HAP101 Wi-Fi HaLow Access Point

User Manual

Version: 1.4

© Vantron Technology, Inc. All rights reserved.

Revision History:

No.	Software Version	Description	Date
V1.0	V200R003.F0000-02	First release	Jan. 10, 2024
V1.1	V200R003.F0000-02	Broke down the steps for web log	Jan. 25, 2024
V1.2	V200R003.F0000-03	Updated the steps in WIFI connection as per the firmware upgrade	Feb 2, 2024
V1.3	V200R003.F0000-04	Added a use case for connecting a camera to the network	Feb. 5, 2024
V1.4	V200R003.F0000-06	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

Table of Contents

Foreword....1
CHAPTER 1 HARDWARE DESCRIPTION....5
1.1 Product Overview....6
1.2 Unpackaging....7
1.3 Specifications....8
1.4 Definition of Interfaces....9
1.4.1 Front view....9
1.4.2 Back view....11
1.5 Serial Port Pinout....12
CHAPTER 2 GETTING STARTED....13
2.1 Setting up the Device....14
2.2 Web Login....15
2.2.1 Login via the 2.4GHz WLAN IP....16
2.2.2 Login via the VLAN IP....18
2.2.3 Login via the WAN Port IP....21
2.3 SSH Login....22
2.4 Wi-Fi HaLow Connection....23
2.4.1 AP mode....23
2.4.2 Station mode....25
2.5 Password Change....26
2.6 Language Change....26
2.7 Factory Reset the Device....27
2.7.1 Hardware reset....27
2.7.2 Software reset....27
CHAPTER 3 DEVICE SETUP IN VANTRONOS....28
3.1 Introduction to VantronOS....29
3.2 Status....30
3.3 Quick Start— Auto Routing....31
3.4 Virtual Tunnel....32
3.4.1 OpenVPN Server....32
3.4.2 VPN Client....34
3.5 User Management....35
3.6 Network....37
3.6.1 Interfaces....37
3.6.1.1 LAN....38
3.6.1.2 WAN....41
3.6.2 Wireless (WIFI)....46
3.6.2.1 Wi-Fi – AP Mode....46
3.6.2.2 Wi-Fi – Client Mode....47
3.6.3 Wi-Fi HaLow....48
3.6.4 Static Routes....48
3.6.5 Firewall....50
3.7 Diagnostics....53

3.8 VTShark 53
3.9 Customization 56
3.9.1 Custom Program 56
3.9.2 IPK Installer 57
3.9.3 Manufacturer Info Customization 58
3.9.4 UDMP Agent 59
3.10 Hardware 60
3.10.1 Ser2TCP 60
3.10.2 Ser2net Environment Setup and Verification 60
3.10.3 Protocol comparison 66
3.11 Services 67
3.12 System 67
3.12.1 System 67
3.12.2 Netlink Bandwidth Monitor (NBM) Setting 69
3.12.3 Administration 71
SSH Login 71
3.12.4 Terminal 73
3.12.5 Mount Points 74
3.12.6 Backup/Flash Firmware 76
3.12.7 Reboot 79
3.13 Logout 79
CHAPTER 4 USE CASE 80
4.1 Application Topology 81
4.2 Setup of H1 (HaLow AP mode) 82
4.3 Setup of H2 and H3 (HaLow STA mode) 87
4.4 Setup of the Cameras and Connection Testing 88
CHAPTER 5 DEBUGGING THE DEVICE 89
CHAPTER 6 DISPOSAL AND PRODUCT WARRANTY 91
6.1 Disposal 92
6.2 Warranty 93
Appendix Regulatory Compliance Statement 94

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.

Intended Users

This manual is intended for:

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

Copyright

Vantron Technology, Inc. ("Vantron") reserves all rights of this manual, including the right to change the content, form, product features, and specifications contained herein at any time without prior notice. An up-to-date version of this manual is available at www.vantrontech.com.

The trademarks in this manual, registered or not, are properties of their respective owners. Under no circumstances shall any part of this user manual be copied, reproduced, translated, or sold. This manual is not intended to be altered or used for other purposes unless otherwise permitted in writing by Vantron. Vantron reserves the right of all publicly released copies of this manual.

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
ℹ	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 HARDWARE DESCRIPTION

1.1 Product Overview

Vantron HAP101 Wi-Fi HaLow access point ("the AP") is designed in compliance with the prominent IEEE 802.11ah (Wi-Fi Haow) standard with IEEE 802.11 b/g/n (2.4GHz Wi-Fi) as an option. 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 (2.4GHz Wi-Fi) and 32.5 Mbps (Wi-Fi HaLow), respectively. By complying with the IEEE 802.11ah standard, HAP101 supports operation in the sub 1GHz license exempt RF bands to avoid the crowded 2.4GHz frequency band. It enables stable connection of over 8,000 clients when working at the AP mode, making it an ideal solution for replacing complex networking requirements in confined spaces.

HAP101 is designed for large-scale dense deployment of low-power stations to eliminate multiple access points in application scenarios such as smart home appliances, surveillance systems, industrial process control, logistics and asset management, portables and wearables, smart city facilities, etc.

1.2 Unpackaging

The Product 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
- 1 x 2.4GHz Wi-Fi antenna
- 1 x Wi-Fi HaLow antenna
- 1 x Qualified certificate

Optional accessories:

- 1 x 12V/1A power adapter
- 1 x Power cord
- 1 x DC power connector
- 1 x RS485 terminal connector

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

1.3 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	
		Antenna: 1T1R	
	Wi-Fi HaLow	Standard: IEE 802.11 ah	
		Frequency range	US: 903.5MHz~926.5MHz / Europe: 863MHz~868MHz
			Japan: 916.5MHz~927.5MHz / Korea: 917.5MHz~923.5MHz
			Singapore: 866MHz~869MHz & 920MHz~925MHz
		Channel bandwidth: 1/2/4/8 MHz	
		Data rate: up to 32.5 Mbps @8MHz or 15 Mbps @4MHz	
		Working mode: AP, STA configurable	
I/O	Fast Ethernet	1 x RJ45, 10/100 Mbps	
	Serial port (Optional)	1 x RS485 (4-pin terminal, 5V output, baud rate: 115200)	
	Antenna	1 x Wi-Fi HaLow antenna	
		1 x 2.4GHz Wi-Fi antenna	
System Control	LED indicators	1 x Power indicator	1 x WLAN activity indicator
		1 x Wi-Fi HaLow activity indicator	1 x Error indicator
	Button	1 x Restore button	
Mechanical	Dimensions	110mm x 73mm x 28mm (with wall mount)	
	Casing material	Plastics (UL94, SP6 compliant)	
	Installation	Wall mounting	
	Heat dissipation	Fanless	
Power	Input	9V ~ 40V DC	
	Port	3-pin terminal (Over-current protection, reverse polarity protection)	
Software	Operating system	VantronOS	
	VPN	OpenVPN, IPSec	
	Device management platform	Vantron BlueSphere GWM	
	Upgrade	Local upgrade, OTA upgrade	
Security	2.4GHz Wi-Fi	64/128-bit WEP, TKIP, WPA, WPA2, AES, WPS	
	Wi-Fi HaLow	WPA3	
Environment Condition	Temperature	Operating: -20℃ ~ +60℃	Storage: -40℃ ~ +85℃
	Humidity	≤ 95% RH (non-condensing)	
	Certificate	FCC, IC	

1.4 Definition of Interfaces

1.4.1 Front view

Indicator/ Interface	Description		
1	LED indicators (Refer to the details below)	1 x Power indicator	
		1 x WLAN indicator	
		1 x Error indicator	
		1 x Wi-Fi HaLow indicator	
2	Pinhole restore button	Short press (0~2 seconds)	Restart the device
		Press for 3~5 seconds	Factory reset the device
		Press for 6~9 seconds	Factory reset the device, with user data cleared
3	WAN port (100Mbps), operating in the WAN area by default		
4	RS485 (baud rate: 115200)		
5	Power terminal (9V~40V DC)		
6	Mounting brackets (screws recommended: M3 x 8mm)		

Description of the LED indicators

1. Power indicator

   When the device is powered on, the power indicator will turn solid green.

2. WLAN indicator

2.4GHz Wi-Fi status	Description
The Wi-Fi module is turned on	The indicator turns solid green
There is Wi-Fi connectivity	The indicator blinks
The Wi-Fi module is turned off	The indicator is off

3. Error indicator

   The error indicator blinks when there is an error.

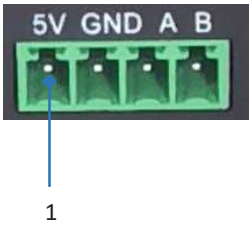
4. Wi-Fi HaLow indicator

Wi-Fi HaLow status	Description
The Wi-Fi HaLow module is turned on	The indicator turns solid green
There is Wi-Fi HaLow connectivity	The indicator blinks
The Wi-Fi HaLow module is turned off	The indicator is off

1.4.2 Back view

Interface	Description
1	Secondary 2.4GHz Wi-Fi antenna connector
2	Wi-Fi HaLow antenna connector
3	Primary 2.4GHz Wi-Fi antenna connector (if only one 2.4GHz Wi-Fi antenna is shipped, connect it to this connector for better signal strength)
4	Mounting brackets (screws recommended: M3 x 8mm)

1.5 Serial Port Pinout



HAP101 optionally includes an RS485 connector for serial communication. The pinout description is as follows:

