HAP103 Wi-Fi HaLow Access Point

User Manual

Version: 1.2

Revision History:

No.	Description	Date
V1.0	First release	Feb 8, 2024
V1.1	Added instructions on MCU and BLE api	Mar. 8, 2024
V1.2	Updated description on Wiegand, BLE, and the relay connector	Jun. 7, 2024

Table of Contents

Foreword

Thank you for purchasing HAP103 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 HAP103 Wi-Fi HaLow access point ("the AP") conforms to the prominent IEEE 802.11ah (Wi-Fi HaLow) standard and IEEE 802.11 b/g/n (2.4GHz Wi-Fi). It offers a complete Wi-Fi connectivity solution for IoT developers who seek for wireless connections that prioritize energy efficiency, extended coverage, obstacle penetration, effortless accessibility, etc.

HAP103 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. With IEEE 802.11ah complied, HAP103 supports stable connection of over 8,000 clients in AP mode, making it an ideal solution for replacing complex networking requirements in confined spaces. It provides user options such as multiple I/Os for data transmission in access control scenarios. The optional PoE Powered Device (PD) feature eliminates the need for a separate power source, providing significant benefits in scenarios where efficient power management and connectivity are crucial.

HAP103 is designed for large-scale dense deployment of low-power stations to eliminate multiple access points in application scenarios such as access control systems, smart home appliances, surveillance systems, logistics and asset management, portables, and wearables.

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:

- HAP103 Wi-Fi HaLow access point
- 2 x 2.4GHz Wi-Fi antenna / 1 x 2.4GHz Wi-Fi antenna + 1 x BT 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
- 1 x Weigand input terminal connector
- 1 x Relay out terminal connector

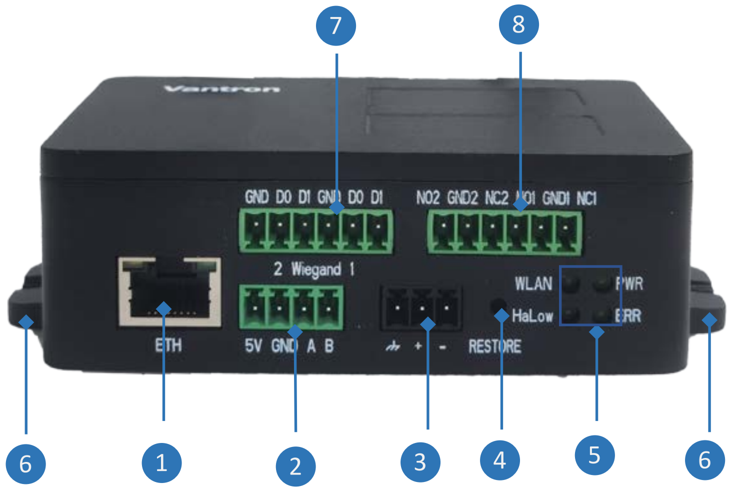
Actual accessories might vary slightly from the list above as the customer order might be different from the standard configuration options.

1.3 Specifications

HAP103			
System	CPU	MediaTek 580MHz MIPS® CPU	
	Wi-Fi HaLow SoC	Morse Micro MM6108	
	Memory	256MB	
	Storage	64MB	
Wireless communication	2.4GHz Wi-Fi	Standard: IEE 802.11 b/g/n	
		Frequency range: 2.412GHz ~ 2.484GHz	
		Channel bandwidth: 20/40 MHz	
		Data rate: up to 150 Mbps	
		Antenna: 2T2R	
	Wi-Fi HaLow	Standard: IEE 802.11 ah	
		Frequency range: 850MHz ~ 950 MHz	
		Channel bandwidth: 1/2/4/8 MHz	
		Data rate: up to 32.5 Mbps @8MHz or 15 Mbps @4MHz	
		Working mode: AP, STA configurable	
	Bluetooth	Optional	
I/O	Fast Ethernet	1 x RJ45, 10/100 Mbps (PoE PD optional)	
	Serial port (Optional)	1 x RS485 (4-pin terminal, 5V output, baud rate: 115200)	
	Antenna	1 x Wi-Fi HaLow SMA connector	
		1 x 2.4GHz Wi-Fi SMA connector	
		1 x 2.4GHz Wi-Fi / BT SMA connector	
	Relay (Optional)	2 x Relay out	
	Input (Optional)	2 x Weigand input (5V)	
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	122mm x 74mm x 35mm (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



Interface / Indicator	Description		
1	WAN port (100Mbps), operating in the WAN area by default		
2	RS485 (baud rate: 115200) / Debug UART (baud rate: 57600), switch by SW3 inside the device		
3	Power terminal (9V~40V DC)		
4	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
5	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	
6	Mounting brackets (screws recommended: M3 x 8mm)		
7	2 x Wiegand input connector (support 26/34-bit Wiegand protocol)		
8	2 x Relay output connector		

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

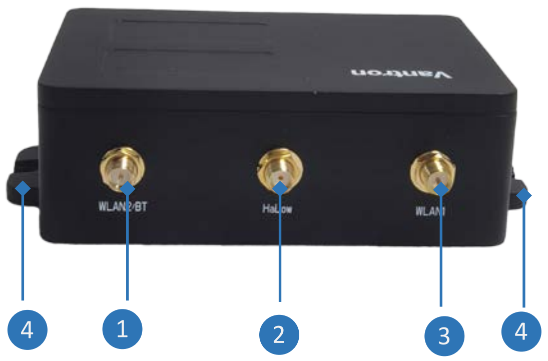
3. Error indicator

   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

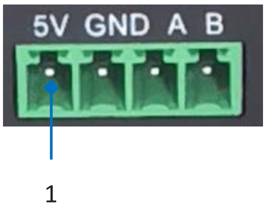
1.4.2 Back view



Interface	Description
1	Secondary 2.4GHz Wi-Fi/BT 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 Connector Pinout

1.5.1 Serial Port



HAP103 implements an RS485 port that supports both serial communication (baud rate: 115200) and device debugging (baud rate: 57600), with pinout as follows:

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

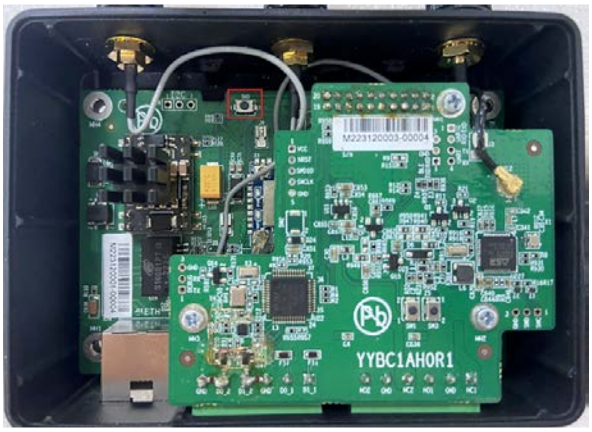
Port wiring: A-A, B-B, GND-GND

The RS485 port operates in the communication mode by default. Input the following command to open the port with a serial port communication program (e.g., microcom) for serial communication:

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

To switch to the debug mode, follow the steps below:

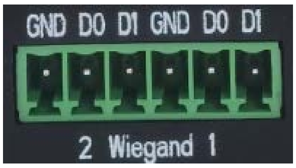
1. Unscrew the bottom screws of the device and remove the top cover;
2. Press the SW3 button inside the device and do **NOT** release;



3. Power on HAP103 and release the SW3 button.

The device will resume to the serial communication mode upon each reboot.

1.5.2 Wiegand Input



Connector	Wiegand Input					
Pin (left-right)	GND	D0	D1	GND	D0	D1
Port name	WIEGAND_D2			WIEGAND_D1		

Port wiring: D0-D0, D1-D1, GND-GND

Card swiping:

1. Connect a card read to WIEGAND_D2 or WIEGAND_D1;
2. Swipe the card and use the following command to retrieve the information.

```
# vt_data_query mcu
{"mcu":{"timestamp":1509,"wigand_num":1,"wigand_info":"d9a5c8"}}
```

When 'wigand_num' = 1, it signifies data from WIEGAND_D1. When 'wigand_num' = 2, it indicates data from WIEGAND_D2.

'wigand_info' displays the card number information.

MCU firmware upgrade for Wiegand:

1. Retrieve the 'session' value:

When interacting with vt_datacapture using curl, it is necessary to use a session (value for the 'token' parameter), and this value needs to be updated periodically;

```
~# curl -X POST -d '{"username": "root", "password": "rootpassword"}'
http://192.168.9.55/api/userlogin
{"token":"d38c6a46d05c01b5cba1ea71fc747d2d","restapi":["userlogin","*"]}
```

When 'Permission Denied' occurs, a new session is needed;

```
curl -X GET -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d'
http://192.168.9.55/api/dc/mcu/model_info
{"code":407,"desc":"Permission Denied"}
```

2. Upload firmware:

```
~# curl -F "file=@/home/mcu.bin" -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d' http://192.168.9.55/api/dc/mcu/upload
```

3. Upgrade firmware (upgrade is successful when no error is returned):

```
~# curl -X POST -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d' http://192.168.9.55/api/dc/mcu/upgrade
```

4. View MCU version information:

```
~# curl -X GET -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d' http://192.168.9.55/api/dc/mcu/model_info
{"model_info":{"version":"1.0.0.0","model":"000000000010"}}
```

1.5.3 Relay Output

Connector	Relay output					
Pin (left-right)	NO2	GND2	NC2	NO1	GND	NC1
Port	12V relay 2			12V relay 1		
Pinout	Default output	Ground	Controlled output	Default output	Ground	Controlled output

The relay power is turned off by default, and the commands for power control are applicable to both relays.

1. Turn on the power for both relays:

```
~# echo 1 > /sys/class/gpio/vantron:green:relays-en/value
```

2. Turn off the power for both relays (both relays will stop work):

```
~# echo 0 > /sys/class/gpio/vantron:green:relays-en/value
```

3. NO1 for relay 1 is enabled by default. Command for enabling it is:

```
~# echo 1 > /sys/class/gpio/vantron:green:relays1/value
```

4. Command for enabling NC1:

```
~# echo 0 > /sys/class/gpio/vantron:green:relays1/value
```

5. NO2 for relay 2 is enabled by default. Command for enabling it is:

```
~#  echo 1 > /sys/class/gpio/vantron:green:relays2/value
```

6. Command for enabling NC2:

```
~#  echo 0 > /sys/class/gpio/vantron:green:relays2/value
```

1.6 BLE Communication

Retrieve the ‘session’ value:

When interacting with vt_datacapture using curl, it is necessary to use a session (value for the ‘token’ parameter), and this value needs to be updated periodically;

```
~# curl -X POST -d '{"username": "root", "password": "rootpassword"}'
http://192.168.9.55/api/userlogin
{"token":"d38c6a46d05c01b5cba1ea71fc747d2d","restapi":["userlogin","*"]}
```

When ‘Permission Denied’ occurs, a new session is needed;

```
curl -X GET -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d'
http://192.168.9.55/api/dc/mcu/model_info
{"code":407,"desc":"Permission Denied"}
```

1.6.1 Pairing with a BLE Assistant

The BLE feature is enabled upon device bootup. You can download a BLE assistant for pairing with HAP103, which is usually named as ‘VT-DGL-AH’.

Once paired, you can enter the following command to check the connection status.

```
~# vt_data_query ble
{"ble":{"timestamp":1717741487,"MAC":"47:cd:eb:be:24:50","conn_status":1,"conn_mode":1}}
```

conn_status: 0 indicates a normal connection, 1 indicates a disconnected status

conn_mode: Indicates the connection mode: 0 (central), 1 (peripheral)

Central: Able to scan and connect to other BLE devices (this mode is currently not supported)

Peripheral: Can be connected to by other BLE devices

After pairing with a BLE assistant:

1. Send data to the BLE assistant from HAP103:

```
~# curl  -X POST -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d'
http://192.168.9.55/api/dc/ble/senddata -d '{"mode": 1, "data": "3132"}'
```

2. Receive data from the BLE assistant;

   1). Open the log to view the real-time data and data received previously;

   ```
   ~#  echo 1 > /tmp/data_capture/run/logger/config/logger.ble.enable
   ~#  echo 7 >/tmp/data_capture/run/logger/config/logger.ble.level
   ~#  tail -f /tmp/data_capture/log/ble.log
   <2024-06-07 06:11:28>  29 recv data : 1234qwe
   ```

   2). Send data from the BLE assistant (this is done on the debugger).

3. Disconnect the BLE assistant from HAP103:

```
~# curl  -X POST -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d'
http://192.168.9.55/api/dc/ble/disconn -d '{"mode": 1}'
```

1.6.2 BLE Firmware Upgrade

1. Upload firmware:

```
~# curl -F "file=@/home/ble.bin" -H 'Authentication: Session
d38c6a46d05c01b5cba1ea71fc747d2d' http://192.168.9.55/api/dc/ble/upload
```

2. Upgrade firmware:

```
~# curl -X POST -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d'
http://192.168.9.55/api/dc/ble/upgrade
```

3. View BLE version information:

```
~# curl -X GET -H 'Authentication: Session d38c6a46d05c01b5cba1ea71fc747d2d'
http://192.168.9.55/api/dc/ble/model_info
{"model_info":{"version":"1.0.0.1","model":"0f0000000000"}}
```

CHAPTER 2 GETTING STARTED

2.1 Setting up the Device

Before you proceed with configuration of HAP103 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 WLAN1 and WLAN2/BT antenna connectors;

   If there is only one WLAN antenna, install it to the WLAN1 connector.
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

HAP103 is designed to allow network connectivity with minimal configuration. That being said, you can configure the network settings and customize the device with the VantronOS interface.

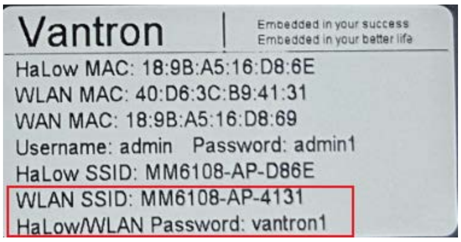
Depending on how the host computer is connected to the Internet, there are two ways to log in to VantronOS for HAP103.

Login Method	Internet Connection of the Host Computer	VantronOS Login by HAP103
Option 1	2.4GHz Wi-Fi connection to HAP103	Use the 2.4GHz WLAN IP of HAP103 as the login address
Option 2	Same Ethernet connection as HAP103	Use the WAN port IP of HAP103 as the login address

No matter which option you choose to log in to VantronOS for HAP103, it is important to note that the IP address of the host computer must be on the same network as HAP103. This network alignment is essential for successful connectivity and operation.

VantronOS Login via Option 1

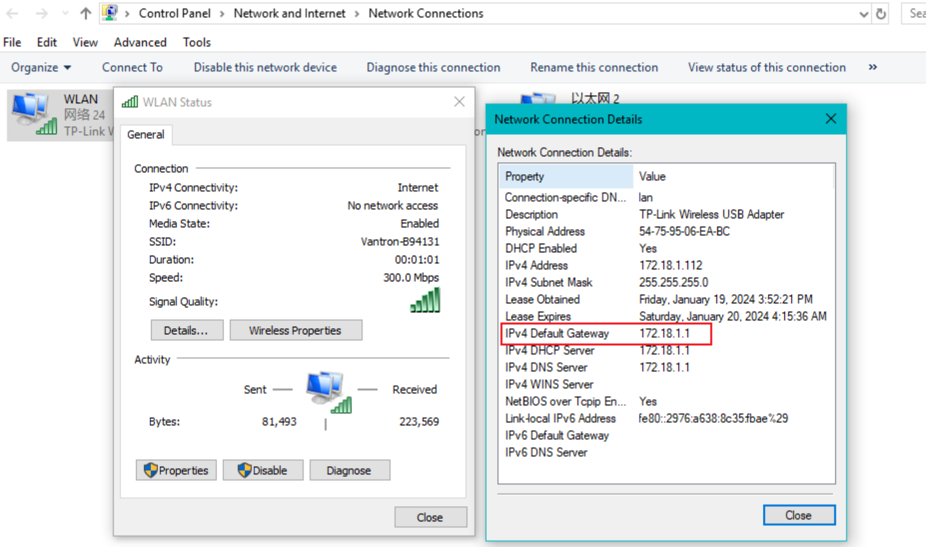
1. Power on the device and the 2.4GHz Wi-Fi will be operating in the AP mode by default;
2. Connect the host computer to the 2.4GHz Wi-Fi of the device using the SSID and default password provided on the device label (like the following);



Vantron | Embedded in your success Embedded in your better life

HaLow MAC: 18:9B:A5:16:D8:6E
WLAN MAC: 40:D6:3C:B9:41:31
WAN MAC: 18:9B:A5:16:D8:69
Username: admin Password: admin1
HaLow SSID: MM6108-AP-D86E
WLAN SSID: MM6108-AP-4131
HaLow/WLAN Password: vantron1

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



Control Panel > Network and Internet > Network Connections
File Edit View Advanced Tools
Organize Connect To Disable this network device Diagnose this connection Rename this connection View status of this connection
WLAN
网络 24
TP-Link V
以太网 2

WLAN Status

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
SSID:	Vantron-B94131
Duration:	00:01:01
Speed:	300.0 Mbps
Signal Quality:	

Activity

	Sent	Received
Bytes:	81,493	223,569

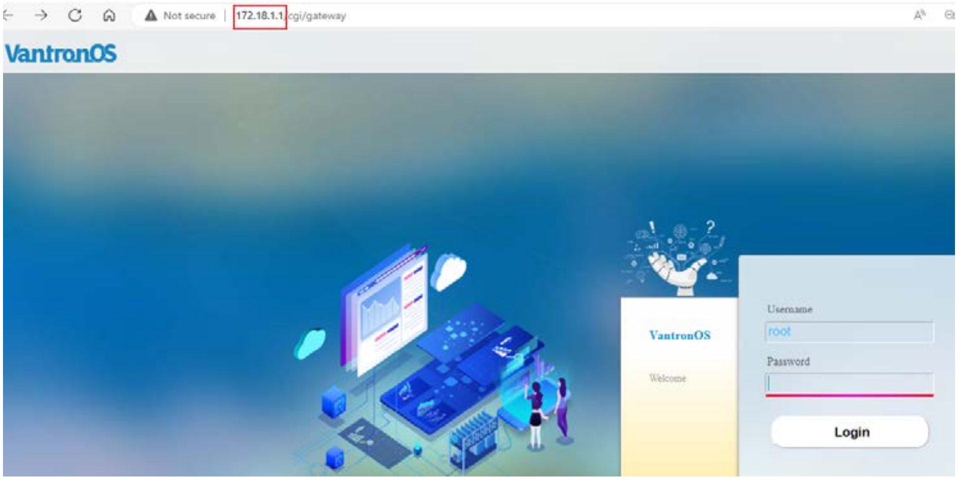
Details...
Wireless Properties
Properties
Disable
Diagnose
Close

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	lan
Description	TP-Link Wireless USB Adapter
Physical Address	54-75-95-06-EA-BC
DHCP Enabled	Yes
IPv4 Address	172.18.1.112
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, January 19, 2024 3:52:21 PM
Lease Expires	Saturday, January 20, 2024 4:15:36 AM
IPv4 Default Gateway	172.18.1.1
IPv4 DHCP Server	172.18.1.1
IPv4 DNS Server	172.18.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::2976:a638:8c35:fbae%29
IPv6 Default Gateway	
IPv6 DNS Server	

4. Use the gateway IP of the prior step as the address for VantronOS login;

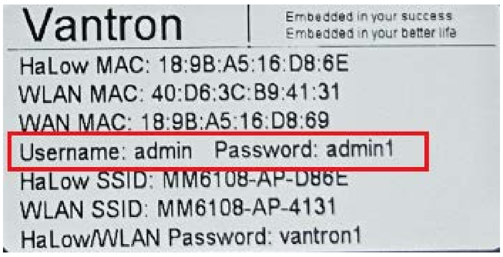


Not secure | 172.18.1.1/cgi/gateway

Username: root

Password:

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



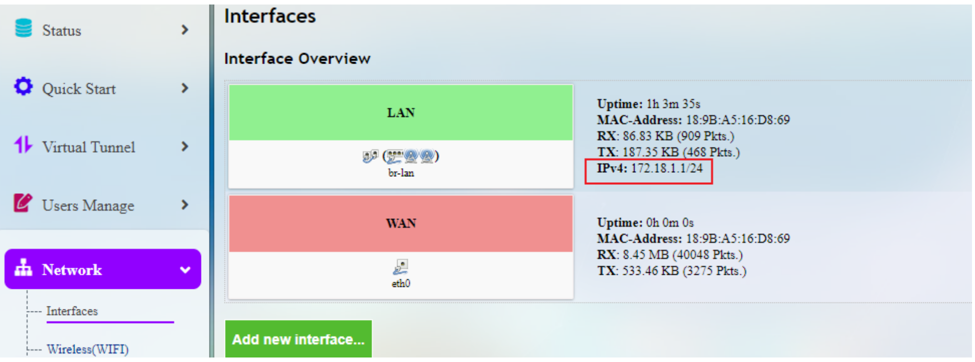
Vantron | Embedded in your success
Embedded in your better life

HaLow MAC: 18:9B:A5:16:D8:6E
WLAN MAC: 40:D6:3C:B9:41:31
WAN MAC: 18:9B:A5:16:D8:69
Username: admin Password: admin1
HaLow SSID: MM6108-AP-D86E
WLAN SSID: MM6108-AP-4131
HaLow/WLAN Password: vantron1

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).



Interfaces

Interface Overview

LAN
br-lan

Uptime: 1h 3m 35s
MAC-Address: 18:9B:A5:16:D8:69
RX: 86.83 KB (909 Pkts.)
TX: 187.35 KB (468 Pkts.)
IPv4: 172.18.1.1/24

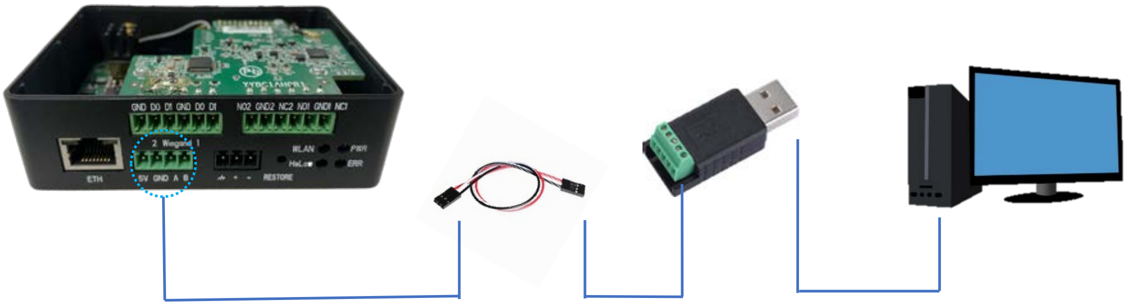
WAN
eth0

Uptime: 0h 0m 0s
MAC-Address: 18:9B:A5:16:D8:69
RX: 8.45 MB (40048 Pkts.)
TX: 533.46 KB (3275 Pkts.)

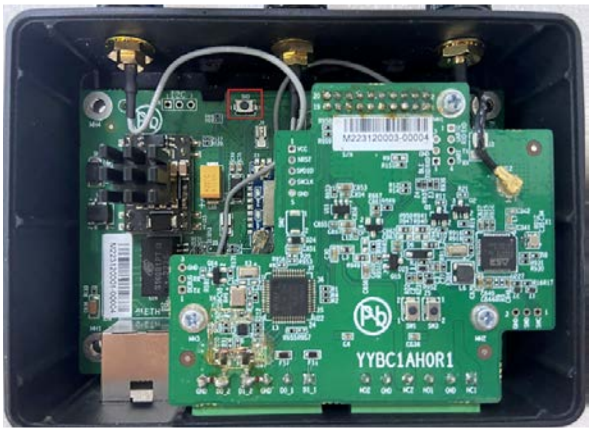
VantronOS Login via Option 2

Since the Ethernet jack of HAP103 operates in the WAN area by default, the WAN port IP address of the device can be identified by engaging the debug UART.

1. Connect the host computer to a router/switch for Internet access;
2. Connect HAP103 to the same router/switch using an Ethernet cable;
3. Unscrew the bottom screws of the device and remove the top cover;
4. Use an RS485 to USB adapter and DuPont wires or other way to connect HAP103 to the host computer;



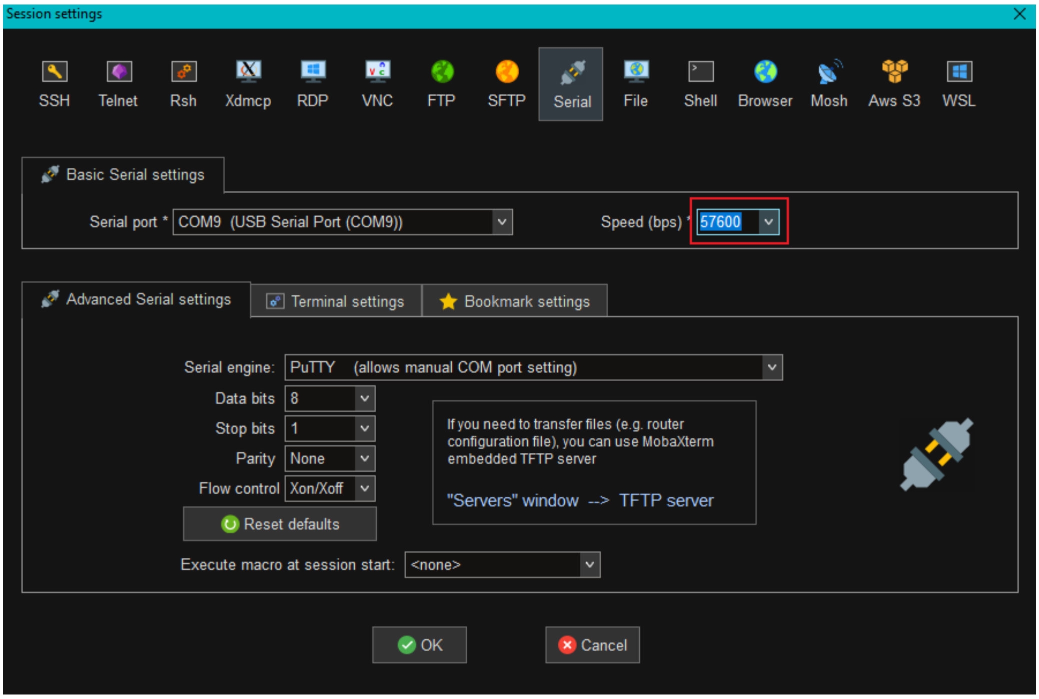
5. Press the SW3 button inside the device and do **NOT** release;



6. Power on HAP103 and release the SW3 button;

7. Open a serial emulator and launch a serial session for HAP103 using the following parameters;

Baud rate	Data bit	Polarity	Stop bit
57600	8	None	1



Session settings

Basic Serial settings

Serial port * COM9 (USB Serial Port (COM9))

Speed (bps) * 57600

Advanced Serial settings

Serial engine: PuTTY (allows manual COM port setting)

Data bits 8

Stop bits 1

Parity None

Flow control Xon/Xoff

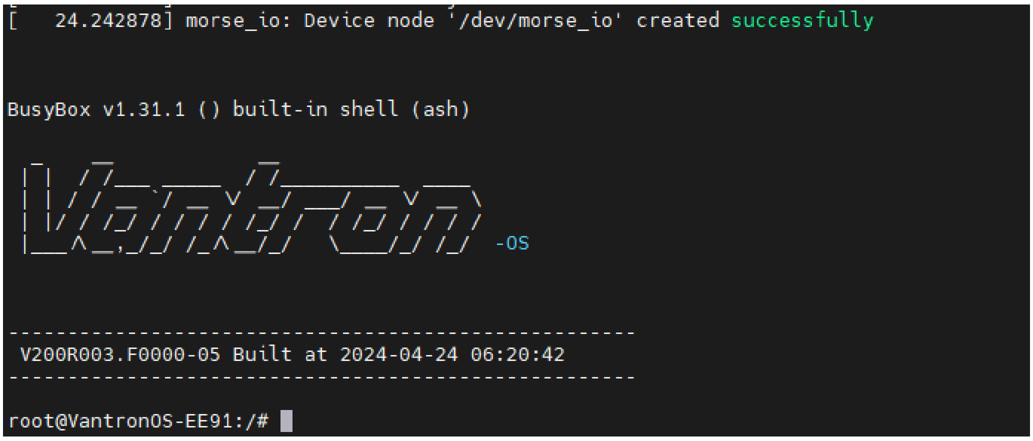
If you need to transfer files (e.g. router configuration file), you can use MobaXterm embedded TFTP server

