HAP101 Wi-Fi HaLow Access Point

User Manual

Version: 2.4

Revision History:

No.	Description	Date
V1.0	First release	Jan. 10, 2024
V1.1	Broke down the steps for web log	Jan. 25, 2024
V1.2	Updated the steps in WIFI connection as per the firmware upgrade	Feb 2, 2024
V1.3	Added a use case for connecting a camera to the network	Feb. 5, 2024
V1.4	1. Added a new option for device web login using the VLAN IP of the device; 2. Clarified the methods of factory resetting the device.	Jun. 24, 2024
V1.5	Updated the definition of ERR indicator	Jul. 23, 2024
V1.6	1. Updated the back view as per design change; 2. Updated the steps for setting up the device; 3. Updated chapter 4 USE CASE	Oct. 12, 2024
V2.0	1. Updated the interface definition as per design change; 2. Added description on the use of DIP switches, the Pair/Restore button, and the definition of the LED indicators based on the updated hardware version; 3. Updated the steps in 2.1 setting up the device; 4. Added description for the use of the DIP switches and LED indicators; 5. Updated the use case as per firmware upgrade	Nov. 18, 2024
V2.1	1. Updated the screenshots as per the function update of the web portal; 2. Added description for the use of ACL, DHCP, and DPP features	Dec. 16, 2024
V2.2	Updated the description of the device interfacing with BlueSphere GWM	Dec. 18, 2024
V2.3	Added description on network interface bridging (2.6)	Feb. 7, 2025
V2.4	1. Updated the description on the bridge mode of 2.4GHz Wi-Fi when switching the WAN port to LAN; 2. Updated the description and steps regarding the WAN port switching in chapter 4 USE CASE accordingly; 3. Updated the debugging method of the device in chapter 5.	Mar. 21, 2025

Table of Contents

Foreword

Thank you for purchasing HAP101 Wi-Fi HaLow Access Point (“the device” or “the Product”). This manual intends to provide guidance and assistance necessary on setting up, operating or maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

Unless otherwise stated, *Wi-Fi* in this manual refers to 2.4GHz Wi-Fi, and *HaLow* refers to Wi-Fi HaLow.

Intended Users

This manual is intended for:

- Network architects
- Network administrators
- Technical support engineers
- Other users

Copyright

Disclaimer

While all information contained herein has been carefully checked to assure its accuracy in technical details and typography, Vantron does not assume any responsibility resulting from any error or features of this manual, nor from improper uses of this manual or the software.

It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without notice.

Technical Support and Assistance

Should you have any question about the Product that is not covered in this manual, contact your sales representative for solution. Please contain the following information in your question:

- Product name and PO number;
- Complete description of the problem;
- Error message you received, if any.

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538

Tel: (650) 422-3128

Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- IC

Please refer to **Appendix** for Regulatory Compliance Statement.

Symbology

This manual uses the following signs to prompt users to pay special attention to relevant information.

	Caution for latent damage to system or harm to personnel
	Attention to important information or regulations

General Safety Instructions

The Product is supposed be installed by knowledgeable, skilled persons familiar with local and/or international electrical codes and regulations. For your safety and prevention of damage to the Product and other equipment connected to it, please read and observe carefully the following safety instructions prior to installation and operation. Keep this manual well for future reference.

- Do not disassemble or otherwise modify the Product. Such action may cause heat generation, ignition, electronic shock, or other damages including human injury, and may void your warranty.
- Keep the Product away from heat source, such as heater, heat dissipater, or engine casing.
- Do not insert foreign materials into any opening of the Product as it may cause the Product to malfunction or burn out.
- To ensure proper functioning and prevent overheating of the Product, do not cover or block the ventilation holes of the Product.
- Follow the installation instructions with the installation tools provided or recommended.
- The use or placement of the operation tools shall comply with the code of practice of such tools to avoid short circuit of the Product.
- Cut off the power before inspection of the Product to avoid human injury or product damage.

Precautions for Power Cables and Accessories

⚠ Use proper power source only. Make sure the supply voltage falls within the specified range. Always check whether the Product is DC powered before applying the power.

⚠ Place the power cable properly at places without extrusion hazards.

⚠ Use only approved antenna(s). Non-approved antenna(s) may produce spurious or excessive RF transmitting power which may violate FCC limits.

⚠ Cleaning instructions:

- Power off before cleaning the Product
- Do not use caustic or aggressive liquids, vapor, or spray
- Clean with a damp cloth
- Do not try to clean exposed electronic components unless with a dust collector

⚠ Power off and contact Vantron technical support engineer in case of the following faults:

- The Product is damaged
- The temperature is excessively high
- Fault is still not solved after troubleshooting according to this manual

⚠ Do not use in combustible and explosive environment:

- Keep away from combustible and explosive environment
- Keep away from all energized circuits
- Unauthorized removal of the enclosure from the device is not allowed
- Do not change components unless the power cable is unplugged
- In some cases, the device may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the device before replacement of the components.

CHAPTER 1 DEVICE INTRODUCTION

1.1 Product Overview

Vantron HAP101 Wi-Fi HaLow access point is designed in compliance with the prominent IEEE 802.11ah (Wi-Fi HaLow) standard and IEEE 802.11 b/g/n (2.4GHz Wi-Fi) standard. It offers a complete Wi-Fi connectivity solution for IoT developers who seek for wireless connections with energy efficiency, extended coverage, obstacle penetration, effortless accessibility, etc.

HAP101 supports up to 1km coverage at ultra-low power consumption while still delivering optimal performance with data rates up to 150 Mbps on 2.4GHz Wi-Fi and 32.5 Mbps on Wi-Fi HaLow. By complying with the IEEE 802.11ah standard, it supports operation in the sub-1GHz license-exempt RF bands to avoid the crowded 2.4GHz frequency band. At the same time, the 2.4GHz Wi-Fi capability ensures compatibility with devices that do not support HaLow.

HAP101 also offers DIP switches for quickly toggling between HaLow access point (AP) and station (STA), as well as for switching configurations between standard HaLow applications and HaLow mesh networks that involve multiple access points. This versatility makes it ideal for long-range sub-GHz networking applications such as smart home appliances, surveillance systems, industrial process control, logistics and asset management, and smart city facilities.

1.2 Unpacking

The device has been carefully packed with special attention to quality. However, should you find any component damaged or missing, please contact your sales executive in due time.

Standard accessories:

- HAP101 Wi-Fi HaLow access point
- 2 x 2.4GHz Wi-Fi antenna
- 1 x Wi-Fi HaLow antenna
- 1 x DC power connector
- 1 x RS485 terminal connector

Optional accessories:

- 1 x 12V/1A power adapter
- 1 x Power cord
- For IP54 version: 1 x Waterproof base + 1 x Waterproof cover

Actual accessories might vary slightly from the list above as the customer order might be different from the standard configuration options.

1.3 Terminologies and Acronyms

Below is a summary of the key terminologies and acronyms that will be covered in this manual.

Table 1-1

Glossary	Description
AP	Access point. It broadcasts the network, allowing other client devices (stations) to join and communicate.
STA	Station. A client device that connects to an access point.
HaLow mesh mode	Compared with the standard HaLow mode, the HaLow mesh mode involves multiple HaLow APs functioning as mesh points to extend the network coverage, typically with one mesh portal connected to a DHCP server for IP allocation and internet access.
Mesh point	A general node that relays data within the mesh network.
Mesh portal	A specific mesh point that connects the mesh network to the outside world, typically providing access to a DHCP server for IP allocation and internet connectivity.
DPP	• Device Provisioning Protocol, defined by Wi-Fi Alliance for **Wi-Fi Easy Connect™**. • It refers specifically to the fast-provisioning state of devices for a standard HaLow connection ("**HaLow DPP**") in this manual.
DCS	Dynamic Channel Selection: once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.

Unless otherwise stated, *Wi-Fi* in this manual refers to 2.4GHz Wi-Fi, and *HaLow* refers to Wi-Fi HaLow.

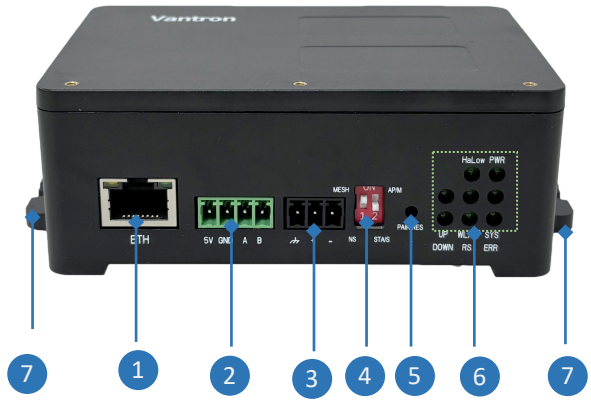
1.4 Specifications

HAP101			
System	CPU	MediaTek 580MHz MIPS® CPU	
	Wi-Fi HaLow SoC	Morse Micro MM6108	
	Memory	256MB	
	Storage	64MB	
WLAN Features	2.4GHz Wi-Fi	Standard: IEE 802.11 b/g/n	
		Frequency range: 2.412GHz ~ 2.462GHz	
		Channel bandwidth: 20/40 MHz	
		Data rate: up to 150 Mbps	
		Fast connection: WPS fast connection supported	
		Working mode: AP, STA (Multiple SSIDs supported in AP mode)	
	Wi-Fi HaLow	Standard: IEE 802.11 ah	
		Frequency range: 903.5MHz~926.5MHz (US)	
		Channel bandwidth: 1/2/4/8 MHz, dynamic channel selection (DCS) supported	
		Transmit power: 21dBm	
		Data rate: up to 32.5 Mbps @8MHz or 15 Mbps @4MHz	
		Application mode: Mesh, Ad Hoc, BridgeWAN, Repeater	
		Fast connection: DPP fast connection supported	
		Working mode: AP, STA (Multiple SSIDs supported in AP mode)	
I/O	Fast Ethernet	1 x RJ45, 10/100 Mbps	
	Serial port	1 x RS485/debugging (RS485 default, 5V output, baud rate: 115200)	
	Antenna	1 x Wi-Fi HaLow antenna	2 x 2.4GHz Wi-Fi antenna
System Control	LED indicators	1 x Power indicator	1 x Wi-Fi HaLow activity indicator
		1 x Uplink indicator	1 x Downlink indicator
		1 x WLAN activity indicator	1 x Error indicator
		1 x Reserved indicator (user-defined)	1 x System indicator
	Button	1 x Pair/Restore button	
	DIP switch	2 x DIP switch (AP & STA; Mesh & other modes)	
Mechanical	Dimensions	IP40 version (With wall mount): 130mm x 74mm x 42mm	
		IP54 version (With wall mount and water proof kit): 130mm x 119mm x 44mm	
	Casing material	Black plastics, UL94, SP6 compliant (Optional: White casing)	
	Installation	Wall mounting	
	IP rating	IP40 (Optional: IP54, enhanced with a waterproof kit)	
Power	Input	9V ~ 40V DC	
	Port	3-pin terminal (Over-current protection, reverse polarity protection)	

HAP101			
Software	Operating system	VantronOS	
	Device management	Vantron BlueSphere GWM (Optional)	
	Upgrade	Local upgrade, OTA upgrade	
	VPN	OpenVPN	
	Network protocol	IPV4, HTTPS, TCP & UPD, NTP client and server, ARP, TLS	
	Link detection	Heartbeat detection, auto reconnection	
	Network reliability	Multi-channel failover, backup between Ethernet, Wi-Fi, HaLow	
	IP application	Ping, Traceroute, DHCP Server/Client	
	IP routing	Static routing, dynamic routing	
Security	2.4GHz Wi-Fi	TKIP, WPA, WPA2, AES, WPS	
	Wi-Fi HaLow	WPA3	
	Firewall	Stateful	
	Access control	MAC address, IP address, URL	
Environmental	Temperature	Operating: -20℃ ~ +70℃	Storage: -40℃ ~ +85℃
	Humidity	≤ 95% RH (non-condensing)	
	Certification	FCC, IC	

1.5 Interfaces and Indicators

1.5.1 Front view



I/O description:

Indicator/ Interface	Description			
1	Ethernet jack (100Mbps), configured as a WAN port by default			
2	RS485/debugging RS485 (**default**): 115200, 8N1; debugging: refer to chapter 5			
3	Power terminal, supporting 9V~40V DC input			
4	DIP Switches	2 x 2 DIP switch. Refer to 1.6 for details.		
5	Pair/Restore button	Activates the device for DPP provisioning or factory reset. Refer to 1.7 for details.		
6	LED indicators in three columns (Refer to 1.8)	/	Wi-Fi HaLow indicator	Power indicator
		Uplink indicator	2.4GHz Wi-Fi indicator	System indicator
		Downlink indicator	Restart indicator	Error indicator
7	Mounting brackets (screws recommended: M3 x 8mm)			

1.5.2 Back view

Interface	Description
1	Diversity 2.4GHz Wi-Fi antenna connector
2	Wi-Fi HaLow antenna connector
3	Primary 2.4GHz Wi-Fi antenna connector
4	Mounting brackets (screws recommended: M3 x 8mm)

1.6 DIP Switches

HAP101 offers two DIP Switches (2 x 2) that can be configured to different modes as detailed below.

Table 1-2

Switch 1	Switch 2	Description
Non-Mesh [Standard HaLow mode]	AP/Portal	The device operates as a HaLow AP
	STA/Point	The device operates as a HaLow station
Mesh [HaLow mesh mode]	AP/Portal	The device operates as a mesh portal
	STA/Point	The device operates as a mesh point

The switches are set to the Non-mesh—STA/Point position (1: UP, 2: Down) by default, and this setting alone does NOT indicate the current working mode of the device. The DIP switches are designed to use in combination with the Pair/Restore button.

1.7 Pair/Restore Button

The Pair/Restore button activates the device for HaLow DPP provisioning or factory reset.

1. **HaLow DPP***: Enables **fast provisioning** of the device for a standard HaLow connection.
2. **Factory Reset**: Clears all custom settings and resets the device to factory defaults.

When the HaLow DPP state is activated, the HaLow indicator blinks at a frequency of 1Hz. If the user does not confirm the action within 3 seconds by leaving the device untouched, the device will return to the normal operation state.

When the factory reset state is activated, all indicators will blink at a frequency of 2Hz. If the user does not confirm the action by short pressing the button within 5 seconds after releasing it, the device will return to the normal operation state.

* Refer to table 1-1 in 1.3 for the details of the mode.

Table 1-3 on the following pages explains the working principle of the button.

1.7.1 Button state: HaLow DPP & factory reset

Table 1-3

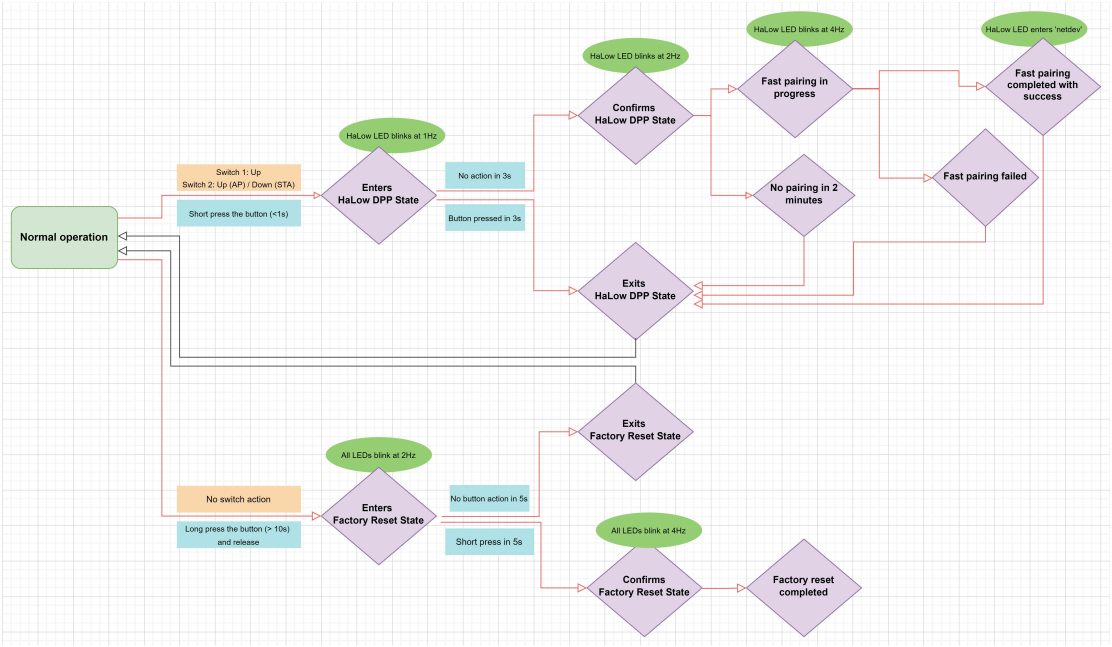
State	Prerequisites	Button Action	Description
HaLow DPP	1. DIP switch 1 set to the non-mesh position (Up); 2. DIP switch 2 set to the AP position (Up) or STA position (Down), depending on the specific use of the device; 3. Device in the normal operation state.	Short press (< 1s)	1. Upon a short press of the button: The device transitions to the HaLow DPP state and the HaLow indicator blinks at a frequency of 1Hz; 2. No action performed in 3 seconds: This state is confirmed and the HaLow indicator blinks at a frequency of 2Hz; 3. Pairing in progress: The HaLow indicator blinks at a frequency of 4Hz; 4. Connection completed & communication in progress: The HaLow indicator enters the 'netdev' mode (Refer to 1.8.2 for the details of the indicator).
Exit the HaLow DPP state	Device in the HaLow DPP state	Short press (< 1s)	The device returns to normal operation upon a short press of the button.
		NA	The device returns to normal operation when there is **no device pairing action in 120s** after the DPP mode is confirmed.
		NA	The device returns to normal operation when the **pairing completes or fails**.
Factory Reset	Device in the normal operation state	Long press (> 10s) – Release – Short press (< 1s) in 5s	1. Long press the button for above 10 seconds and release: All indicators will blink at a frequency of 2Hz, indicating the device is ready for factory resetting; 2. Short press the button for less than 1 second within 5 seconds after release: This confirms the factory reset action, and all indicators will blink at a frequency of 4Hz, indicating the device will proceed with the reset; 3. The Wi-Fi HaLow indicator, power indicator, 2.4GHz Wi-Fi indicator, and system indicator will turn solid green upon successful reset.
Exit the Factory Reset state	Factory Reset state activated	Button not pressed in 5s after release	If the user does not press the button within 5 seconds in the abovementioned step 2, the action will **NOT** be confirmed, and the device will continue to operate in its previous state.

Please refer to 2.2.2 and 2.2.3 for the steps to set up the AP and STA in HaLow DPP mode for fast pairing.

1.7.2 Button state in combination with switches & LEDs

The Pair/Restore button can be used in combination with the DIP switches and LED indicators to better determine the current status of the device as shown below.

Figure 1-1:



1.8 LED Indicators

1.8.1 WLAN indicator

The WLAN indicator has the following statuses. **The 'netdev' mode of the WLAN indicator comprises statuses a~c.**

a. 2.4GHz Wi-Fi module not working: OFF;

b. 2.4GHz Wi-Fi module working: Solid green;

c. 2.4GHz Wi-Fi communication in progress: Blinking regularly;

d. Upon a successful 2.4GHz Wi-Fi connection, the indicator blinks regularly. Meanwhile the UP/DOWN indicator (depending on whether the device is a 2.4GHz Wi-Fi AP or client) will blink at 4Hz for 3s, and later turns solid green;

e. When the device is ready for factory reset, the indicator blinks at 2Hz. After the user confirms the state, the indicator will blink at 4Hz, indicating the device is undergoing a factory reset. Upon successful factory reset, the indicator will turn solid green.

1.8.2 HaLow indicator

The HaLow indicator has the following statuses. **The 'netdev' mode of the HaLow indicator comprises statuses a~c.**

a. Wi-Fi HaLow module not working: OFF;

b. Wi-Fi HaLow module working: Solid green;

c. Wi-Fi HaLow communication in progress: Blinking regularly;

d. When short pressing the Pair/Restore pinhole button to enter the HaLow DPP state:

1) The device enters the HaLow DPP state upon a short press of the button and the HaLow indicator blinks at a frequency of 1Hz;

2) When there is no action within 3 seconds, the device will confirm the HaLow DPP state and the indicator will blink at a frequency of 2Hz;

3) When the device is pairing with another device via Wi-Fi HaLow, the indicator will blink at a frequency of 4Hz;

4) Upon successful connection, the device will exit the HaLow DPP mode, and the indicator blinks regularly. Meanwhile the UP/DOWN indicator (depending on whether the device is a HaLow AP or station) will blink at 4Hz for 3s and later turns solid green.

e. When the device is ready for factory reset, the indicator blinks at 2Hz. After the user confirms the state, the indicator will blink at 4Hz, indicating the device is undergoing a factory reset. Upon successful factory reset, the indicator will turn solid green.

1.8.3 Up & Down indicators

1. Up indicator

- When there is a successful downlink connection via 2.4GHz Wi-Fi AP or HaLow AP of the current device: Solid green;
- When no client device is connected to the current device via 2.4GHz Wi-Fi AP or HaLow AP: OFF;
- When Wi-Fi HaLow AP/2.4GHz Wi-Fi AP pairing is completed with success: Blinking at 4Hz for 3s and later transitioning to solid green.

2. Down indicator

- When there is a successful uplink connection via any of Ethernet WAN, 2.4GHz Wi-Fi STA, and HaLow STA of the device: Solid green;
- When the device does NOT establish a successful uplink connection via any of Ethernet WAN, 2.4GHz Wi-Fi STA, and HaLow STA: OFF;
- When Wi-Fi HaLow STA/2.4GHz Wi-Fi STA pairing is completed with success: Blinking at 4Hz for 3s and later transitioning to solid green.

3. When the device is ready for factory reset, the Up and Down indicators blink at 2Hz. After the user confirms the state, the indicator will blink at 4Hz, indicating the device is undergoing a factory reset.

Note: Users can determine the device status with a combination of the Up/Down indicator and the DPP state Pair/Restore button. However, a successful uplink/downlink connection does not necessarily indicate successful data communication or a successful device pairing.

1.8.4 Restore indicator

- Device restart/reboot in progress: Blinking at 4Hz.
- Device ready for Factory Reset: Blinking at 2Hz; following user confirmation for the reset: blinking at 4Hz, indicating the device is undergoing a factory reset.

1.8.5 Power indicator

- Device properly powered on: Solid green.
- Device not powered on or improperly powered: OFF.
- Device ready for Factory Reset: Blinking at 2Hz; following user confirmation for the state: Blinking at 4Hz, indicating the device is undergoing a factory reset; upon successful factory reset: transitioning to solid green.

1.8.6 System indicator

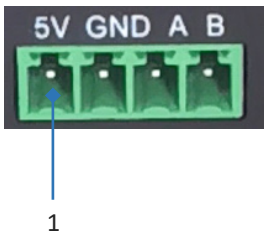
- Preinit state (device tree overlay not mounted): Blinking at 10Hz.
- Upon device boot: Blinking at 1Hz for 3 seconds, then transitioning to solid green.
- Firmware upgrade initiated: Blinking at 4Hz.
- Device ready for Factory Reset: Blinking at 2Hz; following user confirmation for the state: Blinking at 4Hz, indicating the device is undergoing a factory reset; upon successful factory reset: transitioning to solid green.

1.8.7 Error indicator

- Abnormality detected in health check: Blinking at 4Hz
- No abnormality found in health check: OFF
- Device ready for Factory Reset: Blinking at 2Hz; following user confirmation for the state: Blinking at 4Hz, indicating the device is undergoing a factory reset

Note: Abnormalities that cause the Error indicator to blink at 4Hz include loading problems with the HaLow/Ethernet/2.4GHz Wi-Fi interface, failure to start crucial services, and excessive resource occupation. The ERR indicator turns off when there is no abnormality detected.

1.9 Serial Port



HAP101 offers an RS485 connector for serial communication. The default baud rate of the port is 115200, and the pinout description is as follows:

Table 1-4

No.	Signal	Device name	Port	Type	Description
1	VCC	/dev/ttyS0	COM0	P	5V output
2	GND			P	Ground
3	A			I/O	RS485 A signal
4	B			I/O	RS485 B signal

Port wiring: A-A, B-B, GND-GND

Input the following command to open the port with a serial port communication program (e.g., microcom) for serial communication:

```
~# microcom /dev/ttyS0 -s 115200
```

CHAPTER 2 GETTING STARTED

2.1 Setting up the Device

When mounting HAP101 on a vertical surface, please ensure that the device is oriented with the LED indicators pointing down. This positioning allows the LEDs to be visible to the user on the ground.

1. Use two M3 x 8mm screws to fix HAP101 (screw anchors might be necessary);
2. Tighten the screws and gently swing the device to make sure it is fastened;
3. Install the shorter antennas to the WLAN antenna connectors (*silk screened as WLAN1 and* WLAN2*/BT*);

4. Install the longer antenna to the Wi-Fi HaLow antenna connector (*silk screened as HaLow*);

5. Connect the WAN port of HAP101 to the router using the Ethernet cable;

6. Plug the DC power connector into the power terminal of the device and connect it to the power source using the 12V DC adapter to start it.

2.2 Pairing Two HAP101 Devices

You have multiple options to pair two HAP101 devices via Wi-Fi HaLow. Choose the one that best suits your situation.

Typically, each HAP101 operates in both HaLow AP and 2.4GHz Wi-Fi AP mode by default, with a fixed LAN IP of 172.18.2.1. When the device switches to HaLow station/client mode, the LAN IP will change to 172.18.3.1, ensuring proper DHCP server IP allocation.

2.2.1 Pairing via station setup on the web portal

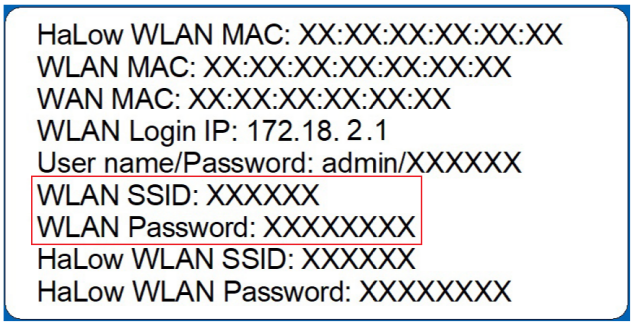
To set an HAP101 to the station mode (**H2**) and connect it to an AP-mode HAP101 (**H1**) via Wi-Fi HaLow, **simply configure H2** using the web-based management portal (VantronOS).

To access VantronOS for H2 from a host computer, connect the host to the 2.4GHz Wi-Fi network of H2, then enter H2's WLAN IP address in a web browser to log in. For additional login methods, please refer to 2.3.

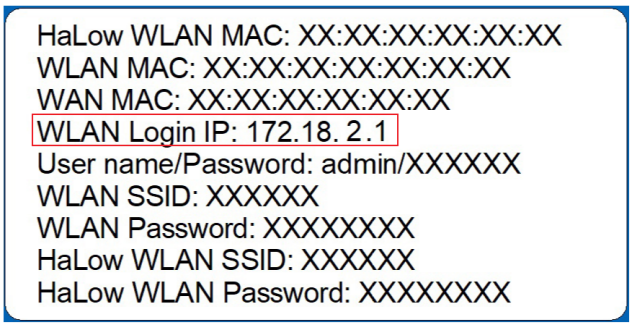
1. Power on **H1** and use an Ethernet cable to connect it to a router that functions as a DHCP server;

The router is used for network access and unified IP allocation. Connecting to it is not necessary if you just intend to verify the HaLow connection.

