SOLUM
Solution provider.

CG16HSS33B

Wi-Fi HaLow Access Point

User Manual

Contents

1. SYSTEM OVERVIEW 3

1.1. SYSTEM INTRODUCTION 3

1.2. NETWORK DIAGRAM 4

1.3. CONTENTS CHECK BEFORE INSTALLATION. 5

1.3.1. Main Product Body 5

1.3.2. Accessories 5

1.4. PARTS AND FUNCTIONS 6

1.4.1. Top Front 6

1.4.2. Rear I/O Port 7

2. HALOW AP'S INSTALLATION AND SETTINGS 8

2.1. HALOW AP'S HARDWARE INSTALLATION 8

2.1.1. Power supply to HaLow AP 8

2.1.2. Connection HaLow AP to HaLow Serial Converter 10

2.1.3. Connecting HaLow AP to HaLow Ethernet Converter 11

2.2. HALOW AP'S SOFTWARE CONFIGURATION 12

2.2.1. Configuration by AP's WEB Interface 12

2.2.2. Setting HaLow AP to Bridge Mode 25

2.2.3. Setting HaLow AP from Bridge Mode back to NAT Mode 35

3. SYSTEM MAINTENANCE 45

3.1. FIRMWARE UPDATE 45

3.2. RESET TO THE FACTORY DEFAUT SETTINGS. 48

3.2.1. Using push buttons 48
3.2.2. Resetting from the WEB UI 49
3.3. HOW TO USE THE WPS BUTTON FUNCTION 50
3.3.1. Using push button 50
3.3.2. WPS Function Description 50
3.3.3. How to Use the WPS Function 51
3.4. SYSTEM SPECIFICATIONS 53
3.5. TERMINOLOGY 54

1. System Overview

1.1. System Introduction

CG16HSS33B System is a 900MHz Wi-Fi(HaLow) AP(referred to as 'HaLow AP') which supports Wi-Fi network's standard known as 802.11ah.This technology operates at Sub-1 GHz spectrum (Especially 900MHz in Korea, Japan, US), and offers long range communication more than the legacy Wi-Fi operating at 2.4 GHz. Wi-Fi HaLow's main Characteristics and advantages are as follows:

- Low Power Consumption: It is designed to consume Low Power, so it is the best for IoT devices such as sensors that must be operated for a long time.

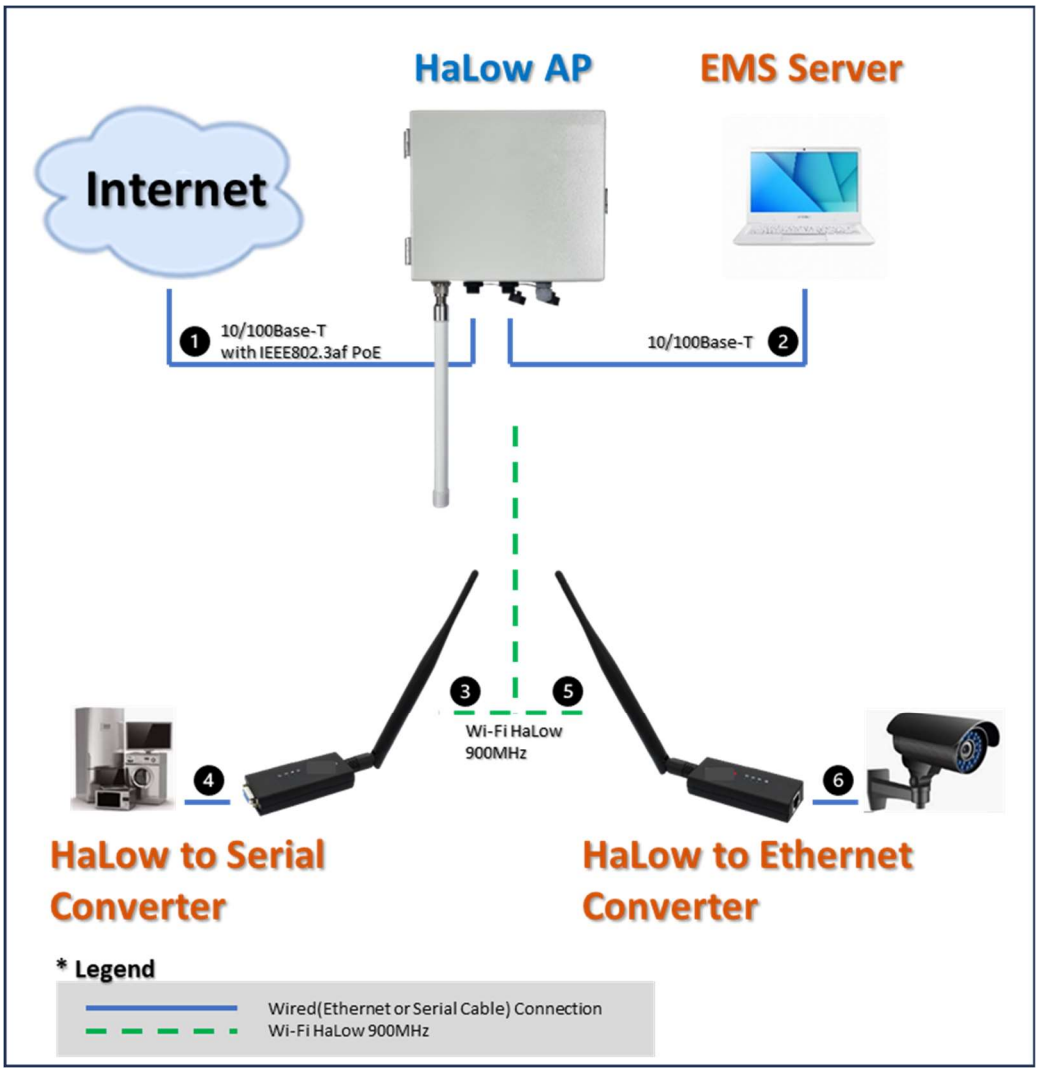
- Wide Area and Long Reach: Wi-Fi HaLow can reach 1.5Km comparing to 10 times of the legacy Wi-Fi Technology. As Low frequency radio signal used in Wi-Fi HaLow passes walls and obstacles more than High frequency radio signal, it is ideal for IoT applications connecting long distance, insides of building and rural area.

- High Connection Density: Wi-Fi HaLow can support 1,024 devices on network. It offers high connect density which is advantageous to IoT applications with multiple connected devices.

- Private Network Extension: The built-in NAPT feature allows personal Wi-Fi HaLow 900MHz wireless network devices to expand and communicate with devices connected to external authorized networks.

- Security and Reliability: Like other Wi-Fi standards, Wi-Fi HaLow supports the latest and most powerful Wi-Fi security feature, the WPA2/WPA3 protocol, to protect devices connected to the network. It also provides reliable data transfer in environments with a lot of interference.

1.2. Network Diagram



Number	Description
1	Connect to Internet network.
2	Connect to the EMS Server.
3	Connect HaLow AP and Station with 900MHz.
4	Connect HaLow Station and IoT device with serial communication cable.
5	Connect HaLow AP and Station with 900MHz.
6	Connect HaLow Station and Network device with Ethernet cable.

1.3. Contents check before installation.

1.3.1. Main Product Body

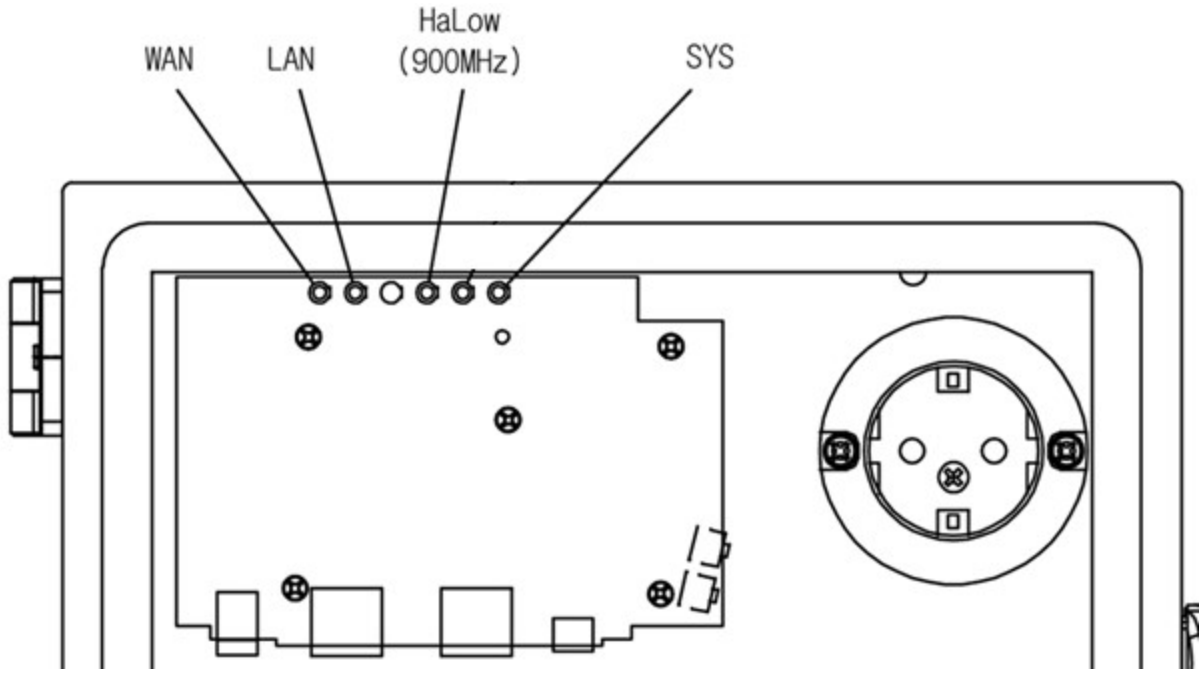
Device	Model Name	Quantity
HaLow AP	CG16HSS33B	1

1.3.2. Accessories

Name	Specification	Quantity

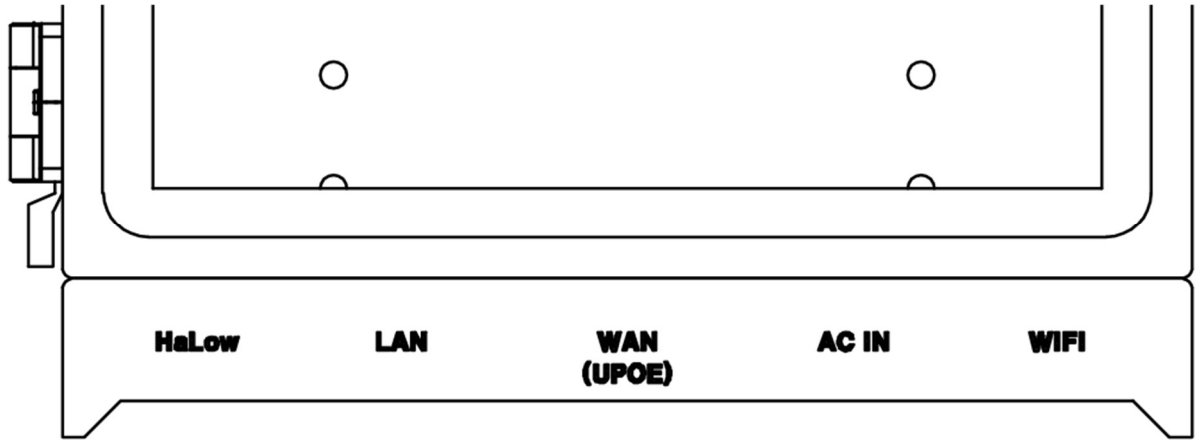
1.4. Parts and Functions

1.4.1. Top Front



No.	LED	Function	Remarks
1	SYS	It means system on.	
2	HaLow (900MHz)	It means HaLow on. It blinks when transmitting data using HaLow.	
3	LAN	It means wired connection with computer or device. If LAN cable is connected, it lights on and blinks when transmitting data.	
4	WAN	LED that indicates a wired connection to the Internet or L2/L3 switch. It turns on when the LAN cable is connected, and blinks when data is being transmitted.	

1.4.2. Rear I/O Port



No.	Name	Function	Remarks
1	HaLow	900MHz Antenna for 802.11ah	
2	LAN	Connect computer or ethernet device.	
3	WAN(PoE)	Connect internet or L2/L3 switch. Supply power with PoE injector or PoE switch.	
4	AC IN		Unused
5	WIFI		Unused

2. HaLow AP's installation and settings

Use the following steps to install 11ah APs and 11ah Stations and set up software for communication between terminals.

2.1. HaLow AP's hardware Installation

Install equipment for communication of station equipment with 11ah AP of CG16HSS33B model.

2.1.1. Power supply to HaLow AP

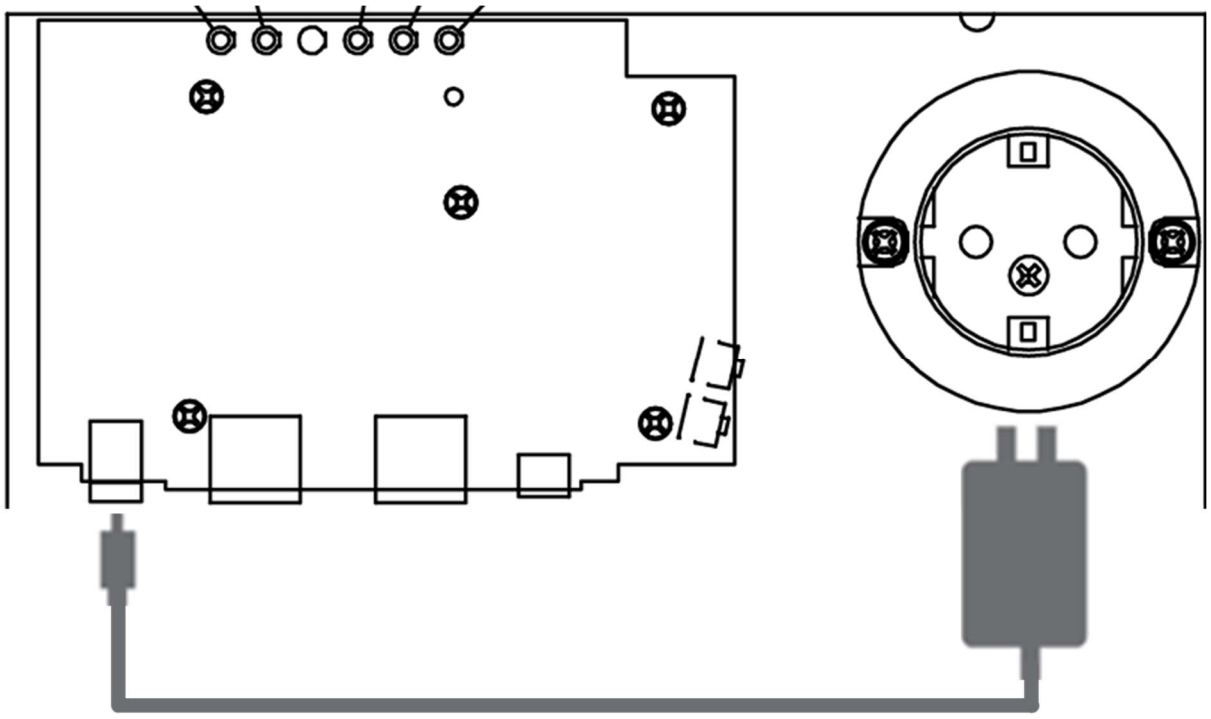
※ Warning

1. By design, this system prioritizes power supply through a power supply adapter. Therefore, when PoE and a power supply adapter are used at the same time, the power supply adapter is selected first.

2. If you disconnect the DC power jack of a product that is operating with the power supply adapter connected, the system goes down and then the system reboots via PoE.

3. It is recommended that only one power source be used for stable system power supply.

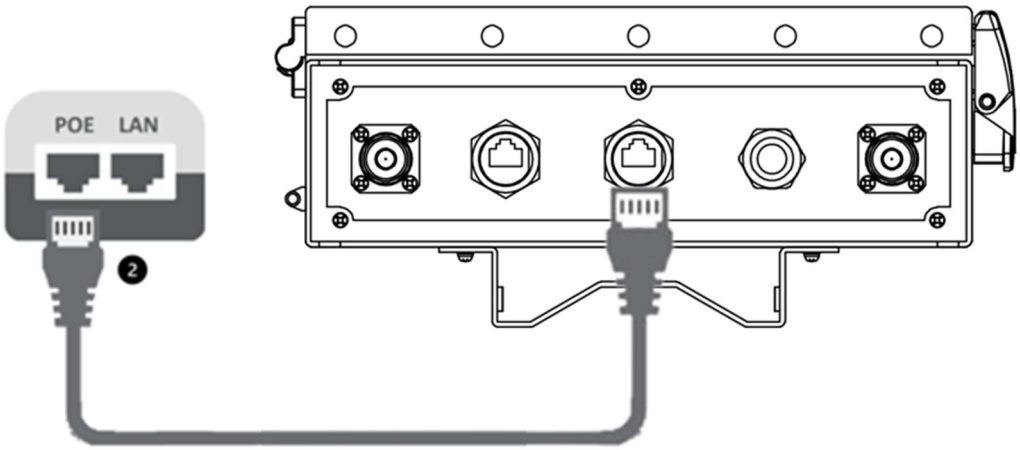
- Power supply by power adaptor
- Connect the power supply adapter included in the product accessory to the power terminal of the HaLow AP.



No.	Description
1	Connect the jack of the power supply adapter to the power terminal of the HaLow AP.
2	Connect the power supply adapter to the outlet.

- Power supply by PoE

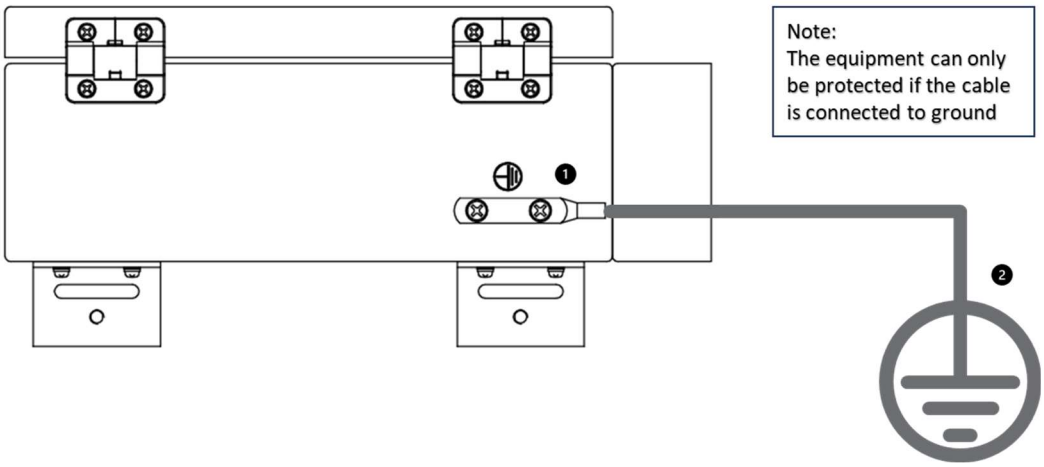
Connect the UTP cable to a PoE port, such as a PoE injector or PoE switch, to the WAN port on the HaLow AP.



No.	Description
1	Connect the UTP cable to the WAN (PoE) port of the HaLow AP.
2	Connect the UTP cable to a PoE port, such as a PoE injector or PoE switch.

- WAN (PoE) port surge protection

External ground terminal on the left side of the HaLow AP device must be connected to ground to protect the WAN (PoE) port.