"Servers" window --> TFTP server

Execute macro at session start: <none>

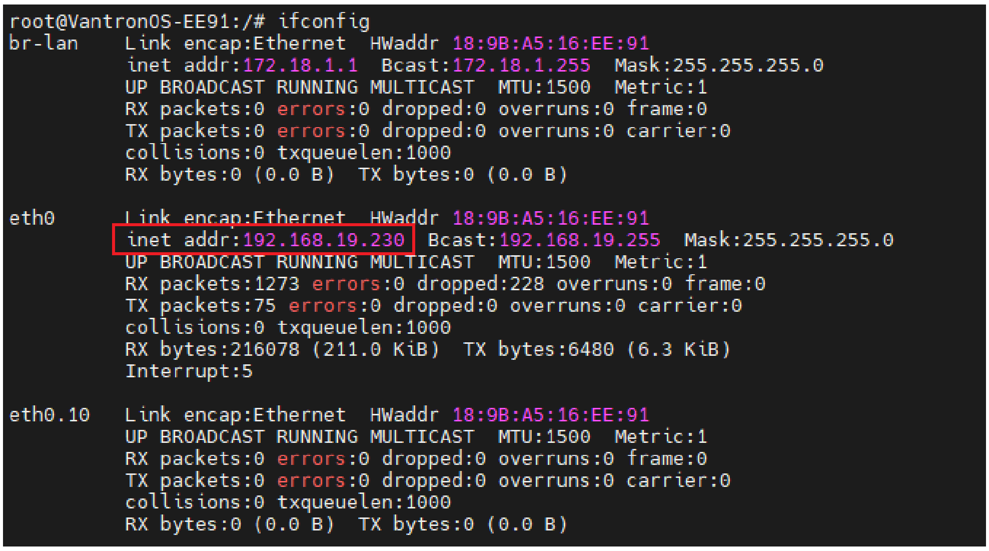
8. Wait for the printing process of the device information;

9. When the message for successful device creation appears, press **Enter**;



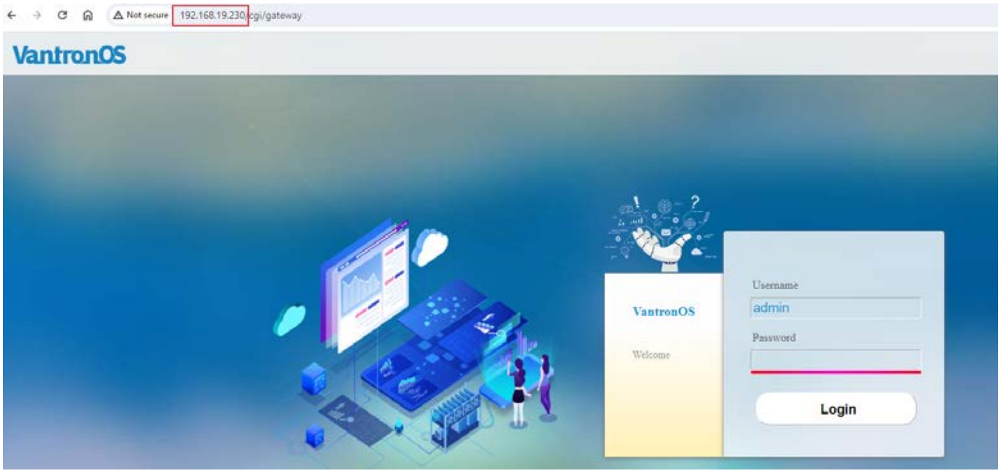
```
[   24.242878] morse_io: Device node '/dev/morse_io' created successfully


BusyBox v1.31.1 () built-in shell (ash)

 _    __            __
| |  / /___ _____  / /__________  ____
| | / / __ `/ __ \/ __/ ___/ __ \/ __ \
| |/ / /_/ / / / / /_/ /  / /_/ / / / /
|___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -OS


-----------------------------------------------------------
 V200R003.F0000-05 Built at 2024-04-24 06:20:42
-----------------------------------------------------------

root@VantronOS-EE91:/#
```

10. Execute the command ifconfig to check out the WAN port IP address of the device;

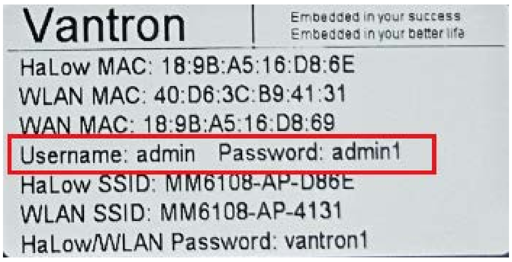


```
root@VantronOS-EE91:/# ifconfig
br-lan    Link encap:Ethernet  HWaddr 18:9B:A5:16:EE:91
          inet addr:172.18.1.1  Bcast:172.18.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0      Link encap:Ethernet  HWaddr 18:9B:A5:16:EE:91
          inet addr:192.168.19.230  Bcast:192.168.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1273 errors:0 dropped:228 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:216078 (211.0 KiB)  TX bytes:6480 (6.3 KiB)
          Interrupt:5

eth0.10   Link encap:Ethernet  HWaddr 18:9B:A5:16:EE:91
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

11. Use the WAN port IP of HAP103 as the address for VantronOS login;



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



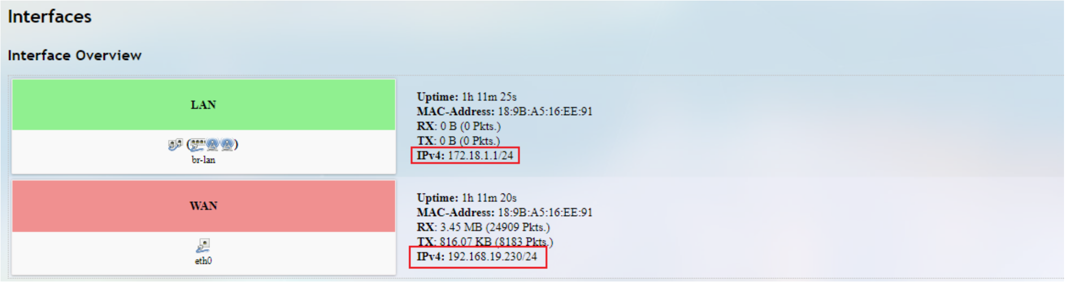
Vantron | Embedded in your success
Embedded in your better life

HaLow MAC: 18:9B:A5:16:D8:6E
WLAN MAC: 40:D6:3C:B9:41:31
WAN MAC: 18:9B:A5:16:D8:69
Username: admin   Password: admin1
HaLow SSID: MM6108-AP-D86E
WLAN SSID: MM6108-AP-4131
HaLow/WLAN Password: vantron1

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

Super user: root   //   password: rootpassword

13. Navigate to **Network > Interfaces** to check the network port information of HAP103.



Interfaces

Interface Overview

LAN

br-lan

Uptime: 1h 11m 25s
MAC-Address: 18:9B:A5:16:EE:91
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 172.18.1.1/24

WAN

eth0

Uptime: 1h 11m 20s
MAC-Address: 18:9B:A5:16:EE:91
RX: 3.45 MB (24909 Pkts.)
TX: 816.07 KB (8183 Pkts.)
IPv4: 192.168.19.230/24

2.3 SSH Login

Depending on how the host computer is connected to the Internet, there are two ways for the SSH login of HAP103.

Option 1— 2.4GHz Wi-Fi connection to HAP103: Use the 2.4GHz WLAN IP of the device as the login address.

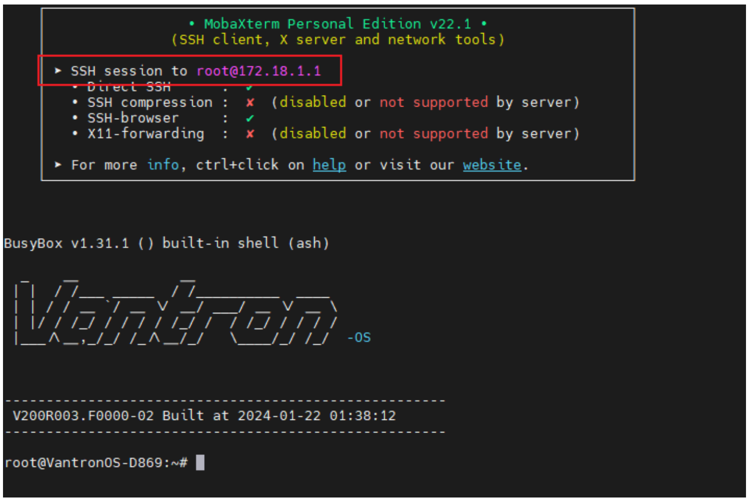
Option 2— Same Ethernet connection as HAP103: Use the WAN port IP of the device as the login address.

Make sure the IP address of the host computer is on the same network as HAP103. Refer to 2.2 for how to identify the2.4GHz 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.

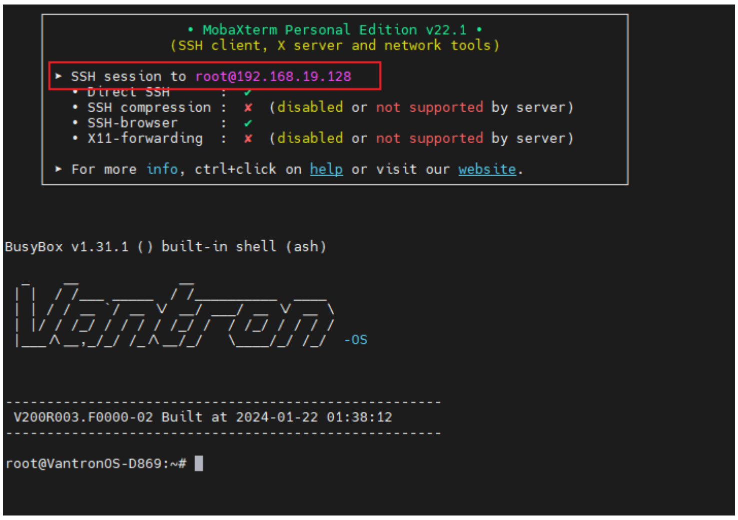
Port	Account	Password
22	root	rootpassword

SSH login with the 2.4GHz WLAN IP of HAP103:



```
              • MobaXterm Personal Edition v22.1 •
            (SSH client, X server and network tools)

 ➤ SSH session to root@172.18.1.1
   • Direct SSH      :  ✓
   • SSH compression :  ✘  (disabled or not supported by server)
   • SSH-browser     :  ✓
   • X11-forwarding  :  ✘  (disabled or not supported by server)

 ➤ For more info, ctrl+click on help or visit our website.


BusyBox v1.31.1 () built-in shell (ash)

-----------------------------------------------------
 V200R003.F0000-02 Built at 2024-01-22 01:38:12
-----------------------------------------------------

root@VantronOS-D869:~#
```

SSH login with the WAN port IP of HAP103:



```
              • MobaXterm Personal Edition v22.1 •
            (SSH client, X server and network tools)

 ➤ SSH session to root@192.168.19.128
   • Direct SSH      :  ✓
   • SSH compression :  ✘  (disabled or not supported by server)
   • SSH-browser     :  ✓
   • X11-forwarding  :  ✘  (disabled or not supported by server)

 ➤ For more info, ctrl+click on help or visit our website.


BusyBox v1.31.1 () built-in shell (ash)

-----------------------------------------------------
 V200R003.F0000-02 Built at 2024-01-22 01:38:12
-----------------------------------------------------

root@VantronOS-D869:~#
```

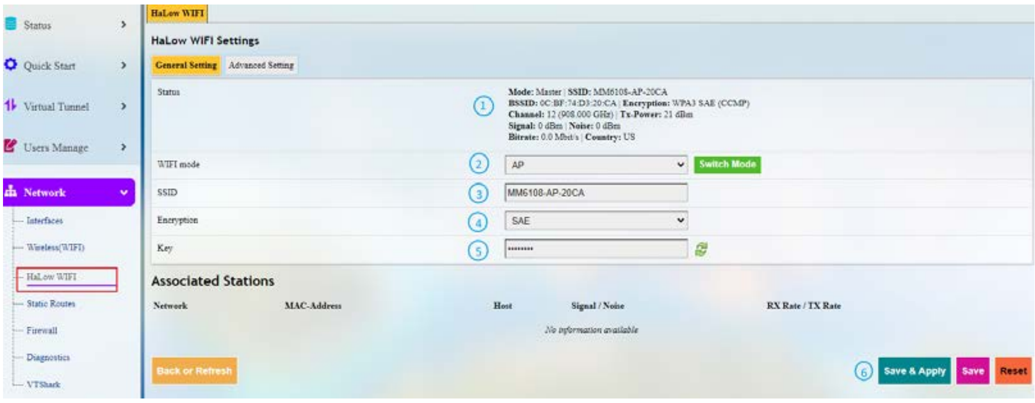
2.4 Wi-Fi HaLow Connection

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;



HaLow WIFI Settings

Status: **Mode:** Master | **SSID:** MM6108-AP-20CA
BSSID: 0C:BF:74:D3:20:CA | **Encryption:** WPA3 SAE (CCMP)
Channel: 12 (908.000 GHz) | **Tx-Power:** 21 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

WIFI mode: AP

SSID: MM6108-AP-20CA

Encryption: SAE

Key: ••••••••

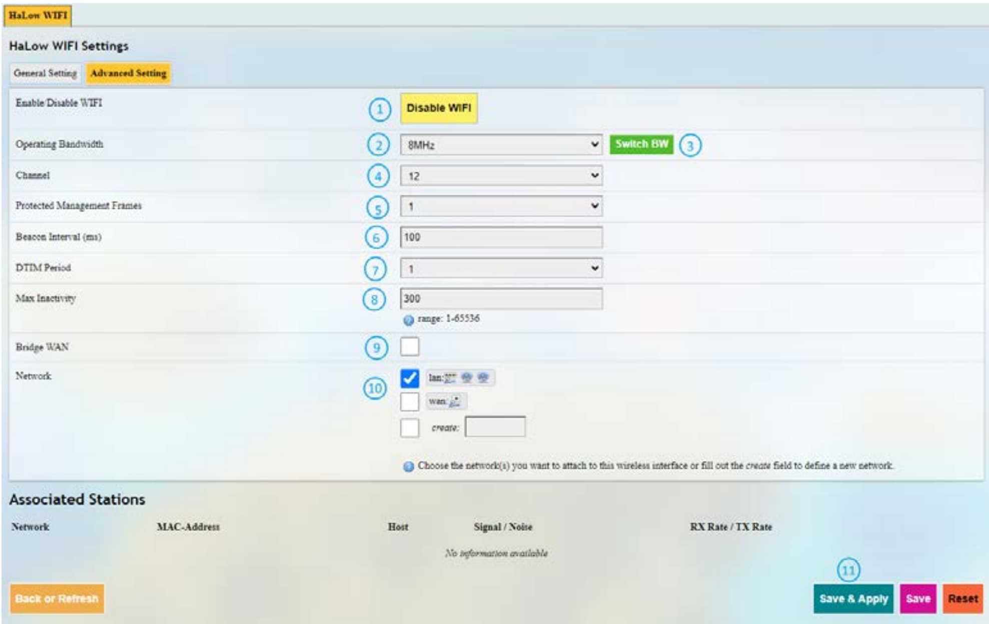
Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
			No information available	

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;



HaLow WIFI Settings

Enable/Disable WIFI	Disable WIFI
Operating Bandwidth	8MHz
Channel	12
Protected Management Frames	1
Beacon Interval (ms)	100
DTIM Period	1
Max Inactivity	300 range: 1-65536
Bridge WAN	□
Network	☑ lan: □ wan: □ *create:* Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
No information available				

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)

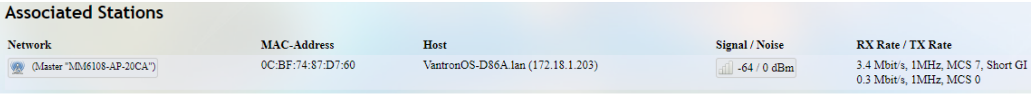
9) Select to bridge the interface to WAN or not

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 HAP103 for HaLow connection, then check the connection status in VantronOS (**Network > HaLow WIFI > Associated Stations**) for the AP-mode HAP103.



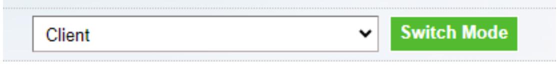
Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
(Master "MM6108-AP-20CA")	0C:BF:74:87:D7:60	VantronOS-D86A.lan (172.18.1.203)	-64 / 0 dBm	3.4 Mbit/s, 1MHz, MCS 7, Short GI 0.3 Mbit/s, 1MHz, MCS 0

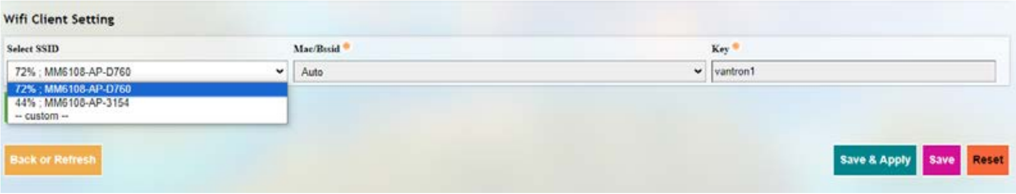
2.4.2 Station mode

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;


Client

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;

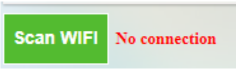

Wifi Client Setting

Select SSID: 72% ; MM6108-AP-D760
72% ; MM6108-AP-D760
44% ; MM6108-AP-3154
-- custom --

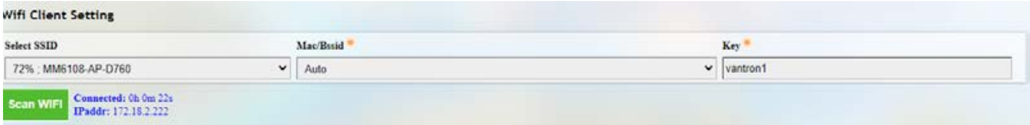
Mac/Bssid: Auto

Key: vantron1

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


No connection

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


Wifi Client Setting

Select SSID: 72% ; MM6108-AP-D760

Mac/Bssid: Auto

Key: vantron1

Connected: 0h 0m 22s
IPaddr: 172.18.2.222

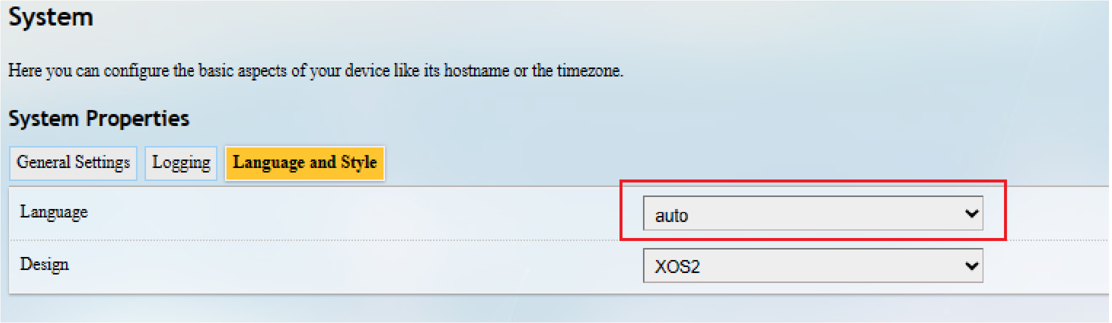
2.5 Password Change

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**.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Language: auto

Design: XOS2

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

English: English interface

Simplified Chinese: Simplified Chinese interface

CHAPTER 3 DEVICE SETUP IN VANTRONOS

3.1 Introduction to VantronOS

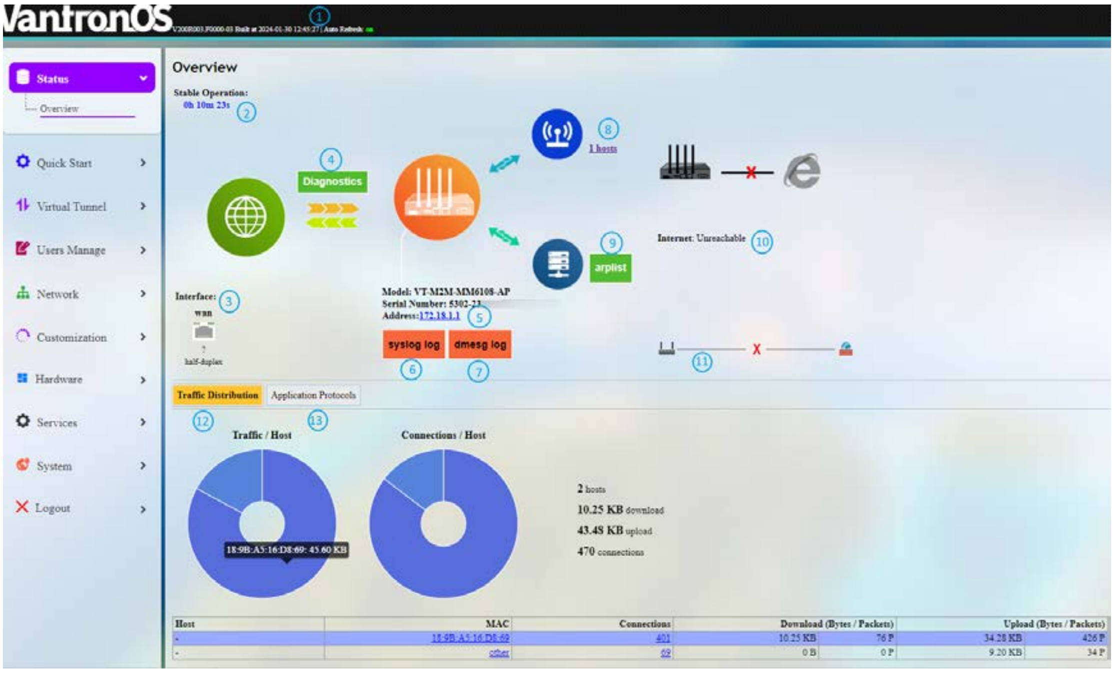
VantronOS is an intelligent operating system developed by the Vantron team, featuring independent system and function development. It is built upon the Linux system and optimized for embedded hardware. The operating system follows a modular design and plug-in expansion approach, utilizing the Linux kernel 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 HAP103, including stable operation duration, number of devices connected to the device, default routing, hardware information, traffic statistics, etc.



Host	MAC	Connections	Download (Bytes / Packets)		Upload (Bytes / Packets)	
-	18:9B:A5:16:D8:69	401	10.25 KB	76 P	34.28 KB	426 P
-	other	69	0 B	0 P	9.20 KB	34 P

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.

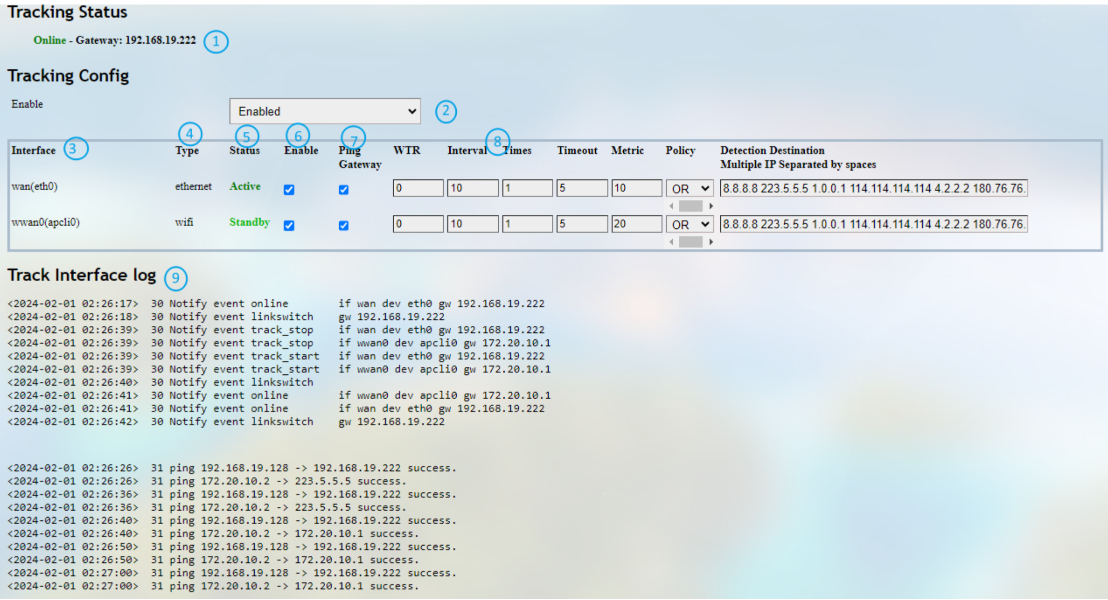
13. Traffic of application layer protocols

3.3 Quick Start— Auto Routing

Automatic routing might be beneficial when HAP103 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.



Tracking Status

Online - Gateway: 192.168.19.222 (1)

Tracking Config

Enable: Enabled (2)

Interface (3)	Type (4)	Status (5)	Enable (6)	Ping Gateway (7)	WTR	Interval (8)	Times	Timeout	Metric	Policy	Detection Destination Multiple IP Separated by spaces
wan(eth0)	ethernet	Active	☑	☑	0	10	1	5	10	OR	8.8.8.8 223.5.5.5 1.0.0.1 114.114.114.114 4.2.2.2 180.76.76.
wwan0(apcli0)	wifi	Standby	☑	☑	0	10	1	5	20	OR	8.8.8.8 223.5.5.5 1.0.0.1 114.114.114.114 4.2.2.2 180.76.76.

Track Interface log (9)

```
<2024-02-01 02:26:17>  30 Notify event online       if wan dev eth0 gw 192.168.19.222
<2024-02-01 02:26:18>  30 Notify event linkswitch   gw 192.168.19.222
<2024-02-01 02:26:39>  30 Notify event track_stop   if wan dev eth0 gw 192.168.19.222
<2024-02-01 02:26:39>  30 Notify event track_stop   if wwan0 dev apcli0 gw 172.20.10.1
<2024-02-01 02:26:39>  30 Notify event track_start  if wan dev eth0 gw 192.168.19.222
<2024-02-01 02:26:39>  30 Notify event track_start  if wwan0 dev apcli0 gw 172.20.10.1
<2024-02-01 02:26:40>  30 Notify event linkswitch
<2024-02-01 02:26:41>  30 Notify event online       if wwan0 dev apcli0 gw 172.20.10.1
<2024-02-01 02:26:41>  30 Notify event online       if wan dev eth0 gw 192.168.19.222
<2024-02-01 02:26:42>  30 Notify event linkswitch   gw 192.168.19.222