No.	Signal	Device name	Port	Type	Description
1	VCC	/dev/ttyS1	COM1	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/ttyS1 -s 115200
```

CHAPTER 2 GETTING STARTED

2.1 Setting up the Device

Before you proceed with configuration of HAP101 access point, follow the steps below to finish the hardware connection.

1. Place the device on a flat surface;
2. Mark the drilling positions on the surface through the screw holes on the mounting brackets;
3. Drill two holes on the marked positions for two M3 x 8mm screws (drill bit: 2.5mm for 0.5mm thread pitch, hole depth: ~8mm);
4. Use two M3 x 8mm screws to fix the device (screw anchors might be necessary);
5. Tighten the screws to fix the device;
6. Install the flat antennas to the WLAN antenna connectors;

   If there is only one WLAN antenna, install it to the connector silk screened as ANT. WLAN1.

7. Install the longer antenna with a slim round tip to the Wi-Fi HaLow antenna connector;
8. Connect the device to a 12V DC power source to start the device.

2.2 Web Login

HAP101 is designed to allow network connectivity with minimal configuration. That being said, you can configure the network settings and customize the device in VantronOS web on a host computer.

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

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

It is important to note that when logging in to VantronOS for HAP101, 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.

Since the Ethernet jack of HAP101 operates in the WAN area by default, the WAN port IP address of the device cannot be determined without removing the upper cover to debug the device using the debug UART located therein.

Therefore, to save the trouble of removing the upper cover involved in option 3, you are advised to identify the 2.4GHz WLAN IP of the device or the VLAN IP of the device for VantronOS login initially, and then proceed with determining the WAN port IP address for later use.

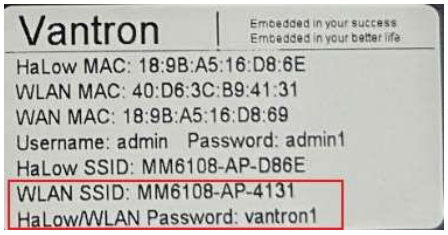
2.2.1 Login via the 2.4GHz WLAN IP

Prerequisites:

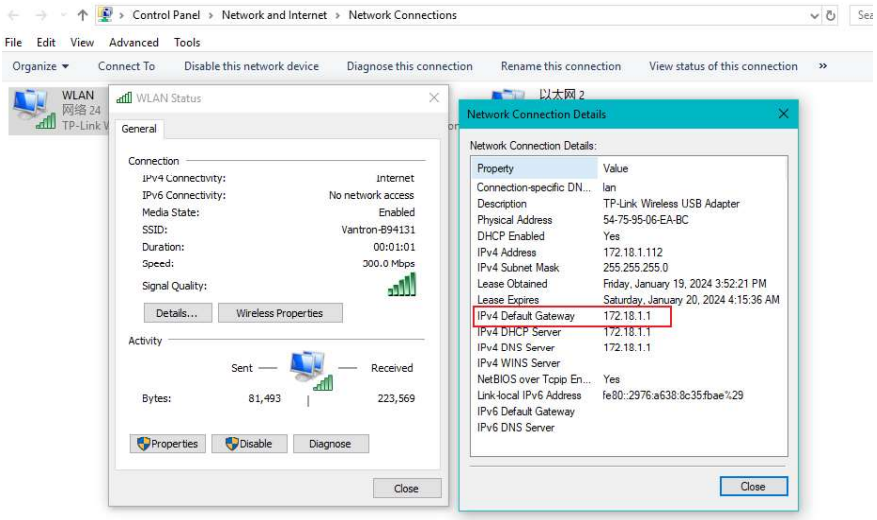
- HAP101 in operating in 2.4GHz Wi-Fi AP mode
- The host computer is connected to HAP101 via the 2.4GHz Wi-Fi

Steps:

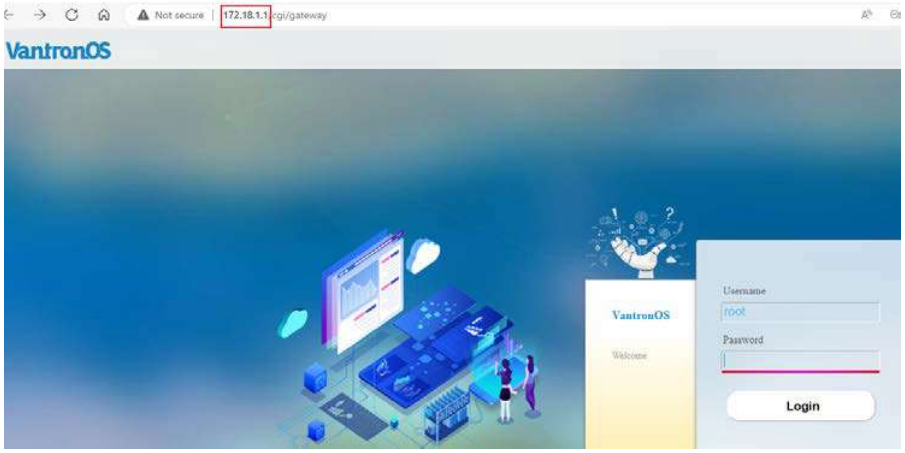
1. Power on the device and the 2.4GHz Wi-Fi will be operating in the AP mode by default;
2. Connect the host computer to the 2.4GHz Wi-Fi of the device using the SSID and default password provided on the device label (like the following)*;*



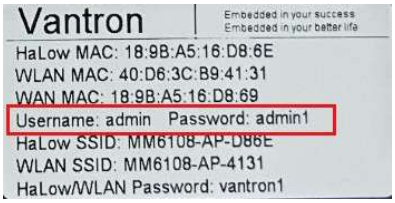
3. Check the details of the wireless connection on the host computer and identify the gateway IP of the 2.4GHz Wi-Fi;



4. Use the gateway IP of the 2.4GHz Wi-Fi identified in the prior step as the address for VantronOS login;



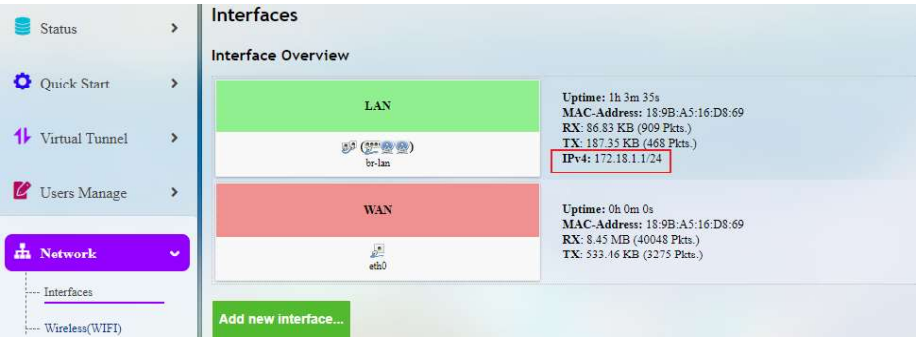
5. The login account and password are provided on the device label;



In case you need higher permission on VantronOS, you can log in as the super user.

Super user: root // password: rootpassword

6. Navigate to **Network > Interfaces** to check the interface information of HAP101 (the 2.4GHz Wi-Fi is bridged on the virtual LAN port that provides DHCP service to connected devices).



2.2.2 Login via the VLAN IP

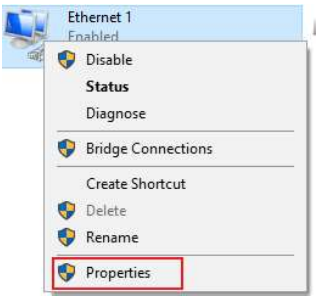
Prerequisites:

- The host computer and HAP101 are connected to the same Ethernet network
- The host computer supports VLAN settings

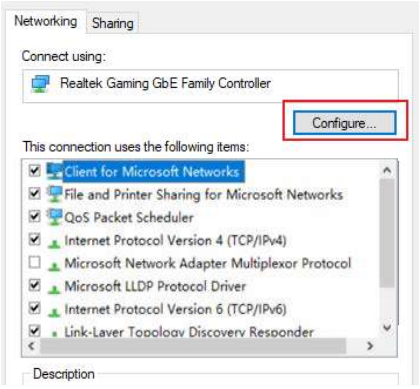
Steps:

Actual settings may vary slightly from the screenshots below.

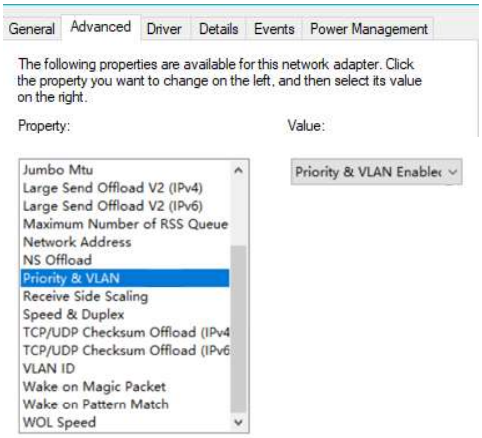
1. Connect both HAP101 and the host computer to the same router/switch for Internet access;
2. Open the **Network & Internet Settings** on the host computer;
3. Right click the network adapter and select **Properties**;



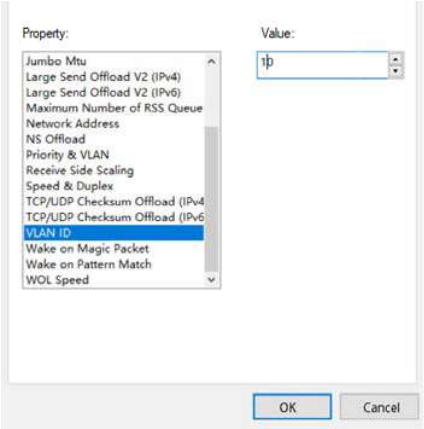
4. Click the **Configure** button in the middle, then click the **Advanced** tab;



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

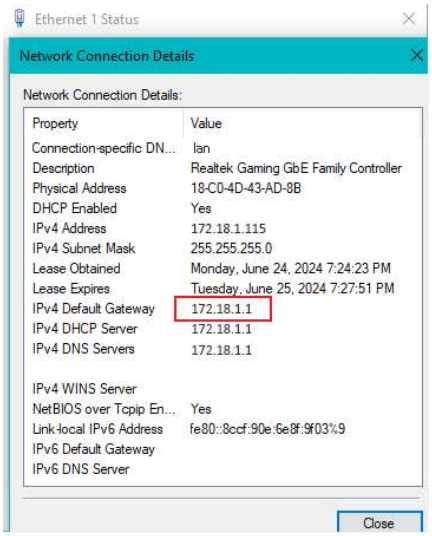


6. Move down to the **VLAN ID** attribute and input '10', then click **OK** to confirm the settings;

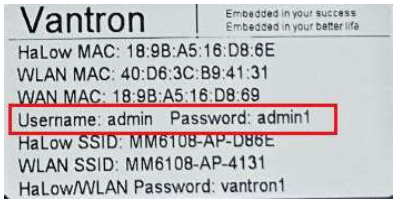


7. Wait a moment and check the network adapter settings;

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



9. The login account and password are provided on the device label.

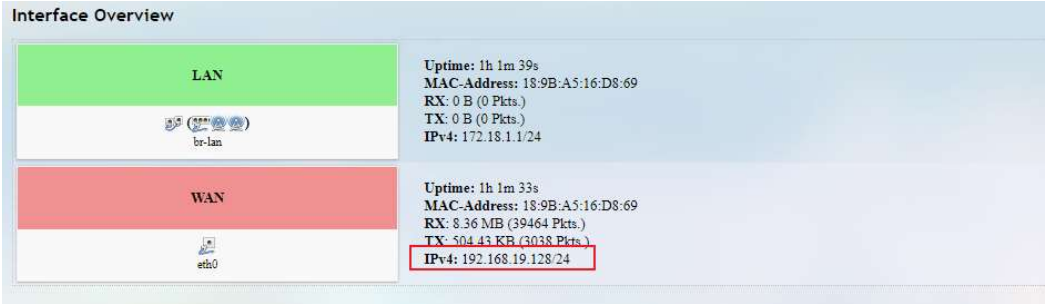


In case you need higher permission on VantronOS, you can log in as the super user.

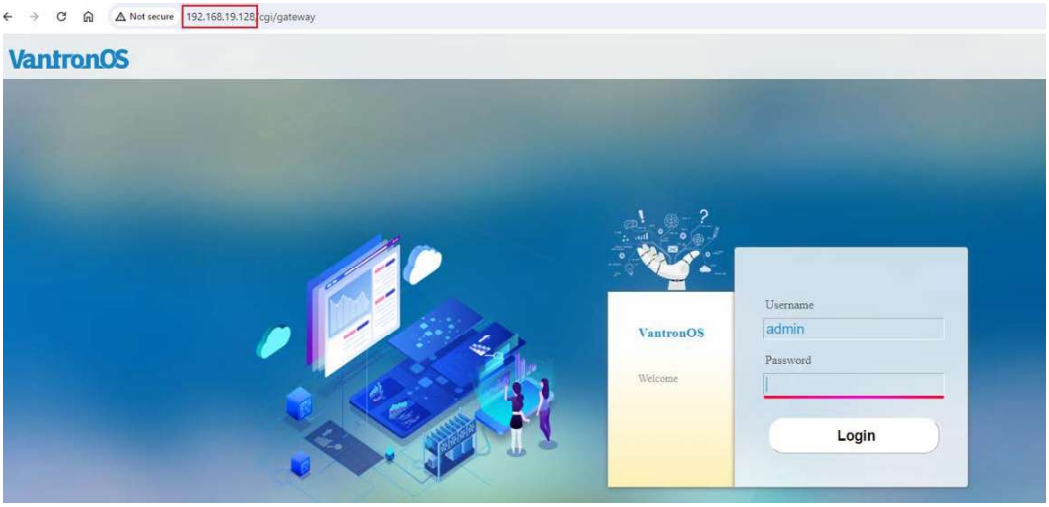
Super user: root // password: rootpassword

2.2.3 Login via the WAN Port IP

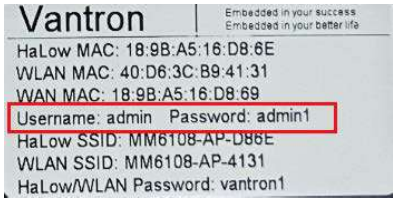
1. Connect the host computer to a router/switch for Internet access;
2. Connect HAP101 to the same router/switch using an Ethernet cable;
3. Connect the host computer to the 2.4GHz Wi-Fi of HAP101 using the SSID and default password provided on the device label;
4. Log in to VantronOS via the steps set out in 2.2.1 or 2.2.2;
5. Navigate to **Network > Interfaces** to identify the WAN port address of HAP101;



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



7. The login account and password are provided on the device label.



In case you need higher permission on VantronOS, you can log in as the super user.

Super user: root // password: rootpassword

2.3 SSH Login

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

Option 1— 2.4GHz Wi-Fi connection to HAP101: Use the 2.4GHz WLAN IP of the device as the login address.

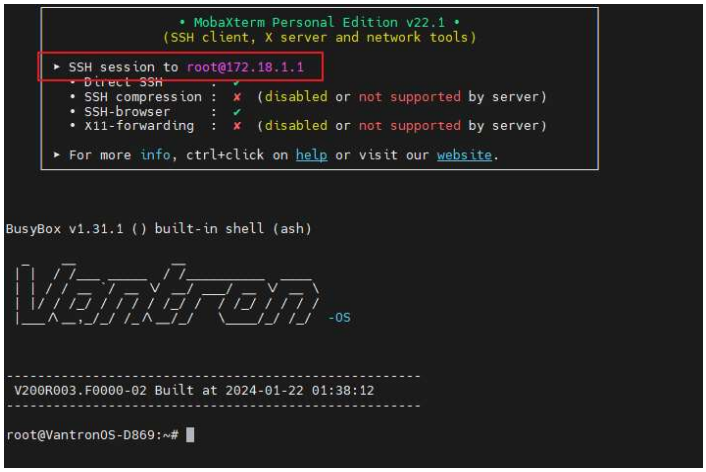
Option 2— Sharing the same Ethernet connection with HAP101: Use the WAN port IP of the device as the login address.

Make sure the IP address of the host computer is on the same network as HAP101. Refer to 2.2 for how to identify the 2.4GHz WLAN IP or WAN port IP of the device.

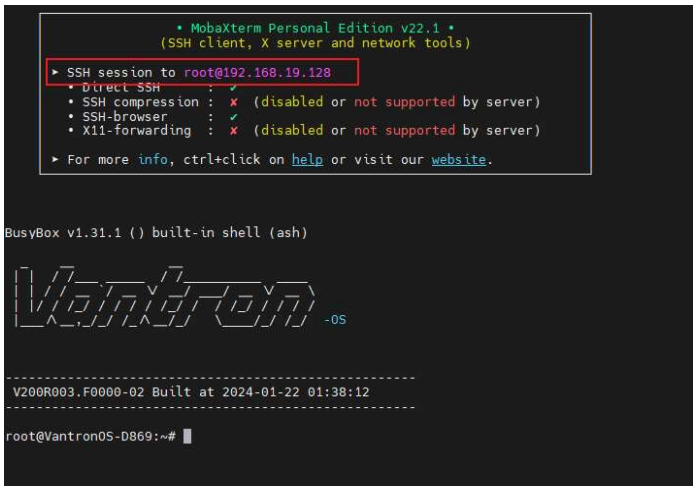
Use the following information for the login. Refer to 3.12.3 for the specific login steps.

Port	Account	Password
22	root	rootpassword

SSH login with the 2.4GHz WLAN IP of HAP101:



SSH login with the WAN port IP of HAP101:



2.4 Wi-Fi HaLow Connection

Wi-Fi HaLow related settings of the device are modified and saved via the **HaLow WIFI** menu in VantronOS**.** Therefore, please select either option provided in 2.2 to log in to VantronOS before you proceed.

2.4.1 AP mode

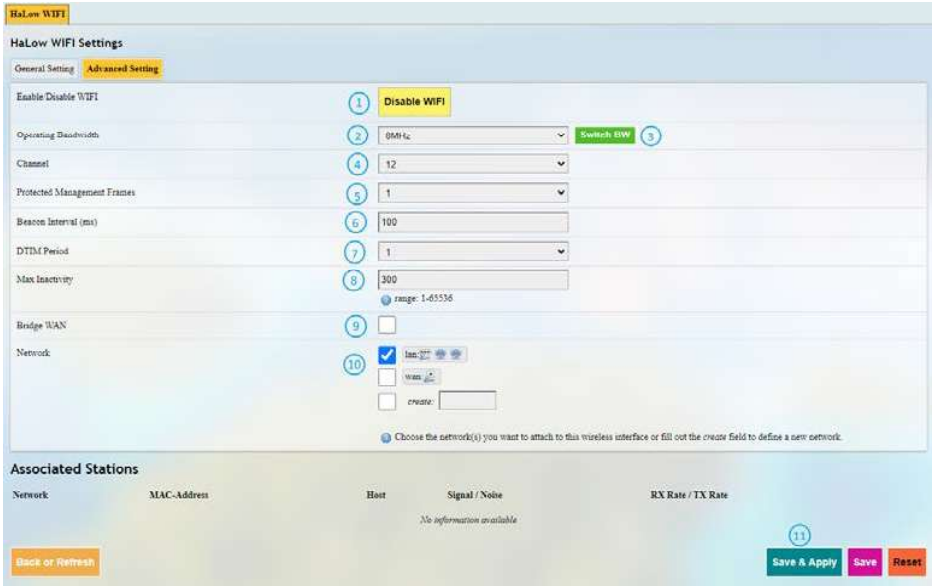
The device is operating in the AP mode by default. To allow other HaLow stations to connect to the device, please follow the steps below:

1. Navigate to **Network > HaLow WIFI;**
2. Check the general settings of the device as a HaLow access point, and modify the configurations as necessary;

Description of the numbered areas

1) Status of the connectivity
2) Select AP as the Wi-Fi HaLow mode and click **Switch Mode** to confirm if necessary
3) Modify the SSID of the device if necessary
4) Select an encryption protocol
5) Set a password for the Wi-Fi HaLow connection
6) Save and apply the settings

3. Modify the advanced settings as necessary;



Description of the numbered areas

1) Disable/Enable Wi-Fi HaLow

2) Select a bandwidth from 1, 2, 4, and 8

3) Click the button to confirm the change if necessary

4) Select a channel from 12, 28, and 44

5) Select a protected management frame

6) Input the beacon interval

7) Select a DTM period

8) Set a maximum inactivity period (between 1 and 65536)

9) Select to bridge the interface to WAN or not

10) Select an interface to bridge

11) Save and apply the settings

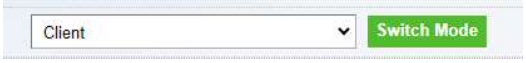
You can keep the default values if not sure.

4. Keep the corresponding settings of the HaLow stations in line with the AP-mode HAP101 for HaLow connection, then check the connection status in VantronOS (**Network > HaLow WIFI > Associated Stations**) for the AP-mode HAP101.

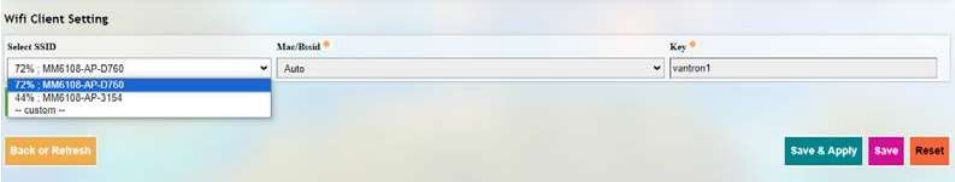
2.4.2 Station mode

The device also supports operation in station mode to connect to an existing HaLow access point. Follow the steps below to connect to an existing HaLow AP.

1. Navigate to **Network > HaLow WIFI;**
2. Under the **General Settings** tab, select the **Client** mode from the drop-down list and switch to this mode;



3. Wait a few seconds to allow the change to apply;
4. Select an IP address protocol between **DHCP** and **STATIC**;
5. Select the encryption protocol to match that of the target access point;
6. Select an SSID from the list and input the password for the access point;



7. If the target SSID is not included in the list, click the SCAN WIFI button to refresh the list, then input the password;

8. Save and apply the settings;
9. Wait a few seconds for successful connection.

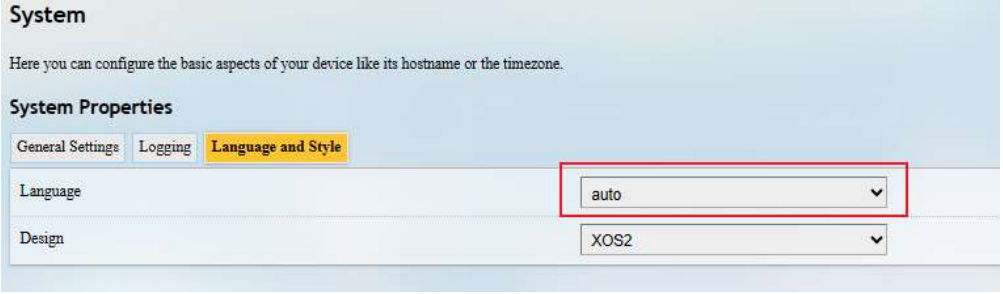
2.5 Password Change

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

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

2.6 Language Change

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



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

English: English interface

Simplified Chinese: Simplified Chinese interface

2.7 Factory Reset the Device

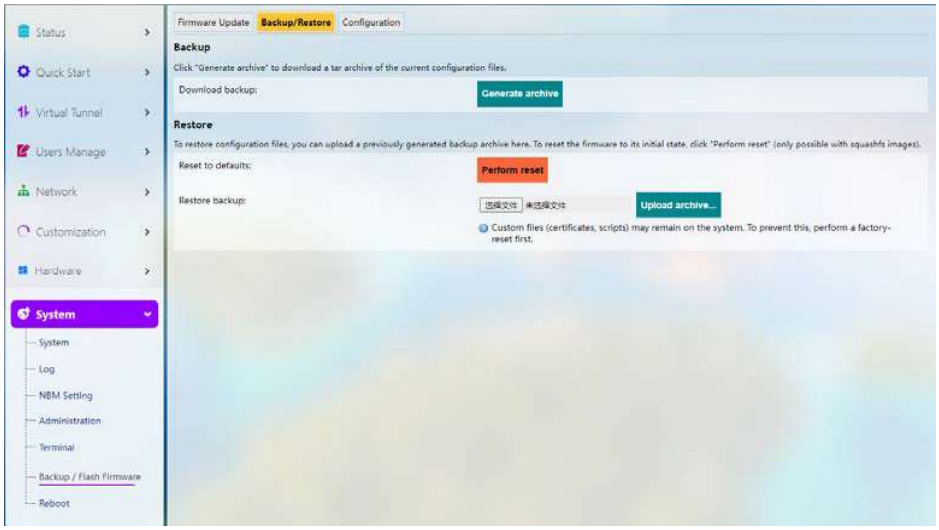
There are two options to factory reset the device, one from both the hardware perspective and the other from the software perspective. Once factory reset, the device will be restored to Wi-Fi HaLow AP mode and 2.4GHz Wi-Fi AP mode by default.

2.7.1 Hardware reset

Device Reset	Action	Description
Factory reset	Long press of the restore button for about 3s~ 5s	Clear customized device settings
Factory reset with user data cleared	Long press of the restore button for about 6s~ 9s	Clear user data saved in system files

2.7.2 Software reset

1. Login VantronOS through any of the methods set out in 2.2 depending on your network 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 3.12.6 about backing up the current configurations before device reset in VantronOS.

CHAPTER 3 DEVICE SETUP IN VANTRONOS

3.1 Introduction to VantronOS

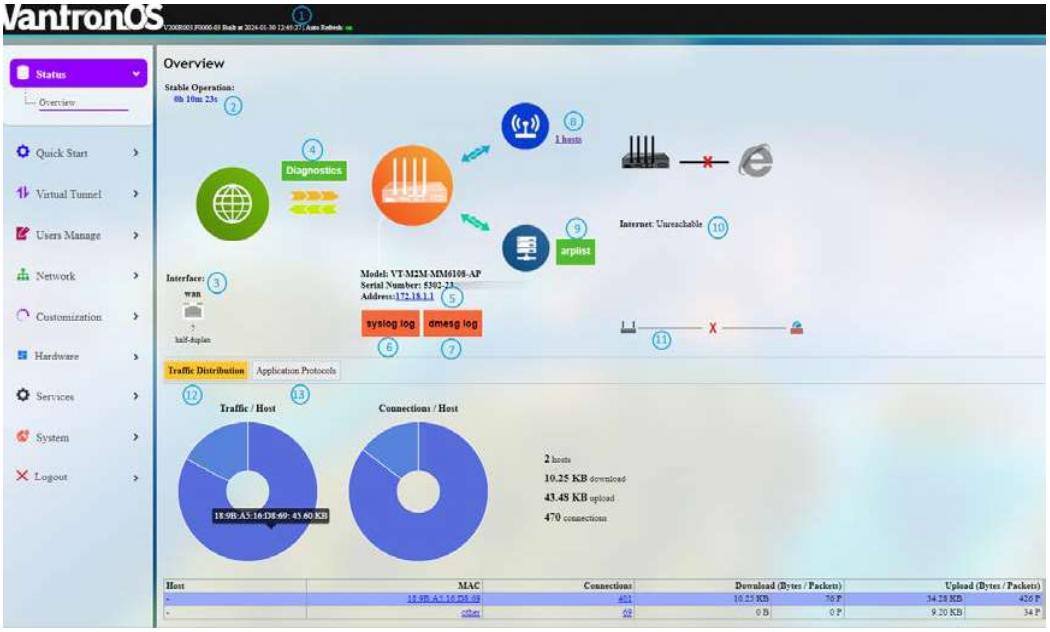
VantronOS is an intelligent operating system developed by the Vantron team, featuring independent system and function development. It is built upon the Linux system and optimized for embedded hardware. The operating system follows a modular design and plug-in expansion approach, utilizing the Linux kernel with a built-in firewall to ensure secure internet connectivity for Vantron IoT communication 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, make sure to save all settings and changes before exit to allow them to take effect.

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 (click to switch the mode)
2. Stable running duration of the device after establishing a network connection
3. Current working status of the Ethernet port
4. A collection of the network diagnostic tools (refer to 3.7 for details)
5. The 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 (N/A to the device)
10. Details of the network that the device is connected to
11. Default route 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 page bottom will get the detailed traffic information of the clients.

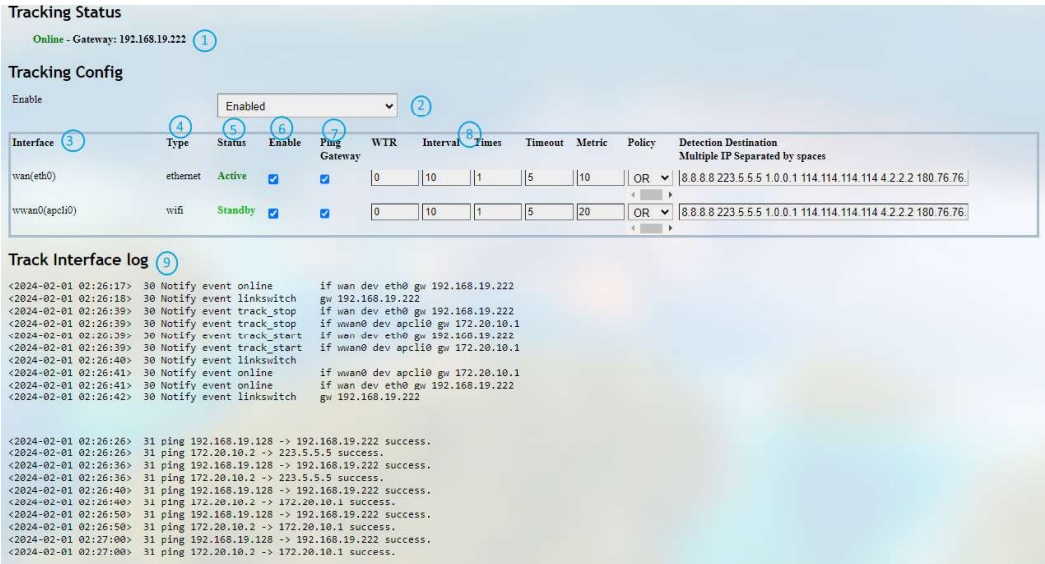
13. Traffic of application layer protocols

3.3 Quick Start— Auto 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 > Wi-Fi (STA) > Wi-Fi HaLow (STA) > others.

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



Description of the numbered areas

1. The interface information and 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. The settings for tracking the interface
9. The tacking log of the interfaces

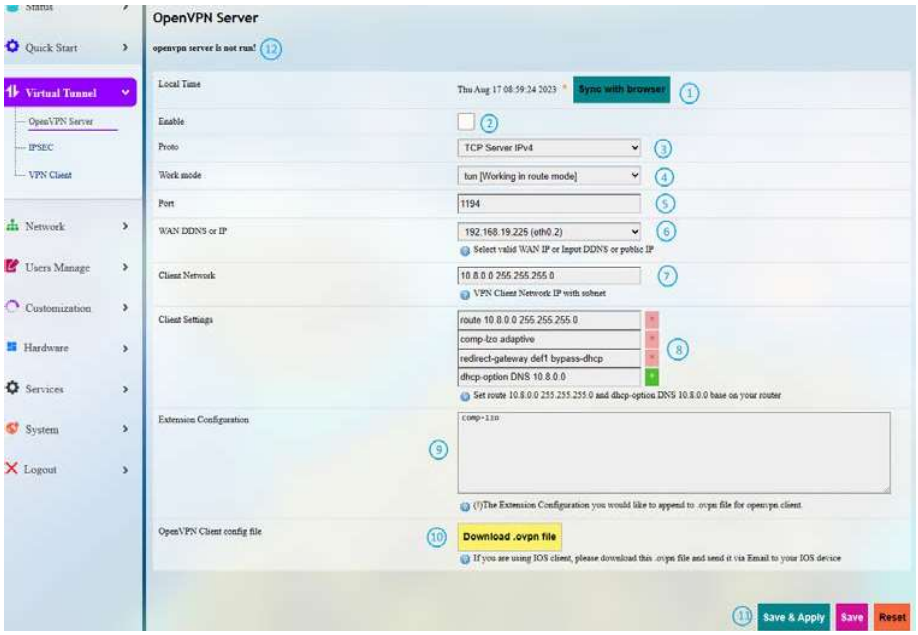
3.4 Virtual Tunnel

A virtual private network (VPN) lets you use the Internet to securely access your network remotely.

You can configure the AP either as an OpenVPN server or a VPN client based on needs.

3.4.1 OpenVPN Server

This page provides virtual private network based on SSL connection and transmission, which features simple and flexible configurations, better security, and no interference.



Follow the steps below to build an OpenVPN server:

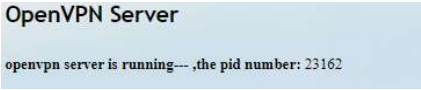
1. Synchronize the device time with the browser (local) time;
2. Enable the server or not after the server is built;
3. Select a protocol (TCP by default);

TCP provides an ordered delivery of data from the user to server (and vice versa), whereas UDP is not dedicated to end-to-end communications, nor does it check the readiness of the receiver.

4. Select a working mode between **tap** and **tun** (tun by default);

***Tap** bridges two ethernet segments at different locations, so use **tap** if you need to connect to remote network (remote desktops, PLCs, controllers, etc.). If you only need network connection, then use **tun**.*

5. Set a port that the server is to monitor;
6. Choose the WAN port IP or DDNS or public IP that the server is to monitor;
7. Assign a virtual IP network for the clients;
8. The basic configurations sent to the clients (not applicable to the tap working mode);
9. The extension configurations sent to the clients;
10. Download the configuration file for client connection (not necessary for server setup);
11. **Save & Apply** the settings;
12. Status of the OpenVPN server after the setup.



Advanced Setting allows you to set the authentication method, certificate authentication options, and renew the system certificate.

Run Log displays the details after the server is set up.

3.4.2 VPN Client

To connect HAP101 to a VPN server and use it as a client, navigate to **Virtual Tunnel > VPN Client** for specific settings.

Description of the numbered areas

1. Synchronize your VPN time with the browser (local) time
2. Select a WAN protocol for the virtual line (OPENVPN & PPTP available)
3. Click to switch to the protocol
4. Check or uncheck the box to enable/disable the protocol

Only when the protocol is enabled will subsequent options be displayed. The subsequent options correspond to the type of WAN protocol selected.

5. If you select OpenVPN as the WAN protocol, you'll have to continue with the configuration using a .ovpn file

If you select PPTP as the WAN protocol, you shall input the PPTP server IP, user name and password as indicated.

6. Select the .ovpn file from the local directory for configuration
7. Upload the file
8. Select to use a certificate or username & password for the authentication

The mode will update automatically, leave it as is.

9. Set the MTU
10. Set the gateway metric (between 1 and 255)

The smaller the number, the higher the priority.

11. Disable/Enable heartbeat detection

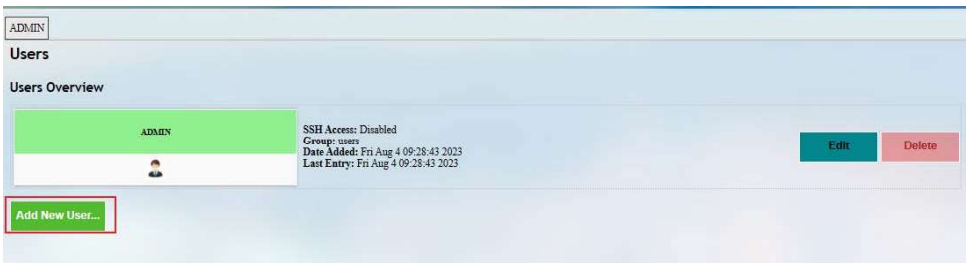
*Select **custom** and enter the IP address for heartbeat detection to enable the mechanism.*

12. Enter a custom DNS server
13. **Save & Apply** the settings
14. Status of the VPN client after the setup

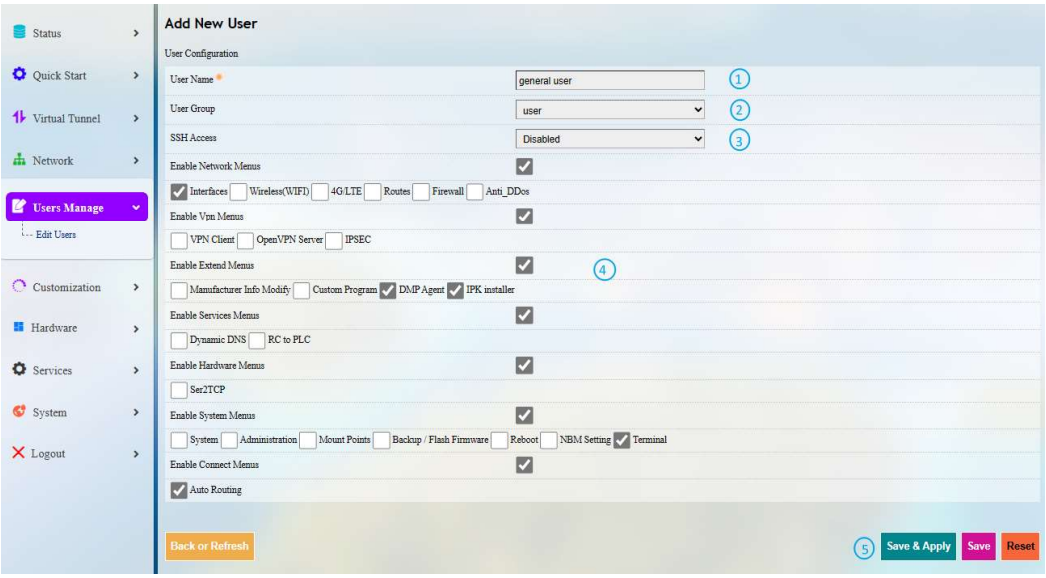
3.5 User Management

User management allows you to add new users or edit the existing users to assign different permissions to different roles.

To add a new user, click the button below the existing user information.



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



Description of the numbered areas

1. Input a username
2. Select a group for the new user