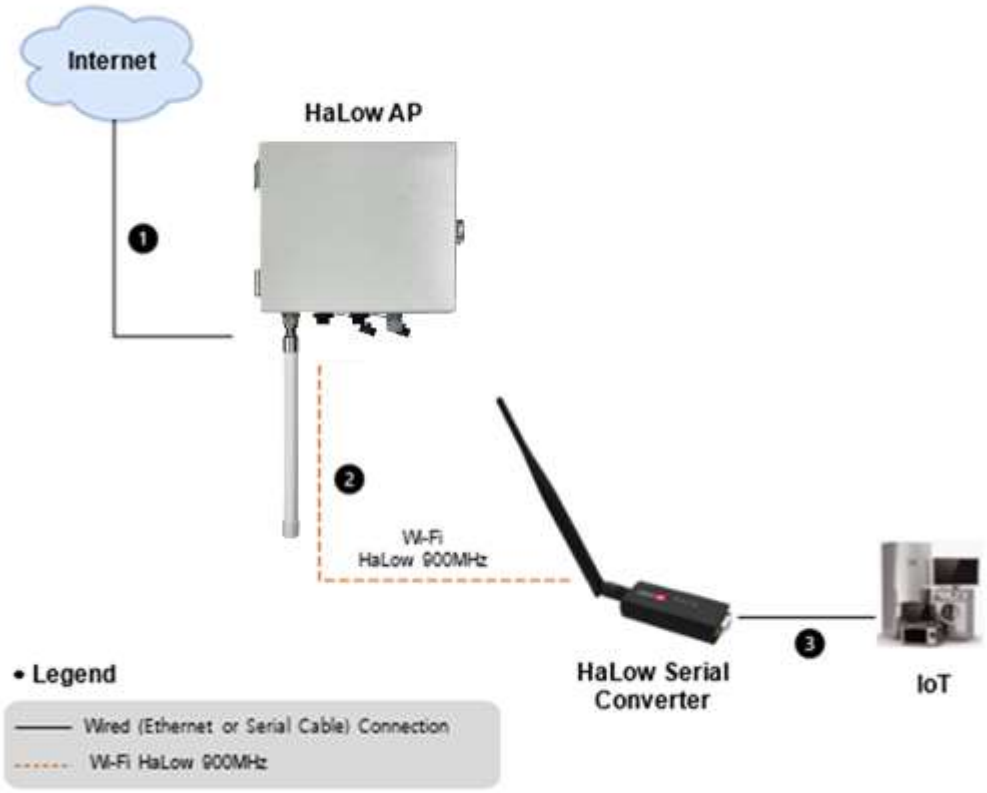


No.	Description
1	Connect the ground cable to the ground terminal of the HaLow AP.
2	Connect the ground cable to ground

2.1.2. Connection HaLow AP to HaLow Serial Converter

This is the configuration diagram of the connection between HaLow AP and HaLow Serial Converter and IoT equipment.

- Network Connection Diagram



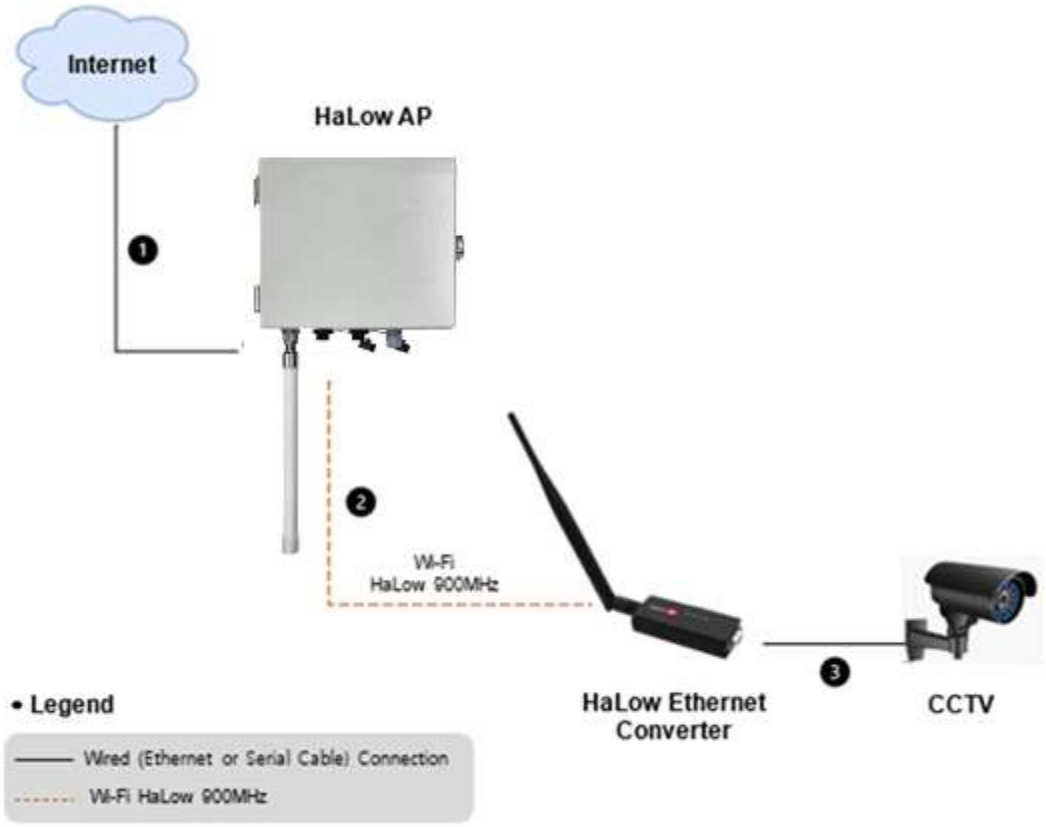
■ Network connection of HaLow communication equipment

No.	Description
1	Connect to the top Internet network.
2	Connect the HaLow AP and HaLow Serial Converter.
3	Connect various IoT devices that support serial communication.

2.1.3. Connecting HaLow AP to HaLow Ethernet Converter

This is the connection diagram between the HaLow AP and the HaLow Ethernet converter and Ethernet equipment.

- Network Connection Diagram



■ Network connection of HaLow devices

No.	Description
1	Connect to the Internet network.
2	Connect the HaLow AP to the HaLow Ethernet converter
3	Connect a variety of network equipment that supports Ethernet communication.

2.2. HaLow AP's Software Configuration

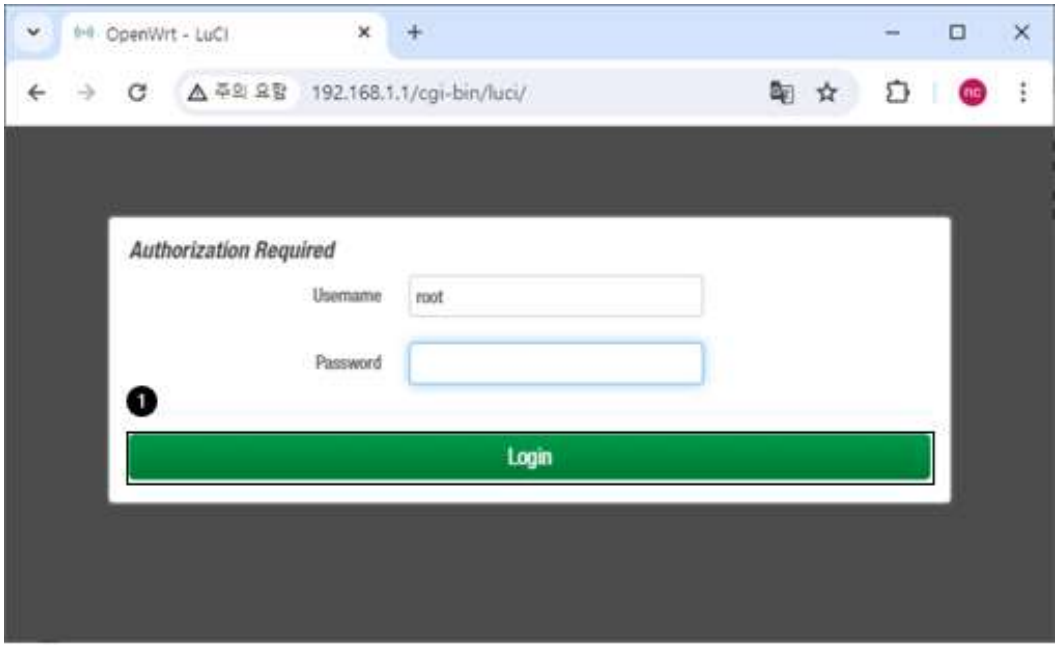
2.2.1. Configuration by AP's WEB Interface

1 Connect to the AP's Web Server.

1.1 Input 'http://192.168.1.1'(1) on the address bar.

1.2 Click on the 'Login'(1).

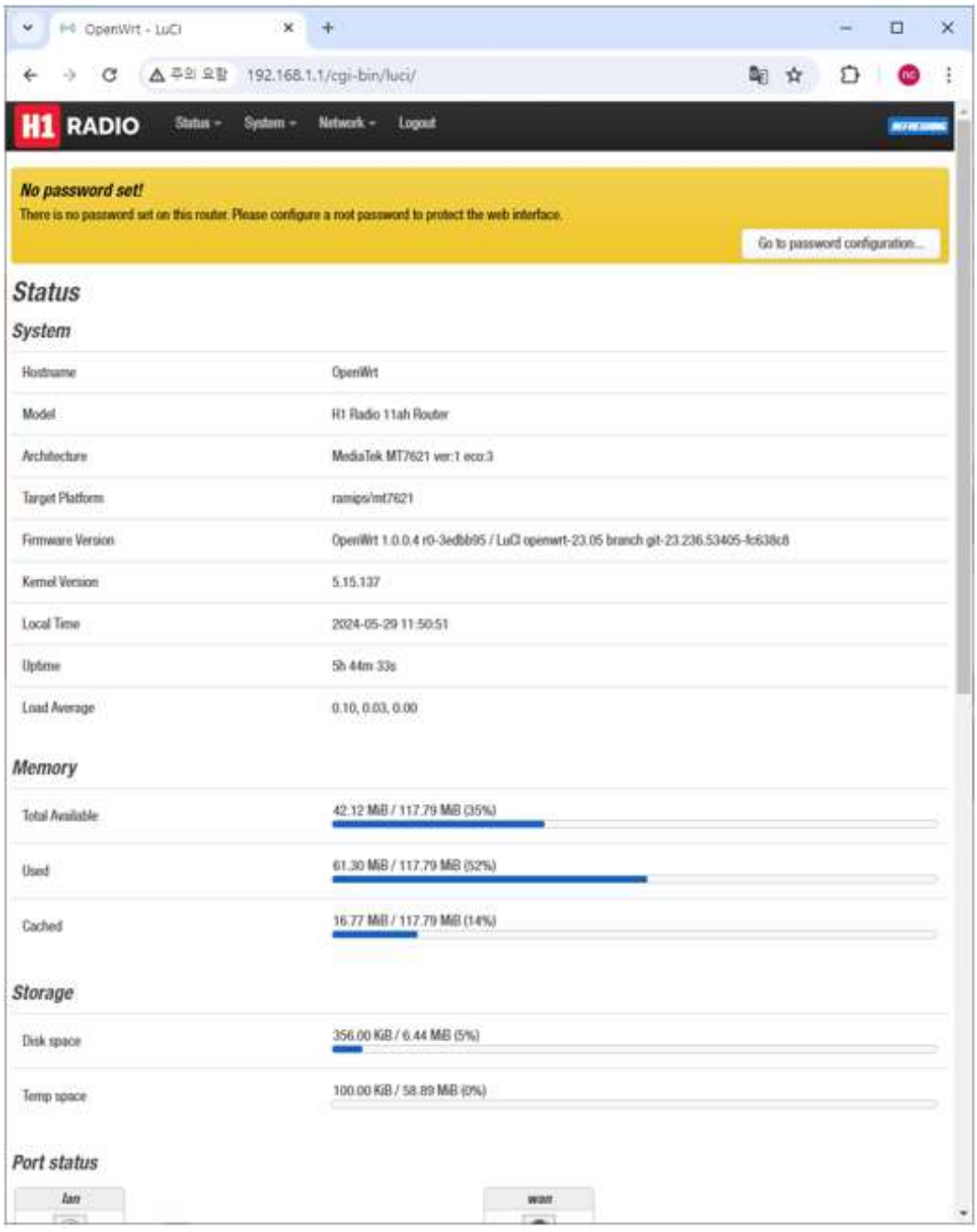
1.2.1 Username: root
1.2.2 Password: blank



2 Set Wi-Fi settings for wired and WiFi 900MHz bands for various AP operations.

2.1 Network connection status

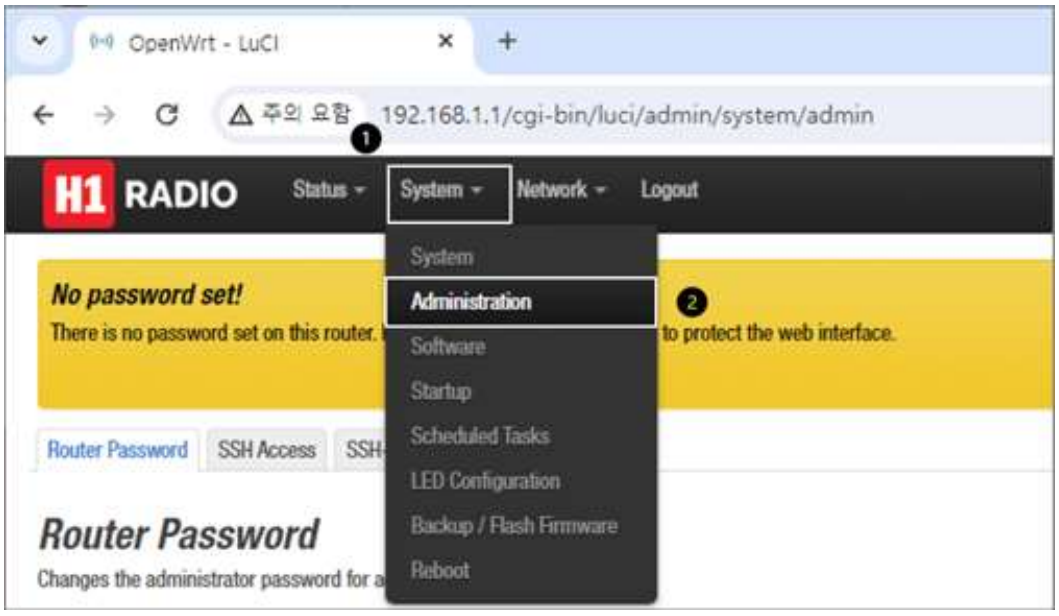
- This is the first screen displayed when you start the web browser and complete.



2.2 Set administrator password.

- This is the first screen displayed when you start the web browser and complete user authentication.

2.2.1 Access: Click ‘Administration’ (2) in the ‘System’ (1) menu.



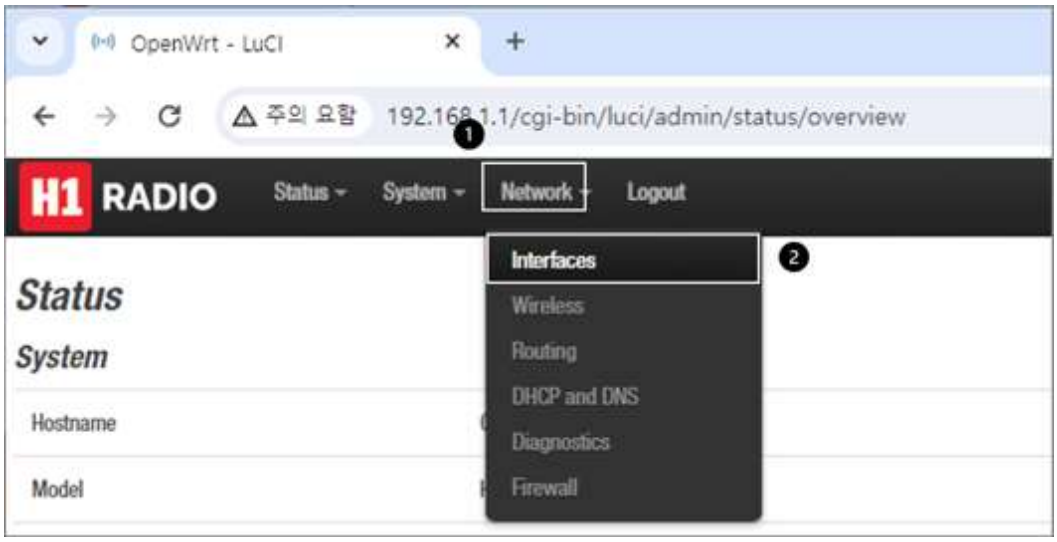
2.2.2 Modify password: Enter a new password in Password (1), enter the same password in Confirmation (2), and click the ‘Save’ (3) button.

No.	Name	Description	Option values
1	Password	New Password	
	Confirmation	New Password confirm	
2	Save	Save your settings.	

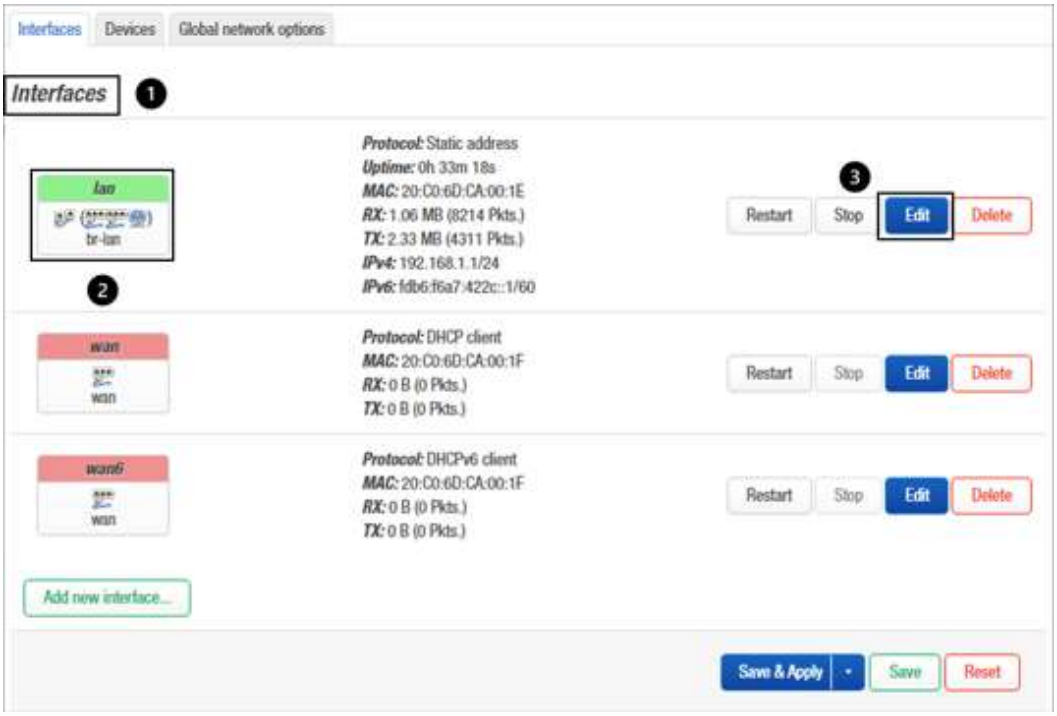
2.3 Wired LAN network setting

- Set the operating environment of the Wired LAN. This setting sets the internal IP address, subnet mask, DHCP server range, DHCP server lease time, and so on.