<2024-02-01 02:26:26>  31 ping 192.168.19.128 -> 192.168.19.222 success.
<2024-02-01 02:26:26>  31 ping 172.20.10.2 -> 223.5.5.5 success.
<2024-02-01 02:26:36>  31 ping 192.168.19.128 -> 192.168.19.222 success.
<2024-02-01 02:26:36>  31 ping 172.20.10.2 -> 223.5.5.5 success.
<2024-02-01 02:26:40>  31 ping 192.168.19.128 -> 192.168.19.222 success.
<2024-02-01 02:26:40>  31 ping 172.20.10.2 -> 172.20.10.1 success.
<2024-02-01 02:26:50>  31 ping 192.168.19.128 -> 192.168.19.222 success.
<2024-02-01 02:26:50>  31 ping 172.20.10.2 -> 172.20.10.1 success.
<2024-02-01 02:27:00>  31 ping 192.168.19.128 -> 192.168.19.222 success.
<2024-02-01 02:27:00>  31 ping 172.20.10.2 -> 172.20.10.1 success.
```

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

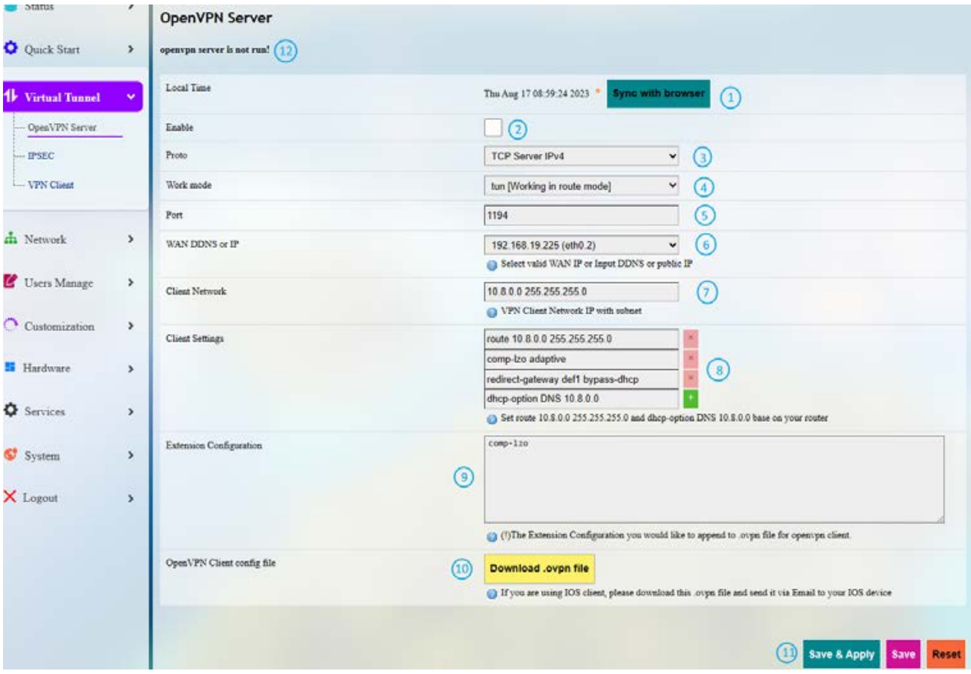
3.4 Virtual Tunnel

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.



OpenVPN Server

openvpn server is not run!

Local Time: Thu Aug 17 08:59:24 2023 * Sync with browser

Enable: □

Proto: TCP Server IPv4

Work mode: tun [Working in route mode]

Port: 1194

WAN DDNS or IP: 192.168.19.225 (eth0.2)
Select valid WAN IP or Input DDNS or public IP

Client Network: 10.8.0.0 255.255.255.0
VPN Client Network IP with subnet

Client Settings:
route 10.8.0.0 255.255.255.0
comp-lzo adaptive
redirect-gateway def1 bypass-dhcp
dhcp-option DNS 10.8.0.0
Set route 10.8.0.0 255.255.255.0 and dhcp-option DNS 10.8.0.0 base on your router

Extension Configuration: comp-lzo
(!)The Extension Configuration you would like to append to .ovpn file for openvpn client.

OpenVPN Client config file: Download .ovpn file
If you are using IOS client, please download this .ovpn file and send it via Email to your IOS device

Save & Apply | Save | Reset

Follow the steps below to build an OpenVPN server:

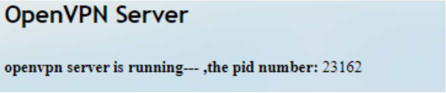
1. Synchronize the device time with the browser (local) time;
2. Enable the server or not after the server is built;
3. Select a protocol (TCP by default);

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.



OpenVPN Server

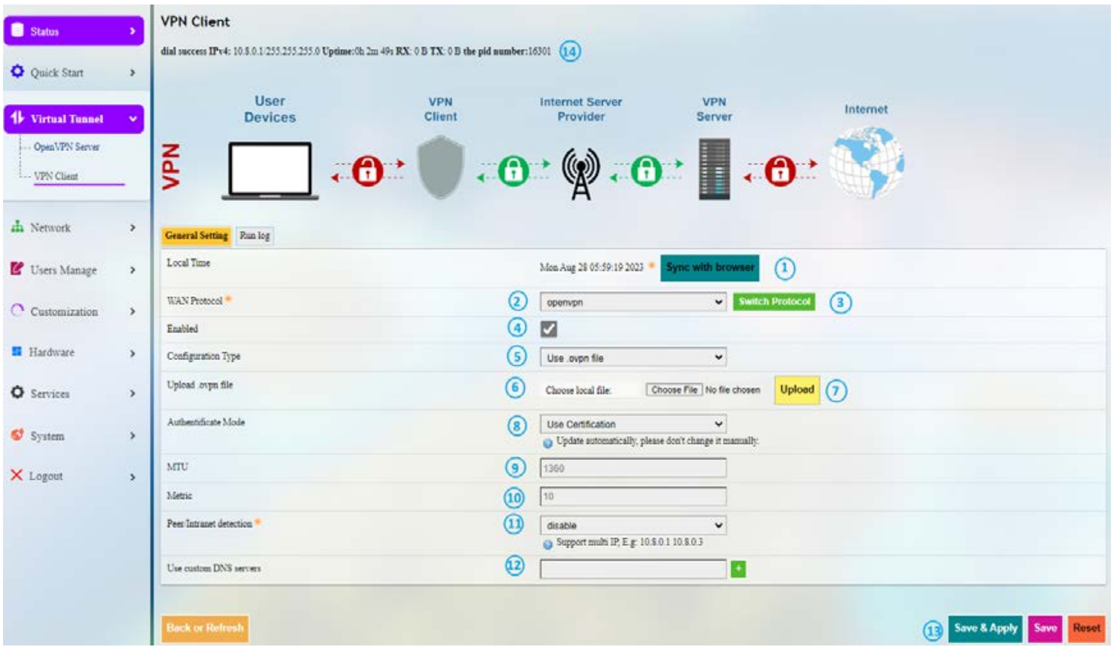
openvpn server is running--- ,the pid number: 23162

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 HAP103 to a VPN server and use it as a client, navigate to **Virtual Tunnel > VPN Client** for specific settings.



VPN Client

dial success IPv4: 10.8.0.1/255.255.255.0 Uptime:0h 2m 49s RX: 0 B TX: 0 B the pid number:16301

Local Time: Mon Aug 28 05:59:19 2023

WAN Protocol *: openvpn

Enabled: ☑

Configuration Type: Use .ovpn file

Upload .ovpn file: Choose local file: No file chosen

Authentificate Mode: Use Certification
Update automatically, please don't change it manually.

MTU: 1360

Metric: 10

Peer Intranet detection *: disable
Support multi IP, E.g: 10.8.0.1 10.8.0.3

Use custom DNS servers:

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

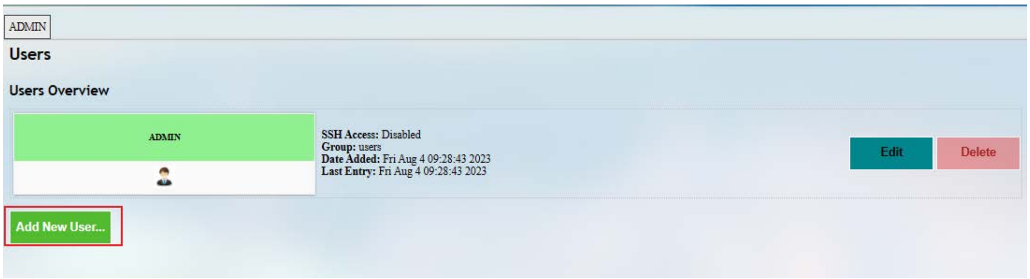
*Select **custom** and enter the IP address for heartbeat detection to enable the mechanism.*

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.



ADMIN

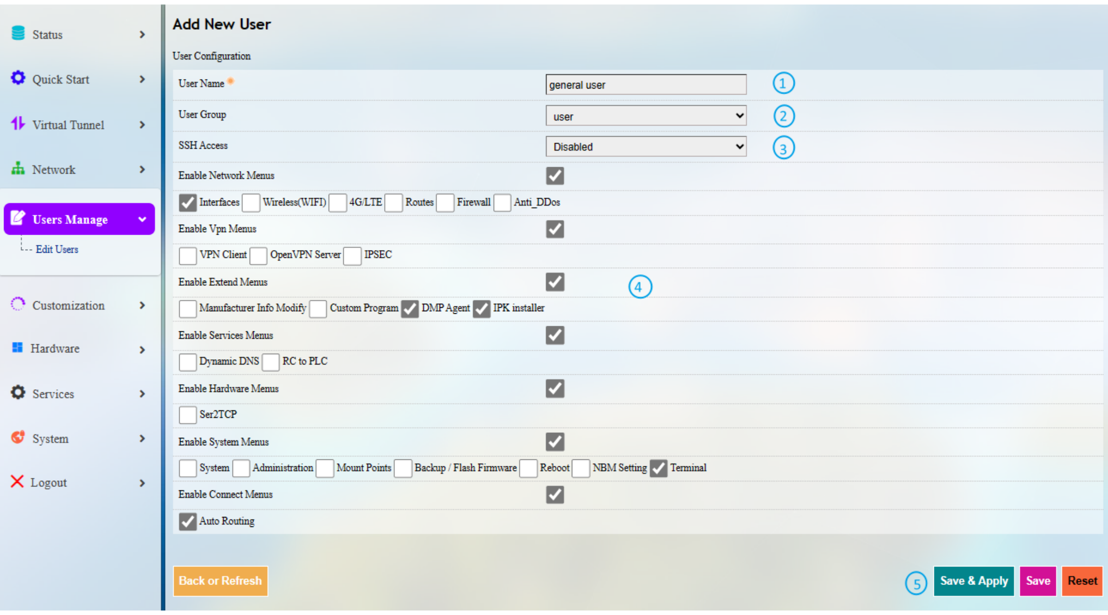
Users

Users Overview

ADMIN

SSH Access: Disabled
Group: users
Date Added: Fri Aug 4 09:28:43 2023
Last Entry: Fri Aug 4 09:28:43 2023

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



Add New User

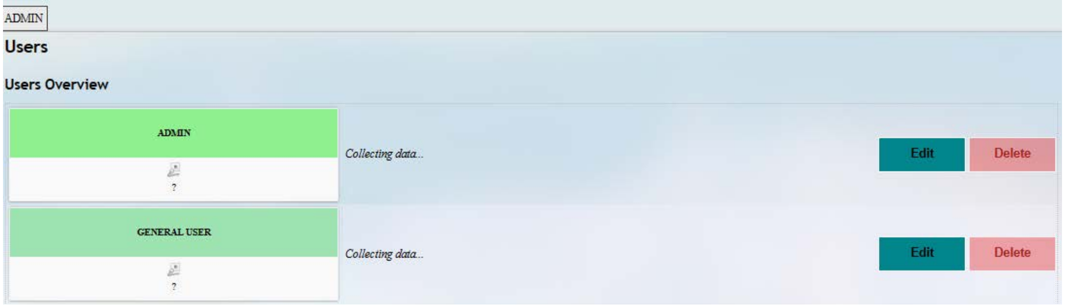
User Configuration

User Name * general user ①
User Group user ②
SSH Access Disabled ③
Enable Network Menus ☑
☑ Interfaces □ Wireless(WIFI) □ 4G/LTE □ Routes □ Firewall □ Anti_DDos
Enable Vpn Menus ☑
□ VPN Client □ OpenVPN Server □ IPSEC
Enable Extend Menus ☑ ④
□ Manufacturer Info Modify □ Custom Program ☑ DMP Agent ☑ IPK installer
Enable Services Menus ☑
□ Dynamic DNS □ RC to PLC
Enable Hardware Menus ☑
□ Ser2TCP
Enable System Menus ☑
□ System □ Administration □ Mount Points □ Backup / Flash Firmware □ Reboot □ NBM Setting ☑ Terminal
Enable Connect Menus ☑
☑ Auto Routing

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.



Users

Users Overview

ADMIN
?
Collecting data...

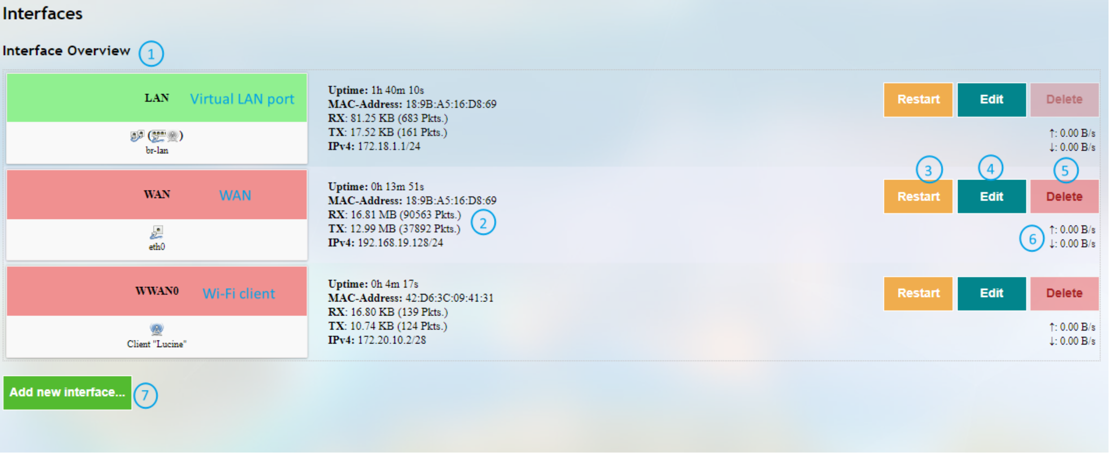
GENERAL USER
?
Collecting data...

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**.



Interfaces

Interface Overview

LAN Virtual LAN port
br-lan

Uptime: 1h 40m 10s
MAC-Address: 18:9B:A5:16:D8:69
RX: 81.25 KB (683 Pkts.)
TX: 17.52 KB (161 Pkts.)
IPv4: 172.18.1.1/24

↑: 0.00 B/s
↓: 0.00 B/s

WAN WAN
eth0

Uptime: 0h 13m 51s
MAC-Address: 18:9B:A5:16:D8:69
RX: 16.81 MB (90563 Pkts.)
TX: 12.99 MB (37892 Pkts.)
IPv4: 192.168.19.128/24

↑: 0.00 B/s
↓: 0.00 B/s

WWAN0 Wi-Fi client
Client "Lucine"

Uptime: 0h 4m 17s
MAC-Address: 42:D6:3C:09:41:31
RX: 16.80 KB (139 Pkts.)
TX: 10.74 KB (124 Pkts.)
IPv4: 172.20.10.2/28

↑: 0.00 B/s
↓: 0.00 B/s

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.

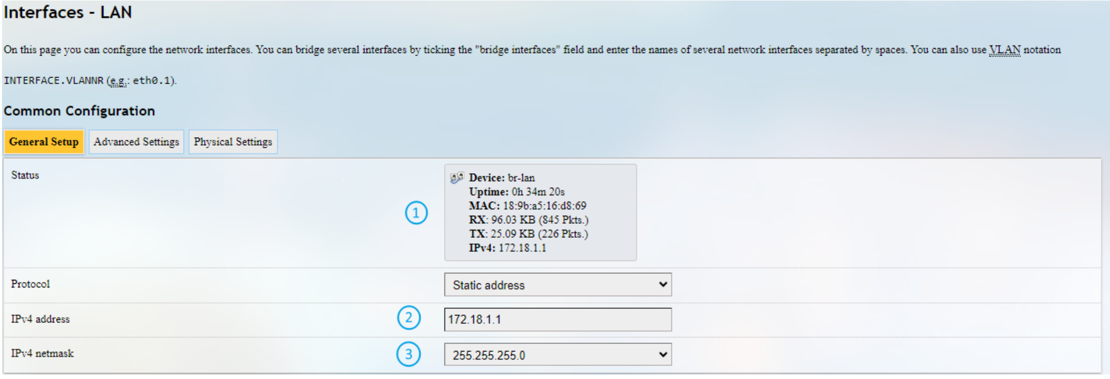
The following section illustrates on how to edit the network interfaces.

3.6.1.1 LAN

The bridged LAN port is for assigning IP addresses to clients connected to HAP103 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.



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Advanced Settings | Physical Settings

Status ① **Device:** br-lan
Uptime: 0h 34m 20s
MAC: 18:9b:a5:16:d8:69
RX: 96.03 KB (845 Pkts.)
TX: 25.09 KB (226 Pkts.)
IPv4: 172.18.1.1

Protocol: Static address

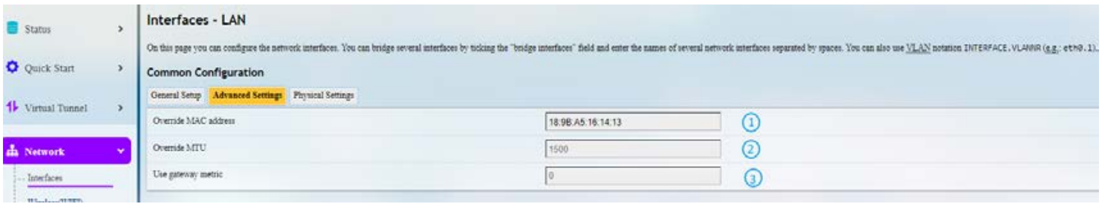
IPv4 address ②: 172.18.1.1

IPv4 netmask ③: 255.255.255.0

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:



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Advanced Settings | Physical Settings

Override MAC address: 18:9B:A5:16:14:13 ①

Override MTU: 1500 ②

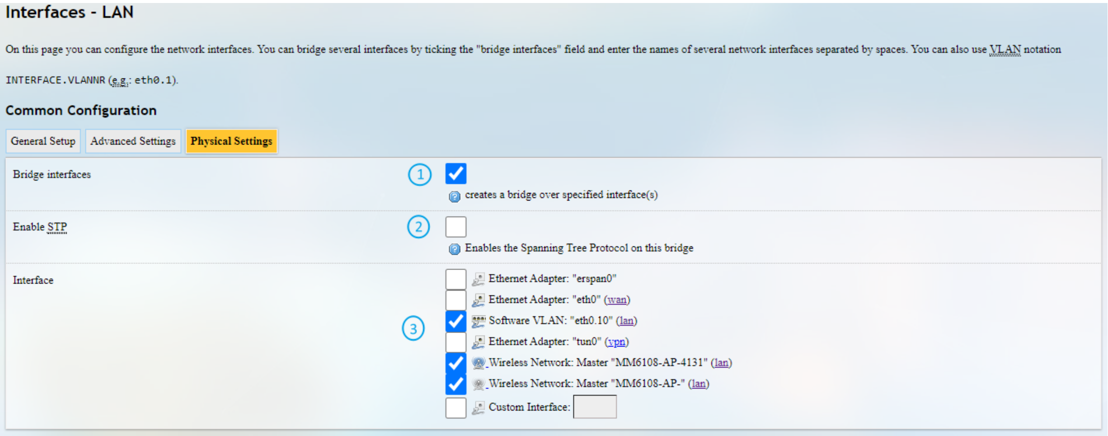
Use gateway metric: 0 ③

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.



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bridge interfaces ① ☑
creates a bridge over specified interface(s)

Enable STP ② □
Enables the Spanning Tree Protocol on this bridge

Interface ③
□ Ethernet Adapter: "erspan0"
□ Ethernet Adapter: "eth0" (wan)
☑ Software VLAN: "eth0.10" (lan)
□ Ethernet Adapter: "tun0" (vpn)
☑ Wireless Network: Master "MM6108-AP-4131" (lan)
☑ Wireless Network: Master "MM6108-AP-" (lan)
□ Custom Interface:

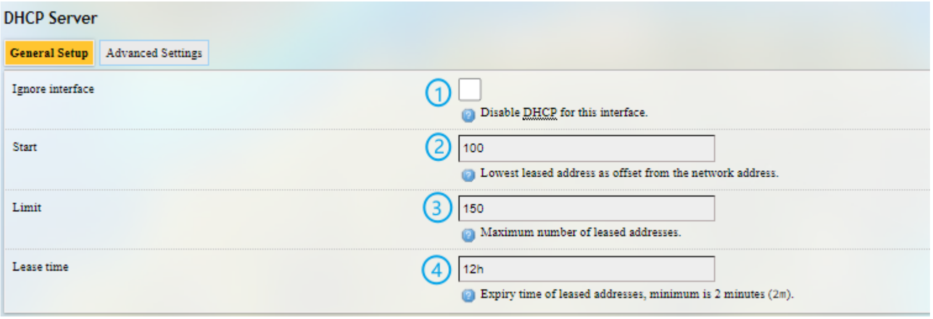
Description of the numbered areas

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:



DHCP Server

Ignore interface ① □ Disable DHCP for this interface.

Start ② 100 Lowest leased address as offset from the network address.

Limit ③ 150 Maximum number of leased addresses.

Lease time ④ 12h Expiry time of leased addresses, minimum is 2 minutes (2m).

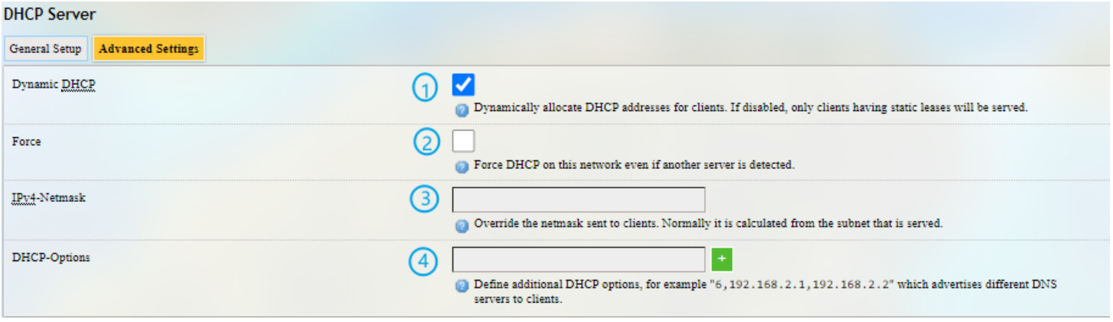
Description of the numbered areas

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 HAP103.

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:



DHCP Server

Dynamic DHCP ① ☑ Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force ② □ Force DHCP on this network even if another server is detected.

IPv4-Netmask ③ Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options ④ + Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

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.

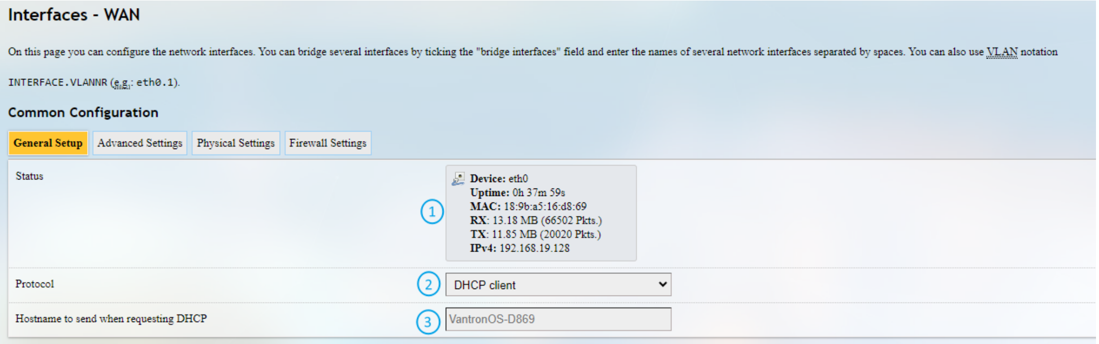
4. Add different DNS servers for client devices

*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.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status
Device: eth0
Uptime: 0h 37m 59s
MAC: 18:9b:a5:16:d8:69
RX: 13.18 MB (66502 Pkts.)
TX: 11.85 MB (20020 Pkts.)
IPv4: 192.168.19.128

Protocol: DHCP client

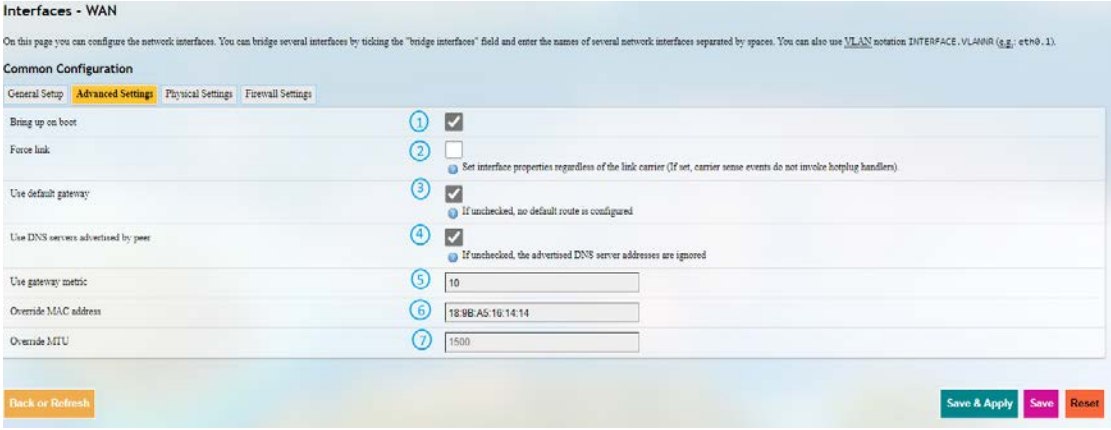
Hostname to send when requesting DHCP: VantronOS-D869

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 HAP103 for requesting DHCP

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

- **Advanced DHCP settings**



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot ① ☑

Force link ② ☐
Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).

Use default gateway ③ ☑
If unchecked, no default route is configured

Use DNS servers advertised by peer ④ ☑
If unchecked, the advertised DNS server addresses are ignored

Use gateway metric ⑤ 10

Override MAC address ⑥ 18:9B:A5:16:14:14

Override MTU ⑦ 1500

Description of the numbered areas

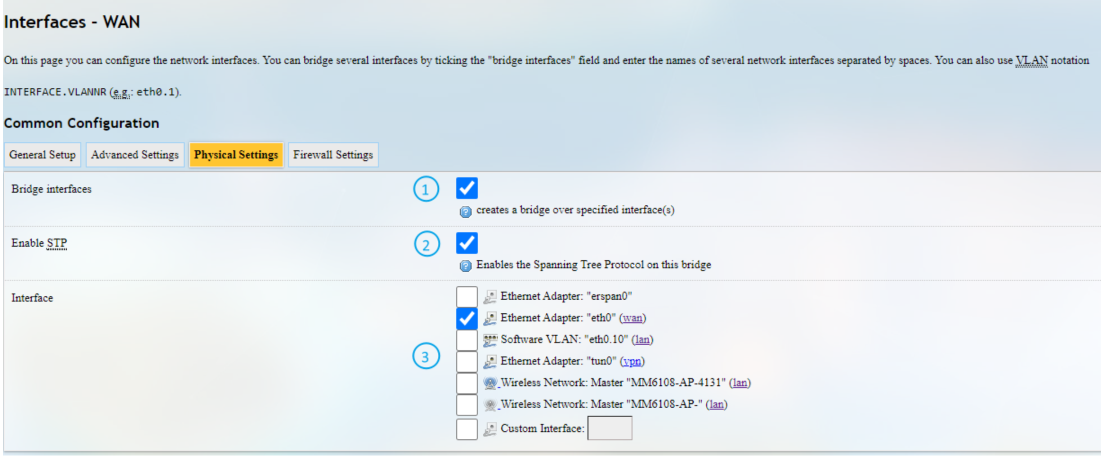
1. Check the box to bring up the port upon device boot
2. Force link (once the box is checked, hotplug handlers will not be invoked after a link change)
3. Enable **Use default gateway**
4. Enable **Use DNS server advertised by peer**

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.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bridge interfaces ☑
creates a bridge over specified interface(s)

Enable STP ☑
Enables the Spanning Tree Protocol on this bridge

Interface
□ Ethernet Adapter: "erspan0"
☑ Ethernet Adapter: "eth0" (wan)
□ Software VLAN: "eth0.10" (lan)
□ Ethernet Adapter: "tun0" (vpn)
□ Wireless Network: Master "MM6108-AP-4131" (lan)
□ Wireless Network: Master "MM6108-AP-" (lan)
□ Custom Interface:

Description of the numbered areas

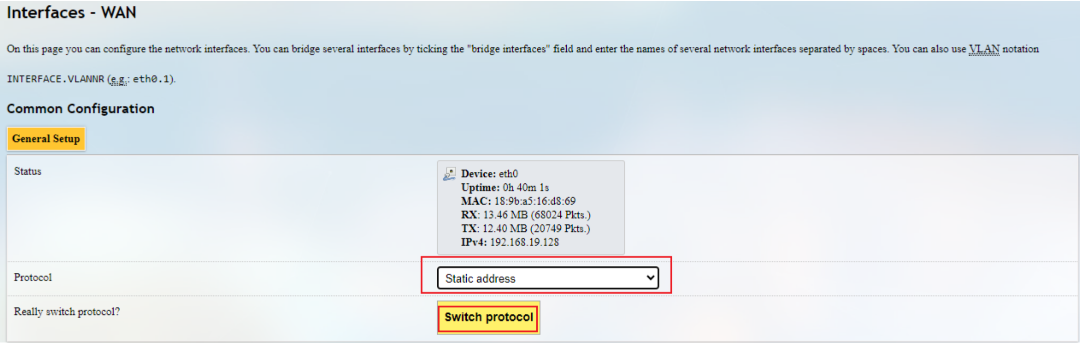
1. Enable/Disable the interface for network bridge
2. Enable/Disable STP protocol
3. Select the interfaces for bridge connection

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**.



Interfaces - WAN

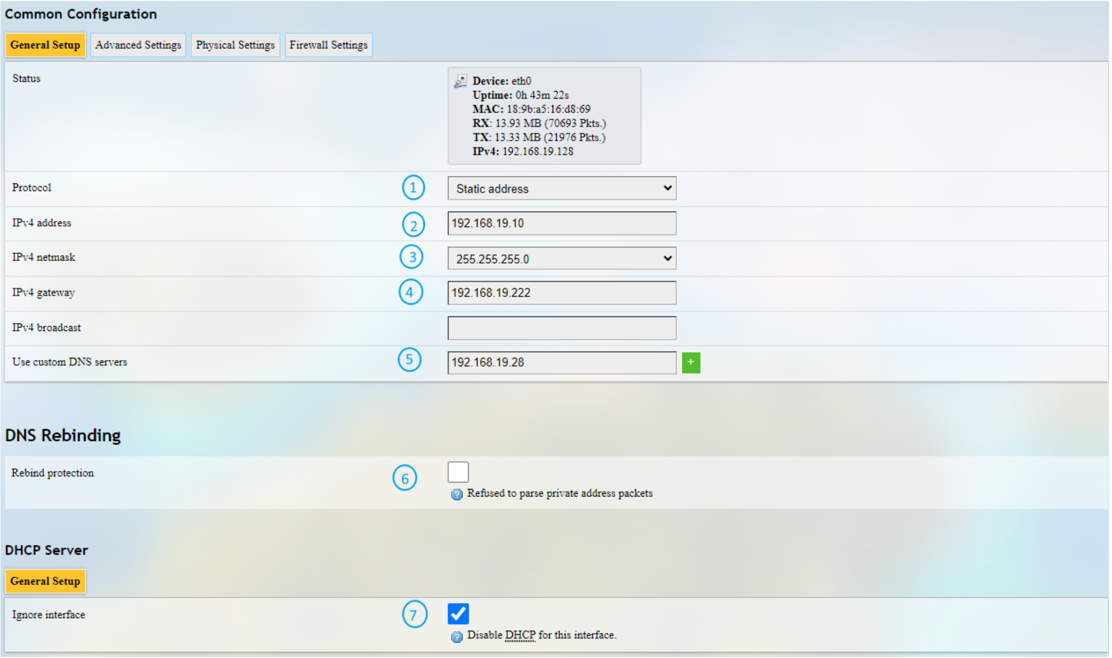
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup

Status	**Device:** eth0 **Uptime:** 0h 40m 1s **MAC:** 18:9b:a5:16:d8:69 **RX:** 13.46 MB (68024 Pkts.) **TX:** 12.40 MB (20749 Pkts.) **IPv4:** 192.168.19.128
Protocol	Static address
Really switch protocol?	Switch protocol

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



Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Status		**Device:** eth0 **Uptime:** 0h 43m 22s **MAC:** 18:9b:a5:16:d8:69 **RX:** 13.93 MB (70693 Pkts.) **TX:** 13.33 MB (21976 Pkts.) **IPv4:** 192.168.19.128
Protocol	1	Static address
IPv4 address	2	192.168.19.10
IPv4 netmask	3	255.255.255.0
IPv4 gateway	4	192.168.19.222
IPv4 broadcast		
Use custom DNS servers	5	192.168.19.28 +

DNS Rebinding

Rebind protection	6	□ Refused to parse private address packets

DHCP Server

General Setup

Ignore interface	7	☑ Disable DHCP for this interface.

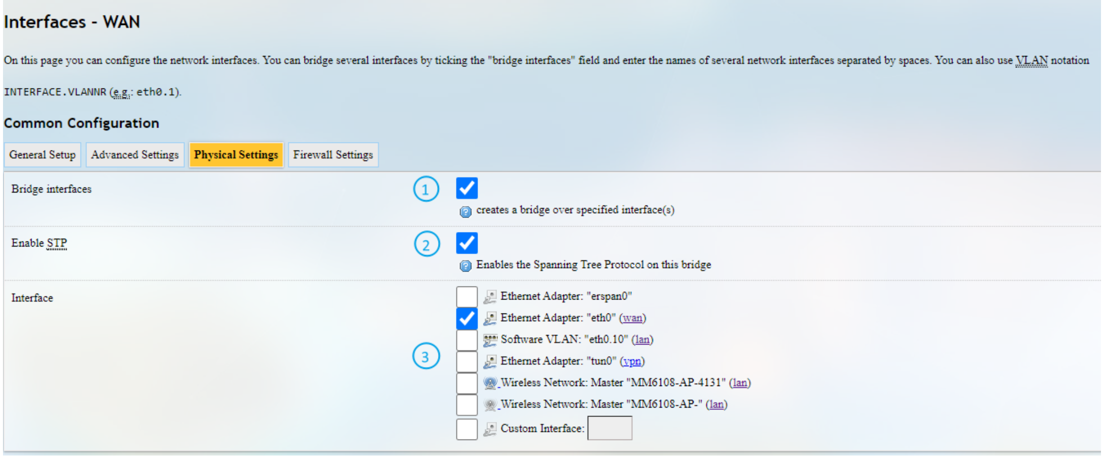
Description of the numbered areas

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.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Advanced Settings | **Physical Settings** | Firewall Settings

Bridge interfaces ① ☑ creates a bridge over specified interface(s)

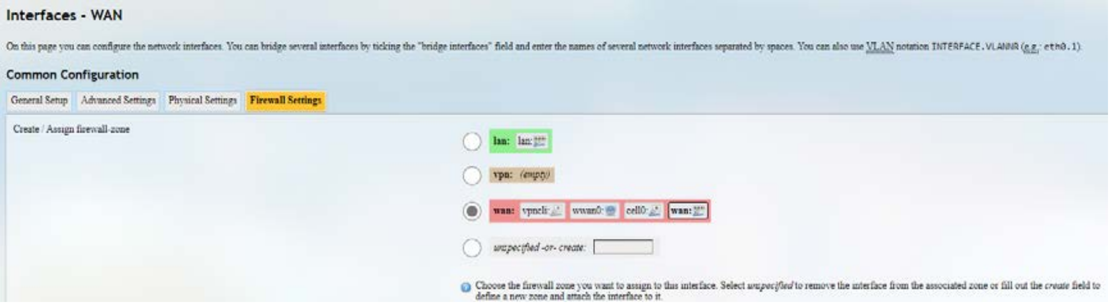
Enable STP ② ☑ Enables the Spanning Tree Protocol on this bridge

Interface ③
- □ Ethernet Adapter: "erspan0"
- ☑ Ethernet Adapter: "eth0" (wan)
- □ Software VLAN: "eth0.10" (lan)
- □ Ethernet Adapter: "tun0" (vpn)
- □ Wireless Network: Master "MM6108-AP-4131" (lan)
- □ Wireless Network: Master "MM6108-AP-" (lan)
- □ Custom Interface:

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.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Advanced Settings | Physical Settings | **Firewall Settings**

Create / Assign firewall-zone
- ○ lan: lan:
- ○ vpn: (empty)
- ● wan: vpncli: wwan0: cell0: wan:
- ○ unspecified -or- create:

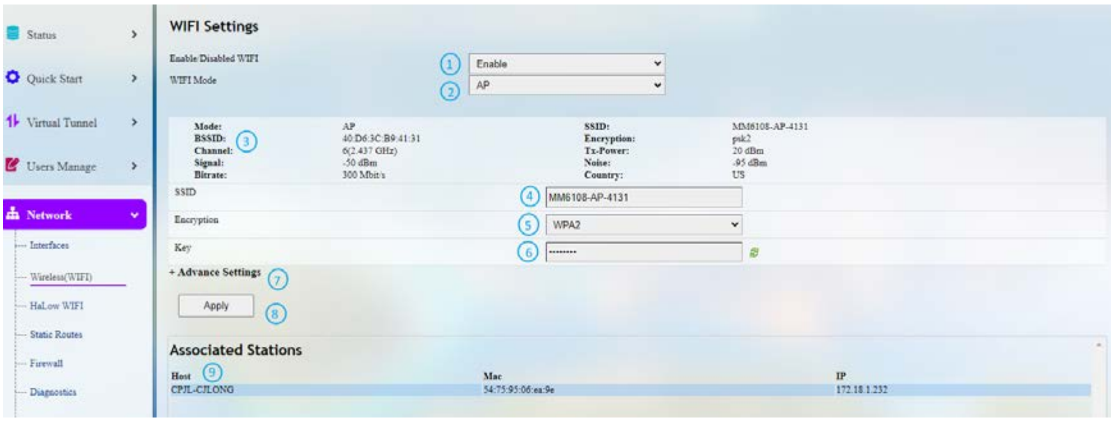
Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

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



WIFI Settings

Enable/Disabled WIFI: Enable

WIFI Mode: AP

Mode:	AP	SSID:	MM6108-AP-4131
BSSID:	40:D6:3C:B9:41:31	Encryption:	psk2
Channel:	6(2.437 GHz)	Tx-Power:	20 dBm
Signal:	-50 dBm	Noise:	-95 dBm
Bitrate:	300 Mbit/s	Country:	US

SSID: MM6108-AP-4131

Encryption: WPA2

Key: ••••••••

Associated Stations

Host	Mac	IP
CPJL-CJLONG	54:75:95:06:ea:9e	172.18.1.232

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 $, `, \.*

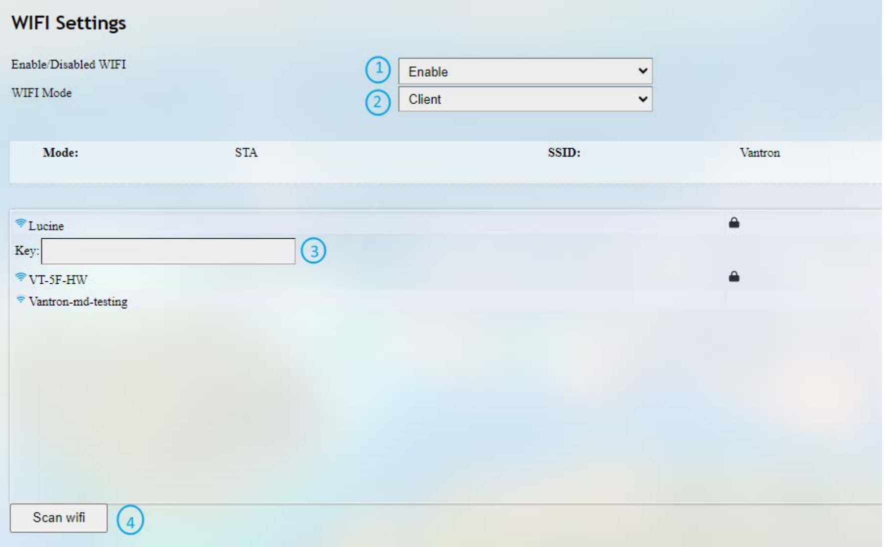
5. Select an encryption protocol
6. Assign a Wi-Fi password (no less than 8 characters)
7. Advanced Wi-Fi settings, including country code, frequency band, and channel
8. Click **Apply** to allow the modifications to take effect
9. List of currently connected devices

3.6.2.2 Wi-Fi – Client Mode

When HAP103 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 HAP103 to Wi-Fi client mode, please connect the host computer and HAP103 to the same router/switch, and use the WAN port IP to log in VantronOS for HAP103.



WIFI Settings

Enable/Disabled WIFI ① Enable

WIFI Mode ② Client

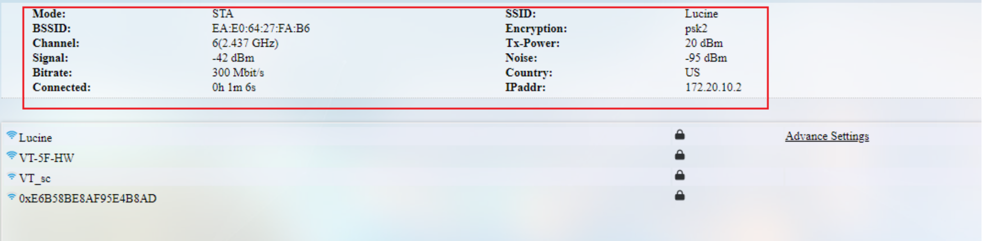
Mode:	STA	**SSID:**	Vantron

Lucine 🔒
Key: ③
VT-5F-HW 🔒
Vantron-md-testing

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.



Mode:	STA	**SSID:**	Lucine
BSSID:	EA:E0:64:27:FA:B6	**Encryption:**	psk2
Channel:	6(2.437 GHz)	**Tx-Power:**	20 dBm
Signal:	-42 dBm	**Noise:**	-95 dBm
Bitrate:	300 Mbit/s	**Country:**	US
Connected:	0h 1m 6s	**IPaddr:**	172.20.10.2

Lucine 🔒 Advance Settings
VT-5F-HW 🔒
VT_sc 🔒
0xE6B58BE8AF95E4B8AD 🔒

You can further configure the device MAC and IP protocol by clicking the **Advanced Settings** option after the SSID.

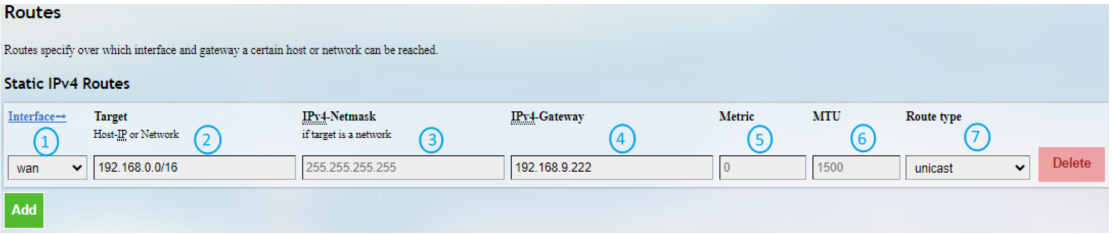
3.6.3 Wi-Fi HaLow

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.



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	MTU	Route type	
wan	192.168.0.0/16	255.255.255.255	192.168.9.222	0	1500	unicast	Delete

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

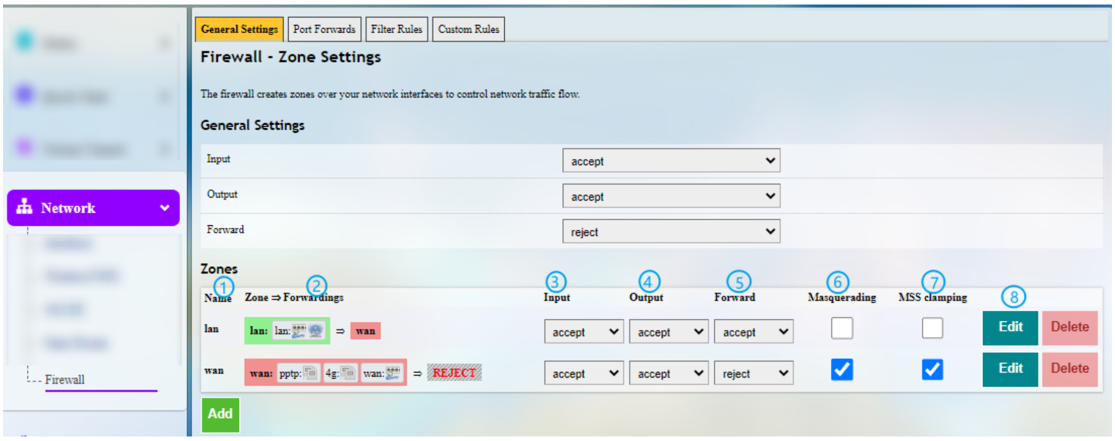
- **General Settings**

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.



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Input	accept
Output	accept
Forward	reject

Zones

Name	Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan	lan: lan: ⇒ wan	accept	accept	accept	□	□	Edit Delete
wan	wan: pptp: 4g: wan: ⇒ REJECT	accept	accept	reject	☑	☑	Edit Delete

Description of the numbered areas

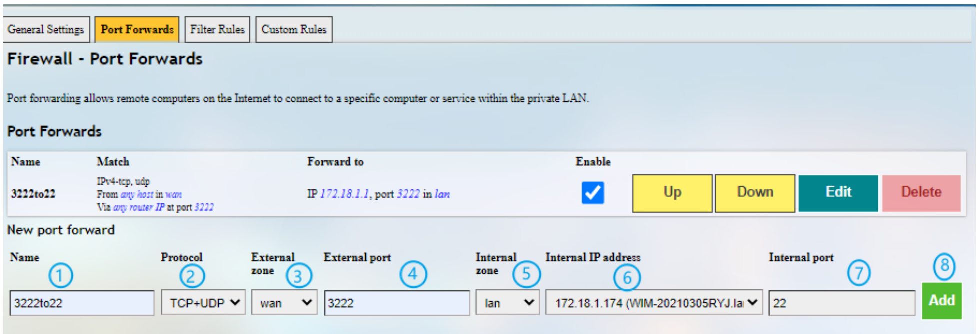
1. Zone names
2. Zone forwarding model description
3. Default policy (ACCEPT, REJECT, DROP) for incoming zone traffic
4. Default policy (ACCEPT, REJECT, DROP) for outgoing zone traffic
5. Default policy (ACCEPT, REJECT, DROP) for forwarded zone traffic
6. Masquerading (NAT)
7. MSS clamping
8. Zone editing

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):



Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable				
3222to22	IPv4-tcp, udp From *any host* in *wan* Via *any router IP* at port *3222*	IP *172.18.1.1*, port *3222* in *lan*	☑	Up	Down	Edit	Delete

New port forward

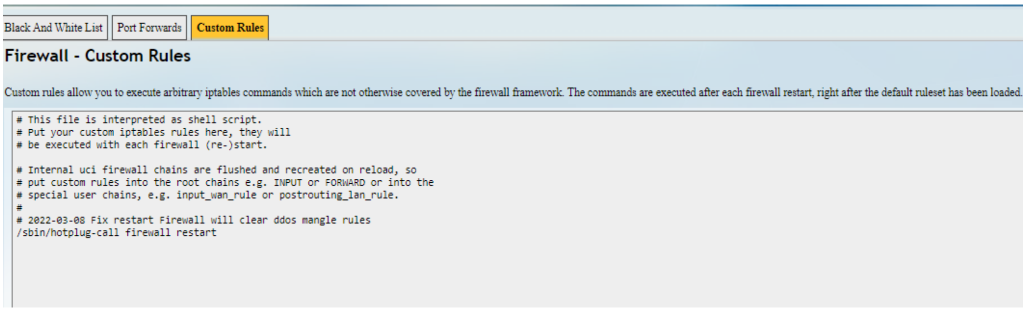
Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
3222to22	TCP+UDP	wan	3222	lan	172.18.1.174 (WIM-20210305RYJ.la	22	Add

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.



Firewall - 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 ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
#
# 2022-03-08 Fix restart Firewall will clear ddos mangle rules
/sbin/hotplug-call firewall restart
```