3. Enable SSH access or not for the new user
4. Expand the menus to enable specific functions for the new user
5. Save the settings before you exit

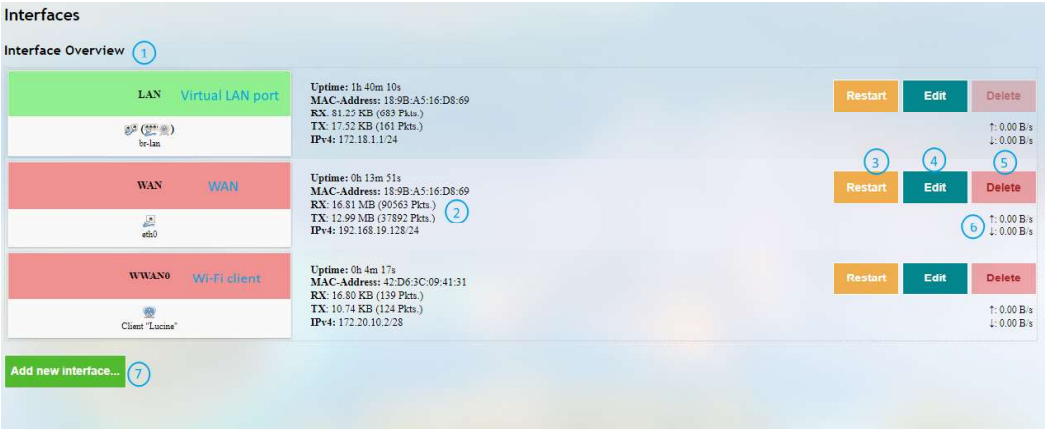
After creating the user, it will be added to the user list. The **Edit** and **Delete** buttons behind a user allow you to enable/disable certain features for this user or delete this user.

3.6 Network

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

3.6.1 Interfaces

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



Take the WAN port for example, the numbered areas are detailed as follows:

1. Interface overview
2. Interface traffic details
3. Restart the interface manually
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 as certain interfaces are related to your prior settings and the communication modules available on the device.

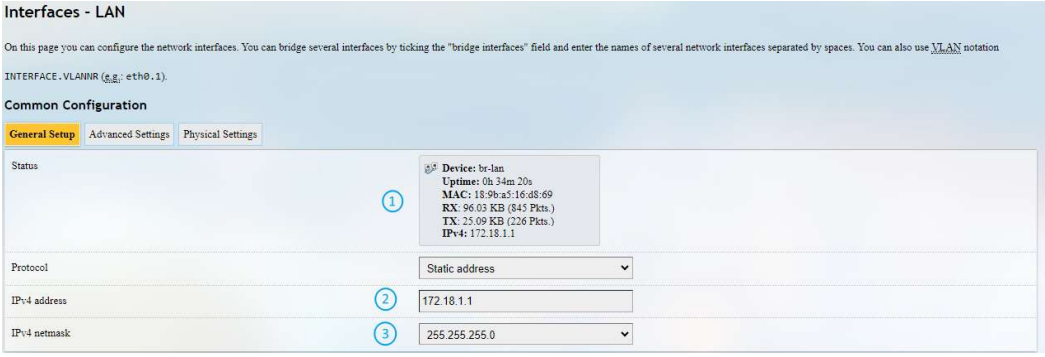
The following section illustrates on how to edit the network interfaces.

3.6.1.1 LAN

The bridged LAN port is for assigning IP addresses to clients connected to HAP101 via 2.4GHz Wi-Fi. You can modify the interface information as necessary.

- **Common Configurations**

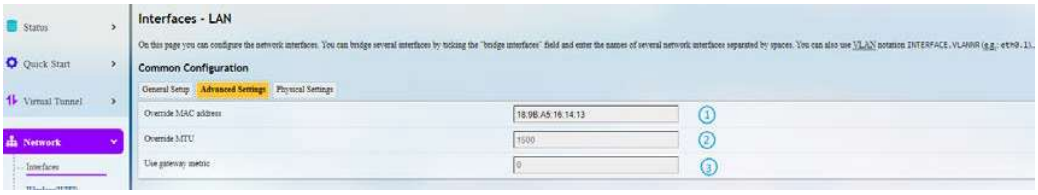
Clicking on the **Edit** button behind the **LAN** port will allow you to access the configurations of the port, and **General Setup** is displayed by default.



Description of the numbered areas

1. Status of the interface
2. The IP address of the port (you can modify as necessary)
3. The LAN port subnet mask

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

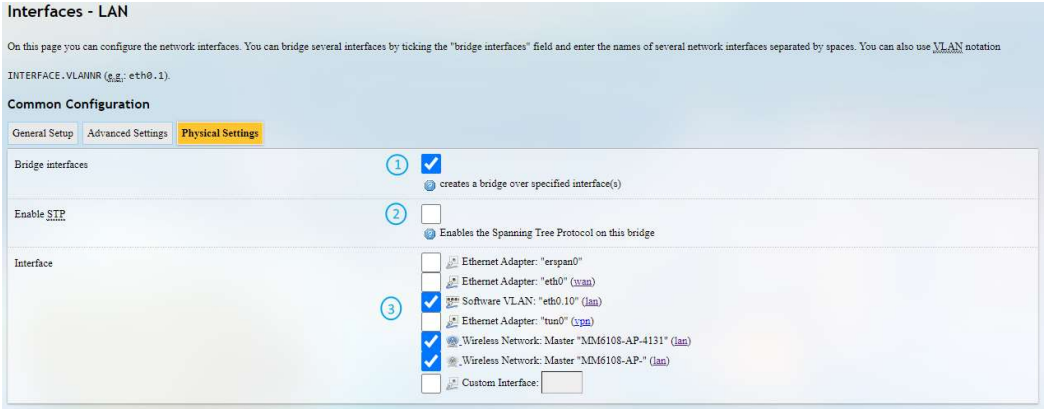


Description of the numbered areas

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

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 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

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

- **DHCP server**

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

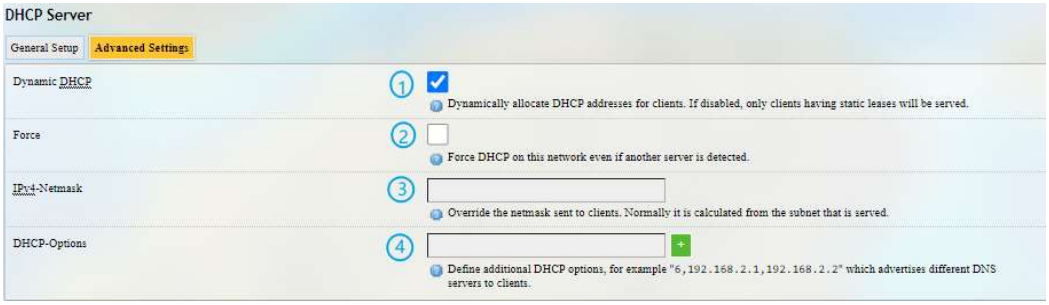
Description of the numbered areas

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. DHCP start address
3. Maximum number of leased addresses (up to 150)
4. Expiry time of 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.

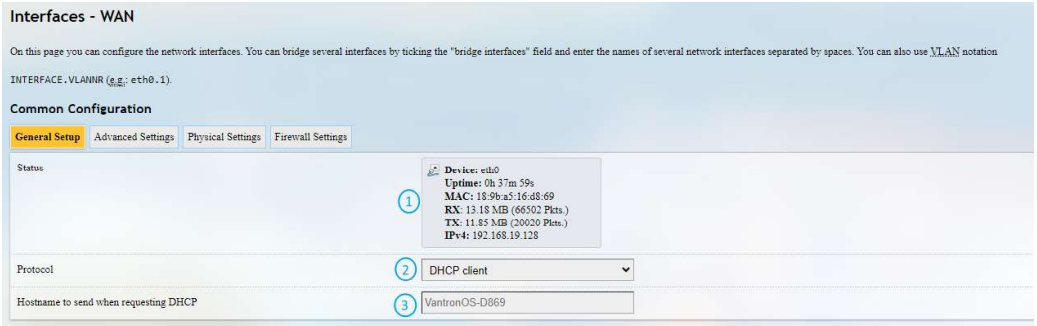
4. Add different DNS servers for client devices

*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.*

3.6.1.2 WAN

- **General DHCP 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. Select a WAN protocol (DHCP client by default)
3. Input a hostname of HAP101 for requesting DHCP

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

- **Advanced DHCP settings**

Description of the numbered areas

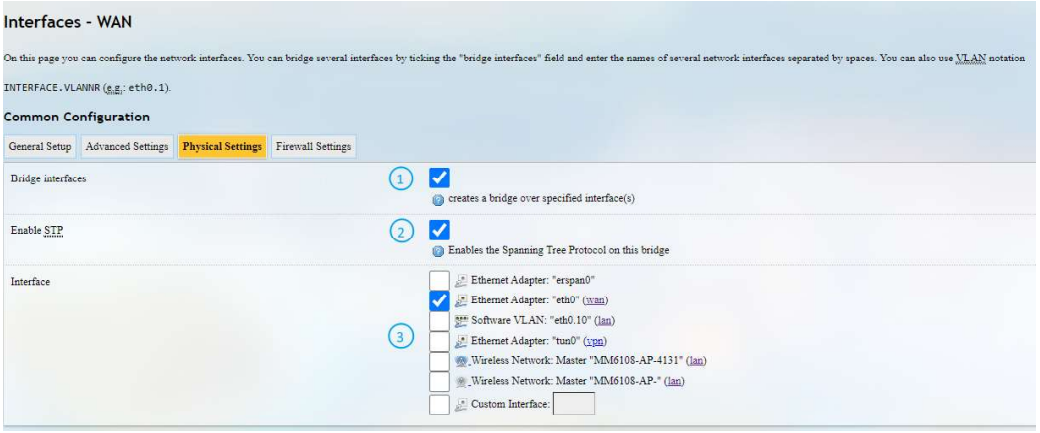
1. Check the box to bring up the port upon device boot
2. Force link (once the box is checked, hotplug handlers will not be invoked after a link change)
3. Enable **Use default gateway**
4. Enable **Use DNS server advertised by peer**

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

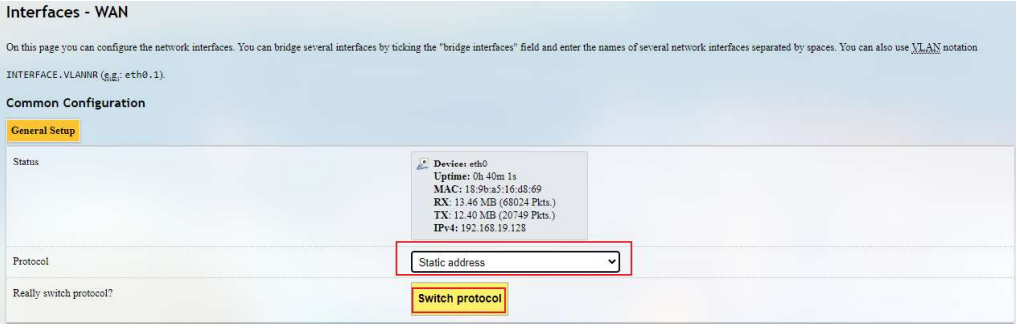
1. Enable/Disable the interface for network bridge
2. Enable/Disable STP protocol
3. Select the interfaces for bridge connection

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

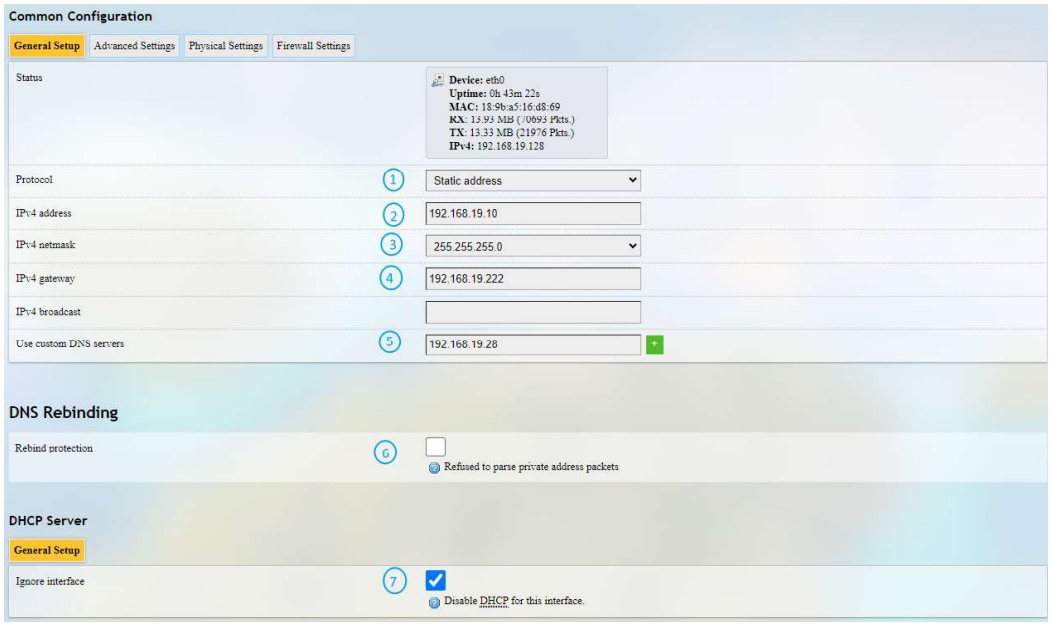
Under the **Firewall Settings** tab, you can choose the firewall zone to assign to this interface.

- **General Static protocol settings**

To activate the static address protocol, select **Static address** from the protocol drop-down list under the **General Setup** tab of the WAN port and click **Switch protocol**.



Upon a click of **Switch protocol**, you'll need to input the IPv4 address, subnet mask, IPv4 gateway, and the IPv4 broadcast.



Description of the numbered areas

1. Current protocol
2. Input an IPv4 address
3. Input an IPv4 netmask
4. Input the IPv4 gateway
5. Set a custom DNS server (can be provided by the carrier or self-defined)
6. DNS re-binding protection (if enabled, parsing of private IP data will be refused)
7. Disable/Enable the DHCP service (keep the default settings)

Leave the field as is if not applicable.

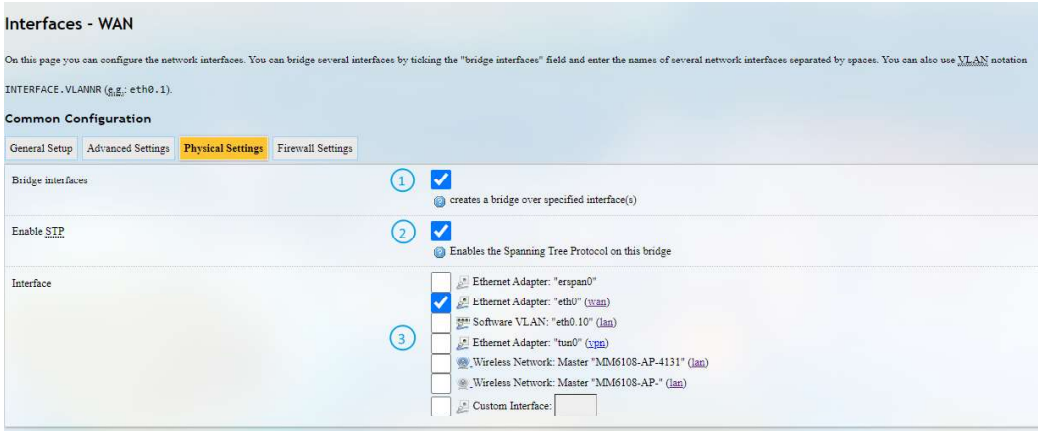
When static address protocol is selected, DHCP server will be automatically disabled.

The advanced settings for static protocol are basically same as those for DHCP protocol.

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

Other available WAN protocols include PPPoE and relay bridge. The settings are dependent on the specific protocols.

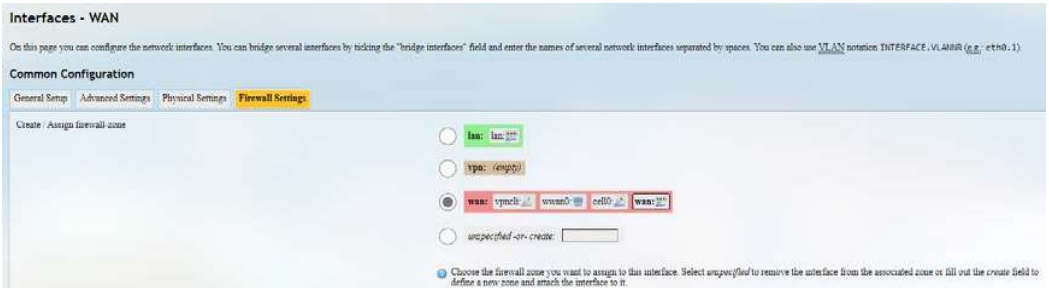
There is a **Physical Settings** tab next to **Advanced settings**, allowing you to configure the WAN port for network bridge.



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

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

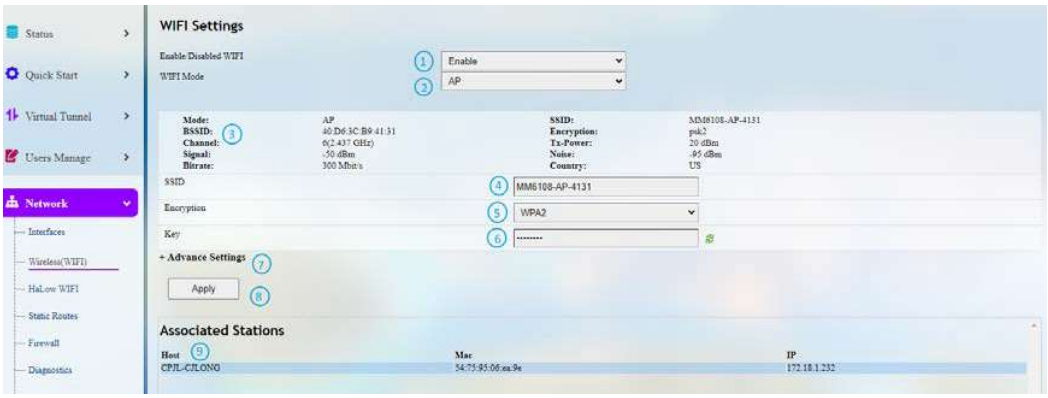


When 'unspecify or create' is selected, you can remove the interface from the associated firewall zone or create a new zone.

3.6.2 Wireless (WIFI)

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

3.6.2.1 Wi-Fi – AP Mode



Description of the numbered areas

1. Enable/Disable the Wi-Fi module
2. Select the Wi-Fi mode (AP for demonstration)
3. AP information
4. Modify the SSID for the AP

The ID name shall not *contain special characters including $, `, \.*

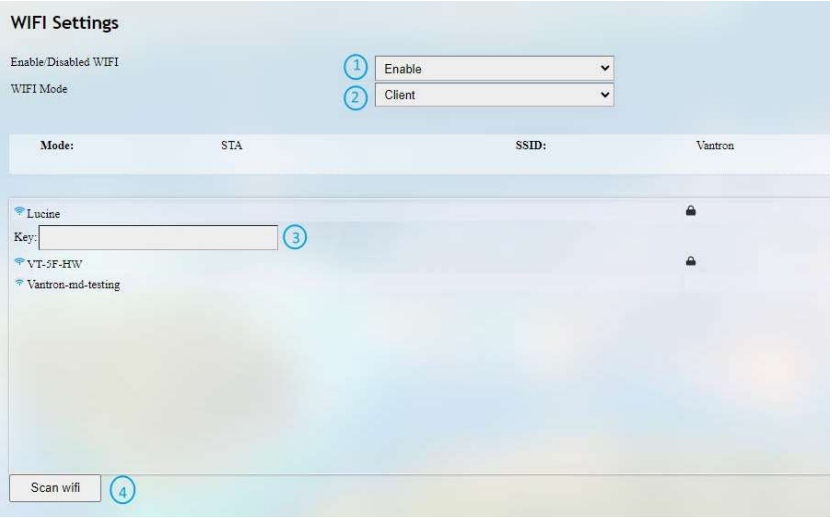
5. Select an encryption protocol
6. Assign a Wi-Fi password (no less than 8 characters)
7. Advanced Wi-Fi settings, including country code, frequency band, and channel
8. Click **Apply** to allow the modifications to take effect
9. List of currently connected devices

3.6.2.2 Wi-Fi – Client Mode

When HAP101 is set as a client on a wireless network, you can further configure the device here.

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

Before switching HAP101 to Wi-Fi client mode, please connect the host computer and HAP101 to the same router/switch, and use the WAN port IP to log in VantronOS for HAP101.



Description of the numbered areas

1. Enable/Disable the Wi-Fi module
2. Select the Wi-Fi mode (Client for demonstration)
3. Click the target access point and input the password for connection
4. Click the **Scan wifi** button to refresh the Wi-Fi list if the target SSID is not identified

When the AP is successfully connected as a client, 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.

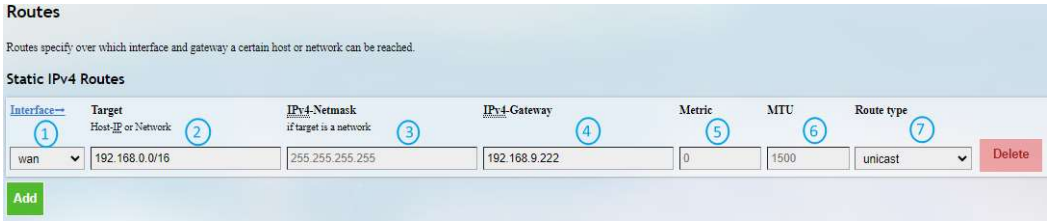
3.6.3 Wi-Fi HaLow

Refer to 2.4 for the Wi-Fi HaLow settings for both AP and station modes.

3.6.4 Static Routes

This is an advanced function allowing you to specify interface rules for route access.

Click **Add** to set up a new static 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. 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.

3.6.5 Firewall

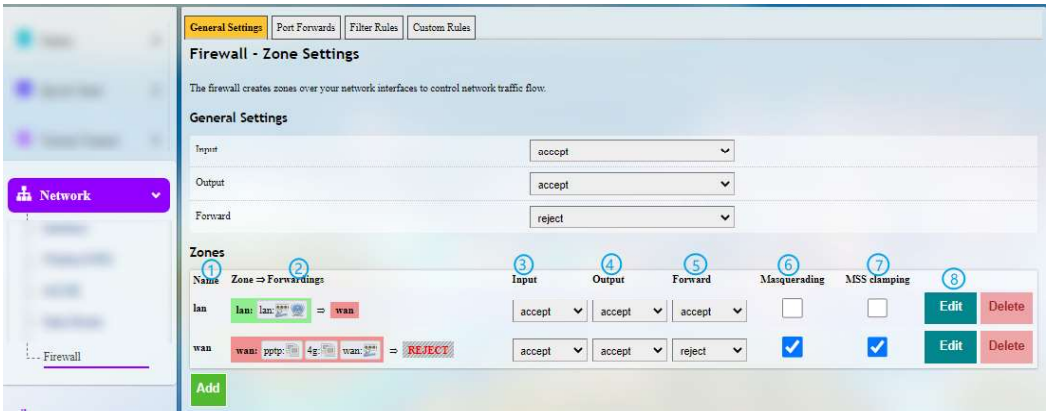
- **General Settings**

The following is a summary of the configuration items that the firewall can define. The minimum firewall configurations usually contain a basic setting item, at least two zones (LAN and WAN) and a forwarding to allow packets to be forwarded from LAN to WAN.

General Settings define the global settings that do not depend on a specific area. The following options can be defined:

Name	Type	Mandatory or not	Default value	Description
Input	String	N	ACCEPT	INPUT chain default strategy (ACCEPT, REJECT, DROP)
Output	String	N	ACCEPT	OUTPUT chain default strategy (ACCEPT, REJECT, DROP)
Forward	String	N	REJECT	FORWARD chain default strategy (ACCEPT, REJECT, DROP)

A zone section groups multiple interfaces and serves as a source or destination for forwardings, rules and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per-zone basis.



Description of the numbered areas

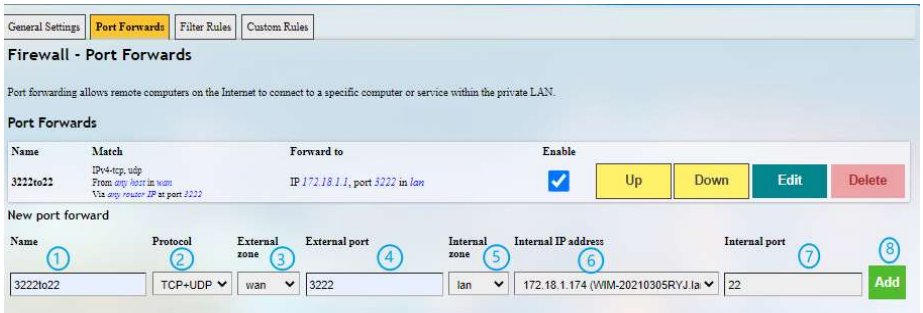
1. Zone names
2. Zone forwarding model description
3. Default policy (ACCEPT, REJECT, DROP) for incoming zone traffic
4. Default policy (ACCEPT, REJECT, DROP) for outgoing zone traffic
5. Default policy (ACCEPT, REJECT, DROP) for forwarded zone traffic
6. Masquerading (NAT)
7. MSS clamping
8. Zone editing

A click of the **Edit** button following each zone will direct you to the detailed zone setting page where general settings, advanced settings and forwarding rules are available.

- **Port Forwards**

The forwarding controls the traffic between zones and may enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, two forwarding setups are required with the dest ports reversed.

Example of port forwarding (To forward port 3222 of the WAN port to port 22 of the LAN host 172.18.1.174):

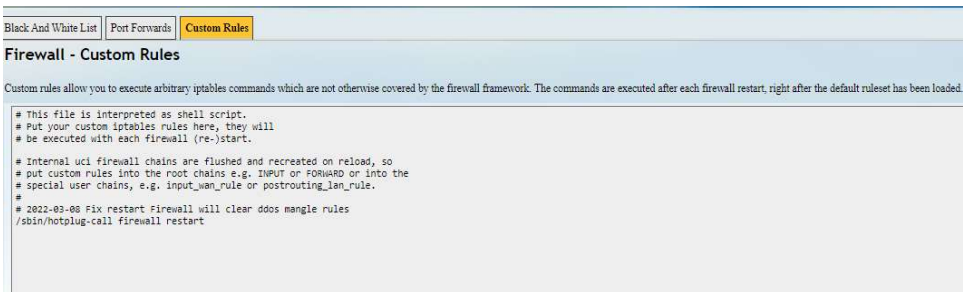


Description of the numbered areas

1. Rule name
2. Forward protocol (TCP/UDP/TCP + UDP are supported)
3. External zone: WAN
4. External port: 3222
5. Internal zone: LAN
6. LAN host: 172.18.1.174
7. Port number of the target host in the internal zone: 22
8. Add the rule to allow it take effect

- **Custom Rules**

Custom rules allow you to execute arbitrary **iptables** commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default rule settings have been loaded.



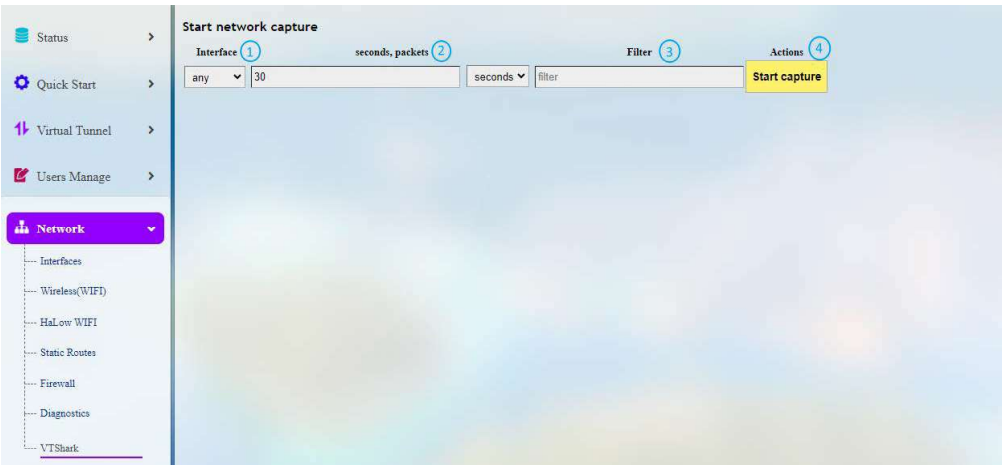
3.7 Diagnostics

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

Tool	Description
Ping	To test the connectivity and measure the response time between the AP and external IP addresses on the internet
Traceroute	To access information about the path that network traffic follows, including the number of hops and the response time of each hop
Nslookup	To query the Domain Name System (DNS) to obtain information about domain names, IP addresses, and DNS records

3.8 VTShark

The **VTShark** feature provides a flexible way to follow up and verify network issues. You can use a network traffic tool (e.g., Wireshark) to open and check the packets captured.



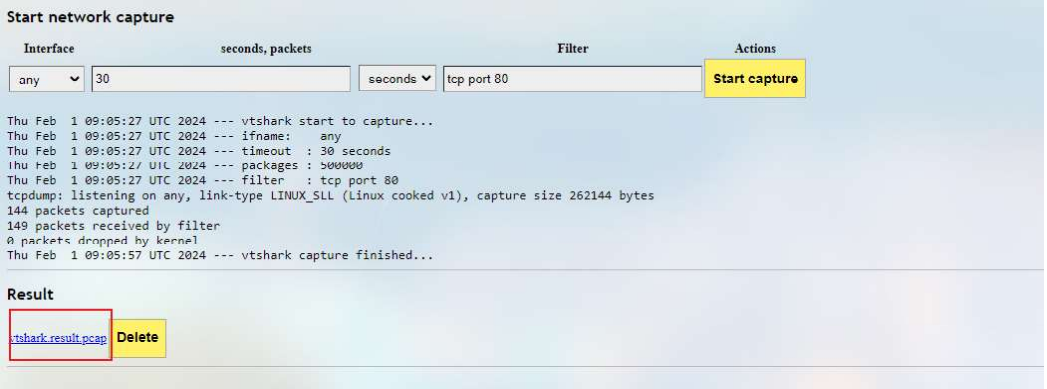
Description of the numbered areas

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

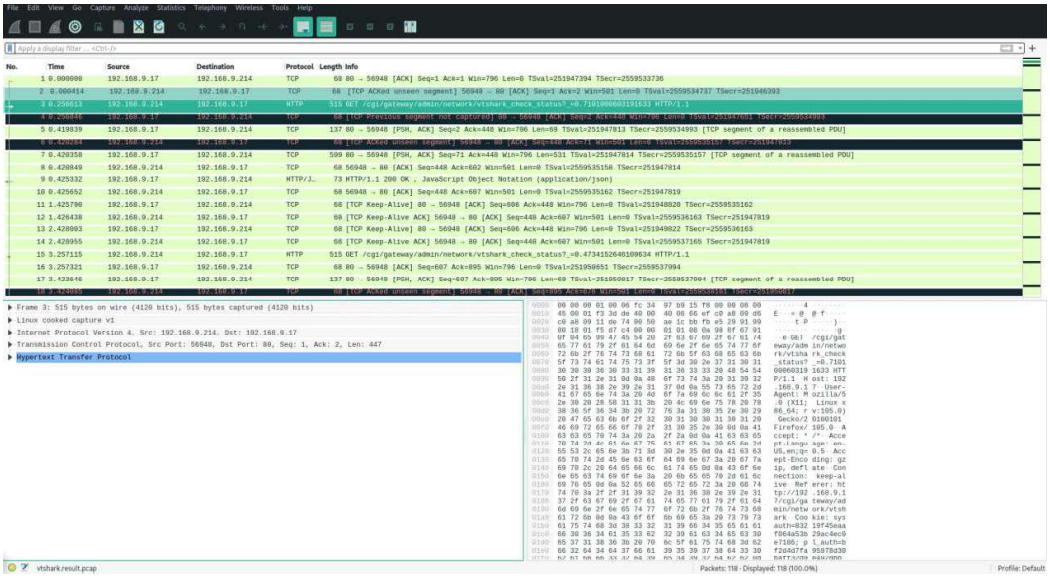
Packets capture by seconds and by packet counts:

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 result will download it to the local directory and you can open it with a network traffic tool (e.g., Wireshark).

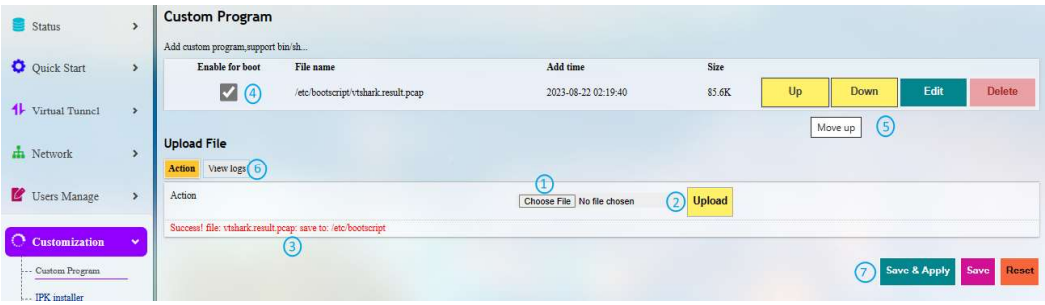


3.9 Customization

Customization provides features to allow users to customize the device or system.

3.9.1 Custom Program

Custom program allows users to upload scripts or programs (sh/bin) to the device and run them at the device startup.

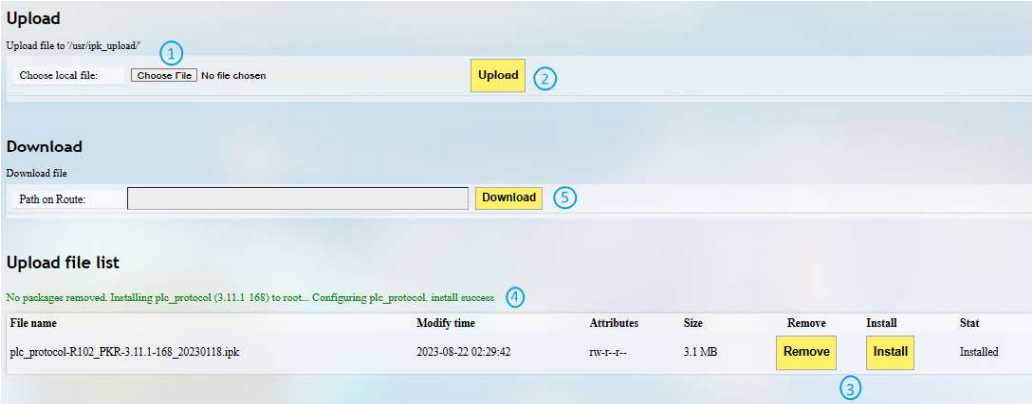


Description of the numbered areas

1. Select a script to upload
2. Upload the script to HAP101
3. When the script is uploaded successfully, the file name and file directory will be displayed here
4. Enable the script, and it will run automatically next time when the device starts up
5. If more than one script is uploaded, you can move any of them up or down to rearrange the script order, and edit/delete the script
6. Check the script log
7. **Save & Apply** the settings

3.9.2 IPK Installer

With IPK Installer, customers can install self-compiled IPK packages to HAP101. Vantron industrial protocol packages are also uploaded from here.

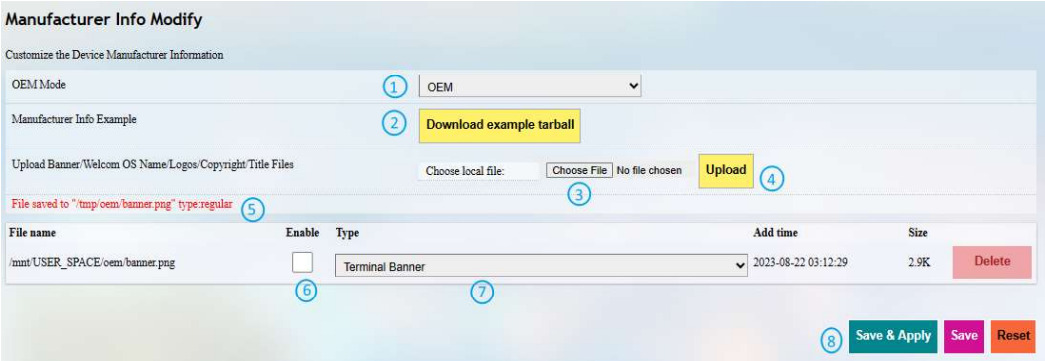


Description of the numbered areas

1. Select an .ipk file from the local directory
2. Click **Upload** to upload the file to the device
3. You can delete or install the file after the .ipk file is uploaded
4. Install the file and wait a moment, there will be a prompt for the installation status
5. You can also input a file path on the device to download the specific file

3.9.3 Manufacturer Info Customization

Once you need to customize the manufacturer information shown in the GUI, navigate to **Customization > Manufacturer Info Modify**, and select **OEM** from the **OEM Mode** drop-down list.



Description of the numbered areas

1. Select the **OEM** mode
2. Download the illustrative .tar file to the local directory
3. Select the target file from the local directory
4. Upload the file to HAP101
5. The path of the file on the device will be displayed here
6. Choose to enable the file or not for next startup
7. Select the type of the file
8. **Save & Apply** the settings

The three modes that customers can choose from the drop-down list based on needs are explained as follows.

Mode	Description
Vantron	All the information displayed in VantronOS will be Vantron-related
Standard	Some of the information displayed in VantronOS will be “Gateway” by default, and some information like the copyright will be left blank.
OEM	All the information displayed will be user tailored

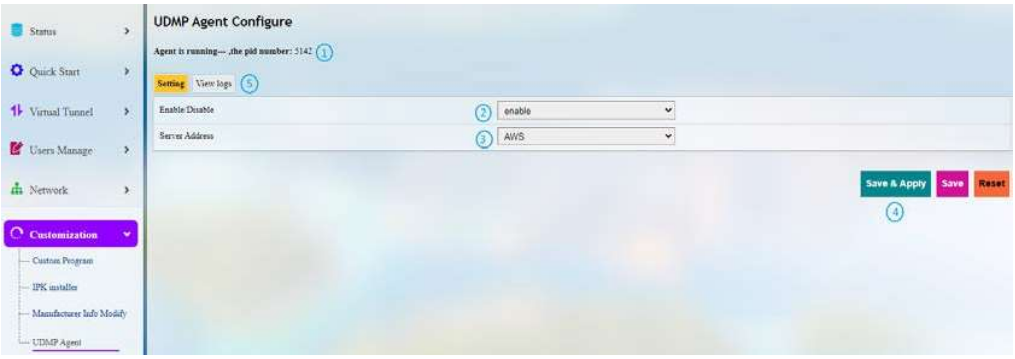
3.9.4 UDMP Agent

Vantron BlueSphere Gateway Management Platform ("GWM") is a cloud-based management portal that empowers organizations to seamlessly provision, monitor, and manage Vantron IoT communication devices, including gateways, routers, and DTUs. By leveraging BlueSphere GWM, organizations can streamline device setup, ensure real-time visibility into device performance, and effortlessly control device configurations. This contributes to enhanced operational efficiency and improved decision-making.

Before you can use BlueSphere GWM for remote management of Vantron IoT devices, please make sure the following prerequisites are met:

- You have obtained a license for log in to BlueSphere GWM
- The UDMP agent is installed on the device for remote management
- The UDMP agent is “enabled”
- The serial number of the device is added to BlueSphere GWM

You can modify the settings of the UDMP agent here.



Description of the numbered areas

1. Status of the UDMP Agent
2. Enable/Disable the Agent
3. Select the cloud server
4. **Save & Apply** the settings
5. View the connection log

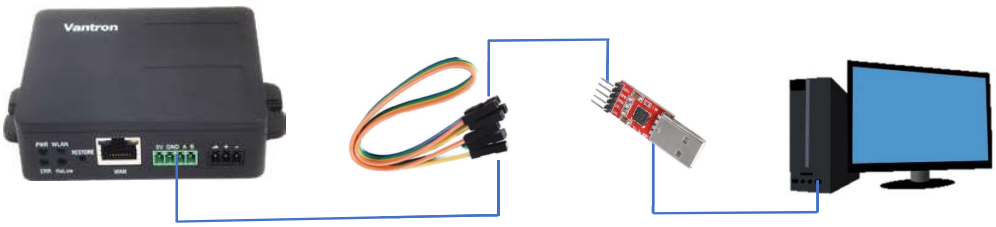
3.10 Hardware

3.10.1 Ser2TCP

Serial to TCP provides an easy way to convert local serial data into Ethernet data and enables two-way communication with remote devices. Each conversion rule can be independently configured to server-side or client-side mode. You can also add, edit or delete a conversion rule on this page.

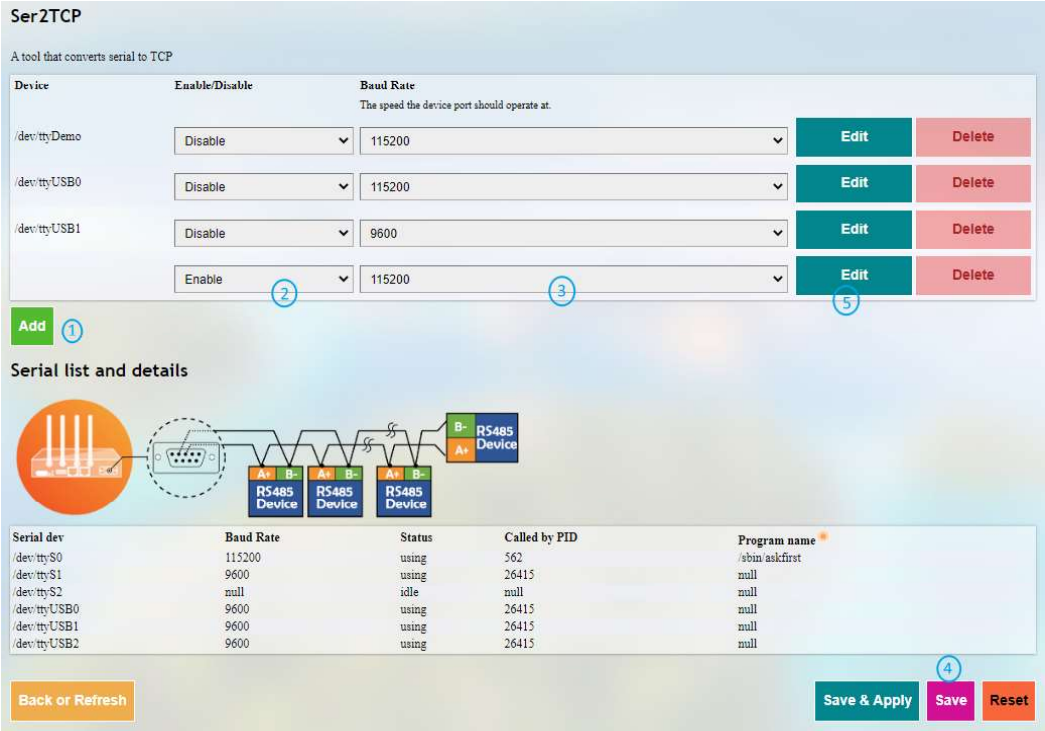
3.10.2 Ser2net Environment Setup and Verification

- Prerequisites
  - An HAP101
  - A Linux host computer (Ubuntu for demonstration here)
  - A USB to TTL serial adapter
  - DuPont cables
  - Connect the serial port of HAP101 to the host computer as follows (refer to 1.5 for the wiring)



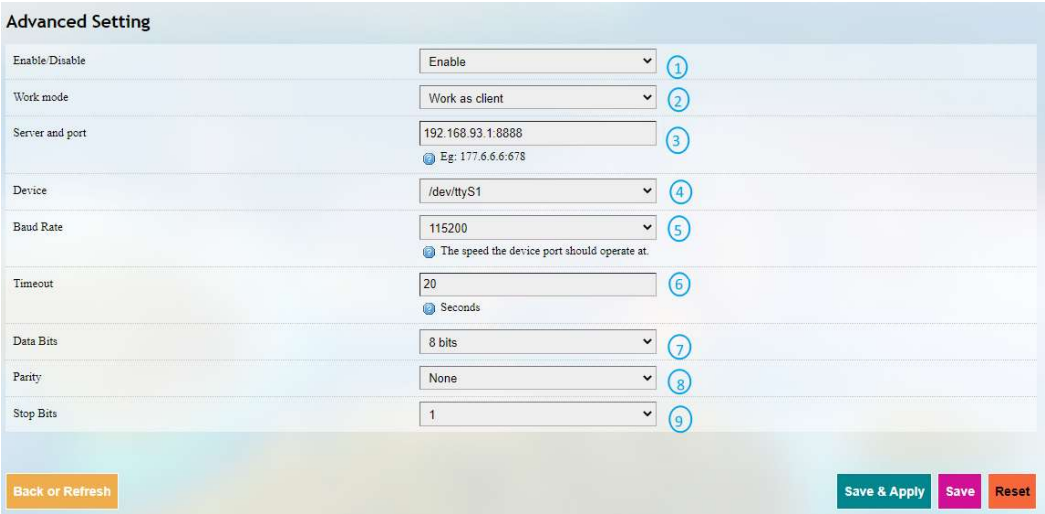
- Client mode

(1) Settings on VantronOS web interface



Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate of the serial port (115200)
4. Save the settings
5. Click **Edit** after the rule to access the advanced settings page



Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as client** mode
3. Input the server address and port number (Ubuntu host shall be the server, and port number is user-defined)
4. Select the serial device from the drop-down list (software node of the serial port is /dev/ttyS1 as described in 1.5)
5. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
6. Set a timeout value
7. Select “8 bits” for the data bit
8. Select “None” for parity
9. Select “1” as the stop bit

Be sure to save above settings before you exit.

(2) The Ser2net process is running as follows:

```
uart2net -c -d 192.168.93.1 -p 8888 -t /dev/ttyS1 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Settings on the Ubuntu host

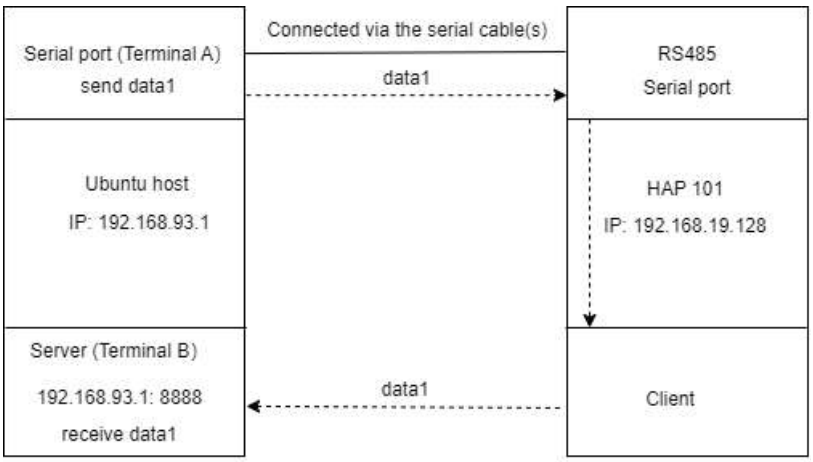
- Use a serial communication program (e.g. microcom) to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (8888 as assigned in prior steps)