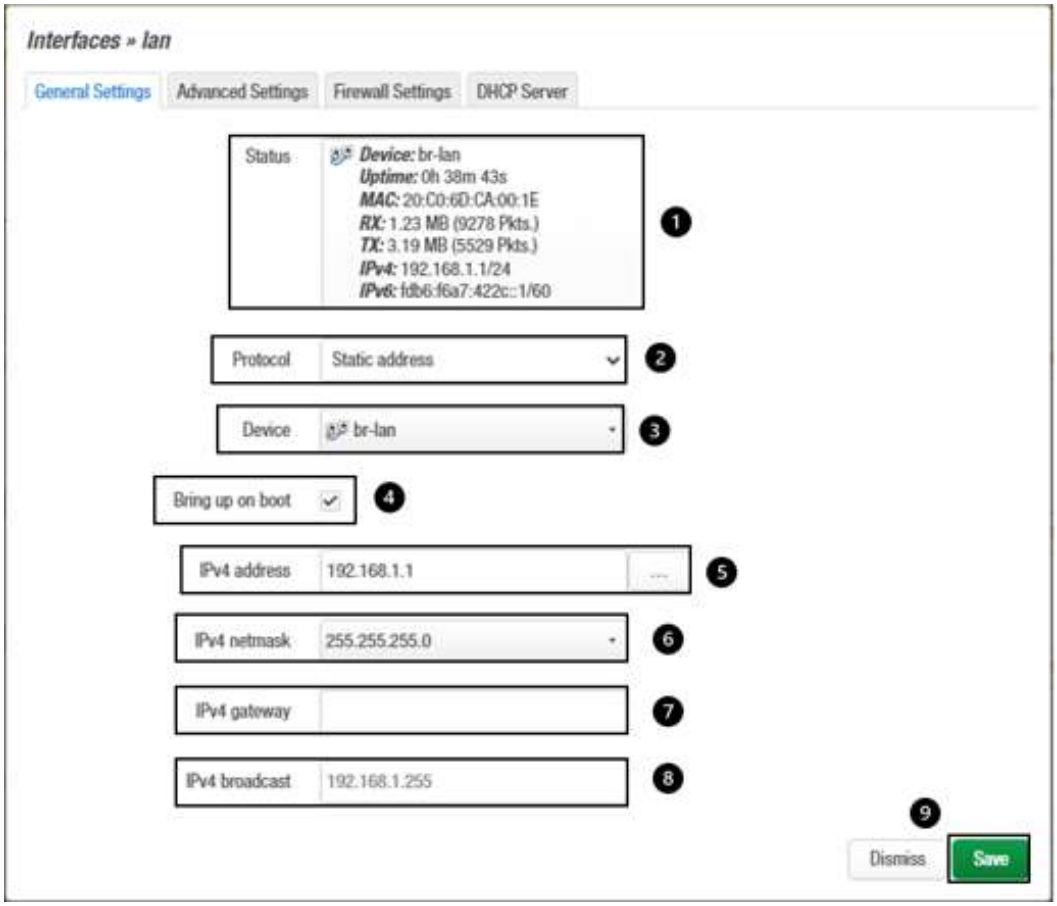
2.3.1 Acesss: Click ‘Network(1) → Interfaces(2)’ on web page.



2.3.2 In ‘Interfaces’ (1), click the Edit (3) button for ‘lan’ (2).

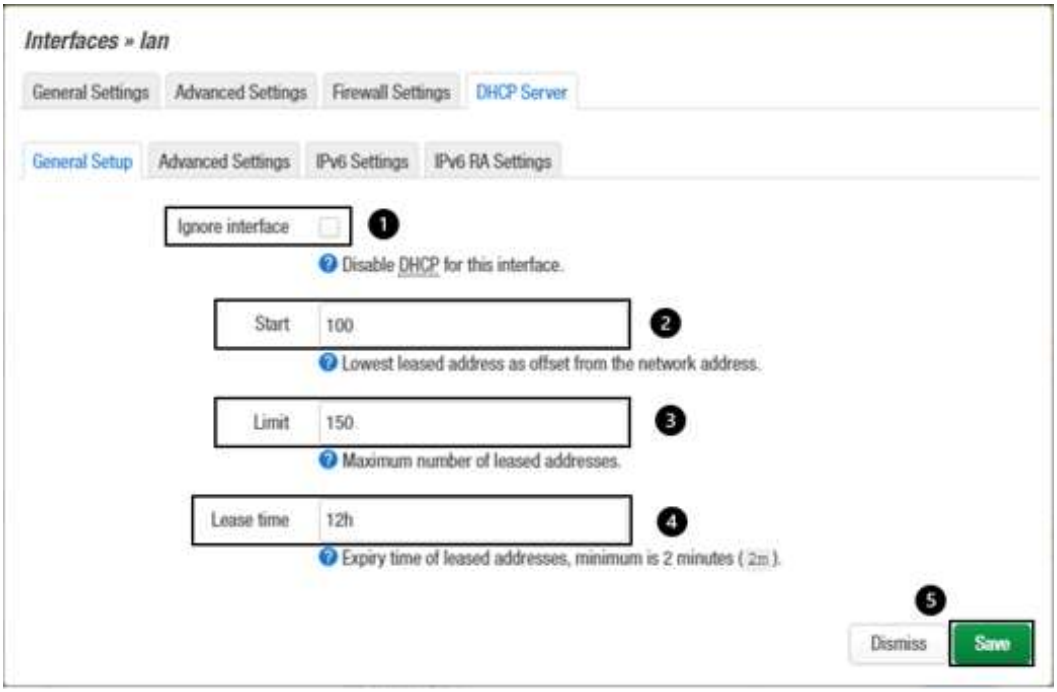


2.3.3 General Settings: Set the default values for the following settings.



No.	Name	Description	Option values
1	Status	LAN status	
2	Protocol	Protocol	DHCP client, DHCPv6 client, Unmanaged, PPP, PPPoE, Static address Default: Static address
3	Device	terminal interface	Default: br-lan
4	Bring up on boot	Bring up at boot	Default: check
5	IPv4 address	IPv4 address	Default: 192.168.1.1
6	IPv4 netmask	IPv4 Subnet mask	Default: 255.255.255.0
7	IPv4 AP	IPv4 Gateway	Default: None
8	IPv4 broadcast	IPv4 broadcast	Default: 192.168.1.255
9	Save	Save your settings.	

2.3.4 DHCP Server: Set DHCP server address range, lease time, etc.

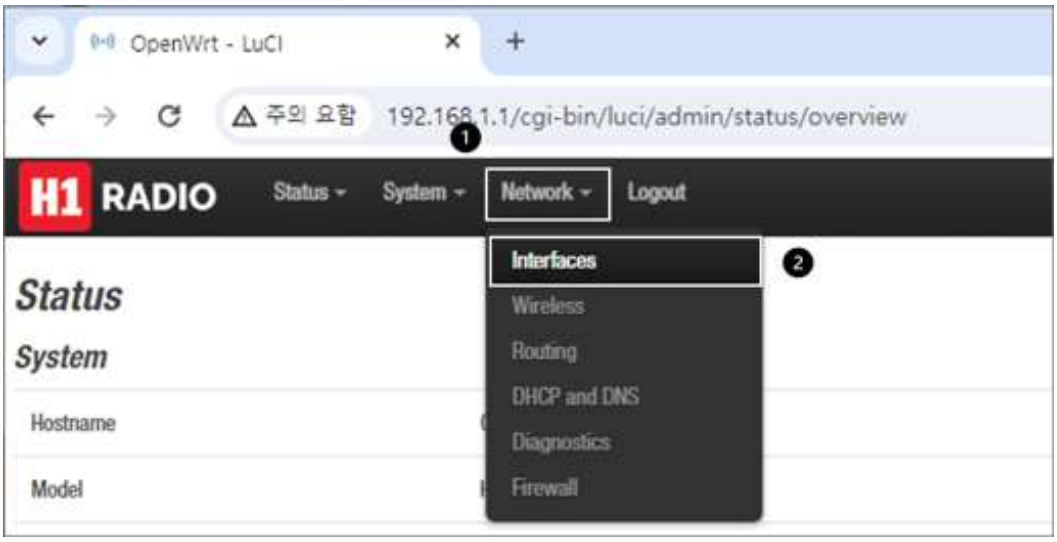


No.	Name	Description	Option values
1	Ignore interface	Ignore Interface	Default: no check
2	Start	Start DHCP server lease address	Default: 100
3	Limit	End DHCP server lease address	Default: 150
4	Lease time	Lease time (minimum: 2minutes)	Default: 12h
5	Save	Save your settings.	

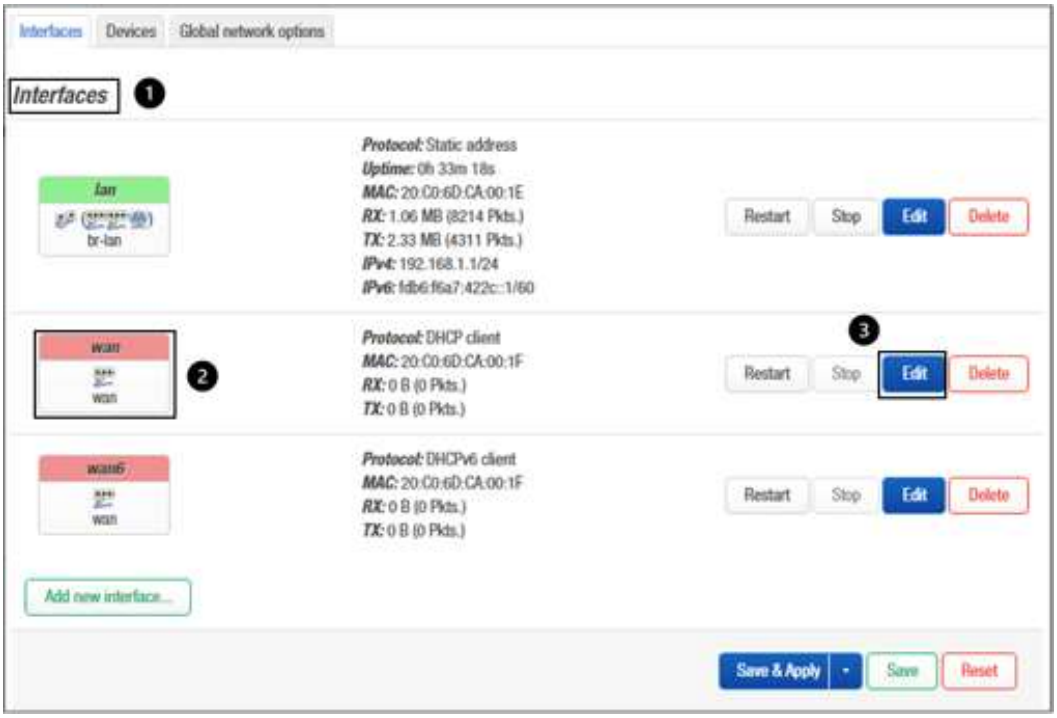
2.4 Wired WAN Network Setting

- Set the operating environment of the wired WAN. This setting checks the Internet connection status, sets the Internet connection method, and DNS address settings.

2.4.1 Connection: Click ‘Interfaces’ (2) in the ‘Network’ (1) menu.



2.4.2 In ‘Interfaces’(1), click the Edit(3) button for ‘wan’(2).



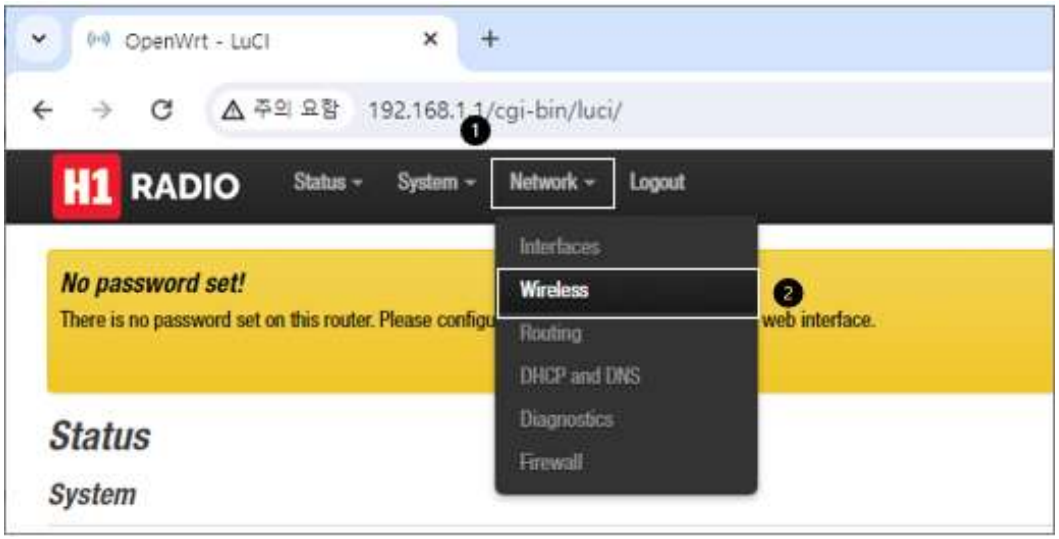
2.4.3 General Settings: Set the basic option values for the setting items below.

No.	Name	Description	Option values
1	Status	WAN Status information	-
2	Protocol	Protocol	DHCP client, DHCPv6 client, Unmanaged, PPP, PPPoE, Static address Default Values: DHCP client
3	Device	Device interface	-
4	Bring up on boot	Bring up on boot	Default: Checked
5	Hostname to send when requesting DHCP	Hostname to send when requesting DHCP	Default: Send
6	Save	Save your settings.	

2.5 Wi-Fi HaLow(900MHz) Network Configuration

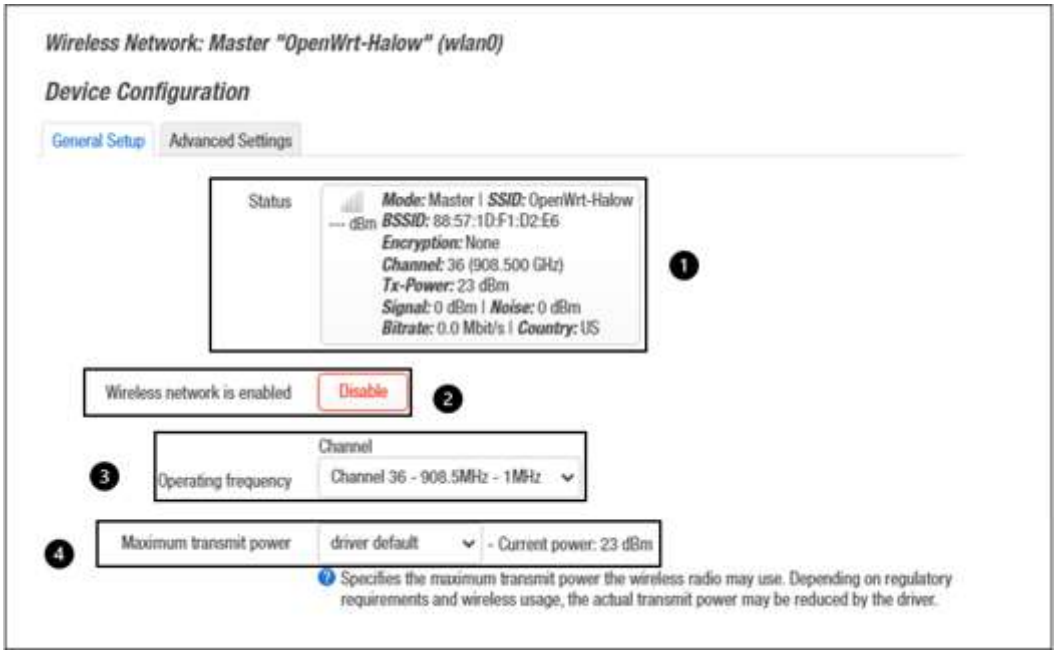
- Configure the operating environment for HaLow. This setting involves configuring the SSID, frequency channel, and encryption method that allow access to HaLow communication terminals.

2.5.1 Connection: Click 'Wireless' (2) from the 'Network' (1) menu.



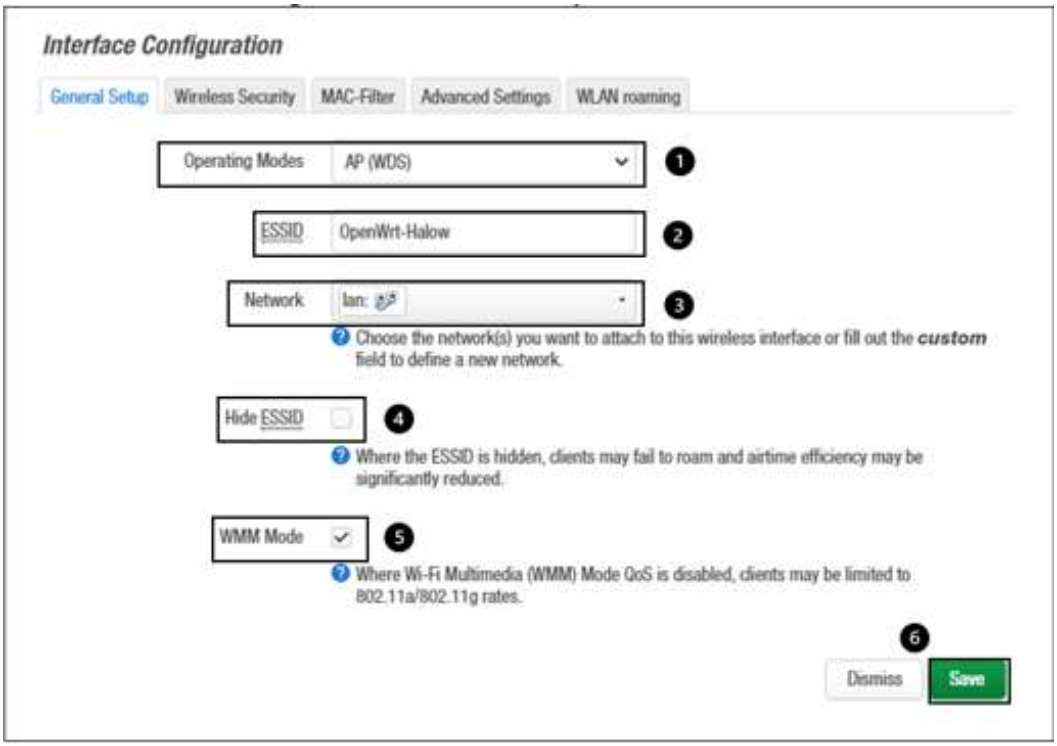
2.5.2 Modify Interface: Click the Edit (3) button for the 'radio1' (2) interface in the 'Wireless Overview' (1) menu.