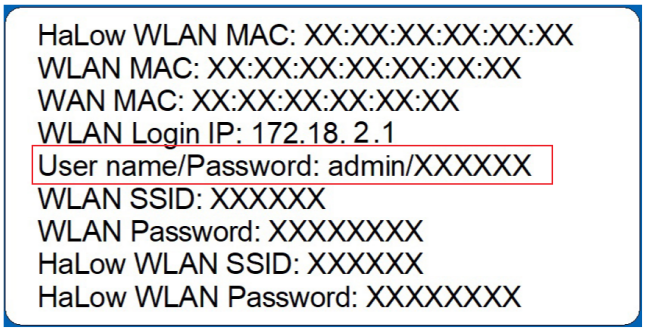
2. Power on **H2**;
3. Connect a host computer to the 2.4GHz Wi-Fi of **H2** using the default SSID and password provided on the device label as shown below;



4. Use the default **WLAN Login IP** provided on the device label of **H2** as the address for VantronOS login;



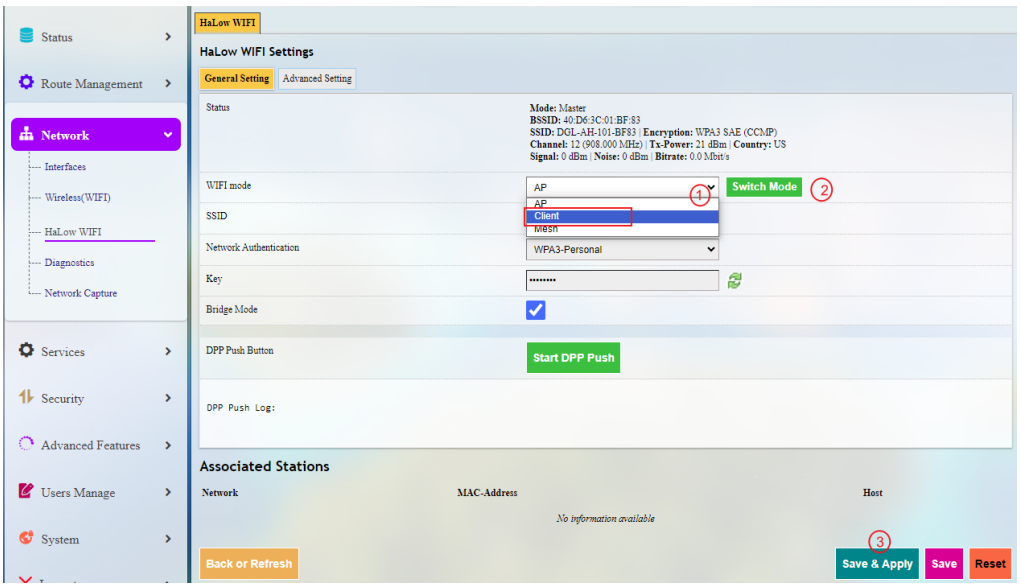
5. Log in to VantronOS using the username and password on the device label;



For higher permissions on VantronOS, log in as a superuser:

Super user: root // password: rootpassword

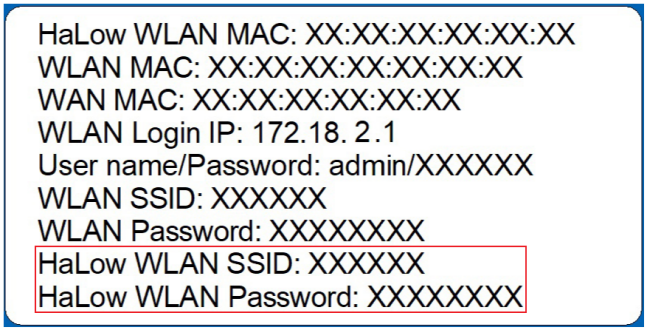
6. Navigate to **Network > HaLow WIFI** and change the HaLow mode of **H2** to **Client**, then wait a few seconds to allow the change to apply;



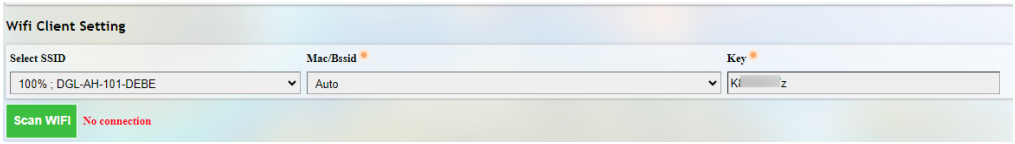
The LAN IP of the device will change to 172.18.3.1 when the HaLow mode switches to Client.

7. Reconnect the host computer to the 2.4GHz Wi-Fi of **H2** and log in to VantronOS using the new WLAN IP: 172.18.3.1;

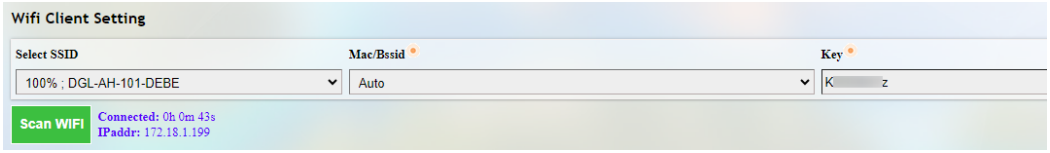
8. Check the device label of **H1** for the HaLow WLAN SSID and password for HaLow connection;



9. Navigate to **Network > HaLow WIFI** in VantronOS for **H2**. Under the **Wifi Client Setting** tab, select the SSID of **H1** from the list and enter the password for HaLow connection;



10. If the target SSID is not included in the HaLow SSID list, click the **SCAN WIFI** button to refresh the list;
11. Save and apply the settings;
12. When **H2** successfully connects to **H1** via Wi-Fi HaLow, the connection status will be displayed next to the **SCAN WIFI** button.



2.2.2 HaLow DPP pairing via hardware setup

DPP (Device Provisioning Protocol) specifically refers to the fast provisioning of HAP101 devices for a standard HaLow connection ("**HaLow DPP**") in this manual. The DIP switches and Pair/Restore button enable a quick HaLow connection via hardware setup. Please refer to 1.6 and 1.7 for the definition of the DIP switches and the Pair/Restore button, respectively.

Scenario: An AP mode HAP101 (**H1**) and a station mode HAP101 (**H2**) are running in the normal operation state.

HaLow DPP configurations on **H1** and **H2** for a standard HaLow connection are as follows.

Table 2-1

Device	Switch 1	Switch 2	Button Action	Result
H1	Non-mesh	AP/Portal	1. Short press the Pair/Restore button to enter the HaLow DPP state; 2. No button action in 3 seconds to confirm the state.	DPP state enabled in the HaLow AP mode
H2	Non-mesh	STA/Point		DPP state enabled in the HaLow station mode

Steps:

1. Short press the Pair/Restore button of **H1** to enter the HaLow DPP state;
2. Perform no action within 3 seconds to confirm the HaLow DPP state;
3. Repeat steps 1 and 2 on **H2** within 120 seconds after **H1** confirms the HaLow DPP state;
4. Wait for the devices to pair;
5. Upon successful connection, the HaLow indicators on both devices will enter the 'netdev' mode. The UP indicator on H1 and the DOWN indicator on H2 will blink at a frequency of 4Hz for 3s and later turn solid green.

The devices will **exit** the DDP state if:

a. H1 and H2 are successfully connected; or

b. The Pair/Restore button is briefly pressed during the DDP state; or

a. The second device does not enable the DDP state in 120 seconds after the first device does or the connection fails.

Once enabled, the HaLow DPP mode remains active for 120 seconds. It is recommended to initiate the DPP mode on the second device immediately after the mode is enabled on the first device to ensure successful pairing.

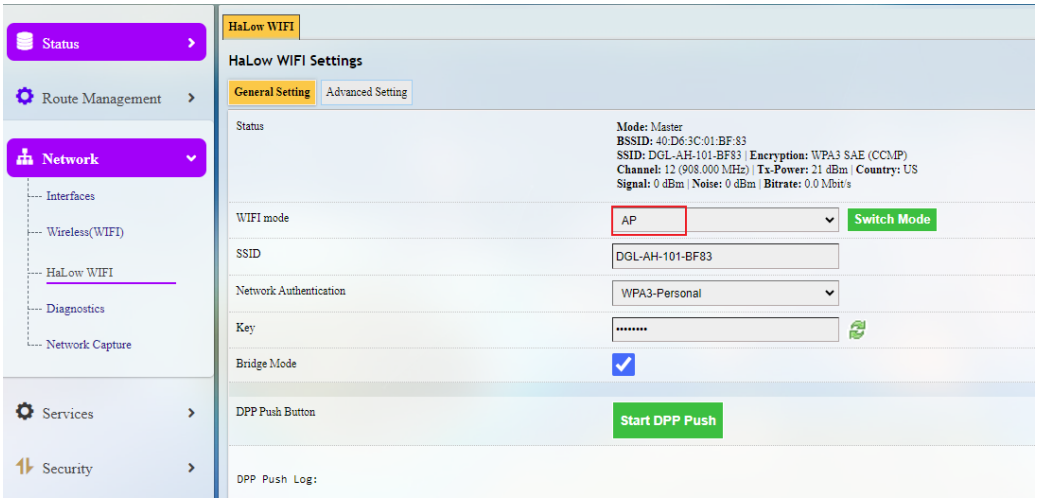
Upon successful pairing, the link between H1 and H2 will be maintained. Since the DPP mode supports only one-to-one pairing, to add a third STA mode device (H3) to the network, configure it similarly to H2 and repeat the above pairing process for H1 and H3.

You can also track the pairing process in **Network > HaLow WIFI** in VantronOS for either device.

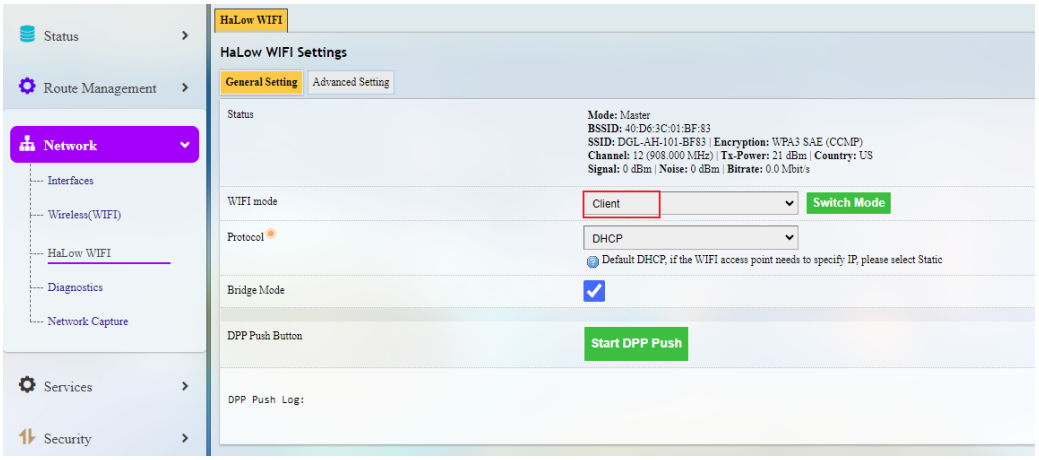
2.2.3 HaLow DPP pairing via software setup

Except the method described in 2.2.1, you can pair an AP-mode HAP101 (**H1**) and a station-mode HAP101 (**H2**) in VantronOS, regardless of the physical settings of the devices.

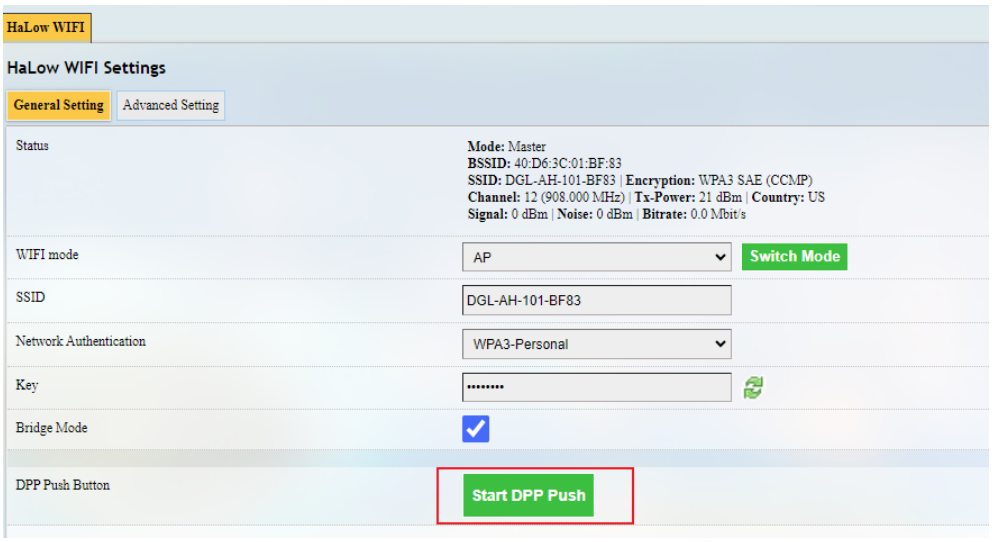
1. Connect a host computer to **H1** via 2.4GHz Wi-Fi and log in to VantronOS for H1 using the WLAN IP of the device (refer to the steps in 2.2.1);
2. Connect another host computer to **H2** via 2.4GHz Wi-Fi and log in to VantronOS for H2 using the WLAN IP of the device (refer to the steps in 2.2.1);
3. Navigate to **Network > HaLow WIFI** in VantronOS separately on both computers;
4. Keep the settings of **H1** unchanged;



5. Switch the HaLow mode of **H2** to **Client**;



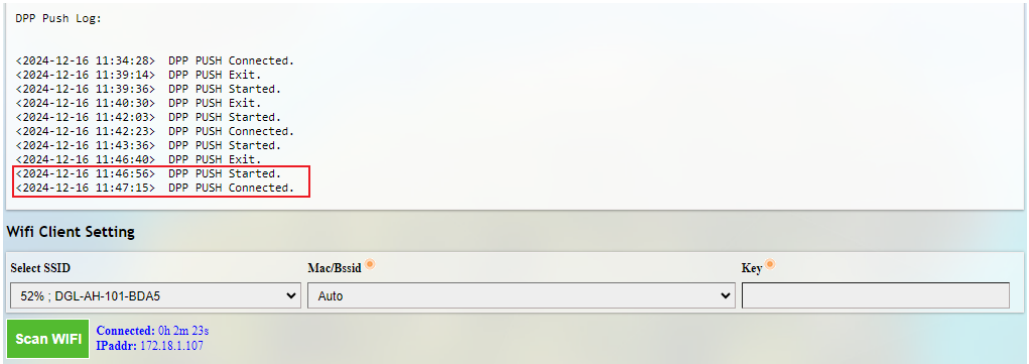
6. Click the **Start DPP Push** buttons on both computers simultaneously;



7. Wait for the devices to pair;

8. Upon successful connection, the HaLow indicators on both devices will enter the 'netdev' mode. The UP indicator on H1 and the DOWN indicator on H2 will blink at a frequency of 4Hz for 3s and later turn solid green;

9. The DPP push log indicates the success or failure state of the connection.



2.3 Web Login

You can configure the network settings and manage the device on the web-based management portal (VantronOS) using a host computer.

Depending on how the **host computer** is connected to HAP101, there are three ways to log in to VantronOS for HAP101.

Table 2-2

Login Method	Connection of the Host Computer	VantronOS Login to HAP101
Option 1	2.4GHz Wi-Fi connection to HAP101	Use the 2.4GHz WLAN IP of HAP101 as the login address
Option 2	Same Ethernet connection as HAP101	Use the VLAN IP of HAP101 as the login address
Option 3	Same Ethernet connection as HAP101	Use the WAN port IP of HAP101 as the login address

No matter which option you choose to log in to VantronOS for HAP101, it is important to note that the IP address of the host computer must be on the same network as HAP101. This network alignment is essential for successful connectivity and operation.

HAP101 provides one single Ethernet port, functioning as a **WAN port** by default.

You have two options to determine the WAN port IP of HAP101. You can use the arp -a command in the shell of the router/switch to display the devices connected to it. By matching the MAC address with the one on the device label, you can identify the corresponding WAN port IP address. Alternatively, you can log in to VantronOS for HAP101 through the other two options listed above, and then figure out the IP using the network interface feature included in the web.

To avoid unexpected troubles, you are advised to identify the 2.4GHz WLAN IP or the VLAN IP of the device for **initial** VantronOS login. Afterward, you can proceed with determining the WAN port IP address in the web for later use.

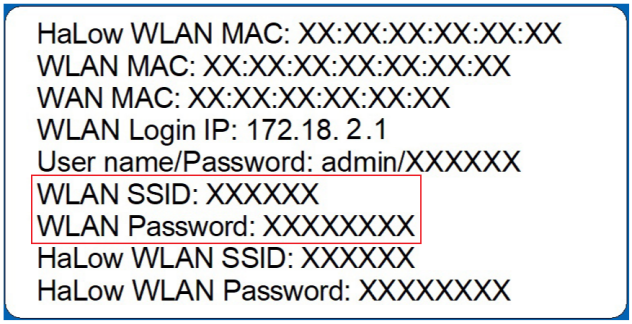
2.3.1 Login via the 2.4GHz WLAN IP

Prerequisites:

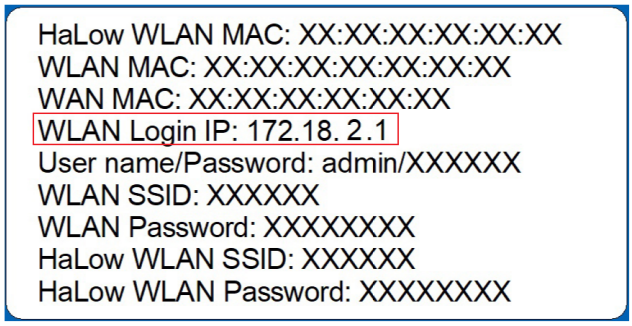
- HAP101 is operating in 2.4GHz Wi-Fi AP mode

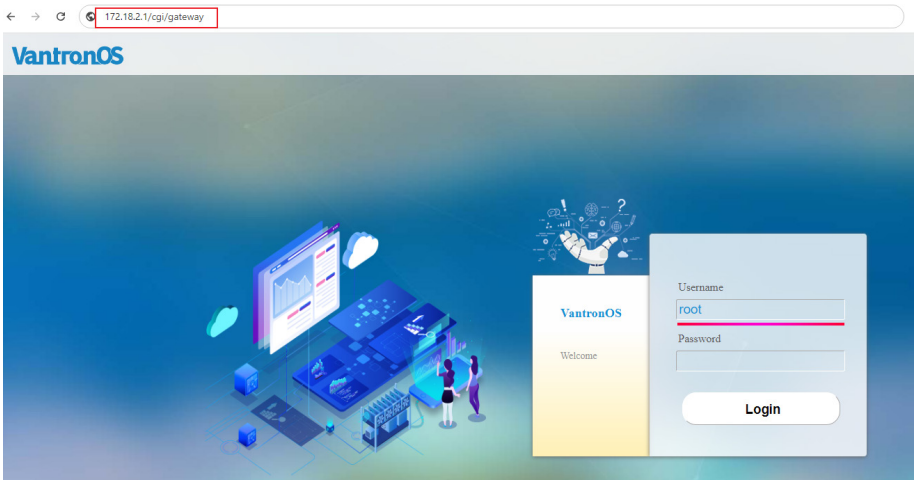
Steps:

1. Power on HAP101 and the 2.4GHz Wi-Fi will be operating in the AP mode by default;
2. Connect the host computer to the 2.4GHz Wi-Fi of the device using the SSID and default password provided on the device label as shown below;

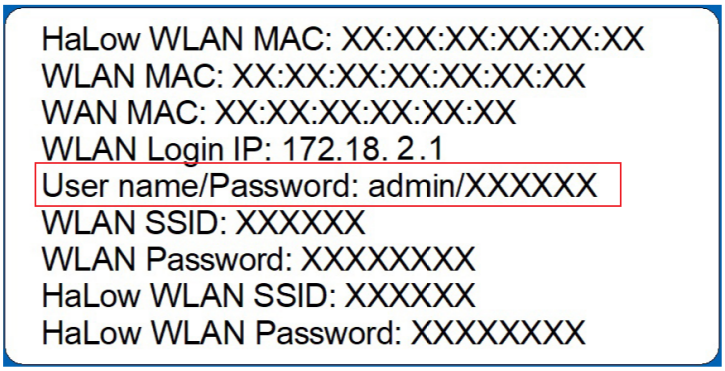


3. Use the WLAN Login IP provided on the device label as the address for VantronOS login;





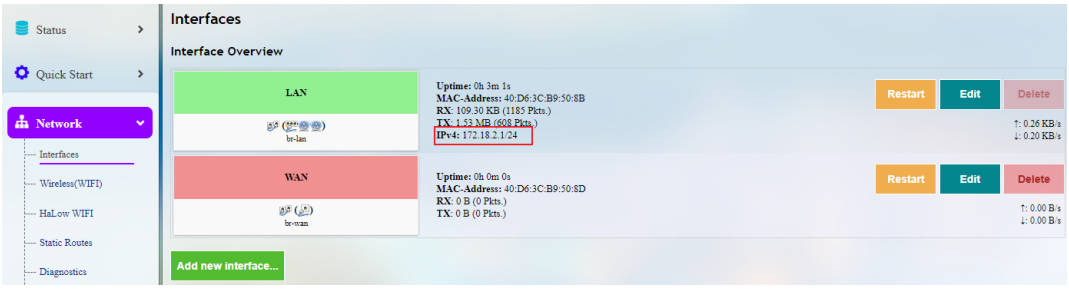
4. Log in to VantronOS using the username and password on the device label;



For higher permissions on VantronOS, log in as a superuser:

Super user: root // password: rootpassword

5. Navigate to **Network > Interfaces** to check the interface information of HAP101.



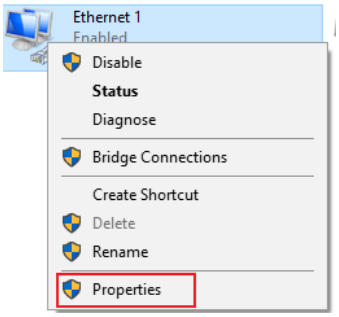
2.3.2 Login via the VLAN IP (Windows PC)

Prerequisites:

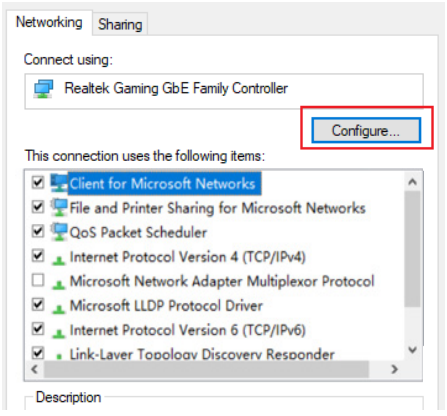
- The host computer supports VLAN settings (some may require installation of corresponding network adapter driver)

Steps:

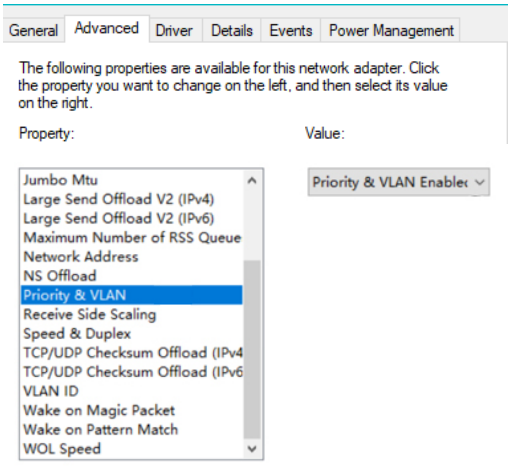
1. Connect the Windows host computer to the WAN port of HAP101;
2. Open the **Network & Internet Settings** on the host computer;
3. Right click the network adapter and select **Properties**;



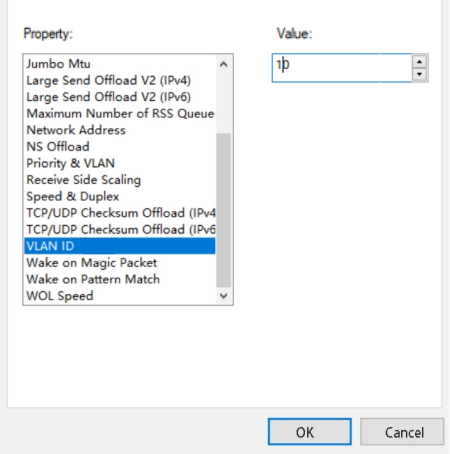
4. Click the **Configure** button in the middle, then click the **Advanced** tab;



5. Select **Priority & VLAN** from the list, and make sure the value is **Priority & VLAN Enabled**;

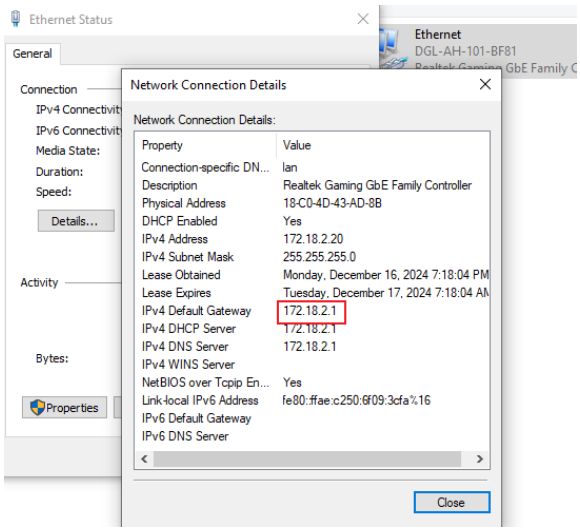


6. Move down to the **VLAN ID** attribute and input **'10'** as the value, then click **OK** to confirm the settings;

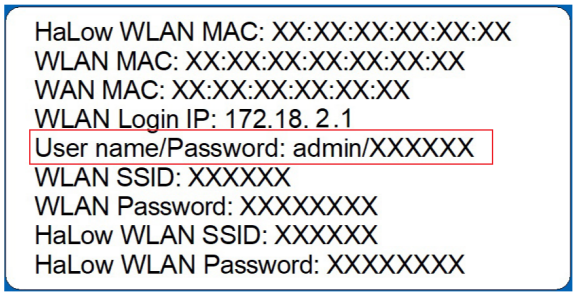


7. Wait a moment and check the network adapter settings;

8. Use the IPv4 default gateway for VantronOS login to HAP101;



9. Log in to VantronOS using the username and password provided on the device label.



For higher permissions on VantronOS, log in as a superuser:

Super user: root // password: rootpassword

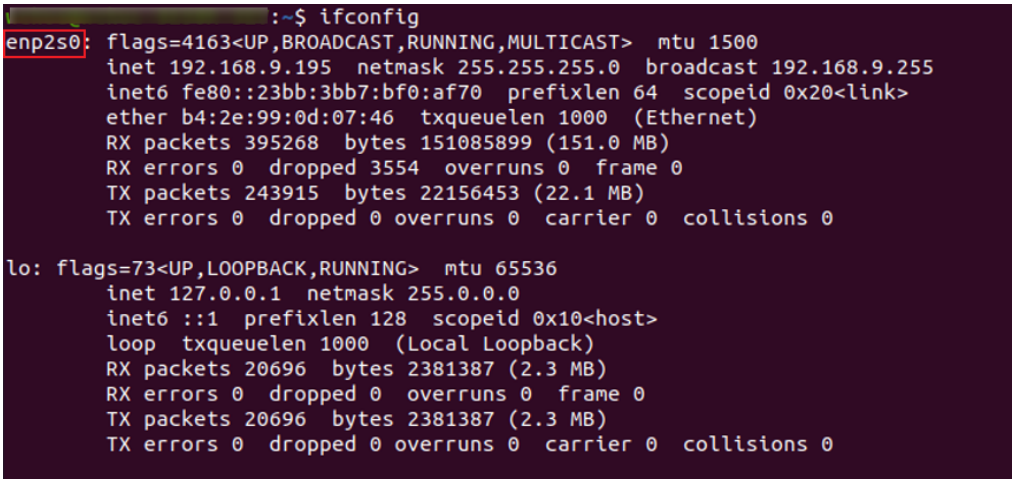
In some cases, to enable the Ethernet interface again, you may need to reset the VLAN settings to their default configuration:

- *Disable Priority & VLAN*
- *Set the VLAN ID back to 0*

2.3.3 Login via the VLAN IP (Linux PC)

Steps:

1. Connect the Linux host computer to the WAN port of HAP101;
2. Open a terminal on the host computer and use the ifconfig command to figure out the Ethernet interface of the computer;



The Ethernet interface of the computer is mapped as enp2s0 as shown above.

3. Create a VLAN interface (e.g., vlan10) on the Ethernet interface (enp2s0 in this case) with a VLAN ID (e.g., 10);

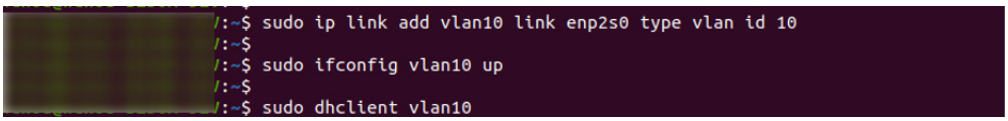
```
$ sudo ip link add vlan10 link enp2s0 type vlan id 10
```

4. Bring the VLAN interface up;

```
$ sudo ifconfig vlan10 up
```

5. Use DHCP to obtain an IP address for the newly created VLAN interface;

```
$ sudo dhclient vlan10
```



6. Check the network interfaces on the host computer and confirm if the VLAN interface receives an IP;

```
$ ifconfig
```

```
:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.9.195  netmask 255.255.255.0  broadcast 192.168.9.255
        inet6 fe80::23bb:3bb7:bf0:af70  prefixlen 64  scopeid 0x20<link>
        ether b4:2e:99:0d:07:46  txqueuelen 1000  (Ethernet)
        RX packets 395428  bytes 151117664 (151.1 MB)
        RX errors 0  dropped 3554  overruns 0  frame 0
        TX packets 244474  bytes 22210247 (22.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 21700  bytes 2469950 (2.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21700  bytes 2469950 (2.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vlan10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.2.114  netmask 255.255.255.0  broadcast 172.18.2.255
        inet6 fe80::b62e:99ff:fe0d:746  prefixlen 64  scopeid 0x20<link>
        ether b4:2e:99:0d:07:46  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 1102 (1.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 8743 (8.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The VLAN interface is assigned with an IP of 172.18.2.114 by the VLAN gateway (HAP101).

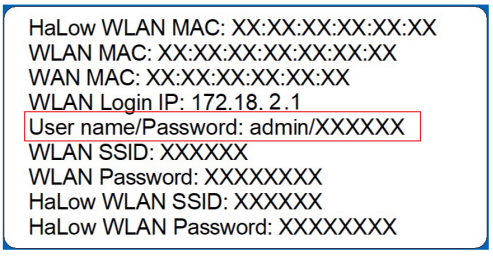
7. Run the ip route command to check the IP address of the VLAN gateway (HAP101).