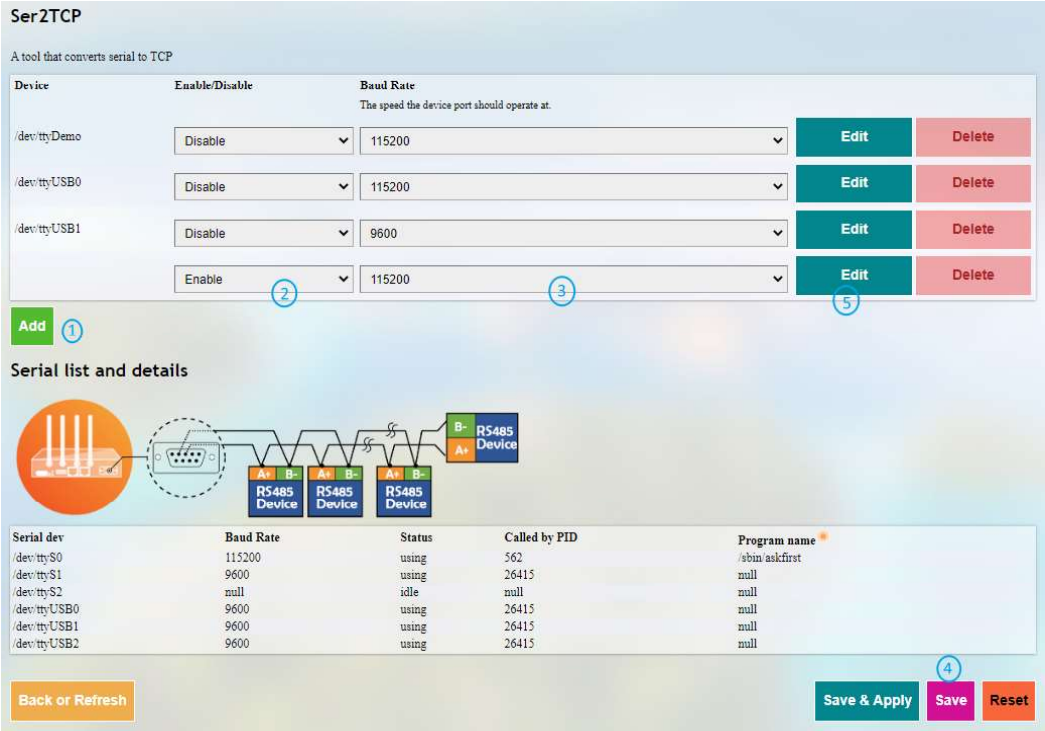
```
tcpudp_test tcp server:tcpudp_test -p 8888
```