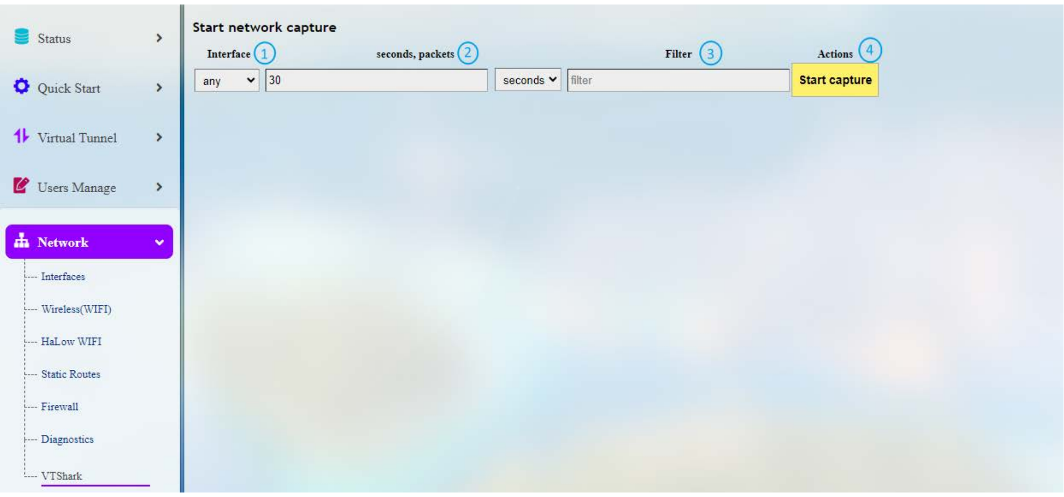
3.7 Diagnostics

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.



Start network capture

Interface: any

seconds, packets: 30 seconds

Filter: filter

Actions: Start capture

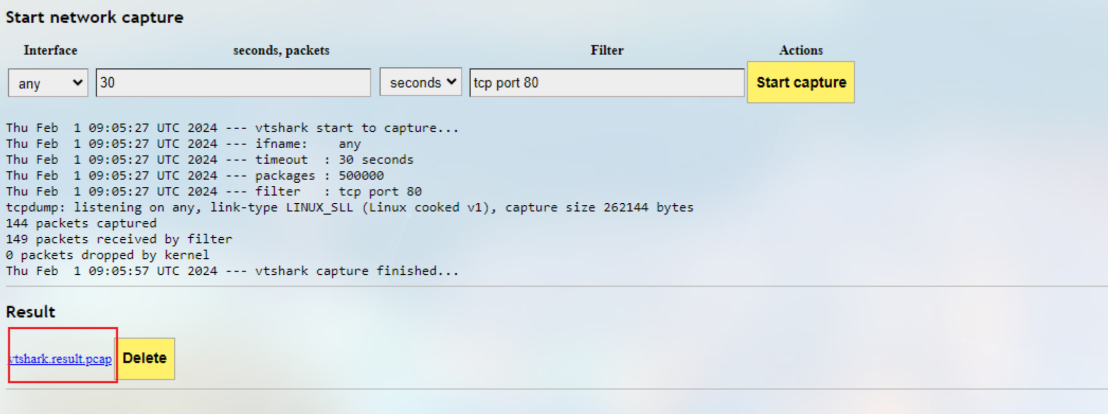
Description of the numbered areas

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.



Start network capture

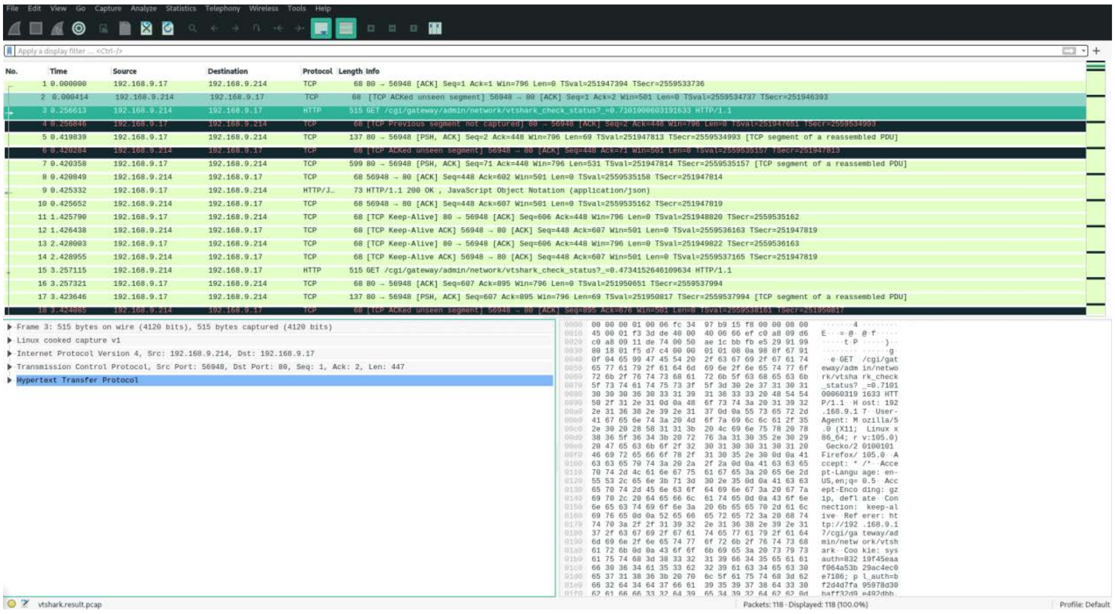
Interface	seconds, packets		Filter	Actions
any	30	seconds	tcp port 80	Start capture

```
Thu Feb  1 09:05:27 UTC 2024 --- vtshark start to capture...
Thu Feb  1 09:05:27 UTC 2024 --- ifname:    any
Thu Feb  1 09:05:27 UTC 2024 --- timeout  : 30 seconds
Thu Feb  1 09:05:27 UTC 2024 --- packages : 500000
Thu Feb  1 09:05:27 UTC 2024 --- filter   : tcp port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
144 packets captured
149 packets received by filter
0 packets dropped by kernel
Thu Feb  1 09:05:57 UTC 2024 --- vtshark capture finished...
```