```
:~$ ip route
default via 172.18.2.1 dev vlan10
default via 192.168.9.222 dev enp2s0 proto static metric 20100
10.42.0.0/24 dev enp2s0 proto kernel scope link src 10.42.0.195 metric 100
169.254.0.0/16 dev enp2s0 scope link metric 1000
172.18.1.0/24 dev enp2s0 proto kernel scope link src 172.18.1.195 metric 100
172.18.2.0/24 dev vlan10 proto kernel scope link src 172.18.2.114
192.168.9.0/24 dev enp2s0 proto kernel scope link src 192.168.9.195 metric 100
```

*The IP address of HAP101 is **172.18.2.1** in this case. Please note that when HAP101 switches to the HaLow station mode, its IP will change to 172.18.3.1 accordingly.*

8. Use above IP address of HAP101 for VantronOS login.

9. Use the username and password provided on the device label for authentication.



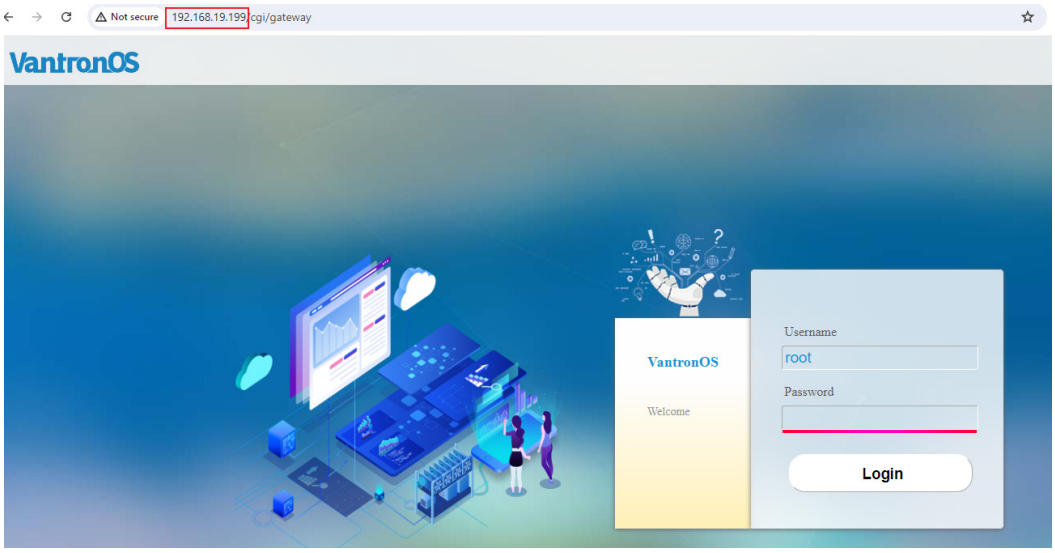
For higher permissions on VantronOS, log in as a superuser:

Super user: root // password: rootpassword

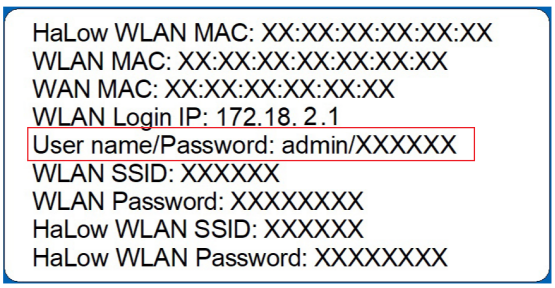
2.3.4 Login via the WAN port IP

1. Log in to VantronOS via the steps set out in 2.3.1 or 2.3.2;
2. Connect the host computer to a router/switch using an Ethernet cable;
3. Connect HAP101 to the same router/switch using an Ethernet cable;
4. Navigate to **Network > Interfaces** to identify the WAN port address of HAP101;

5. Use the WAN port IP of HAP101 as the address for VantronOS login;



6. Log in to VantronOS using the username and password provided on the device label.



For higher permissions on VantronOS, log in as a superuser:

Super user: root // password: rootpassword

2.4 SSH Login

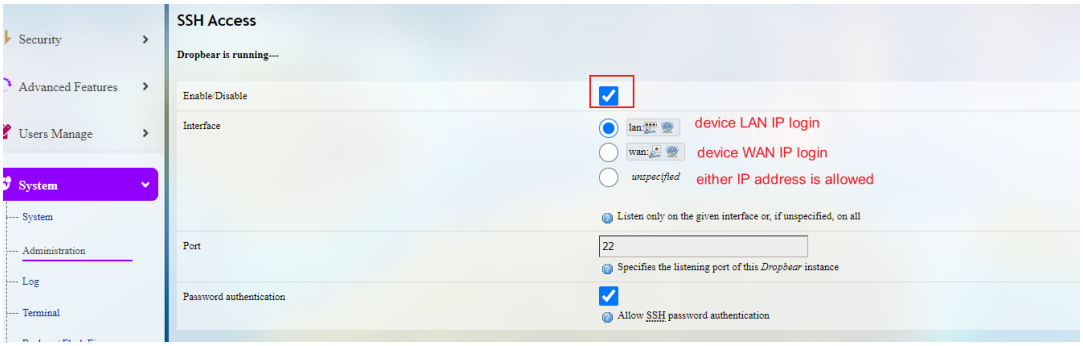
Depending on **how the host computer is connected to the device**, there are two ways for the SSH login to HAP101.

Option 1— If the host computer is connected to HAP101 via 2.4GHz Wi-Fi: Use the 2.4GHz WLAN IP of the device as the login address (see device label).

Option 2— If the host computer and HAP101 are on the same Ethernet WAN network: Use the WAN port IP of the device as the login address.

Make sure the IP address of the host computer is on the same network as HAP101 before the SSH login of HAP101.

By default, SSH login is **disabled**. You need enable the feature in vantronOS: **System > Administration > SSH Access**.

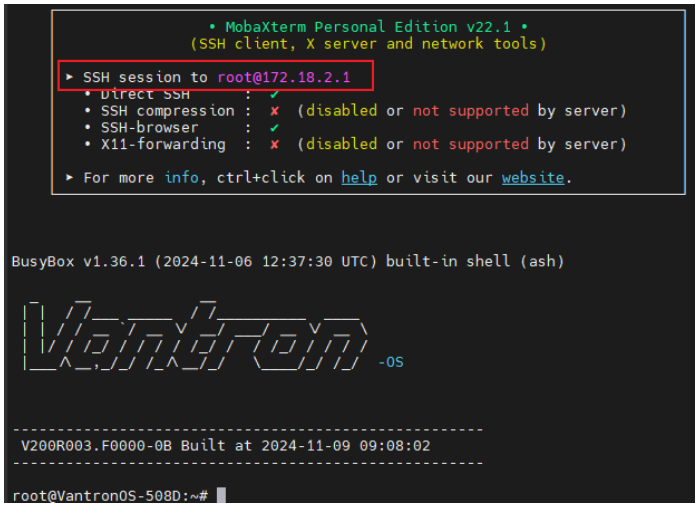


Refer to 3.10.2 for the specific login steps.

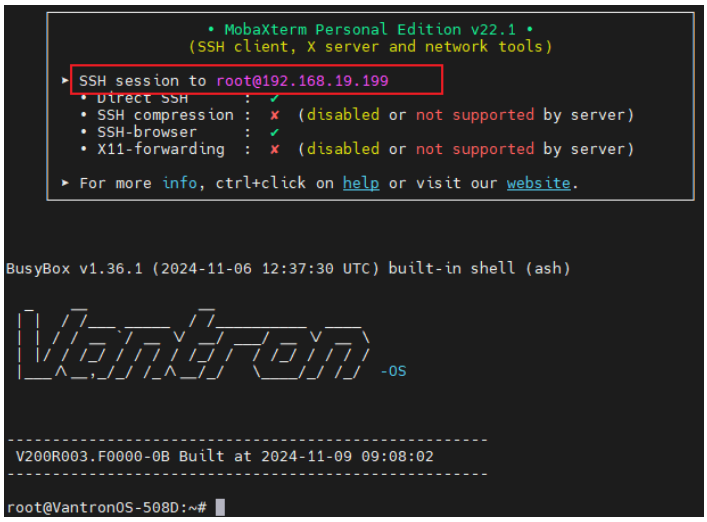
Use the following information for the login.

Port	Account	Password
22	root	rootpassword

Example SSH login with the 2.4GHz WLAN IP of HAP101:



Example SSH login with the WAN port IP of HAP101:



2.5 Wi-Fi HaLow Mode

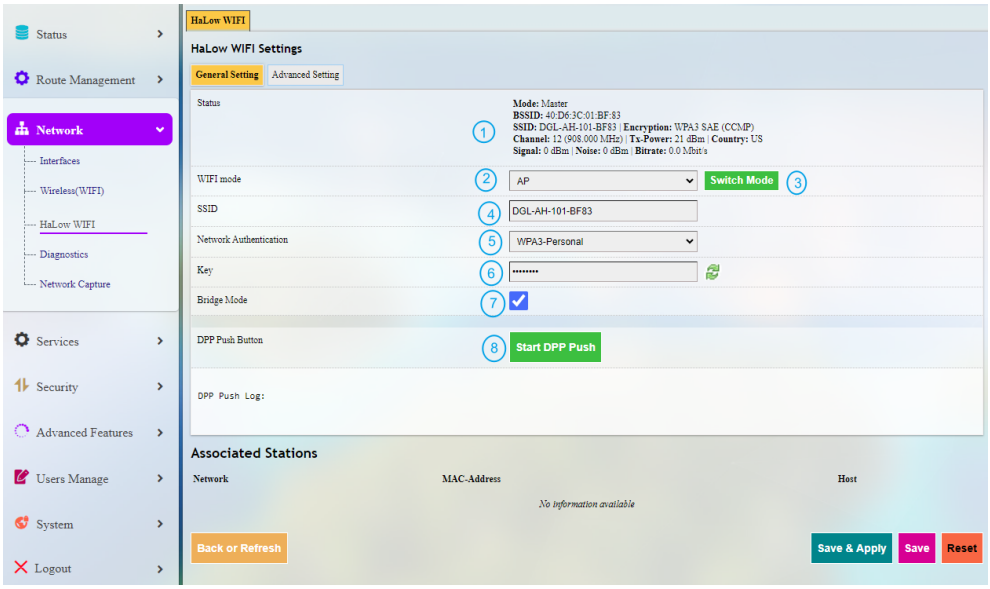
Wi-Fi HaLow related settings of the device are modified and saved via the **HaLow WIFI** menu in VantronOS**.** Therefore, please select an option provided in 2.3 to log in to VantronOS before you proceed.

2.5.1 AP mode

HAP101 is operating in the HaLow AP mode by default. To check the general HaLow information, follow the steps below:

1. Log in to VantronOS for the AP mode HAP 101 via any of the options provided in 2.3;
2. Navigate to **Network > HaLow WIFI**;

3. The general settings of the device are displayed and you can modify the configurations as needed.



Description of the numbered areas

1) Device general status information

2) The device operates in the HaLow AP mode by default and you can switch the mode using the drop-down list

3) You need confirm the mode change using the **Switch** button

4) HaLow SSID of the device

5) Authentication method for a HaLow connection

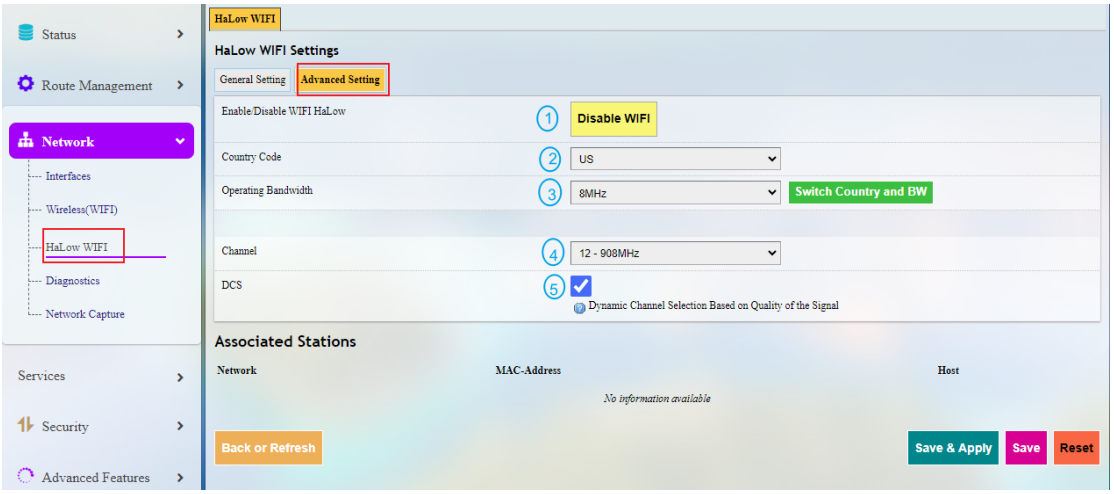
6) Default password for a HaLow connection (clicking the refresh button will display the password)

7) The HaLow interface is bridged to the Ethernet interface by default. This means that when the device is connected to a DHCP server through the WAN port, station devices connected to it via HaLow will receive an IP address from the DHCP server;

8) Pressing the **Start DPP Push** buttons simultaneously on the web portals for the AP mode HAP101 and the station mode HAP101 will initiate a DPP pairing between the devices.

Make sure to save the changes to allow them to apply, if any.

To check the advanced settings of an AP mode device, click the **Advanced Setting** button next to the **General Setting** button.



Description of the numbered areas

1) Disable/Enable the Wi-Fi HaLow feature;
2) The country codes include US, AU, and EU;
3) The device supports 1/2/4/8MHz operating bandwidth;
4) The device supports 12/28 operating channels;
5) Enable/Disable the Dynamic Channel Selection (DCS) feature. Once enabled, the device will automatically select the channel with the strongest signal.

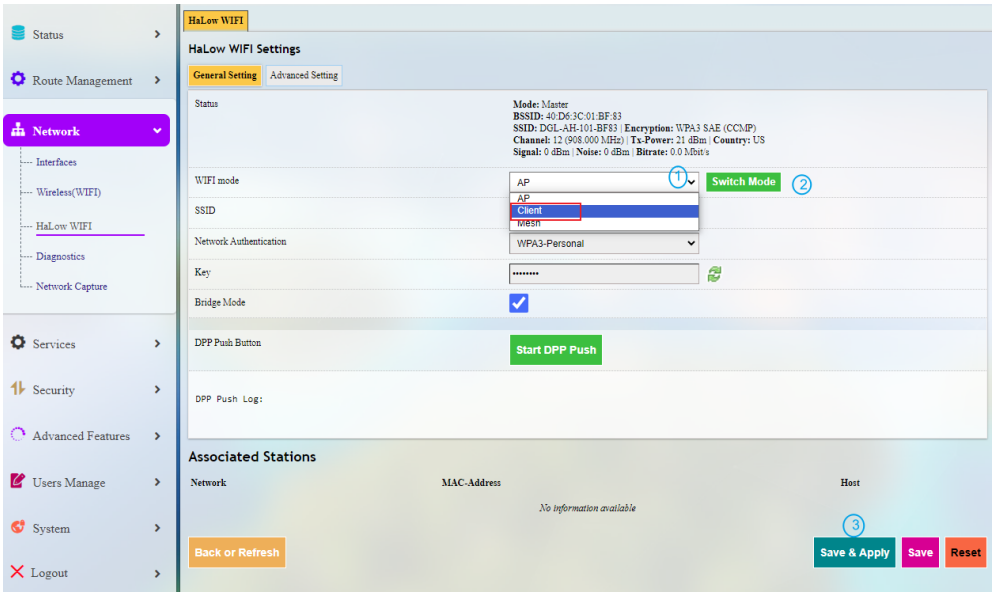
Make sure to save the changes to allow them to apply, if any.

To establish a HaLow connection, set up the station mode device using the HaLow SSID and key of the AP mode device. You can check the connection status in the web portal of the AP mode HAP101 (**Network > HaLow WIFI > Associated Stations**).

2.5.2 Station mode

The device is designed to connect to an existing HaLow access point when operating as a station. Follow the steps below to connect a station mode device to an existing HaLow AP.

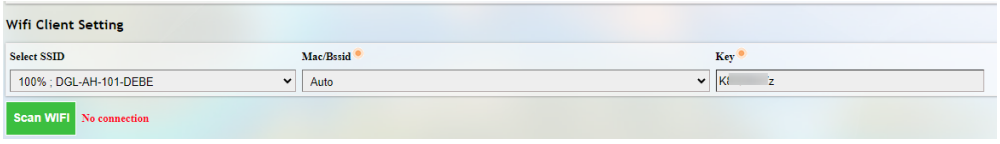
1. Log in to VantronOS for the AP mode HAP 101 via any of the options provided in 2.3;
2. Navigate to **Network > HaLow WIFI**;
3. Change the HaLow mode of the device to **Client**;



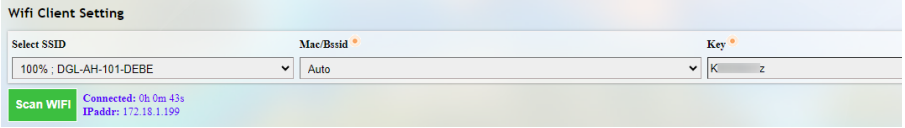
4. Wait a few seconds to allow the change to apply;

   *The LAN IP of the device will change to **172.18.3.1** when the HaLow mode switches to **Client**.*

5. Reconnect the host computer to the 2.4GHz Wi-Fi of the device;
6. Log in to VantronOS using the new WLAN IP: **172.18.3.1**;
7. Navigate to **Network > HaLow WIFI**. Under the **Wifi Client Setting** tab, select the SSID of the target AP mode HAP101 from the list and enter the password for HaLow connection (refer to the SSID & password on the label of the AP mode device);

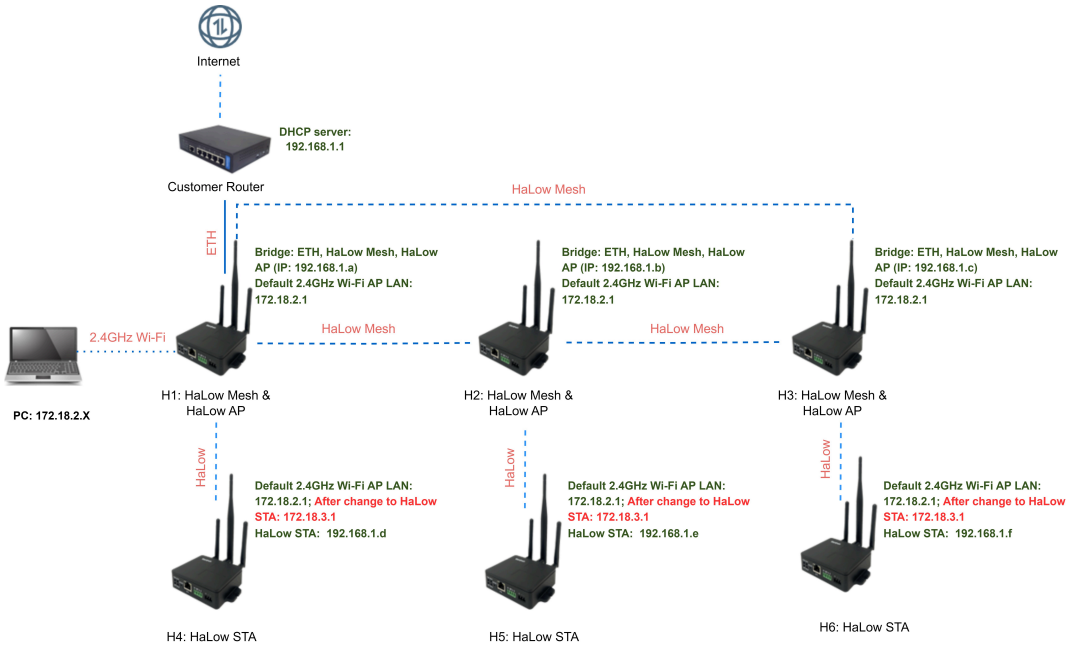


8. If the target SSID is not included in the HaLow SSID list, click the **SCAN WIFI** button to refresh the list;
9. Save and apply the settings;
10. When the device successfully connects to the AP mode device via Wi-Fi HaLow, the connection status will be displayed next to the **SCAN WIFI** button.



2.5.3 Mesh mode

When an HAP101 operates in the **Mesh** mode, it supports both mesh and AP features. This allows it to establish a mesh network with other devices in the Mesh mode while also enabling other station mode HaLow devices to connect to it, like the following topology.

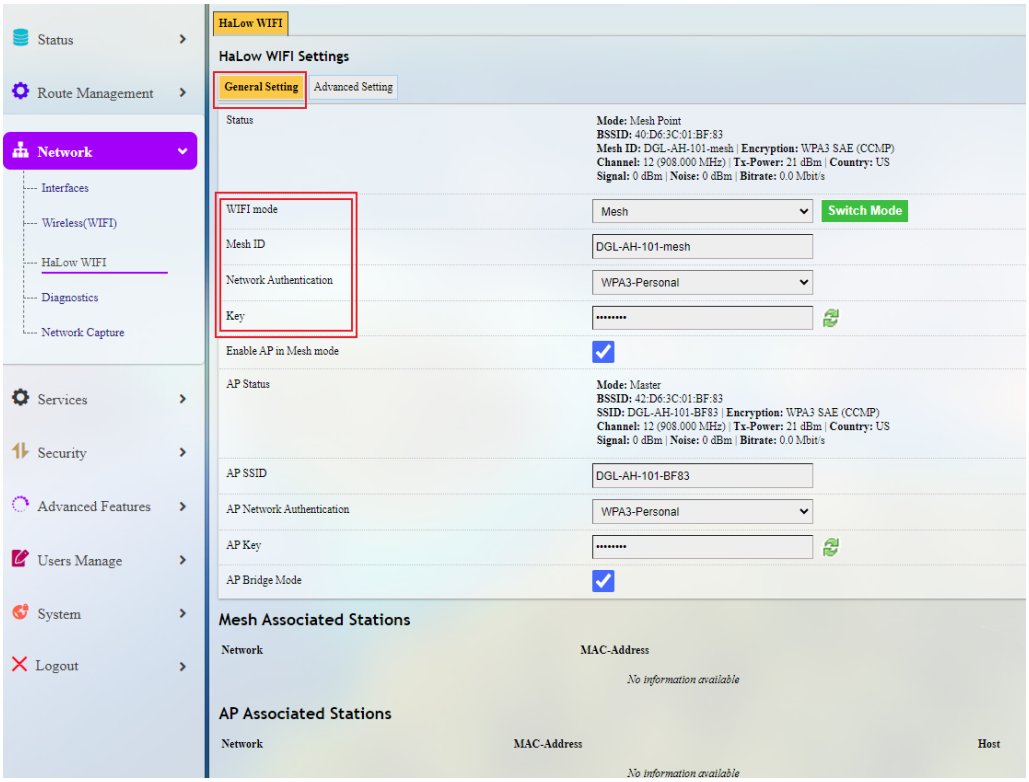


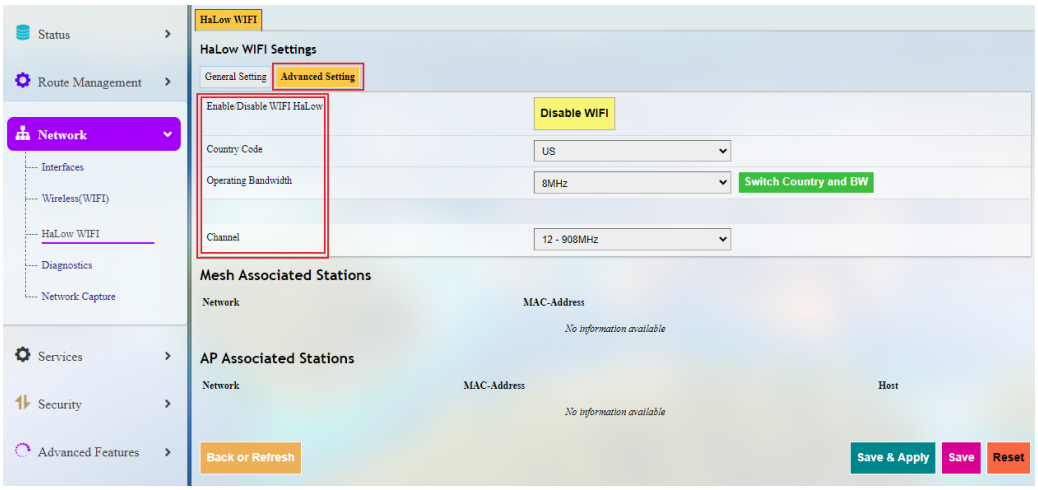
To establish a HaLow mesh network, follow the steps below:

1. Connect an AP-mode HAP101 (H1 in above topology) to a DHCP server via Ethernet or Wi-Fi;
2. Log in to VantronOS separately for the AP-mode devices (H1, H2, H3) that will be used to establish the mesh network;

   Refer to 2.3 for the login steps.

3. Set the following parameters of the abovementioned AP-mode devices to be the same;





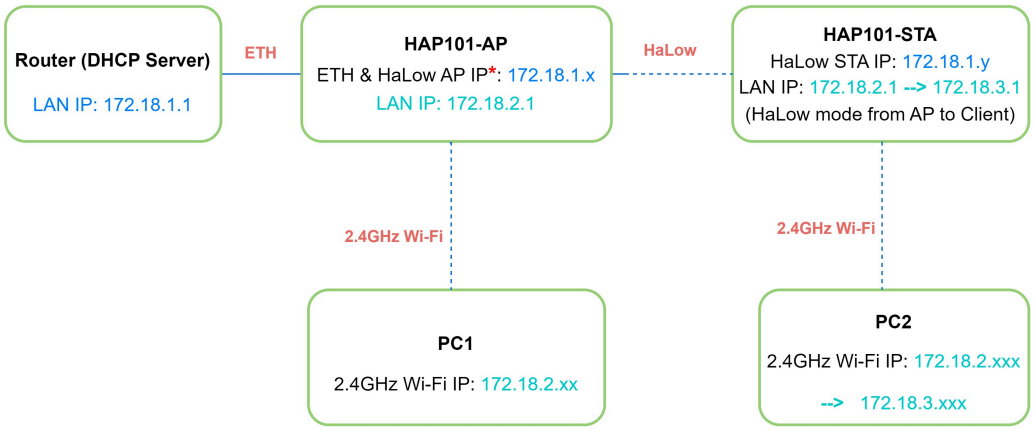
4. After completing above settings, a mesh network is established between the devices (H1, H2, H3), and you can check the connection under the **Mesh associated Stations** tab of the device connected to the DHCP server;

5. You can then connect station mode devices (H4, H5, H6) to the mesh mode devices via HaLow using the individual **AP SSID** and **AP key** of the mesh mode devices.

   *After a device switches from the HaLow **AP** mode to the **Client** mode, its 2.4GHz Wi-Fi AP LAN IP will change to 172.18.3.1 accordingly. If you need to access the VantronOS web portal for it, use the updated IP address to log in after connecting the PC to the device.*

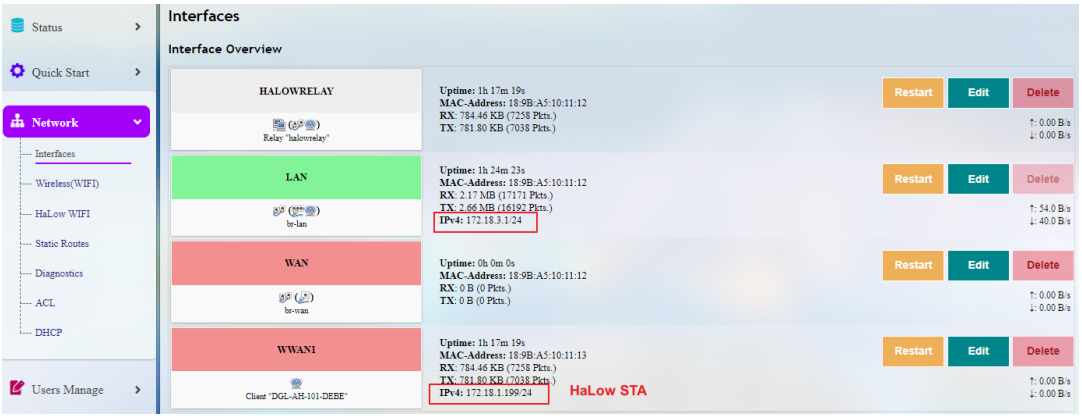
2.6 Network Interface Bridging

The bridge mode of each HAP101's **HaLow** is enabled by default. As a result, when an AP-mode HAP101 connects to a DHCP server via an Ethernet cable, clients connected to it via **Wi-Fi HaLow** will receive an IP address from the DHCP server, as shown in the diagram below.



In the above topology, when connecting PC1 to HAP101-AP via 2.4GHz Wi-Fi and logging into HAP101-AP's VantronOS on PC1 using the WLAN IP address of HAP101-AP, the network interface information will likely appear as follows.

Similarly, when connecting PC2 to HAP101-STA via 2.4GHz Wi-Fi and logging into HAP101-STA's VantronOS on PC2 using the WLAN IP address of HAP101-STA, the network interface information is likely shown as follows.



2.7 Ethernet Port Modification

The device's Ethernet port defaults to **WAN** mode, enabling connections to external networks for internet access. However, it can be reconfigured to operate in LAN mode to support local device connectivity.

Generally, users need to switch the Ethernet port from WAN to LAN mode in the following scenarios:

1. **AP-mode HAP101 with 2.4GHz Wi-Fi in Client Mode**:

   When the 2.4GHz Wi-Fi of an AP-mode HAP101 is operating in the client mode, users may need to access the device's VantronOS via the Ethernet LAN port.

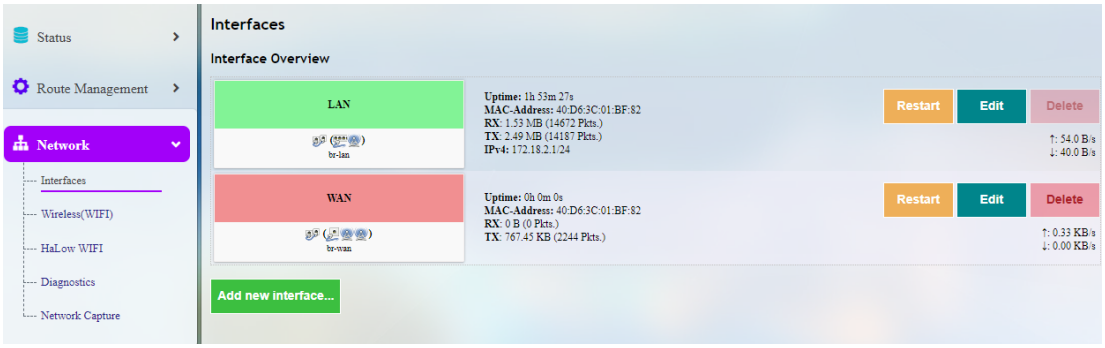
2. **STA-mode HAP101 with Bridged 2.4GHz Wi-Fi**:

   When the bridge mode of the 2.4GHz Wi-Fi of a STA-mode HAP101 is enabled, clients connected to the 2.4GHz Wi-Fi receive IP addresses from a DHCP server of the upstream network. In this case, switching the Ethernet port to LAN mode allows users to access the device's VantronOS locally.

2.7.1 WAN port to LAN port

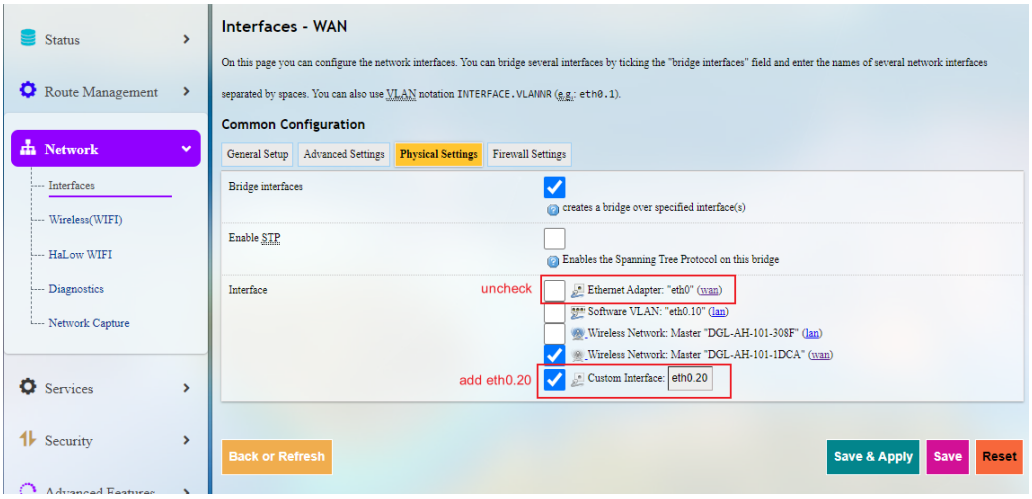
a. AP-mode HAP101 with 2.4GHz Wi-Fi in Client Mode

1. Log in to the device's VantronOS via 2.4GHz Wi-Fi as instructed in 2.3.1;
2. Navigate to **Network > Interfaces**;



3. Click the **Edit** button after **WAN**, then click the **Physical Settings** tab to edit the interface;

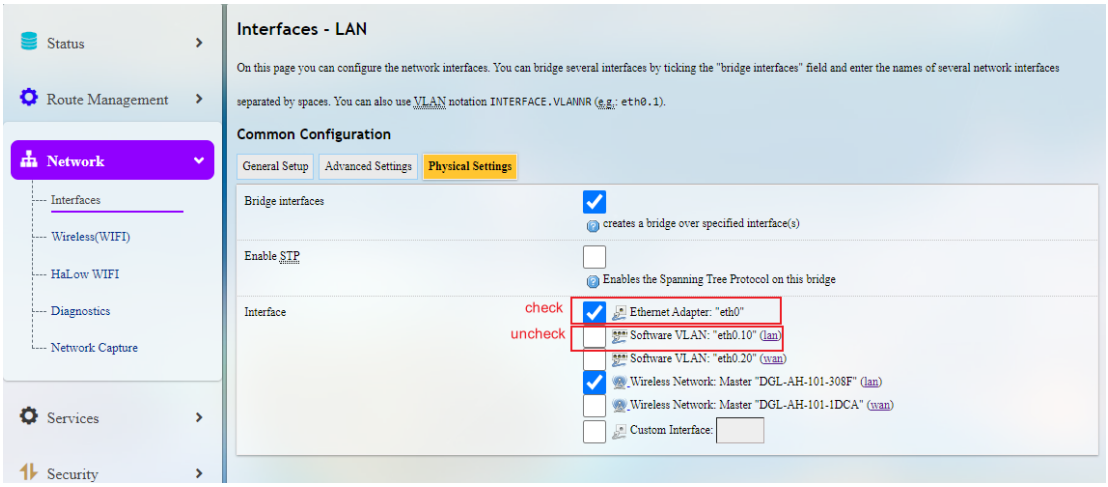
4. Uncheck the box next to “eth0”, add an “eth0.20” interface and select it;