2.5.3 Device Configuration Menu's General Setup: Set the default option values.



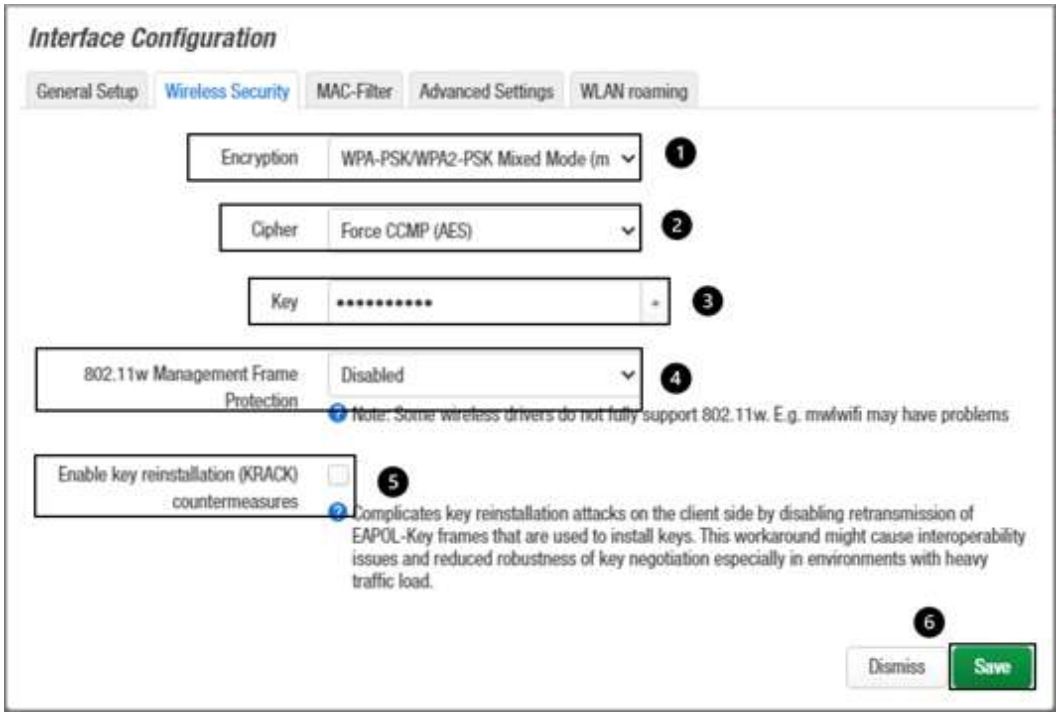
No.	Name	Description	Option values
1	Status	900MHz Wi-Fi status information	-
2	Wireless network is enabled	Use of 900MHz Wi-Fi SSID	Disable, Enable Default: Enable
3	Operation frequency	Displays channel	Channel 36 ~ 116 Default: Channel 36 – 908.5MHz – 1MHz
4	Maximum transmit power	Maximum transmission power	Driver default, 0dBm ~ 23dBm Default: driver default

2.5.4 Interface Configuration's General Setup:



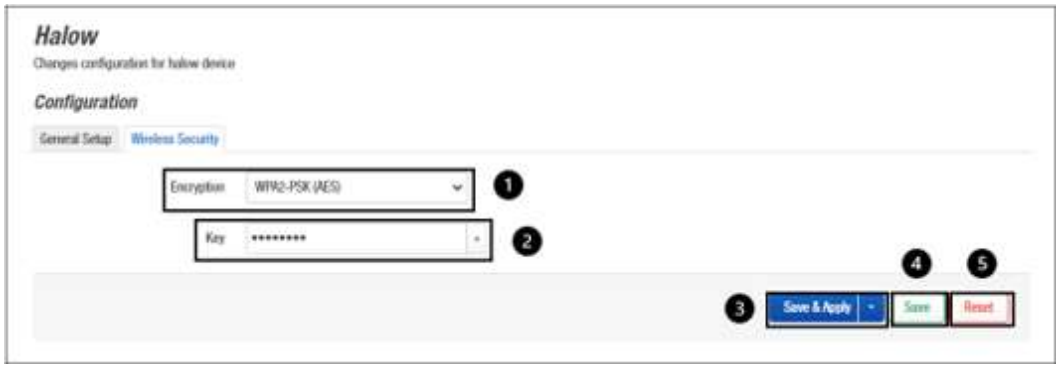
No.	Name	Description	Option values
1	Operating Modes	Display operation modes	AP, Client AP, Ad-Hoc, 802.11s, Pseudo Ad-Hoc(ahdemo), Monitor, AP(WDS), Client AP(WDS) Default: AP(WDS)
2	ESSID	Set ESSID	-
3	Network	Displays interface	Default: lan
4	Hide ESSID	Hide ESSID	Default: unchecked
5	WMM Mode	Wi-Fi Multimedia power saving	Default: checked
6	Save	Save your settings.	

2.5.5 Set encryption option values in Wireless Security of Interface Configuration.Set encryption option values in Wireless Security of Interface Configuration.



No.	Name	Description	Option values
1	Encryption	Display encryption method	WPA2-PSK, WPA3-SAE, WPA2-PSK/WPA3-SAE Mixed Mode, WPA-PSK/WPA2-PSK Mixed Mode, WPA-PSK, OWE, No Encryption Default: No Encryption
2	Cipher	Display security	Auto, Force CCMP(AES), Force TKIP, Force TKIP and CCMP(AES) Default: auto
3	Key	Set password	Default: none
4	802.11w Management Frame Protection	802.11w management frame protection	Disabled, Optional, Required Default: Disabled
5	Enable key reinstallation(KRACK) countermeasures	Activate countermeasures against key reinstallation attacks	Default: unchecked
6	Save	Save your settings.	

2.5.6 Interface Configuration's Wireless Security:



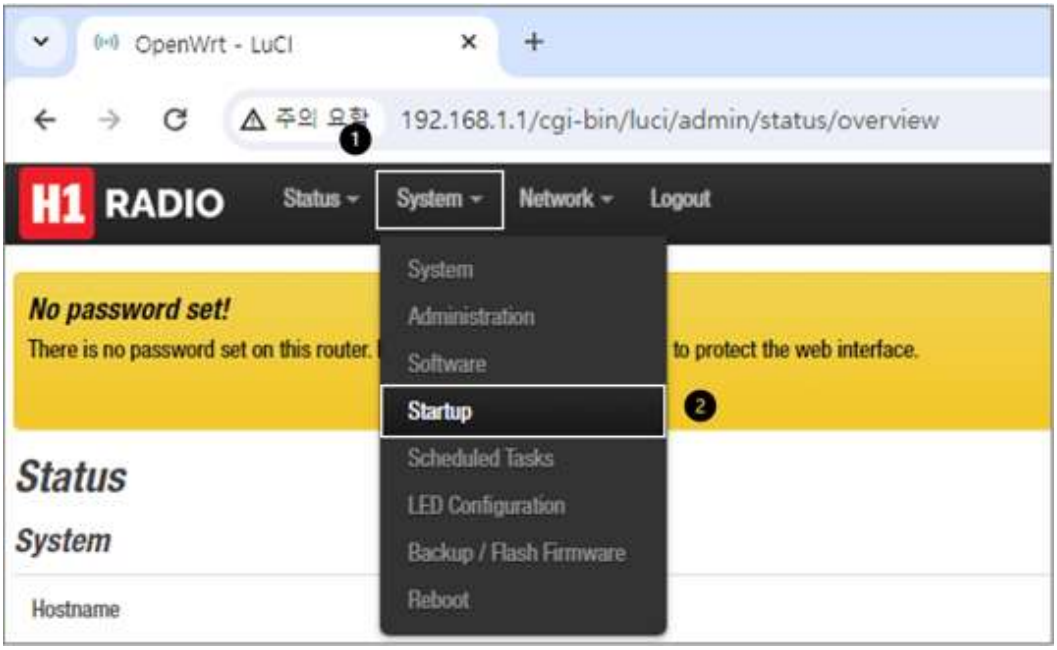
No.	Name	Description	Option values
1	Encryption	Display encryption method	No Encryption, WPA2-PSK(AES), WPA3-OWE, WPA3-SAE Default: No Encryption
2	Key	Set password	Default: blank
3	Save & Apply	Save and apply the settings	
4	Save	Save your settings	
5	Reset	Restore settings to default	

2.2.2. Setting HaLow AP to Bridge Mode

- This sets the HaLow AP from the default NAT mode to Bridge mode.

1 Deactivate Services(disable the NAT feature.)

1.1 Access: Click 'Startup' (2) from the 'System' (1) menu.

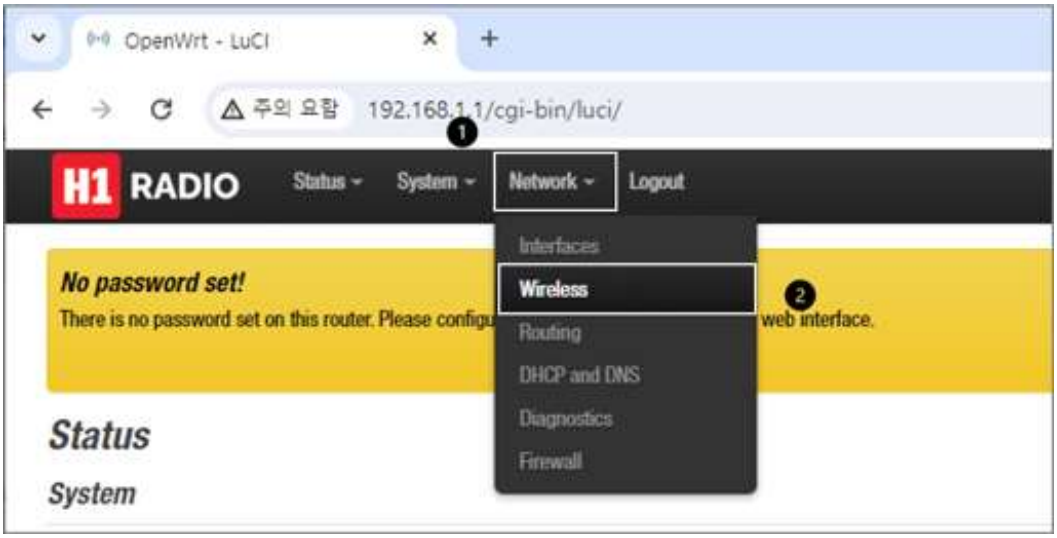


1.2 Deactivate services(disable NAT features): Deactivate the following services in the 'Startup' menu's 'Initscripts'.

- dnsmasq (IPv4 DHCP server daemon)
- firewall (firewall)
- odhcpd (IPv6 DHCP)

2 HaLow Settings

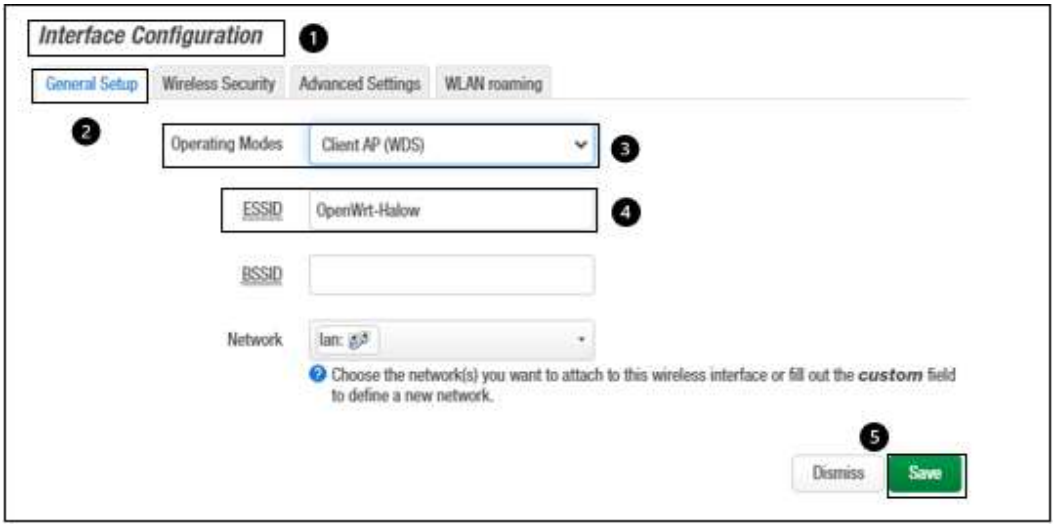
2.1 Access: Click 'Wireless' (2) from the 'Network' (1) menu.



2.2 Modify interface: Click the Edit (3) button next to the 'radio1' (2) interface in the 'Wireless Overview' (1) menu.

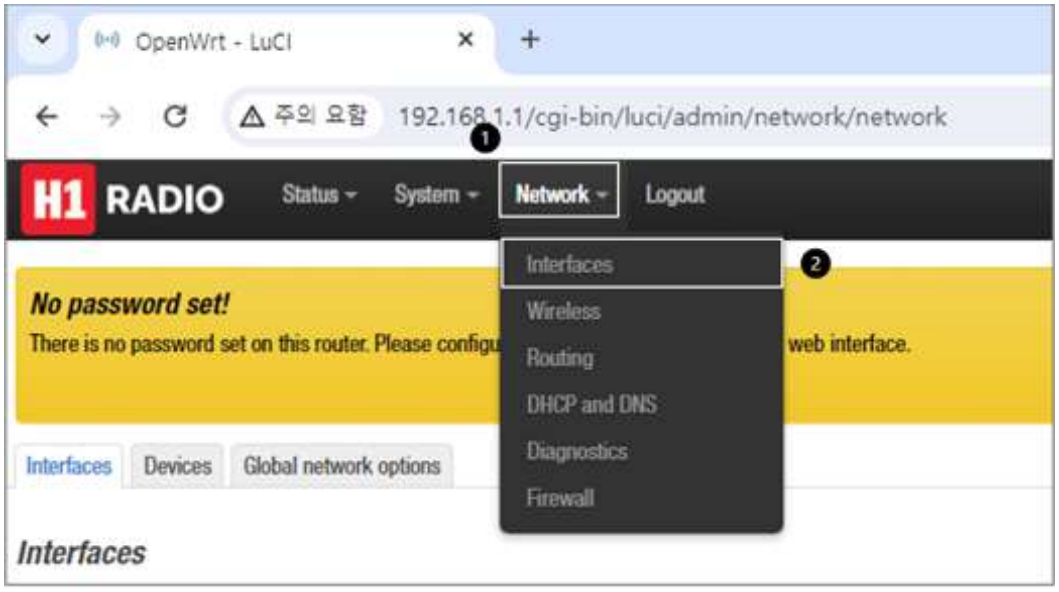
2.3 Interface Configuration(Network Service Settings): Set in the Following Order

2.3.1 Navigate to the 'Interface Configuration' Menu: Access the menu to configure various settings of your network interface.
2.3.2 Select 'General Setup': Choose this option to specify general settings for the network interface.
2.3.3 Select 'Operating Modes': Choose 'Client AP(WDS)' from the list of operating modes. This mode allows the Access Point (AP) to operate in Wireless Distribution System mode, enabling it to act as both an access point and a wireless bridge.
2.3.4 Enter 'OpenWrt-Halow' in the ESSID Field: Set the ESSID (Extended Service Set Identifier) to 'OpenWrt-Halow'. This is the network name that will be broadcasted and visible to other devices.
2.3.5 Click the 'Save' Button: Save the settings to ensure that all the changes made are applied and preserved.

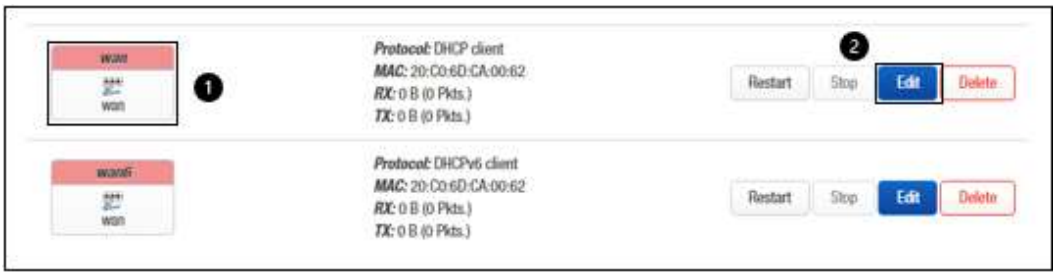


3 WAN Settings

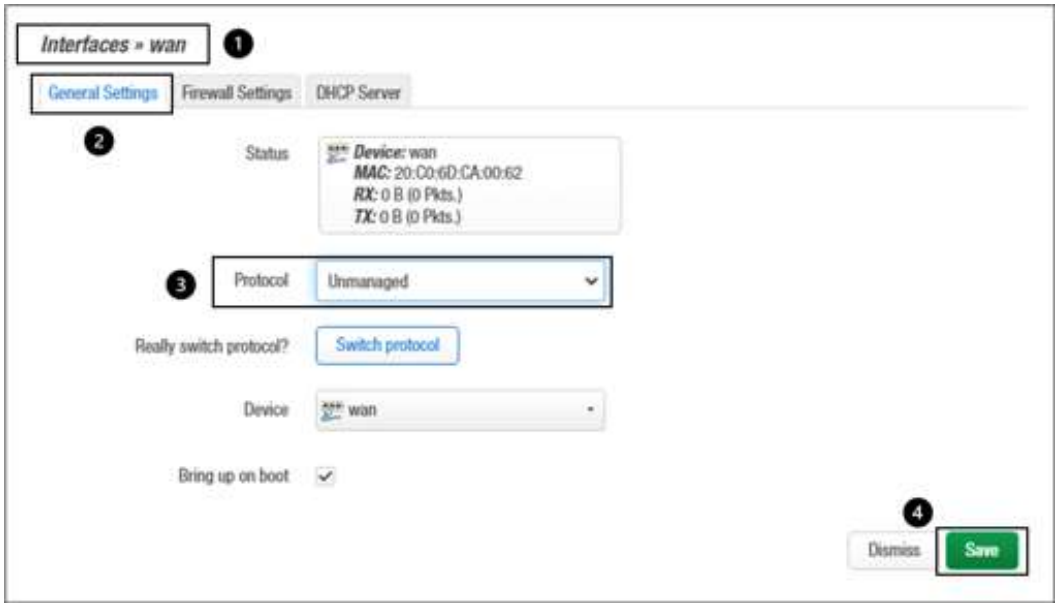
3.1 Access: Click 'Interfaces' (2) from the 'Network' (1) menu.



3.2 Modify interface: Click the Edit (2) button on the 'wan' (1) interface in the 'Interfaces' menu.

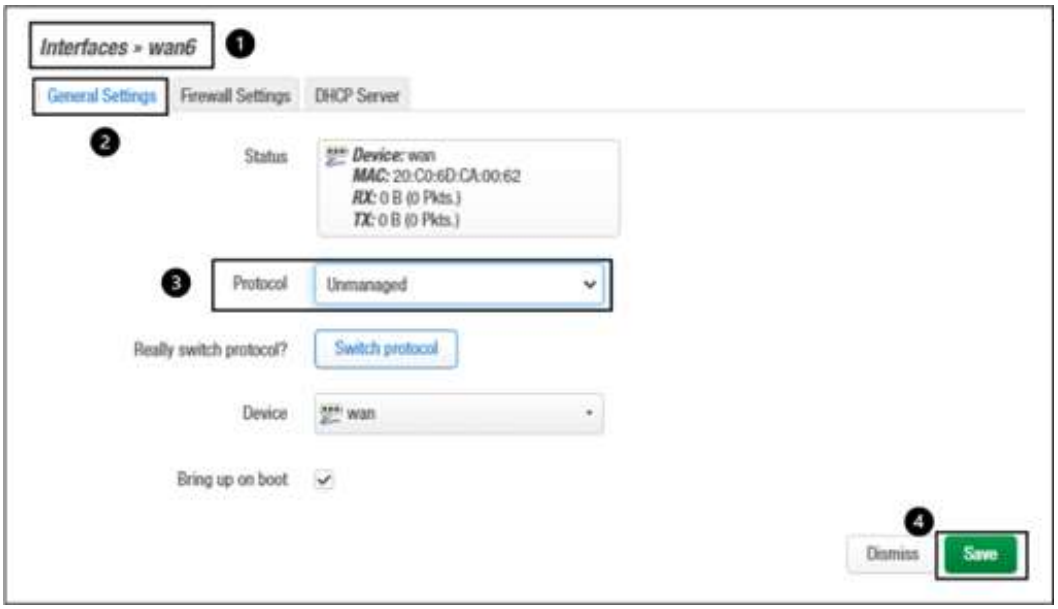


3.3 Protocol settings: Set the Protocol to 'Unmanaged' (3) in the 'General Settings' (2) of 'Interfaces >> wan' (1) and then click the Save (4) button.