Result

vtshark.result.pcap

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



```
No.  Time      Source         Destination    Protocol Length Info
  1 0.000000  192.168.9.17   192.168.9.214  TCP        68 80 → 56948 [ACK] Seq=1 Ack=1 Win=796 Len=0 TSval=251947394 TSecr=2559533736
  2 0.000414  192.168.9.214  192.168.9.17   TCP        68 [TCP ACKed unseen segment] 56948 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=2559534737 TSecr=251946393
  3 0.256613  192.168.9.214  192.168.9.17   HTTP      515 GET /cgi/gateway/admin/network/vtshark_check_status?_=0.7101000603191633 HTTP/1.1
  4 0.256846  192.168.9.17   192.168.9.214  TCP        68 [TCP Previous segment not captured] 80 → 56948 [ACK] Seq=2 Ack=448 Win=796 Len=0 TSval=251947651 TSecr=2559534993
  5 0.419839  192.168.9.17   192.168.9.214  TCP       137 80 → 56948 [PSH, ACK] Seq=2 Ack=448 Win=796 Len=69 TSval=251947813 TSecr=2559534993 [TCP segment of a reassembled PDU]
  6 0.420284  192.168.9.214  192.168.9.17   TCP        68 [TCP ACKed unseen segment] 56948 → 80 [ACK] Seq=448 Ack=71 Win=501 Len=0 TSval=2559535157 TSecr=251947813
  7 0.420358  192.168.9.17   192.168.9.214  TCP       599 80 → 56948 [PSH, ACK] Seq=71 Ack=448 Win=796 Len=531 TSval=251947814 TSecr=2559535157 [TCP segment of a reassembled PDU]
  8 0.420849  192.168.9.214  192.168.9.17   TCP        68 56948 → 80 [ACK] Seq=448 Ack=602 Win=501 Len=0 TSval=2559535158 TSecr=251947814
  9 0.425332  192.168.9.17   192.168.9.214  HTTP/J…    73 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
 10 0.425652  192.168.9.214  192.168.9.17   TCP        68 56948 → 80 [ACK] Seq=448 Ack=607 Win=501 Len=0 TSval=2559535162 TSecr=251947819
 11 1.425790  192.168.9.17   192.168.9.214  TCP        68 [TCP Keep-Alive] 80 → 56948 [ACK] Seq=606 Ack=448 Win=796 Len=0 TSval=251948820 TSecr=2559535162
 12 1.426438  192.168.9.214  192.168.9.17   TCP        68 [TCP Keep-Alive ACK] 56948 → 80 [ACK] Seq=448 Ack=607 Win=501 Len=0 TSval=2559536163 TSecr=251947819
 13 2.428003  192.168.9.17   192.168.9.214  TCP        68 [TCP Keep-Alive] 80 → 56948 [ACK] Seq=606 Ack=448 Win=796 Len=0 TSval=251949822 TSecr=2559536163
 14 2.428955  192.168.9.214  192.168.9.17   TCP        68 [TCP Keep-Alive ACK] 56948 → 80 [ACK] Seq=448 Ack=607 Win=501 Len=0 TSval=2559537165 TSecr=251947819
 15 3.257115  192.168.9.214  192.168.9.17   HTTP      515 GET /cgi/gateway/admin/network/vtshark_check_status?_=0.4734152646109634 HTTP/1.1
 16 3.257321  192.168.9.17   192.168.9.214  TCP        68 80 → 56948 [ACK] Seq=607 Ack=895 Win=796 Len=0 TSval=251950651 TSecr=2559537994
 17 3.423646  192.168.9.17   192.168.9.214  TCP       137 80 → 56948 [PSH, ACK] Seq=607 Ack=895 Win=796 Len=69 TSval=251950817 TSecr=2559537994 [TCP segment of a reassembled PDU]
 18 3.424085  192.168.9.214  192.168.9.17   TCP        68 [TCP ACKed unseen segment] 56948 → 80 [ACK] Seq=895 Ack=676 Win=501 Len=0 TSval=2559538161 TSecr=251950817
```

```
▸ Frame 3: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits)
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.9.214, Dst: 192.168.9.17
▸ Transmission Control Protocol, Src Port: 56948, Dst Port: 80, Seq: 1, Ack: 2, Len: 447
▸ Hypertext Transfer Protocol
```

```
0000  00 00 00 01 00 06 fc 34  97 b9 15 f8 00 00 08 00   ·······4 ········
0010  45 00 01 f3 3d de 40 00  40 06 66 ef c0 a8 09 d6   E···=·@· @·f·····
0020  c0 a8 09 11 de 74 00 50  ae 1c bb fb e5 29 91 99   ·····t·P ·····)··
0030  80 18 01 f5 d7 c4 00 00  01 01 08 0a 98 8f 67 91   ········ ······g·
0040  0f 04 65 99 47 45 54 20  2f 63 67 69 2f 67 61 74   ··e·GET  /cgi/gat
0050  65 77 61 79 2f 61 64 6d  69 6e 2f 6e 65 74 77 6f   eway/adm in/netwo
0060  72 6b 2f 76 74 73 68 61  72 6b 5f 63 68 65 63 6b   rk/vtsha rk_check
0070  5f 73 74 61 74 75 73 3f  5f 3d 30 2e 37 31 30 31   _status? _=0.7101
0080  30 30 30 36 30 33 31 39  31 36 33 33 20 48 54 54   00060319 1633 HTT
0090  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 31 39 32   P/1.1··H ost: 192
00a0  2e 31 36 38 2e 39 2e 31  37 0d 0a 55 73 65 72 2d   .168.9.1 7··User-
00b0  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
00c0  2e 30 20 28 58 31 31 3b  20 4c 69 6e 75 78 20 78   .0 (X11;  Linux x
00d0  38 36 5f 36 34 3b 20 72  76 3a 31 30 35 2e 30 29   86_64; r v:105.0)
00e0  20 47 65 63 6b 6f 2f 32  30 31 30 30 31 30 31 20    Gecko/2 0100101 
00f0  46 69 72 65 66 6f 78 2f  31 30 35 2e 30 0d 0a 41   Firefox/ 105.0··A
0100  63 63 65 70 74 3a 20 2a  2f 2a 0d 0a 41 63 63 65   ccept: * /*··Acce
0110  70 74 2d 4c 61 6e 67 75  61 67 65 3a 20 65 6e 2d   pt-Langu age: en-
0120  55 53 2c 65 6e 3b 71 3d  30 2e 35 0d 0a 41 63 63   US,en;q= 0.5··Acc
0130  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 67 7a   ept-Enco ding: gz
0140  69 70 2c 20 64 65 66 6c  61 74 65 0d 0a 43 6f 6e   ip, defl ate··Con
0150  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0160  69 76 65 0d 0a 52 65 66  65 72 65 72 3a 20 68 74   ive··Ref erer: ht
0170  74 70 3a 2f 2f 31 39 32  2e 31 36 38 2e 39 2e 31   tp://192 .168.9.1
0180  37 2f 63 67 69 2f 67 61  74 65 77 61 79 2f 61 64   7/cgi/ga teway/ad
0190  6d 69 6e 2f 6e 65 74 77  6f 72 6b 2f 76 74 73 68   min/netw ork/vtsh
01a0  61 72 6b 0d 0a 43 6f 6f  6b 69 65 3a 20 73 79 73   ark··Coo kie: sys
01b0  61 75 74 68 3d 38 33 32  31 39 66 34 35 65 61 61   auth=832 19f45eaa
01c0  66 30 36 34 61 35 33 62  32 39 61 63 34 65 63 30   f064a53b 29ac4ec0
01d0  65 37 31 38 36 3b 20 70  6c 5f 61 75 74 68 3d 62   e7186; p l_auth=b
01e0  66 32 64 34 64 37 66 61  39 35 39 37 38 64 33 30   f2d4d7fa 95978d30
01f0  62 61 66 66 33 32 64 39  65 34 39 32 64 62 62 0d   baff32d9 e492dbb·
```

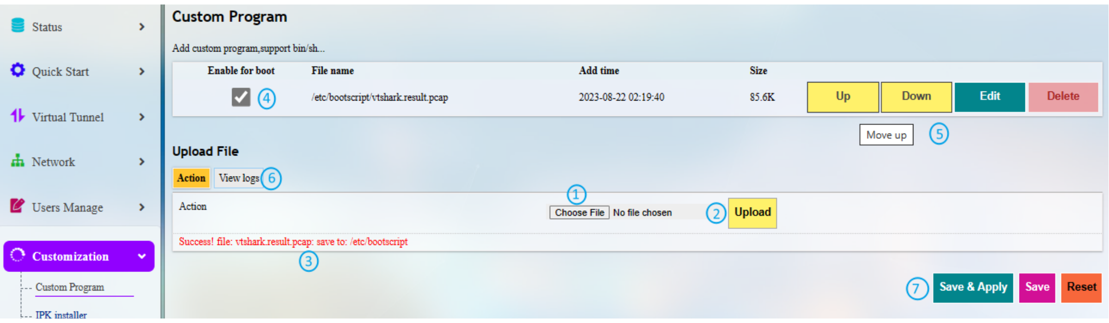
vtshark.result.pcap Packets: 118 · Displayed: 118 (100.0%) Profile: Default

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.



Custom Program

Add custom program,support bin/sh...

Enable for boot	File name	Add time	Size
☑	/etc/bootscript/vtshark.result.pcap	2023-08-22 02:19:40	85.6K

Upload File

Action

No file chosen

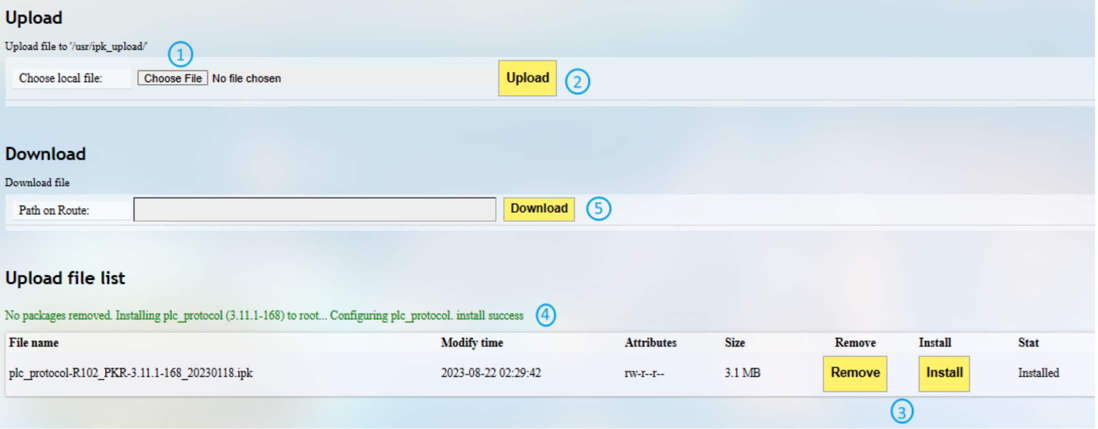
Success! file: vtshark.result.pcap: save to: /etc/bootscript

Description of the numbered areas

1. Select a script to upload
2. Upload the script to HAP103
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 HAP103. Vantron industrial protocol packages are also uploaded from here.



Upload

Upload file to '/usr/ipk_upload/'

Choose local file: Choose File No file chosen

Download

Download file

Path on Route:

Upload file list

No packages removed. Installing plc_protocol (3.11.1-168) to root... Configuring plc_protocol. install success

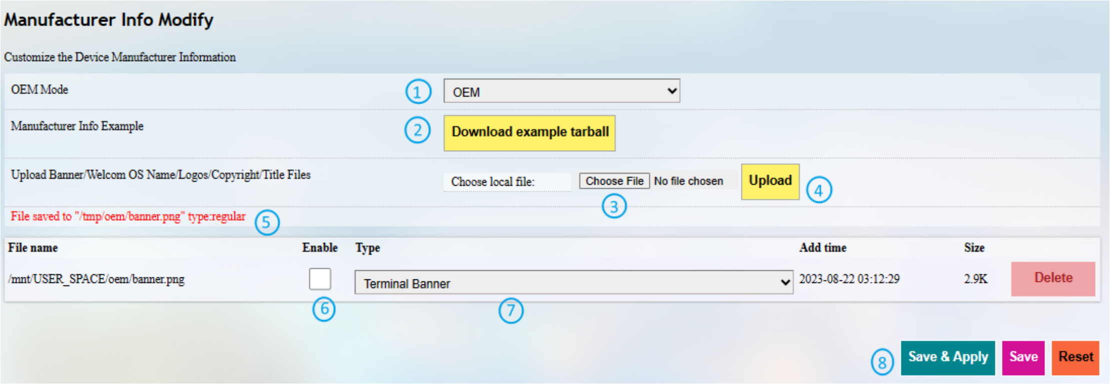
File name	Modify time	Attributes	Size	Remove	Install	Stat
plc_protocol-R102_PKR-3.11.1-168_20230118.ipk	2023-08-22 02:29:42	rw-r--r--	3.1 MB	Remove	Install	Installed

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.



Manufacturer Info Modify

Customize the Device Manufacturer Information

OEM Mode: OEM

Manufacturer Info Example: Download example tarball

Upload Banner/Welcom OS Name/Logos/Copyright/Title Files: Choose local file: Choose File No file chosen Upload

File saved to "/tmp/oem/banner.png" type:regular

File name	Enable	Type	Add time	Size	
/mnt/USER_SPACE/oem/banner.png	□	Terminal Banner	2023-08-22 03:12:29	2.9K	Delete

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 HAP103
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

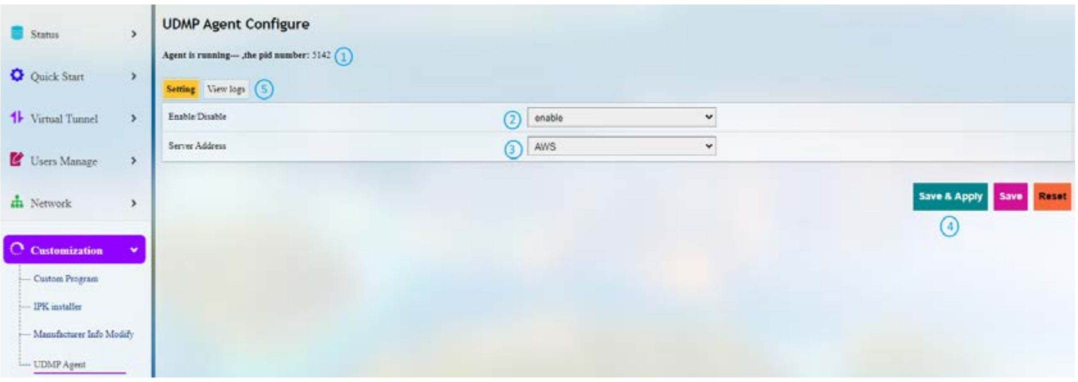
3.9.4 UDMP Agent

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.



UDMP Agent Configure

Agent is running--- ,the pid number: 5142 ①

Enable/Disable ② enable

Server Address ③ AWS

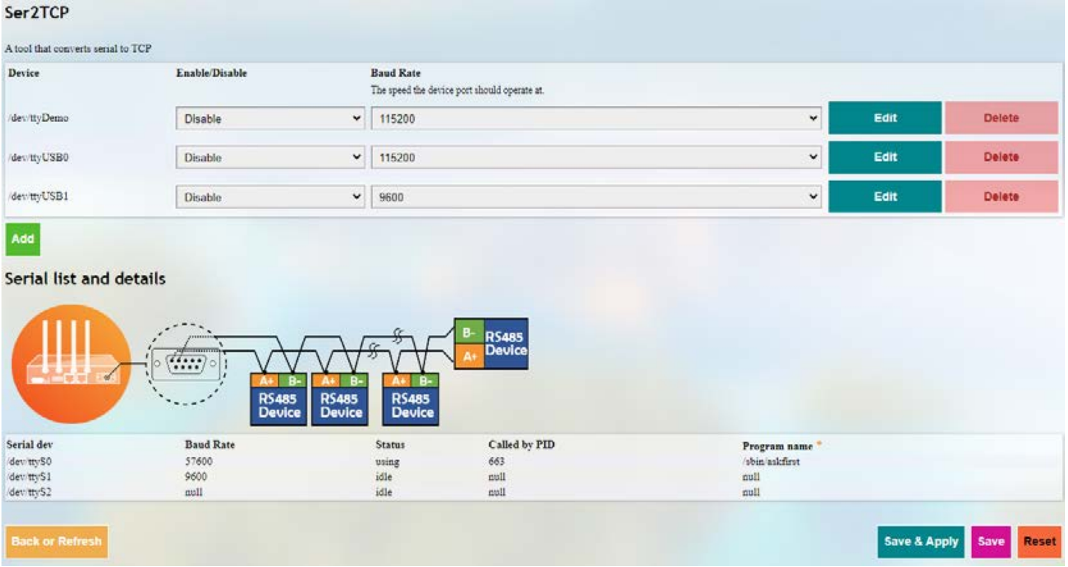
Description of the numbered areas

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.



Ser2TCP

A tool that converts serial to TCP

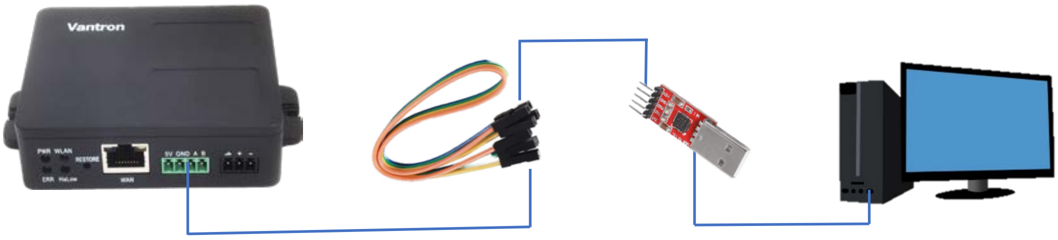
Device	Enable/Disable	Baud Rate The speed the device port should operate at.		
/dev/ttyDemo	Disable	115200	Edit	Delete
/dev/ttyUSB0	Disable	115200	Edit	Delete
/dev/ttyUSB1	Disable	9600	Edit	Delete

Serial list and details

Serial dev	Baud Rate	Status	Called by PID	Program name
/dev/ttyS0	57600	using	663	/sbin/askfirst
/dev/ttyS1	9600	idle	null	null
/dev/ttyS2	null	idle	null	null

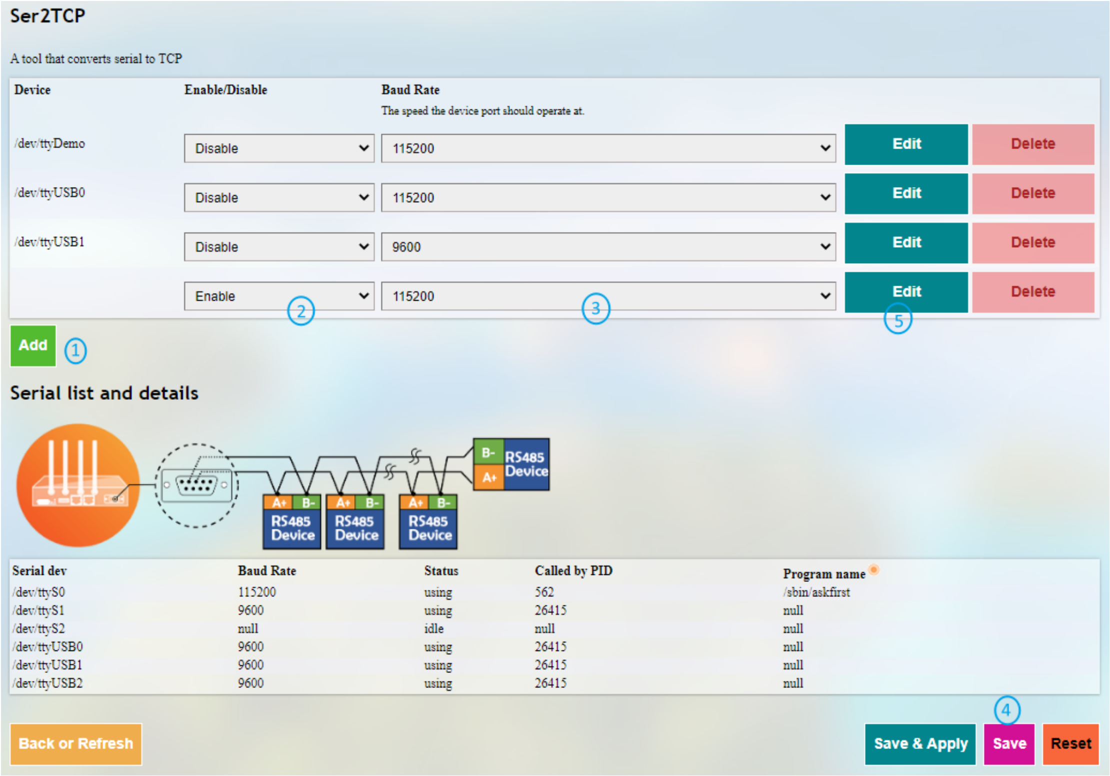
3.10.2 Ser2net Environment Setup and Verification

- Prerequisites
  - An HAP103
  - A Linux host computer (Ubuntu for demonstration here)
  - A USB to TTL serial adapter
  - DuPont cables
  - Connect the serial port of HAP103 to the host computer as follows (refer to 1.5 for the wiring)



- Client mode

(1) Settings on VantronOS web interface



Ser2TCP

A tool that converts serial to TCP

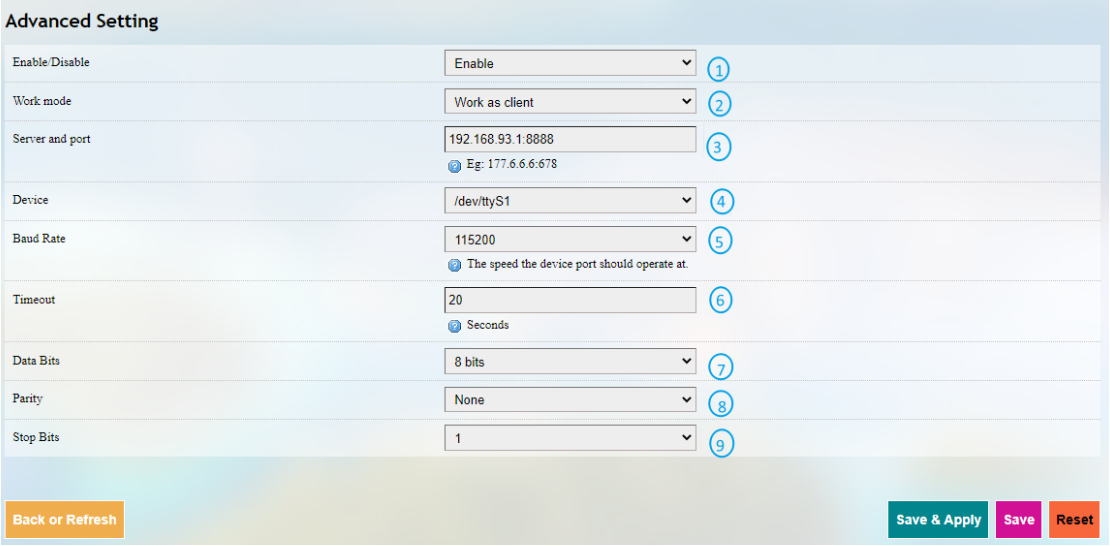
Device	Enable/Disable	Baud Rate The speed the device port should operate at.		
/dev/ttyDemo	Disable	115200	Edit	Delete
/dev/ttyUSB0	Disable	115200	Edit	Delete
/dev/ttyUSB1	Disable	9600	Edit	Delete
	Enable	115200	Edit	Delete

Serial list and details

Serial dev	Baud Rate	Status	Called by PID	Program name
/dev/ttyS0	115200	using	562	/sbin/askfirst
/dev/ttyS1	9600	using	26415	null
/dev/ttyS2	null	idle	null	null
/dev/ttyUSB0	9600	using	26415	null
/dev/ttyUSB1	9600	using	26415	null
/dev/ttyUSB2	9600	using	26415	null

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



Advanced Setting

Enable/Disable	Enable ①
Work mode	Work as client ②
Server and port	192.168.93.1:8888 ③ Eg: 177.6.6.6:678
Device	/dev/ttyS1 ④
Baud Rate	115200 ⑤ The speed the device port should operate at.
Timeout	20 ⑥ Seconds
Data Bits	8 bits ⑦
Parity	None ⑧
Stop Bits	1 ⑨

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

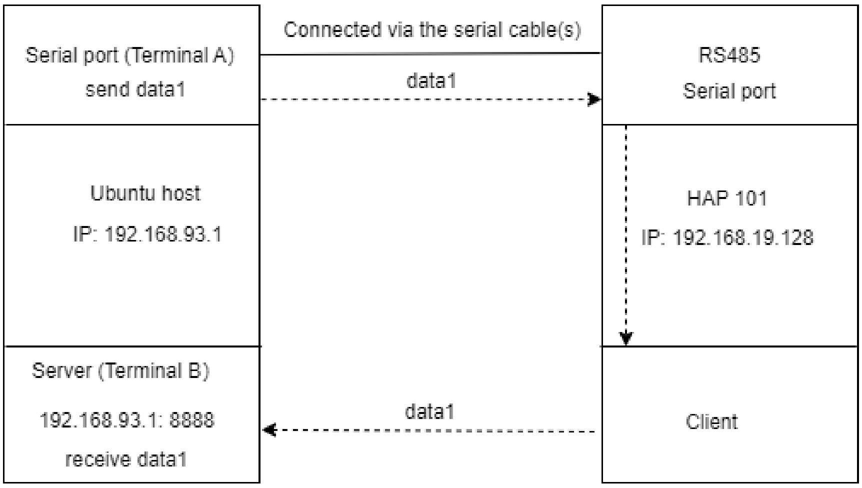
- Use a serial communication program (e.g. microcom) to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

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

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

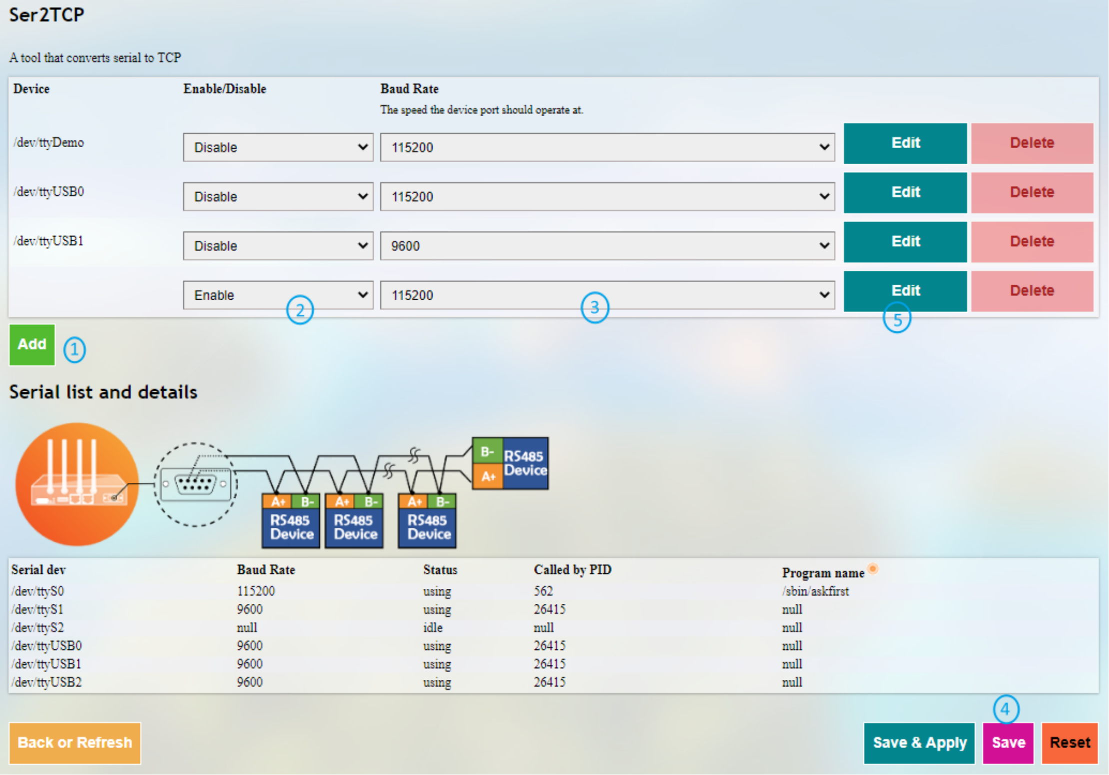
```
tcpudp_test tcp server:tcpudp_test -p 8888
```

- 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



Ser2TCP

A tool that converts serial to TCP

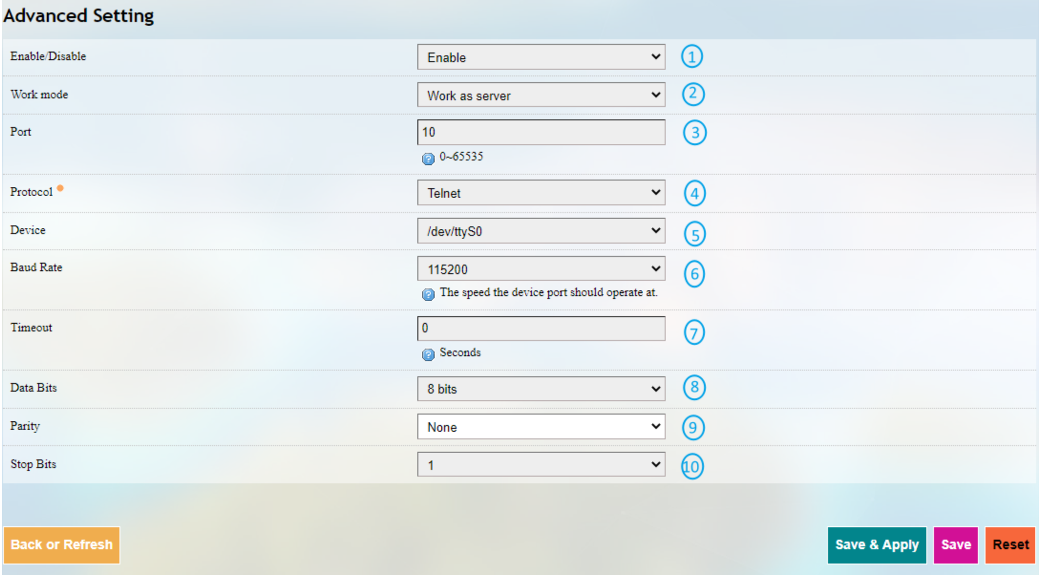
Device	Enable/Disable	Baud Rate The speed the device port should operate at.		
/dev/ttyDemo	Disable	115200	Edit	Delete
/dev/ttyUSB0	Disable	115200	Edit	Delete
/dev/ttyUSB1	Disable	9600	Edit	Delete
	Enable	115200	Edit	Delete

Serial list and details

Serial dev	Baud Rate	Status	Called by PID	Program name
/dev/ttyS0	115200	using	562	/sbin/askfirst
/dev/ttyS1	9600	using	26415	null
/dev/ttyS2	null	idle	null	null
/dev/ttyUSB0	9600	using	26415	null
/dev/ttyUSB1	9600	using	26415	null
/dev/ttyUSB2	9600	using	26415	null

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



Advanced Setting

Enable/Disable	Enable ①
Work mode	Work as server ②
Port	10 ③ 0~65535
Protocol	Telnet ④
Device	/dev/ttyS0 ⑤
Baud Rate	115200 ⑥ The speed the device port should operate at.
Timeout	0 ⑦ Seconds
Data Bits	8 bits ⑧
Parity	None ⑨
Stop Bits	1 ⑩

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

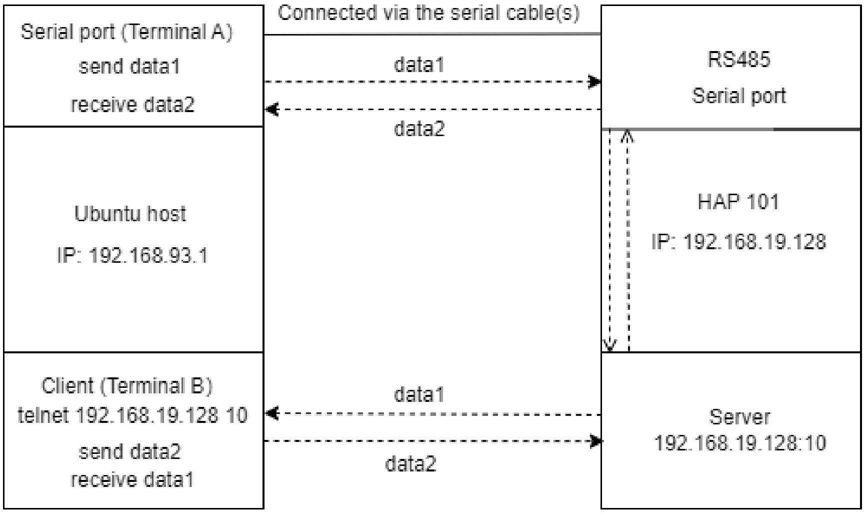
- Use a serial communication program (e.g., microcom) to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
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:

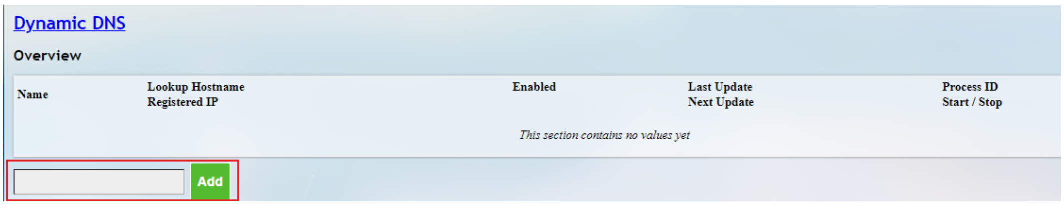
1) Raw: enables the port and transfers all data as-is between the port and the long integer.