5. Save and apply the settings, and the system will automatically return to the **Interfaces** page;

6. Click the **Edit** button after **LAN**, then click the **Physical Settings** tab to edit the interface;

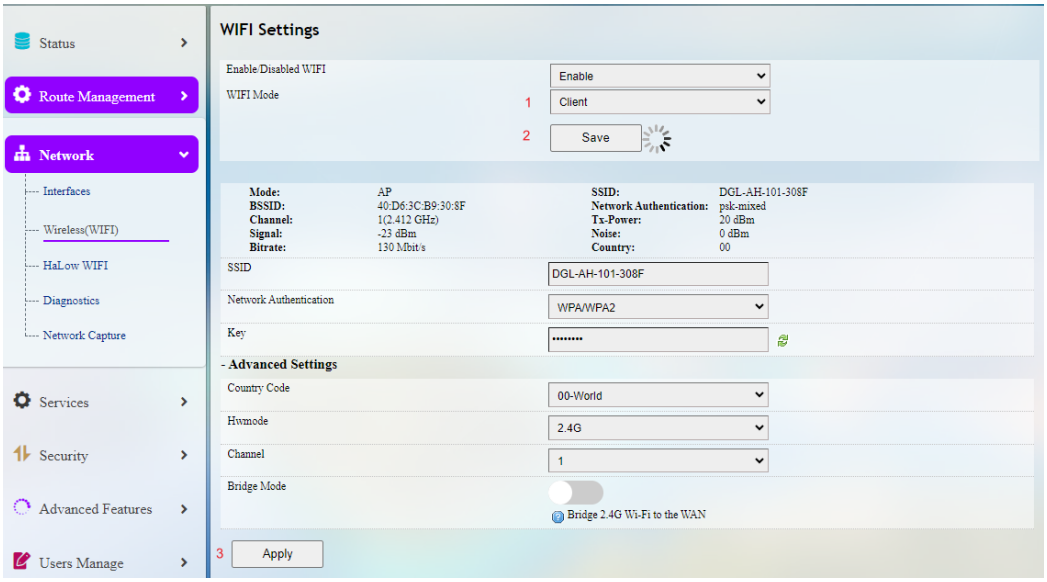
7. Check the box next to “eth0”, and check the box next to “eth0.10”;



8. Save and apply the settings, and the system will automatically return to the **Interfaces** page;

   If the 2.4GHz Wi-Fi connection between the host computer and HAP101 is interrupted, reconnect the host computer to the device via 2.4GHz Wi-Fi and log in to VantronOS as described in step 1.

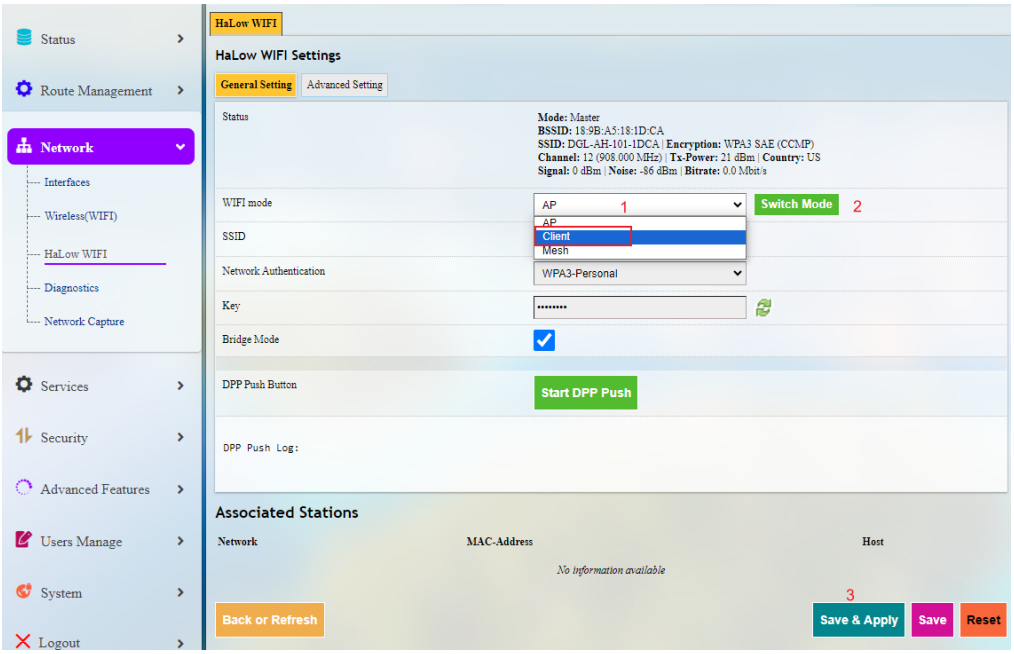
9. Navigate to **Network > Wireless (WIFI)**, and switch the 2.4GHz Wi-Fi to the client mode;



10. Refresh the page and VantronOS is not accessible, indicating the host computer is disconnected from the 2.4GHz Wi-Fi of the device;
11. Connect the host computer to the device via the Ethernet port using an Ethernet cable;
12. Log in to VantronOS using the LAN IP of the device: **172.18.2.1**.

b. STA-mode HAP101 with Bridged 2.4GHz Wi-Fi

1. Log in to the device's VantronOS via 2.4GHz Wi-Fi as instructed in 2.3.1;
2. Navigate to **Network > HaLow WIFI**;
3. Change the HaLow mode of the device to **Client**;

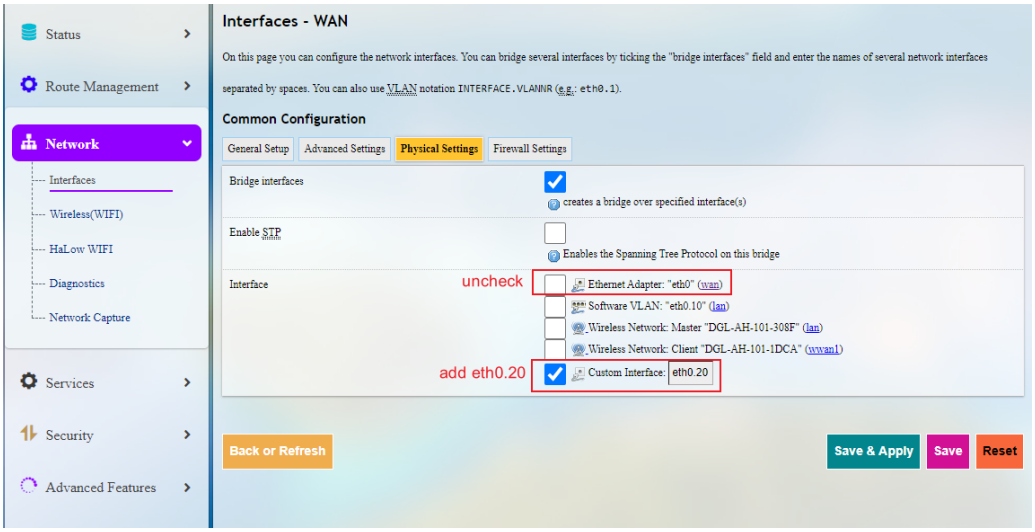


4. Reconnect the host computer to HAP101 using the 2.4GHz Wi-Fi, and log in to VantronOS using the IP: 172.18.3.1;

5. Navigate to **Network > Interfaces**;

6. Click the **Edit** button after **WAN**, then click the **Physical Settings** tab to edit the interface;

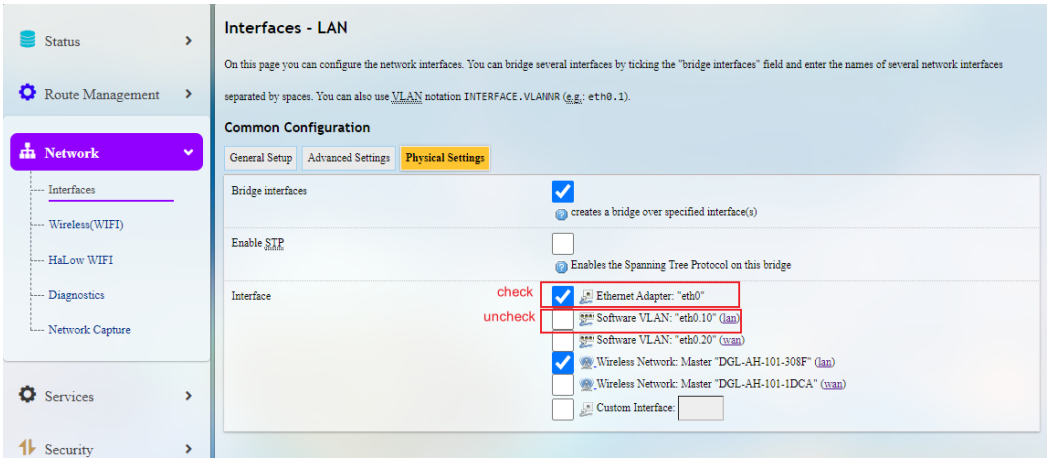
7. Uncheck the box next to “eth0”, and add an “eth0.20” interface;



8. Save and apply the settings, and the system will automatically return to the **Interfaces** page;

9. Click the **Edit** button after **LAN**, then click the **Physical Settings** tab to edit the interface;

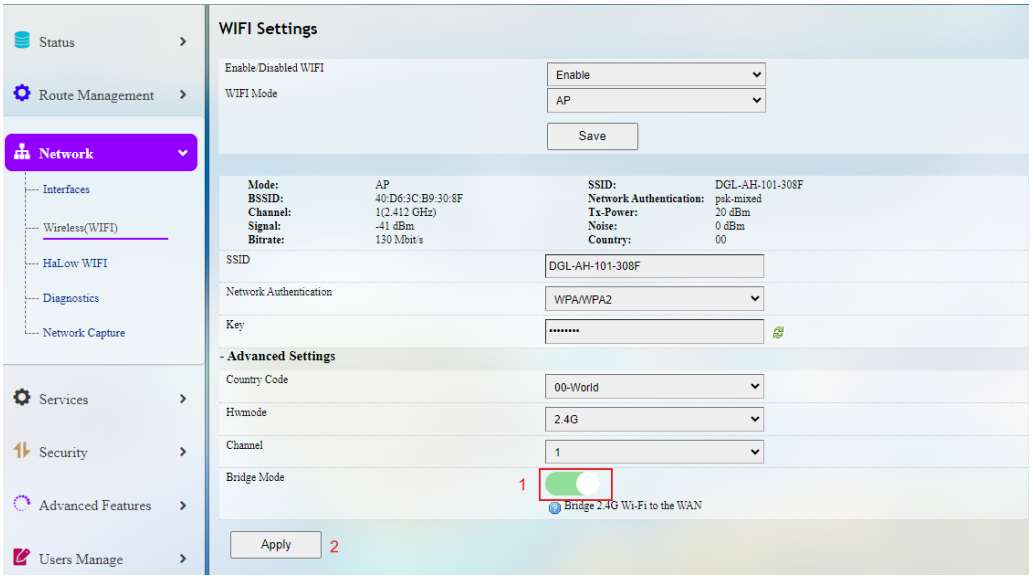
10. Check the box next to “eth0”, and uncheck the box next to “eth0.10”;



11. Save and apply the settings, and the system will automatically return to the **Interfaces** page;

    If the 2.4GHz Wi-Fi connection between the host computer and HAP101 is interrupted, reconnect the host computer to the device via 2.4GHz Wi-Fi and log in to VantronOS as described in Step 4.

12. Navigate to **Network > Wireless (WIFI)**, and enable the bridge mode of 2.4GHz Wi-Fi;



11. Refresh the page and VantronOS is not accessible because the 2.4GHz Wi-Fi of the device is bridged;

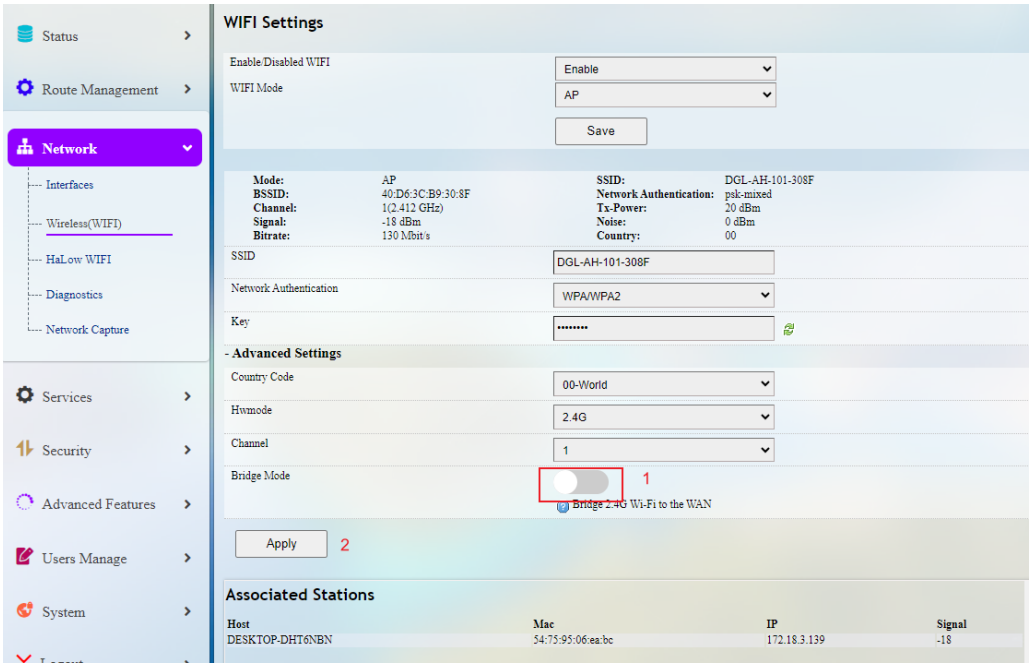
12. Connect the host computer to the device via the Ethernet port using an Ethernet cable;

13. Log in to VantronOS using the LAN IP of the device: **172.18.3.1**.

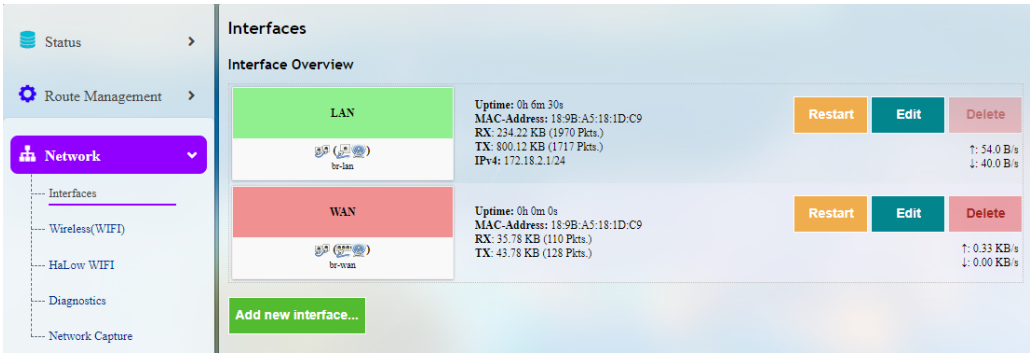
2.7.2 LAN port back to WAN port

To revert the LAN port back to its original WAN port function after the modification, follow the steps below:

1. Connect the host computer to the device **via the Ethernet port** using an Ethernet cable;
2. Navigate to **Network > Wireless (WIFI)**, and disable the bridge mode of the 2.4GHz Wi-Fi;

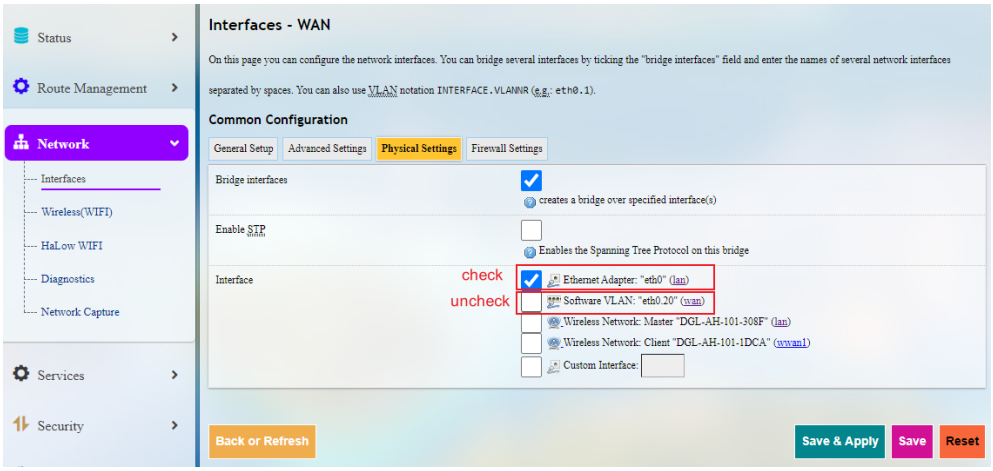


3. Connect the host computer to the 2.4GHz Wi-Fi of the device and log in to VantronOS using the LAN IP based on the HaLow mode of the device (172.18.2.1 for HaLow AP, 172.18.3.1 for HaLow STA);
4. Navigate to **Network > Interfaces**;



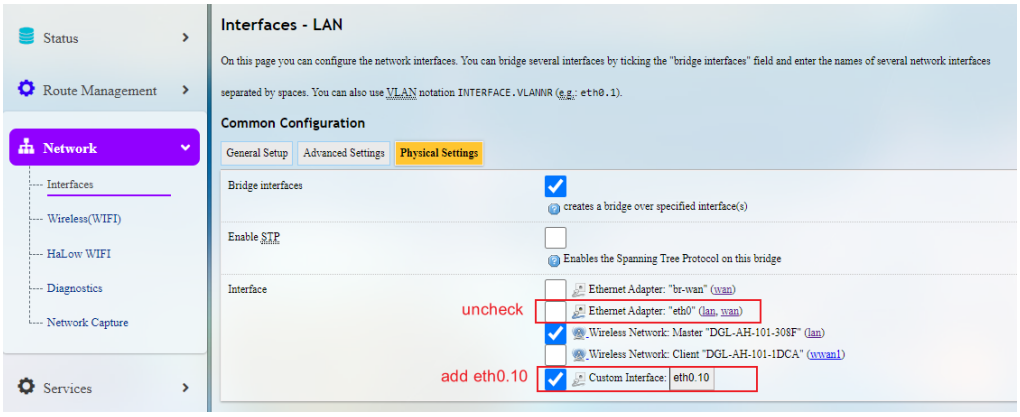
5. Click the **Edit** button after **WAN**, then click the **Physical Settings** tab to edit the interface;

6. Check the box next to “eth0”, and uncheck the box next to “eth0.20”;



7. Save and apply the settings, and the system will automatically return to the **Interfaces** page;

8. Click the **Edit** button after LAN, then click the **Physical Settings** tab to edit the interface;



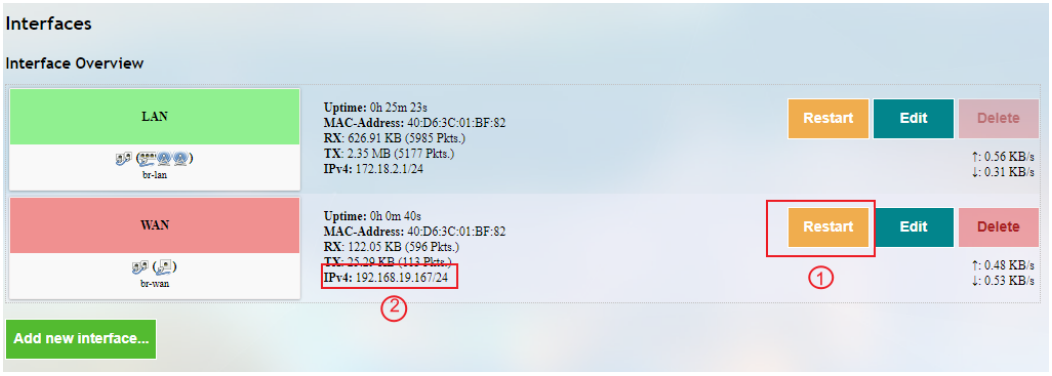
9. Save and apply the settings, and the system will automatically return to the **Interfaces** page;

10. If the device is operating in HaLow STA mode, you can optionally switch it to the AP mode and access VantronOS using the IP: 172.18.2.1.

11. When VantronOS returns to the Interface page, the Ethernet port has been modified to a WAN port;

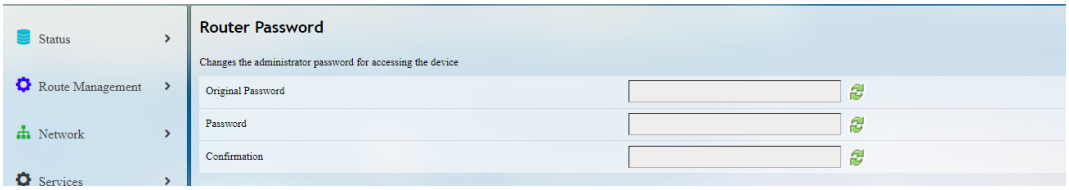
12. Connect the device to a router or switch through the Ethernet port;

13. Restart the WAN port and you will see the WAN port IP allocated by the router or switch.



2.8 Password Change

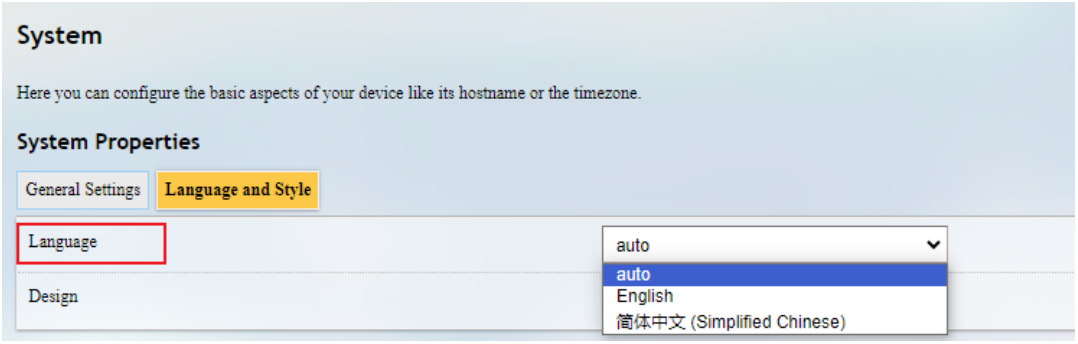
It is up to you to decide whether you would like to change the login password for the current user after logging in to VantronOS.



1. Navigate to **System > Administration > Router Password**;
2. Input the original password for the current user;
3. Input a new password and confirm the password;
4. Save and apply the settings;
5. The system will log out automatically;
6. Log in with the new password.

2.9 Language Change

Currently the system supports simplified Chinese and English. The system language is set to automatically follow the browser language by default. You can change the system language by navigating to **System > System > System Properties > Language and Style** in VantronOS.



Auto: System language based on the browser language (default)

English: English interface

Simplified Chinese: Simplified Chinese interface

2.10 Factory Reset the Device

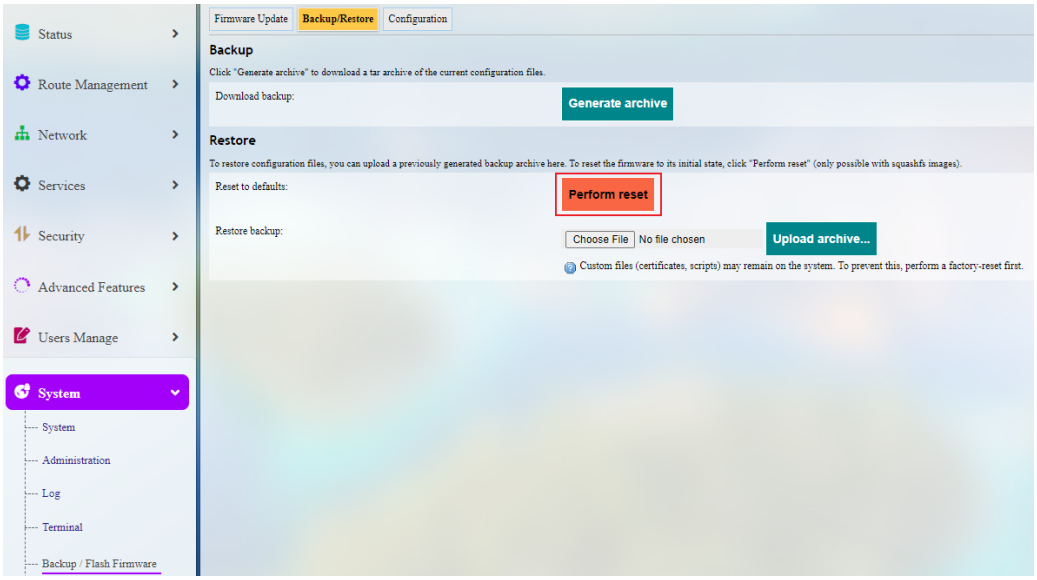
There are two options to factory reset the device, one from the hardware perspective and the other from the software perspective. Once factory reset, the device will be restored to Wi-Fi HaLow AP mode and 2.4GHz Wi-Fi AP mode by default.

2.10.1 Hardware reset

Action	Result
1. Long press (> 10s) the Pair/Restore button; 2. Release the button; 3. Short press the button (< 1s) within 5s after release.	Factory reset the device with all user data cleared

2.10.2 Software reset

1. Login to VantronOS through any of the methods set out in 2.3 depending on the connection of the host computer;
2. Navigate to **System > Backup/Flash Firmware > Backup/Restore** in VantronOS;



3. Click the **Perform reset** button in red;
4. Customized settings will be restored to default.

   You can find more in 3.8.5 about backing up the current configurations before device reset in VantronOS.

CHAPTER 3 DEVICE SETUP IN VANTRONOS

3.1 Introduction to VantronOS

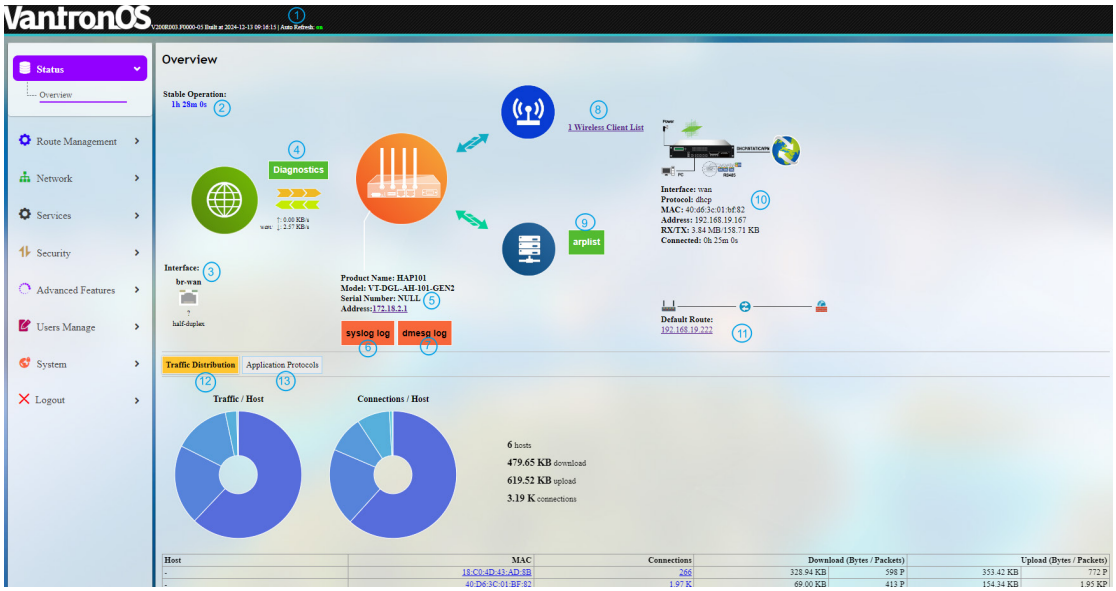
VantronOS is an intelligent operating system developed by Vantron team, facilitating the configuration and management of Vantron IoT communication devices. It is built upon the Linux system and optimized for embedded hardware. The operating system follows a modular design and plug-in expansion approach, utilizing the Linux kernel with a built-in firewall to ensure secure internet connectivity for the devices, protecting them from potential attacks.

VantronOS incorporates a user-friendly UI interface based on the MVC framework, providing a simple and efficient setting entry for users. Additionally, it offers seamless interfacing with various cloud management platforms, including the self-developed BlueSphere GWM, as well as popular platforms like Azure, Alibaba Cloud, Huawei Cloud, and RootCloud. This enables users to remotely monitor, operate, and diagnose devices without the need for on-site technical support engineers. VantronOS facilitates the interconnection and interaction between users and the Industrial Internet of Things, enhancing the overall efficiency and convenience of device management.

In the following sections, key features of VantronOS are described. Unless otherwise stated, ***Wi-Fi*** in this manual refers to 2.4GHz Wi-Fi, and ***HaLow*** refers to Wi-Fi HaLow.

3.2 Status

This page provides the overall information of HAP101, including stable operation duration, number of devices connected to the device, default routing, hardware information, traffic statistics, etc.



Description of the numbered areas

1. Firmware version and auto refresh on/off button (click the on/off button enable/disable auto refresh)
2. Stable running duration of the device after establishing a network connection
3. Current working status of the Ethernet WAN port
4. A collection of the network diagnostic tools (refer to 3.4.4 for details)
5. The product name, model, serial number, and management address of the device
6. System log information
7. Kernel log information
8. Number of clients connected to the device via 2.4GHz Wi-Fi

You will access the Wi-Fi settings upon a click of the number.

9. Address information of clients connected to the device via Ethernet
10. Current network connection information of the device
11. Default route (gateway) currently used by the device
12. Traffic distribution of clients connected to the device displayed by MAC addresses

Clicking on each MAC address in the table at the bottom page will get the detailed traffic information of the clients.

13. Traffic of application layer protocols

3.3 Route Management

3.3.1 Automatic network routing

Automatic routing might be beneficial when HAP101 is running in the 2.4GHz Wi-Fi station mode or Wi-Fi HaLow station mode. It ensures that the device maintains Internet access when multiple links are available. It features automatic link detection, automatic route switching, and recovery.

The default link detection and data forwarding are prioritized based on the following rule: Ethernet > 2.4GHz Wi-Fi (STA) > Wi-Fi HaLow (STA) > others. The smaller the **metric**, the higher the priority.

The following screenshot demonstrates the network priority of the device when it has Ethernet, Wi-Fi HaLow, and 2.4GHz Wi-Fi connections.

Description of the numbered areas

1. The status of the current connection
2. Enable/Disable link detection for the device (once disabled, there will be no tracking information)
3. Current network interfaces
4. Type of the network interfaces that the device is connected to
5. The status of the current network interfaces
6. Enable/Disable the specific interface (once disabled, this interface will be offline)
