's node configuration function. Please contact your local distributor or PicoCELA for the contract procedure.

Firewall Feature Configuration

When the parent unit (core) is used in router mode, the firewall function can be configured: go to the node list in PicoManager and click on the  configuration icon for the parent unit (core). Select "Security" from the tabs on the left side of the screen, then select the Firewall tab.

Select the Firewall tab




To add a rule, click the "+" button to display the settings table.

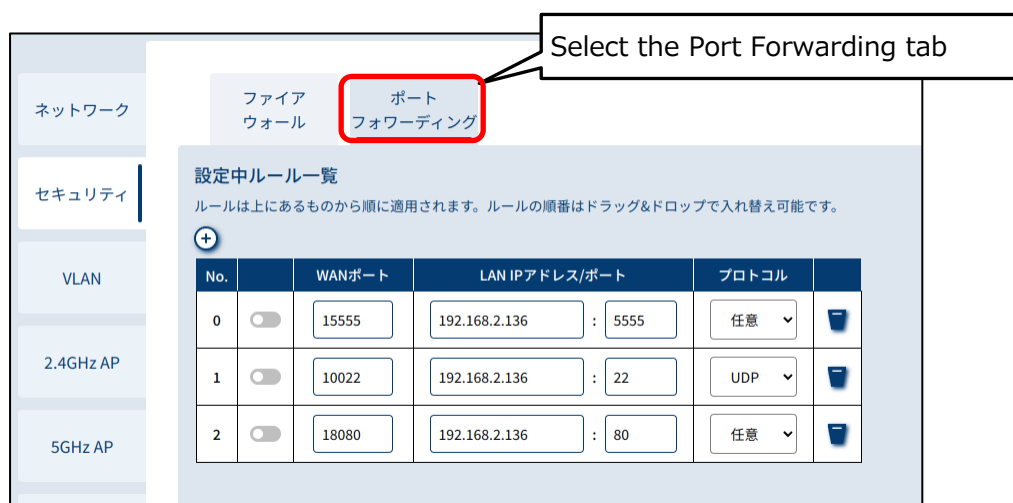
Refer to the table below for each setting item. The settings are applied in the order of the highest setting. The order of settings can be changed by drag & drop.

Setting items	Configuration details
Enable button	This button activates the setting. Grayed-out status does not reflect the setting.
Directions.	Sets the direction in which data packets are sent. WAN⇒LAN": Packet setting in the direction of transmission from the WAN side to the internal LAN LAN⇒WAN": Packet setting for the direction of transmission from the internal LAN to the external WAN side
VLAN ID	Specify the VLAN ID to be configured VLAN ID can be a preconfigured VLAN ID in the VLAN table

sender	Specify the IP address, subnet mask, and port number of the source terminal to which the rule is applied Subnet mask must be specified by prefix length Example: 255.255.255.0 ⇒ 24 If port number is "blank", all port numbers are covered
destination (of transmission)	Specify the IP address, subnet mask, and port number of the destination terminal to which the rule is applied Subnet mask must be specified by prefix length Example: 255.255.255.0 ⇒ 24 If port number is "blank", all port numbers are covered
protocol	Specifies the protocol to which the rule is applied Protocols that can be specified: TCP, UDP, TCP+UDP, any (all)
operation	Allows or prohibits the set communication
delete button	Click on the trash to delete settings

Configure port forwarding functionality

When the parent unit (core) is used in router mode, the port forwarding function can be configured: display the node list in PicoManager and click the configuration  for the parent unit (core). Select "Security" from the tabs on the left side of the screen, then select the "Port Forwarding" tab.



To add a rule, click the "+" button to display the settings table.

Refer to the following table for each setting item. The settings are applied in the order of the highest setting. The order of settings can be changed by drag & drop.

Setting items	Configuration details
Enable button	This button activates the setting. Grayed-out status does not reflect the setting.
WAN Port	Specifies the source port number

LAN IP address/ port	Specifies the IP address of the LAN-side device to be published as a server, etc. Specifies the destination port number when forwarding packets to a specific device on the LAN side to be published as a server, etc.
protocol	Specifies the protocol to which the rule is applied Protocols that can be specified: TCP, UDP, any (all)
delete button	Click on the trash to delete settings

7.6 Access Point Settings

Display the main menu and select "Settings". Select "5GHz/2.4GHz AP Settings" or "Common AP Settings" from the submenu.

After changing the settings, click the "Save" button. To apply the saved settings to the device, click the "Apply changes" button. All settings saved in each screen will be applied to the device.

5GHz/2.4GHz wireless configuration

Set the radio frequency band for the AP line. This unit can be configured for 5 GHz and 2.4 GHz band Wi-Fi connections.

When using both 5GHz and 2.4GHz bands, "5GHz AP Settings" and "2.4GHz AP Settings" must be set respectively in the side menu.

5GHz AP setting screen】 【2.4GHz AP setting screen】 【 5GHz AP setting screen】 【2.4GHz AP setting screen】 【2.4GHz AP setting screen】

5GHz AP設定

無線設定 SSID設定

Select the Wireless

無線周波数帯	<input checked="" type="checkbox"/> 有効
環境	屋内
無線モード	802.11ax
帯域幅	40MHz
チャンネル	auto
スキャン間隔 チャンネルautoのみに有効	24時間に1回
DTIM期間	2
RTS閾値	2347
送信出力	100% (-0dB)
端末接続切断	<input checked="" type="checkbox"/> 有効
RSSI閾値	-65
ビーコン フレーム送信間隔	100
最大再送信カウンタ	7

See the following table,

2.4GHz AP設定

無線設定 SSID設定

無線周波数帯	<input checked="" type="checkbox"/> 有効
無線モード	802.11ax
帯域幅	20MHz
チャンネル制限 チャンネル12, 13を利用しない	<input type="checkbox"/> 有効
チャンネル	auto
スキャン間隔 チャンネルautoのみに有効	24時間に1回
DTIM期間	2
RTS閾値	2347
送信出力	100% (-0dB)
端末接続切断	<input checked="" type="checkbox"/> 有効
RSSI閾値	-65
ビーコン フレーム送信間隔	100
最大再送信カウンタ	7

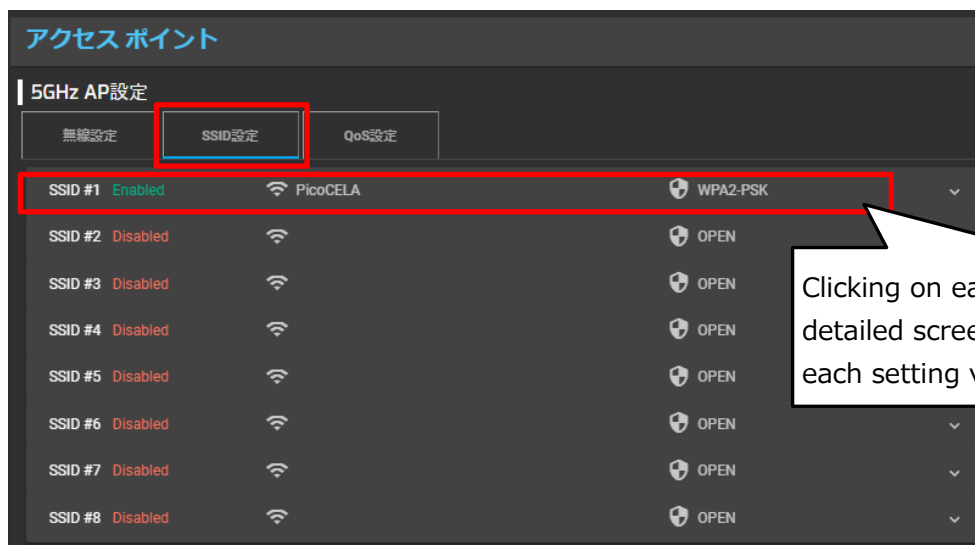
See the following table,

(data) item	Contents	Possible values	Factory setting
5G/2.4G AP Settings radio frequency band	Specifies whether or not each frequency band is used If disabled, the AP function for the frequency band in question will not be available	Check: Enable Unchecked: Disabled	Check: Enable
5G AP Settings environment	Specify the environment in which this equipment is to be installed in the 5 GHz band only When indoor is selected, W52, W53, and W56 channels can be selected. When outdoor is selected, only W56 channel can be selected.	5G: Indoor/outdoor	5G: Indoor
5G/2.4G AP Settings wireless mode	2.4GHz: Specify IEEE802.11b/g/n/ax 5GHz: IEEE802.11/a/n/ac/ax can be specified	2.4G: 11b/g/n 5G: 11a/n/ac	2.4G: 11ax 5G: 11ax
5G/2.4G AP Settings bandwidth	Specifies the bandwidth of the communication channel to be used The bandwidth that can be specified depends on the frequency band and radio mode	20MHz 40MHz 80MHz 160MHz	2.4G: 20MHz 5G: 40MHz
2.4G AP Settings channel restriction	Specify to restrict channel selection in the 2.4GHz band When channel restriction is enabled, channels 12 and 13 cannot be selected. Even if "Auto" is specified for the channel setting in the next section, 12ch and 13ch are not selected.	Check: Enabled Unchecked: Invalid	Unchecked: Invalid
5G/2.4G AP Settings channel	Specifies the communication channel to be used Configurable channels vary depending on wireless mode, bandwidth, and indoor/outdoor settings When you change the wireless mode, bandwidth, or indoor/outdoor settings, please re-configure the channel settings *Please specify a channel away from the channel set in the backhaul setting and the channel set in the 5GHz AP setting.	Configurable channels are defined by radio mode, bandwidth, indoor/outdoor When set to Auto, the channel is automatically selected at startup.	2.4G: Auto 5G: Auto
5G/2.4G AP Settings Scanning Interval	Specifies the optimum channel search interval (channel scan interval) when "Auto" setting is selected for channel setting Shortening the channel search interval may affect high-speed DFS performance.	Once every 24 hours Once every 12 hours Once every 8 hours Once every 6 hours	Once every 24 hours
5G/2.4G AP Settings DTIM Period	DTIM (Delivery Traffic Indication Message) transmission interval can be set	2.4G: Values from 1 to 255 5G: Values from 1 to 255	2.4G: 2 5G: 2
5G/2.4G AP Settings RTS Threshold	Can specify the standard packet size when sending RTS (Request to Send) packets	2.4G: 0 to 2347 values 5G: 0 to 2347 values	2.4G: 2347 5G: 2347
5G/2.4G AP Settings Transmission output	Specifies the transmission output Controlling the output can reduce the radio coverage area	2.4G: 10%/25%/50%/100 5G: 10%/25%/50%/100	2.4G: 100 5G: 100

5G/2.4G AP Settings terminal disconnection	When terminal disconnection is enabled, the RSSI value of the STA side (PC or other terminal side) is checked, and if it is lower than the specified RSSI value, the connection of the STA is disconnected from the AP side, allowing the STA to move to an AP with a higher signal level		
5G/2.4G AP Settings RSSI threshold	Specifies the RSSI threshold for disconnection when terminal disconnection is enabled in the previous section	-45dBm to -95dBm	2.4 GHz: -65dBm 5GHz: -65dBm
5G/2.4G AP Settings Beacon frame transmission interval	Specifies the beacon cycle (unit: msec). A shorter beacon cycle makes it easier for Wi-Fi-connected terminals to detect the access point, but reduces communication efficiency.	2.4G: 15-65535 5G: 15-65535	2.4G: 100 5G: 100
5G/2.4G AP Settings maximum retransmission counter	Specifies the number of retransmissions in case of frame transmission failure (e.g., Ack not received).	2.4G: 1-14 5G: 1-14	2.4G: 7 5G: 7

SSID setting

Set the SSID for the AP line. This unit can be configured for 5GHz and 2.4GHz band Wi-Fi connections.



SSID settings: General settings (name, security settings related, etc.)

Display the detail screen and set the SSID name, authentication and encryption method, passphrase, etc.

アクセスポイント

5GHz AP設定

無線設定 SSID設定 QoS設定

SSID #1 **Enabled** PicoCELA WPA2-PSK

一般設定 Radius設定 VLAN MA

SSID ☒ 有効

名前 PicoCELA
先頭と末尾のスペースは自動的に削除して保存されます

認証と暗号化方式 WPA2-PSK

パスフレーズ

文字の長さは8から63までです

ステルスSSID ☐ 有効

端末間通信禁止 ☐ 有効

端末数 128

Enable or disable SSID

Set any SSID name

Set the authentication/encryption

Set passphrase for accessing SSID

Set to enable stealth SSID usage

Permission/prohibition of terminal-to-

Set the maximum number of

Settings are the same for 5G/2.4GHz.

(data) item	Contents	Possible values	Factory setting
Wireless Settings SSID	Specify SSID enable/disable setting If disabled, the target SSID will not be sent A total of 16 SSIDs can be registered: 8 SSIDs at 5 GHz and 8 SSIDs at 2.4 GHz.	Check: Enabled Unchecked: Invalid	SSID #1: 5G: Enabled 2.4G: Enabled SSID #2 or later: invalid
Wireless Settings Name	Specify SSID.	Half-width alphanumeric characters, Japanese	SSID #1: 5G: PicoCELA_A 2.4G: PicoCELA_G SSID #2 or later unset
Wireless Settings Authentication and encryption methods	Specify authentication and encryption methods If "Open" is set, communication security with the terminal is not guaranteed; WPA2 and WPA3 are recommended. WEP is not supported If Enterprise is specified, please configure the Radius server *OWE mode (Wi-Fi Enhanced Open) is a new WF security standard for public networks based on Opportunistic Wireless Encryption (OWE) Ensures privacy through encryption in unsecured, open networks [OWE Configuration Example] <OWE only mode>	Open WPA2-Personal WPA/WPA2-Personal WPA2-Enterprise WPA/WPA2-Enterprise WPA3-Personal WPA2/WPA3-Personal WPA3-Enterprise WPA2/WPA3-Enterprise WPA3-Enterprise (192bit mode) OWE	SSID #1: WPA2-Personal SSID #2 or later: OPEN

	<p>1. set "OWE" as the authentication and encryption method</p> <p>Set "None" for OPEN SSID</p> <p>In this case, only terminals that support OWE can be connected.</p> <p><OWE Transition mode></p> <p>1. set SSID#1 to "OWE" (*Stealth setting is not available)</p> <p>Set SSID#2 to "OPEN</p> <p>Set "SSID#2" to the OPEN SSID of SSID#1</p> <p>Disclose SSID#2 to users</p> <p>Each terminal connects to SSID#2, and OWE-enabled terminals use OWE mode.</p> <p>The OWE-supporting terminal is connected with SSID#1 at SSID#1 and the OWE-unsupporting terminal is connected with SSID#2</p> <p>Non-OWE-compliant terminals are connected with "Security Protection</p> <p>The network is not "done".</p> <p>SSID#1 and SSID#2 cannot have the same name.</p>		
Wireless Settings OPEN SSID	<p>This setting is required when "OWE" is selected for authentication and encryption method</p> <p>Please refer to [OWE Setting Example] above for the setting method.</p> <p>*The same OPEN SSID cannot be specified from multiple SSIDs set in OWE</p>	None SSID set to OPEN on the device	None
Wireless Settings pass phrase	<p>When WPA2-Personal, WPA/WPA2-Personal, WPA3-Personal, or WPA2/WPA3-Personal is specified, a password is specified</p> <p>Be sure to change the passphrase to any passphrase from the factory setting to protect your communication security.</p>	<p>When WPA2-Personal, WPA/WPA2-Personal, or WPA2/WPA3-Personal is selected:</p> <p>At least 8 and up to 63 single-byte alphanumeric characters</p> <p>When WPA3-Personal is selected:</p> <p>Up to 128 single-byte alphanumeric characters</p>	SSID#1: picocela SSID#2 or later unset
Wireless Settings stealth SSID	You can specify whether to use stealth mode, which does not perform beacon notification for SSID (ESSID).	Unchecked: Invalid Check: Enabled	2.4G: Disabled 5G: Disabled
Wireless Settings Number of terminals	The maximum number of terminals that can be connected can be specified for each SSID	1-128	2.4G: 128 5G: 128

If you specify one of the following for "Authentication and Encryption Methods", please configure the Radius server settings. This section describes the settings for the primary. When setting up a secondary, please refer to the primary.