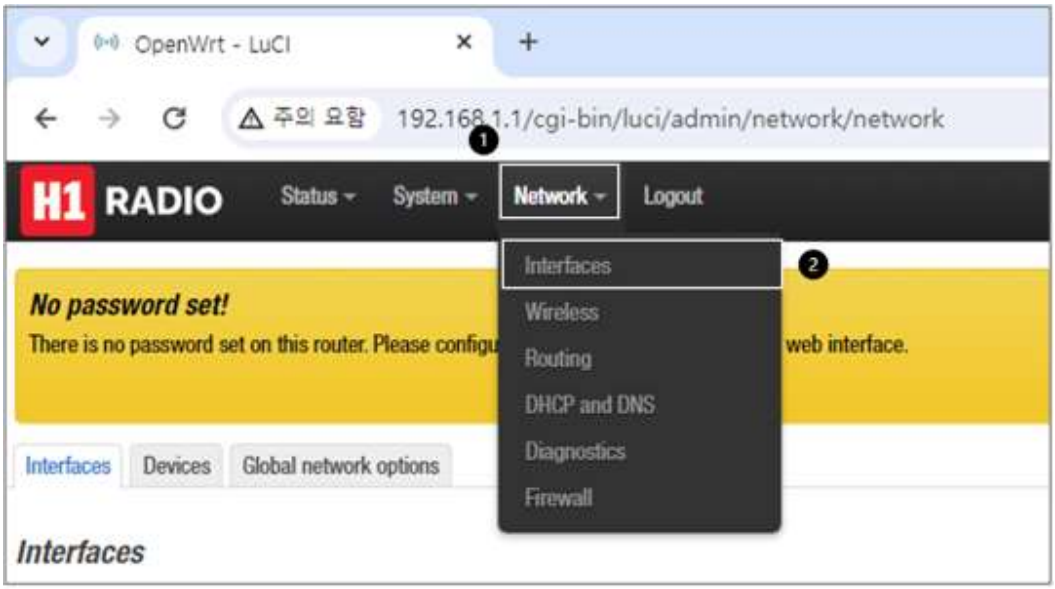
3.4 Interface modification: In the same way, change the settings of the ‘wan6’ (1) interface by clicking the ‘Edit’ (2) button.

3.5 Protocol settings: In ‘General Settings’ (2) of ‘Interfaces >>wan6’ (1), set ‘Protocol’ to ‘Unmanaged’ (3) and click the ‘Save’ (4) button.

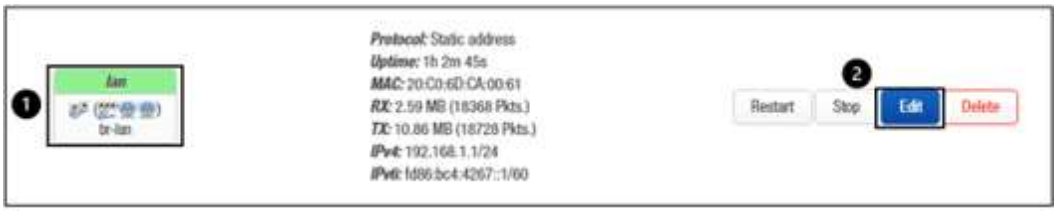


4 LAN Settings

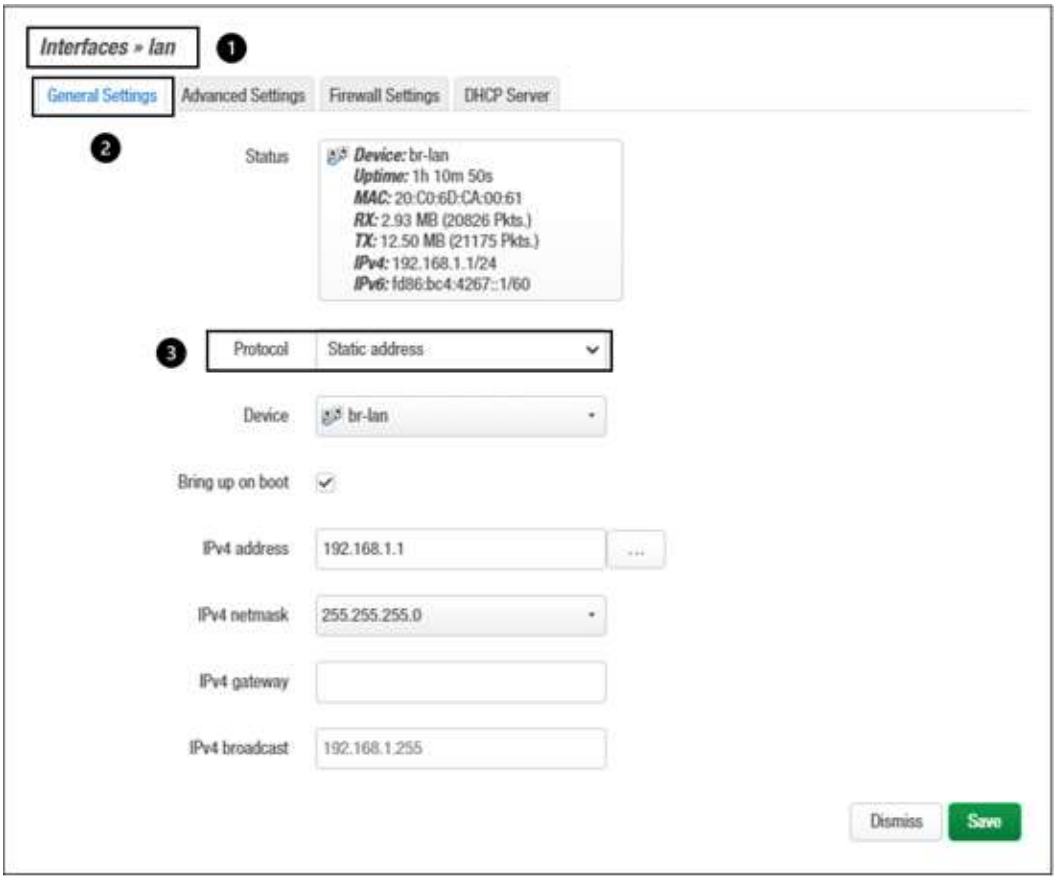
4.1 Access: Click 'Interfaces' (2) from the 'Network' (1) menu.



4.2 Modify interface: Click the 'Edit' (2) button on the 'lan' (1) interface in the 'Interfaces' menu.



4.3 Protocol settings: Set the protocol in the General Settings (2) of the 'lan' (1) interface to either 'Static address' (default) or 'DHCP client'.

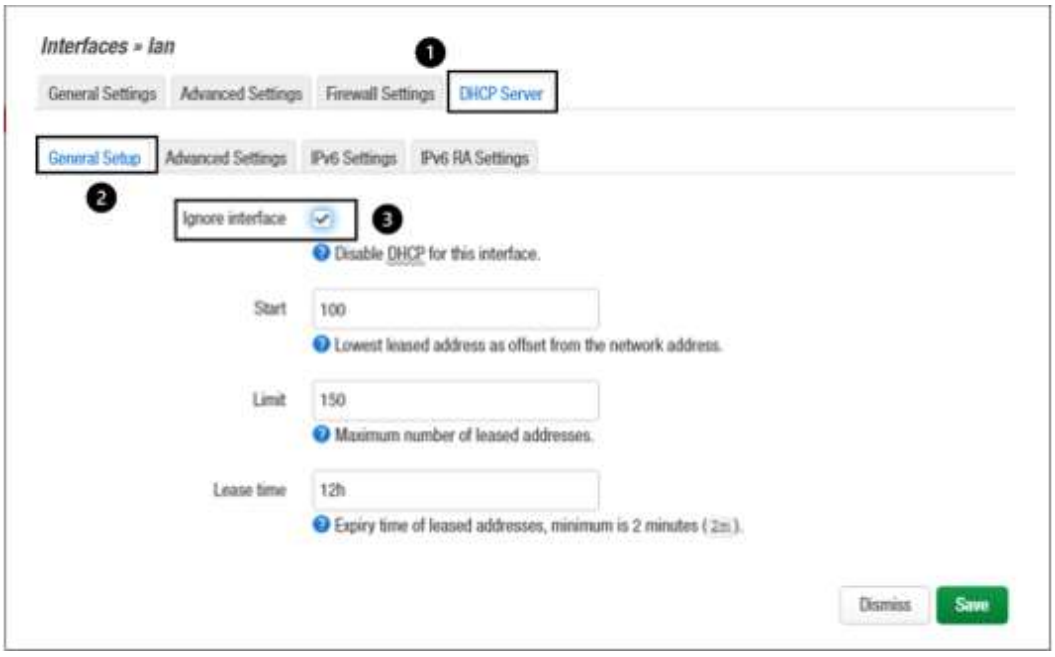


4.3.1 Set Protocol to 'Static address' (1): Set the IPv4 address to '192.168.1.100' (2), the IPv4 netmask to '255.255.255.0' (3), and the IPv4 broadcast to '192.168.1.255' (4).

4.3.2 Set Protocol to 'DHCP client' (1): Operate as a DHCP client.

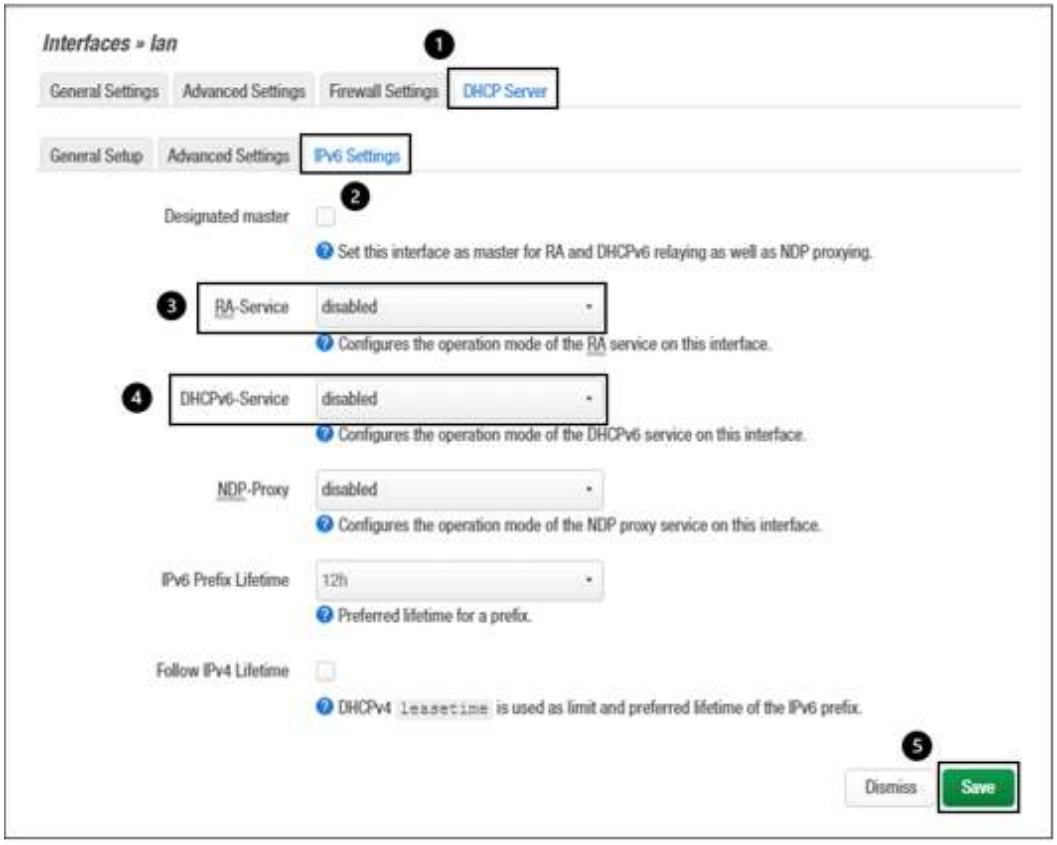
✓ When setting the protocol to 'DHCP client', you must factory reset the HaLow AP to enable web server access. (Factory reset method: Refer to the 'Reset button to restore factory settings' feature in section '3. System Maintenance' of the HaLow AP user manual.)

4.4 Configure DHCP Server: In the 'General Setup' (2) of the 'DHCP Server' (1), check the 'Ignore interface' (3) option.

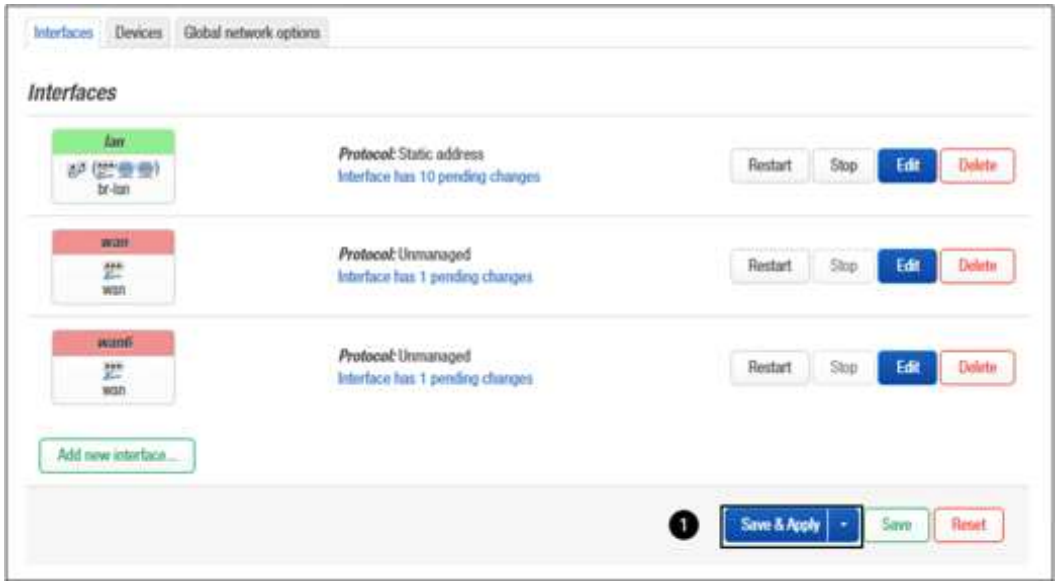


4.5 Set IPv6 Settings: Follow these steps:

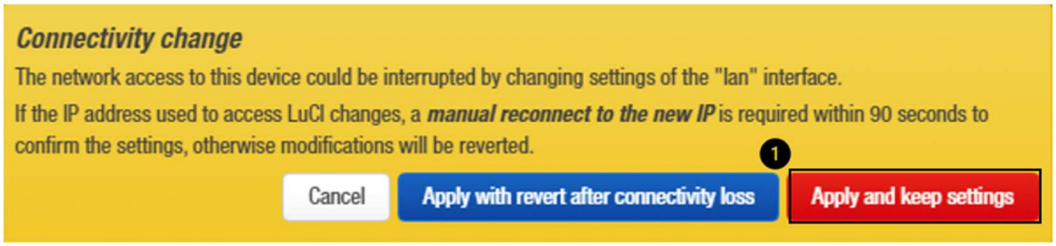
1. Navigate to the 'DHCP Server' menu.
2. Select 'IPv6 Settings'.
3. Set the 'RA-Service' option to 'disabled'.
4. Set the 'DHCPv6-Service' option to 'disabled'.
5. Click the 'Save' button to save the changes.



5 Apply Settings: Click the 'Save & Apply' (1) button to apply the settings.



6 Final Application: Click the 'Apply and keep settings' (1) button to complete all settings.

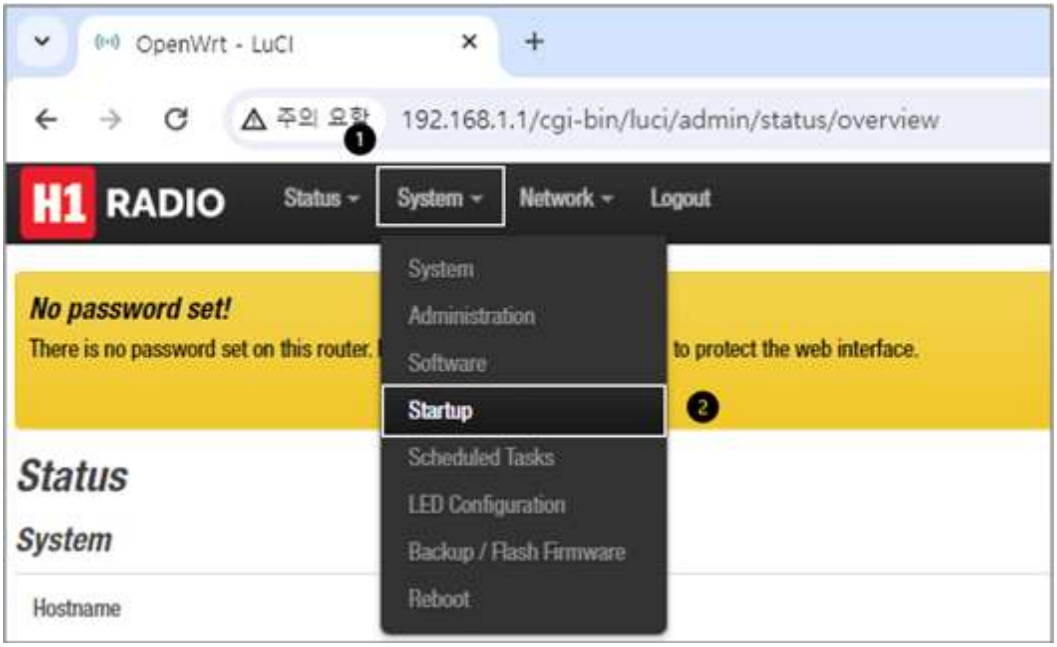


2.2.3. Setting HaLow AP from Bridge Mode back to NAT Mode

This section describes the procedure to switch a HaLow Access Point (AP) from Bridge mode to Network Address Translation (NAT) mode.