- Input data in terminal A and open another terminal (B) to receive the data (the topology is as follows)



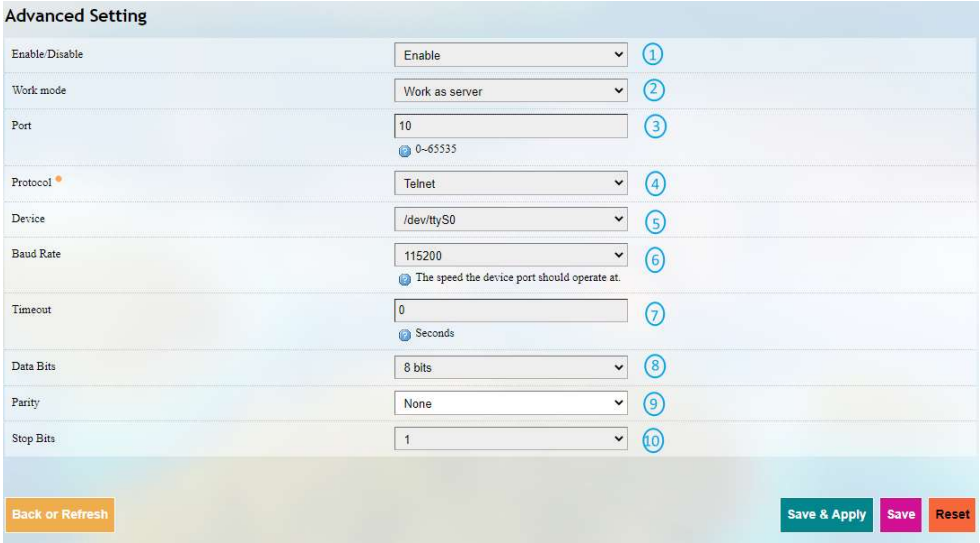
- Server mode

(1) Settings on VantronOS web interface



Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate of the serial port (115200)
4. Save the settings
5. Click **Edit** after the rule to access the advanced settings page



Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as server** mode
3. Input the port number (user-defined)
4. Select a protocol from the drop-down (**Telnet** for instance, see 3.10.3 for the difference between the protocols)
5. Select the serial device from the drop-down (software node of the serial port is /dev/ttyS1 as described in 1.5)
6. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
7. Set a timeout value
8. Select “8 bits” for the data bit
9. Select “None” for parity
10. Select “1” as the stop bit

Be sure to save above settings before you exit.

(2) The Ser2net process is running as follows:

```
/usr/sbin/ser2net -n -c /tmp/ser2net.conf
```

(3) Settings on the Ubuntu host

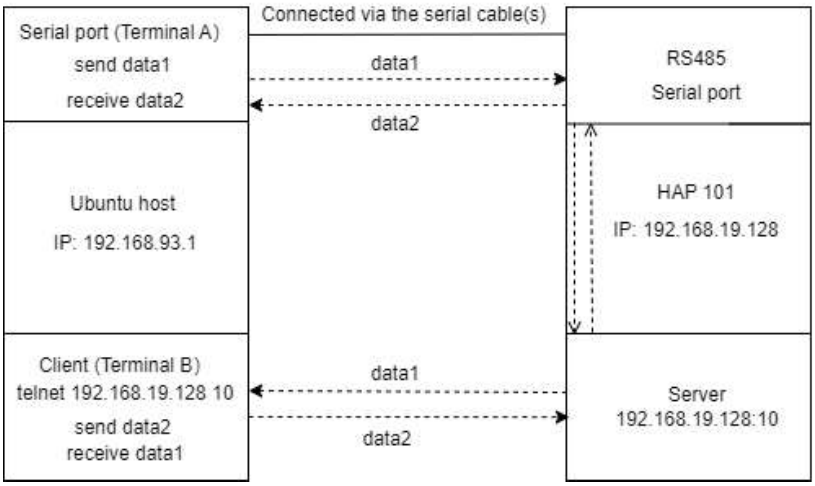
- Use a serial communication program (e.g., microcom) to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (10 as assigned in prior steps) in terminal B using Telnet protocol

```
telnet 192.168.19.128 10
```

- Terminals A and B can send and receive data in both directions (the topology is as follows)



3.10.3 Protocol comparison

Under the server mode, two protocols are available which are differentiated as below:

1) Raw: enables the port and transfers all data as-is between the port and the long integer.

2) Telnet: enables the port and runs the telnet protocol on the port to set up telnet parameters.

3.11 Services

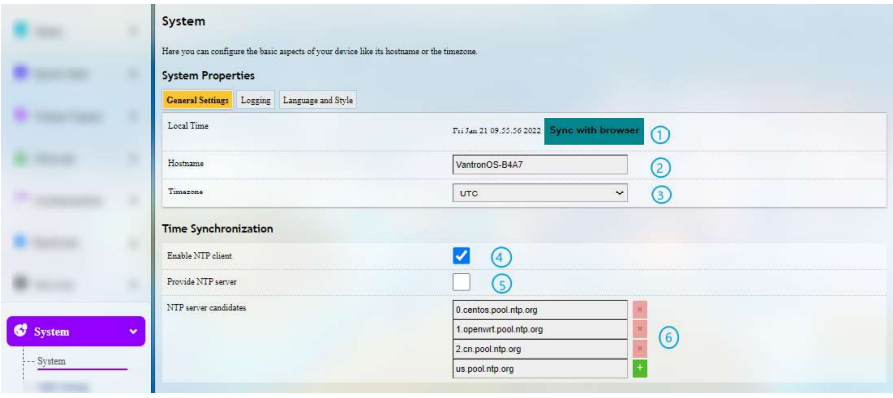
Dynamic DNS is a technology in domain name system (DNS) that automatically updates the content of Name Server, often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information.

Input a name of the subdomain or root domain and click **Add** button, and you will be directed to the setup page of the dynamic DNS. Then you can edit the service as needed.

3.12 System

3.12.1 System

Apart from the device settings you might make in the previous sections, here you can configure the device 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
2. Change the name of the host
3. Select a time zone
4. Enable/Disable NTP online time adjustment
5. Start the NTP server (the AP is used as the NTP server)
6. NTP online time server

For log-related settings, click the **Logging** tab next to the **General settings** tab.

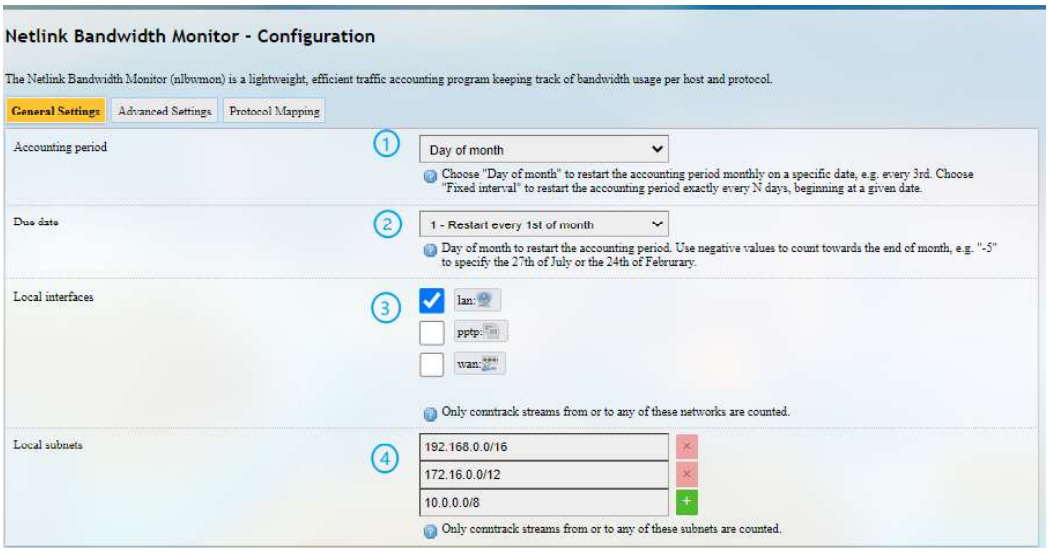
Description of the numbered areas

1. Buffer size of the system log
2. Address of the log server
3. Port of the log server
4. Protocol used by the log server
5. Path of the file for the system log
6. Output level of the console log
7. Cron log level

For **language settings**, please refer to 2.6.

3.12.2 Netlink Bandwidth Monitor (NBM) Setting

- **General Settings**



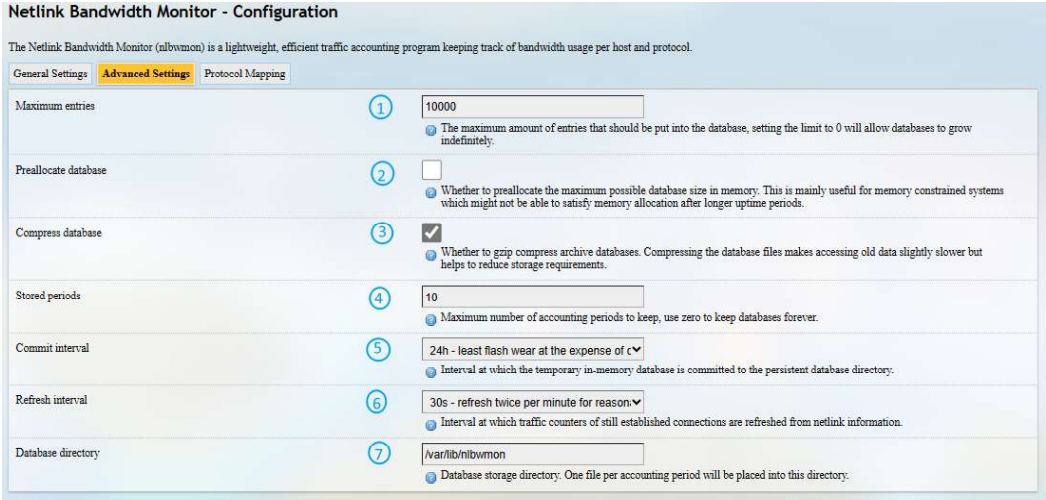
Description of the numbered areas

1. Set how long you would like the monitoring activities to be reported
2. Specify a date in a month for restarting another round of monitoring activities

Applicable when Day of month is selected in 1.

3. Select the interfaces to monitor
4. Local subnets

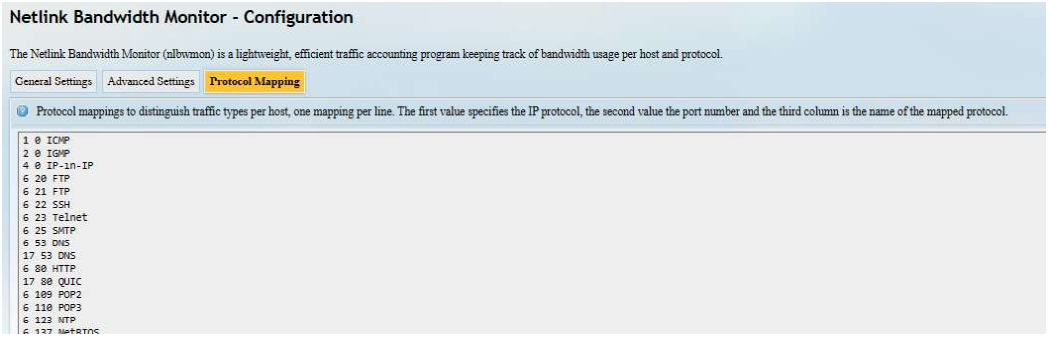
Under the **Advanced Settings** tab, you can further set up the monitoring activities.



Description of the numbered areas

1. Set the maximum count of entries to store in the database ('0' for no limit)
2. Check the box to pre-allocate a database (more frequently applicable to devices with less memory space)
3. Check the box to compress the database
4. Maximum count of reporting periods to store ('0' for no limit)
5. Time interval for submitting the temporary database to the persistent database
6. Time interval for refreshing the traffic counters from the netlink information
7. Directory of the database

Protocol Mapping can be used to distinguish traffic types per host. Each mapping takes one line, with the first value being the IP protocol, the second value being the port number, and the third value being the name of the mapping protocol.

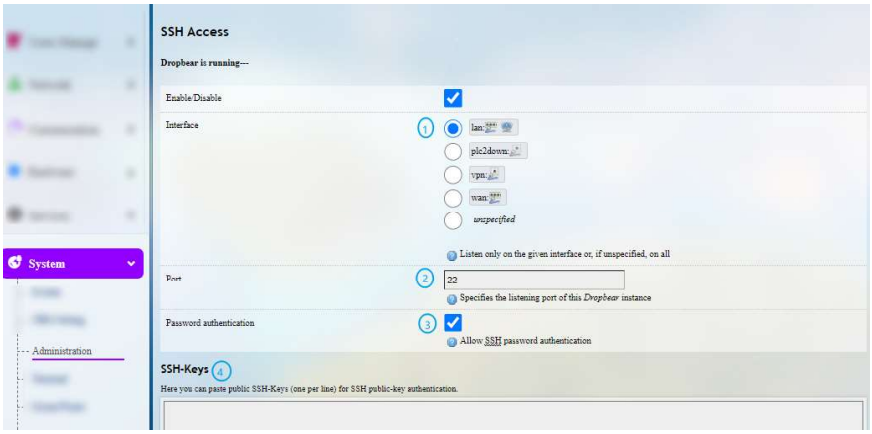


3.12.3 Administration

You can reset the password for accessing the device in the Administration menu. Please refer to 2.5 for details.