- WPA2-Enterprise
- WPA/WPA2-Enterprise
- WPA3-Enterprise
- WPA2/WPA3-Enterprise

アクセスポイント

5GHz AP設定

無線設定 SSID設定 QoS設定

SSID #1 Enabled PicoCELA WPA2-EAP

一般設定 **Radius設定** VLAN MAC フィルタリング

共有Radiusの使用 ☒ 有効

以下は共有のRadius設定項目です。変更は全てのSSIDに反映します。

Radiusサーバ e.g. 192.168.1.1 or server.domain

Radiusポート 1812

Radiusパスワード

Radiusアカウントサーバー e.g. 192.168.1.1 or server.domain

Radiusアカウントポート 1813

Radiusアカウントパスワード

Radius NAS-identifier

Specify whether to use shared or individual Radius

Specify the IP address of the Radius server to be

Specify port number of Radius server to use

Specify the password for the Radius server to be

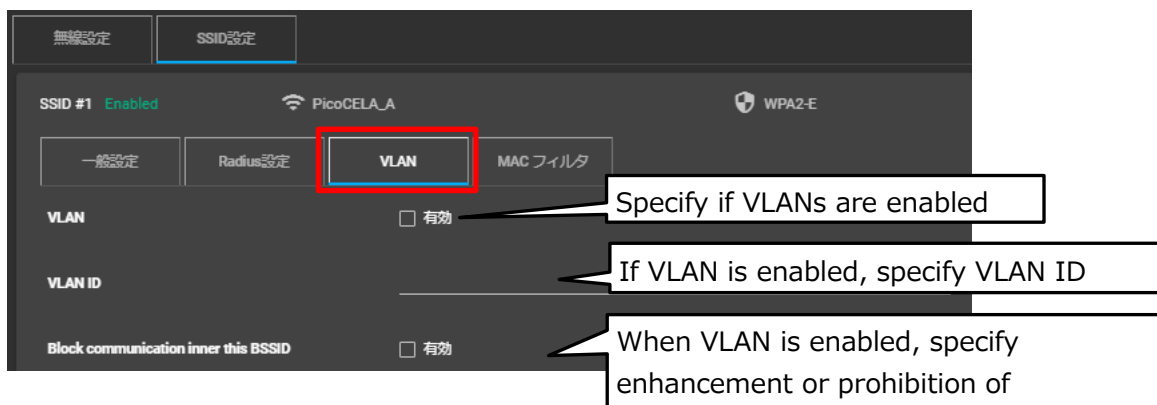
The following Radius accounting servers are

(data) item	Contents	Possible values	Factory setting
Radius Settings Use of shared Radius settings	WPA2-EAP/WPA-EAP mixed mode and WPA2/EAP selection Specifies whether to use the shared Radius setting when	Unchecked: Not used Check: Use	Check: Use
Radius Settings Radius Server Radius Port Radius Password	WPA2-EAP/WPA-EAP mixed mode and WPA2/EAP selection Hours, Specify the IP address of the shared or individually configured Radius server Specifies the port number of the shared or individually configured Radius server Specify password for shared or individually configured Radius servers		IP address: Not set Port number: 1812 Password: Not set
Radius Settings accounting server accounting port	WPA2-EAP/WPA-EAP mixed mode and WPA2/EAP selection Hours,		IP address: Not set

accounting password	Specifies the IP address of the shared or individually configured Radius accounting server Specifies the port number of the shared or individually configured Radius accounting server Specify password for shared or individually configured Radius accounting server		Port number: 1813 Password: Not set
Radius Settings NAS-Identifier	You can set the string that will be used as the NAS Identifier in the Radius request. The setting is optional and can be left unset.	half-width alphanumeric character Blank, Japanese is not acceptable.	unset

SSID setting: VLAN setting

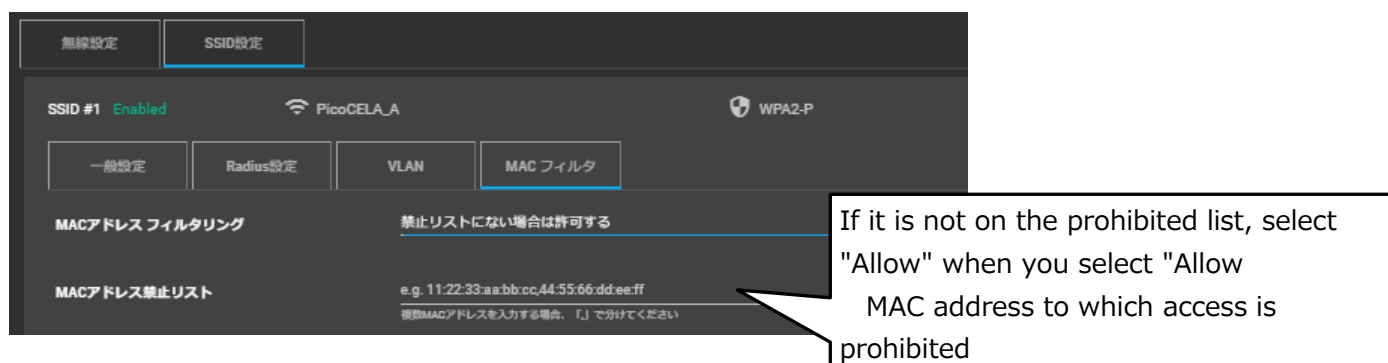
To configure VLAN settings for each SSID, click the "VLAN Settings" tab to display the VLAN Settings screen.



(data) item	Contents	Possible values	Factory setting
VLAN] VLAN	Specifies whether VLANs are used	Unchecked: Invalid Check: Enabled	5G: Disabled 2.4G: Disabled
VLAN] VLAN ID	Select the VLAN ID specified in the VLAN table Please set the VLAN configuration in the VLAN table in advance	VLAN ID specified in the VLAN table	
VLAN] terminal-to-terminal communication prohibited	Specify whether to allow or prohibit communication between terminals connected within the same BSSID In the VLAN table settings, under "Communication settings within the same BSSID". This setting is available only when "Communication settings within the same BSSID are configured in each BSSID setting" is specified.	Unchecked: Permitted Check: Prohibited	

SSID setting: MAC address filtering setting

For each SSID, you can configure settings to allow or prohibit access to the SSID by the MAC address of the connecting terminal. Select the "MAC Filter" tab to display the MAC Address Filtering Settings screen.



(data) item	Contents	Possible values	Factory setting
MAC Filter MAC address filtering	Specify MAC address filtering settings	invalid Allowed if not on the prohibited list Prohibited if not on the permitted list Using the Radius server's MAC address filter	invalid
MAC Filter MAC address block list	Specify the MAC address to prohibit connection When "Allow if not in the prohibited list" is selected, the registered MAC address will be prohibited from accessing the system. Please refer to the following example to describe the format of the MAC address (the same applies to the description in the case of prohibition) Use ":" (colon) to separate bytes in the MAC address and "," (comma) to separate between MAC addresses. Do not insert a space after the comma. (Example) "AA:AA:AA:AA:AA:AA,BB:BB:BB:BB:BB:BB"	MAC address The number of addresses that can be set is Max 1000 addresses	no designation
MAC Filter MAC address authorization list	Specify the MAC address to be allowed to connect When you select "If it is not in the allow list, prohibit", the registered MAC address will be allowed access	MAC address The number of addresses that can be set is Max 1000 addresses	no designation

MAC Filter Use Radius server	Specify "Use Radius server MAC address filter Please refer to the chapter "12 Application Usage Settings" in the built-in Radius server configuration method described below for how to use the MAC address filter function of the Radius server and configure it.	Follow Radius server specifications	
---------------------------------	---	-------------------------------------	--

Common AP Settings

This section describes the items to be set for the 5GHz and 2.4GHz bands in common. Settings cannot be made for each frequency band or SSID. Select "Common AP Settings" from the side menu to display the settings screen.

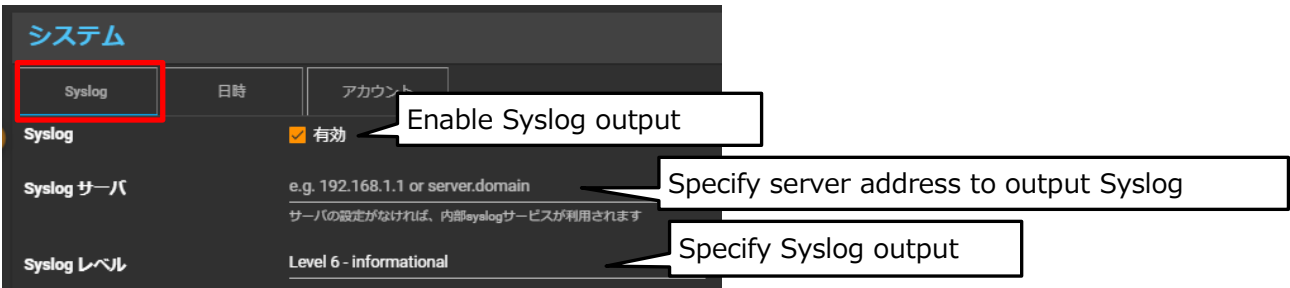
(data) item	Contents	Possible values	Factory setting
Common settings Keep-alive period (seconds)	Specifies the keep-alive transmission cycle	60 to 3600	120
Common settings Antenna Type	Specifies the antenna to be connected to the access point side of the device Select "Standard" when using the antenna supplied as a standard accessory *Directional antennas can be used with the PCWL-0510 outdoor unit *Operation with a directional antenna connected while the standard is selected may violate radio laws.	standard directivity	standard
Common settings 802.11k (proximity reporting)	Specify whether or not to use the fast roaming function by IEEE802.11k *High-speed roaming function reduces network downtime during roaming if the PC or smartphone terminal also supports IEEE802.11k.	Unchecked: Invalid Check: Enabled	

7.7 system setup

Display the main menu and select "Settings". Select "System" from the submenu. After changing the settings, click the "Save" button. Click the "Apply changes" button to apply the saved settings to the device. All settings saved in each screen will be applied to the device.

System Log Settings

You can configure the system log output settings. This section describes how to configure the settings. Click on the "Syslog" tab to configure the settings.



(data) item	Contents	Possible values	Factory setting
Syslog validation	Logs can be configured to be output to an external server	Disable: Unchecked Enable: Check	validation
Syslog Server address	IP address of the external server that outputs Syslog can be set		unset
Syslog Syslog Type	You can set the level of log output to an external server	Level0: emergencies Level 1: alerts Level 2: critical Level3: ERRORS Level 4: warnings Level 5: NOTIFICATIONS Level 6: informational Level7: Debugging	Level 6

Time setting

You can retrieve time data and configure time-related settings. The following describes how to set this up (select the Date/Time tab).

The screenshot shows the 'システム' (System) settings page with the '日時' (Date/Time) tab selected. The settings are as follows:

- NTP**: ☐ 有効 (Enabled). Callout: Enable setting for getting time.
- NTP サーバ**: e.g. 192.168.1.1 or server.domain. Callout: Specify NTP server address or domain.
- 時間更新間隔**: 24 Hours. Callout: Specifies the cycle for obtaining time.
- タイムゾーン**: Asia/Tokyo. Callout: Specify the time zone of your.
- 日時**: Thu Jun 18 18:19:25 JST 2020. Callout: Current date. A clock icon next to the time indicates a button to set date and time.

(data) item	Contents	Possible values	Factory setting
Date and Time NTP Enable	You can set whether to retrieve time information from an NTP server	Disable: Unchecked Enable: Check	nullification
Date and Time NTP Server	Specify the IP address or NTP server domain name of the NTP server		unset
Date and Time time update interval	You can set the update interval to retrieve time information from an NTP server	3 hours 6 hours 12 hours 24 hours 48 hours	24 hours
Date and Time time zone	You can set the time zone for the region where the equipment will be installed	Time zone of each country	GMT+9:00 Tokyo, Seoul
Date and Time Date and Time	Displays the current date and time inside the unit Click on the clock button for manual setting		

Account Settings

You can set up or change the account for logging in to the monitoring system. This section describes how to set it up.

システム

Syslog 日時 **アカウント**

ホスト名
このデバイスの名前 PCWL-0400 Specify the host

ユーザ名
このアカウントの名前 admin Specify login ID

パスワード
このアカウントのパスワード Specify login password

(data) item	Contents	Possible values	Factory setting
host name host name	You can set the name of the host name	half-width alphanumeric character	PCWL-0500
account login name	You can set the login name to access the WEB UI settings screen. (If you change the login name, the next time you log in, you will be able to access only with the login name you set.	half-width alphanumeric character	admin
account (computer) password	You can set a password to access the WEB UI settings screen. The next time you log in, you will be able to access the screen by entering the password you set. Be sure to set and keep your password!	half-width alphanumeric character	picocela

8 Check status (operating condition)

The operational status of the monitoring system can be checked on the status screen. You can also select items displayed on the status screen to display them on the dashboard. This section describes the items displayed on the status screen and how to display them on the dashboard.

Display the main menu and select "Status."

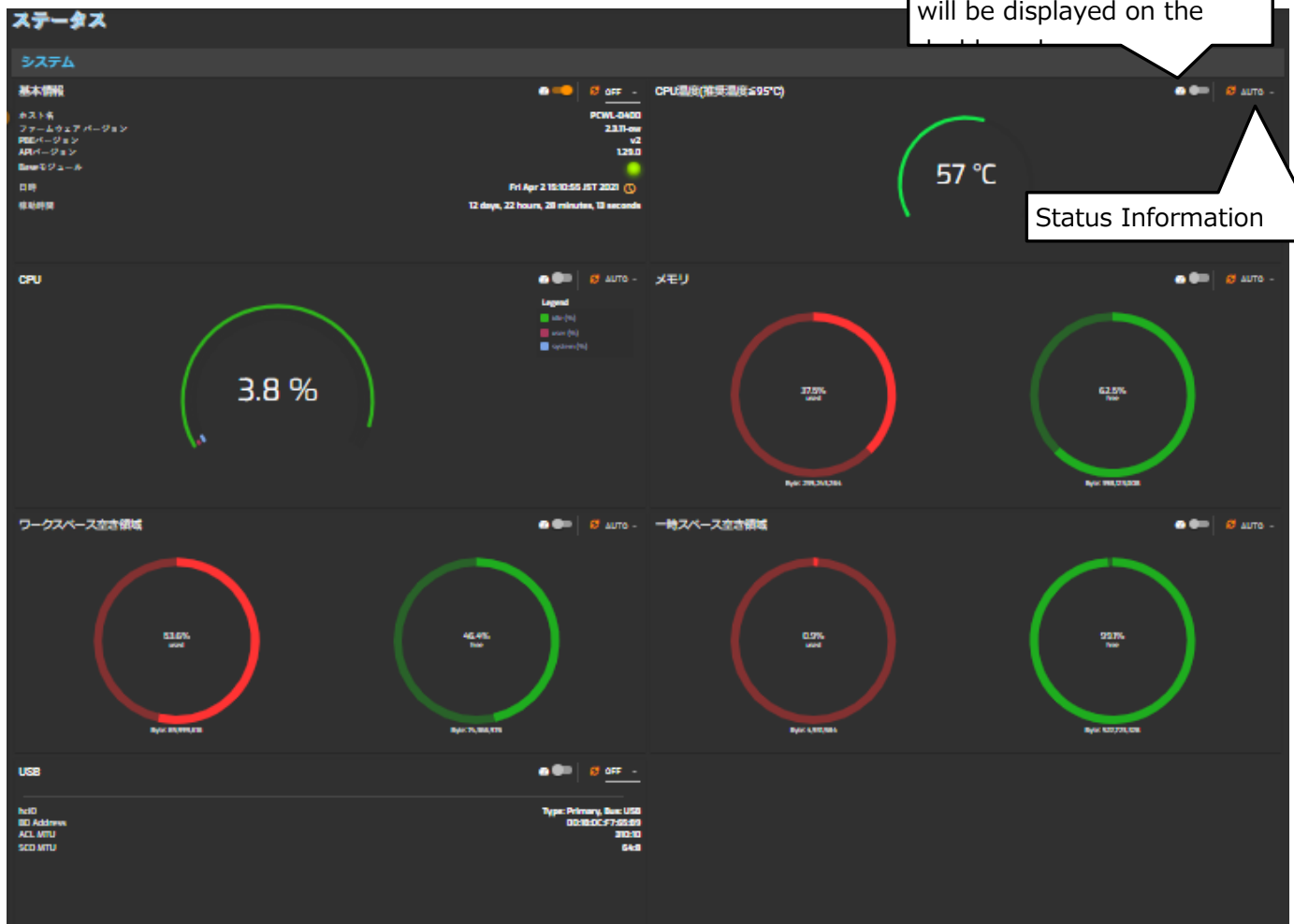
8.1 system status

Select "Status→System" from the main menu to display system-related information.