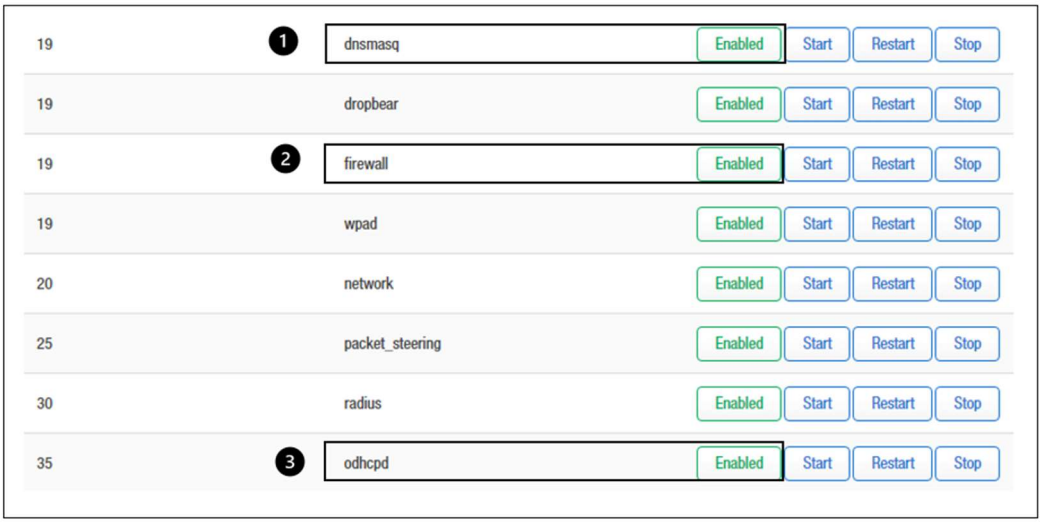
1 Activate Services

1.1 Access: Click 'Startup' (2) in the 'System' (1) menu.



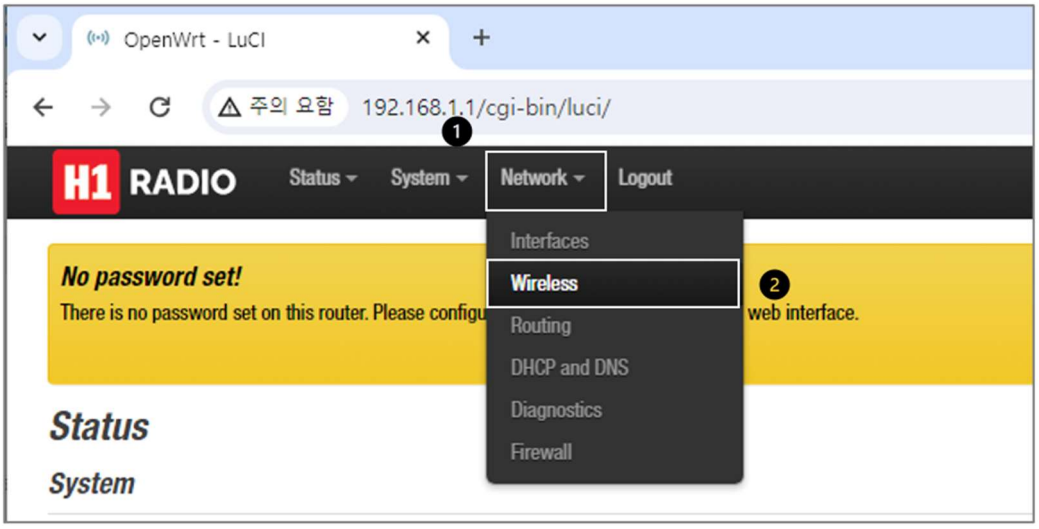
1.2 Activate services: In the 'Startup' menu's 'Initscripts', activate the following services:

- dnsmasq (IPv4 DHCP server daemon)
- firewall (firewall)
- odhcpd (IPv6 DHCP)

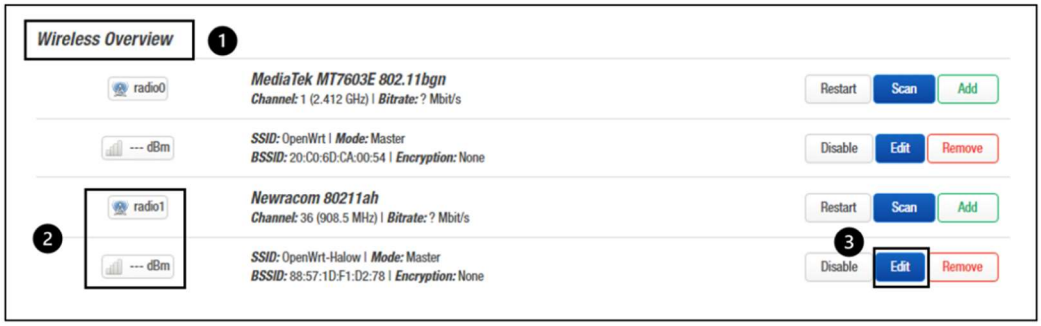


2 HaLow Settings

2.1 Access: Click 'Wireless' (2) in the 'Network' (1) menu.

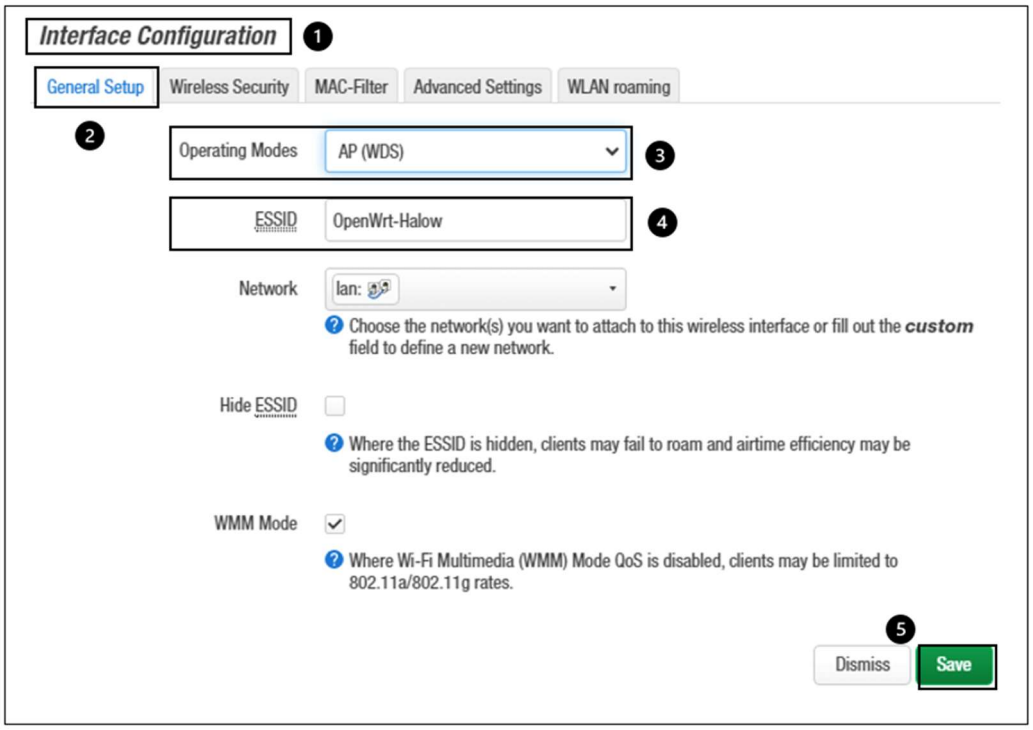


2.2 Modify interface: Click the 'Edit' (3) button next to the 'radio1' (2) interface in the 'Wireless Overview' (1) menu.



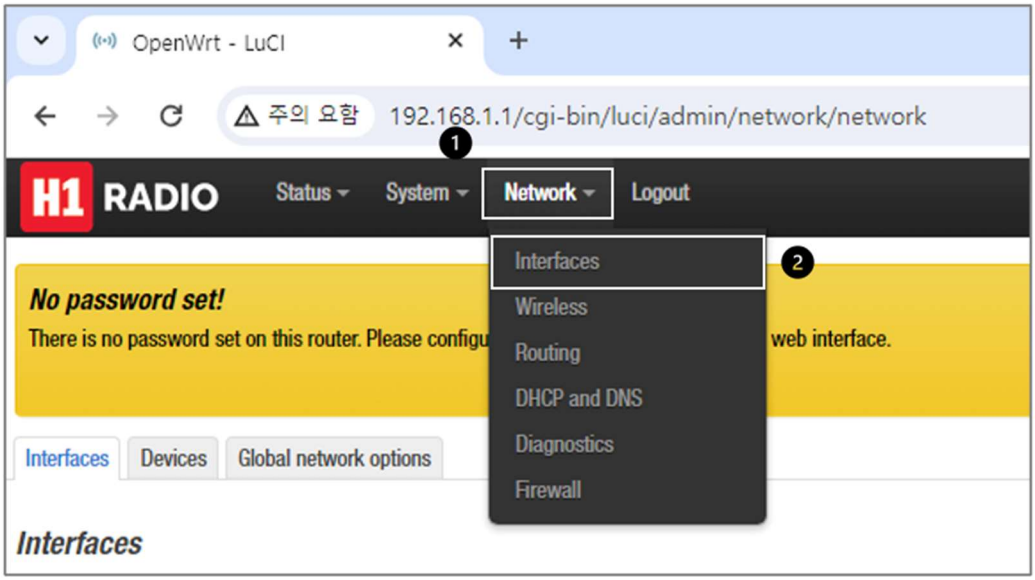
2.3 Interface Configuration: Set in the Following Order

1. Navigate to the 'Interface Configuration' Menu: Access the menu to configure various settings of your network interface.
2. Select 'General Setup': Choose this option to specify general settings for the network interface.
3. Select 'Operating Modes': Choose 'AP(WDS)' from the list of operating modes. This mode allows the Access Point (AP) to operate in Wireless Distribution System mode, enabling it to act as both an access point and a wireless bridge.
4. Enter 'OpenWrt-Halow' in the ESSID Field: Set the ESSID (Extended Service Set Identifier) to 'OpenWrt-Halow'. This is the network name that will be broadcasted and visible to other devices.
5. Click the 'Save' Button: Save the settings to ensure that all the changes made are applied and preserved.

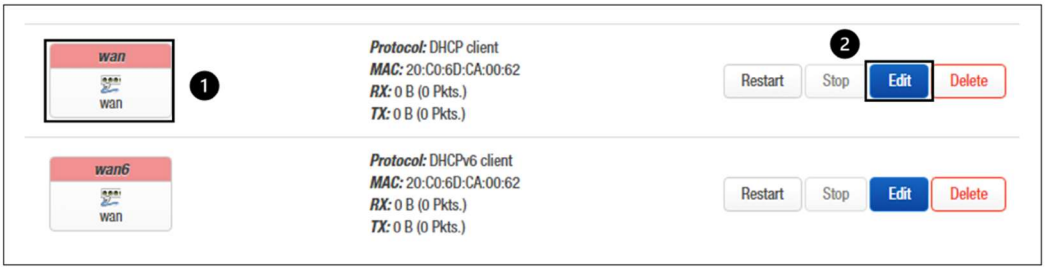


3 WAN Settings

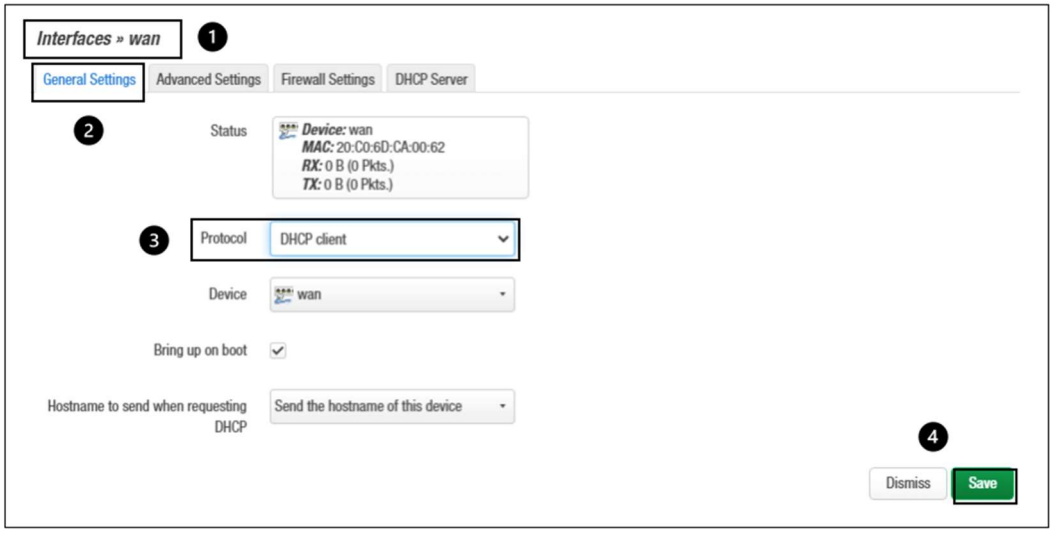
3.1 Access: Click 'Interfaces' (2) in the 'Network' (1) menu.



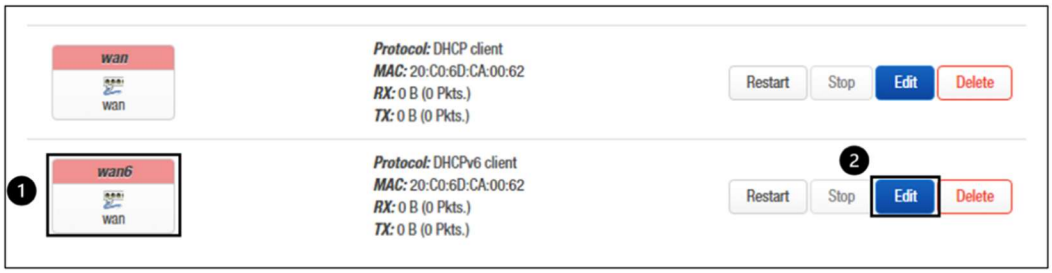
3.2 Modify interface: Click the 'Edit' (2) button for the 'wan' (1) interface in the 'Interfaces' menu.



3.3 Protocol settings: Set the protocol to 'DHCP client' (3) in the 'General Settings'(2) of 'Interfaces >> wan' (1) and then click the 'Save' (4) button.

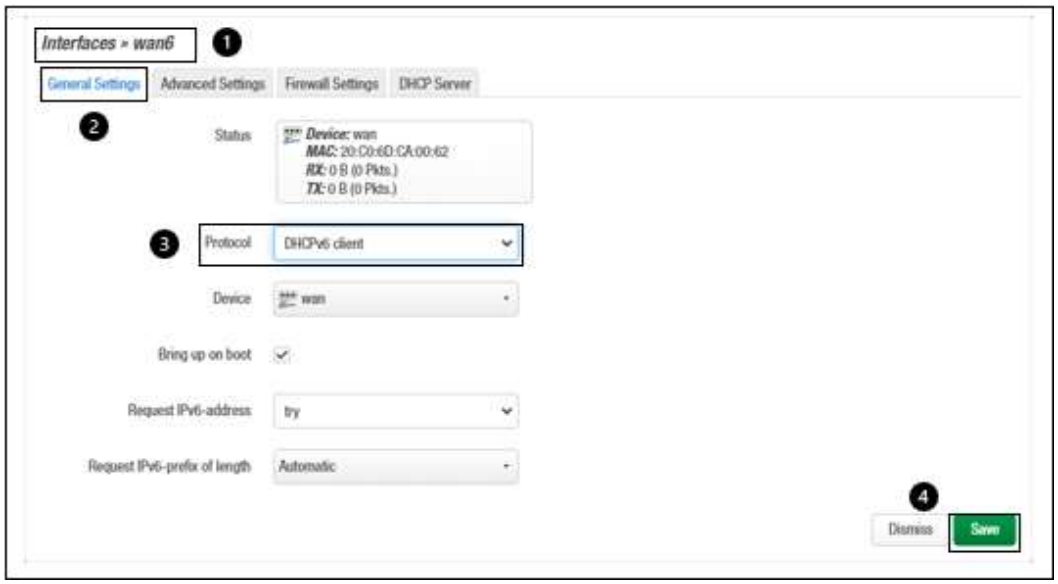


3.4 Modify Interface: Change the 'wan6' (1) Interface Settings Using the Same Method.



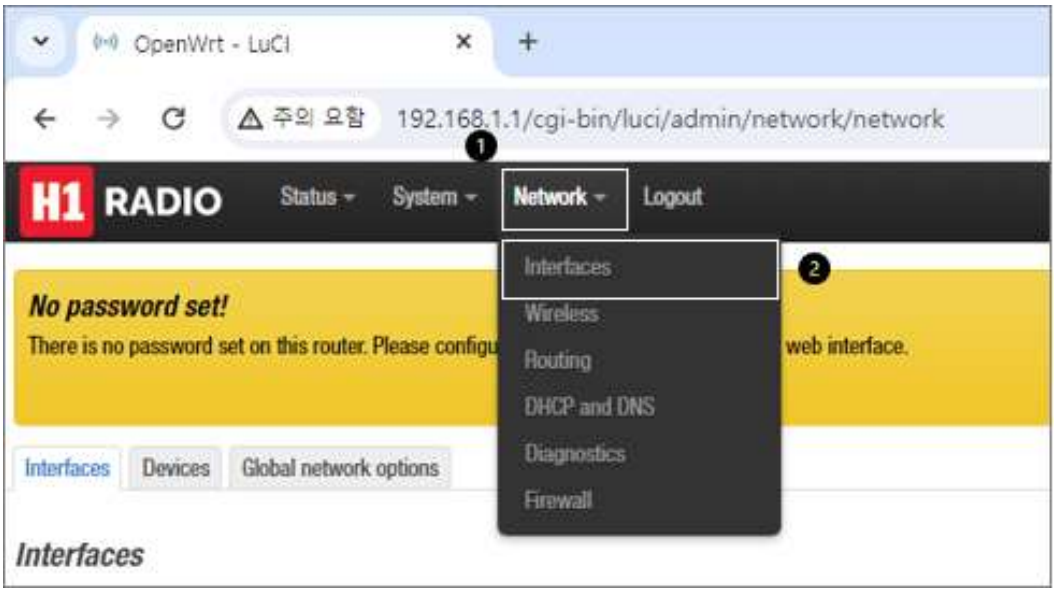
3.5 Protocol Settings: Configure the 'wan6' (1) Interface as a 'DHCPv6 client.

1. Navigate to 'Interfaces >> wan6' (1): Access the settings specific to the 'wan6' interface, which is typically used for handling IPv6 WAN (Wide Area Network) traffic.
2. Go to 'General Settings' (2): Enter the General Settings section of the 'wan6' interface.
3. Set 'Protocol' to 'DHCPv6 client' (3): Select 'DHCPv6 client' from the protocol options. This setting will configure the interface to automatically receive IPv6 address and other configuration details from a DHCPv6 server.
4. Click the 'Save' Button (4): Save the changes to apply the new protocol settings. This ensures that the 'wan6' interface will operate as a DHCPv6 client, dynamically receiving its IPv6 configuration.

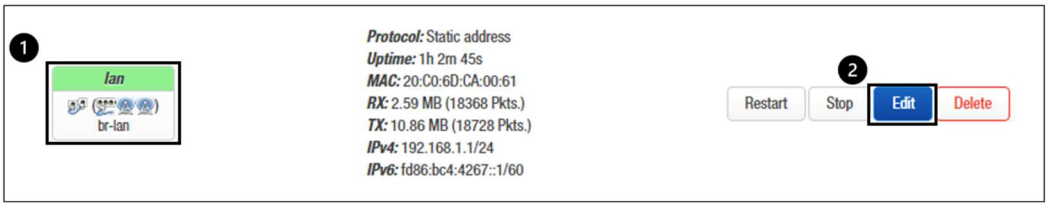


4 LAN Settings

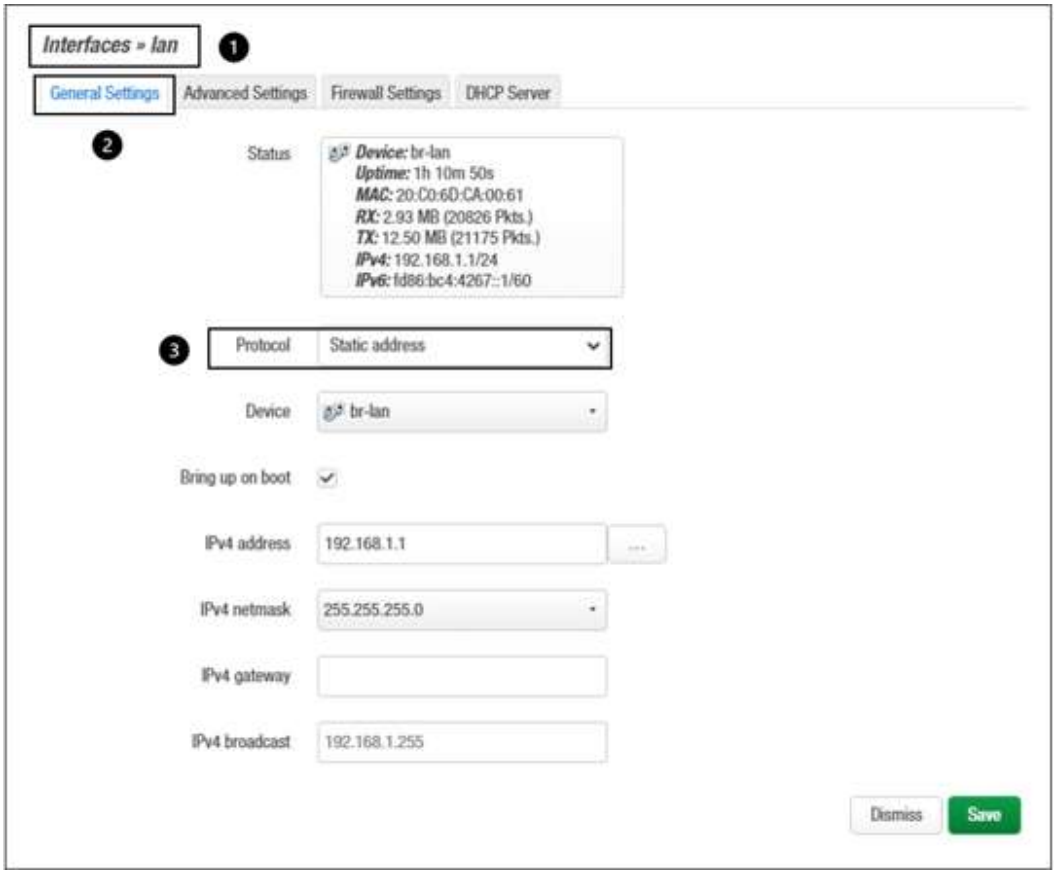
4.1 Access: Click 'Interfaces' (2) in the 'Network' (1) menu.