SSH Login

Step 1: Navigate to **System > Administration** in VantronOS, and enable dropbear;



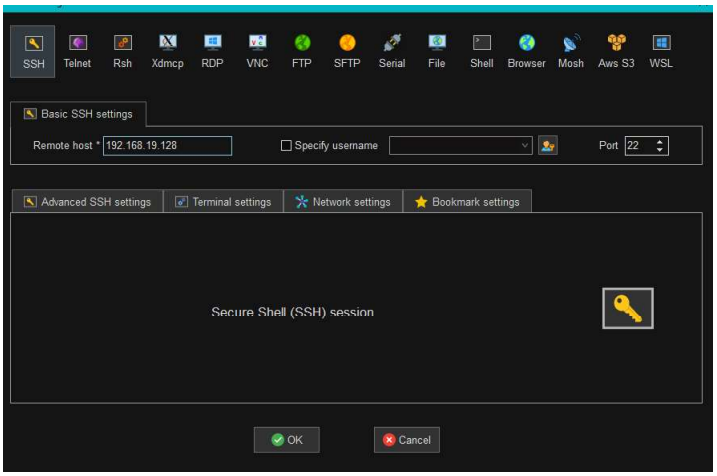
Description of the numbered areas

1) Select a port to access (When “unspecified” is selected, all the ports will be monitored.)
2) Specify a port for monitoring (port 22 by default)
3) Allow SSH password authentication
4) Add SSH-Keys for public key authentication

Step 2: Open an SSH emulator (PuTTY or MobaXterm recommended) in the Windows host;

Step 3: Launch an SSH session on the SSH emulator;

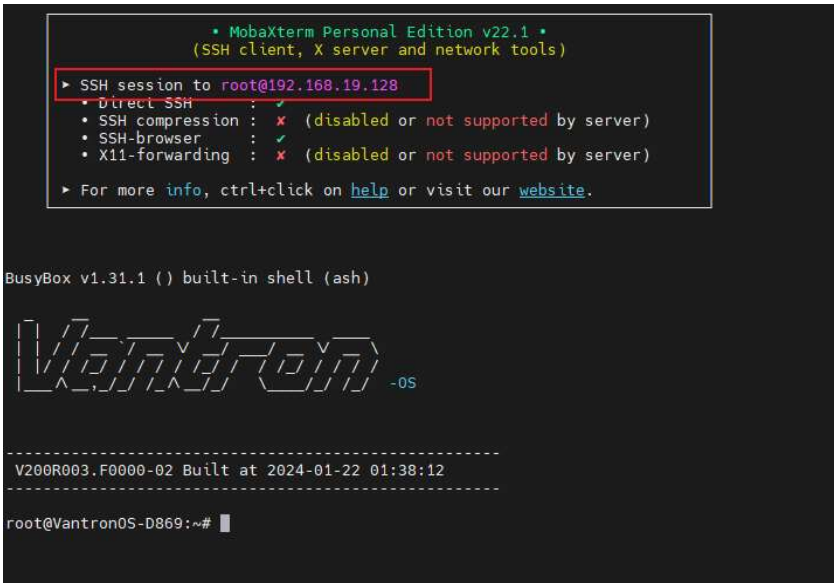
Step 4: Input the IP address of the device (WAN port IP or 2.4GHz WLAN IP) and keep the default port No. (22) unchanged;



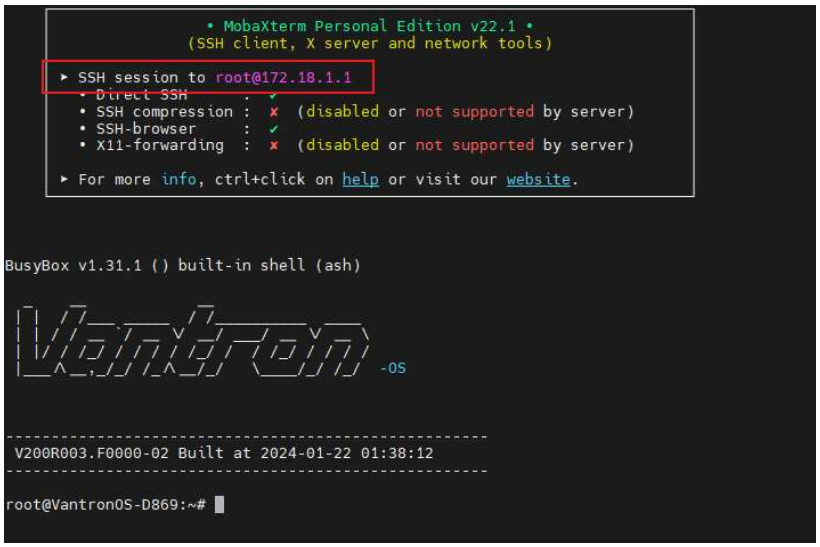
Step 5: Click **OK** to start the session;

Make sure the IP address of the host computer is on the same network as HAP101. Refer to 2.2 for how to identify the 2.4GHz WLAN IP or WAN port IP of the device.

SSH login with the WAN port IP of HAP101:

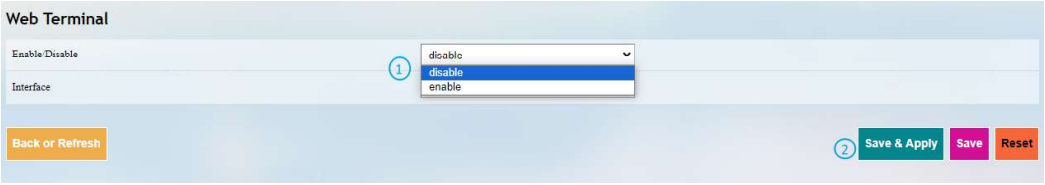


SSH login with the 2.4GHz WLAN IP of HAP101:



3.12.4 Terminal

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



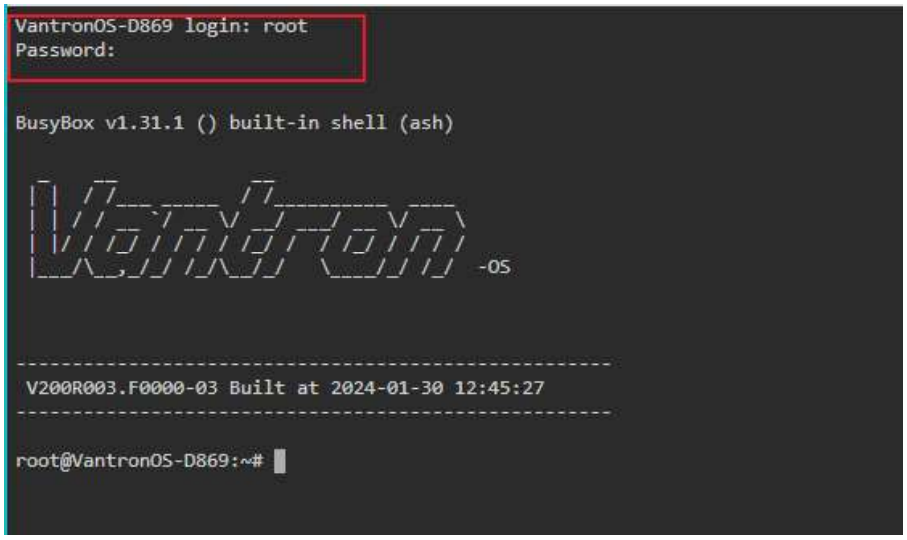
Step 1: Select **enable** from the drop-down list;

Step 2: Save the change;

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

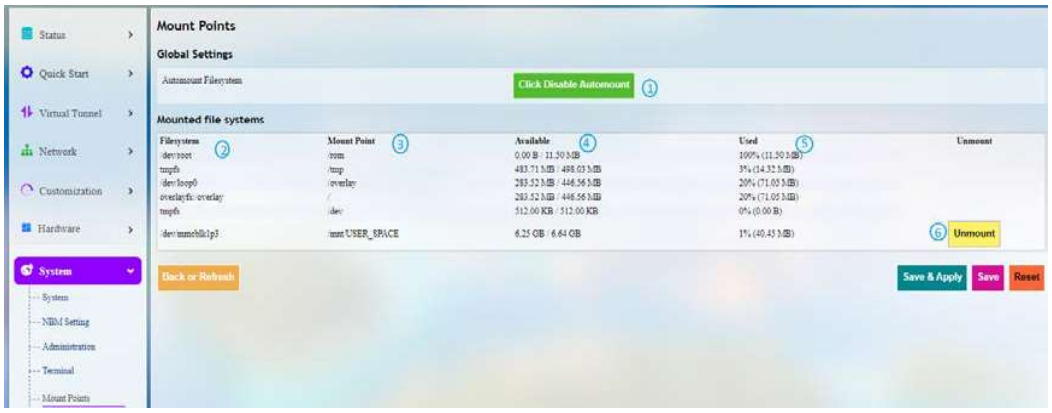
Login account: root

Login password: rootpassword (invisible while typing)



3.12.5 Mount Points

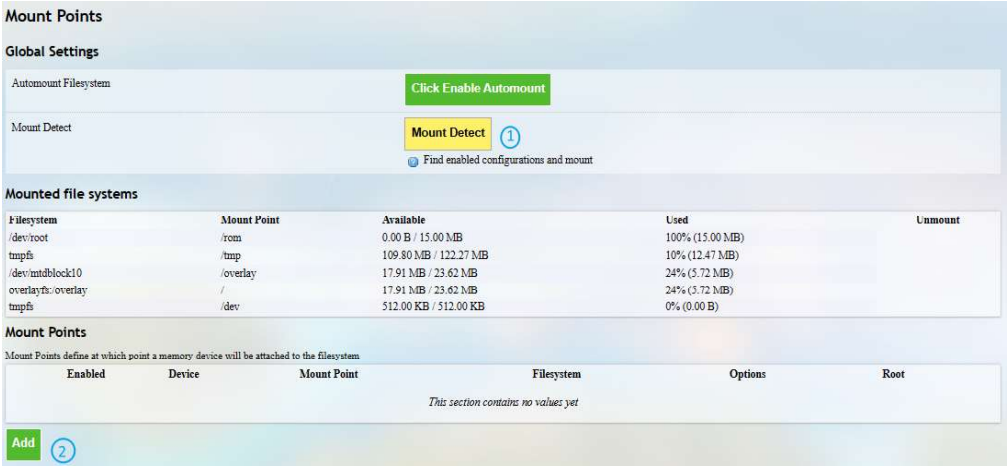
You can enable/disable automount and check the mounting information here.



Description of the numbered areas

1. Disable/Enable automatic mount
2. File path on the device
3. Mount point directory
4. Available space in the mount point
5. Space used in percentage
6. If you have previously mounted a file to the device, you can manually unmount the file here

To manually mount a file, click the **Click Disable Automount** button first and then proceed with the settings.



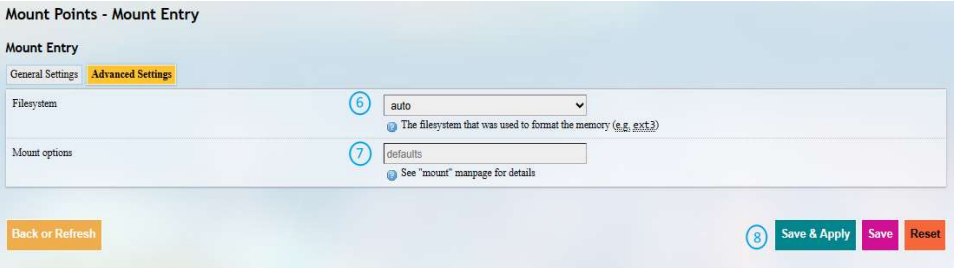
Description of the numbered areas

1. Detect the available mount points
2. Click **Add** to add a mount point

Click the **Edit** button behind the newly added mount point for more settings.

3. Check the box to enable the mount point after creation
4. Select/Input the UUID of the device (you can also use the partitional label instead of the UUID)
5. Select the mount point

Then click the **Advanced Settings** tab to access advanced settings.



6. Select the file system for formatting the memory
7. Input the mount options
8. Save the settings and click the **Back or Refresh** button to return to the general settings

The mount point is created as above.

3.12.6 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

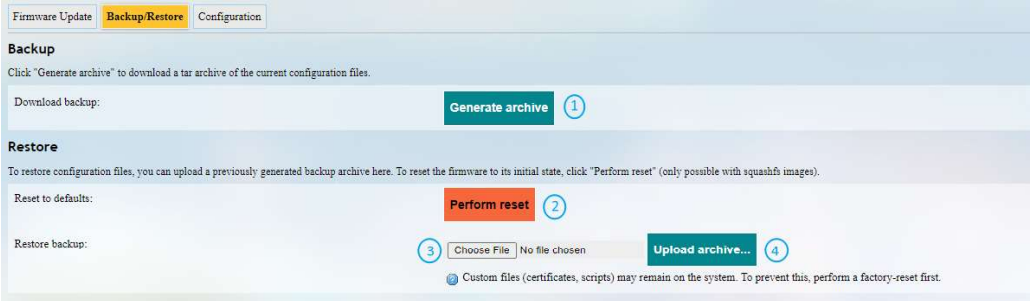
1. Check the box to keep the user settings while upgrading the device (not recommended)
2. Select the new firmware from the local directory
3. Click the button to upload the firmware
4. Upload progress of the package

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 firmware upgrade is in process;

The login page will be refreshed once the upgrade finishes and you can log in to check the firmware version on the homage.

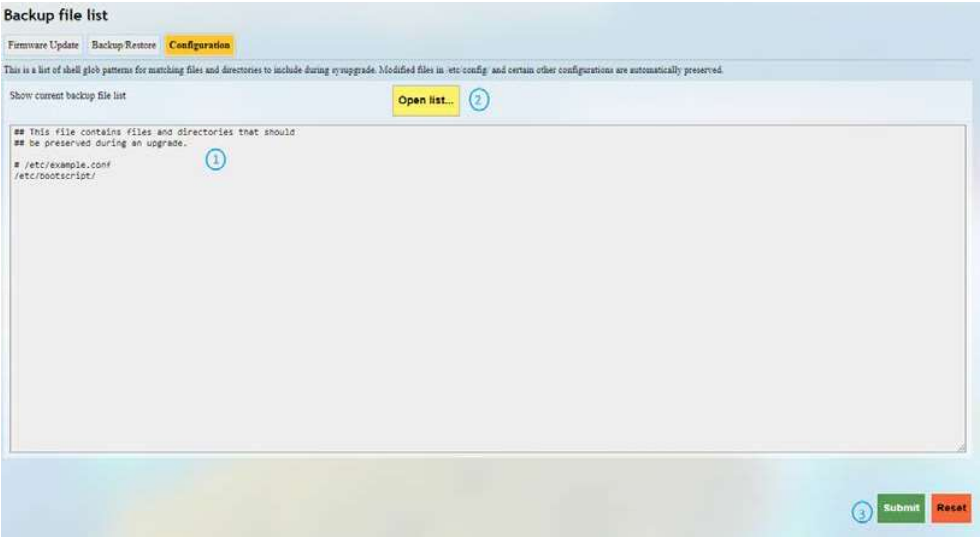
Under the **Backup/Restore** tab, you can back up your settings and download the package, including the configuration files and pre-set folders, restore the factory settings of the device, and upload a backup package saved before.



Description of the numbered areas

1. Click the button to back up the system configurations (include 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 to restore the backup settings
4. Upload the package

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

3.12.7 Reboot

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

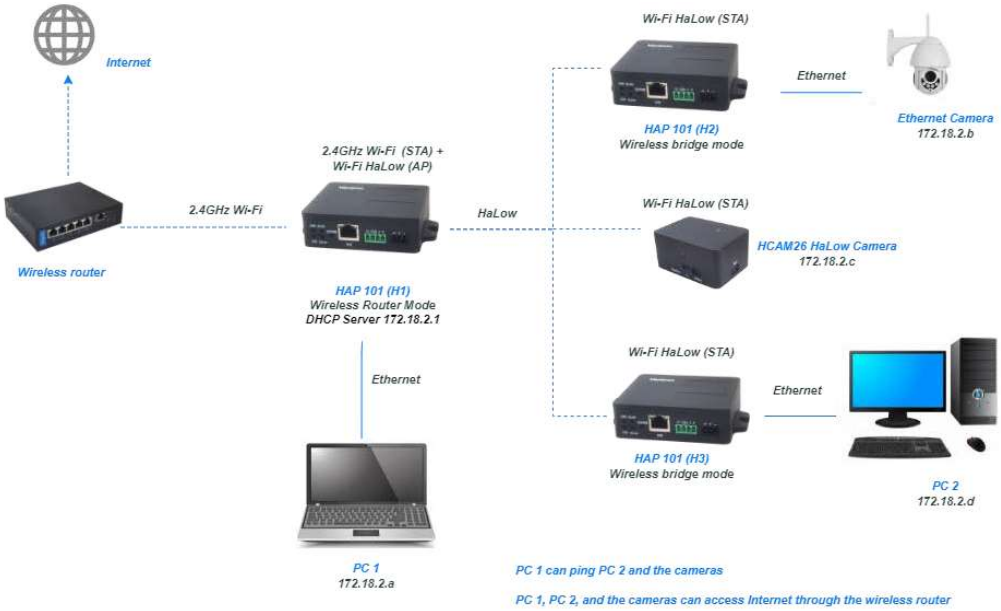
3.13 Logout

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.

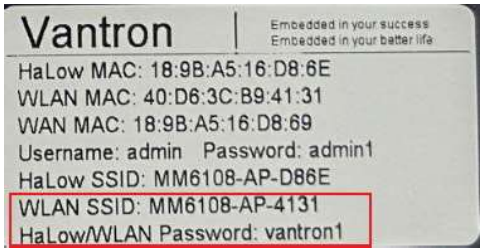


In the above topology, three HAP101 devices are used.

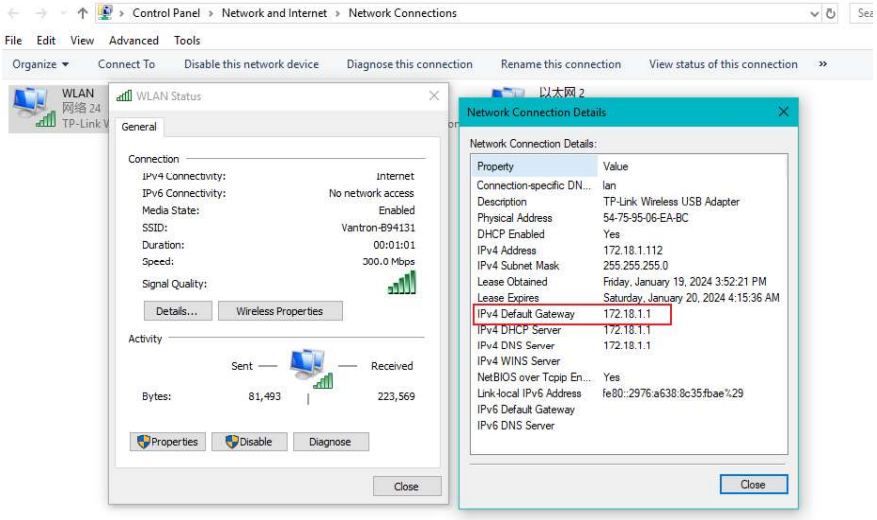
- H1, H2, and H3 operate in 2.4GHz Wi-Fi AP mode and Wi-Fi HaLow AP mode by default;
- H1 is later set to 2.4GHz Wi-Fi station mode and connected to a wireless router;
- H2 & H3 are then set to Wi-Fi HaLow station mode and connected to H1 via Wi-Fi HaLow;
- An Ethernet camera is connected to H2 via Ethernet with IP address on the same network as H1;
- HCAM26 HaLow IP camera is connected to H1 via Wi-Fi HaLow;
- The Ethernet jack of H1 is modified from its default WAN area to LAN area in order to enable the DHCP service;
- PC 1 is connected to H1 via Ethernet, and PC 2 is connected to H1 via Ethernet after wireless bridging;
- PC 1, PC 2, and the cameras can access Internet through the wireless router, and the status of the cameras is trackable on both PC 1 and PC 2.