System-related status can be checked for the following

- Basic Information
- Temperature information of equipment
- CPU utilization
- Memory usage
- Disk utilization
- USB Related Information
- Event Record

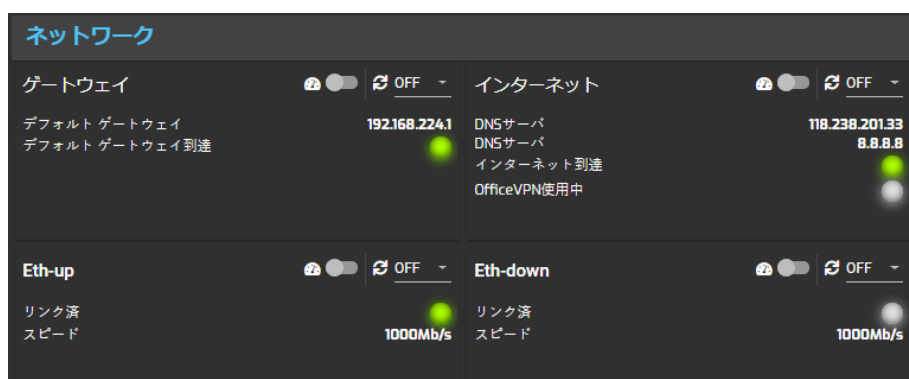
Switch for display on dashboard
Items that are turned on will be displayed on the



8.2 Network Status

Select "Network" from the submenu to view network-related status. The items displayed are as follows

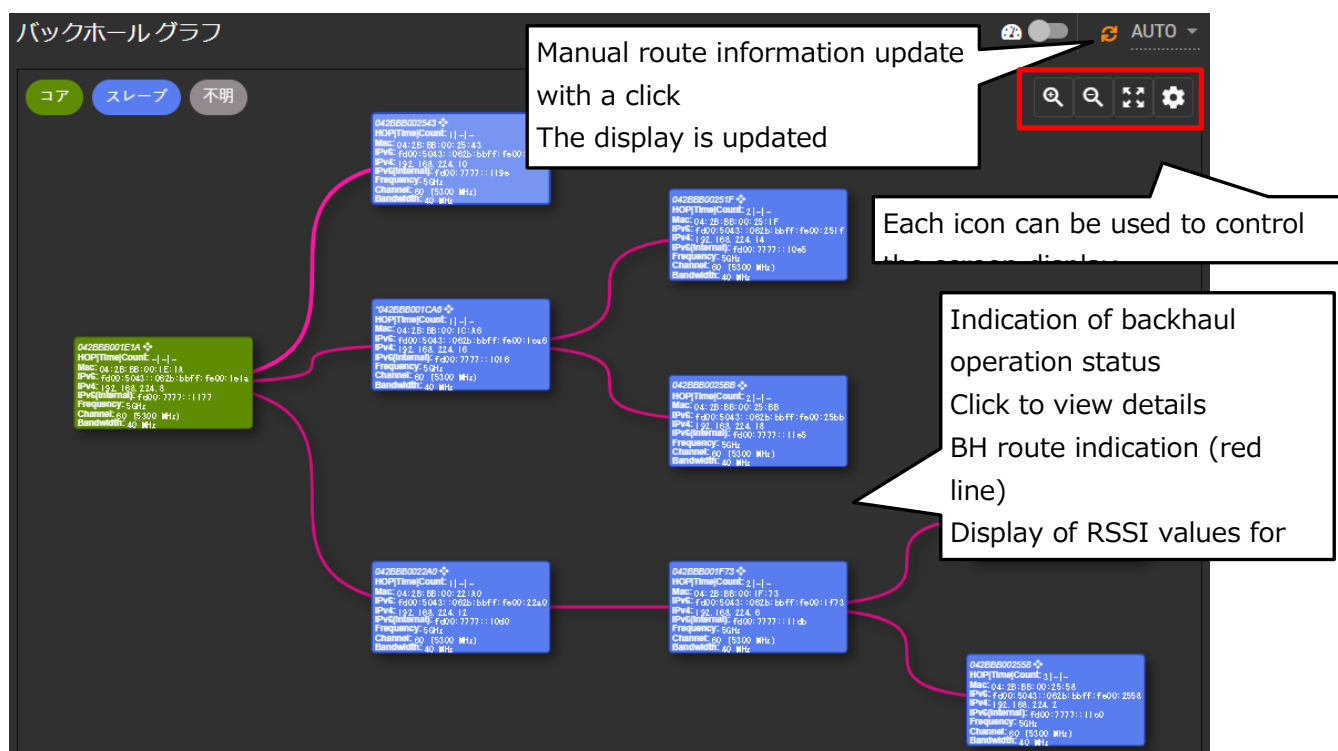
- Gateway Information
- Internet Related Information
- ETH-up port related information
- ETH-DOWN Port Related Information



8.3 Backhaul (relay line) status

Select "Backhaul" from the submenu to display backhaul-related information.

The following screen shows backhaul routes and information on each node.



Displays link information for each node in the backhaul.

バックホール リンク

15s

Filter

ノードID	親ノードID	シグナル	シグナル平均	受信ビットレート	受信バイト	送信バイト	接続時間	非活動時間	親ノード無線MAC
042BBB001E74	042BBB002FE	-39 [-43, -85, -81] dBm	-41 [-43, -86, -81] dBm	400.0 Mbit/s VHT-MCS 9 40MHz short GI VHT-NSS 2	1.39 MB	0.28 MB	525 seconds	100 ms	04:f0:21:4c:ea:77

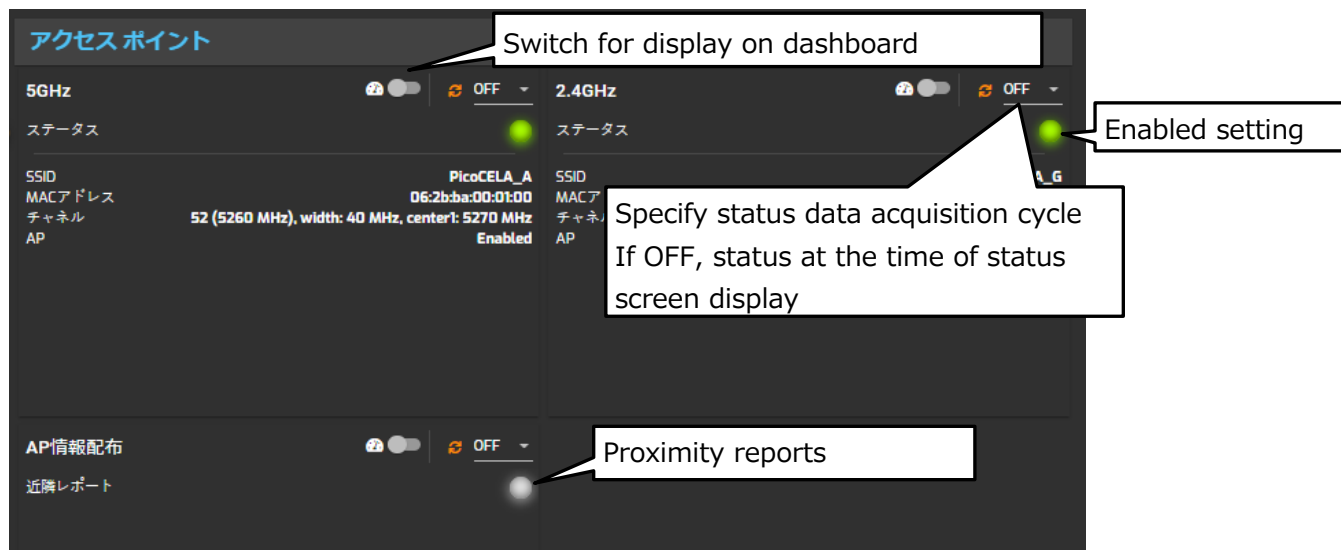
ページ毎の表示数 10 全 1 件中 1 - 1 件

(data) item	Contents
node ID	Own node ID (MAC address)
Parent node ID	Upper-level node ID (MAC address) connected by backhaul
signal	RSSI values with upper connected nodes (values in parentheses are per antenna)
signal mean	Average value of the above Signal over a period of time (values in parentheses are for each antenna)
received bit rate	Receiving side bearer rate *Not actual throughput
received byte	Total amount of data received since equipment startup
Sent Byte	Total data volume sent since equipment startup
connect time	Backhaul connection elapsed time
inactive time	Time after backhaul connection, when no data communication is occurring
Parent Node Wireless MAC	MAC address of the parent node's backhaul-side wireless LAN

8.4 access point status

Select "Access Points" from the submenu to display access point-related information.

- 5GHz Access Point Related Information
- 2.4GHz access point related information
- AP Information Distribution (802.11k) Related Information



8.5 Node access method via backhaul

Each node for which a backhaul route has been constructed can access each node via the backhaul network to check its status. The access method is described below.

① Confirmation of settings

To access each node via backhaul, please make sure that all nodes have the following settings

VLAN ID in VLAN table: Accessibility to each node according to the untagged operation mode setting

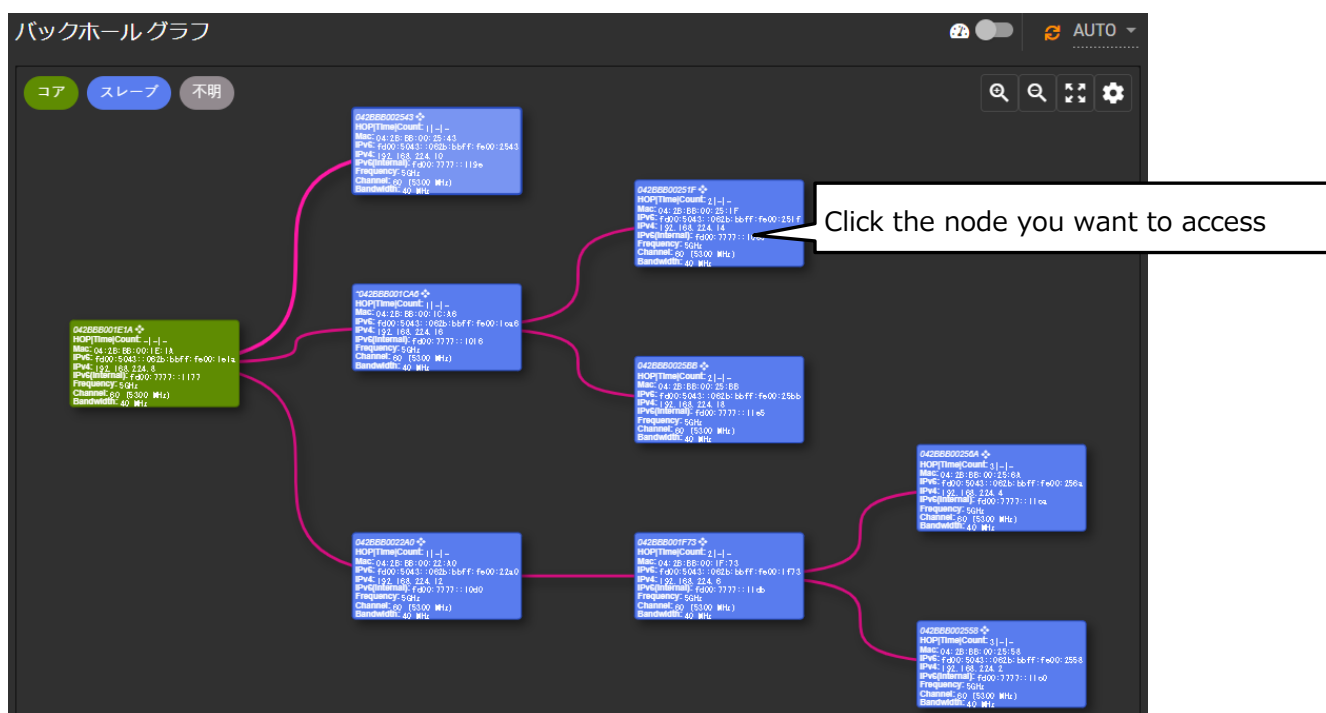
Operation mode: Access to each node via backhaul is allowed in office mode

Operation mode: No access to each node via backhaul when in guest mode


Operation mode: Custom mode and when "Disable inter-terminal communication via same backhaul" is enabled

does not allow access to each node

- ② Displays the following backhaul statuses



- ③ Click the node you want to access in the graph to display the following screen

 button to log in to the selected node

Node ID	042B8B00271A
Wlan BH address	04:f0:21:4b:3e:00
Wlan BH channel	36 (5180 MHz), width: 40 MHz, center1: 5190 MHz
Wlan BH type	mesh point
DFS agent	
PBE	
BH WPA supplicant	
Node mac address	04:2B:BB:00:27:1A
WAN IPv4	None
LAN IPv4	192.168.1.254
Eth-up IPv4	None
IPv6	fd00:5043:062b:bbff:fe00:271a
IPv6(internal)	None
Time	
Count	40

and log in to the node
When accessing with an IPv4 address

and log in to the node
When accessing with an IPv6 address

- ④ Enter the user name and password from the login screen to log in to the node.

For each node selected in the backhaul graph, you can make settings, check status, perform diagnostics (described below), and perform maintenance operations.

9 diagnostic function

The monitoring system can perform throughput measurement between backhaul devices (between nodes) and Internet speed measurement utilizing an Internet speed measurement site.