7. Select to ping the gateway of the interface or not
8. Settings for tracking the interface (The smaller the **metric**, the higher the priority)
9. The tacking log of the interfaces

3.3.2 Static routing

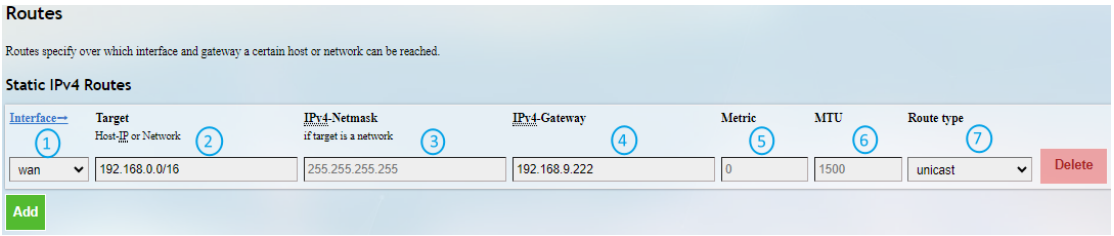
The static routing feature allows you to specify interface rules for route access.

Example:

Requirement: When the device has both 2.4GHz Wi-Fi (station) and Ethernet WAN connections, the internal network (192.168.0.0 - 192.168.255.254) is accessed via the WAN port by the internal server. Other data access is realized via the 2.4GHz Wi-Fi interface.

Static routing:

Click the **Add** button on the page to set up a new static route and configure the route.



Description of the numbered areas

1. Select an interface to configure the route
2. Input the host IP address of the destination
3. Input the subnet mask of the destination (255.255.255.255 by default)
4. Input the IPv4 gateway address as the exit interface/next hop
5. Set the gateway metric (The smaller the number, the higher the priority)

6. Set the MTU
7. Select a route type (refer to the details next page)

Be sure to save the settings before you exit the page.

Description of the route type:

Type	Description
Unicast	The route entry describes real paths to the destinations covered by the route prefix.
Local	The destinations are assigned to this host. The packets are looped back and delivered locally.
Broadcast	The destinations are broadcast addresses. The packets are sent as link broadcasts.
Multicast	IP datagrams are sent to a group of interested receivers in a single transmission. It is not present in normal routing tables.
Unreachable	The destinations are unreachable. Packets are discarded and the ICMP message of host unreachable is generated. The local senders will receive an EHOSTUNREACH error.
Prohibit	The destinations are unreachable. Packets are discarded and the ICMP message of communication administratively prohibited is generated. The local senders will receive an EACCES error.
Blackhole	The destinations are unreachable. Packets are discarded silently. The local senders will receive an EINVAL error.
Anycast	The destinations are any cast addresses assigned to this host. They are mainly equivalent to local with one difference that such addresses are invalid when used as the source address of any packet.

3.4 Network

Users can change the settings related to the available network interfaces in the **Network** page.

3.4.1 Interfaces

All the network interfaces currently available and configurable are displayed under **Network > Interfaces**.

The numbered areas are detailed as follows:

1. Interface overview
    - HaLow relay: This interface appears when the Wi-Fi HaLow station interface is bridged
    - LAN: virtual LAN port for 2.4GHz Wi-Fi AP/HaLow AP/VLAN gateway (default address: 172.8.2.1 and changes to 172.18.3.1 when the HaLow mode switches to **Station**)
    - WAN: default Ethernet port
    - WWAN0: 2.4GHz Wi-Fi client interface
    - WWAN1: Wi-Fi HaLow station interface
2. Interface traffic and address details
3. Manually restart the interface
4. Edit the interface settings
5. Delete the interface
6. Instantaneous traffic of the interface
7. Add a new interface

The interfaces may differ from what is shown above depending on the Internet connection of the device.

3.4.1.1 LAN

The LAN port is a virtual interface for 2.4GHz Wi-Fi AP/HaLow AP/VLAN gateway. Its default IP address is 172.8.2.1, which changes to 172.18.3.1 when HaLow mode switches to Station. You can modify the interface information as needed.

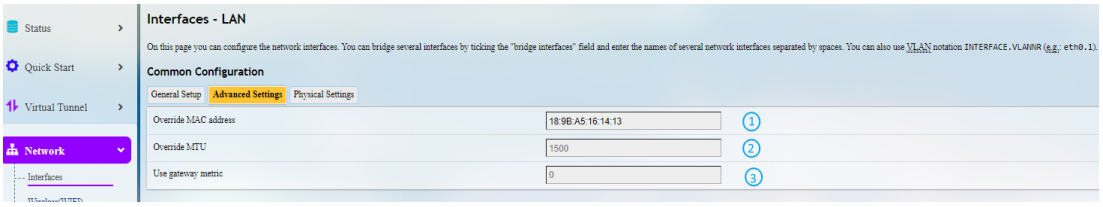
- **Common Configurations**

Clicking on the **Edit** button behind the **LAN** port allows you to access the configurations of the port, and **General Setup** is displayed by default.

Description of the numbered areas

1. Status of the interface
2. The interface protocol is set to static as default to avoid IP conflict
3. The static IP address of the port (you can modify as needed)
4. The LAN port subnet mask

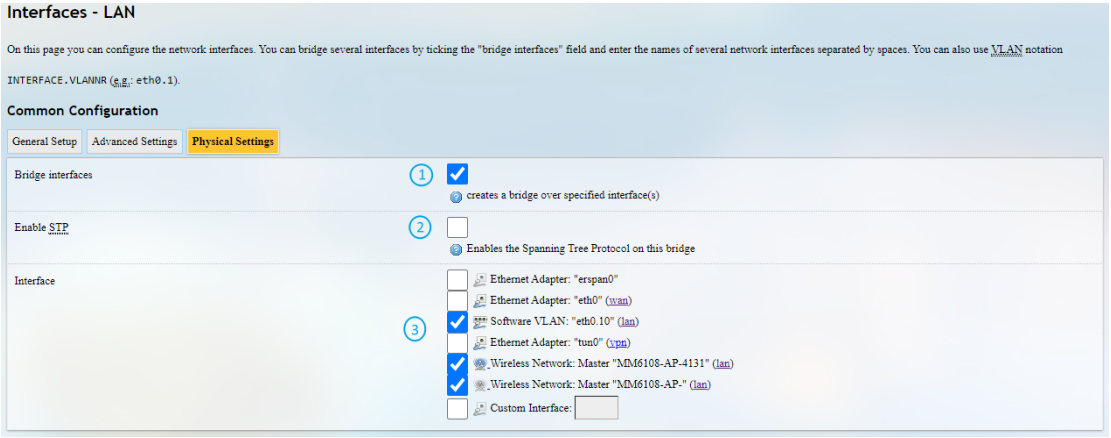
In the **Advanced Settings** next to the general setup:



Description of the numbered areas

1. MAC address cloning
2. Set the MTU (keep the default setting)
3. Set a gateway metric (keep the default setting)

There is a **Physical Settings** tab next to **Advanced settings**, allowing you to configure the LAN port for network bridge.



Description of the numbered areas

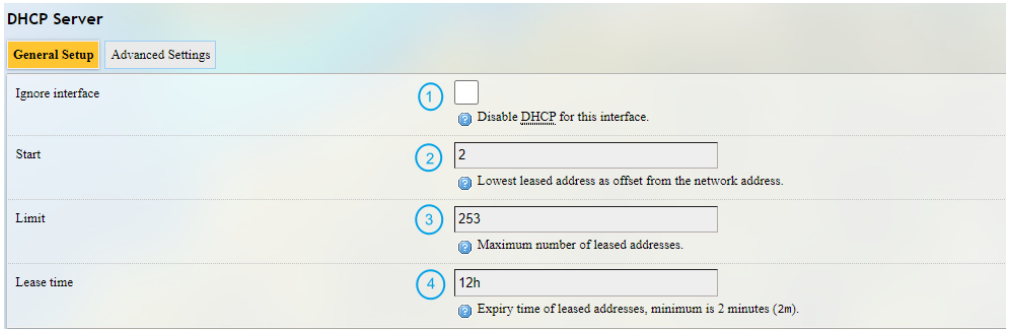
1. Enable/Disable the interface for network bridge
2. Enable/Disable STP protocol
3. Select the interfaces for bridge connection

Once bridged, the interfaces will be on the same network segment, sharing the same IP. Be sure to save the settings before you exit the page.

- **General DHCP server**

The DHCP service dynamically allocates IP addresses to devices connected to HAP101 via the LAN port (2.4GHz Wi-Fi AP/HaLow AP/VLAN gateway). If either 2.4GHz Wi-Fi AP or HaLow AP is bridged to the Ethernet WAN port, the DHCP service on the corresponding interface will be disabled. In this case, IP addresses will be assigned by the DHCP server for the WAN port.

In the **General Setup** page of **DHCP Server**, DHCP could be set up with more details:



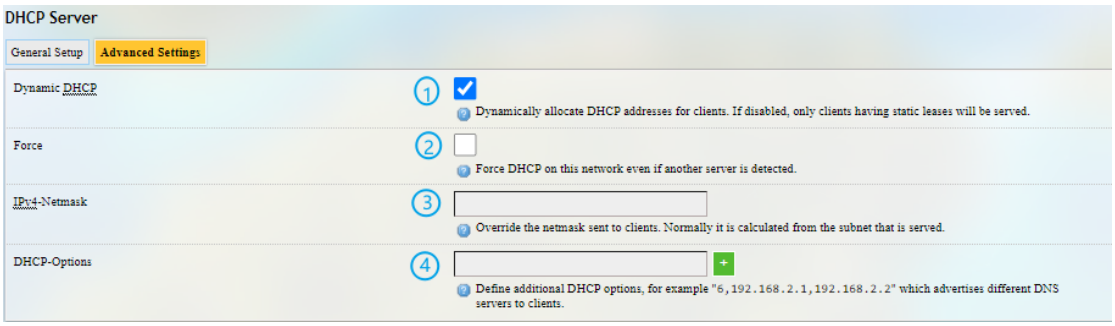
Description of the numbered areas

1. Disable/Enable the DHCP service

If disabled, the DHCP service will not be available to the client devices connected to the LAN port of HAP101.

2. Start number of the leased addresses when the DHCP service is enabled
3. Maximum number of the leased addresses
4. Expiry time of the leased addresses (min. 2m)

Advanced Settings of DHCP Server:



Description of the numbered areas

1. Enable/Disable allocation of DHCP addresses for client devices
2. Force enablement of DHCP service (to bypass other servers)
3. Override the netmask sent to clients

Normally it is based on the subnet that is served.

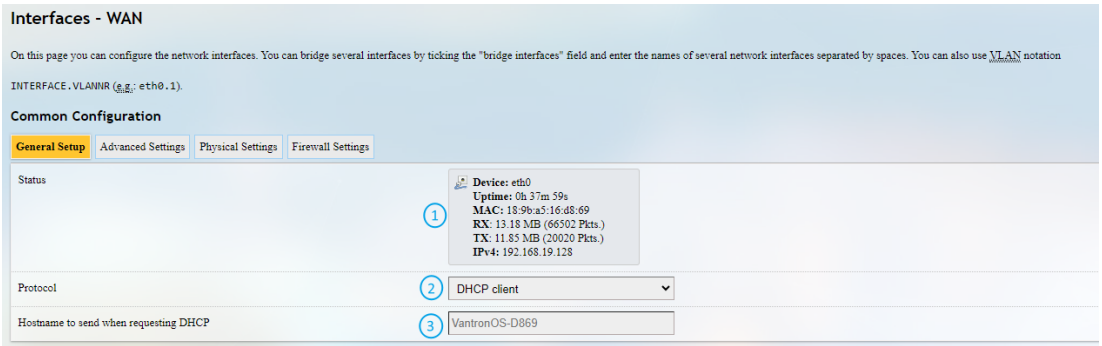
4. Add different DNS servers for client devices

*Be sure to save the settings before you exit the page. Clicking on **Back or Refresh** will get you back to the general information of the network interface.*

3.4.1.2 WAN

- **General settings**

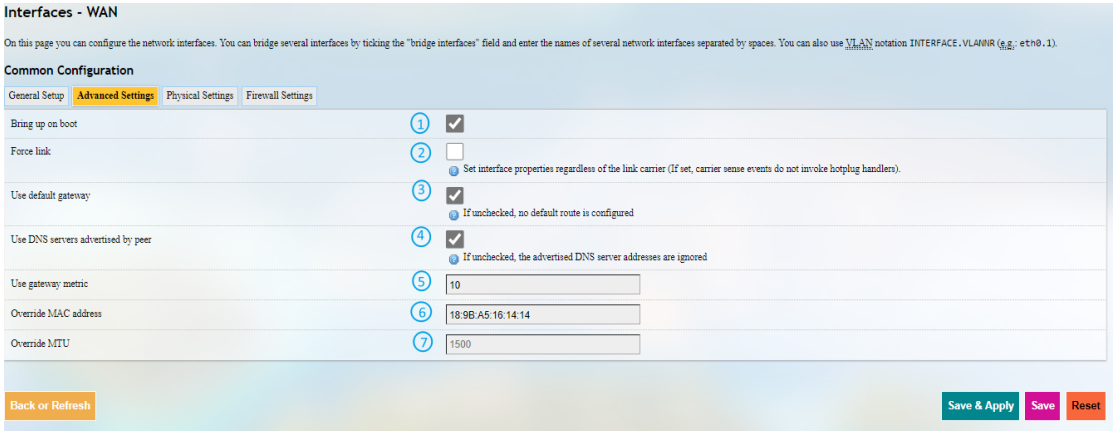
Clicking on the **Edit** button behind the **WAN** port will allow you to access the configurations of the WAN port, and **General Setup** is displayed by default.



Description of the numbered areas

1. Status of the WAN port
2. Current WAN protocol (‘DHCP client’ indicates that the port obtains an IP from the DHCP server after establishing an Ethernet connection.)
3. Default hostname of the device when requesting DHCP

- **Advanced settings**



Description of the numbered areas

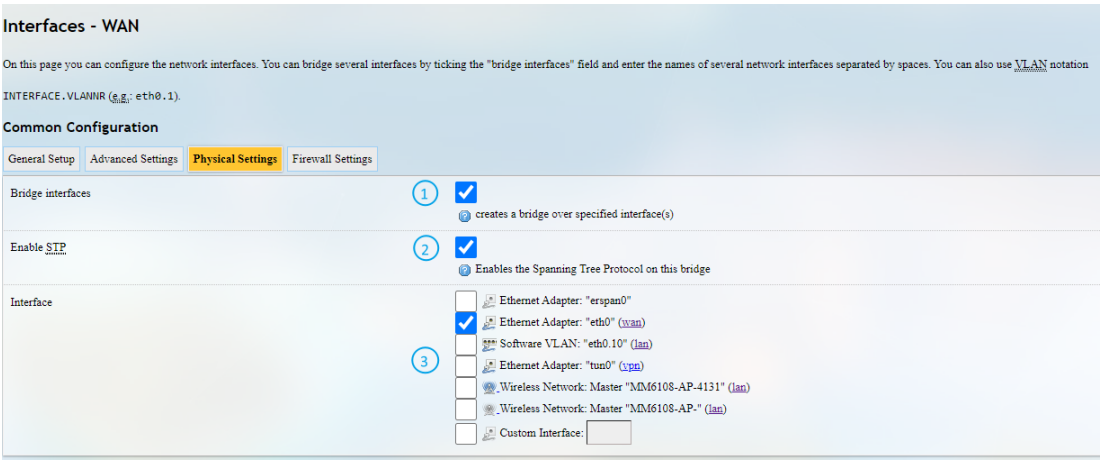
1. Check the box to bring up the port upon device boot
2. Force link (once the box is checked, hotplug handlers will not be invoked after a link change)
3. Enable/Disable **Use default gateway**
4. Enable/Disable **Use DNS server advertised by peer**

If this option is disabled, you will need to define a DNS server.

5. Set a gateway metric
6. MAC address cloning
7. Set the MTU

Be sure to save the settings before you exit the page.

There is a **Physical Settings** tab next to **Advanced settings**, allowing you to configure the WAN port for network bridge.

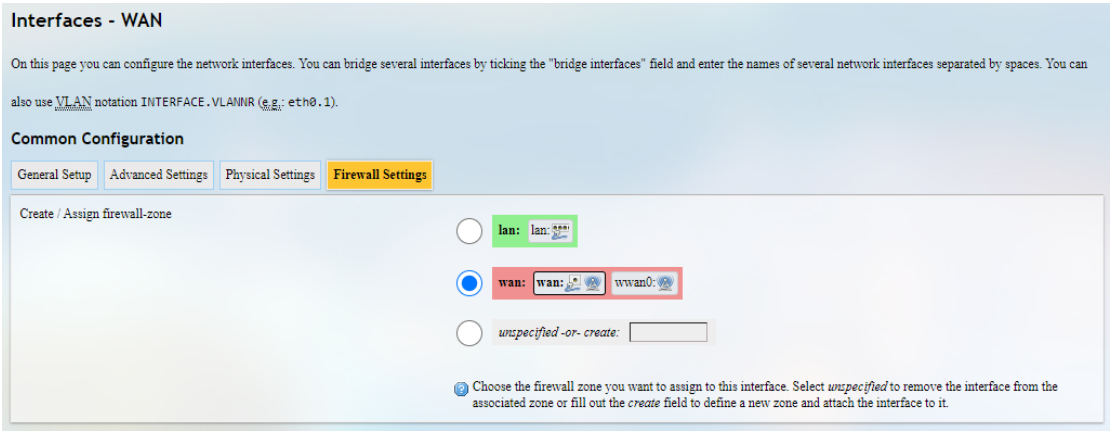


Description of the numbered areas

1. Enable/Disable the interface for network bridge
2. Enable/Disable STP protocol
3. Select the interfaces for bridge connection

Be sure to save the settings before you exit the page.

There is a **Firewall Settings** tab next to the **Physical settings** tab, allowing you to create or designate a firewall zone.



When ‘unspecify or create’ is selected, you can remove the interface from the associated firewall zone or create a new zone.

Refer to 2.6.1 and 2.6.2 to change the Ethernet port of the device to a LAN port or revert it to a WAN port depending on your needs.

3.4.2 Wireless (WIFI)

You can switch the device between AP and client modes for a 2.4GHz Wi-Fi connection.

3.4.2.1 Wi-Fi – AP Mode

Description of the numbered areas

1. Enable/Disable the Wi-Fi module
2. Select a Wi-Fi mode (AP mode by default)
3. If you have switched the Wi-Fi mode in the prior step, click **Save** to apply the change
4. Wi-Fi AP information
5. Wi-Fi AP SSID

Make sure the name does not contain special characters including $, `, \.

6. Authentication method for the connection
7. Wi-Fi password (no less than 8 characters)

Clicking the refresh icon will display/hide the password

8. Country code (**00** applies to all regions)
9. Wi-Fi frequency band (determined by the hardware)

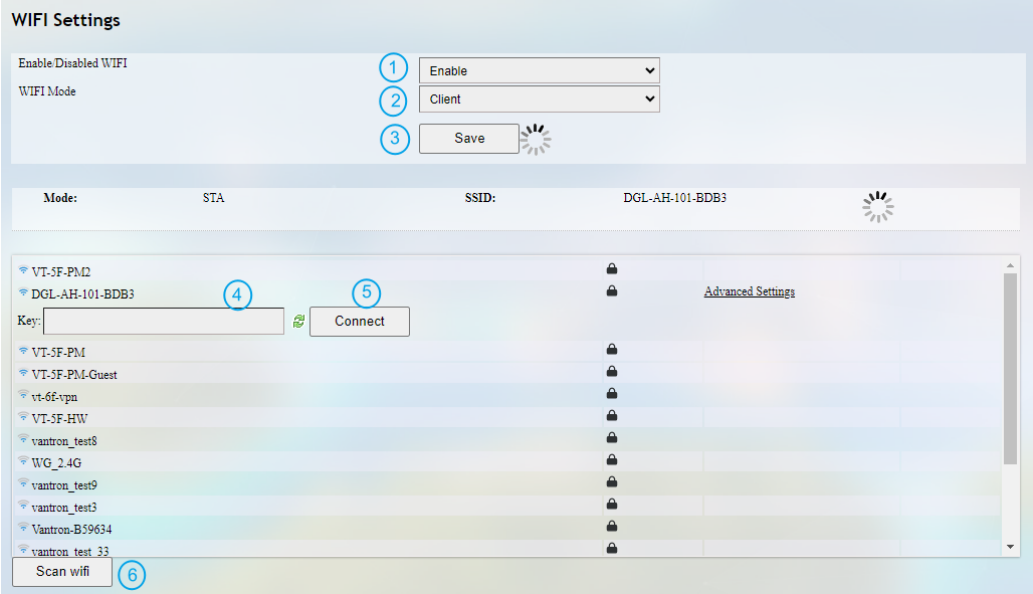
10. You can select a signal channel from the drop-down list
11. Toggle the button to bridge the 2.4GHz Wi-Fi with the Ethernet interface (After bridging, clients connected to HAP101 via 2.4GHz Wi-Fi will receive a valid IP from the DHCP server when the Ethernet port of HAP101 is connected to the server.)
12. If you have modified the Wi-Fi settings, make sure to click **Apply** to allow the changes to take effect
13. List of client devices currently connected to the 2.4GHz Wi-Fi of the device

3.4.2.2 Wi-Fi – Client Mode

When HAP101 is set as a 2.4GHz Wi-Fi client, you can further configure the device here and connect it to an AP.

*A wwan0 port will be added (shown in the **Interface** page) when the Wi-Fi client mode is enabled.*

After setting an HAP101 to the Wi-Fi client mode, please make sure the host computer and HAP101 are connected to the same network if you need to log in to VantronOS for the device.

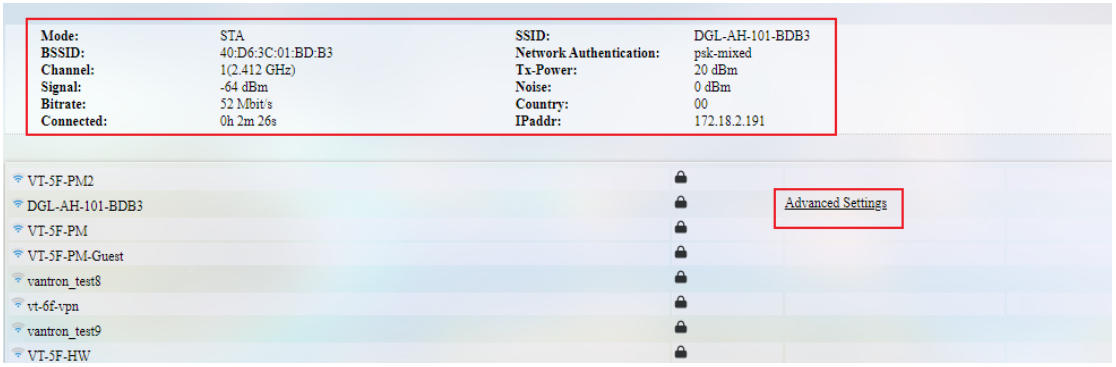


Follow the steps below to connect the device to a Wi-Fi AP:

1. Enable the Wi-Fi module;
2. Select the Wi-Fi **Client** mode from the drop-down list;
3. Click the **Save** button to apply the change;
4. Click the target access point and input the password of the access point