4.2 Setup of H1 (HaLow AP mode)

1. Connect PC 1 to the HaLow-AP-mode HAP101 (H1) via 2.4GHz Wi-Fi using the WLAN SSID and password provided on the device label (like the following);

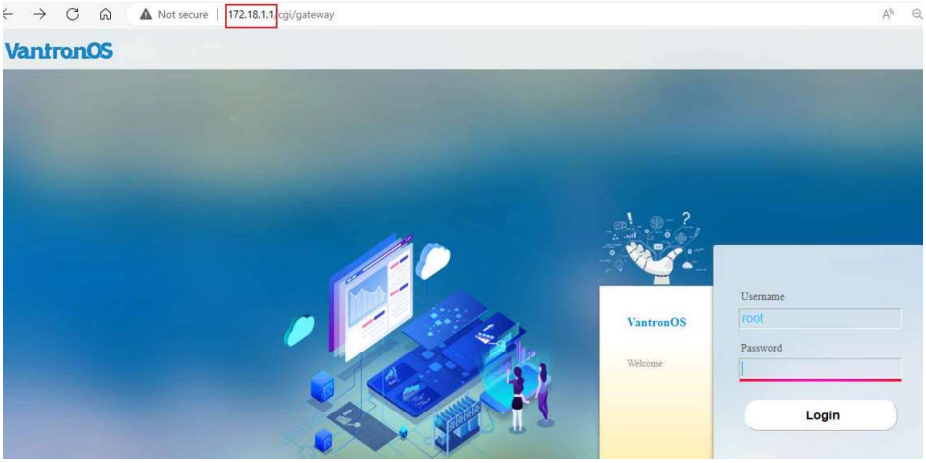


2. Check the details of the wireless connection on PC 1 and identify the gateway IP of the 2.4GHz Wi-Fi;

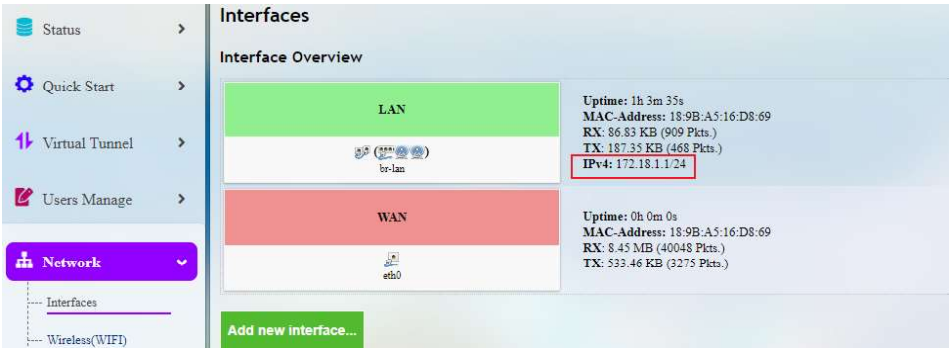


3. Log in to VantronOS for H1 as the super user using the gateway IP identified in the prior step;

   Super user: root password: rootpassword



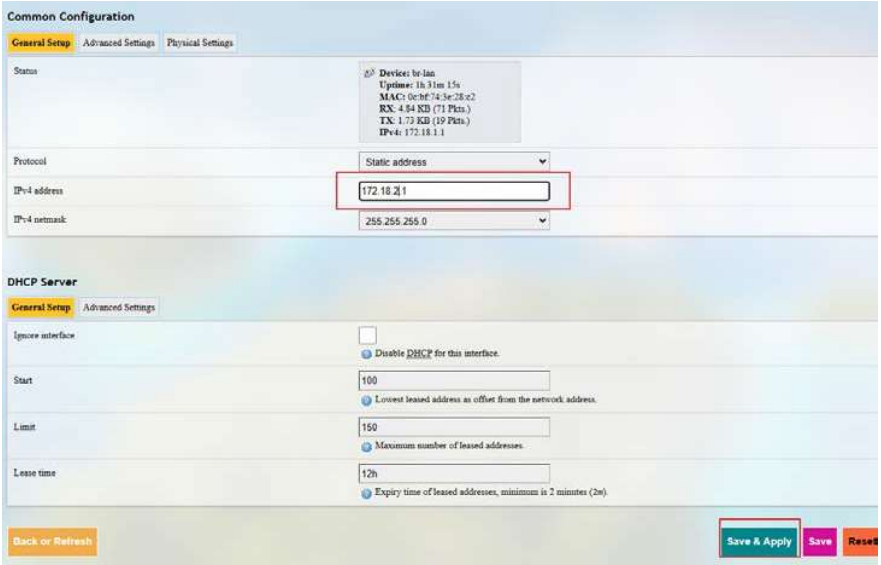
4. Navigate to **Network > Interfaces** to check the interface information of H1 (the 2.4GHz Wi-Fi is bridged on the virtual LAN port that provides DHCP service to connected devices);



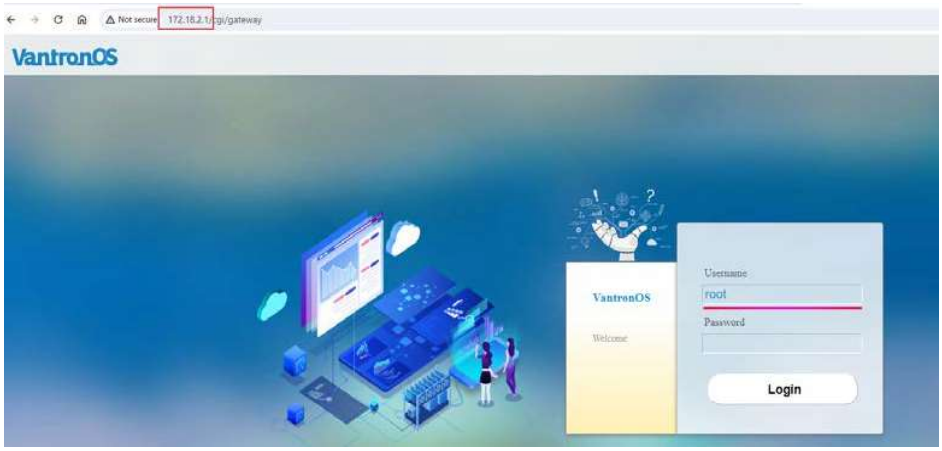
*Since the virtual LAN IP addresses of all HAP101 devices are set to the same by default. To ensure valid dynamic IP assignment to H2 and H3 that will be connected to H1 in the following steps, please change the LAN IP of H1 to a **different** one (e.g., 172.18.2.1).*

5. Click the **Edit** button behind the LAN port;

6. Input a new LAN IP (e.g., 172.18.2.1) for H1 under the **General Setup** tab and save the changes;

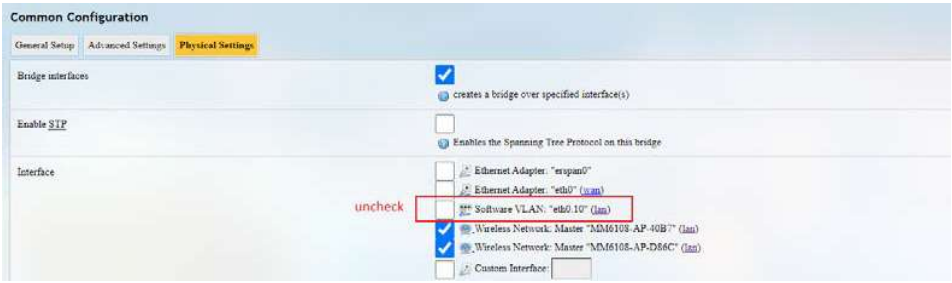


7. Re-connect PC 1 to H1 via 2.4GHz Wi-Fi and log in to VantronOS using the new gateway IP (LAN IP);

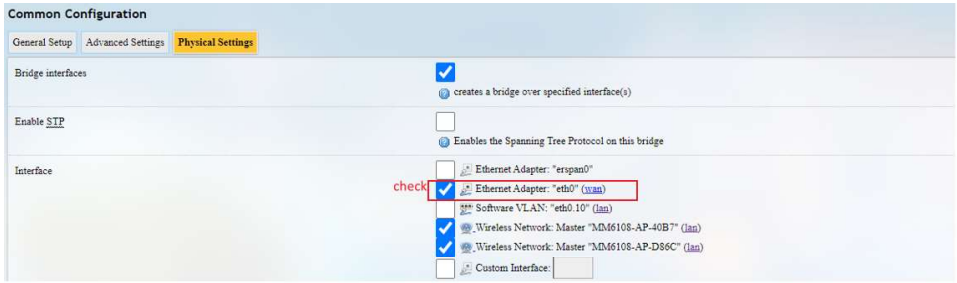


8. Navigate to **Network > Interfaces > LAN > Edit > Physical Settings**;

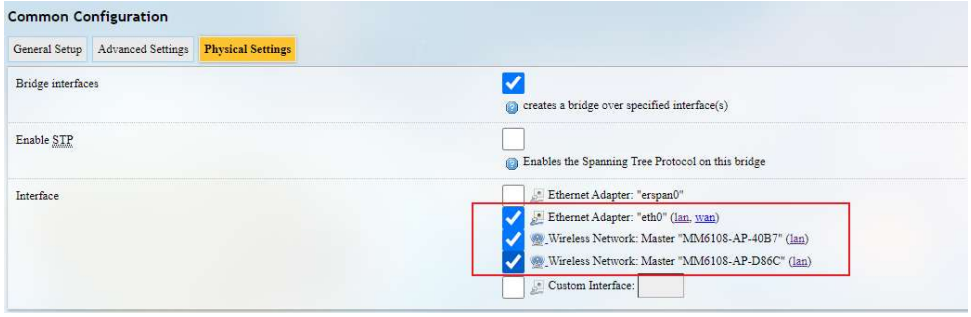
9. Uncheck the box before **Software VLAN: "eth0.10" (lan)** and save the change;



10. Navigate to **Network > Interfaces > LAN > Edit > Physical Settings** again;
11. Check the box before **Ethernet Adapter: "eth0" (wan)** and keep the other options unchanged;

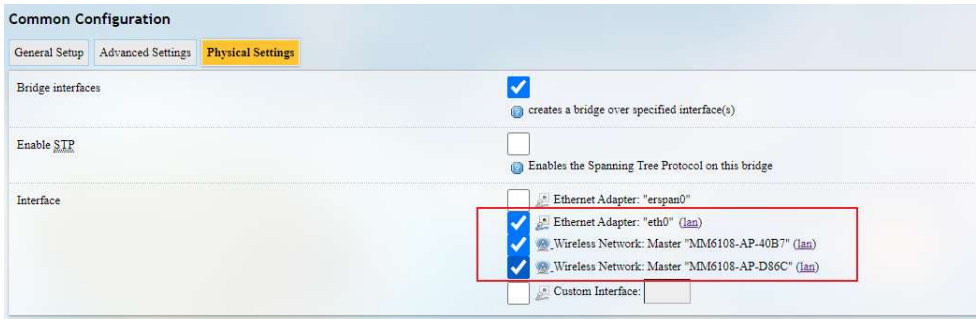


12. Save the changes and the LAN port settings will be as follows;



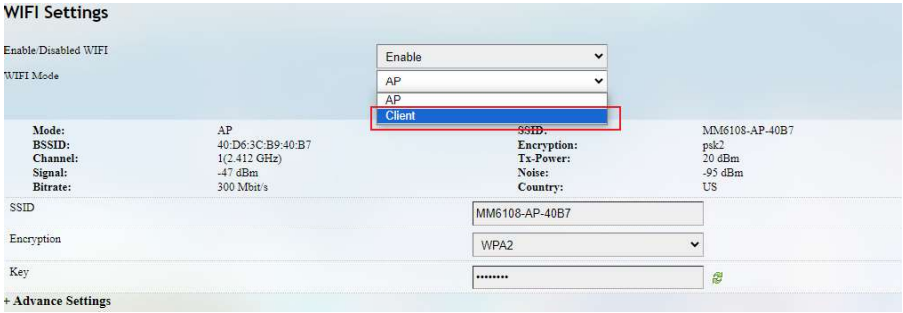
13. Return to the **Interfaces** window, and click the **Delete** button behind the WAN port to change the Ethernet jack of H1 to LAN;

14. After the WAN port is deleted, the LAN port status will be changed to the following:

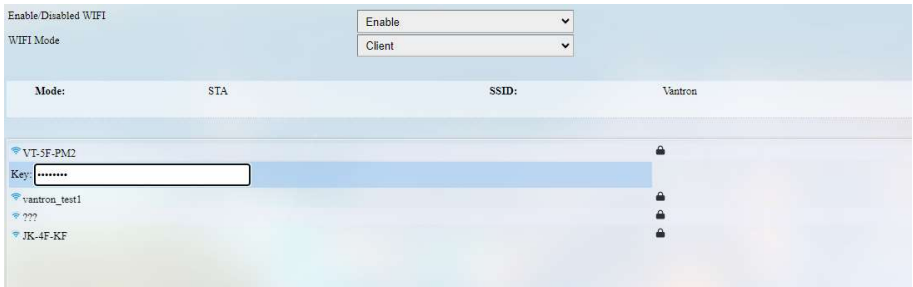


Steps 8-14 tell how to set the Ethernet jack from WAN to LAN for connecting the host computer. You can refer to 2.2.2 for VLAN settings on the host computer so that you can login VantronOS for HAP101 from the host computer without performing these steps.

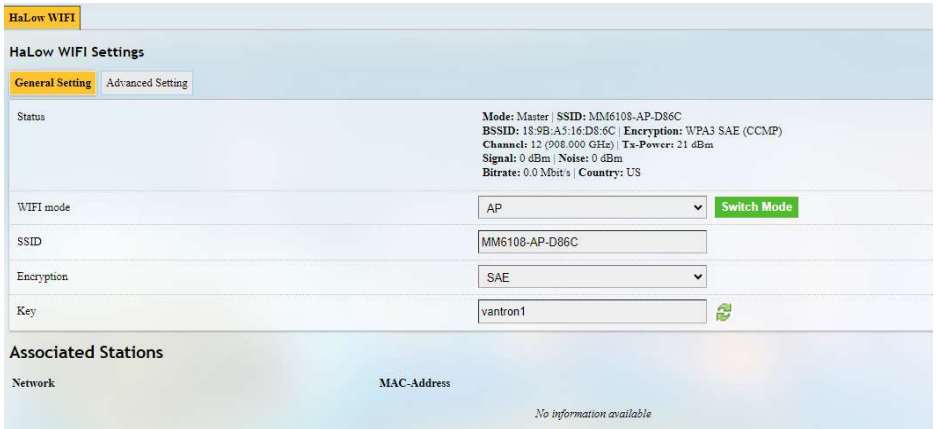
15. Use an Ethernet cable to connect H1 and PC1, and log in VantronOS for H1 with the gateway IP (LAN IP) set in step 6;
16. Navigate to **Network > Wireless (WIFI)**;
17. Change the mode of H1 to Wi-Fi client;



18. Power on the wireless router and connect it to Internet;
19. Return to the VantronOS web page;
20. Select the SSID of the wireless router and enter the password to connect H1 to the wireless router via 2.4GHz Wi-Fi;



21. Navigate to **Network > HaLow WIF;**
22. Make sure H1 is operating in the HaLow AP mode and take down its SSID, encryption protocol and password for future use in case the device label lacks such information.



4.3 Setup of H2 and H3 (HaLow STA mode)

1. Use the WLAN SSID and password provided on the device label to connect PC 2 to H2 via 2.4GHz Wi-Fi;
2. Identify the gateway IP of the 2.4GHz Wi-Fi as per step 2 in 4.2;
3. Log in to VantronOS for H2 as the super user using the gateway IP identified in the prior step;

   Super user: root password: rootpassword

4. Navigate to **Network > Halow WIFI > General Setting** to set the Wi-Fi HaLow mode of H2 to **Client**;

5. Connect H2 to H1 via Wi-Fi HaLow;

6. Navigate to **Network > Halow WIFI > Advanced Setting** and enable the **Relay** feature;

7. Follow the prior steps to connect H3 to H1 via Wi-Fi HaLow.

4.4 Setup of the Cameras and Connection Testing

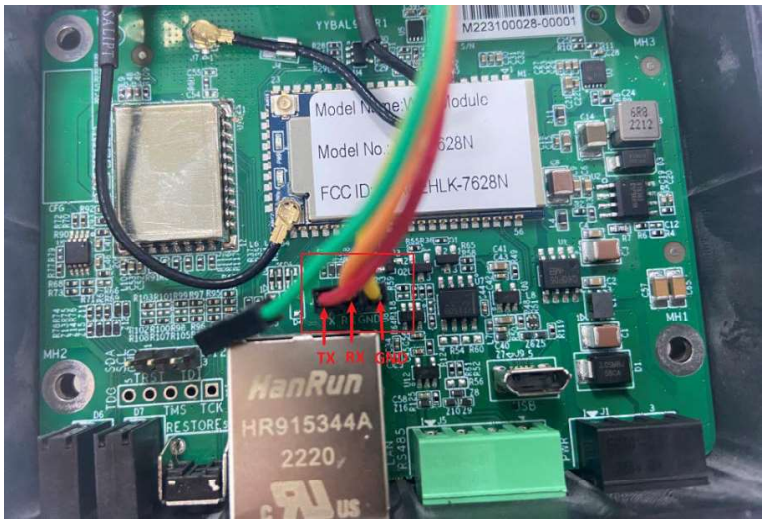
1. Use a USB Type-A to Type-C cable to connect HCAM26 HaLow IP camera to the host computer;
2. Enter the device shell and connect it to H1 via Wi-Fi HaLow using ABD commands;

   Next time the HaLow camera will re-connect to H1 automatically in case of unexpected failures.
3. Use an Ethernet cable to connect an Ethernet camera to H2;
4. Set a static IP address for the camera on the same network as H1 in case it cannot obtain a valid IP address automatically;
5. Use an Ethernet cable to connect PC 2 to H3, and PC 2 will automatically obtain an IP on the same network as H1;
6. Use the ping command with the destination Ethernet IP address to confirm whether PC 1 or PC 2 can receive replies from the cameras or the other PC. This will verify the connectivity between PC 1, PC 2, and the cameras;
7. Finally, PC 1, PC 2, and the cameras can access Internet through the wireless router, and you can use PC 1 or PC 2 to ping the other PC and the cameras.

CHAPTER 5 DEBUGGING THE DEVICE

In the event that you need to debug HAP101, please follow the steps below to set up the device.

1. Unscrew the upper cover of HAP101 from the bottom and remove it;
2. Find the debug UART (J2) located behind the RJ45 jack;
3. Use a USB-to-TTL adapter to connect the debug UART to a host computer (**TXD-RXD, RXD-TXD, GND-GND)**;



4. Power on HAP101 with a 12V DC power adapter;
5. Lauch a serial communication program and open a serial session for HAP101 using the parameters below.

Baud rate	Data bit	Polarity	Stop bit
57600	8	None	1

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 Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate this equipment.

RF Radiation Exposure Statement:

1. This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.
2. The device has been evaluated to meet general RF exposure requirement.

IC Statement

This device complies with ISED's licence-exempt RSSs. 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.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

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

1. Le dispositif ne doit pas produire de brouillage préjudiciable, et
2. Ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radio électrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.