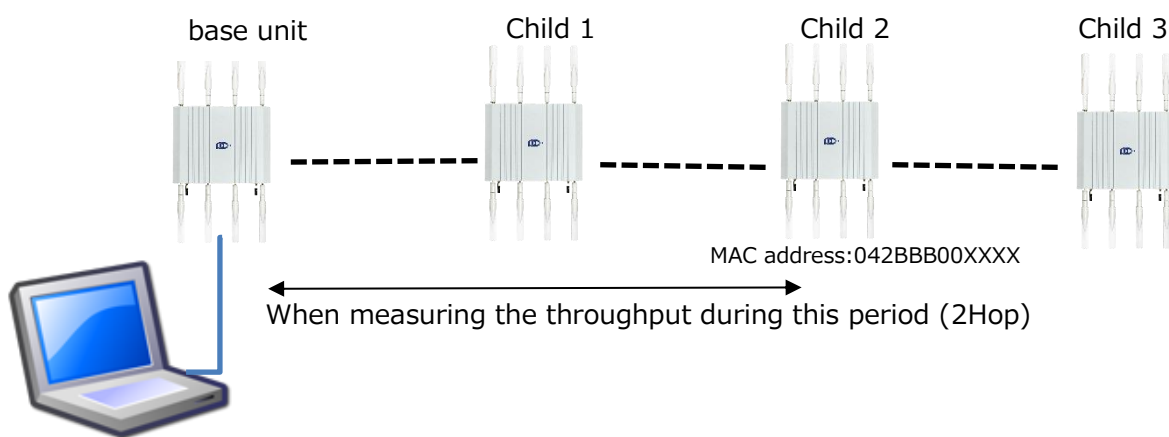
9.1 Network Throughput Measurement

Network throughput measurement can measure the throughput of backhaul lines between devices (between nodes) using iperf3 installed in the unit.

This section describes the procedure for measuring network throughput.

ステップ 1 : Log in to the management screen of the device to be measured.

The following connection configuration is used as an example.



Log in to one of the units to be measured (the parent unit in the example shown in the figure above), select Diagnostics from the main menu, and then select Network Throughput from the submenu to display the Throughput Measurement screen.



ステップ 2 : Designation of iperf3 client

Designate the device to be measured (in this case, Child 2) as an iperf3 client.

The screenshot shows the 'iPerf3クライアントとして実行する' (Run as iPerf3 client) section. It includes a 'サーバ' (Server) list with two entries: '#1 [OK]' and '#2 [OK]'. The MAC address '042BBB002543' is displayed. Below the list is an 'オプション' (Options) button. At the bottom, there are buttons for '履歴' (History), 'アップロード' (Upload), and 'ダウンロード' (Download).

Callouts and instructions:

- *Please execute when you connect a separate PC to the AP for measurement and start this unit as an
- After specifying a server from the list, the Run button is activated and when clicked, the measurement
- Click to display the MAC address of the node connected to the backhaul route. Specify the MAC address of Child 2 from the list
- Measured results are displayed as history. Click on the button to view its history. History will be deleted when moving from one
- Click "History" to download and upload historical data

To specify Iperf options, click "Options" and set each parameter.

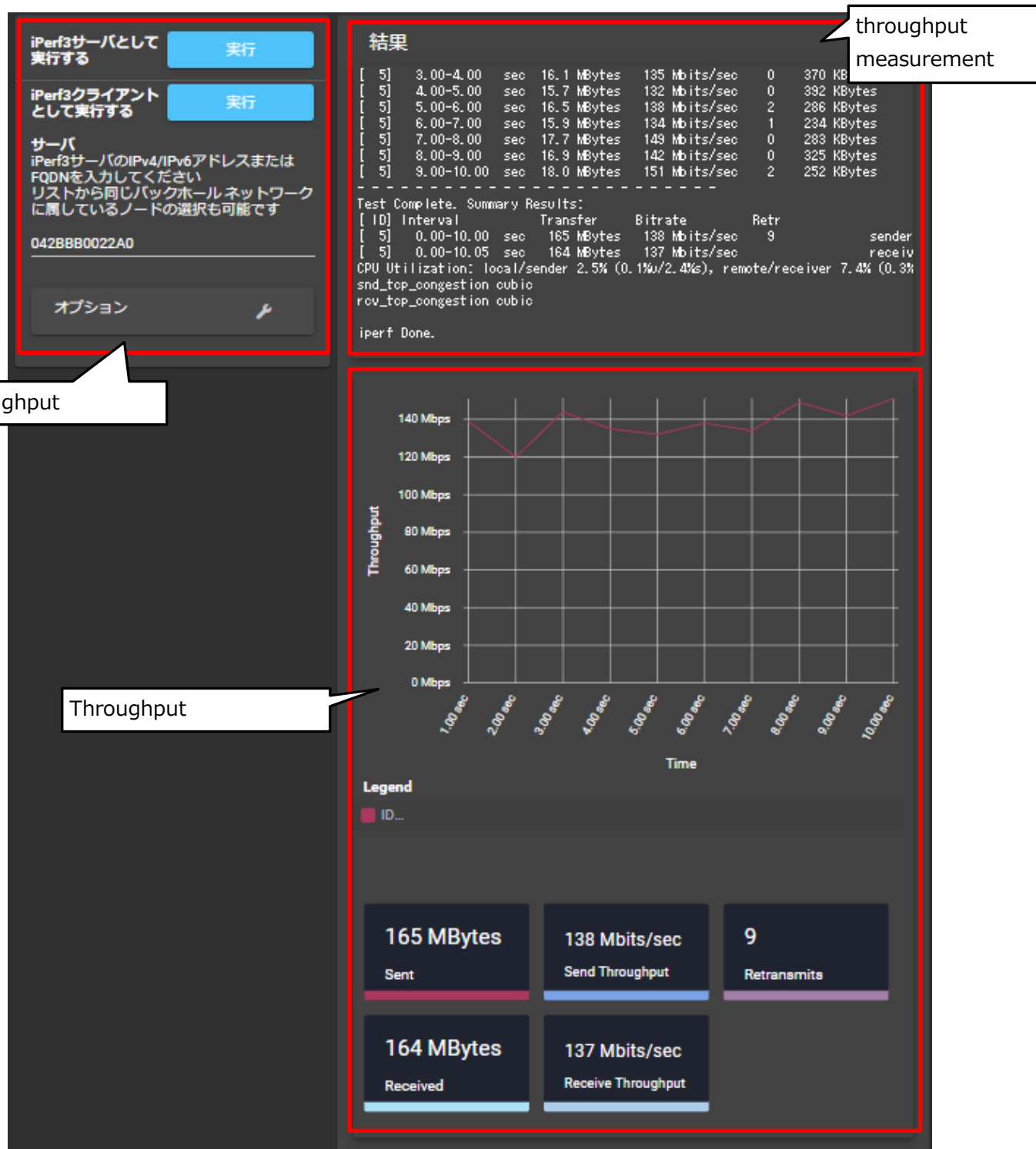
The screenshot shows the 'オプション' (Options) menu. It includes settings for 'タイム' (Time), 'プロトコル' (Protocol), 'リバース' (Reverse), 'ビットレート' (Bit rate), 'ウィンドウサイズ' (Window size), 'バッファサイズ' (Buffer size), '表示間隔' (Display interval), and 'オミット' (Omit).

Callouts and instructions:

- Specify the time to
- TCP or UDP specified as measurement
- Specify to measure in the reverse
- Specify bit rate (bandwidth limit). Default settings are unlimited TCP and 1 Mbps UDP
- Specify window size
- Specify buffer size
- Specify the interval for
- Specify to truncate the first n

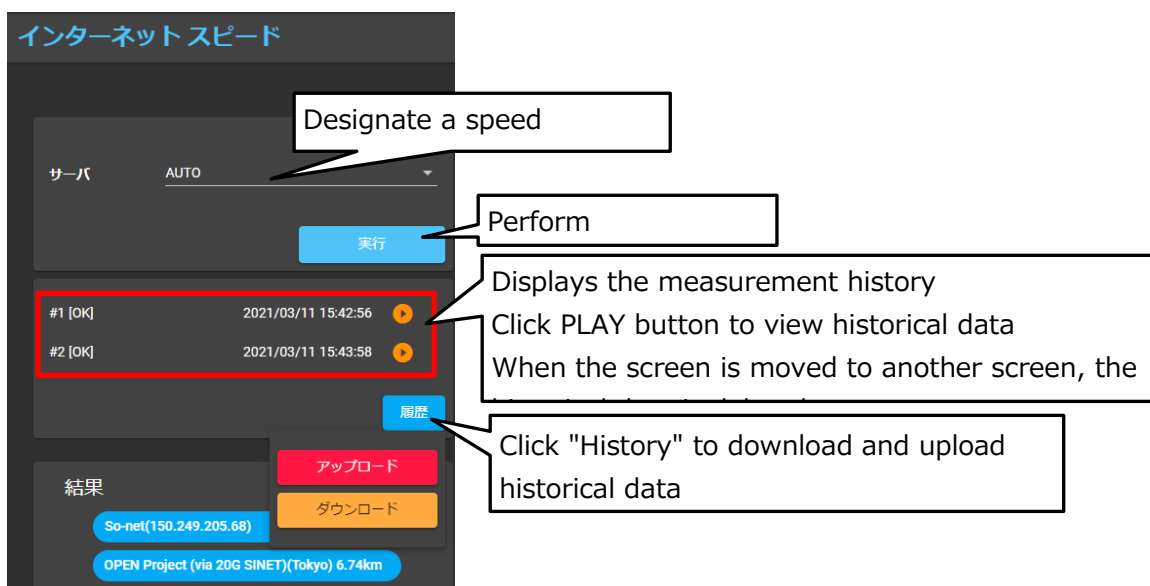
ステップ 3 : Display of network throughput measurement results

If the measurement is successfully performed, the following results are displayed, confirming the throughput of the backhaul line between devices in the installation environment.

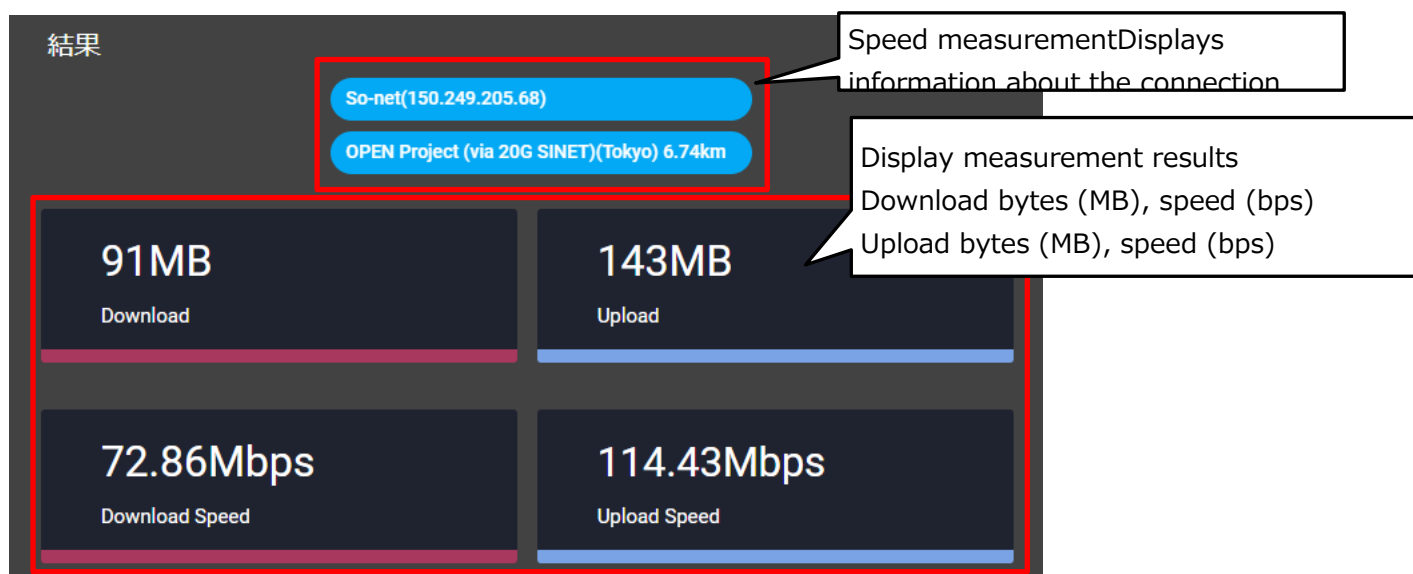


9.2 Internet Speed Measurement

This unit can perform Internet speed measurements. Perform measurement by an external speed measurement site and display the measurement results. Select Internet Speed from the submenu to display the Internet Speed Measurement screen. Specify the server to connect to and click "Execute" to run the measurement. The measurement results will be displayed as follows. When "Auto" is selected for the speed measurement destination (server), the device will automatically select a measurement site close to the installation location and perform the measurement.



The measurement results are displayed as follows



*[Attention.

Internet speed measurement is a measurement function that utilizes external sites and OSS. Therefore, the measurement results are not guaranteed by our company, as they are affected by the state of the line and the state of the external site. Please use these values as reference values for monitoring when the

unit is installed or in the installation environment. In addition, if a site specification change occurs, the measurement function may not be available until the firmware of the main unit has been updated.

9.3 access point scan function

This unit can collect information on access points in the vicinity. You can investigate suspicious access points, etc., and check radio interference conditions. Select "AP Scan" from the submenu to display the Access Point Information Collection screen.

Click "Execute" to collect information on nearby access points
***When executing AP scan, 2.4GHz or 5GHz AP function may experience a communication performance**

Displays the measurement history
 Click the button to display historical data
 When the screen is moved to another screen, the

Click "History" to view historical data.

Displays information on detected access points in the vicinity

The screenshot shows a table of detected access points with columns for name, MAC address, and signal strength (dBm). A list of nearby access points is displayed, including details like SSID, MAC address, and signal strength (dBm). Buttons for '実行' (Execute), '履歴' (History), 'アップロード' (Upload), and 'ダウンロード' (Download) are visible.

9.4 Confirmation of reachability

You can check the reachability between devices and measure the response time using the Ping command. Select "Reachability" from the submenu to display the reachability check screen.

of the instrument to measure response time.

Specify the number of times to send pings

Displays ping response results

Displays the measurement history
 Click the button to display historical data
 When the screen is moved to another screen, the

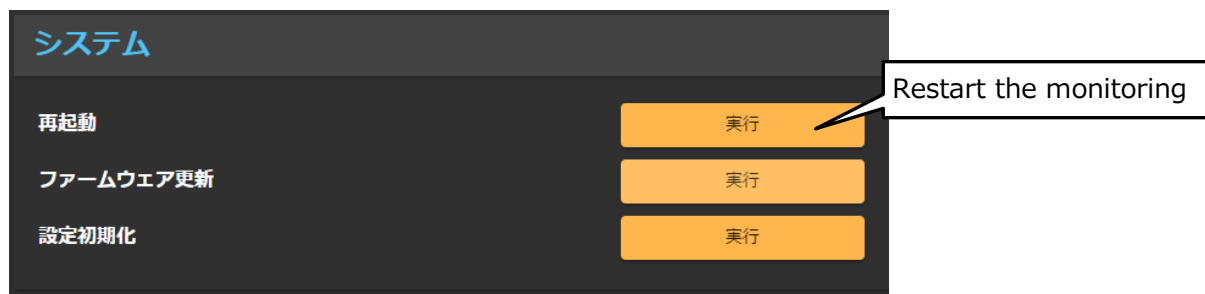
The screenshot shows the 'Host' field set to 'www.google.co.jp' and the 'Count' field set to '5'. A '実行' (Execute) button is present. Below the table, there is a '履歴' (History) button. The '結果' (Result) section displays the output of the ping command, including the IP address, data bytes, sequence number, TTL, and response time for each packet, as well as overall statistics like packet loss and round-trip times.

10 Maintenance Functions

This section describes maintenance-related operations such as firmware updates for this device. Select "Maintenance" from the main menu.