5. Click the **Connect** button to join the network

6. Click the **Scan wifi** button to refresh the Wi-Fi list if the target SSID is not identified

When the device is successfully connected to a Wi-Fi AP, the network information will be displayed above the SSID list. You can further configure the device MAC and IP protocol by clicking the **Advanced Settings** option after the SSID.



3.4.3 Wi-Fi HaLow

Refer to 2.5 for the Wi-Fi HaLow settings for HaLow AP, Station, and Mesh modes.

After setting an HAP101 to the HaLow client mode, the LAN IP of the device will change to 172.18.3.1. Please make sure the host computer and HAP101 are connected to the same network and use the updated IP address for VantronOS login when needed.

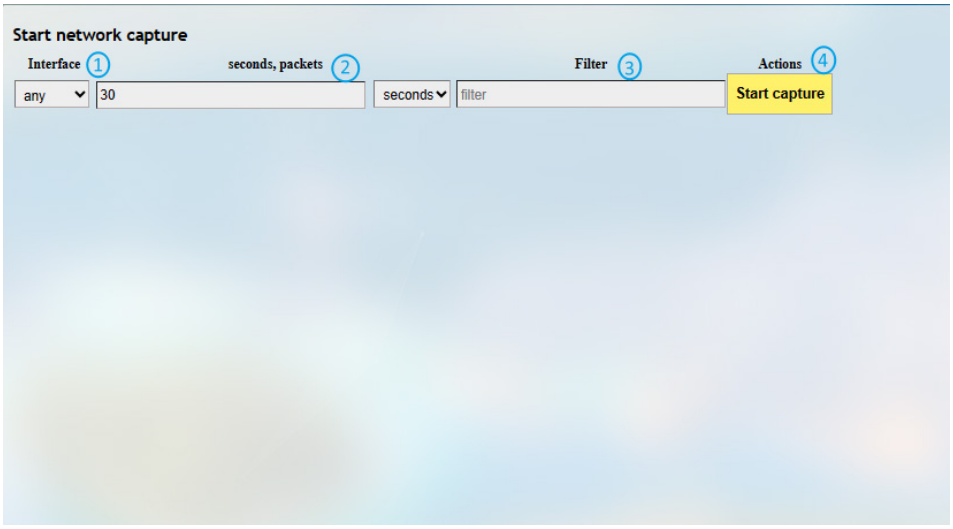
3.4.4 Diagnostics

Tools available in **Diagnostics** are explained below:

Tool	Description
Ping	To test the connectivity and measure the round-trip response time between HAP 101 and external IP addresses on the internet.
Traceroute	To trace the path that network traffic takes to reach a destination, showing the number of hops and the response time of each hop along the way.
Nslookup	To query the Domain Name System (DNS) to obtain information about domain names, IP addresses, and DNS records associated with a domain.

3.4.5 Network capture

The **Network capture** feature provides a flexible way to follow up and verify network issues. You can use wireshark to open and check the packets captured.



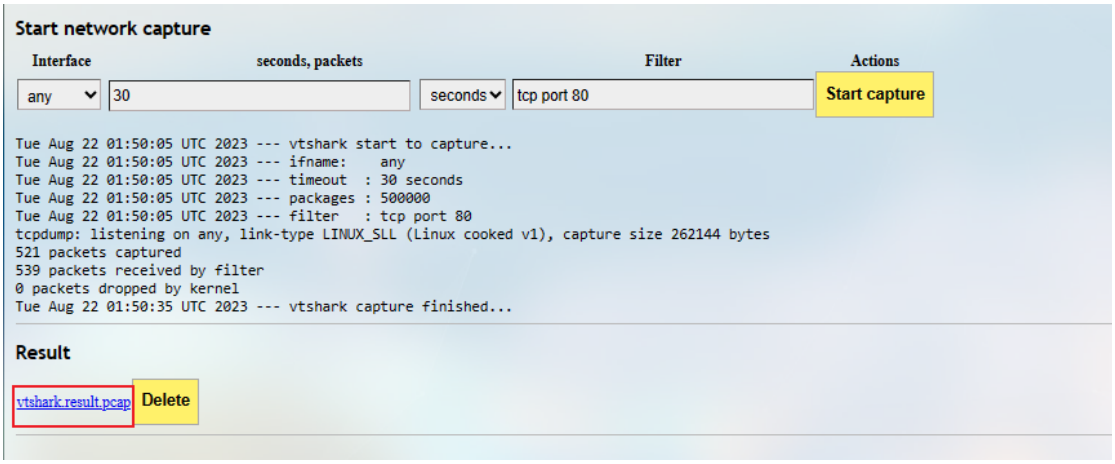
Description of the numbered areas

1. The interface from which the packets are captured (all interfaces are selected by default)
2. The measurement by which the data packets are captured (by seconds or by packet counts as explained below)
3. The filter for capturing the designated packets (more details are available at https://www.tcpdump.org/manpages/pcap-filter.7.html for advanced filtering)
4. Start the data capturing

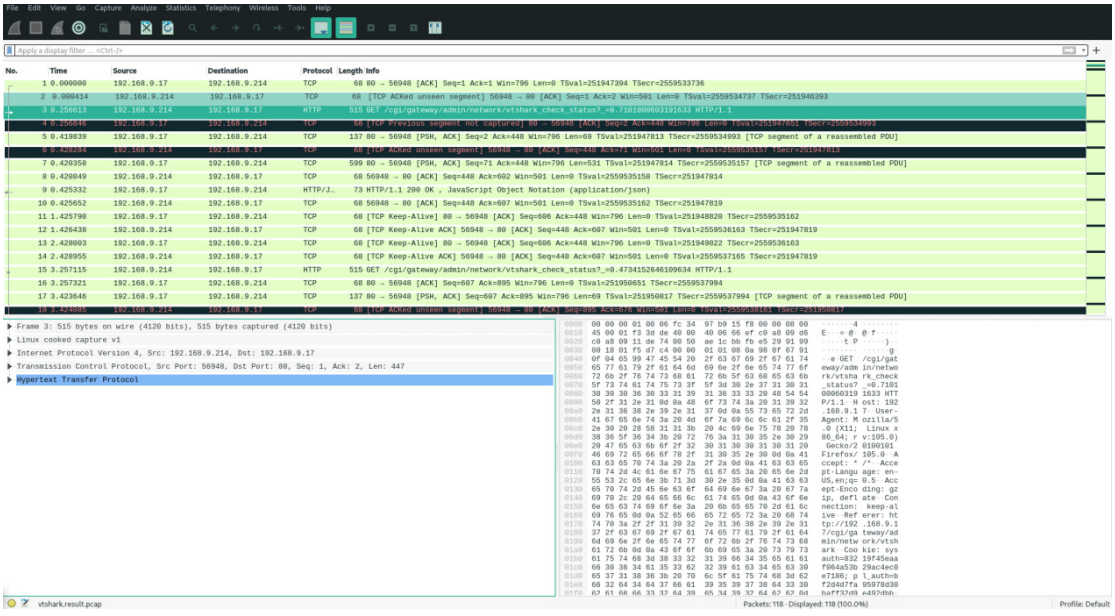
Packets capturing by seconds and by packet counts:

Measurement	Description
Seconds	To specify a time duration for data capturing. For instance, you can input '10/20/30…' for the data capturing, which indicates that the capture will stop in 10/20/30 seconds.
	The system supports up to 500,000 packets for the time-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset time duration.
Packets	To specify the count of packets for data capturing. For instance, you can input '100/200/500…' for the data capturing, which indicates that the capture will stop when 100/200/500 packets have been captured.
	The system supports up to 10 minutes (600 seconds) for the packet-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset packet counts.

In the following scenario, the capture targets at all interfaces for the http packets from ‘tcp port 80’ for 30 seconds.



Clicking the link will download the result to the local directory and you can open it with wireshark.



3.5 Services – DHCP Server

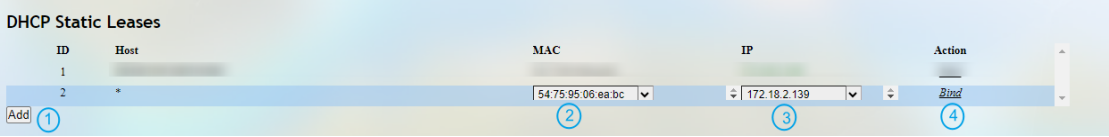
The DHCP service dynamically allocates IP addresses to devices connected to HAP101 via the LAN port (2.4GHz Wi-Fi AP/HaLow AP/VLAN gateway). If either 2.4GHz Wi-Fi AP or HaLow AP is bridged to the Ethernet WAN port, the DHCP service on the corresponding interface will be disabled. In this case, IP addresses will be assigned by the DHCP server for the WAN port.

The DHCP server settings are kept the same as those provided in the **DHCP Server** feature for the LAN port. Modifying the parameters in either section will take effect to the port. Refer to 3.4.1.1 for the general and advanced settings of the LAN port.

Description of the numbered areas

1. Current virtual LAN port status of the device (default IP: 172.18.2.1)
2. Enable/Disable the DHCP service
3. Start number of the leased addresses when the DHCP service is enabled
4. Maximum number of the leased addresses
5. Expiry time of the leased addresses (min. 2m)
6. Address of the DNS server
7. Click Save to apply the settings if any of above parameters is changed

The **DHCP Static Leases** feature allows you to allocate a static IP to a specific client device connected to HAP101 using the MAC of the client device.



Description of the numbered areas

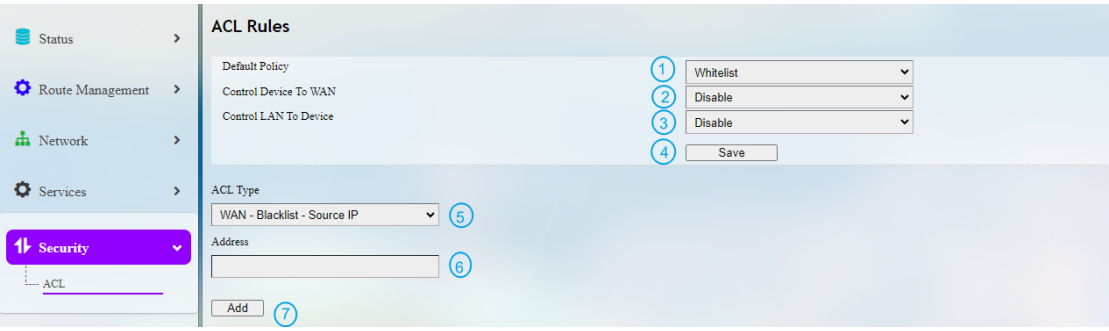
1. Click the **Add** button to configure the target client device
2. Select the MAC of the target device from the drop-down list
3. Input a static address for the target device and make sure it is on the same network as the LAN port DHCP server
4. Click ***Bind*** to allow the settings to take effect

3.6 Security – ACL

By setting an access control list (ACL) rule, you can enable/disable the forwarding of the specified addresses.

Whitelist policy: **All addresses but those added to the ACL have the access**

Blacklist policy: **All addresses but those released to the ACL are blocked**



Follow the steps below to create an ACL rule:

1. Select a whitelist or blacklist policy;
2. Control the access of HAP101 in a WAN network (“**disable”** indicates that the newly created rule will not be applied);
3. Control the access of HAP101 in a LAN network (“**disable”** indicates that the newly created rule will not be applied);
4. If you have made changes, make sure to save them;

5. Select an ACL type;

*If you have selected the **whitelist policy**, you need to configure the **blacklist IP**. Otherwise, the rule will not take effect. "Source IP" refers to the IP from which the access requirement is initiated towards HAP101 and "Destination IP" refers to the IP to which the access requirement is initiated from HAP101.*

6. Enter the addresses that match the rule;
7. Click **Add** to create the rule;
8. Repeat above steps to add more rules.

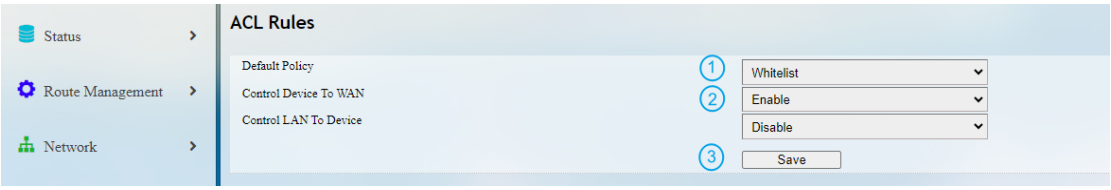
3.6.1 Whitelist ACL rule

Example Scenario:

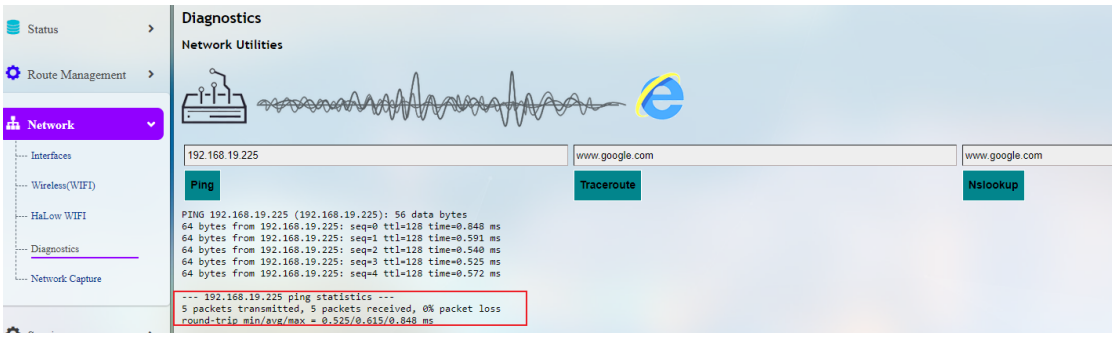
- **Devices**: An HAP101 and another device are connected to the same router, which acts as the DHCP server.
- **IP Addresses**:
  - HAP101: 192.168.19.167
  - A device in the same WAN network: 192.168.19.225

Requirement: Block HAP101 from accessing an IP in the same WAN network.

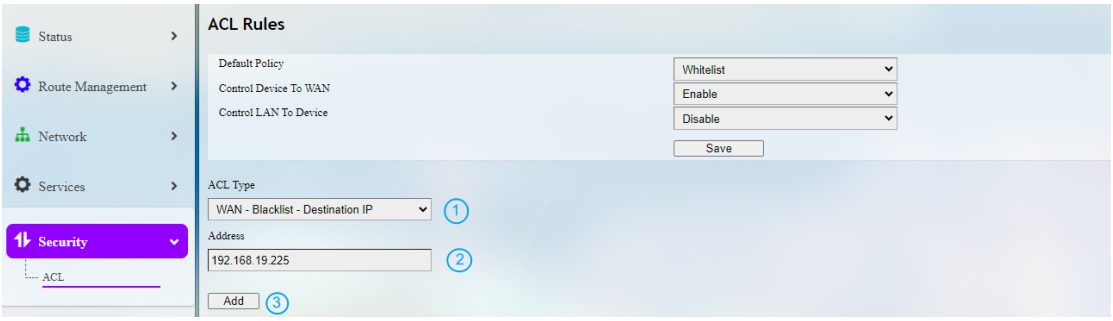
Network status before IP blocking:



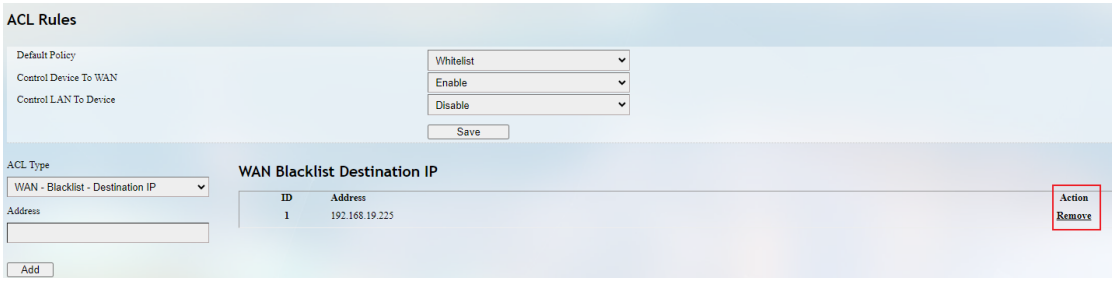
1. Select the **Whitelist** policy;
2. Enable the "to WAN" rule;
3. Save the changes and check the result in **Network > Diagnostics > Ping**.



Rule setting:

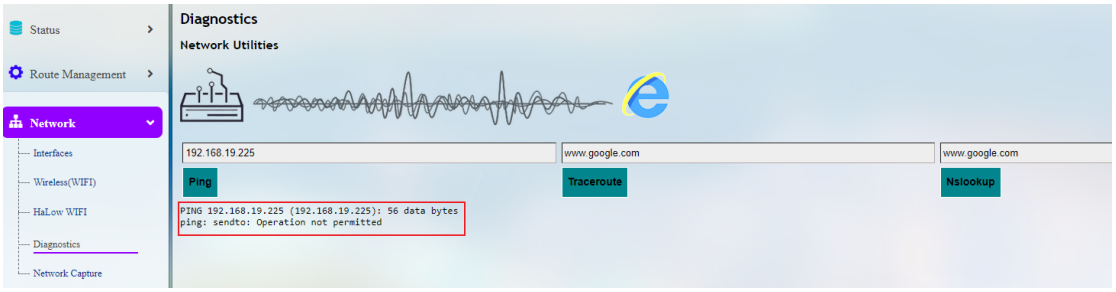


1. Select a blacklist control rule for the destination IP;
2. Specify the IP that the device is not allowed to access;
3. Click **Add** to create the rule;



Once the rule is created, you can delete it when it is not needed.

4. Navigate to **Network > Diagnostics > Ping** and Ping the destination IP.



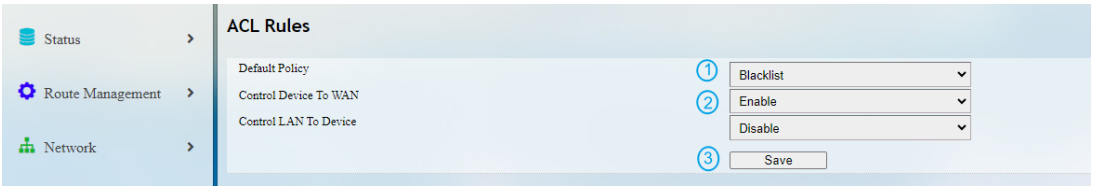
3.6.2 Blacklist ACL rule

Example Scenario:

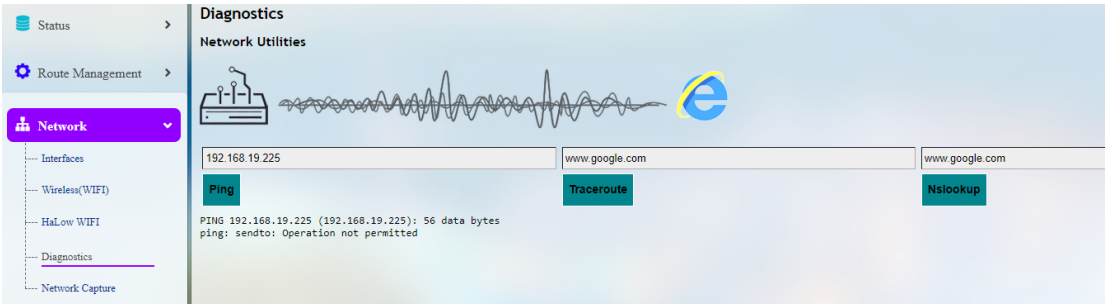
- **Devices**: An HAP101 and multiple other devices are connected to the same router, which acts as the DHCP server.
- **IP Addresses**:
  - HAP101: 192.168.19.167
  - A device in the same WAN network: 192.168.19.225

Requirement: Only allow HAP101 to access a specified IP in the same WAN network.

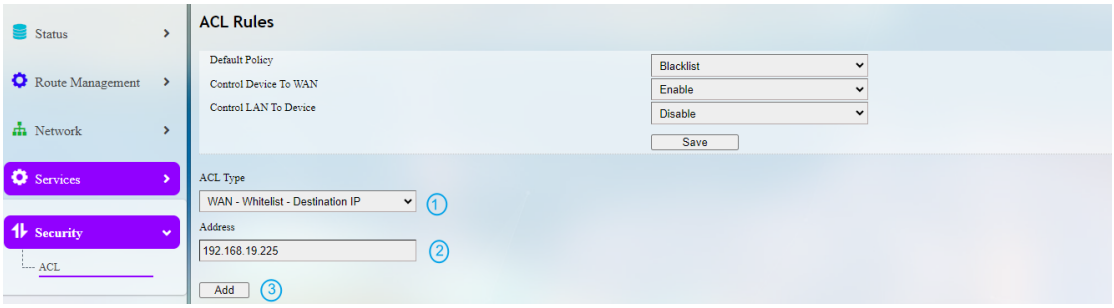
Network status before IP release:



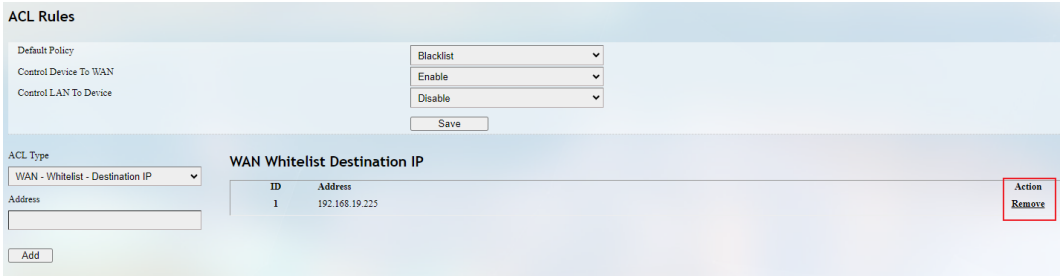
4. Select the **Blacklist** policy;
5. Enable the “to WAN” rule;
6. Save the changes and check the result in **Network > Diagnostics > Ping**.



Rule setting:

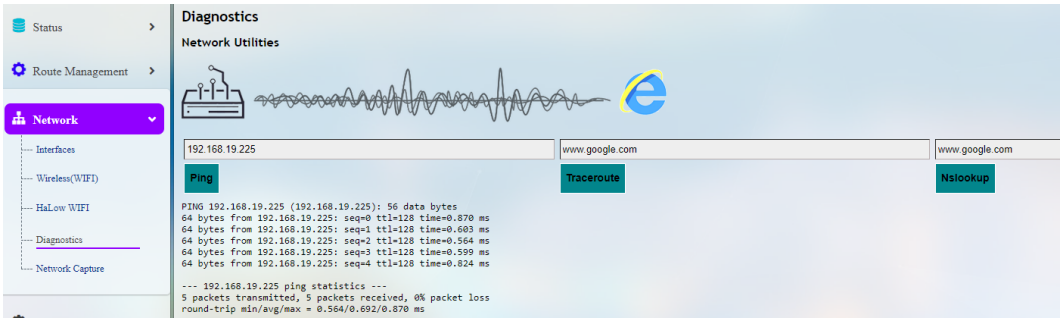


1. Select a whitelist control rule for the source IP;
2. Specify the IP that the device is allowed to access;
3. Click **Add** to create the rule;



Once the rule is created, you can delete it when it is not needed.

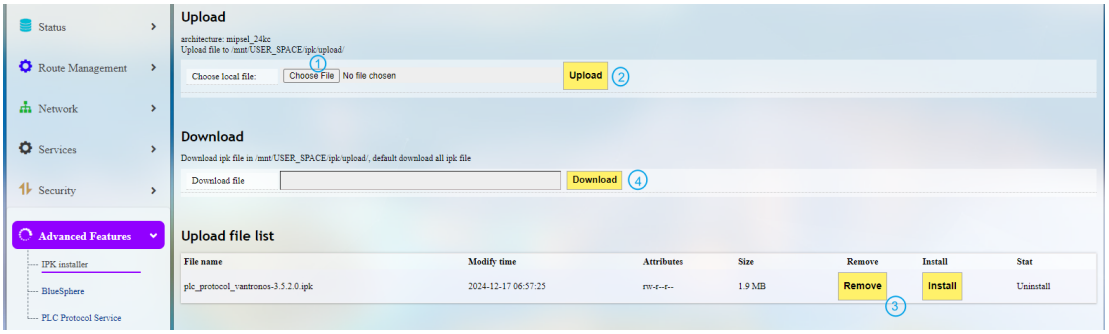
4. Navigate to **Network > Diagnostics > Ping** and Ping the destination IP.



3.7 Advanced Features

3.7.1 IPK Installer

With IPK Installer, users can upload and install self-compiled IPK packages on the device, or download packages from the device to the local directory.



Description of the numbered areas

1. Select an .ipk file from the local directory
2. Click **Upload** to upload the file to the device (default path: /mnt/USER_SPACE/ipk/upload/)
3. You can delete or install the file after the .ipk file is uploaded
4. You can also input a file path (in /mnt/USER_SPACE/ipk/upload/) to download a specific file to the local directory

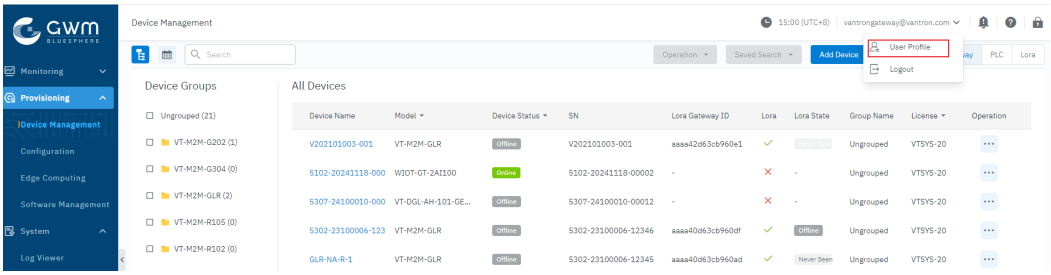
3.8 BlueSphere

HAP101 can be remotely managed through BlueSphere GWM, a cloud-based management portal that empowers organizations to effortlessly provision, monitor, and manage Vantron IoT communication devices.

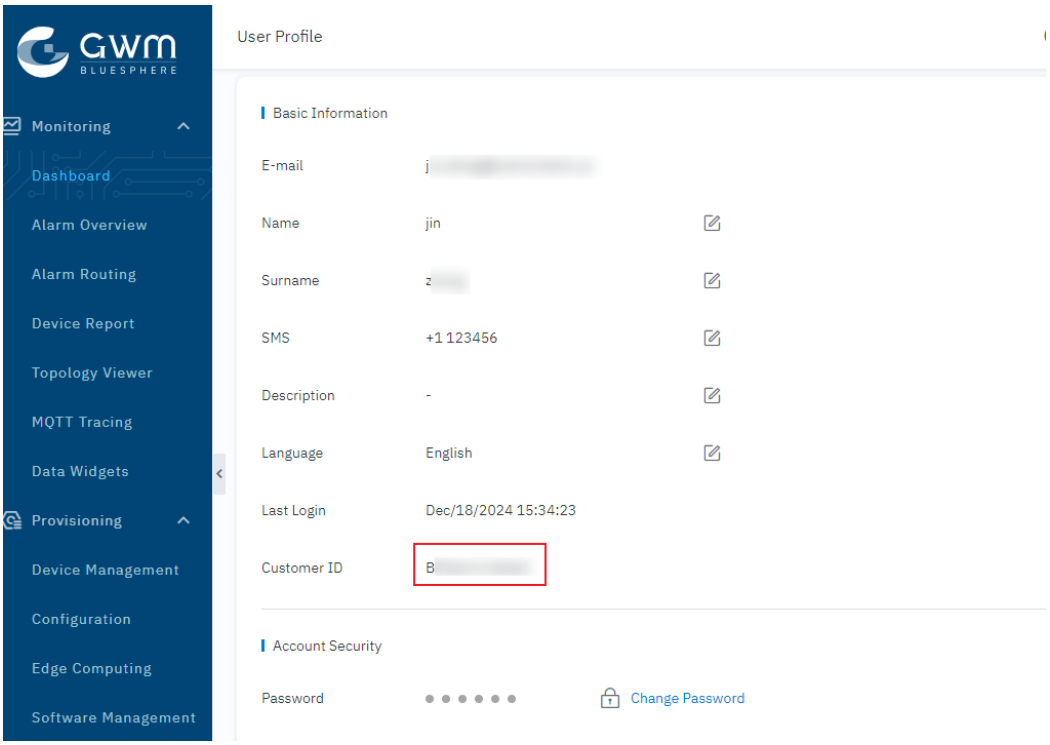
By entering the **customer ID** copied from BlueSphere GWM, you can enroll HAP101 into BlueSphere GWM for remote control and view the device communication log directly in VantronOS. Follow the steps below to enroll the device.

1. Log in to BlueSphere GWM at https://gatewaymanager.bluesphere.cloud/#/login with your authorized account and corresponding password;

2. Click the user account in the top right corner and select the **User Profile** option after the login;

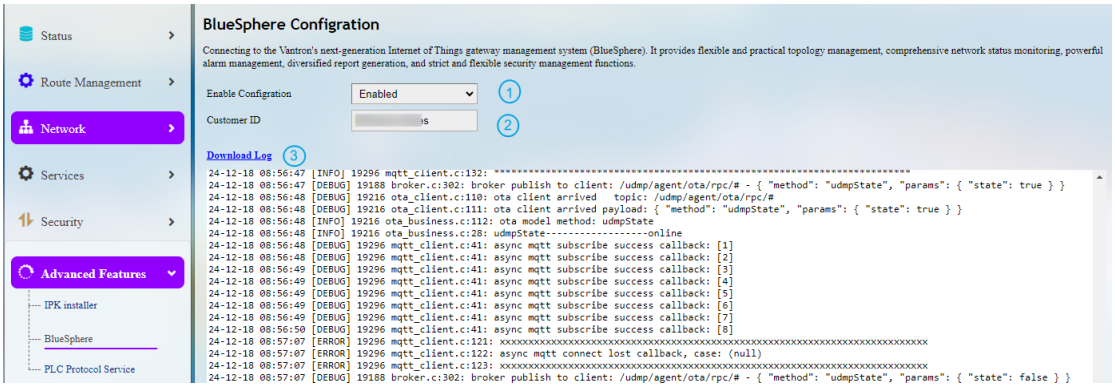


3. Locate the **Customer ID** and copy it for use in subsequent steps;



4. Connect HAP101 to internet;

5. Refer to 2.3 for VantronOS login to HAP101 and navigate to **Advanced Features > BlueSphere;**



1) Paste the customer ID;

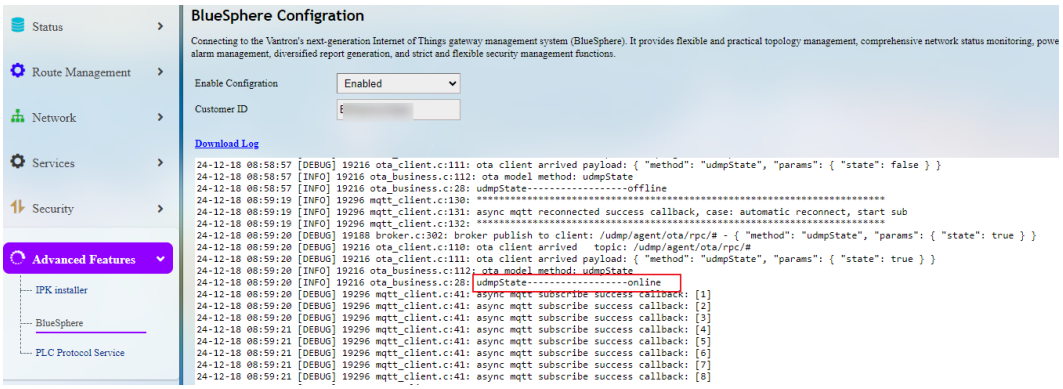
2) Enable the configuration;

3) The device log will be automatically printed and you can click the link to download.

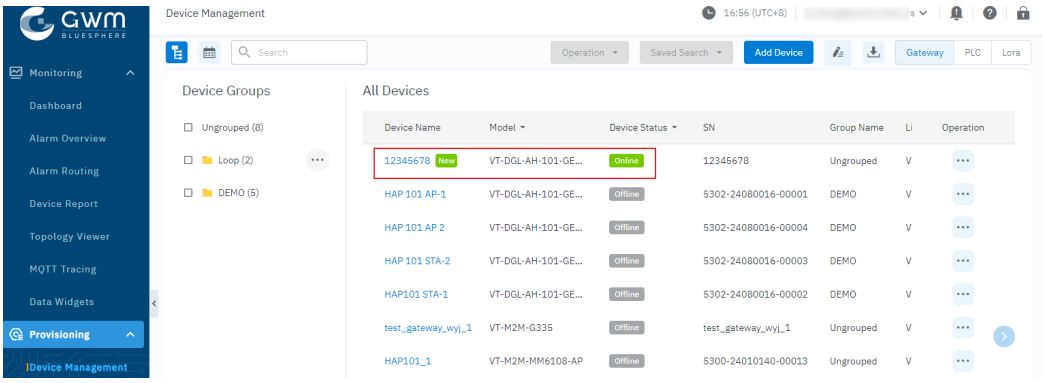
6. Wait for the UDMP Agent to download and install;

The UDMP Agent is the application that allows HAP101 to interface with BlueSphere GWM.

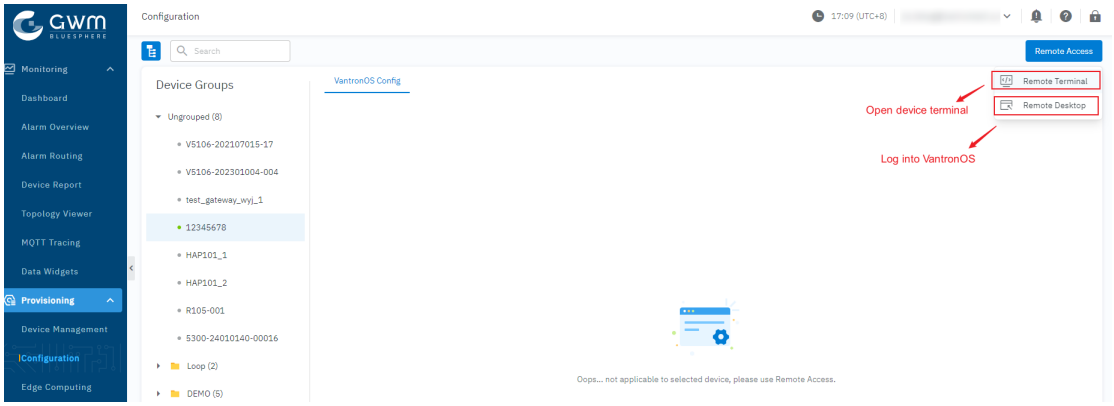
7. When the UDMP agent is online, it indicates the device is enrolled to BlueSphere GWM with success;



8. Return to BlueSphere GWM, and navigate to **Provisioning > Device Management** to view the device status.