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.



Dynamic DNS

Overview

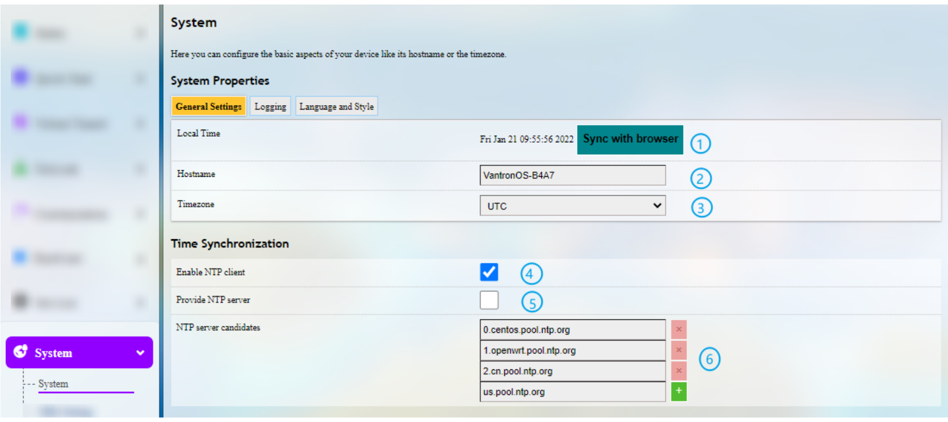
Name	Lookup Hostname Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop

This section contains no values yet

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.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time: Fri Jan 21 09:55:56 2022

Hostname: VantronOS-B4A7

Timezone: UTC

Time Synchronization

Enable NTP client ☑

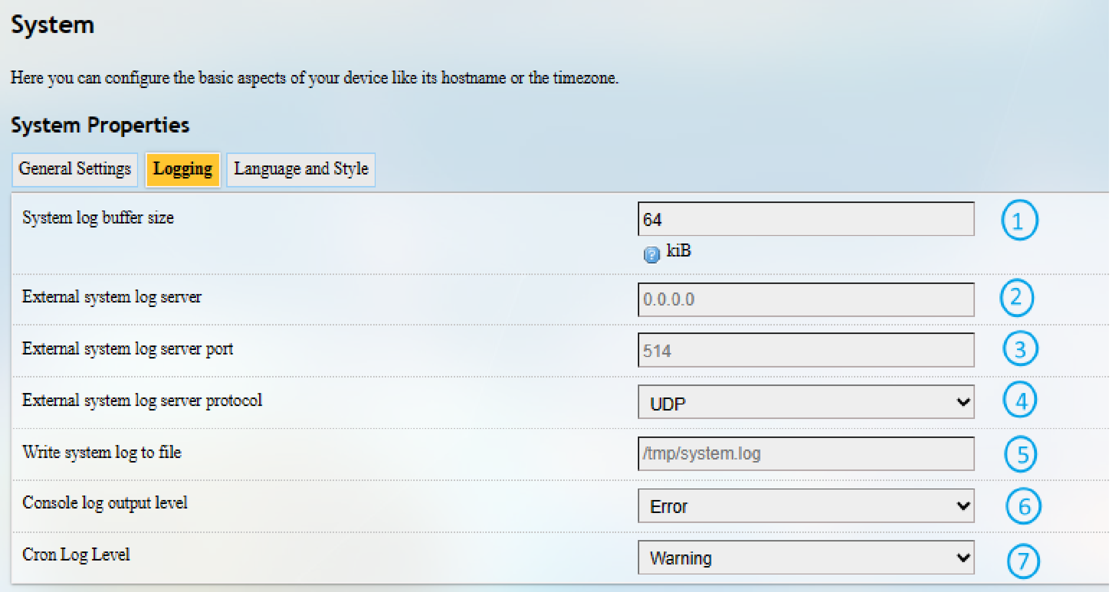
Provide NTP server □

NTP server candidates: 0.centos.pool.ntp.org, 1.openwrt.pool.ntp.org, 2.cn.pool.ntp.org, us.pool.ntp.org

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.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

System log buffer size	64 kiB	1
External system log server	0.0.0.0	2
External system log server port	514	3
External system log server protocol	UDP	4
Write system log to file	/tmp/system.log	5
Console log output level	Error	6
Cron Log Level	Warning	7

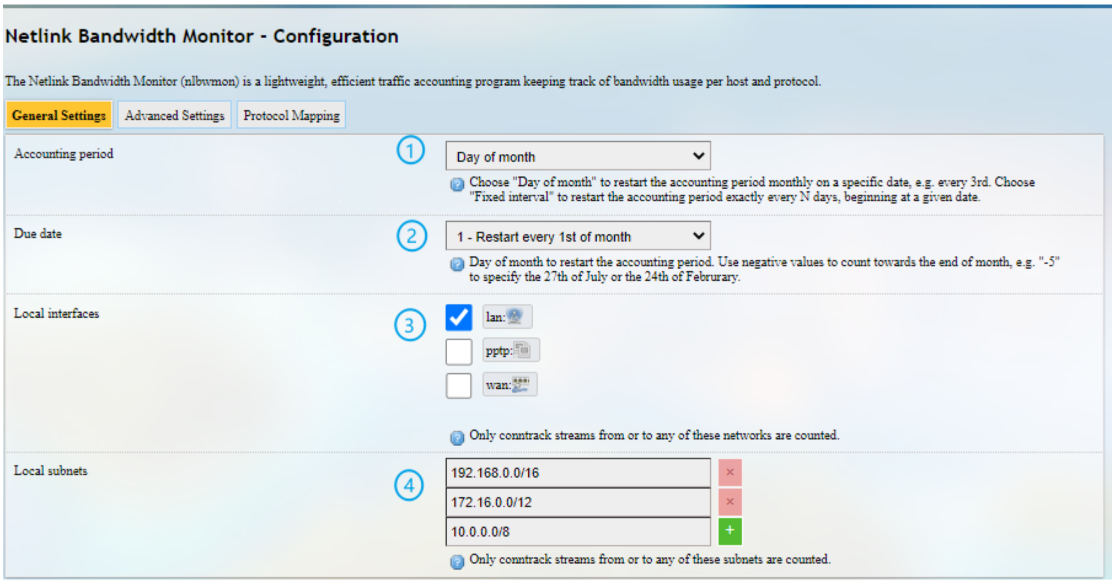
Description of the numbered areas

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**



Netlink Bandwidth Monitor - Configuration

The Netlink Bandwidth Monitor (nlbwmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

Accounting period: Day of month

Choose "Day of month" to restart the accounting period monthly on a specific date, e.g. every 3rd. Choose "Fixed interval" to restart the accounting period exactly every N days, beginning at a given date.

Due date: 1 - Restart every 1st of month

Day of month to restart the accounting period. Use negative values to count towards the end of month, e.g. "-5" to specify the 27th of July or the 24th of Februrary.

Local interfaces:
☑ lan:
□ pptp:
□ wan:

Only conntrack streams from or to any of these networks are counted.

Local subnets:
192.168.0.0/16 ×
172.16.0.0/12 ×
10.0.0.0/8 +

Only conntrack streams from or to any of these subnets are counted.

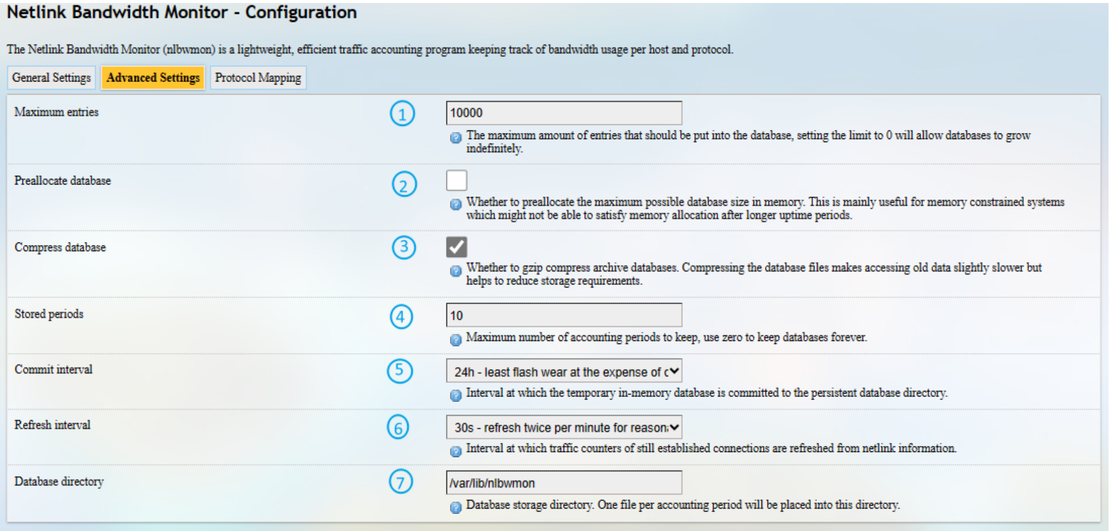
Description of the numbered areas

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.



Netlink Bandwidth Monitor - Configuration

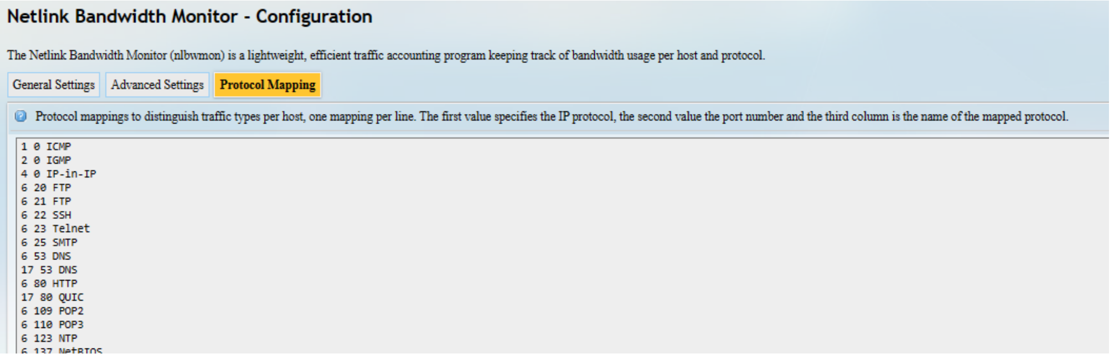
The Netlink Bandwidth Monitor (nlbwmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

Maximum entries	1	10000 The maximum amount of entries that should be put into the database, setting the limit to 0 will allow databases to grow indefinitely.
Preallocate database	2	□ Whether to preallocate the maximum possible database size in memory. This is mainly useful for memory constrained systems which might not be able to satisfy memory allocation after longer uptime periods.
Compress database	3	☑ Whether to gzip compress archive databases. Compressing the database files makes accessing old data slightly slower but helps to reduce storage requirements.
Stored periods	4	10 Maximum number of accounting periods to keep, use zero to keep databases forever.
Commit interval	5	24h - least flash wear at the expense of c Interval at which the temporary in-memory database is committed to the persistent database directory.
Refresh interval	6	30s - refresh twice per minute for reason: Interval at which traffic counters of still established connections are refreshed from netlink information.
Database directory	7	/var/lib/nlbwmon Database storage directory. One file per accounting period will be placed into this directory.

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.



Netlink Bandwidth Monitor - Configuration

The Netlink Bandwidth Monitor (nlbwmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

Protocol mappings to distinguish traffic types per host, one mapping per line. The first value specifies the IP protocol, the second value the port number and the third column is the name of the mapped protocol.

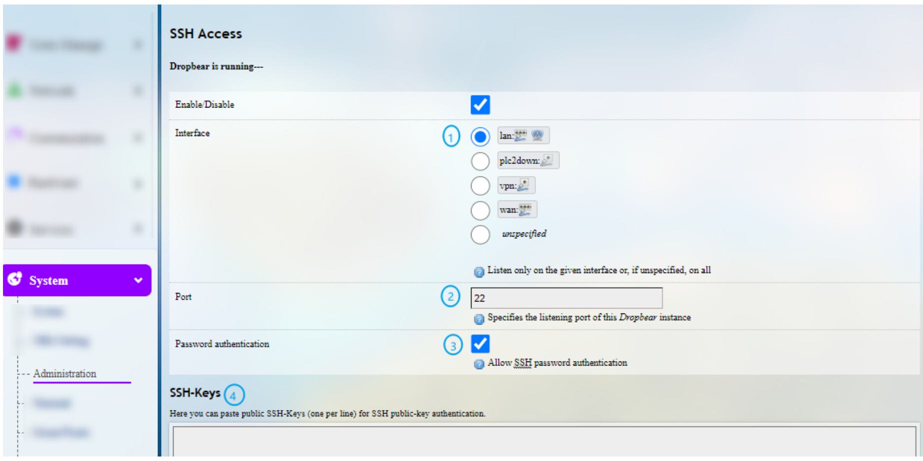
```
1 0 ICMP
2 0 IGMP
4 0 IP-in-IP
6 20 FTP
6 21 FTP
6 22 SSH
6 23 Telnet
6 25 SMTP
6 53 DNS
17 53 DNS
6 80 HTTP
17 80 QUIC
6 109 POP2
6 110 POP3
6 123 NTP
6 137 NetBIOS
```

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;



SSH Access

Dropbear is running---

Enable/Disable ☑

Interface (1) ● lan: ○ plc2down: ○ vpn: ○ wan: ○ *unspecified*

Listen only on the given interface or, if unspecified, on all

Port (2) 22

Specifies the listening port of this *Dropbear* instance

Password authentication (3) ☑

Allow SSH password authentication

SSH-Keys (4)

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

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)

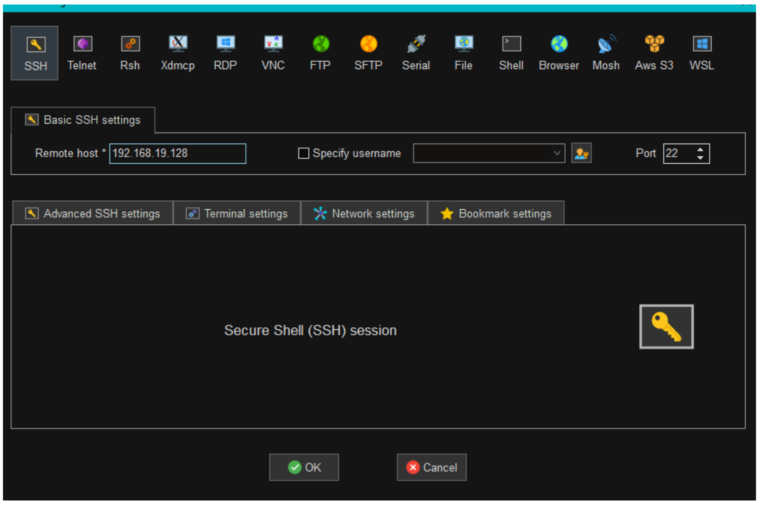
3) Allow SSH password authentication

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;



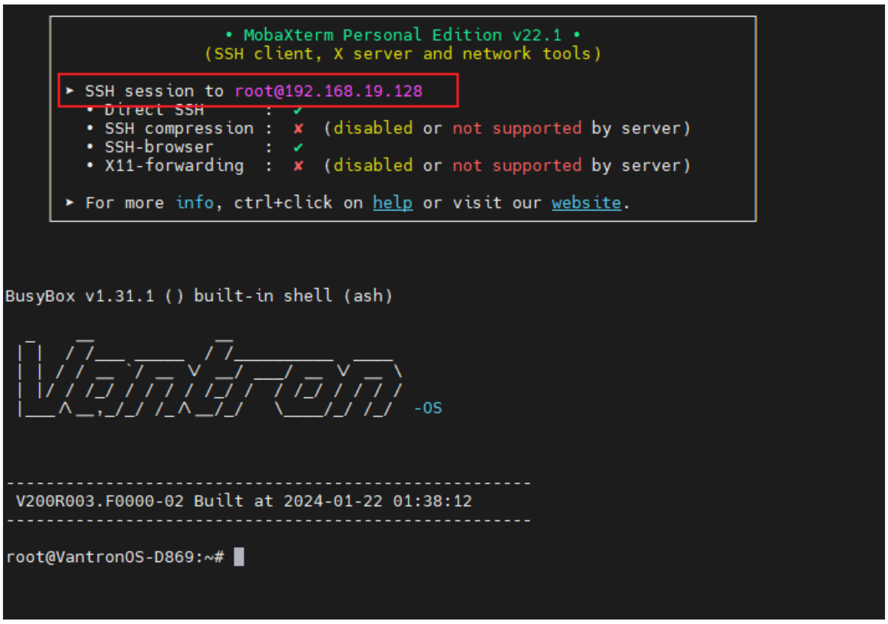
Basic SSH settings

Remote host * 192.168.19.128 ☐ Specify username Port 22

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

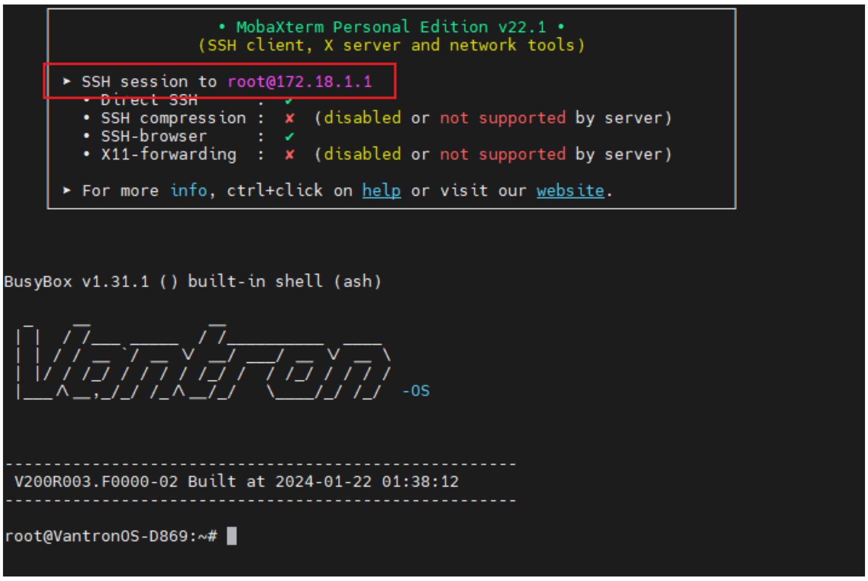
Make sure the IP address of the host computer is on the same network as HAP103. Refer to 2.2 for how to identify the 2.4GHz WLAN IP or WAN port IP of the device.

SSH login with the WAN port IP of HAP103:



```
                 • MobaXterm Personal Edition v22.1 •
               (SSH client, X server and network tools)

      ➤ SSH session to root@192.168.19.128
        • Direct SSH      :  ✓
        • SSH compression :  ✘  (disabled or not supported by server)
        • SSH-browser     :  ✓
        • X11-forwarding  :  ✘  (disabled or not supported by server)

      ➤ For more info, ctrl+click on help or visit our website.


BusyBox v1.31.1 () built-in shell (ash)

  _    __            __
 | |  / /___ _____  / /__________  ____
 | | / / __ `/ __ \/ __/ ___/ __ \/ __ \
 | |/ / /_/ / / / / /_/ /  / /_/ / / / /
 |___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -OS


 -----------------------------------------------------
  V200R003.F0000-02 Built at 2024-01-22 01:38:12
 -----------------------------------------------------

root@VantronOS-D869:~#
```

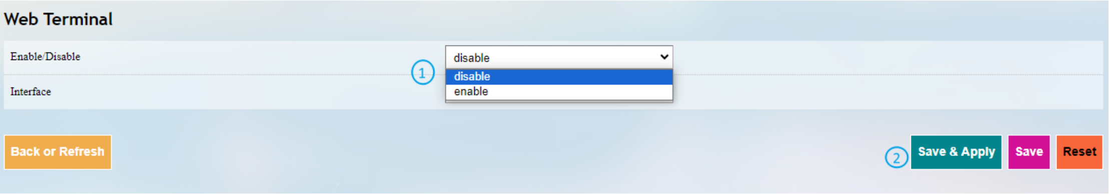
SSH login with the 2.4GHz WLAN IP of HAP103:



```
                 • MobaXterm Personal Edition v22.1 •
               (SSH client, X server and network tools)

      ➤ SSH session to root@172.18.1.1
        • Direct SSH      :  ✓
        • SSH compression :  ✘  (disabled or not supported by server)
        • SSH-browser     :  ✓
        • X11-forwarding  :  ✘  (disabled or not supported by server)

      ➤ For more info, ctrl+click on help or visit our website.


BusyBox v1.31.1 () built-in shell (ash)

  _    __            __
 | |  / /___ _____  / /__________  ____
 | | / / __ `/ __ \/ __/ ___/ __ \/ __ \
 | |/ / /_/ / / / / /_/ /  / /_/ / / / /
 |___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -OS


 -----------------------------------------------------
  V200R003.F0000-02 Built at 2024-01-22 01:38:12
 -----------------------------------------------------

root@VantronOS-D869:~#
```

3.12.4 Terminal

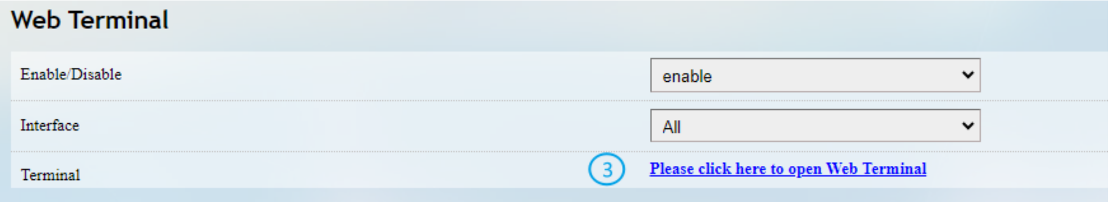
When navigating to **System > Terminal**, users can **enable** the Web terminal for logging in the shell of the device.



Web Terminal

Enable/Disable: disable

Interface



Web Terminal

Enable/Disable: enable

Interface: All

Terminal: Please click here to open Web Terminal

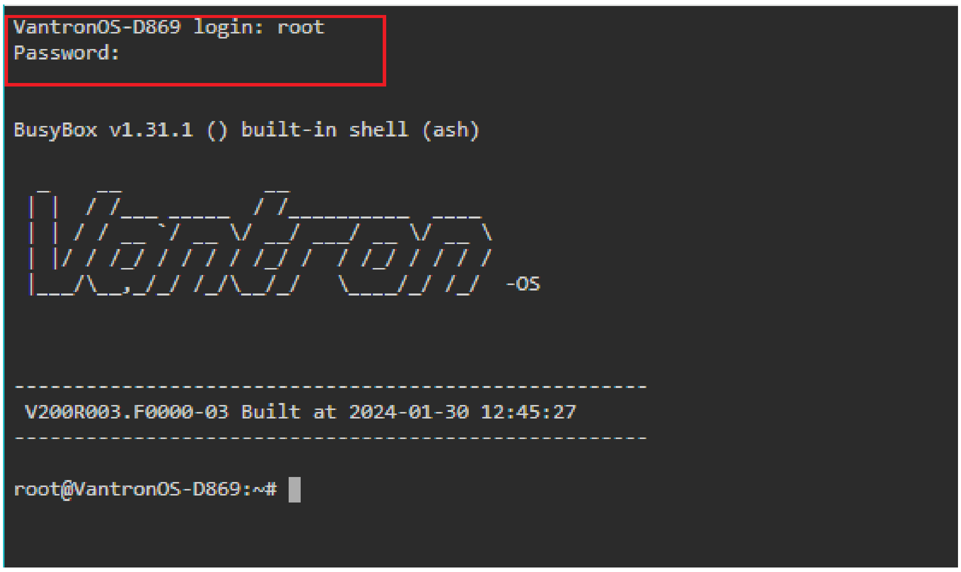
Step 1: Select **enable** from the drop-down list;

Step 2: Save the change;

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

Login account: root

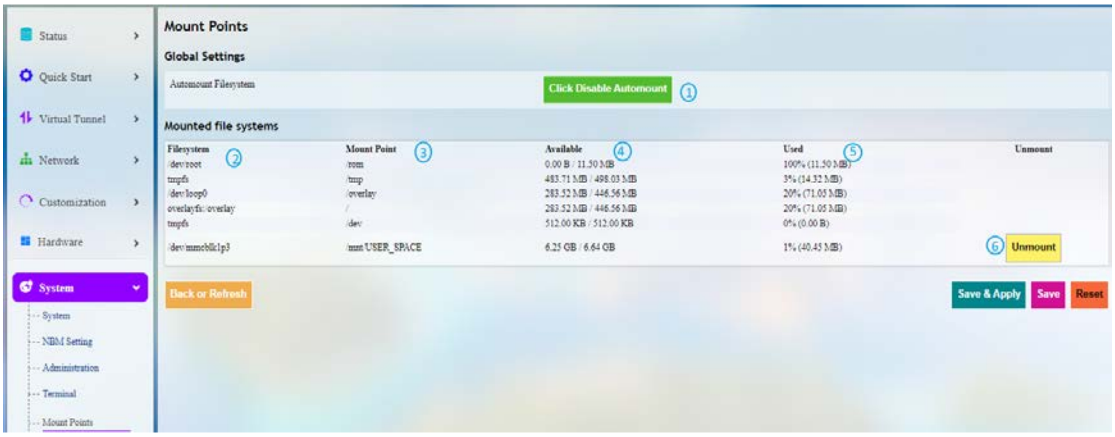
Login password: rootpassword (invisible while typing)



```
VantronOS-D869 login: root
Password:


BusyBox v1.31.1 () built-in shell (ash)

  _    __            __
 | |  / /___ _____  / /__________  ____
 | | / / __ `/ __ \/ __/ ___/ __ \/ __ \
 | |/ / /_/ / / / / /_/ /  / /_/ / / / /
 |___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -OS


-----------------------------------------------------
 V200R003.F0000-03 Built at 2024-01-30 12:45:27
-----------------------------------------------------

root@VantronOS-D869:~#
```

3.12.5 Mount Points

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



Mount Points

Global Settings

Automount Filesystem 1

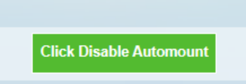
Mounted file systems

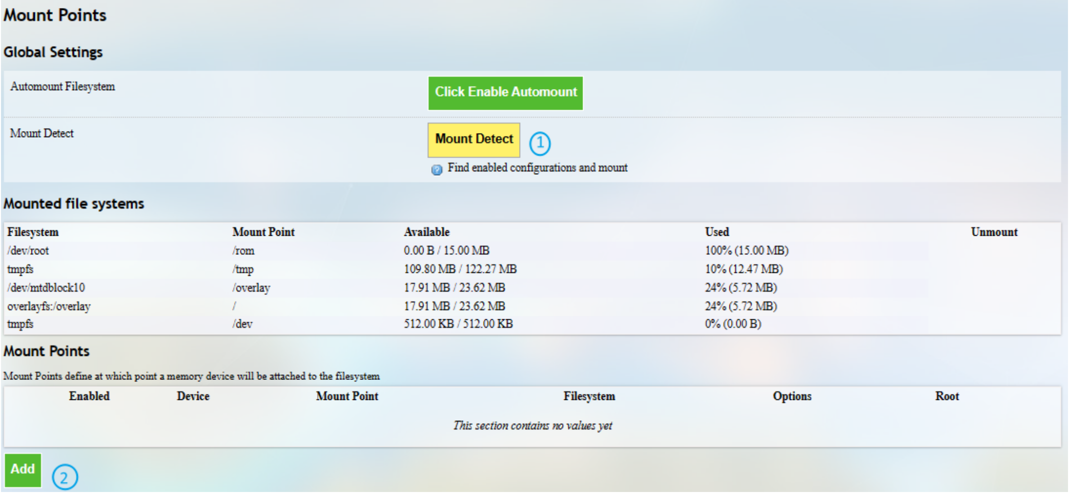
Filesystem 2	Mount Point 3	Available 4	Used 5	Unmount
/dev/root	/rom	0.00 B / 11.50 MB	100% (11.50 MB)	
tmpfs	/tmp	483.71 MB / 498.03 MB	3% (14.32 MB)	
/dev/loop0	/overlay	283.52 MB / 446.56 MB	20% (71.05 MB)	
overlayfs:/overlay	/	283.52 MB / 446.56 MB	20% (71.05 MB)	
tmpfs	/dev	512.00 KB / 512.00 KB	0% (0.00 B)	
/dev/mmcblk1p3	/mnt/USER_SPACE	6.25 GB / 6.64 GB	1% (40.45 MB)	6 Unmount

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.