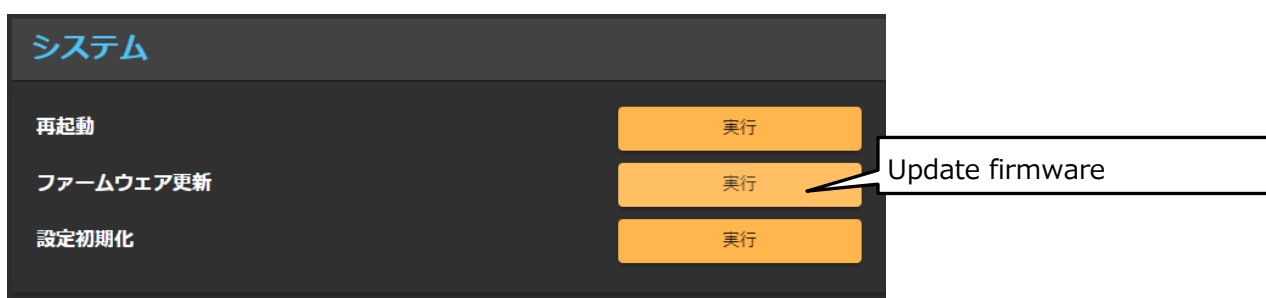
10.1 Reboot equipment

You can execute a restart of the monitoring system from the administration screen. Select "System" from the submenu and click "Execute" on the reboot. It takes approximately 2 minutes to restart the device.



10.2 Firmware update

The firmware update of the device can be performed from the Administration screen. Select "System" from the submenu and click "Run" for the firmware update.



Please follow the procedure below to update the firmware.

- ① Obtain the latest firmware version from PicoCELA or your distributor
- ② Click the Firmware Update button in Maintenance, select the latest firmware version you have obtained, and click "Open".



③ Perform a firmware update

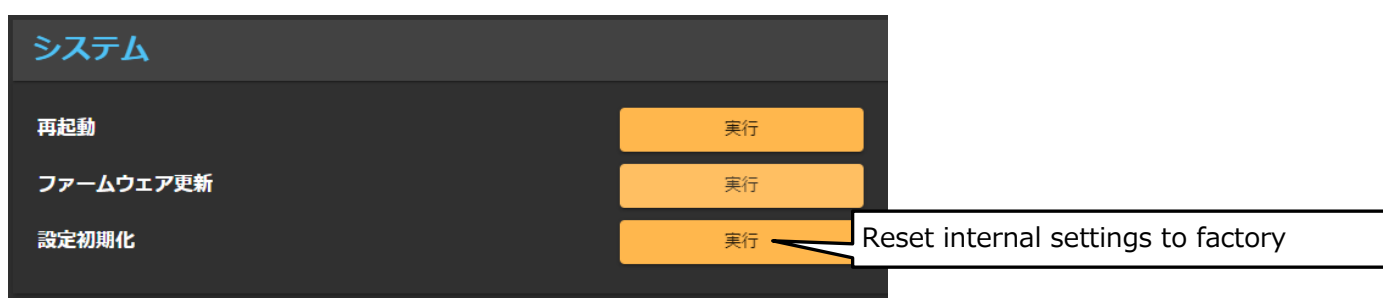
Click "Confirm" on the screen below to execute the firmware update. If you wish to initialize settings together with the firmware update, tick the Initialize Settings checkbox and click "Confirm" to perform the firmware update and initialization at the same time.



Firmware updates can also be performed from PicoManager (recommended method), and nodes connected to PicoManager (PCWL5 series products) can be upgraded at once. PicoManager is prepared with the latest firmware.

10.3 initialization

You can restore the settings of the device to the factory defaults from the administration screen. Select "System" from the side menu, and click "Execute" under "Initialize Settings".



Initialization of settings can also be performed by pressing the reset button on the device itself for at least 10 seconds.

10.4 Backhaul Maintenance

Backhaul routes can be manually reconstructed. Select "Backhaul" from the submenu.



Backhaul route reconstruction (rerouting) can also be performed with a reroute switch on the device itself.

10.5 logging

You can output the log of the internal part of the device for maintenance purposes. In case of equipment failure, click the button to download the log to your own PC and send it to PicoCELA.



11 Connection settings with PicoManager

In order to use PicoManager's cloud service functions, you need to register an account for PicoManager and a license for each device in advance. After the pre-registration is completed, the activation process for each device is executed. After the activation is completed, you can use services such as remote monitoring and device diagnostics from PicoManager.

PCWL-0500 comes bundled with the standard PicoManager functions. For more information, please contact the distributor where you purchased the PCWL-0500 or PicoCELA.

11.1 PicoManager account registration and license registration

How to register an account

Please follow the steps below to register an account with PicoManager.

1. Check the "Subject: Invitation to Account Portal" email sent by the distributor or PicoCELA
2. Access the URL in the invitation e-mail.
3. Agree to the Terms of Use on the account registration screen, and register the prescribed items (all required items) on the following screen.
4. After registering each item, click the "Save" button to complete registration.



The form is a vertical stack of input fields for account registration. It includes fields for 'ログインID' (Login ID), 'パスワード' (Password), 'アカウント名' (Account Name), '担当者名' (Responsible Person Name), '会社名' (Company Name), '部署名' (Department Name), '郵便番号' (Postal Code), '住所' (Address), '電話番号' (Phone Number), 'FAX', '言語' (Language), and 'タイムゾーン' (Time Zone). A '保存' (Save) button is at the bottom. A note below the account name field provides an example: 'お客様のアカウントの表示名。例：ピコセラ, ピコセラ 大阪支店'.

ログインID	<input type="text"/>			
パスワード	<input type="password"/>			
アカウント名	<input type="text"/>		担当者名	<input type="text"/>
お客様のアカウントの表示名。例：ピコセラ, ピコセラ 大阪支店				
会社名	<input type="text"/>		部署名	<input type="text"/>
郵便番号	<input type="text"/>			
住所	<input type="text"/>			
電話番号	<input type="text"/>		FAX	<input type="text"/>
言語	Japanese		タイムゾーン	Asia/Tokyo(UTC+0)
<input type="button" value="保存"/>				

Account Verification

Please follow the steps below to verify the account you have registered with PicoManager.

1. After registering an account, check the email with the following subject line sent by PicoManager

Subject: Notification of PicoManager Account Registration Completion

2. Access the PicoManager URL in the email
3. Sign in with your registered login name and password.
4. Select "Account Management" from the menu on the left side of the screen and confirm the contents of the registered information.

PicoManager® マニュアル確認

アカウント管理

API

セキュリティ

接続デバイス

オプション

アカウント管理

基本情報

アカウント名

担当者名

連絡先

会社名

部署名

郵便番号

住所

電話番号

メールアドレス

表示

言語 ja

タイムゾーン Asia/Tokyo

How to register a license

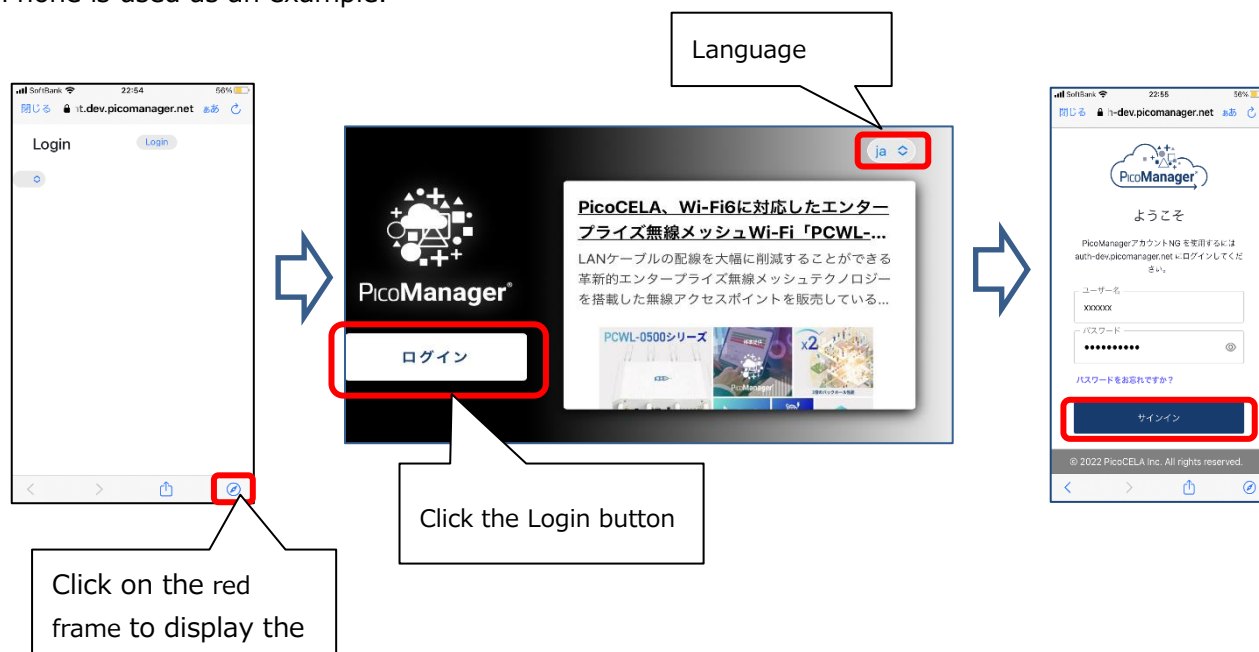
Please follow the procedure below to register PicoManager license for each device (node).

1. Confirm that you have completed the account registration described in the previous section.
If the account is not registered, the license cannot be registered.
2. Access the license registration site by scanning the QR code on the "WELCOME Card" that comes with the device with your smartphone camera.



- When the following login page appears, follow the steps to sign in with the login name and password registered in the account registration.

iPhone is used as an example.



- After signing in, the following license registration screen will appear. Confirm that the account name and the MAC address of the device to be registered are correct, and click the Register button to register the license.

PicoManager[®] アカウント名 ▼

License Register

アカウント名	アカウント名表記
担当者名	氏名表記
MACアドレス	機器のMACアドレス表記

上記内容でライセンスを登録します。

アカウントおよびMACアドレスが正しいことを確認の上、登録ボタンをクリックしてください。

アカウントが異なる場合は、正しいアカウントでログインしてください。

[登録](#) [ログアウト](#)

account.dev.picomanager.net

Verify that each item is correct.
If correct, click the "Register" button at the bottom of the screen to complete registration.

- After clicking the "Register" button, the license registration is complete when the following registration completion screen is displayed.

PicoManager[®] アカウント名 ▼

License Register

アカウント名	アカウント名表記
担当者名	氏名表記
MACアドレス	機器のMACアドレス表記

上記内容でライセンスが登録されました。

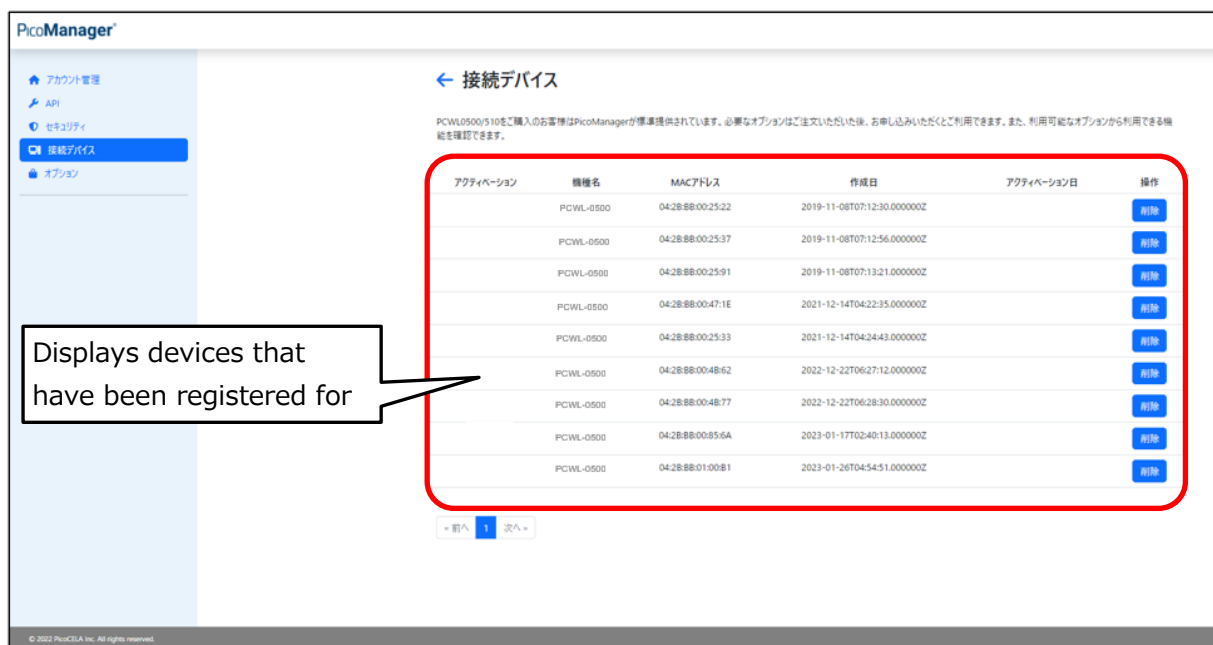
接続デバイスメニューから確認できます。

[接続デバイス](#)

© 2022 PicoCELA Inc. All rights reserved. [ユーザーガイド](#) [プライバシー](#)
[よくある質問](#) [お問い合わせ](#)

account.dev.picomanager.net

6. If you have purchased more than one device, follow steps 2 through 5 to register licenses for all devices.
7. After completing the license registration of all devices, access the account management screen, select "Connected Devices" from the menu, and check the device registration status. The process is complete when all registered devices are displayed. Perform the activation process for each device in the next section.



11.2 PicoManager Activation

The PicoManager activation process is required for all devices to use PicoManager services. The activation process consists of two operations: automatic activation and manual activation. Once the activation is completed, the standard PicoManager services are available.

auto-activation

Once an account and license have been registered in advance and the device is ready for Internet communication, the device will automatically connect to PicoManager and perform the activation process.

To see the result of the activation process, access the Account Management screen, select "Connected Devices" from the menu, and the following screen will be displayed.

Check if all the MAC addresses of the licensed devices are displayed. If not, check the Internet communication status of the device and whether or not a license has been registered. It may take several minutes to display the information.

If your network environment requires connection via a proxy server, please refer to "Manual Activation Operation" in the next section.

PicoManager

← 接続デバイス

PCWL0500/S10をご購入のお客様はPicoManagerが標準提供されています。必要なオプションはご注文いただいた後、お申し込みいただくご利用できます。また、利用可能なオプションから利用できる機能を確認できます。

アクティベーション	機種名	MACアドレス	作成日	アクティベーション日	操作
✓	PCWL-0400	04:2B:8B:00:25:22	2019-11-08T07:12:30.000000Z	2021-12-14 06:10:53	削除
✓	PCWL-0400	04:2B:8B:00:25:37	2019-11-08T07:12:56.000000Z	2022-06-01 08:52:44	削除
✓	PCWL-0400	04:2B:8B:00:25:91	2019-11-08T07:13:21.000000Z	2021-12-14 07:09:40	削除
✓	PCWL-0400	04:2B:8B:00:47:1E	2021-12-14T04:22:35.000000Z	2021-12-14 09:44:54	削除
✓	PCWL-0400	04:2B:8B:00:25:33	2021-12-14T04:24:43.000000Z		削除
✓	PCWL-0400	04:2B:8B:00:4B:62	2022-12-22T06:27:12.000000Z	2023-01-04 23:54:37	削除
✓	PCWL-0400	04:2B:8B:00:4B:77	2022-12-22T06:28:30.000000Z	2022-12-22 23:13:33	削除
✓	PCWL-0400	04:2B:8B:00:85:6A	2023-01-17T02:40:13.000000Z	2023-01-17 02:49:41	削除
✓	PCWL-0500	04:2B:8B:01:00:B1	2023-01-26T04:54:51.000000Z	2023-01-26 05:02:19	削除

activation status
✓Display is complete

Displays the date and time of the activation

© 2022 PicoCell Inc. All rights reserved.