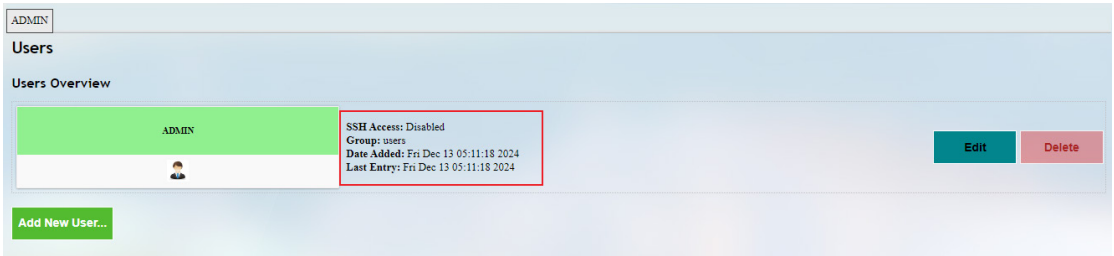
The newly enrolled device will be named by its **serial number** by default. Clicking the device name will direct you to the configuration page where you can start a remote session.



3.9 User Management

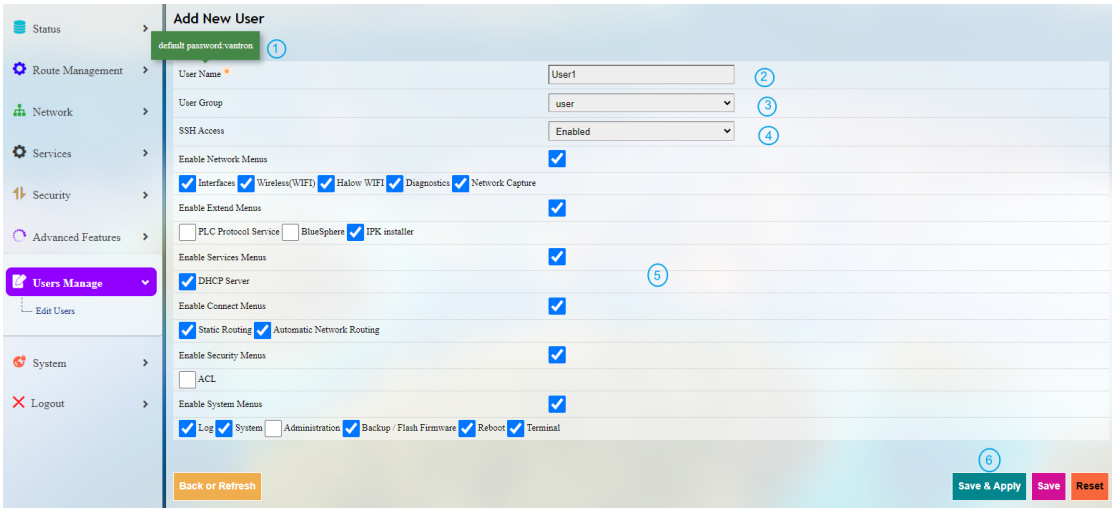
User management page displays the current user information and allows you to add new users or edit the existing users to assign different permissions to different roles.

Key information of the current user:



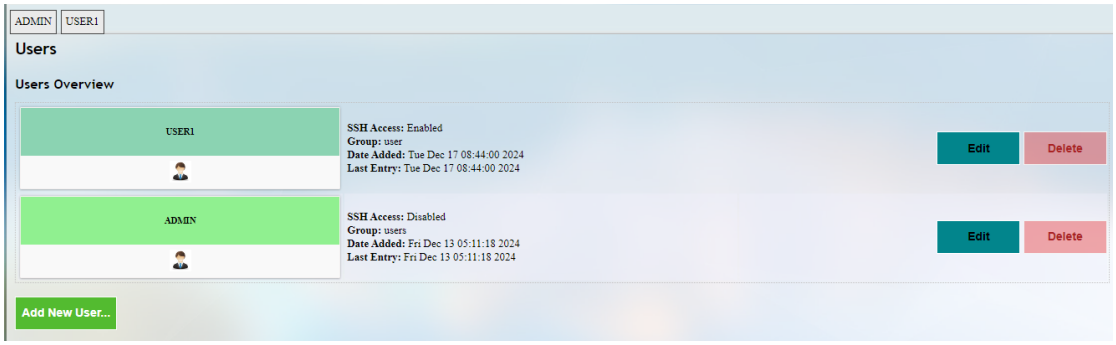
To add a new user, click the **Add New User** button below the existing user.

In the new page, you can create the user and enable certain features for the user.



1. **Default password of the new user is "vantron"**;
2. Input a username (no space allowed);
3. Select a user group that will define the permissions and roles for the new user;
4. Choose whether to grant the new user SSH access to the device. If enabled, the user can log in remotely via SSH;
5. Check the box next to the first-level menu items to expand the sub-menus, where you can configure additional specific permissions and functions for the new user;
6. Save and apply the settings before you exit

After creating the user, it will be added to the user list, with key information displayed.



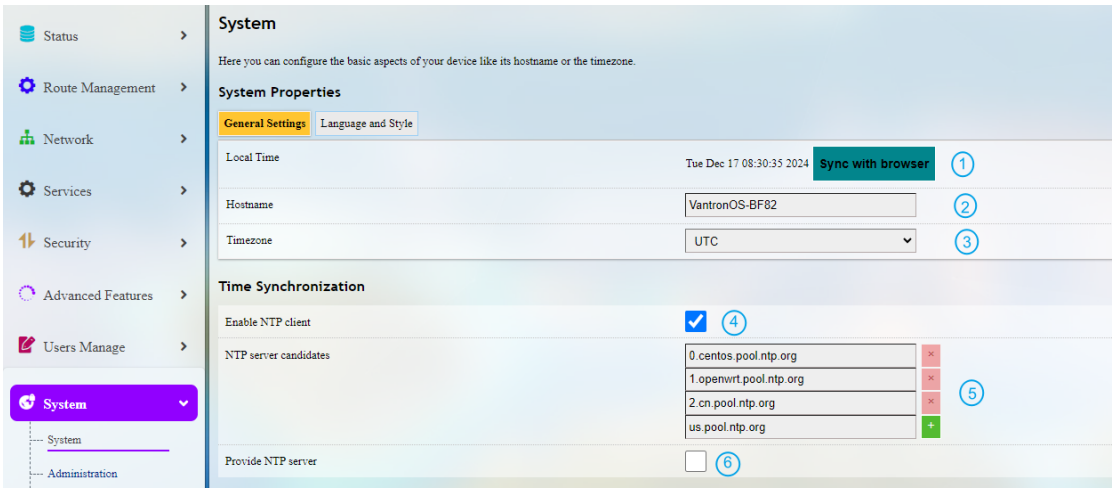
Clicking the **Edit**/**Delete** button behind a user allows you to:

- **Edit**: Enable or disable specific features or permissions for this user.
- **Delete**: Remove the user from the system entirely.

3.10 System

3.10.1 System

Apart from the device settings you might have made in previous sections, here you can configure the device system in more details, including the host name, time zone, administrative password and so on.



Description of the numbered areas

1. Synchronize the device time with the browser (local) time upon a click of the button
2. Host name of the device displayed when logging in to the device terminal
3. Device time zone
4. Enable/Disable NTP online time adjustment
5. NTP server candidates that can be used to synchronize the internal clock of the device with an accurate time source
6. Enable/Disable the NTP online time server

HAP101 is used as an NTP server.

For **language settings**, please refer to 2.8.

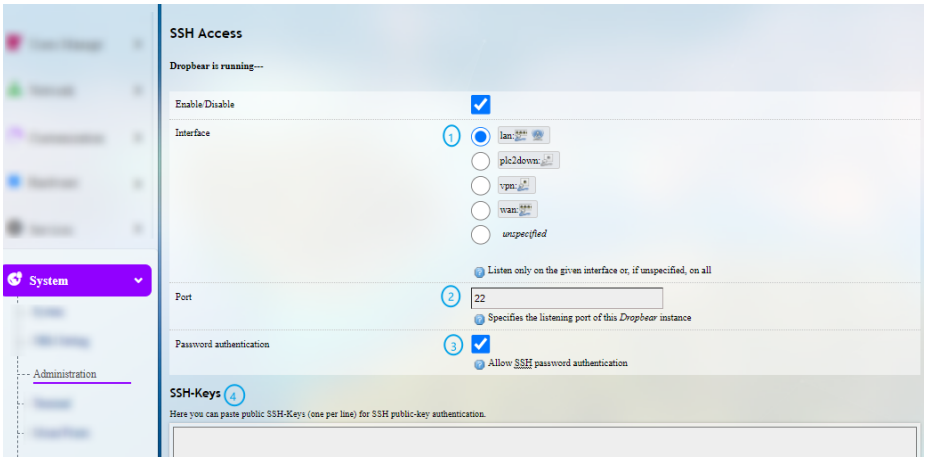
3.10.2 Administration

You can reset the password for accessing the web portal of the device in the **Administration** menu. Please refer to 2.7 for details.

SSH Login

Follow the steps below to initiate an SSH login to the device on a Windows computer.

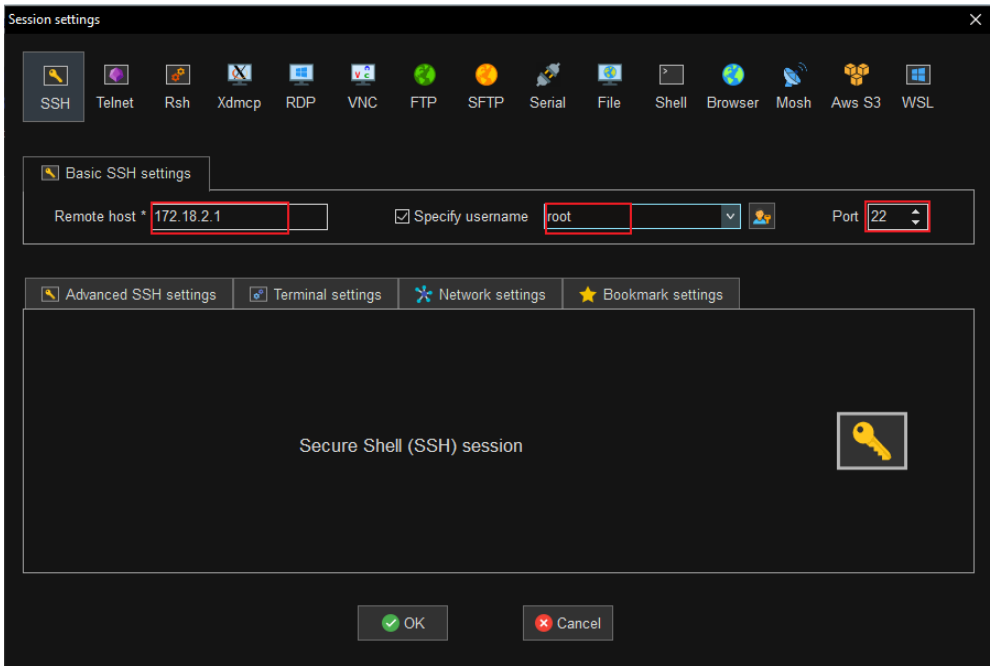
1. Make sure the Windows computer is on the same network as HAP101;
2. Navigate to **System > Administration** in VantronOS, and enable **Dropbear**;



1) Depending on the connectivity of the host computer and HAP101, select a port to access (When “unspecified” is selected, SSH login is available through both ports);
2) Specify a port number for monitoring (port 22 by default)
3) Enable SSH password authentication
4) Optionally, add SSH-Keys for public key authentication

3. Open a terminal emulator (PuTTY or MobaXterm recommended) on the Windows computer;
4. Launch an SSH session on the terminal emulator;

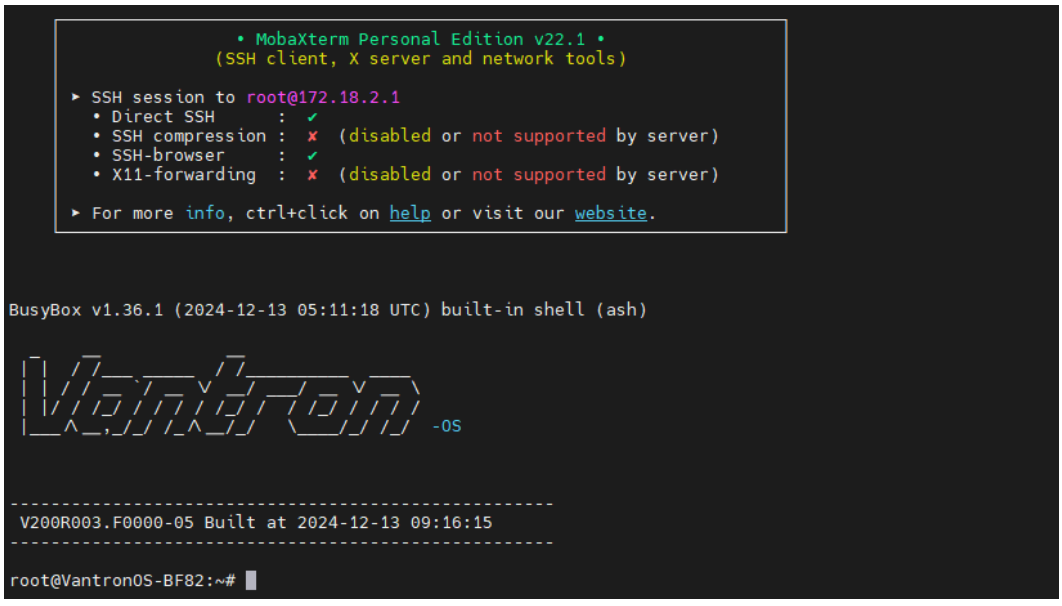
5. Input the IP address of the device (WAN port IP or 2.4GHz WLAN IP depending on the device connectivity and previous configuration), specify the username as “root”, and leave the port number as the default port 22 (unless you’ve configured a different port);



6. Click **OK** to start the session;

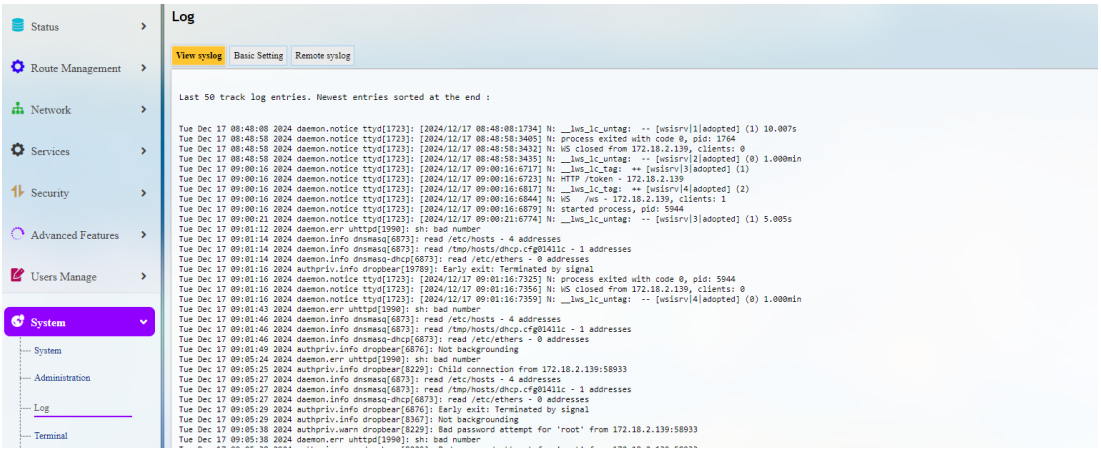
7. Input the password (rootpassword) to log in.

Example SSH login with the 2.4GHz WLAN IP of HAP101:

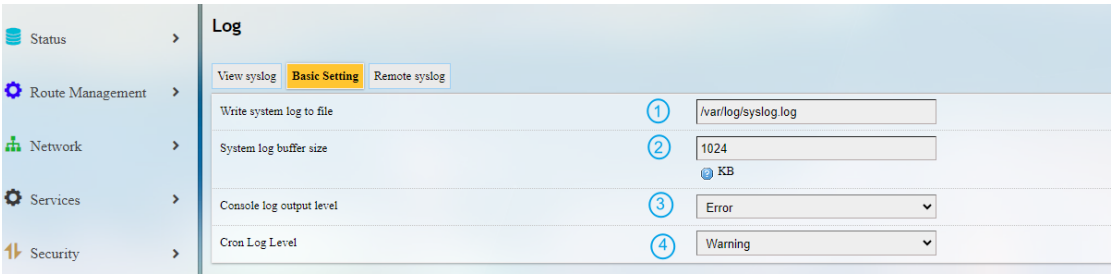


3.10.3 Log

The **Log** feature allows you to view the system logs under the **View syslog** tab. The last 50 entries are displayed on the page with the latest on the top.



For the log-related settings, click the **Basic Setting** tab.

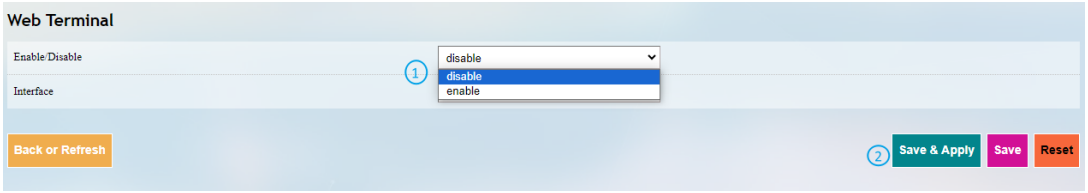


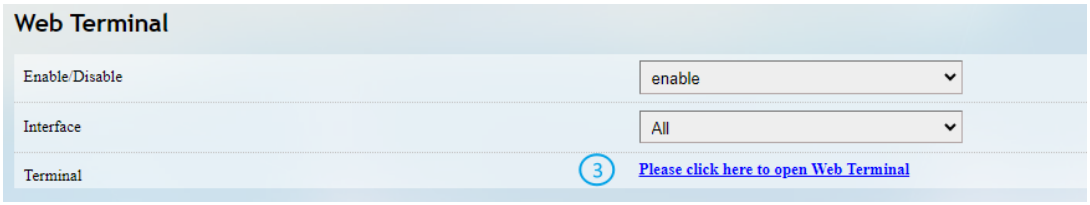
Description of the numbered areas

1. Storage path of the system log
2. Buffer size allowed for storing the system log
3. Output level of the console log
4. Output level of the cron log

3.10.4 Terminal

When navigating to **System > Terminal**, users can **enable** the Web terminal for logging into the shell of the device.





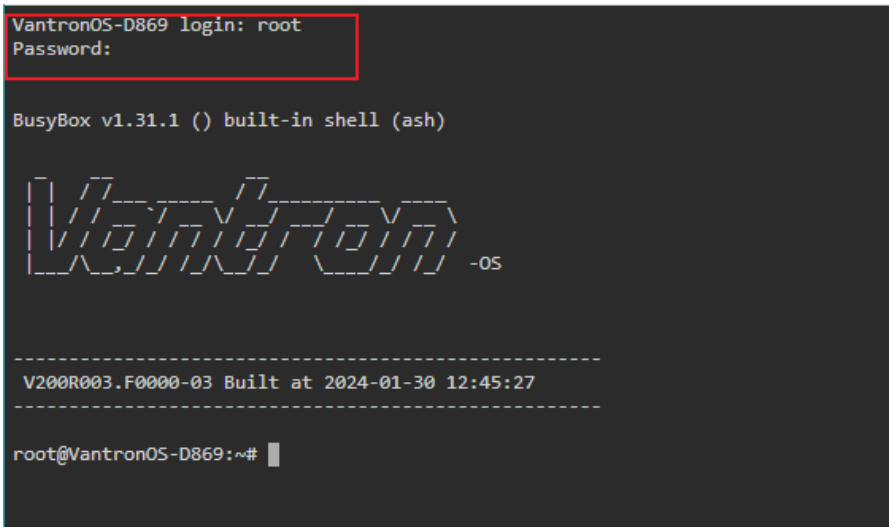
Step 1: Select **enable** from the drop-down list;

Step 2: Save the change;

Step 3: Click the link to open the web terminal.

Login account: root

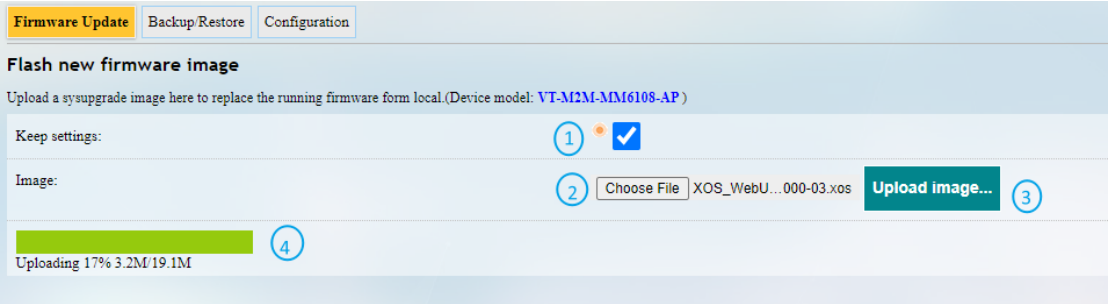
Login password: rootpassword (invisible while typing)



3.10.5 Backup/Flash Firmware

The Backup/Flash Firmware menu allows users to update the firmware, backup/restore user settings, and restore factory settings (clear user settings).

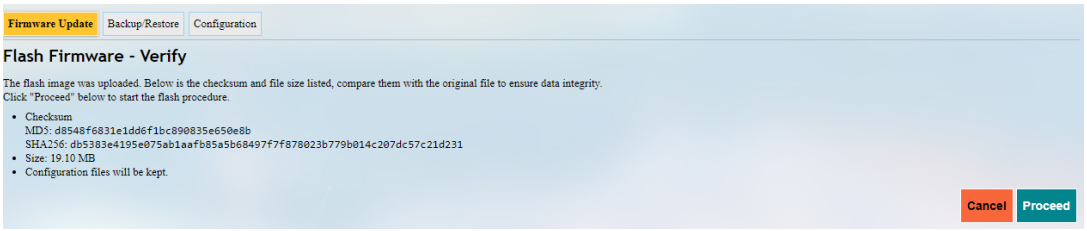
Firmware Update



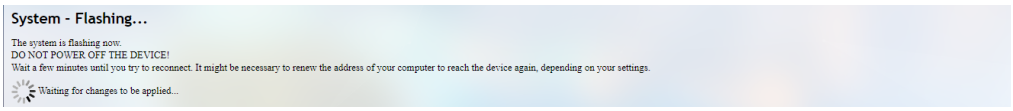
Description of the numbered areas

1. Check the box to keep the user settings while upgrading the device
2. Select the new firmware from the local directory
3. Click the button to upload the firmware
4. Upload progress of the package

When the detailed information of the firmware is displayed, check if the firmware is correct, then click **Proceed** to start the upgrading.

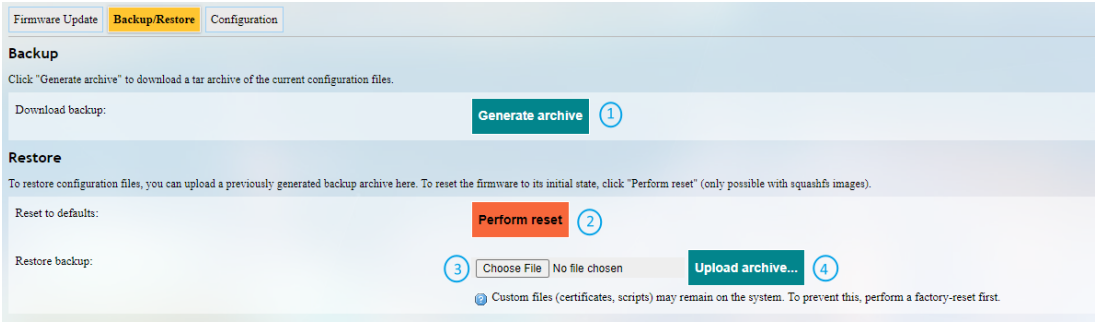


It will take some time for the upgrade and DO NOT power off the device when the upgrade is in process.



While the web portal may not show the completion of the firmware upgrade, you can monitor the LED indicators to track its progress. Once the upgrade is complete, the following indicators will turn solid green: the Wi-Fi HaLow indicator, the 2.4GHz Wi-Fi indicator, the power indicator, and the system indicator.

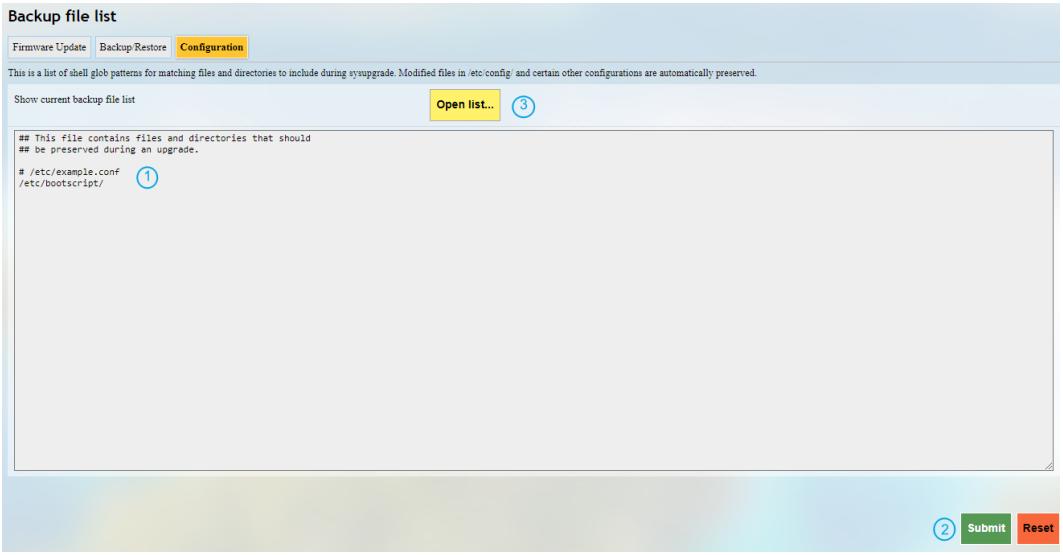
Under the **Backup/Restore** tab, you can back up your settings and download the package, including the configuration files and pre-set folders. Additionally, you can restore the device to its factory settings or upload a previously saved backup package.



Description of the numbered areas

1. Click the button to back up the system configurations (including only the configuration files and preset files other than user files or programs)
2. Factory reset the device (user configurations will be cleared)
3. Select a backup package from the local directory
4. Upload the backup package to restore the settings

Under the **Configuration** tab, you can customize the configuration files or directories to be retained during the upgrade.



Description of the numbered areas

1. Input the configuration file or directory to be retained during the upgrade
2. Click **Submit** to confirm the setting
3. Open the list of configuration files kept during the upgrade

3.10.6 Reboot

Make sure you don’t have any ongoing process before rebooting the device.

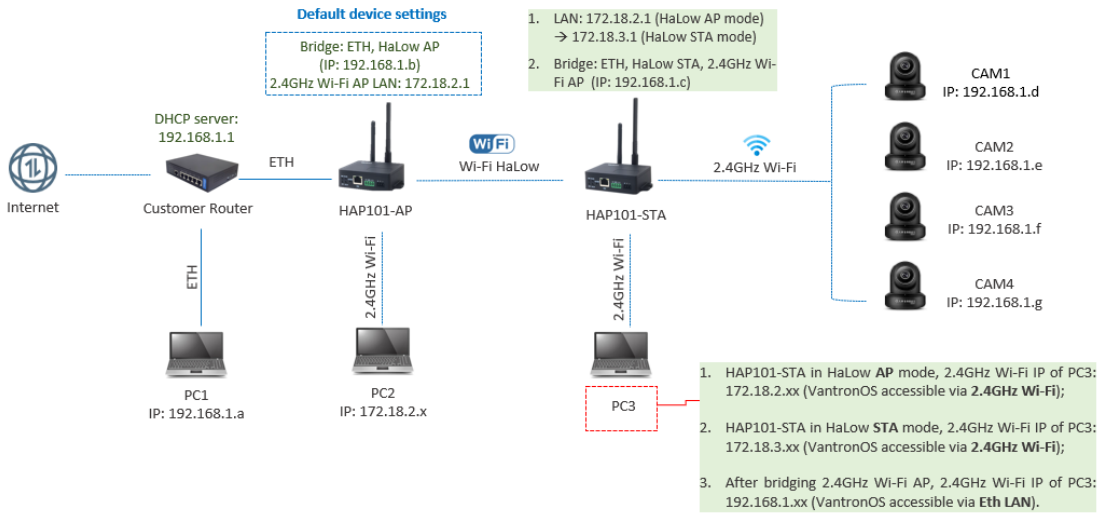
3.11 Logout

You will exit the web interface with a click on the **Logout** tab. If you need make changes to any of your settings, you can log in the web again with default account (root) and password (rootpassword). Make sure you have saved the changes before logout.

CHAPTER 4 USE CASE

4.1 Application Topology

A typical use case for HAP101 devices is to monitor the status of connected cameras. The following topology involves two HAP101 devices, one in AP mode and the other is later switched to the station mode.



- With the firmware upgraded to **V200R003.F0000-0B** or later:
  1. Each HAP101 device operates in HaLow AP and 2.4GHz Wi-Fi AP modes, with default LAN IP set to 172.18.2.1;
  2. When an HAP101 switches from HaLow AP mode to HaLow STA mode, its LAN IP will change to 172.18.3.1;
  3. ETH and HaLow AP of each AP mode HAP101 are bridged, so that after an HAP101 connects to a DHCP server through an Ethernet cable, clients connected to it via Wi-Fi HaLow will obtain an IP from the DHCP server.
- In the above topology:
  1. **HAP101-AP is all set and requires no change**;
  2. HAP101-STA is switched from the default HaLow AP mode to the **HaLow station** mode to connect to HAP101-AP and obtain an IP from the DHCP server;
  3. HaLow station of HAP101-STA is bridged by default, allowing itself to obtain an IP from the DHCP server when connected to HAP101-AP via Wi-fi HaLow;
  4. The 2.4GHz Wi-Fi AP of HAP101-STA is later manually bridged. As a result, client devices connected to HAP101-STA via 2.4GHz Wi-Fi will receive an IP address from the DHCP server. However, they cannot communicate with HAP101-STA;

5. PC1 can manage all devices that obtain IP addresses from the DHCP server, while PC2 manages HAP101-AP. When PC3 connects to HAP101-STA via 2.4GHz Wi-Fi, it receives an IP address from the DHCP server but cannot access HAP101-STA's VantronOS. However, if the Ethernet port of HAP101-STA is reconfigured from WAN to LAN, HAP101-STA's VantronOS becomes accessible via an Ethernet connection using the device's LAN IP address.

- After the setup, to view the IP of the cameras, you will need:

  1. Log in to HAP101-STA's VantronOS via an Ethernet connection using the device's LAN IP address;
  2. Check the IP address of the clients on the 2.4GHz Wi-Fi connection page.

4.2 Wiring

Power on HAP101-AP and connect it to a router (DHCP server) using an Ethernet cable. This connection allows HAP101-AP to obtain an IP from the DHCP server. To retrieve this IP (depending on your needs):

1. Connect a PC (PC2 in the topology) to the 2.4GHz Wi-Fi of HAP101-AP using the WLAN SSID and WLAN password on the device label of HAP101-AP;
2. Log in to VantronOS for HAP101-AP using the provided WLAN login IP and user information;

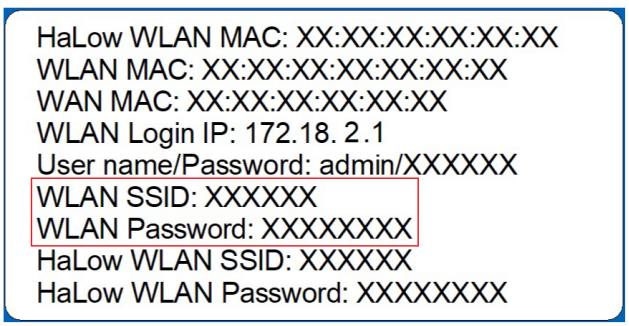
   Refer to steps 2 through 4 in 4.3.1 if you are not sure about steps 1 and 2.
3. Navigate to **Network > Interfaces > WAN** to check the IP information.

4.3 Setup of HAP101-STA

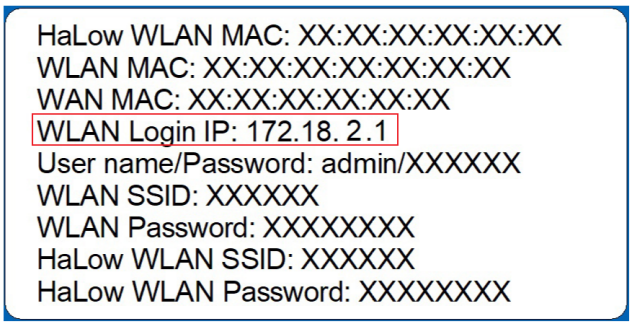