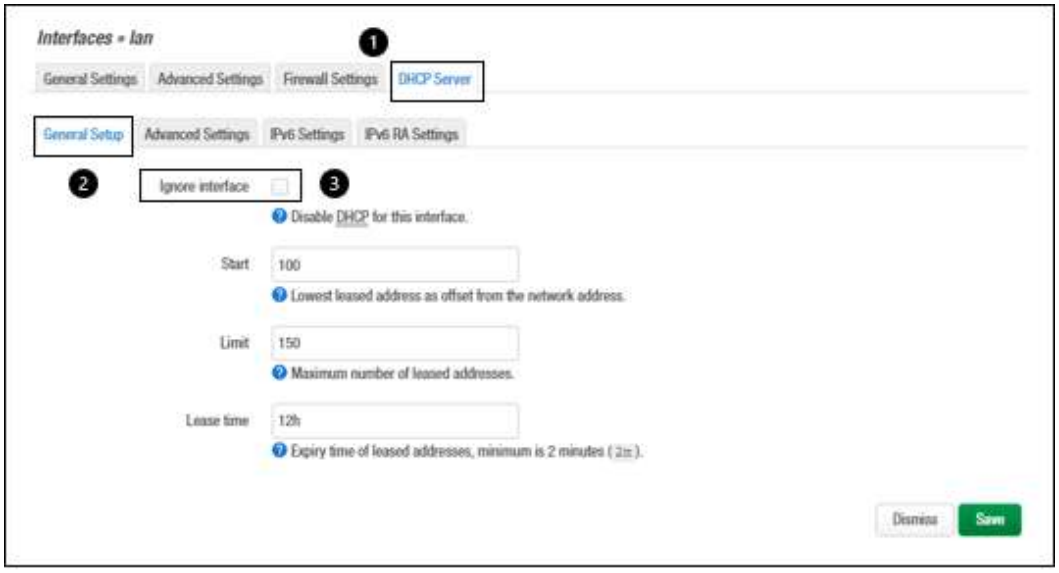
4.2 Modify Interface: Click the 'Edit' (2) button for the 'lan' (1) interface in the 'Interfaces' menu.



4.3 Protocol Settings: In the 'General Settings' (2) of 'Interfaces >> lan' (1), set the Protocol (3) to 'Static address'.

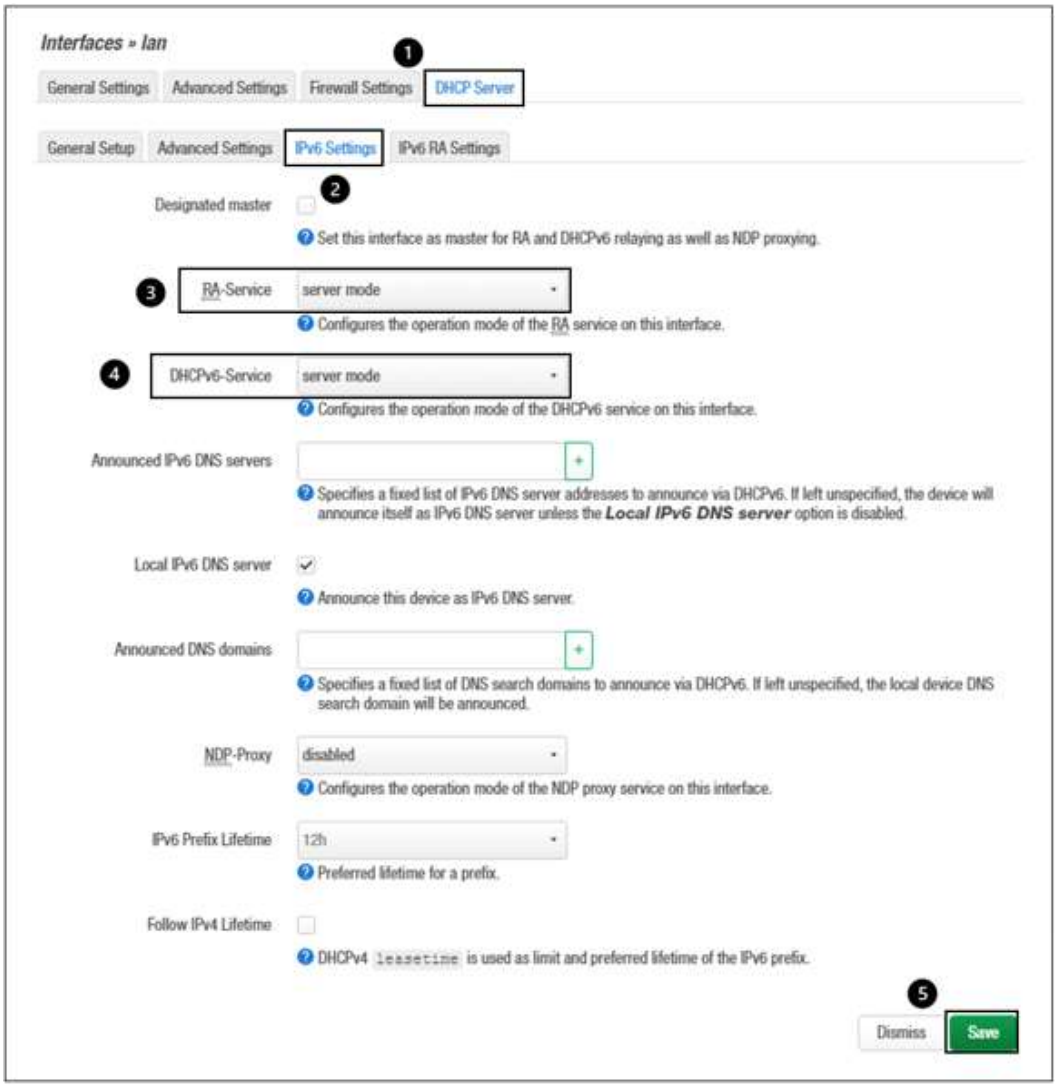


4.4 Configure DHCP Server: In the 'General Setup' (2) of the 'DHCP Server' (1), uncheck the 'Ignore interface' (3) option.

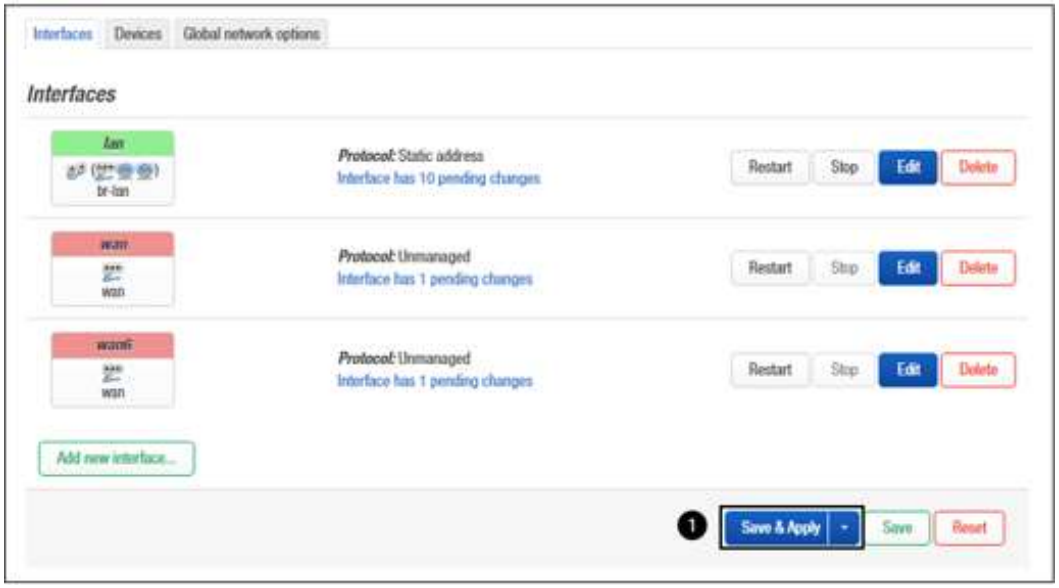


4.5 Set IPv6 Settings: Configure the settings in the following order:

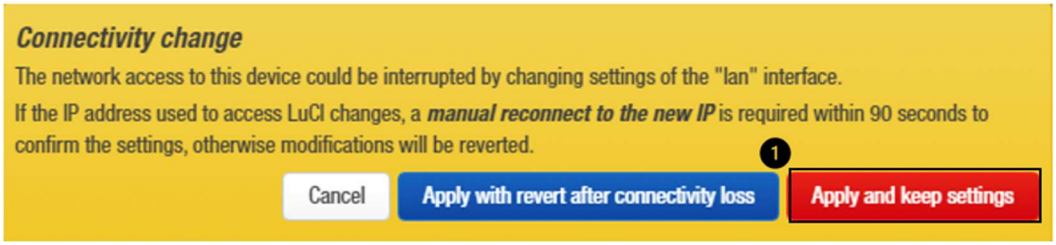
1. Navigate to the 'DHCP Server' Menu: Access this menu to manage DHCP server settings, including IPv6 configurations.
2. Select 'IPv6 Settings': Choose this option to configure the IPv6-specific settings of your DHCP server.
3. Set 'RA-Service' to 'server mode': Configure the Router Advertisement (RA) service to operate in 'server mode'. This setting allows the DHCP server to send IPv6 router advertisements, helping IPv6 clients on the network configure themselves automatically.
4. Set 'DHCPv6-Service' to 'server mode': Enable the DHCP server to assign IPv6 addresses to clients automatically. Setting this to 'server mode' ensures that IPv6 addresses, and other related network configuration parameters are dynamically distributed to clients.
5. Click the 'Save' Button: Save the changes to apply your IPv6 settings. This step is crucial to ensure that the configurations take effect and that the network operates smoothly with IPv6 addressing and service advertisement.



5 Apply Settings: Click the 'Save & Apply' (1) button to implement the changes you have made.



6 Final Application: Click the 'Apply and keep settings' (1) button to finalize all configurations.



3. System maintenance

3.1. Firmware update

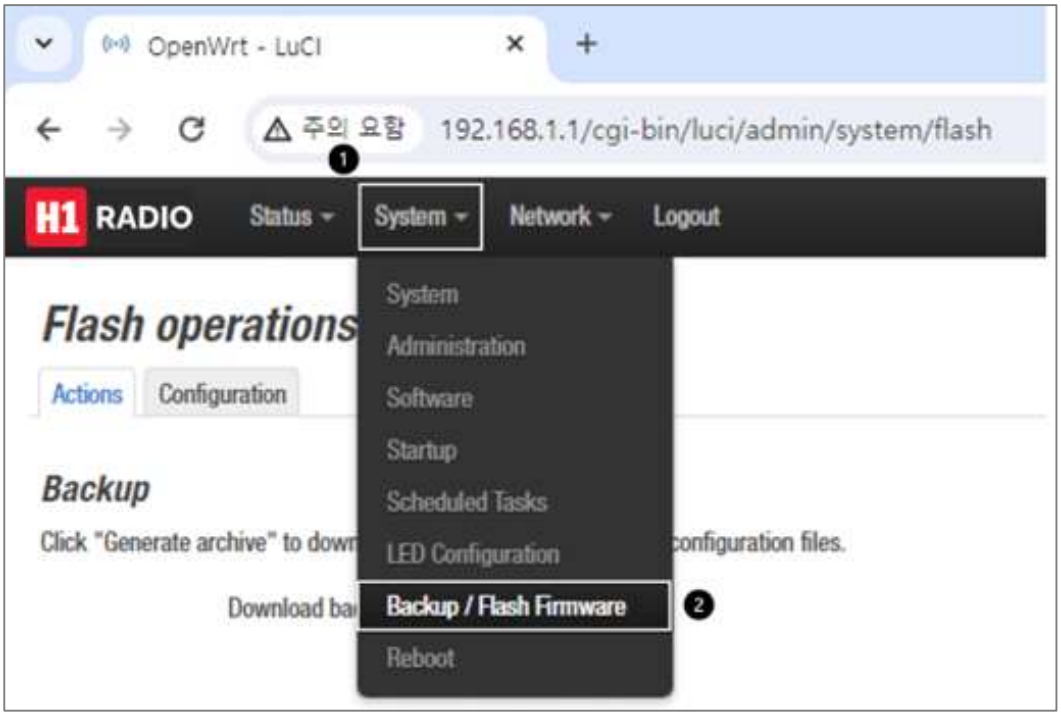
Describes the procedure for updating the firmware that runs the CG16HSS33B System.

1. Download the CG16HSS33B model firmware of the HaLow AP to your PC.
2. Use a web browser to access the Web server firmware update page for the CG16HSS33B model.

- Updating the firmware

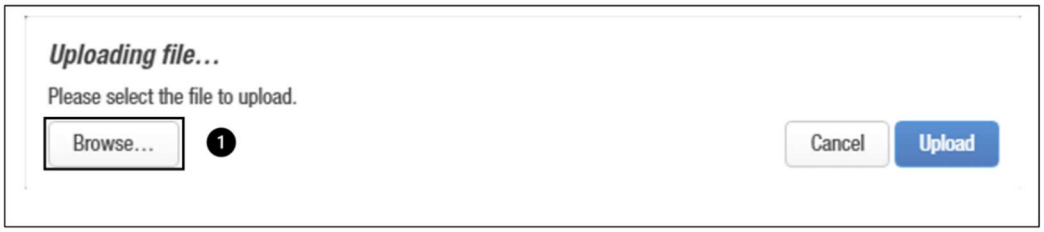
  Describes the procedure for updating the firmware.

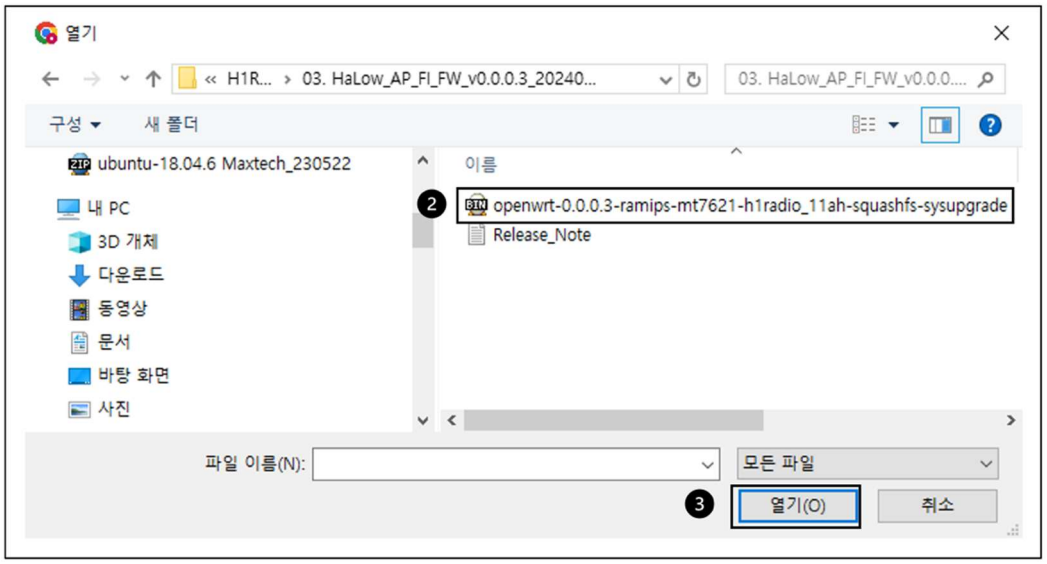
  A. Click ‘System(1) → Backup / Flash Firmware(2)’ on the WEB screen.



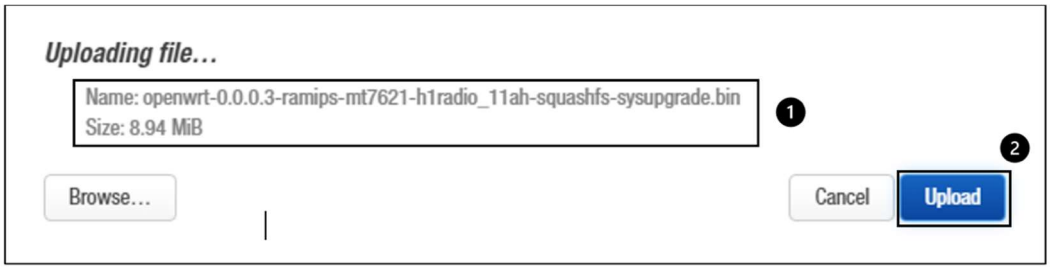
B. Click the 'Flash image.' (1) button of Flash new firmware image in Actions of Flash operations.

C. Uploading file. pop-up window will appear. In the pop-up window, click the ‘Browse.’ button (1) to select the firmware update file downloaded to your PC (2) and click the ‘Open’ button (3).



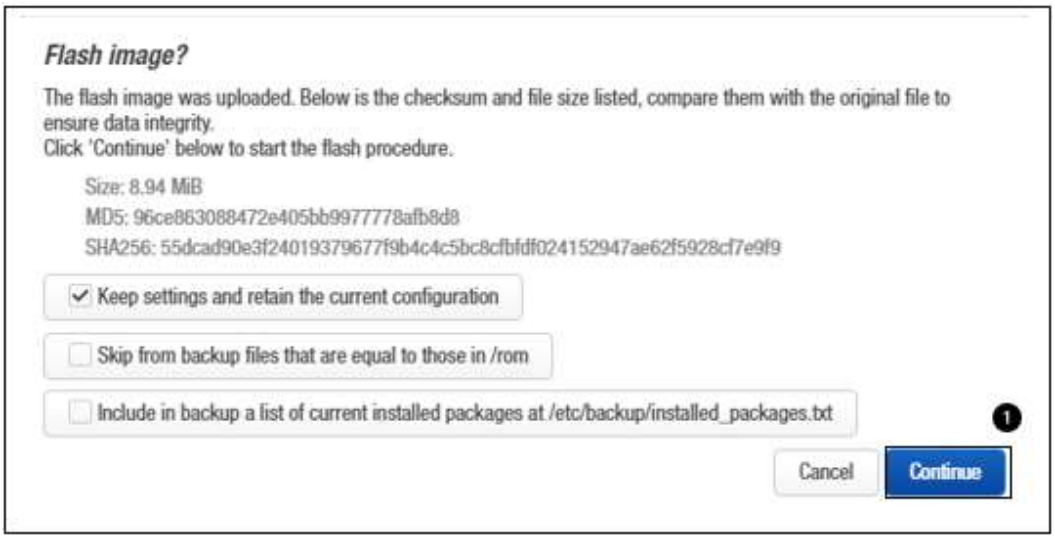


D. Back in the Uploading file… When you return to the pop-up window, the 'Firmware file name, size' (1) will be displayed. Click the 'Upload' button (2).