Manual Activation Operation

Activation of PicoManager can be performed manually. Access the unit's WEB UI (administration screen), click "PicoManager Related Settings" in the main menu, and select "Activation" in the submenu to display the following screen.

アクティベーション

アクティベート

Perform activation to use PicoManager

VPNプロキシ ☐ 有効

VPNプロキシホスト example-proxy.picomanager.net

VPNプロキシポート 3128

Set for http/https communication and connection via VPN proxy

Do not turn off the device and maintain the Internet connection for several minutes until the activation operation is complete and appears in the "Connected Devices" section of PicoManager's Account Management screen.

The connection between PicoManager and the device communicates via https protocol. If your network environment requires http/https connection via a VPN proxy, please set the VPN proxy to "Enabled (✓)" and configure the VPN proxy host name and VPN proxy port settings.

12 Application Usage Settings

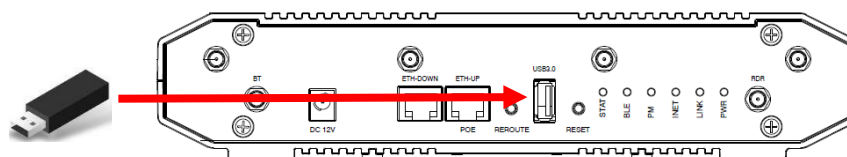
To use the built-in applications of the IF1-WF01, settings on the IF1-WF01 must be made on the IF1-WF01. To configure the settings on the device side, select "Applications" from the main menu to display the application settings screen.

12.1 Shared File Server Settings

By inserting a USB memory stick into the USB connector on the rear panel of the unit, it can be used as a shared file server within a local network.

USB memory sticks can be installed regardless of Core/Branch. They can also be attached to multiple devices to increase the capacity of a shared file server.

Supported file systems are exFAT/FAT32/FAT16/ext4. NTFS is not supported.



The following is the setup procedure for using a shared file server, which must be set up on all PCWL-0500s with USB flash drives installed.

1. Attach a USB memory device to the unit (insert and remove the USB memory device when the unit is turned off).
2. Turn on the monitoring system and connect a PC to access the management screen.
3. After making changes, click "Save" at the bottom of the screen to save the settings.
4. Select "Applications" -> "Samba" from the main menu to move to the following screen

13 Building a Wireless LAN Area with PCWL: The Basics

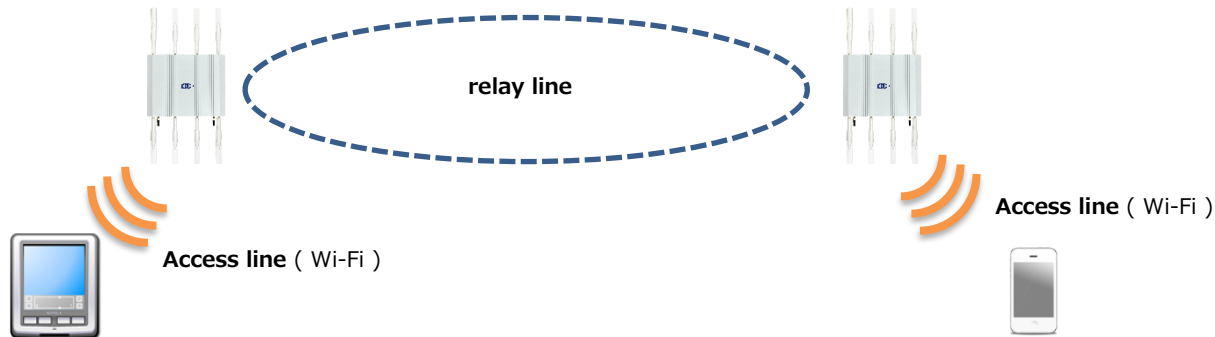
13.1 BH and AP

PCWL (devices in the following figures are shown as PCWL-0500, and PCWL-0510 as well) has two functions: a wireless relay function called a wireless backhaul (wireless BH) and an access point function called an AP.

The access point function (AP) serves as an access line for wireless LAN (Wi-Fi) and, like a general access point, has an SSID and is capable of WEP/WPA/WPA2 security. The frequency bands used are 2.4GHz and 5GHz, supporting 802.11b/g/n/ax in the 2.4GHz band and 802.11a/n/ac/ax in the 5GHz band.

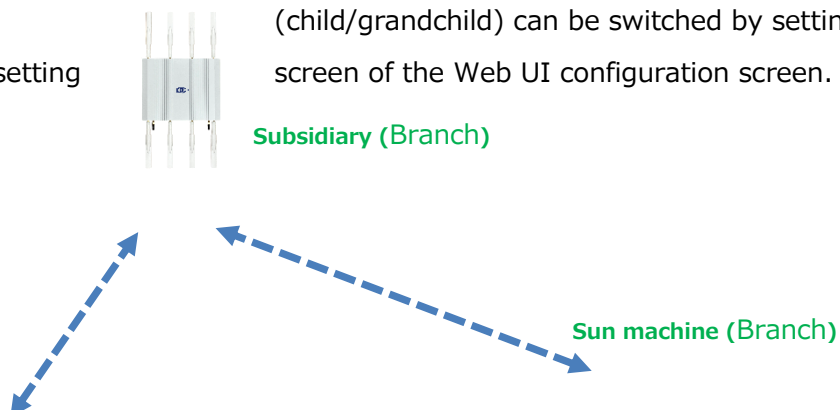
The wireless relay function (wireless BH) uses our proprietary algorithm to efficiently communicate and relay between PCWLs. **The** frequency band used is equivalent to W52, W53, and W56 of 802.11a/n/ac/ax in the 5 GHz band. Therefore, **W52 and W53 are for indoor use only when set to W52 and W53**. During relay, data is protected by AES128 encryption for secure communication.

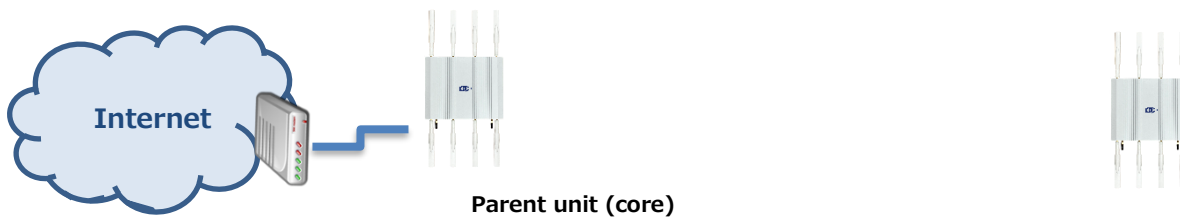
Both relay and access lines correspond to Layer 2 (data link layer) as a protocol stack.



13.2 Parent (core) and child (branch)

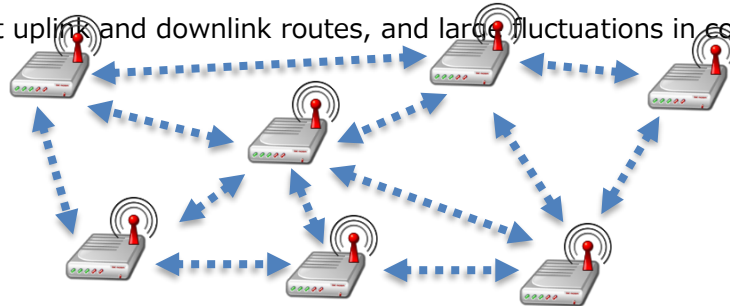
PCWLs are broadly classified into a core unit, which is the parent, and a branch unit, which is the child/grandchild connected to the core unit. Both the core and the branch are the same device, but the core (parent) and the branch (child/grandchild) can be switched by setting the operation mode in the backhaul setting screen of the Web UI configuration screen.



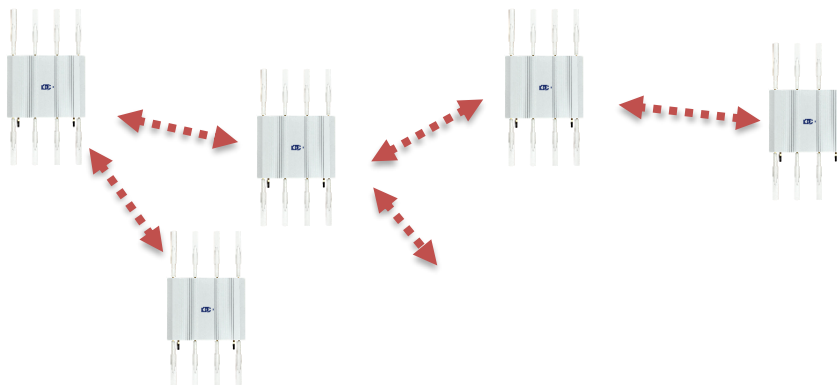


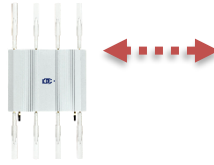
13.3 Optimal route construction and rerouting

In wireless communication between access points, each device generally determines the upper access point according to its own policy, and the network is constructed by overlapping them. It is also called a mesh network because of its mesh-like shape. While this form of network is said to be highly autonomous and fault-tolerant, it also has problems such as the possibility of redundant communication paths, inconsistent uplink and downlink routes, and large fluctuations in communication quality.



PCWL achieves stable communication by forming a quasi-static path with a tree structure centered on the core through intercommunication between devices (JP-A-2008-18337). The construction of a stable communication path with this tree structure and the inclusion of a radio module specialized for relaying enables high communication quality to be maintained even when the number of radio hops increases. Furthermore, by pressing the reroute button on one PCWL, the optimal route construction algorithm operates in waves, and all PCWLs in the same network reconstruct the optimal route based on the latest information. In other words, **anyone can build a wireless network at the touch of a button, which normally requires specialized wireless knowledge.**



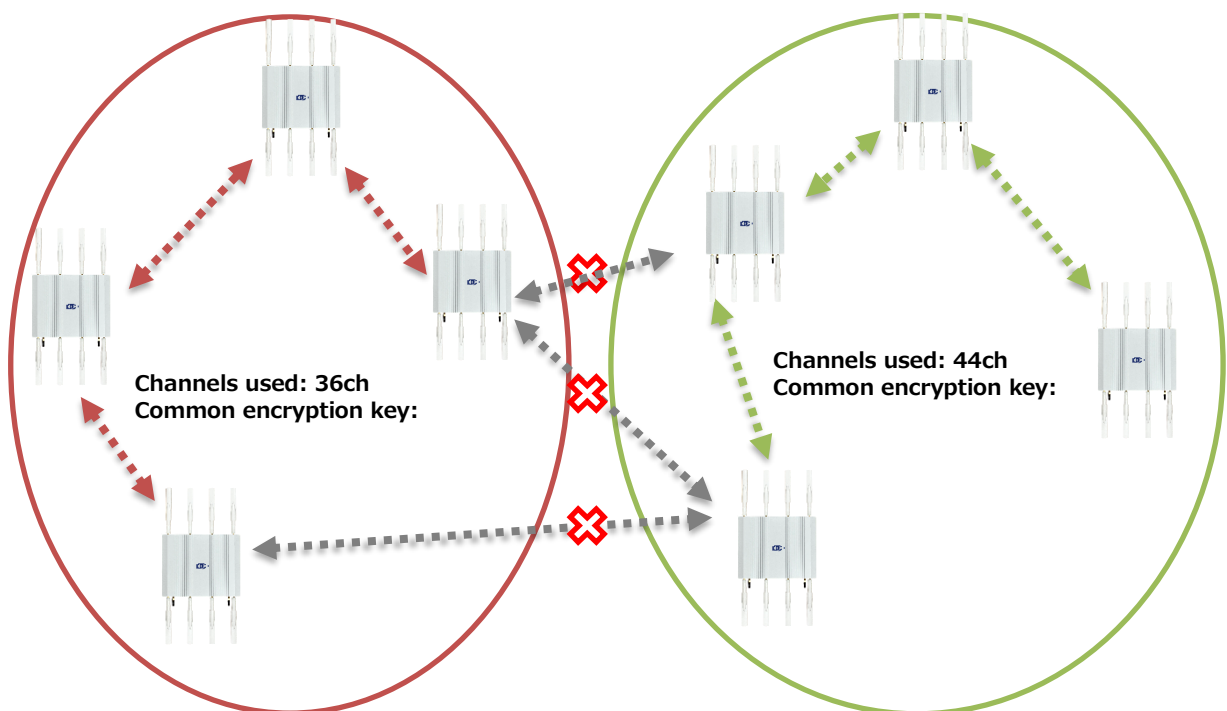


13.4 Network partitioning

One core can logically have 256 branches connected to it. However, for practical purposes, it is desirable to separate the network by a few to several dozen units for several reasons.

- Load is placed on the core corresponding to the root in the tree structure (speed may be reduced here)
- Increased hop count (reduced speed)
- If the number of PCWLs in a network is large, the number of Wi-Fi terminals using that network also increases, which increases the communication volume and places a burden on the relay lines. Also, networks may be divided in consideration of the number of users and communication volume (data volume and communication frequency).

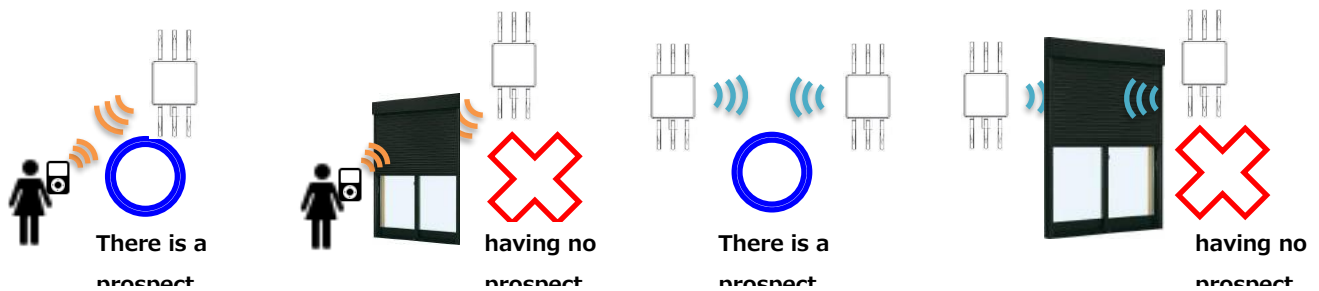
To separate the networks, change the relay line (Mesh) settings. If the channel used and the common encryption key are the same, they will be the same network. If these values are different, even if PCWLs are adjacent to each other, they will be different networks and wireless relay will not be performed.



13.5 Prospects

The frequency bands used in wireless LAN (both 2.4 GHz and 5 GHz bands) have strong linear propagation characteristics. Therefore, it is necessary for two wireless LAN devices to be in an unobstructed position where they can see each other.

In the case of PCWL, there are two types of lines: access lines for communication with wireless LAN terminals and wireless relay lines for communication between PCWLs. For access lines, a line of sight is required "between wireless LAN terminals and PCWLs" and for wireless relay lines, a line of sight is required "between PCWLs".



In addition, radio quality is affected by various factors such as distance, presence of obstructions, presence or absence of reflective objects and their reflectance (absorptance), and air flow. Considering these factors, it is desirable to install at a height that is not easily affected by the movement of people or objects.