Follow the steps below to set up HAP101-STA and connect it to HAP101-AP.

4.3.1 HaLow

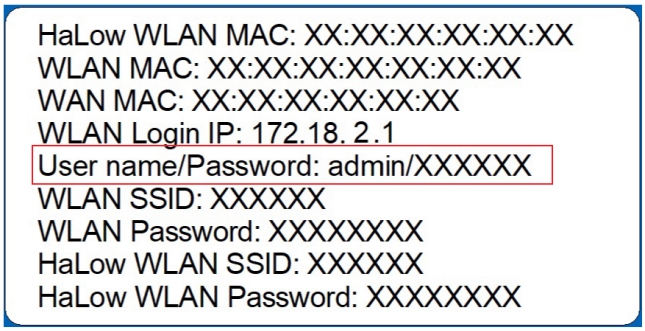
1. Power on HAP101-STA;
2. Connect the host computer to the 2.4GHz Wi-Fi of HAP101-STA using the default SSID and password provided on the device label as shown below;



3. Use the default **WLAN Login IP** provided on the device label of HAP101-STA as the address for VantronOS login;



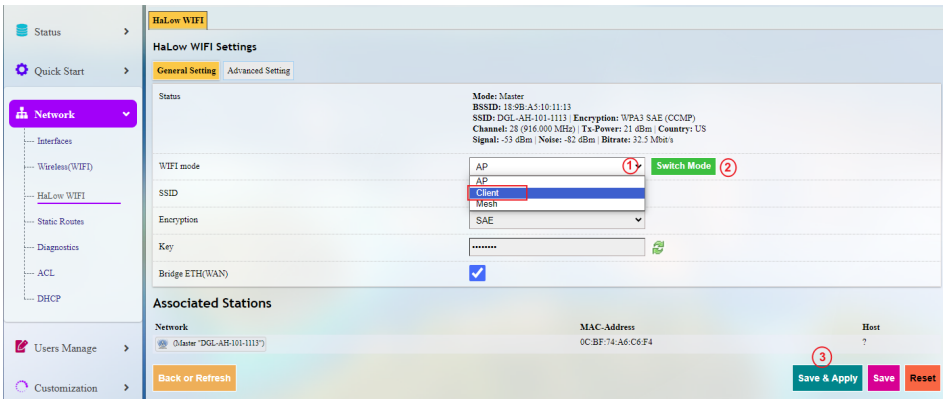
4. Log in to VantronOS using the username and password on the device label;



* *For higher permissions on VantronOS, log in as a superuser:*

Super user: root // password: rootpassword

5. Navigate to **Network > HaLow WIFI**, and change the HaLow mode of HAP101-STA to **Client**;

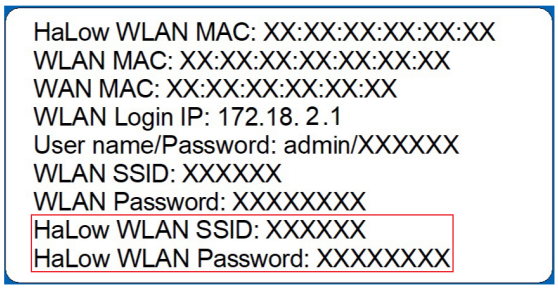


* *The LAN IP of the device will change to **172.18.3.1** when the HaLow mode switches to **Client**.*

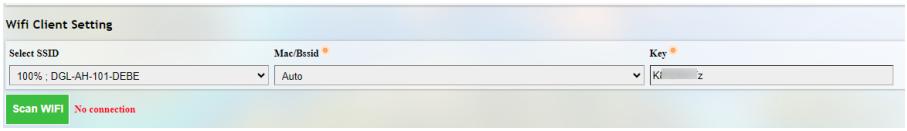
6. Save the settings and wait a few seconds to allow the change to apply;

7. Reconnect the host computer to the 2.4GHz Wi-Fi of HAP101-STA and log in to VantronOS using the new WLAN IP: **172.18.3.1**;

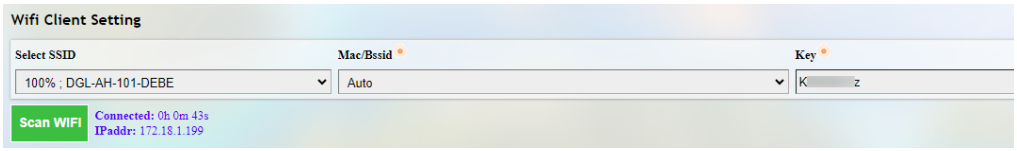
8. Check the device label of **HAP101-AP** for the HaLow WLAN SSID and password;



9. Navigate to **Network > HaLow WIFI** in HAP101-STA's VantronOS;
10. Under the **Wifi Client Setting** tab, select the SSID of HAP101-AP from the list and enter the password for HaLow connection;



11. If the target SSID is not included in the HaLow SSID list, click the **SCAN WIFI** button to refresh the list;
12. Save and apply the settings;
13. When HAP101-STA successfully connects to HAP101-AP via Wi-Fi HaLow, the connection status will be displayed next to the **SCAN WIFI** button.



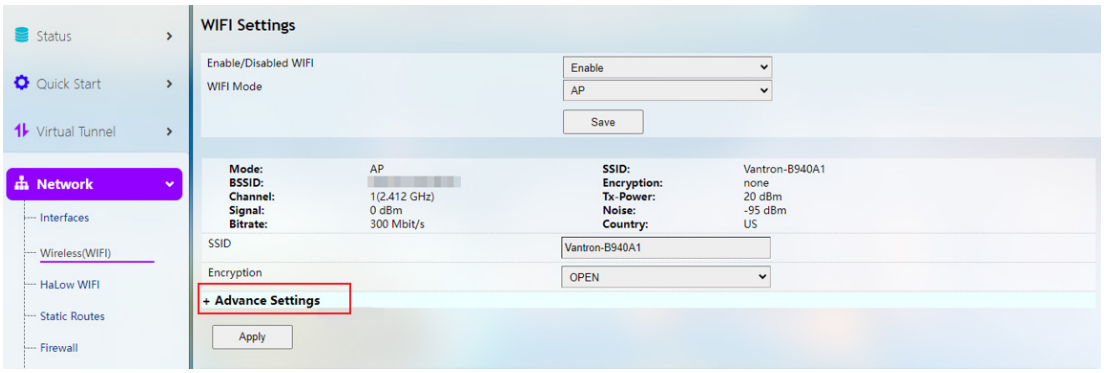
After these settings, HAP101-STA connects to HAP101-AP via Wi-Fi HaLow and obtains an IP from the DHCP server.

4.3.2 Reconfiguring WAN to LAN

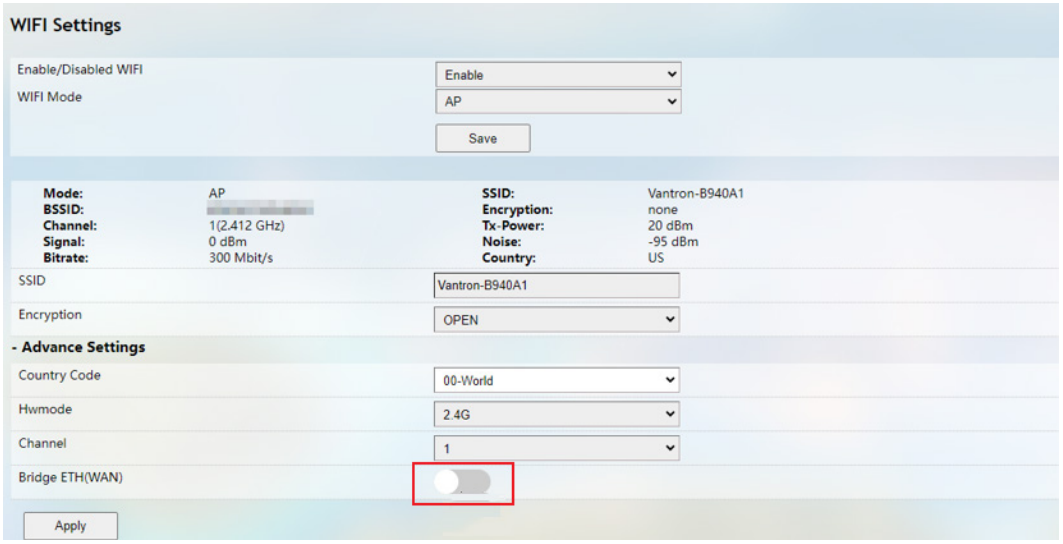
Follow the steps in section 2.7.1 part b for switching the Ethernet port from the default WAN mode to LAN mode. Once reconfigured, PC3 can connect to the device via Ethernet and access VantronOS using the device's LAN IP address: **172.18.3.1** (HaLow station mode)**.**

4.3.3 2.4GHz Wi-Fi

1. Navigate to **Network > Wireless (WIFI)**;
2. Click **Advance Settings** to expand the menu;



3. Toggle the button behind **Bridge ETH (WAN)** to bridge the 2.4GHz Wi-Fi to Ethernet.



This configuration bridges the 2.4GHz Wi-Fi AP, therefore devices connected to HAP101-STA via 2.4GHz Wi-Fi will obtain an IP from the DHCP server.

4.4 Viewing Camera IPs

Please refer to the camera's guide for connecting multiple cameras to HAP101-STA through 2.4GHz Wi-Fi. After finishing all settings, the cameras will obtain an IP from the DHCP server.

The following is a summary of the process for viewing the camera IPs in the given topology:

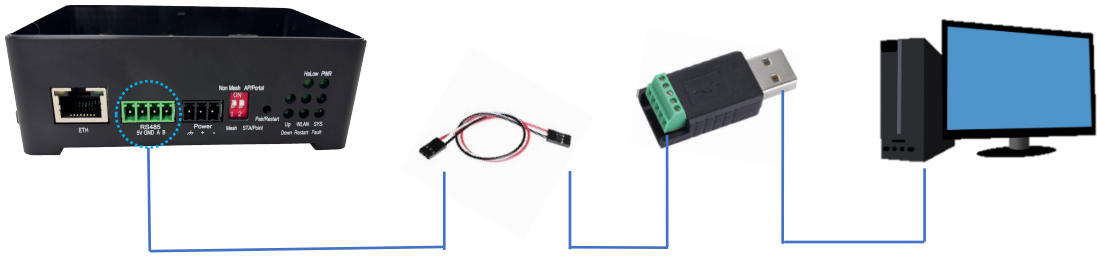
1. Connect HAP101-AP to the DHCP server via Ethernet;
2. Connect a PC (PC3 in the topology) to HAP101-STA via 2.4GHz Wi-Fi;
3. Log in to HAP101-STA's VantronOS using the WLAN IP (172.18.2.1 by default), and the provided username and password on the device label;
4. Switch the HaLow mode of HAP101-STA **from AP to Client** and reconnect PC3 to it for VantronOS login using the new WLAN IP (172.18.3.1);
5. Connect HAP101-STA to HAP101-AP and take down the HaLow station IP of HAP101-STA obtained from the DHCP server (next to the **Scan WIFI** button on the HaLow WIFI page);
6. Switch the Ethernet port of HAP101-STA from WAN mode to LAN mode, to allow local access of the device from Ethernet;
7. Bridge the 2.4GHz Wi-Fi of HAP101-STA and connect the cameras to HAP101-STA via 2.4GHz Wi-Fi;
8. Connect PC3 to HAP101-STA **via Ethernet** and access HAP101-STA's VantronOS using the LAN IP (172.18.3.1);
9. Navigate to **Network > Wireless (WIFI)** and check the details of the 2.4GHz Wi-Fi connection under the **Associated Stations** tag where the camera IPs are displayed.

CHAPTER 5 DEBUGGING THE DEVICE

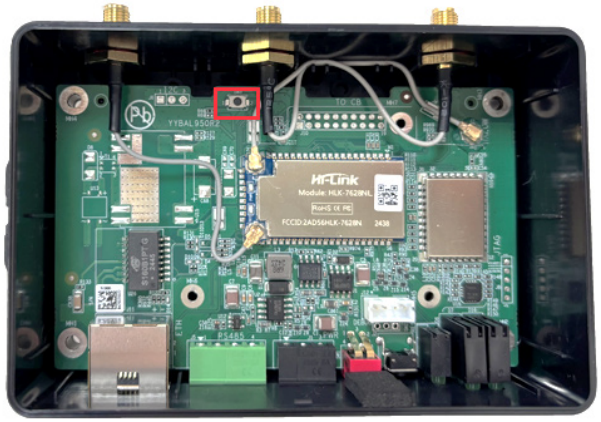
The serial port operates in the RS485 mode by default, and can be switched to debug mode for troubleshooting the device. It will automatically revert to standard RS485 operation upon each power cycle.

Follow the steps below to set up the device for the debugging purpose.

1. Unscrew the bottom screws of the device and remove the top cover;
2. Use an RS485 to USB adapter and DuPont wires (A-A, B-B, GND-GND) or other way to connect HAP101 to the host computer;

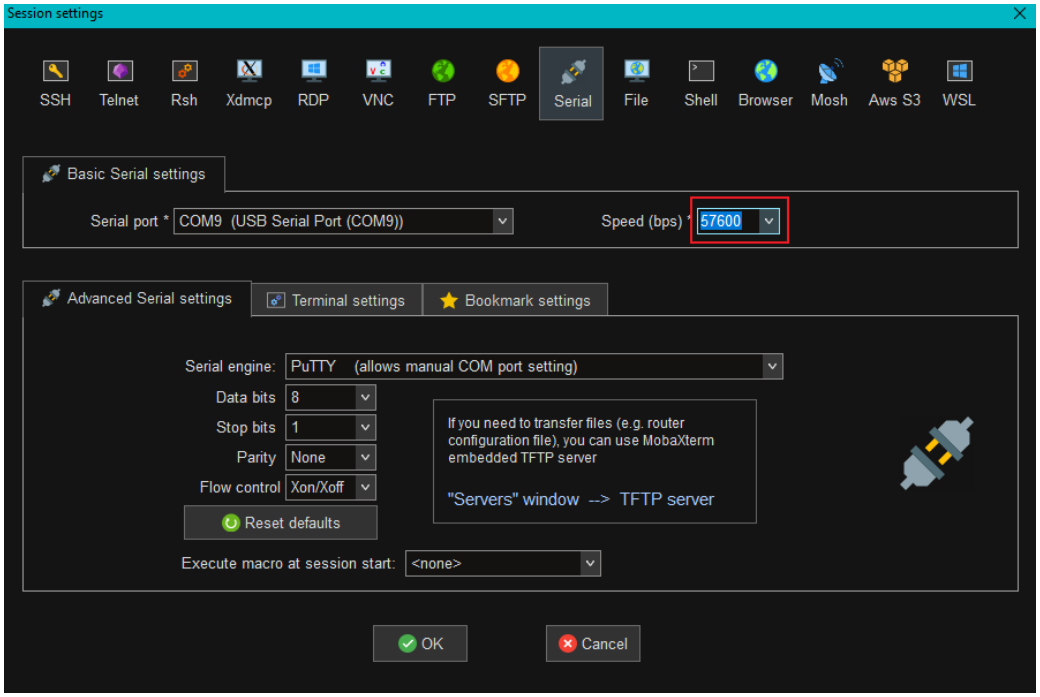


3. Press the **SW3** button inside the casing and do **NOT** release;

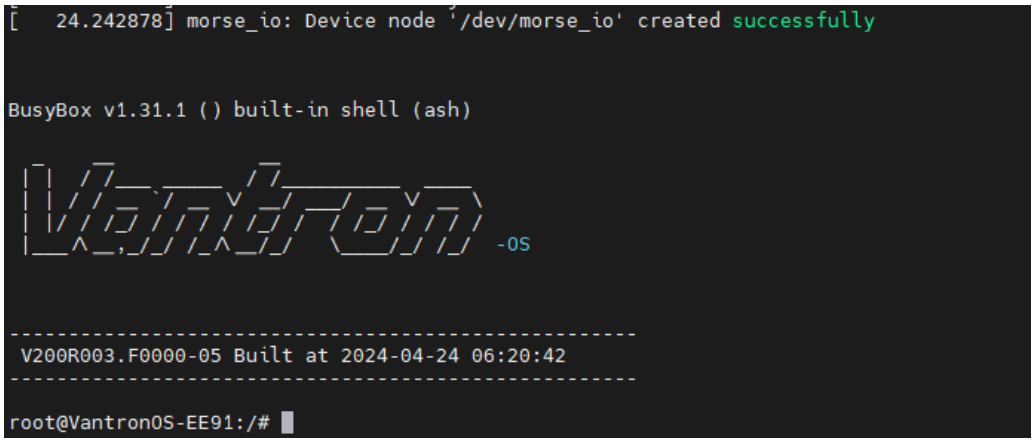


4. Power on HAP101 and release the SW3 button after 2 seconds;
5. Open a serial communication program and launch a serial session using the parameters below:

Baud rate	Data bit	Polarity	Stop bit
57600	8	None	1



6. Wait for the device information to be printed in the console;
7. When the message for successful device creation appears, press **Enter** and proceed with the debugging operations;



If the device is connected to a router or switch via the WAN port, you can determine the IP address by running the ifconfig command in the console.

CHAPTER 6 DISPOSAL AND PRODUCT WARRANTY

6.1 Disposal

When the device comes to end of life, you are suggested to properly dispose of the device for the sake of the environment and safety.

Before you dispose of the device, please back up your data and erase it from the device.

It is recommended that the device is disassembled prior to disposal in conformity with local regulations. Please ensure that the abandoned batteries are disposed of according to local regulations on waste disposal. Do not throw batteries into fire or put in common waste canister as they are explosive. Products or product packages labeled with the sign of “explosive” should not be disposed of like household waste but delivered to specialized electrical & electronic waste recycling/disposal center.

Proper disposal of this sort of waste helps avoid harm and adverse effect upon surroundings and people’s health. Please contact local organizations or recycling/disposal center for more recycling/disposal methods of related products.

6.2 Warranty

Product warranty

VANTRON warrants to its CUSTOMER that the Product manufactured by VANTRON, or its subcontractors will conform strictly to the mutually agreed specifications and be free from defects in workmanship and materials (except that which is furnished by the CUSTOMER) upon shipment from VANTRON. VANTRON's obligation under this warranty is limited to replacing or repairing at its option of the Product which shall, within **24 months** after shipment, effective from invoice date, be returned to VANTRON's factory with transportation fee paid by the CUSTOMER and which shall, after examination, be disclosed to VANTRON's reasonable satisfaction to be thus defective. VANTRON shall bear the transportation fee for the shipment of the Product to the CUSTOMER.

Out-of-Warranty Repair

VANTRON will furnish the repair services for the Product which are out-of-warranty at VANTRON's then-prevailing rates for such services. At customer's request, VANTRON will provide components to the CUSTOMER for non-warranty repair. VANTRON will provide this service as long as the components are available in the market; and the CUSTOMER is requested to place a purchase order up front. Parts repaired will have an extended warranty of 3 months.

Returned Products

Any Product found to be defective and covered under warranty pursuant to Clause above, shall be returned to VANTRON only upon the CUSTOMER's receipt of and with reference to a VANTRON supplied Returned Materials Authorization (RMA) number. VANTRON shall supply an RMA, when required within three (3) working days of request by the CUSTOMER. VANTRON shall submit a new invoice to the CUSTOMER upon shipping of the returned products to the CUSTOMER. Prior to the return of any products by the CUSTOMER due to rejection or warranty defect, the CUSTOMER shall afford VANTRON the opportunity to inspect such products at the CUSTOMER's location and no Product so inspected shall be returned to VANTRON unless the cause for the rejection or defect is determined to be the responsibility of VANTRON. VANTRON shall in turn provide the CUSTOMER turnaround shipment on defective Product within **fourteen (14) working days** upon its receipt at VANTRON. If such turnaround cannot be provided by VANTRON due to causes beyond the control of VANTRON, VANTRON shall document such instances and notify the CUSTOMER immediately.

Appendix Regulatory Compliance Statement

FCC Compliance Statement

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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Exposure to radio frequency energy:

The radiated output power of this device meets the limits of FCC radio frequency exposure limits. This device should be operated with a minimum separation distance of 20cm (8 inches) between the equipment and a person’s body.

NOTE: 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.

IC Statement

This device complies with ISED Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Exposure to radio frequency energy:

The radiated output power of this device meets the limits of ISED Canada radio frequency exposure limits. This device should be operated with a minimum separation distance of 20cm (8 inches) between the equipment and a person's body.

Le présent appareil est conforme aux CNR d'ISDE Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

La bande 5150–5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

L'exposition à l'énergie radiofréquence:

La puissance de sortie rayonné de cet appareil est conforme aux limites de la ISDE Canada limites d'exposition aux fréquences radio. Cet appareil doit être utilisé avec une distance minimale de séparation de 20cm entre (8 pouces) l'appareil et le corps d'une personne.