E. The progress bar moves to upload the file.

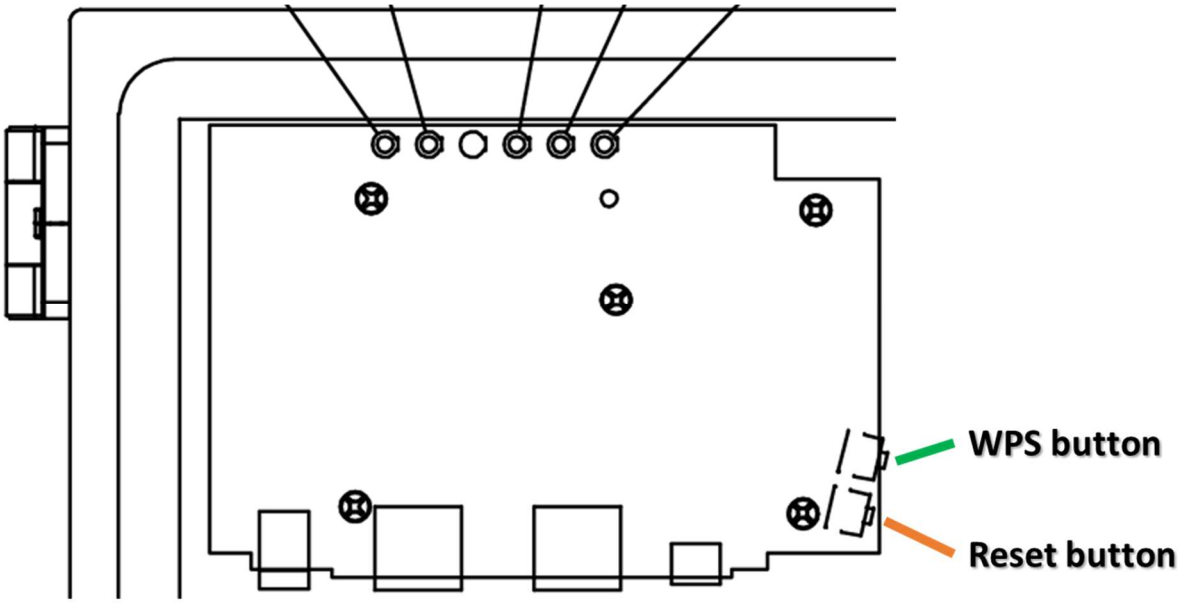
F. Click the 'Continue' button (1) to proceed with the firmware update.



3.2. Reset to the factory defaut settings.

3.2.1. Using push buttons

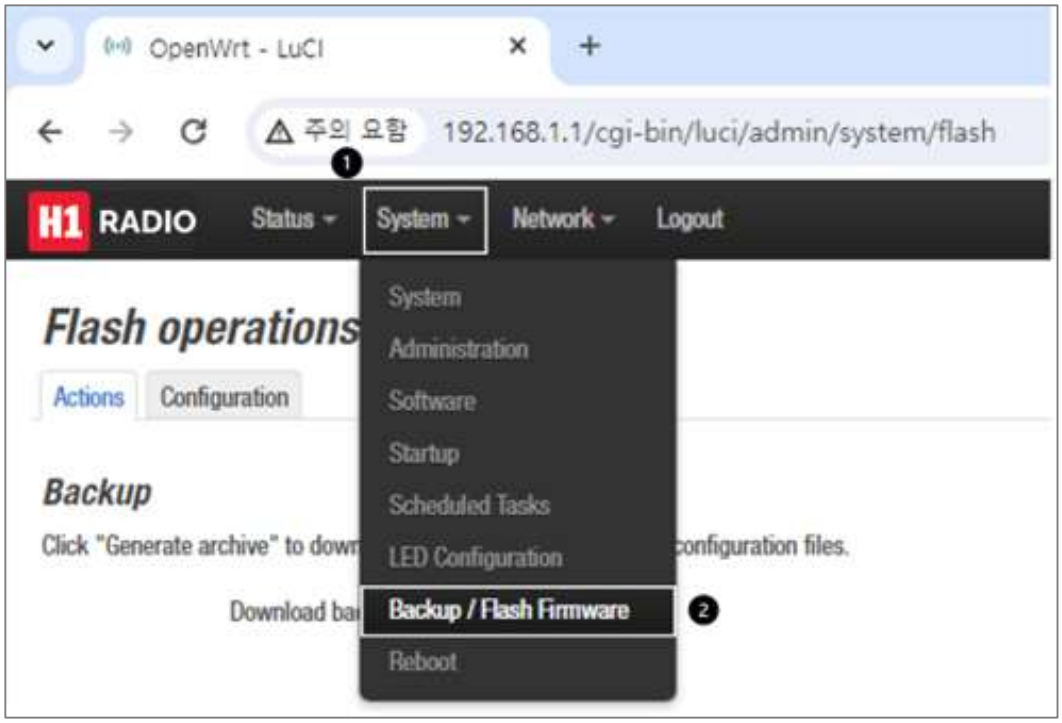
1. Press and hold the Reset button on the side of the product for 5 seconds, release it as shown in the image below.



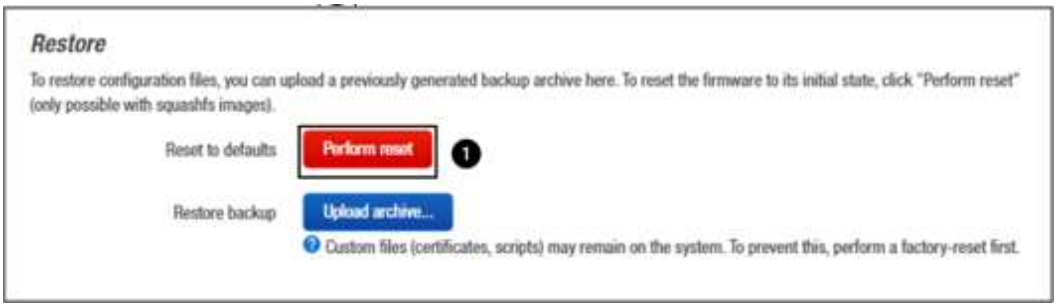
2. The front LEDs will turn off and the system will reboot.

3.2.2. Resetting from the WEB UI

1. Click ‘System(1) → Backup / Flash Firmware(2)’ on the WEB screen.



2. Click the 'Perform reset' (1) button under Reset to defaults in Restore.

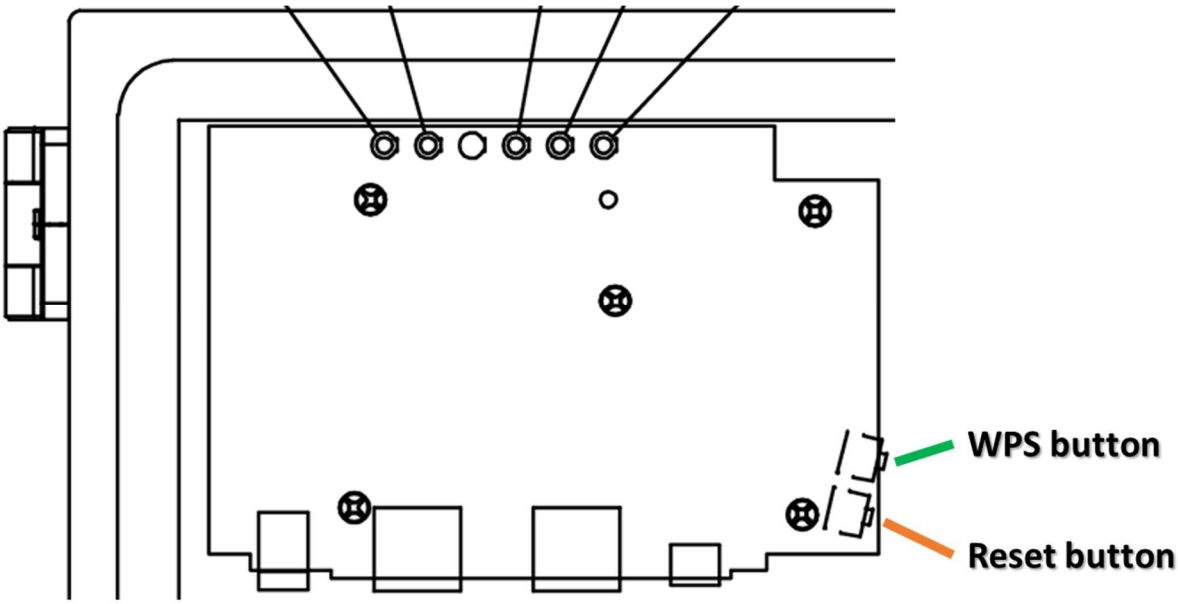


3. Click the ‘OK’ (1) button in the pop-up window, and the system will reboot.

3.3. How to Use the WPS button Function

3.3.1. Using push button

- The WPS button is located on the side of the product as shown in the image below.



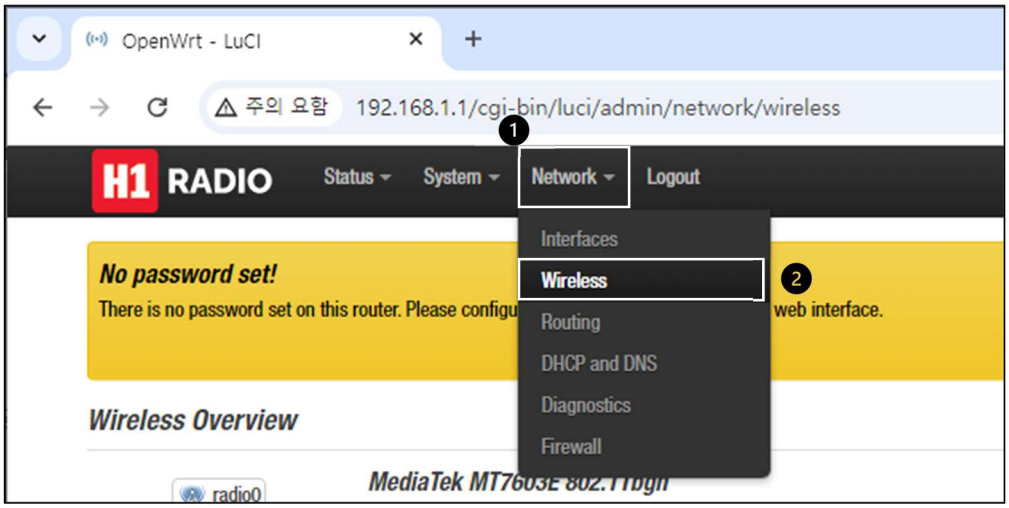
3.3.2. WPS Function Description

1. There is no WPS LED.
2. There is no WPS stop function. After starting WPS, wait 2 minutes and then restart it.
3. Enable WPS on only one wireless network at a time, if possible. (Running multiple WPS processes simultaneously may cause issues.)
4. Only WPS PBC (Push Button Configuration) mode is supported.

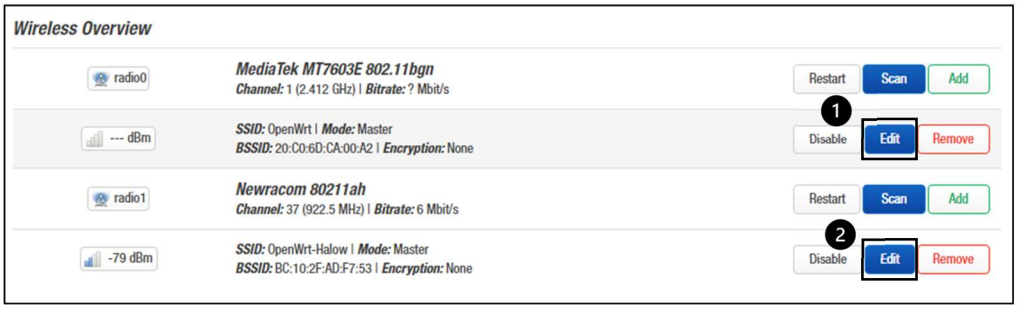
3.3.3. How to Use the WPS Function

1. How to turn on the WPS function: Wireless password setup

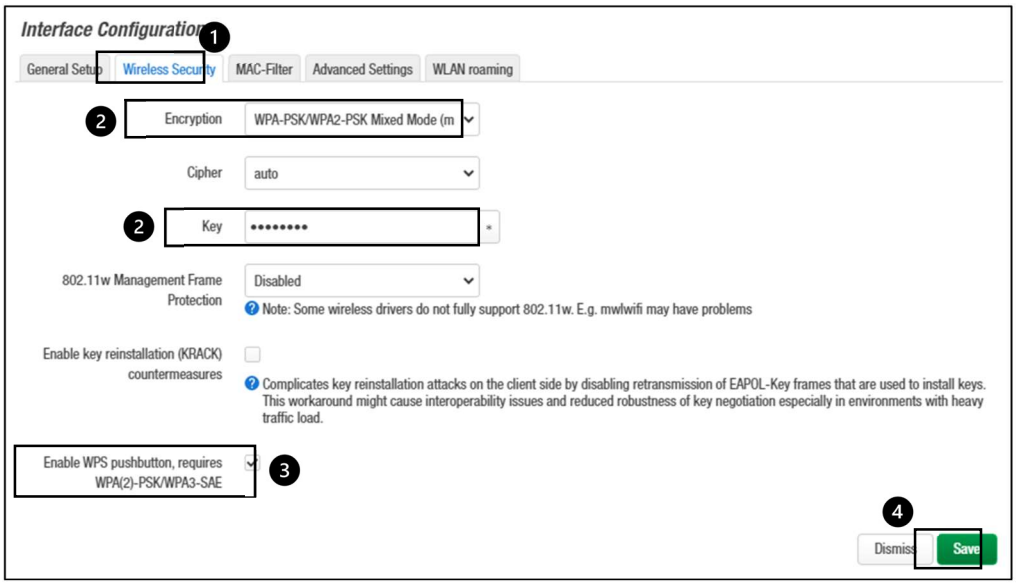
   A. In the 'Network' (1) menu, click on 'Wireless' (2).



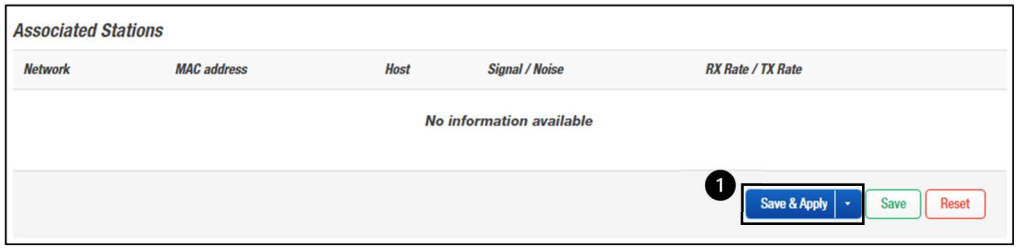
   B. In the 'Wireless Overview' menu, click the 'Edit' button for either '900MHz' (2).



C. In the 'Interface Configuration' menu, go to the 'Wireless Security' (1) tab, set 'Encryption' to 'WPA-PSK/WPA2-PSK' and configure the 'Key' (2). Then, check the 'Enable WPS pushbutton...' (3) option, and click the 'Save' (4) button to save the settings.



D. Click the 'Save & Apply' (1) button to complete the configuration.



2. How the WPS button works

Button Press Time	Mode	Description
Less than 3seconds	AP(WDS) Mode	Starts all APs with AP (WDS) mode for the wireless network.
More than 3seconds	Client(WDS) Mode	1. Starts all Clients with Client (WDS) mode for the wireless network. 2. Settings are saved after successful WPS connection.

3.4. System specifications

Item		Description
Wi-Fi HaLow	Standard	IEEE802.11ah 920MHz can be used at the same time
	Encryption Settings	AES (WPA2-Personal, WPA3-Personal)
	Networking Management Utils	wpa_supplicant, hostapd
	Frequency Band	902 ~ 928MHz, 1T * 1R
	Channel Band Width	1/2/4MHz
	Data Rate	Max. 15Mbps
	TX Power	23dBm@MCS10, 13dBm@MCS7
	RX Sensitivity	-106dBm@MCS10, -87dBm@MCS7
	Modulation	OFDM (BPSK, QPSK, 16QAM, 64QAM)
	Antenna	External (2.5dBi, Omni directional)
WAN		1-port 10/100/1000Base-T (with IEEE802.3af PoE)
WAN port Surge protection	Maximum Discharge Current (Imax)	20kA
LAN		1-port 10/100/1000Base-T
Buttons		1* Reset
Operating Environment		Temperature: -20 ~ 50℃ Humidity: 10~90% (non-condensing)
LED		SYS, HaLow, LAN, WAN
Weight		2.3kg
Size		250(W) x 250(D) x 115(H)mm
Power		PoE IEEE802.3af, Class0, 15.4W

Terminology

900MHz Wi-Fi (HaLow) AP	A HaLow Access Point (AP) is a device that enables both HaLow communication and legacy Wi-FI(2.4GHz) communication within a network. It serves as a central hub that connects wireless devices together and provides them with access to the network and the internet.
900MHz Wi-Fi (HaLow) Stations(STAs)	A HaLow Station refers to a device that connects to a Wi-Fi HaLow network as a client. In other words, it's a device that uses Wi-Fi HaLow technology to communicate with a HaLow Access Point (AP) or with other HaLow-enabled devices. Some common types of HaLow stations are HaLow serial converters and HaLow Ethernet converters.
AES	Abbreviation for Advanced Encryption Standard. It is a "next-generation standard encryption method" adopted for information processing within the U.S. government. It is satisfied with the standards of the regulations (cryptography strength, processing speed, etc.), and the specifications are also published, so it is used in a wide range of fields. It is adopted as one of the IEEE802.11i encryption methods.
ESSID	Abbreviation for Extended Service Set Identifier. It is often called SSID. The wireless LAN access point that constitutes the wireless LAN and the identifier attached to the wireless terminal. It is used to group wireless LAN. You can't communicate unless the same ESSID is set on the wireless LAN access point and the wireless terminal. BSS (Basic Service Set), one group centered on wireless LAN access points, is the smallest unit of wireless LAN infrastructure communication by 802.11, but multiple ESS (Extended Service Set) with multiple bundles of BSS is defined, taking into account roaming when straddling the wireless LAN access point of
IEEE802.11ah	The IEEE 802.11ah standard, also known as Wi-Fi HaLow, is part of the IEEE 802.11 set of WLAN standards. It's distinct for operating in frequency bands below 1 GHz (specifically in the 900 MHz band in the U.S.), unlike most Wi-Fi standards that operate in the 2.4 GHz and 5 GHz bands. This standard was designed to address the needs of modern IoT (Internet of Things) applications, offering unique advantages for devices that require long-range connectivity and low power consumption. Here are some key features and benefits of 802.11ah (Wi-Fi HaLow)
PSK	Abbreviation for Pre-Shared Key. A shared (secret) key used to generate an encryption key in the TKIP encryption protocol. It is called a "pre-shared key" because it is not used to encrypt directly, but to generate an encryption key. PSK may represent an authentication method that uses a pre-shared key.
WPA	Abbreviation for Wi-Fi Protected Access. A new security standard standardized by the Wi-Fi Alliance. The security strength is stronger than the WEP method. In the WPA specification, the encryption protocol "AES" is not required, so even if you support WPA, you may not support AES.
WPA-PSK	Represents a method that does not use an external server for authentication with WPA.
WPA2-Personal	It is also called WPA2-PSK. Table of methods that do not use an external server for authentication with WPA2
WPA3-Personal	WPA3-Personal is a security standard designed to enhance the security of wireless networks. It's an evolution of WPA2, aiming to provide stronger protections against offline dictionary attacks and ensure forward secrecy. Here are some key features and improvements WPA3-Personal brings to wireless network security
Access Point(AP) Mode	Access Point (AP) mode is a configuration setting available in Wi-Fi networking devices, including routers and dedicated access points, that allows the device to act as a central transmitter and receiver of wireless radio signals. In AP mode, the device creates a wireless local area network (WLAN) that enables multiple wireless clients (like smartphones, laptops, tablets, and smart home devices) to connect to a wired network. This mode is fundamental for setting up Wi-Fi networks in homes, offices, and public spaces.

Repeater Mode	Repeater or extender mode is a configuration used in wireless networking to expand the coverage area of a Wi-Fi network. This mode allows a Wi-Fi device, such as a range extender or a router configured as a repeater, to pick up the signal from an existing wireless network and retransmit it, effectively extending the network's reach to areas where the signal was previously weak or non-existent.
Wi-Fi Stations(STAs)	The term "stations" (STAs) refers to any devices that connect to a Wi-Fi network and are not acting as an access point (AP). Stations can include a wide range of devices such as smartphones, laptops, tablets, smart TVs, IoT devices, and essentially any wireless client that uses Wi-Fi to connect to a network

FCC Information to User

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

Caution

THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE.

SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

IMPORTANT NOTE : FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.