In addition, radio waves pass through objects that do not conduct electricity easily, such as wood and glass, and are reflected by objects that conduct electricity easily, such as metal. For this reason, when the shielding material is glass, it is unlikely to be an obstacle, but reinforced concrete beams and the like are obstacles for radio waves.

13.6 Importance of temporary installation

When installing PCWL, **be sure to perform a test by temporary installation, not by sudden installation work.**

Especially when two or more PCWLs are used to form a wireless LAN area, since mutual communication between PCWLs is essential, temporarily install PCWLs as close as possible to the planned installation location and check the wireless status of the relay line (PCWL link status), access line, and throughput.

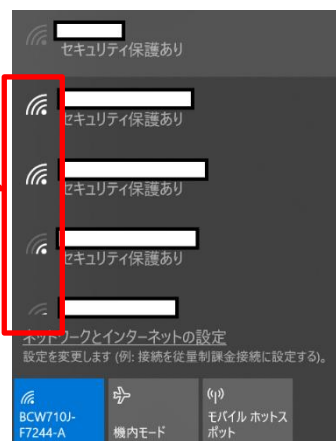
Since it is not possible to change the installation location once the actual installation work is done, first check these items in a temporary installation, and if there are any problems, change the installation location or change the number of units to be installed.

13.7 How to check the wireless status of the access line

Check the wireless strength of the access line. A simple way to check is to display a list of access points on a wireless LAN (Wi-Fi)-equipped smartphone, iPad, or laptop computer, and check the strength using icons or other means.

The icon next to the list of access points allows you to check the approximate wireless strength

*Screenshots are for Windows 10



13.8 How to check the wireless status of relay lines

Since the relay line uses stealth mode for wireless communication, it cannot be checked in the same way as the access line. Therefore, it is checked by the link establishment status between PCWLs.

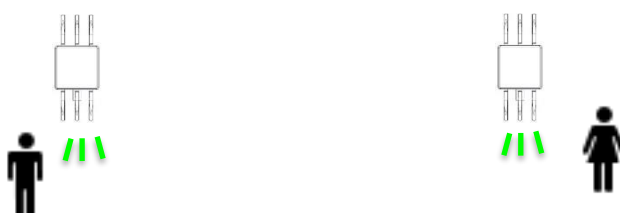
1. A supervisor will be assigned to each of the two temporarily installed PCWLs so that the LED lights of the two PCWLs can be checked.



2. Press the reroute button on the front panel of the main unit of PCWL far from the core.



3. Check the color of the Link LED lamp.



The LED lamps blue, green, yellow, and red indicate increasing link strength in that order. If the link is not established, the light is off or

Flashing.

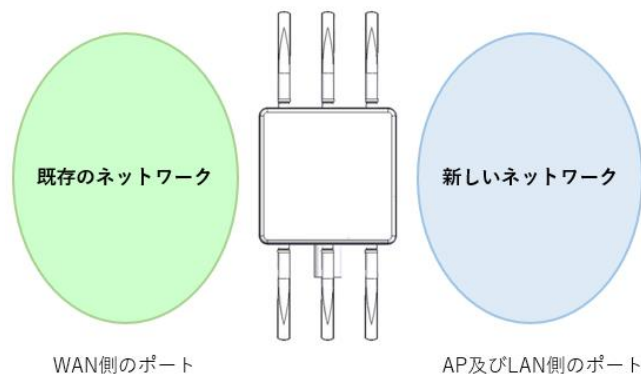
- If the LED lamp is red or off or keeps blinking, please reconsider the installation location, change the location, and recheck.

Recommended is blue or green light

13.9 IP network partitioning

Similar to the network partitioning at the Wi-Fi level described in 8.4 Network Partitioning, IP networks can be properly partitioned for easier management.

By using PCWL's router mode, a new IP network can be configured at the access point (AP) and LAN side.



The new IP network will have a different IP address, netmask, and default gateway than the existing IP network. After setting the router mode, connect a terminal to confirm that the correct settings are reflected.

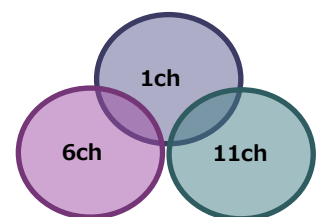
14 Building a Wireless LAN Area with PCWL: Applications

14.1 About Channels

This section explains how to set up the appropriate channels.

The access line can be configured for either the 2.4 GHz frequency band compliant with 802.11 b/g/n or the 5 GHz frequency band compliant with 802.11a/n/ac/ax.

In the 2.4GHz band, there are 1 to 11 channels in 5MHz increments. Since the channel width is 22 MHz, it is necessary to separate channels by at least 5 channels to prevent interference, and generally 1ch/6ch/11ch is used. In

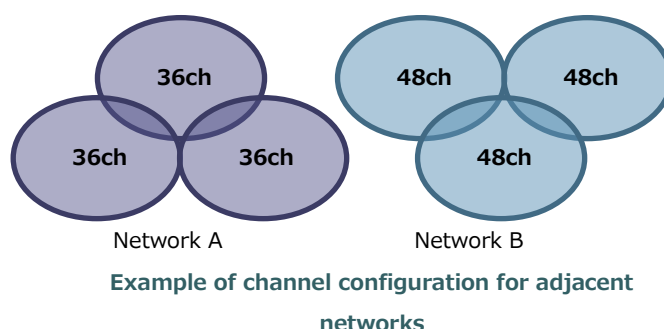


Example of adjacent node channel configuration

addition, neighboring nodes can use different channels to prevent interference.

In the 5 GHz band, channel settings vary depending on the bandwidth setting of 20 MHz, 40 MHz, or 80 MHz. 4 channels (36, 40, 44, 48) are available for 802.11a/n/ac/ax W52 when set to 20 MHz; 4 channels (52, 56, 60, 64) for W53; 11 channels (100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140) are available; when 40MHz or 80MHz bandwidth is set, the selectable channels are limited and only the selectable channels are displayed on the setting screen. When using the 5 GHz band for the access line, there is a possibility of interference with the relay line, so please set the channels used for the access line and the relay line as far apart as possible. For example, if W52 is used for the relay line, W56 should be assigned to the access line.

The relay line uses the 802.11a/n/ac/ax W52, W53 and W56 5GHz frequency bands. When the bandwidth is set to 20MHz, there are 4 channels (36ch/40ch/44ch/48ch) for W52, 4 channels (52ch/56ch/60ch/64ch) for W53, 11 channels (100ch/104ch/108ch/112ch/116ch/120ch/124ch/128ch/132ch/136ch/140ch) for W56. When the 40MHz or 80MHz bandwidth is set, the selectable channels are limited and only the selectable channels are displayed on the setting screen. The setting screen displays only the selectable channels.



Note that the **channels assigned to W52 and W53 are for indoor use only. Please change the setting to the W56 channel for outdoor use.**

14.2 About DFS

This section describes the differences in behavior when W52 (36ch to 48ch), W53 (52ch to 64ch), or W56 (100ch to 140ch) is set as the channel used for the relay line.

The frequency bands defined in W53 and W56 overlap with the frequency bands used by various existing radars (weather radar, etc.). Therefore, when using this frequency band, it is required by law that a function to change the frequency band used, called DFS (Dynamic Frequency Selection), be installed to ensure that wireless LAN communications do not affect weather radar and other radar systems.

Therefore, when W53 or W56 is set, the behavior is different from that of the W52 setting. In addition, when radar waves are detected, the DFS function changes to another channel, resulting in the following behavior.

- ▶ A channel scan is performed to determine the channel to be changed. During this time, the LINK LED blinks quickly and the wireless terminal cannot access the Internet. This condition may last for more than one minute.
- ▶ After the channel scan, a period of time (60 seconds or more) is required to check for the presence of radar signals, called a CAC (Channel Availability Check). When the LINK LED lights up, the channel transition is complete and Internet access is available.
- ▶ Since the channel is automatically changed, it may operate on a different channel than the one you have set.
- ▶ When a radar wave is detected on the relay line and the channel shifted overlaps with the channel of the access point, the relay line has priority and the channel shift of the access line occurs.

DFS activation is determined by analyzing the reception patterns of interfering waves in the band in accordance with the standards specified by laws and regulations. In **rare cases, DFS activation may also be determined for interfering waves other than radar waves, but this is not abnormal.**

*When DFS is activated, **communication is temporarily disconnected for a minute or more (several minutes in longer cases).** This is a measure to comply with legal standards and **is not abnormal.**

High-speed DFS function

PCWL-0500 has a dedicated device for radar wave detection. During startup, the dedicated device continuously monitors radar waves on a channel other than the one used for the backhaul line. When radar waves are detected on the backhaul channel, the system immediately shifts to the pre-monitored channel if no radar waves are detected on the other channel in the last minute. Compared to conventional equipment, this system significantly reduces the instantaneous network breakdown time when radar waves are detected on the backhaul channel.

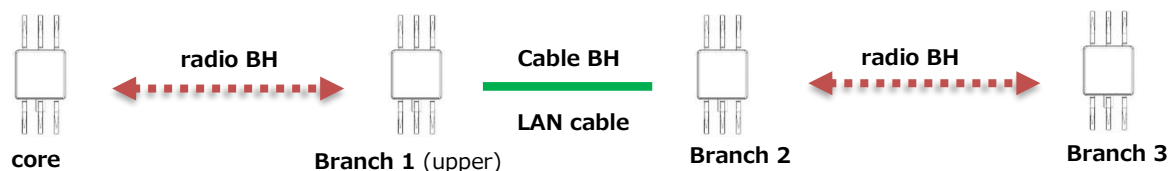
Depending on the occurrence of radar waves in the pre-monitoring channel, the network momentary breakdown time may be longer.

When the device starts up, it takes time to detect radar waves for 1 minute before Wi-Fi signal output.

14.3 About Wired Backhaul

Normally in PCWL, relaying between nodes (PCWL) is done wirelessly, but instead of wireless, a wired LAN cable can be used to create a relay route. This is the wired backhaul function. This is useful when wireless relay is difficult due to obstructions.

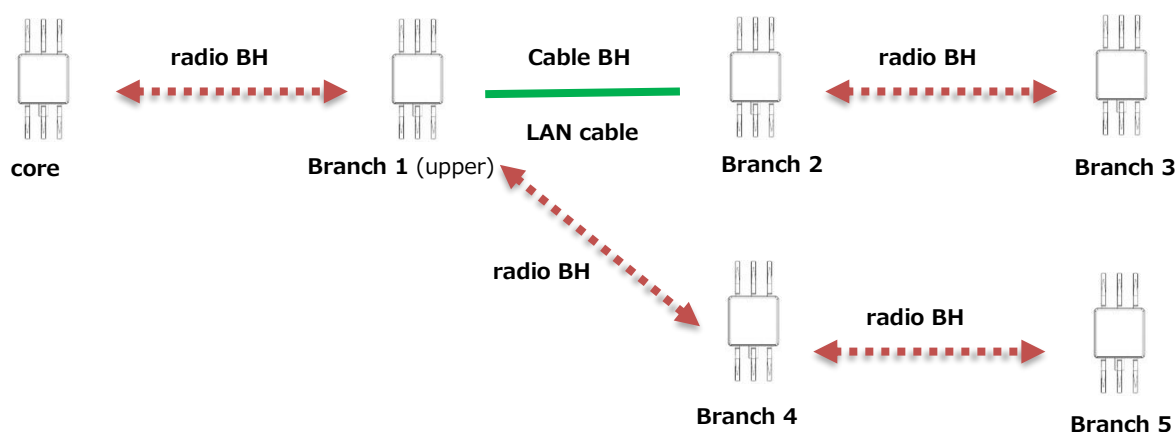
■ Wired BH configuration image



A wired backhaul connection can be constructed by connecting ETH-down on the upper side and ETH-up on the lower side. Please note that a wired backhaul connection cannot be established if the connection is made in the opposite direction.

It is also possible to use both wired and wireless backhaul as shown below.

■ Image of wired and wireless BH configuration



14.4 Forgot your login password?

If you forgot the password for accessing the web management screen (factory setting: picocela) in the password change, you must reset it to the factory setting.

If the password is forgotten, the Web UI screen cannot be accessed; use the reset switch on the rear panel of the unit. Press and release the reset switch for at least 12 seconds to perform settings initialization (factory default).

Also, please note that if the settings are initialized, all settings will be initialized to the factory defaults.

15 Interconnection with PCWL-0400 series

PCWL-0500/0510 and PCWL-0400 can be interconnected for backhaul. This chapter describes the connection specifications for interconnection.

Description.

15.1 PCWL Series Interconnection Specifications

PCWL-0400 series (hereinafter referred to as PCWL-0400) and PCWL-0500 are connected according to the following rules.

- Connection between PCWL-0400 via IEEE802.11ac wireless LAN standard
- Connection between PCWL-0400 and PCWL-0500 via IEEE802.11ac wireless LAN standard
- Connection between PCWL-0500 and PCWL-0500 using IEEE802.11ax wireless LAN standard
- When PCWL-0400 is the parent unit (Core), connect with the set bandwidth
- If PCWL-0500 is the parent unit (Core) and the backhaul bandwidth is set to 160 MHz, PCWL-0400 will be connected with a bandwidth of 80 MHz.

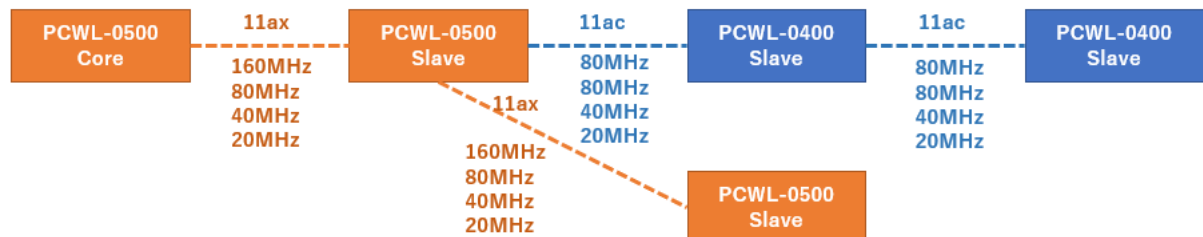
(Note) If the PCWL-0400 firmware is v2.9.4, the backhaul bandwidth of the PCWL-0500 parent unit will be

Set to 80 MHz. 160 MHz setting is not guaranteed.

1. PCWL-0400 parent unit (core) in operation



2. PCWL-0500 parent unit (core) in operation



15.2 Interconnection Limitations

PCWL-0400 firmware version limitations

To interconnect, update the PCWL-0400 series firmware version to the latest version after the following version.

PCWL-0400 firmware version: V2.10.1 or later

In addition, the following restrictions apply depending on the PCWL-0400 firmware version

V2.9.3 or earlier PCWL-0500 cannot be interconnected with PCWL-0500.

V2.9.4 : Backhaul bandwidth of 160MHz for PCWL-0500 cannot be set
All nodes are backhauled with 802.11ac wireless LAN standard

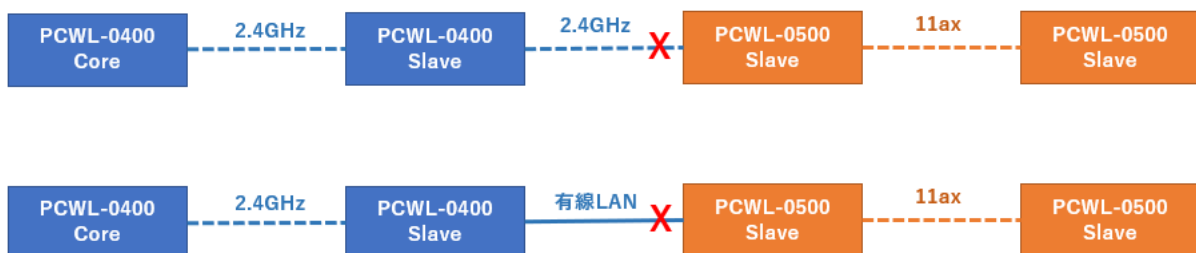
802.11k (proximity AP reporting) roaming restrictions

When PCWL-0500 and PCWL-0400 are mixed, the proximity AP list information cannot be shared between PCWL-0500 and PCWL-0400. Therefore, the reconnection time (network disconnection time) when roaming between PCWL-0500 and PCWL-0400 will be longer than when they are not mixed.

Prohibition of 2.4GHz backhaul operation

PCWL-0500 does not support 2.4GHz backhaul connection; interconnection operation is not possible when PCWL-0400 is used for 2.4GHz backhaul connection.

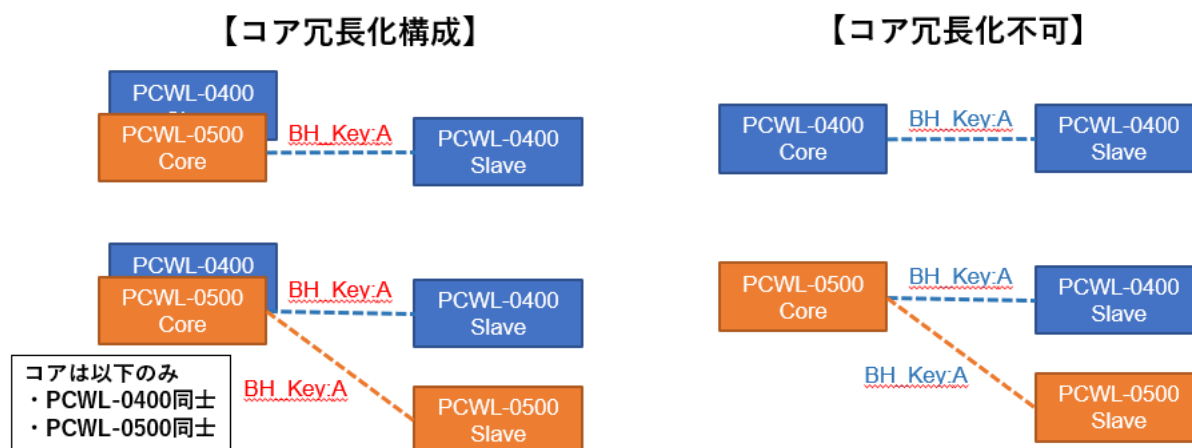
Wired backhaul operation connecting PCWL-0400 and PCWL-0500 with a LAN cable is also not supported. 5GHz radio frequency band should be used for operation when constructing a backhaul network by mixing PCWL-0500 and PCWL-0400.



Backhaul connection to the PCWL-0500 at the latter stage is possible by setting the PCWL-0500 connected by wire as the parent unit (core) when connecting to a wired LAN in the above configuration.

Limitations of parent unit (core) redundant operation

The PCWL series can have redundant parent units (cores). When performing redundancy of the parent unit (core), the parent units should be configured as PCWL-0400 units or PCWL-0500 units. Redundant configurations that mix PCWL-0400 and PCWL-0500 parent units are not supported.

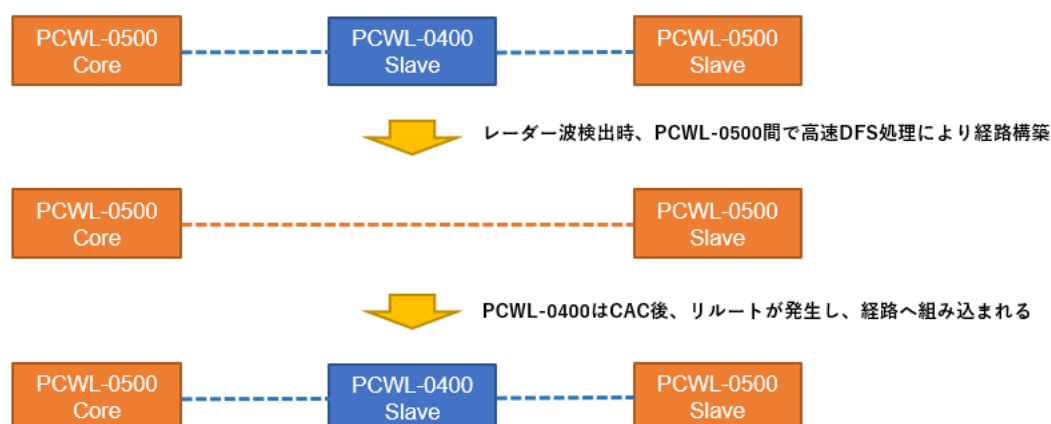


Limitations of Fast DFS Operation

PCWL-0500 has high-speed DFS functionality, but the following limitations occur when mixed with PCWL-0400.

- High-speed DFS function is disabled when PCWL-0400 is the parent unit (core)
- When PCWL-0500 is the parent unit (core)
 - Route construction between PCWL-0500 by high-speed DFS
 - PCWL-0400 is incorporated into the route after CAC as before

An example of mixed use is shown below.



16 salient points

16.1 PCWL-0500 main specifications

<Access line

(data) item	various factors or elements
Wireless LAN Standard ^{*1}	2.4GHz: IEEE802.11b/g/n/ax 5GHz : IEEE802.11a/n/ac/ax
maximum transmission rate ^{*2}	802.11b: 11Mbps 802.11g: 54Mbps 802.11a: 54Mbps 802.11n: 288Mbps (20MHz), 600Mbps (40MHz) 802.11ac: 346Mbps(20MHz), 800Mbps(40MHz), 1733Mbps(80MHz)/ (80+80MHz) 802.11ax: 572Mbps (20MHz), 1144Mbps (40MHz), 2400Mbps (80MHz) /(80+80MHz)
MIMO spatial stream	4 ^{*3} (Both 2.4GHz and 5GHz are supported)
Peak Antenna Gain	2.4GHz: 3dBi 5 GHz: 4 to 6 dBi (depending on frequency band)
Wireless output	17dBm Max *Output level varies depending on frequency bandwidth
frequency band ^{*4}	802.11b/g/n/ax: 2.412 to 2.462 GHz (1 to 11channels) 802.11n/a/ac/ax: 5.15 to 5.850 GHz W52: 36 to 48 channels W53: 52 to 64 channels W56: 100 to 144ch W58: 149 to 165ch
multiple SSID	Up to 16 settings possible (2.4GHz: 8, 5GHz: 8)
stealth SSID	configurable
Maximum number of terminals that can be connected	128 (2.4GHz) 128 (5GHz)
Wireless Authentication Security	OPEN WPA/WPA2-Personal WPA2-Personal WPA/WPA2-Enterprise WPA2-Enterprise WPA3-Personal WPA2/WPA3-Personal WPA3-Enterprise WPA2/WPA3-Enterprise WPA3-Enterprise (192bit) OWE

Other Functions	IEEE802.11k, IEEE802.11r/v (PicoManager linked function) VLAN support, terminal-to-terminal communication settings MAC address filtering AP off function DTIM interval setting Maximum retransmission count setting
-----------------	--

<Relay line

(data) item	various factors or elements
Operation Mode	Bridge mode, router mode (PPPoE connection also possible)
Wireless LAN Standard	IEEE802.11n/a/ac/ax (5GHz)
maximum transmission rate ^{*2}	IEEE802.11ax 572Mbps (20MHz), 1144Mbps (40MHz), 2400Mbps (80MHz), 4800Mbps (160MHz)
frequency band ^{*4}	4.90 to 5.00 GHz (W49: 184 to 196ch) 5.15 to 5.25 GHz (W52: 36 to 48ch) 5.26~5.36GHz (W53 : 52~64ch) 5.47 to 5.725 GHz (W56: 100 to 140ch) 5.725~5.850GHz (W58: 149~165ch)
MIMO spatial stream	4 ^{*3}
Peak Antenna Gain	5 GHz: 4 to 6 dBi (depending on frequency band)
Wireless output	19dBm Max *Output level varies depending on frequency bandwidth
Wireless Security	AES encryption with SAE method
routing control method	PicoCELA proprietary method Dynamic tree control method with adaptive route update function
frame transfer method	PicoCELA proprietary method L2 multistage bridge system with periodic intermittent transmission applied
Other	Wired/wireless hybrid relay WLAN Interface setting function (Eth-up port/PPPoE) Minimum CW length variable setting function Variable maximum retransmission count setting function Fast route recovery function Leaf mode setting function (setting conditions for route construction)

*1) When using the 5GHz band, the same channel as the relay line cannot be used.

*2) Maximum transmission rate means bearer rate and does not guarantee the achievement of each speed


*3) However, when 11n/ac/ax mode is used

*4) Access lines and relay lines may interfere with each other depending on their respective frequency assignments. Frequencies should be allocated as far apart as possible. Available frequency bands are defined by the country.

<Hardware

(data) item	various factors or elements
SoC	IPQ8072A
processor	Quad-core ARM A53
storage	2GB RAM/16GB eMMC
Body size	L260×H52×D205(mm)
Antenna length	153cm
Main unit weight	Approx. 1700g
Power consumption	Max 30W
DC input	12V ± 5%
interface	USB3.0 x1 Reroute button x1 Reset button x1 2.5GbE port x2 (RJ45 modular jack) 6 LED lamps (Power, Link, Stat, INET, PM, BLE) Antenna connection terminal: RP-SMA connector x 10 4 for access line, 4 for relay line, x1 for Radar Scan, x1 for Bluetooth
Operating temperature range	0 to 50°C
Storage temperature range	-30 to 70°C
Power Over Ethernet	PoE power receiving (Eth-up port/IEEE802.3at/bt) ^{*5}

<AC adapter (option): HYT-1205000

(data) item	various factors or elements
Input voltage	100 to 240Vac
Input frequency	50 to 60Hz
input	1.5A max
Output voltage	12V ± 5%
Output current	5A max
Output power	60W max
Plug Dimensions	2.1φ x 5.5 x 9.5mm 
Dimensions	53(L) x 34(W) x 119(H)mm
weight	

DC cord length	1.5m
----------------	------

*5) When supplying power to the main unit via PoE, connect to Eth-up.

When connecting a device to the USB terminal, power the unit with IEEE802.3bt (60W).

16.1 PCWL-0510 main specifications

<Access line

(data) item	various factors or elements
Wireless LAN Standard* ¹	2.4GHz: IEEE802.11b/g/n/ax 5GHz : IEEE802.11a/n/ac/ax
maximum transmission rate* ²	802.11b: 11Mbps 802.11g: 54Mbps 802.11a: 54Mbps 802.11n: 288Mbps (20MHz), 600Mbps (40MHz) 802.11ac: 346Mbps(20MHz), 800Mbps(40MHz), 1733Mbps(80MHz)/ (80+80MHz) 802.11ax: 572Mbps (20MHz), 1144Mbps (40MHz), 2400Mbps (80MHz) /(80+80MHz)
MIMO spatial stream	4* ³ (Both 2.4GHz and 5GHz are supported)
Antenna Gain	2.4GHz: 4.5dBi 2.4GHz: 13.5dBi 5GHz : 7dBi 5GHz :15.5dBi
Wireless output	17dBm Max *Output level varies depending on frequency bandwidth
frequency band* ⁴	802.11b/g/n/ax: 2.412 to 2.462 GHz (1 to 11 channels))802.11n/a/ac/ax: 5.15 to 5.850 GHz W52: 36 to 48 channels W53: 52 to 64 channels W56: 100 to 144ch W58: 149 to 165ch
multiple SSID	Up to 16 settings possible (2.4GHz: 8, 5GHz: 8)
stealth SSID	configurable
Maximum number of terminals that can be connected	128 (2.4GHz) 128 (5GHz)
Wireless Authentication Security	OPEN WPA/WPA2-Personal WPA2-Personal WPA/WPA2-Enterprise WPA2-Enterprise WPA3-Personal WPA2/WPA3-Personal

	WPA3-Enterprise WPA2/WPA3-Enterprise WPA3-Enterprise (192bit) OWE
Other Functions	IEEE802.11k, IEEE802.11r/v (PicoManager linked function) VLAN support, terminal-to-terminal communication settings MAC address filtering AP off function DTIM interval setting Maximum retransmission count setting

<Relay line

(data) item	various factors or elements
Operation Mode	Bridge mode, router mode (PPPoE connection also possible)
Wireless LAN Standard	IEEE802.11n/a/ac/ax (5GHz)
maximum transmission rate ^{*2}	IEEE802.11ax 572Mbps (20MHz), 1144Mbps (40MHz), 2400Mbps (80MHz), 4800Mbps (160MHz)
frequency band ^{*4}	5.15 to 5.25 GHz (W52: 36 to 48ch) 5.26~5.36GHz (W53 : 52~64ch) 5.47 to 5.725 GHz (W56: 100 to 140ch) 5.725~5.850GHz (W58: 149~165ch)
MIMO spatial stream	4 ^{*3}
Peak Antenna Gain	5GHz : 7dBi
Wireless output	19dBm Max *Output level varies depending on frequency bandwidth
Wireless Security	AES encryption with SAE method
routing control method	PicoCELA proprietary method Dynamic tree control method with adaptive route update function
frame transfer method	PicoCELA proprietary method L2 multistage bridge system with periodic intermittent transmission applied
Other	Wired/wireless hybrid relay WLAN Interface setting function (Eth-up port/PPPoE) High-speed DFS Minimum CW length variable setting function Variable maximum retransmission count setting function Fast route recovery function Leaf mode setting function (setting conditions for route construction)

*1) When using the 5GHz band, the same channel as the relay line cannot be used.

- *2) Maximum transmission rate means bearer rate and does not guarantee the achievement of each speed
- *3) However, when 11n/ac/ax mode is used
- *4) Access lines and relay lines may interfere with each other depending on their respective frequency assignments. Frequencies should be allocated as far apart as possible. Available frequency bands are defined by the country.

<Hardware

(data) item	various factors or elements
SoC	IPQ8076A
processor	Quad-core ARM A53
storage	2GB RAM/16GB eMMC
Body size	L304×H294×D82(mm)
Antenna length	183cm
Main unit weight	Approx. 3200g
Power consumption	Max 30W
DC input	12V ± 5%
interface	Reroute button x1 Reset button x1 2.5GbE port x2 (RJ45 modular jack) 6 LED lamps (Power, Link, Stat, INET, PM, BLE) Antenna connection terminal: N connector connector × 10 4 for access line, 4 for relay line, x1 for Radar Scan, x1 for Bluetooth
Operating temperature range	-30 to 70°C
Storage temperature range	-30 to 70°C
Power Over Ethernet	PoE power receiving (Eth-up port/IEEE802.3bt)*6

<AC adapter (option): RKPO-JET125000CD-6

(data) item	various factors or elements
Input voltage	100 to 240Vac
Input frequency	50 to 60Hz
input	1.5A max
Output voltage	12V ± 5%

Output current	5A max
Output power	60W max
Plug Dimensions	M8
Dimensions	140mm(L) x 50mm(W) x 36(H)mm
weight	Approx. 3200g
DC cord length	2.7m

*5) When supplying power to the main unit via PoE, connect to Eth-up.

Use Manual Statement

FCC Statement

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. 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.

This device complies with part 15 of the 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.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

RF Exposure

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

No necessary to perform SAR testing

PCWL-0500

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. " applying power to the main unit via PoE, connect to Eth-up.

PCWL-0510

The antennas used for this transmitter must be installed to provide a separation distance of at least 55 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. " applying power to the main unit via PoE, connect to Eth-up.