Mount Points

Global Settings

Automount Filesystem — Click Enable Automount

Mount Detect — Mount Detect 1
Find enabled configurations and mount

Mounted file systems

Filesystem	Mount Point	Available	Used	Unmount
/dev/root	/rom	0.00 B / 15.00 MB	100% (15.00 MB)	
tmpfs	/tmp	109.80 MB / 122.27 MB	10% (12.47 MB)	
/dev/mtdblock10	/overlay	17.91 MB / 23.62 MB	24% (5.72 MB)	
overlayfs:/overlay	/	17.91 MB / 23.62 MB	24% (5.72 MB)	
tmpfs	/dev	512.00 KB / 512.00 KB	0% (0.00 B)	

Mount Points

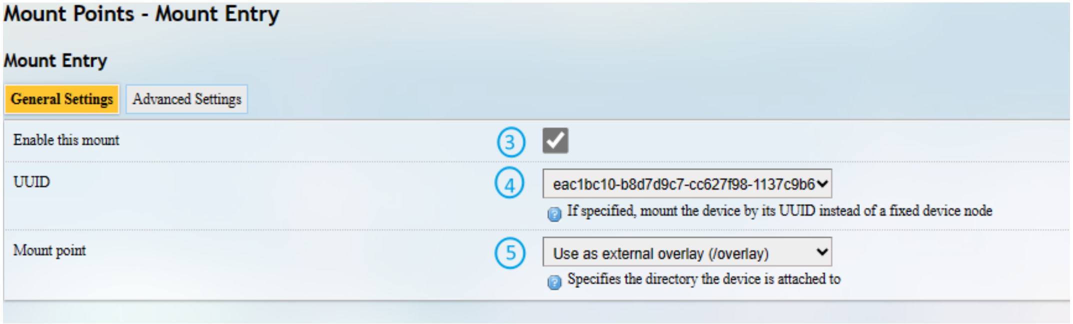
Mount Points define at which point a memory device will be attached to the filesystem

Enabled	Device	Mount Point	Filesystem	Options	Root
This section contains no values yet					

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.



Mount Points - Mount Entry

Mount Entry

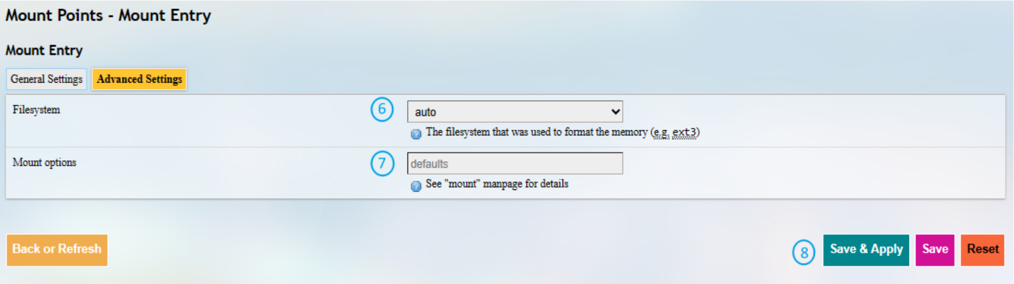
3 Enable this mount ☑

4 UUID: eac1bc10-b8d7d9c7-cc627f98-1137c9b6
If specified, mount the device by its UUID instead of a fixed device node

5 Mount point: Use as external overlay (/overlay)
Specifies the directory the device is attached to

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.



Mount Points - Mount Entry

Mount Entry

General Settings | Advanced Settings

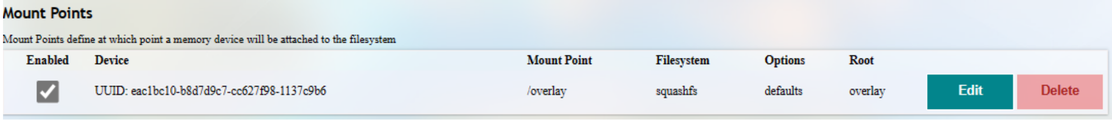
Filesystem ⑥ auto
The filesystem that was used to format the memory (e.g. ext3)

Mount options ⑦ defaults
See "mount" manpage for details

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



Mount Points

Mount Points define at which point a memory device will be attached to the filesystem

Enabled	Device	Mount Point	Filesystem	Options	Root		
☑	UUID: eac1bc10-b8d7d9c7-cc627f98-1137c9b6	/overlay	squashfs	defaults	overlay	Edit	Delete

The mount point is created as above.

3.12.6 Backup/Flash Firmware

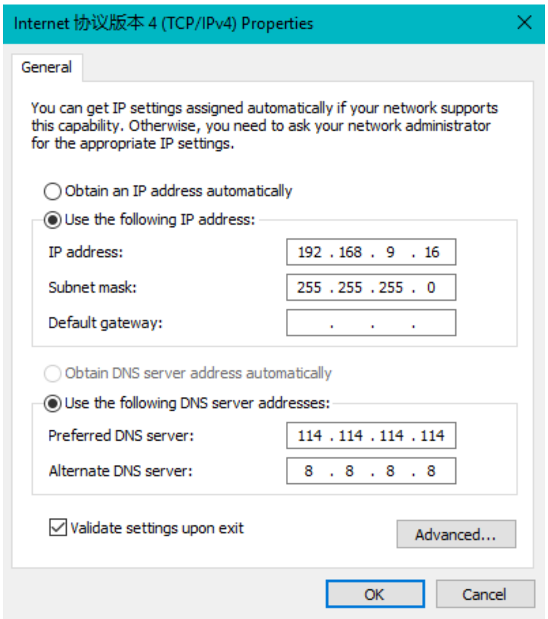
Currently HAP103 only supports firmware upgrade with TFTP rather than from the VantronOS web.

Follow the steps below for the TFTP firmware flashing on a Windows host computer.

1. Click **Control Panel\Network and Internet\Network Connections**;

2. Click the network icon and access the internet protocol (TCP/IPv4) Properties;

3. Set a static IP for the host computer like the following;



Internet 协议版本 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 9 . 16

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 114 . 114 . 114 . 114

Alternate DNS server: 8 . 8 . 8 . 8

☑ Validate settings upon exit

4. Unzip the firmware package and the package typically includes two files:

   - U-boot firmware:

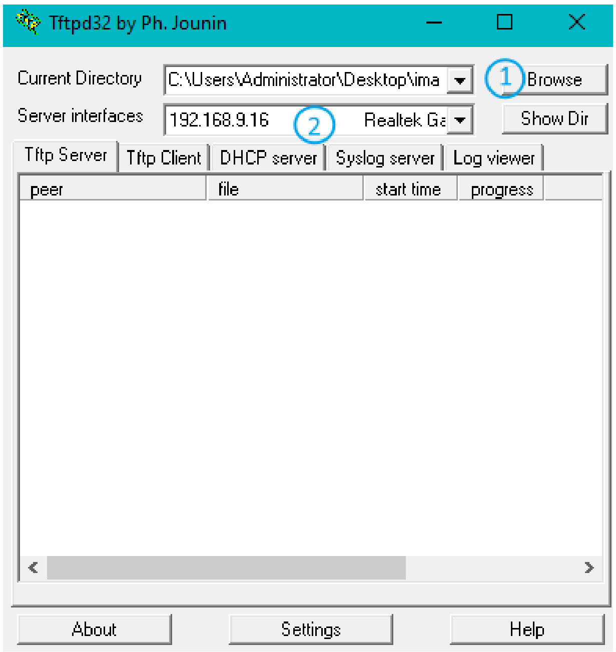
     xxxx-u-boot.bin

   - System firmware:

     xxxx-sysupgrade.bin

5. Unzip the **tftpd.zip** file to a specified folder, then open the folder and run **tftpd32.exe**;

6. Click **Browse** to open the directory of the firmware and select the static IP of the host PC as the server interface;



Current Directory: C:\Users\Administrator\Desktop\ima

Server interfaces: 192.168.9.16 Realtek Ga

Description of the numbered areas:

(1). Click **Browse** to open the directory of the firmware;

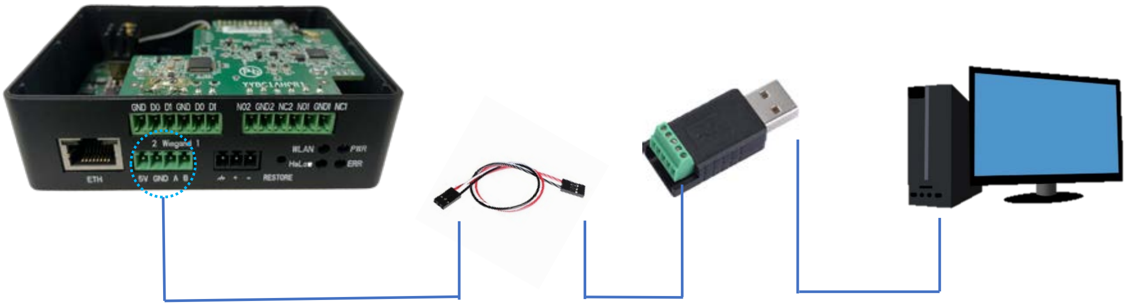
(2). Select the static IP **address** from the drop-down list (the one assigned to the host computer in step 3).

7. Connect the host computer to a router/switch for Internet access;

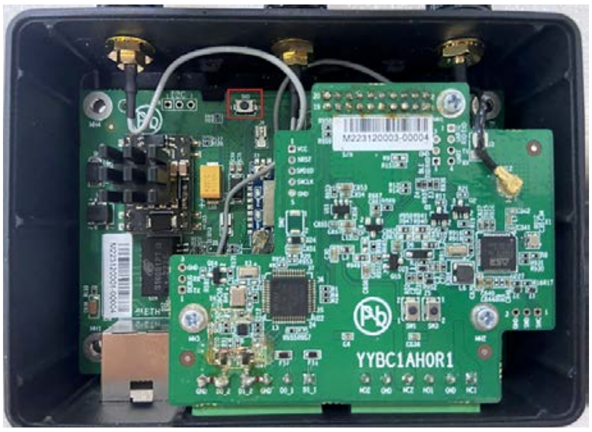
8. Connect HAP103 to the same router/switch using an Ethernet cable;

9. Unscrew the bottom screws of the device and remove the top cover;

10. Use an RS485 to USB adapter and DuPont wires or other way to connect HAP103 to the host computer;



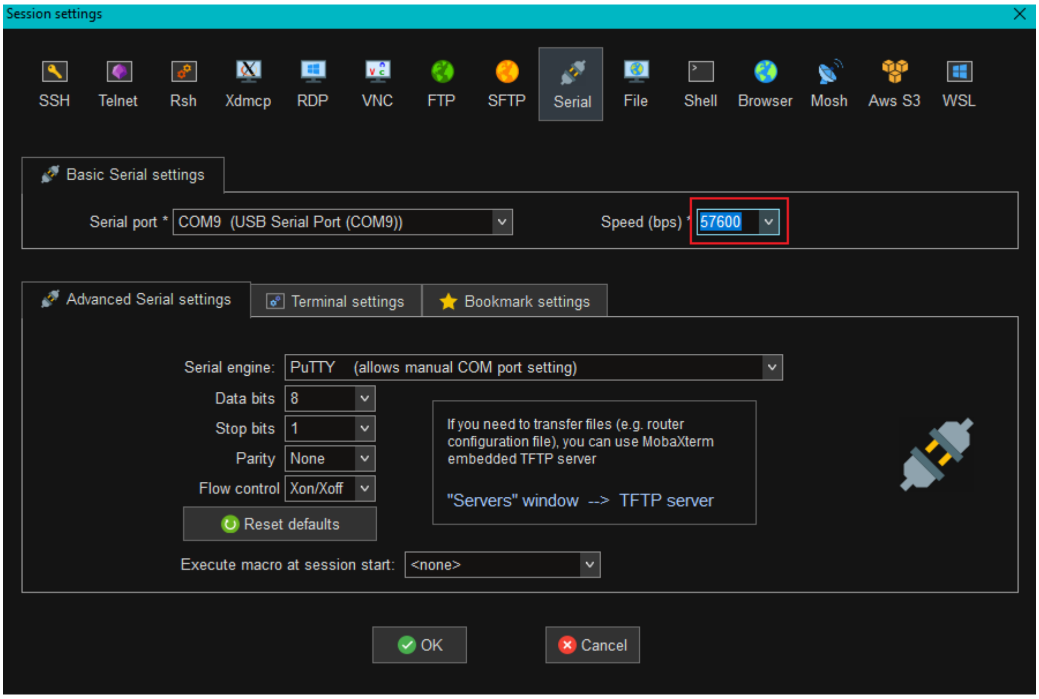
11. Press the SW3 button inside the device and do **NOT** release;



12. Power on HAP103 and release the SW3 button;

13. Open a serial communication program and launch a serial session for HAP103 using the parameters below.

Baud rate	Data bit	Polarity	Stop bit
57600	8	None	1



Basic Serial settings

Serial port * COM9 (USB Serial Port (COM9))

Speed (bps) * 57600

Advanced Serial settings

Serial engine: PuTTY (allows manual COM port setting)

Data bits 8

Stop bits 1

Parity None

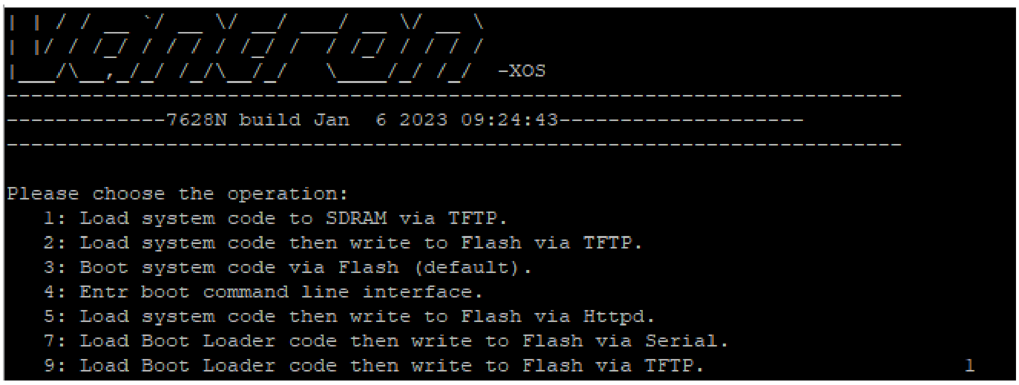
Flow control Xon/Xoff

If you need to transfer files (e.g. router configuration file), you can use MobaXterm embedded TFTP server

"Servers" window --> TFTP server

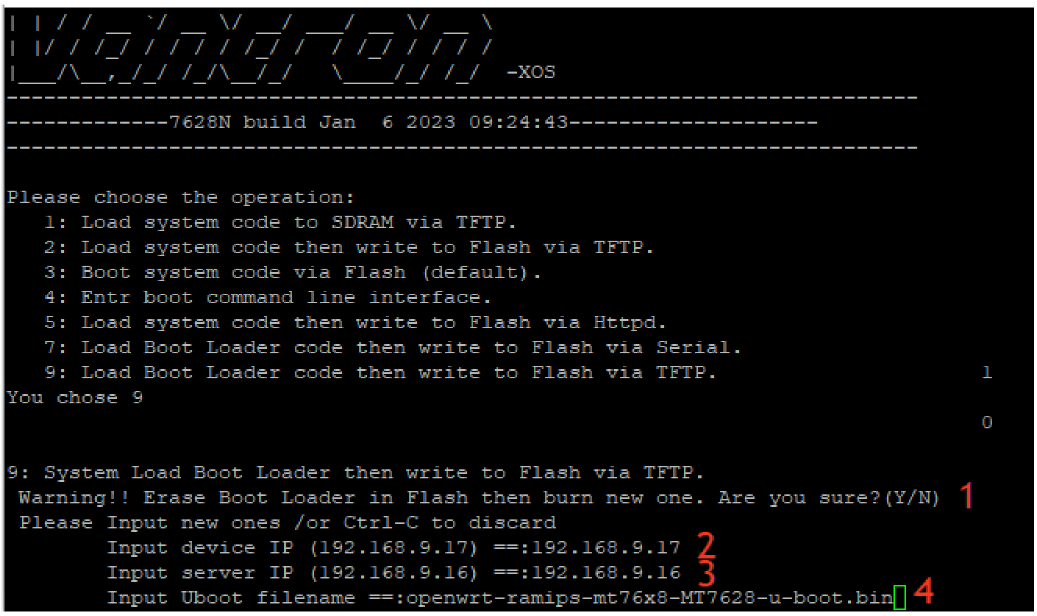
Execute macro at session start: <none>

14. Long press the SW3 button and input “9” immediately when the following prompt shows up to enter **u-boot** TFTP flashing;



```
| |/ / __ `/ __ \/ __/ ___/ __ \/ __ \
| |/ / /_/ / / / / /_/ /  / /_/ / / / /
|___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -XOS
--------------------------------------------------------------------------
-------------7628N build Jan  6 2023 09:24:43--------------------
--------------------------------------------------------------------------

Please choose the operation:
   1: Load system code to SDRAM via TFTP.
   2: Load system code then write to Flash via TFTP.
   3: Boot system code via Flash (default).
   4: Entr boot command line interface.
   5: Load system code then write to Flash via Httpd.
   7: Load Boot Loader code then write to Flash via Serial.
   9: Load Boot Loader code then write to Flash via TFTP.                    1
```

15. In the subsequent page, follow the instructions set out in the description below;



```
| | / /  __ `/  __ \/  __/  ___/  __ \/  __ \
| |/ / /_/ / / / / /_/ /   / /_/ / / / /
|___/\__,_/_/ /_/\__/_/    \____/_/ /_/  -XOS
-------------------------------------------------------------------------
-------------7628N build Jan  6 2023 09:24:43--------------------

-------------------------------------------------------------------------

Please choose the operation:
   1: Load system code to SDRAM via TFTP.
   2: Load system code then write to Flash via TFTP.
   3: Boot system code via Flash (default).
   4: Entr boot command line interface.
   5: Load system code then write to Flash via Httpd.
   7: Load Boot Loader code then write to Flash via Serial.
   9: Load Boot Loader code then write to Flash via TFTP.                  1
You chose 9
                                                                           0

9: System Load Boot Loader then write to Flash via TFTP.
 Warning!! Erase Boot Loader in Flash then burn new one. Are you sure?(Y/N)
 Please Input new ones /or Ctrl-C to discard
        Input device IP (192.168.9.17) ==:192.168.9.17
        Input server IP (192.168.9.16) ==:192.168.9.16
        Input Uboot filename ==:openwrt-ramips-mt76x8-MT7628-u-boot.bin
```

Description of the numbered areas:

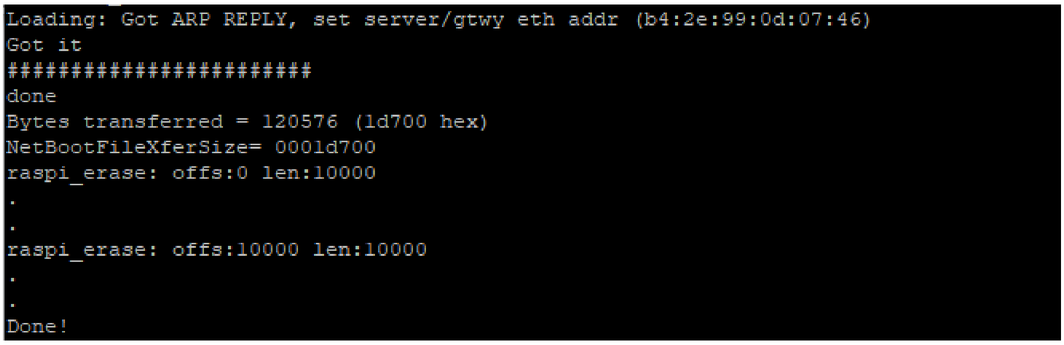
(1). Input “Y”;

(2). Input an IP address on the same network as the host PC, and press **Enter**;

(3). Input the static IP of the host PC (TFTP server), and press **Enter**;

(4). Input the file name of u-boot firmware, and press **Enter**.

16. U-boot flashing finishes when the window changes to the following;

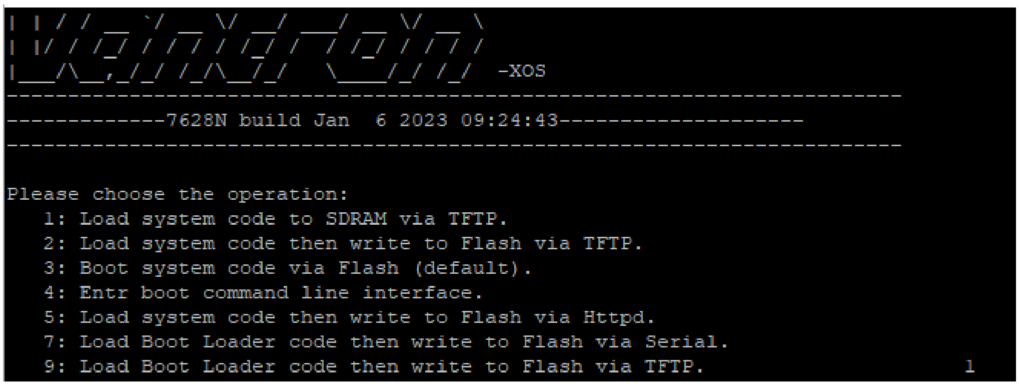


```
Loading: Got ARP REPLY, set server/gtwy eth addr (b4:2e:99:0d:07:46)
Got it
########################
done
Bytes transferred = 120576 (1d700 hex)
NetBootFileXferSize= 0001d700
raspi_erase: offs:0 len:10000
.
.
raspi_erase: offs:10000 len:10000
.
.
Done!
```

17. Press the SW3 button and hold it before re-powering the device;

18. Follow step 13 to open the serial port;

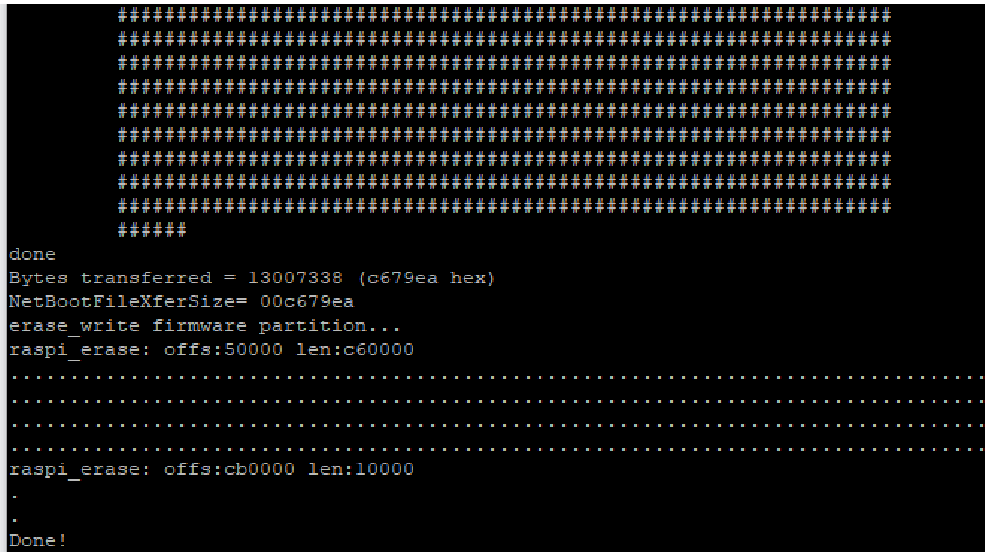
19. Long press the SW3 button and input “2” immediately when the following prompt shows up to enter **system** TFTP flashing;



```
| | / / __ `/ __ \/ __/ ___/ __ \/ __ \
| |/ / /_/ / / / / /_/ /  / /_/ / / / /
|___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -XOS
--------------------------------------------------------------------------
-------------7628N build Jan  6 2023 09:24:43--------------------
--------------------------------------------------------------------------

Please choose the operation:
   1: Load system code to SDRAM via TFTP.
   2: Load system code then write to Flash via TFTP.
   3: Boot system code via Flash (default).
   4: Entr boot command line interface.
   5: Load system code then write to Flash via Httpd.
   7: Load Boot Loader code then write to Flash via Serial.
   9: Load Boot Loader code then write to Flash via TFTP.                   1
```

20. Follow the same operations as out in step 15;

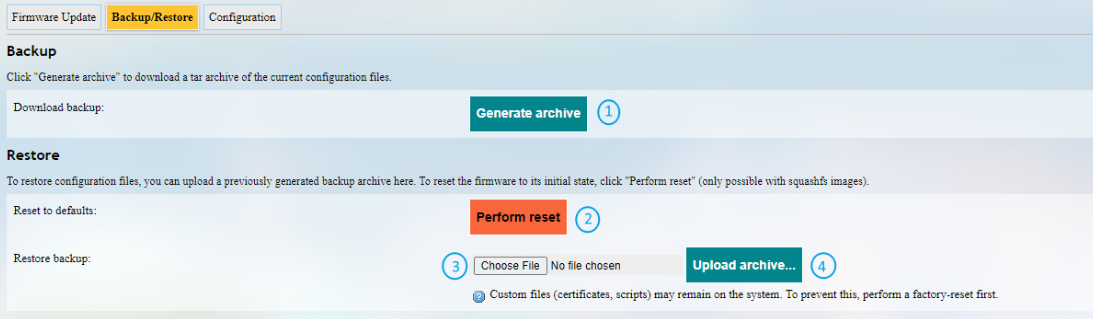
21. System flashing finishes when the window changes to the following;



```
         ################################################################
         ################################################################
         ################################################################
         ################################################################
         ################################################################
         ################################################################
         ################################################################
         ################################################################
         ################################################################
         ######
done
Bytes transferred = 13007338 (c679ea hex)
NetBootFileXferSize= 00c679ea
erase_write firmware partition...
raspi_erase: offs:50000 len:c60000
.................................................................................
.................................................................................
.................................................................................
.................................................................................
raspi_erase: offs:cb0000 len:10000
.
.
Done!
```

22. The device will restart when the flashing finishes.

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.



Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup:

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults:

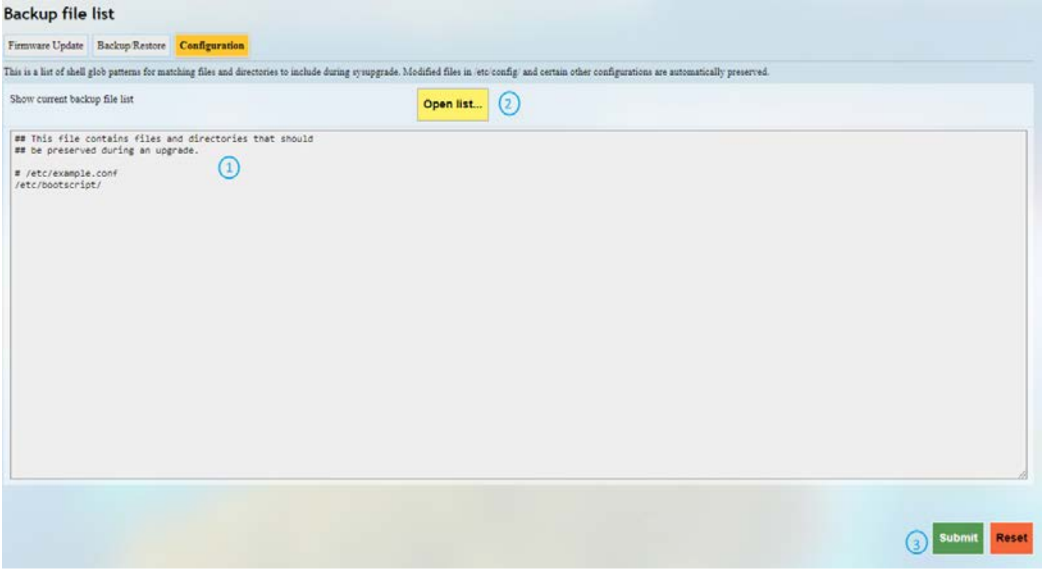
Restore backup: No file chosen

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

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 client 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.



Backup file list

This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modified files in /etc/config/ and certain other configurations are automatically preserved.

Show current backup file list

```
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
/etc/bootscript/
```

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.

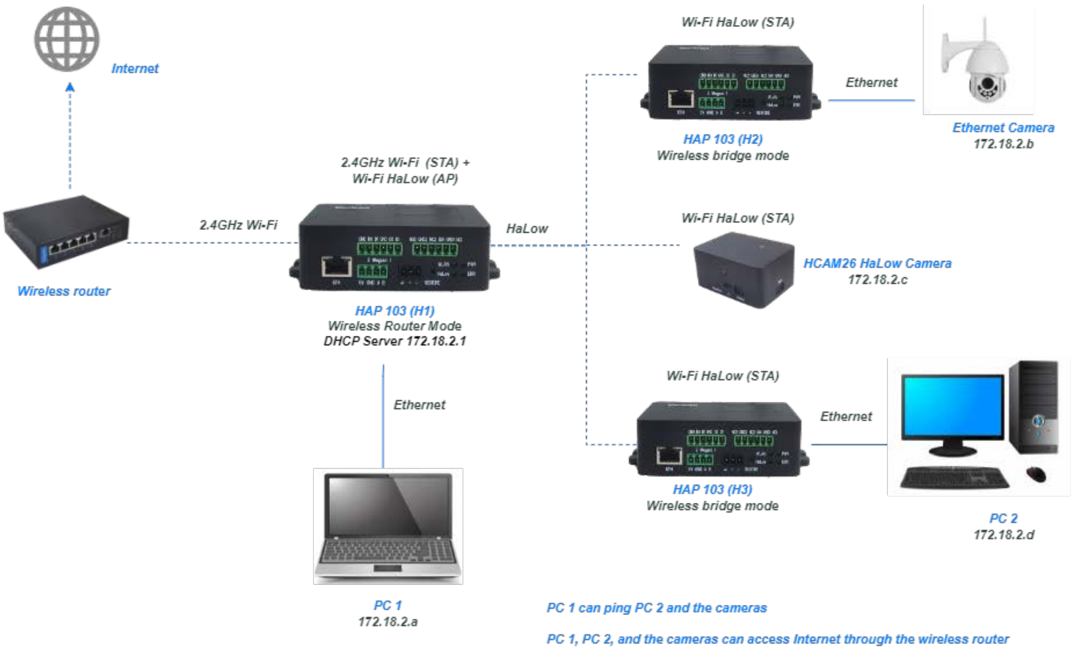
3.13 Logout

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 HAP103 devices is to monitor the status of connected cameras.

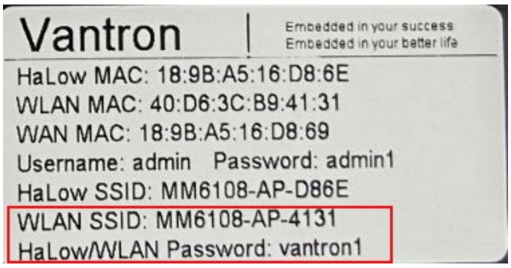


In the above topology, three HAP103 devices are used.

- 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)

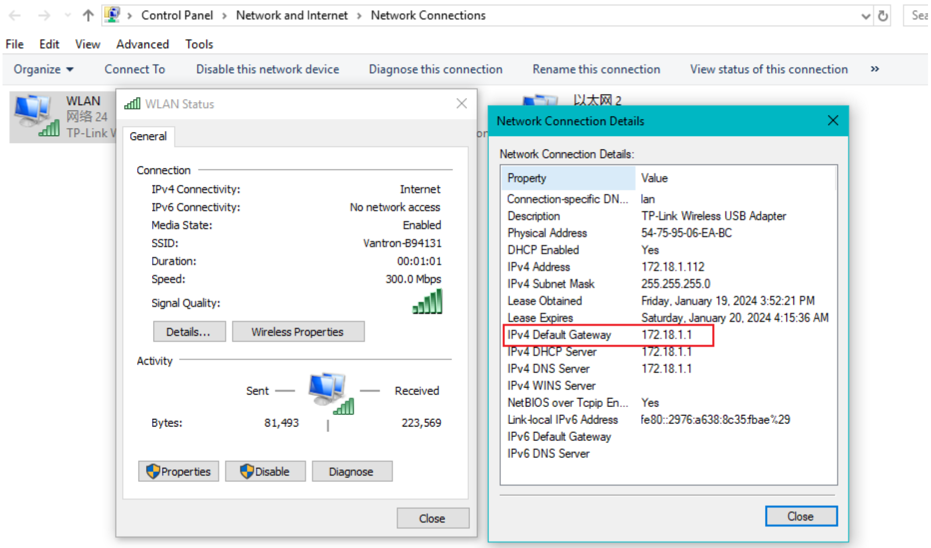
1. Connect PC 1 to the HaLow-AP-mode HAP103 (H1) via 2.4GHz Wi-Fi using the WLAN SSID and password provided on the device label (like the following);



Vantron | Embedded in your success
Embedded in your better life

HaLow MAC: 18:9B:A5:16:D8:6E
WLAN MAC: 40:D6:3C:B9:41:31
WAN MAC: 18:9B:A5:16:D8:69
Username: admin Password: admin1
HaLow SSID: MM6108-AP-D86E
WLAN SSID: MM6108-AP-4131
HaLow/WLAN Password: vantron1

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



Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
SSID:	Vantron-B94131
Duration:	00:01:01
Speed:	300.0 Mbps
Signal Quality:	

Activity

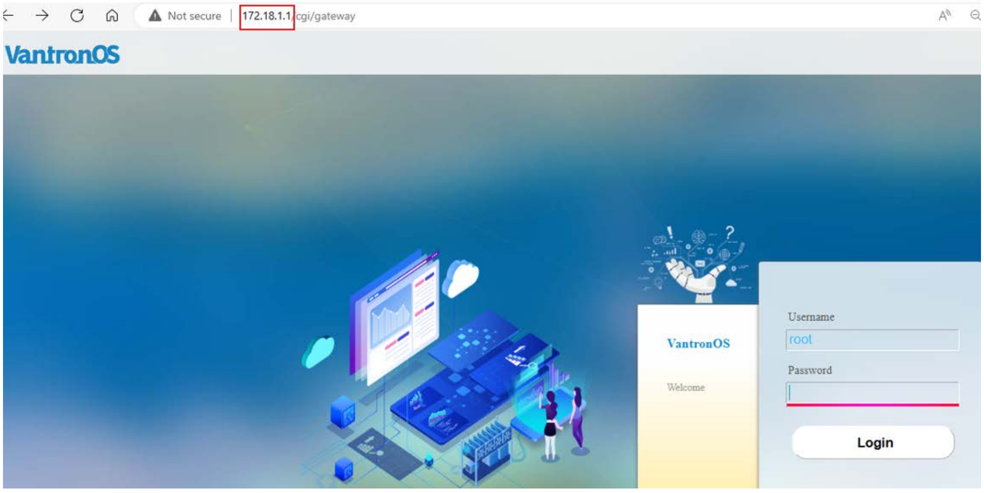
	Sent	Received
Bytes:	81,493	223,569

Network Connection Details:

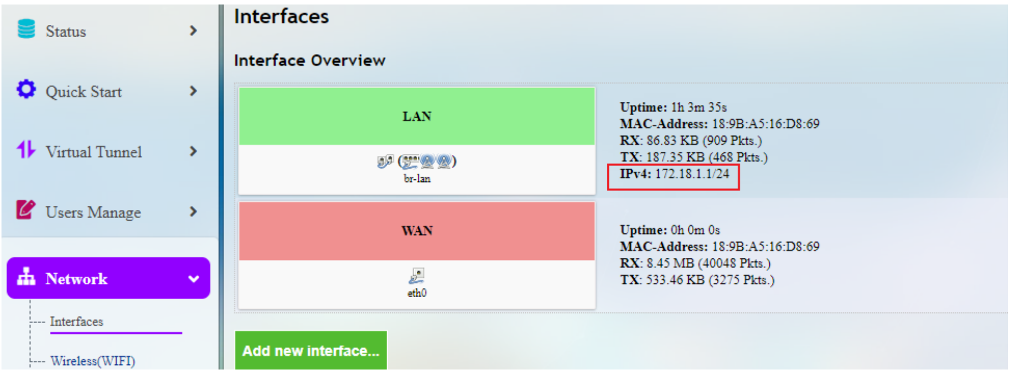
Property	Value
Connection-specific DN...	lan
Description	TP-Link Wireless USB Adapter
Physical Address	54-75-95-06-EA-BC
DHCP Enabled	Yes
IPv4 Address	172.18.1.112
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, January 19, 2024 3:52:21 PM
Lease Expires	Saturday, January 20, 2024 4:15:36 AM
IPv4 Default Gateway	172.18.1.1
IPv4 DHCP Server	172.18.1.1
IPv4 DNS Server	172.18.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::2976:a638:8c35:fbae%29
IPv6 Default Gateway	
IPv6 DNS Server	

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);

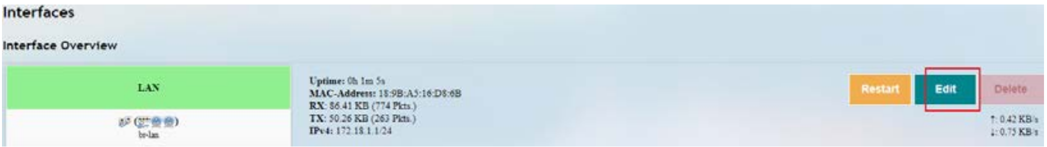


LAN
Uptime: 1h 3m 35s
MAC-Address: 18:9B:A5:16:D8:69
RX: 86.83 KB (909 Pkts.)
TX: 187.35 KB (468 Pkts.)
IPv4: 172.18.1.1/24

WAN
Uptime: 0h 0m 0s
MAC-Address: 18:9B:A5:16:D8:69
RX: 8.45 MB (40048 Pkts.)
TX: 533.46 KB (3275 Pkts.)

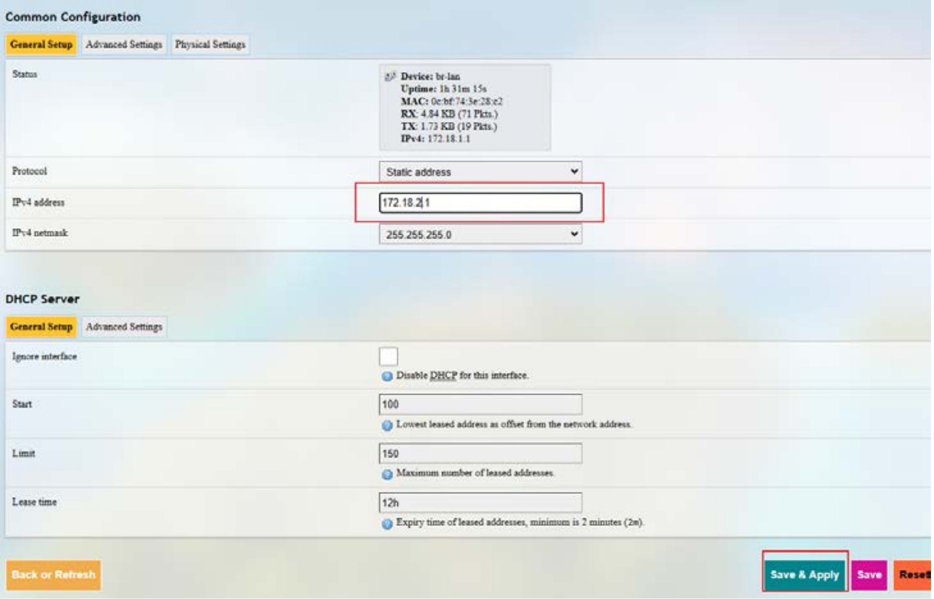
Since the virtual LAN IP addresses of all HAP103 devices are the same by default. To ensure valid dynamic IP assignment to H2 and H3 that will be connected to H1 in the following steps, please change the LAN IP of H1 to a ***different*** *one (e.g., 172.18.2.1).*

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



Uptime: 0h 1m 5s
MAC-Address: 18:9B:A5:16:D8:6B
RX: 86.41 KB (774 Pkts.)
TX: 50.26 KB (263 Pkts.)
IPv4: 172.18.1.1/24

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



Common Configuration

Status: Device: br-lan
Uptime: 1h 31m 15s
MAC: 0c:bf:74:3e:28:c2
RX: 4.84 KB (71 Pkts.)
TX: 1.73 KB (19 Pkts.)
IPv4: 172.18.1.1

Protocol: Static address

IPv4 address: 172.18.2.1

IPv4 netmask: 255.255.255.0

DHCP Server

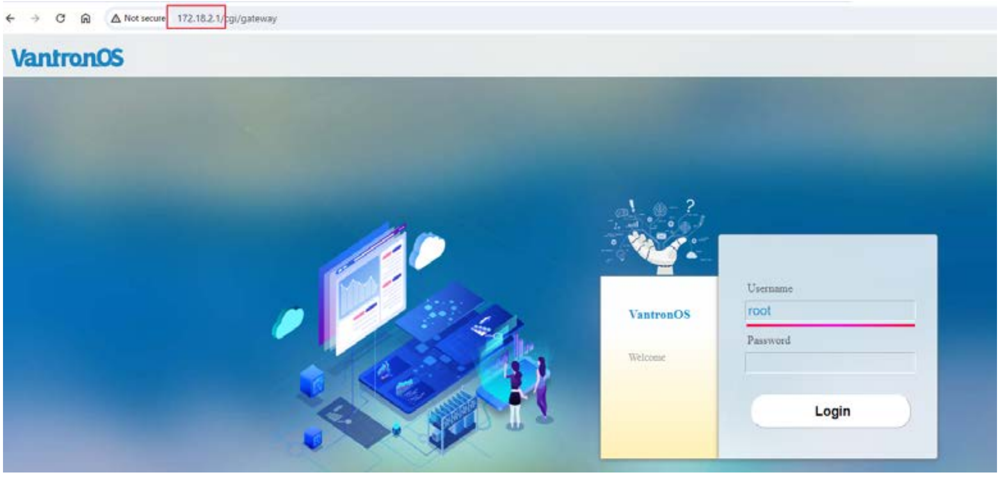
Ignore interface: □ Disable DHCP for this interface.

Start: 100 — Lowest leased address as offset from the network address.

Limit: 150 — Maximum number of leased addresses.

Lease time: 12h — Expiry time of leased addresses, minimum is 2 minutes (2m).

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



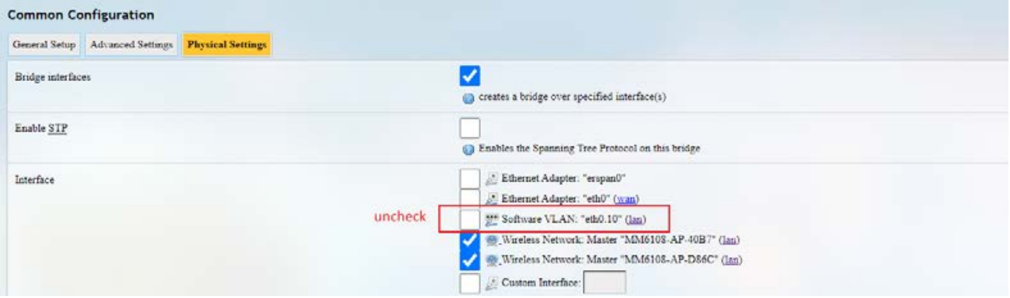
Not secure 172.18.2.1/cgi/gateway

Username: root

Password:

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

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



Common Configuration

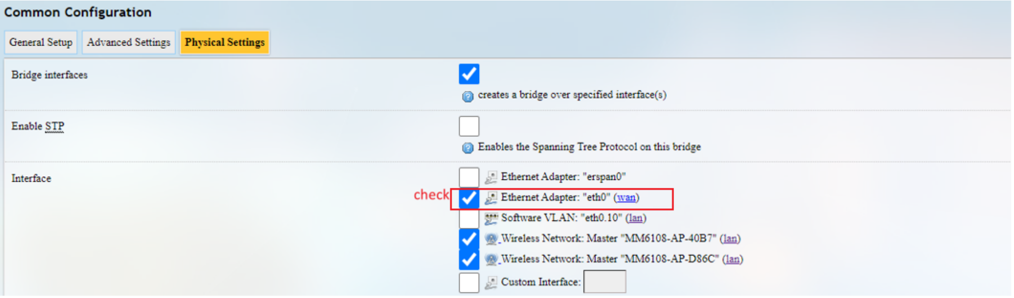
Bridge interfaces: ☑ creates a bridge over specified interface(s)

Enable STP: □ Enables the Spanning Tree Protocol on this bridge

Interface:
□ Ethernet Adapter: "erspan0"
□ Ethernet Adapter: "eth0" (wan)
□ Software VLAN: "eth0.10" (lan)
☑ Wireless Network: Master "MM6108-AP-40B7" (lan)
☑ Wireless Network: Master "MM6108-AP-D86C" (lan)
□ Custom Interface:

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;



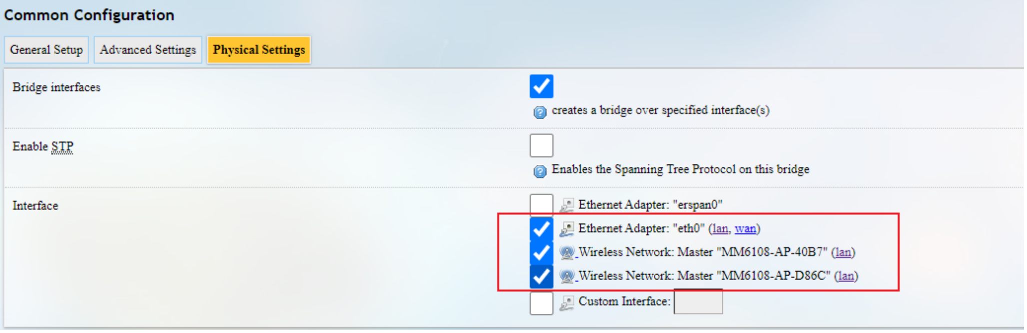
Common Configuration

Bridge interfaces ☑ creates a bridge over specified interface(s)

Enable STP □ Enables the Spanning Tree Protocol on this bridge

Interface
□ Ethernet Adapter: "erspan0"
check ☑ Ethernet Adapter: "eth0" (wan)
Software VLAN: "eth0.10" (lan)
☑ Wireless Network: Master "MM6108-AP-40B7" (lan)
☑ Wireless Network: Master "MM6108-AP-D86C" (lan)
□ Custom Interface:

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



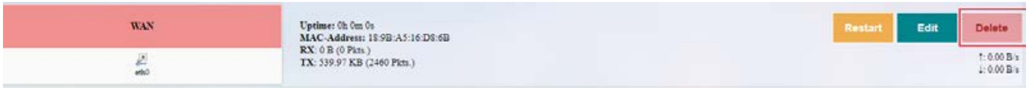
Common Configuration

Bridge interfaces ☑ creates a bridge over specified interface(s)

Enable STP □ Enables the Spanning Tree Protocol on this bridge

Interface
□ Ethernet Adapter: "erspan0"
☑ Ethernet Adapter: "eth0" (lan, wan)
☑ Wireless Network: Master "MM6108-AP-40B7" (lan)
☑ Wireless Network: Master "MM6108-AP-D86C" (lan)
□ Custom Interface:

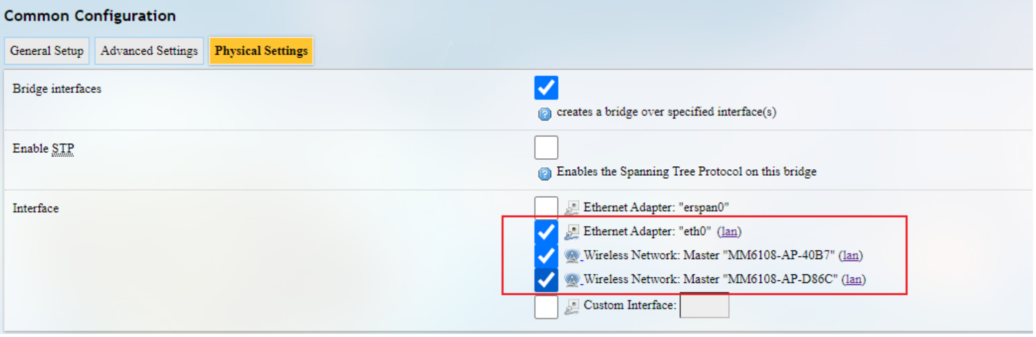
13. Return to the **Interfaces** window, and click the **Delete** button behind the WAN port to change the Ethernet jack of H1 to LAN;



Uptime: 0h 0m 0s
MAC-Address: 18:9B:A5:16:D8:6B
RX: 0 B (0 Pkts.)
TX: 539.97 KB (2460 Pkts.)

↑: 0.00 B/s
↓: 0.00 B/s

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



Common Configuration

Bridge interfaces ☑ creates a bridge over specified interface(s)

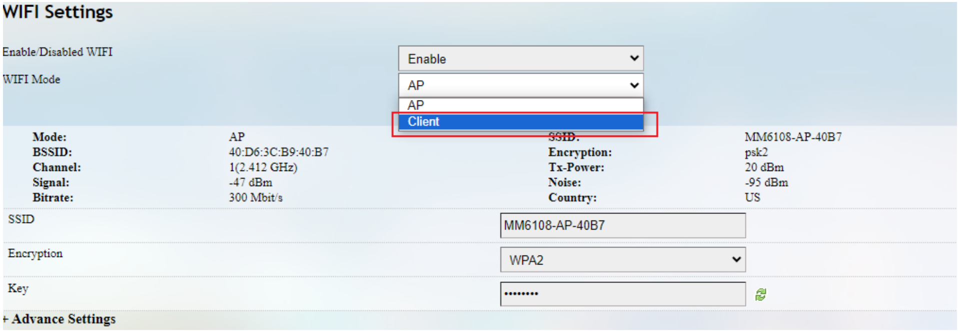
Enable STP □ Enables the Spanning Tree Protocol on this bridge

Interface
□ Ethernet Adapter: "erspan0"
☑ Ethernet Adapter: "eth0" (lan)
☑ Wireless Network: Master "MM6108-AP-40B7" (lan)
☑ Wireless Network: Master "MM6108-AP-D86C" (lan)
□ Custom Interface:

15. Use an Ethernet cable to connect H1 and PC1, and log in to VantronOS for H1 with the new gateway IP (LAN IP) set in step 6;

16. Navigate to **Network > Wireless (WIFI)**;

17. Change the 2.4GHz Wi-Fi mode of H1 to **Client**;



WIFI Settings

Enable/Disabled WIFI: Enable

WIFI Mode: AP

Mode: AP
BSSID: 40:D6:3C:B9:40:B7
Channel: 1(2.412 GHz)
Signal: -47 dBm
Bitrate: 300 Mbit/s
SSID: MM6108-AP-40B7
Encryption: psk2
Tx-Power: 20 dBm
Noise: -95 dBm
Country: US

SSID: MM6108-AP-40B7

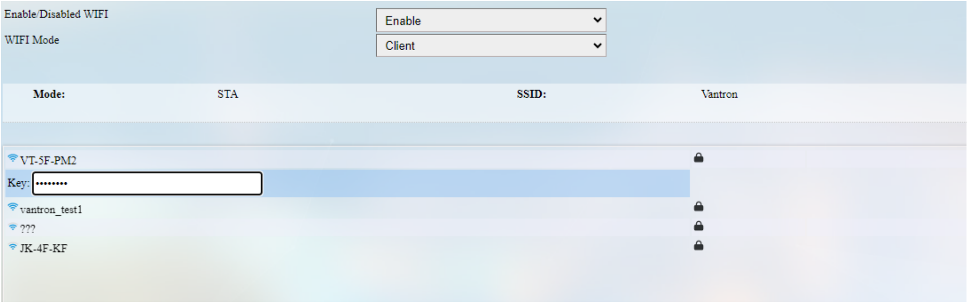
Encryption: WPA2

Key: ••••••••

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;



Enable/Disabled WIFI: Enable

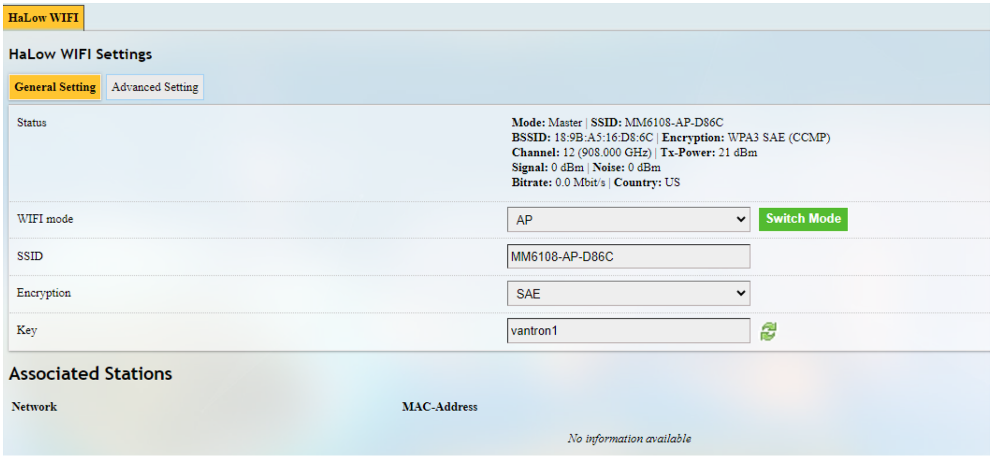
WIFI Mode: Client

Mode: STA
SSID: Vantron

VT-5F-PM2
Key: ••••••••
vantron_test1
???
JK-4F-KF

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.



HaLow WIFI Settings

Status:
Mode: Master | **SSID:** MM6108-AP-D86C
BSSID: 18:9B:A5:16:D8:6C | **Encryption:** WPA3 SAE (CCMP)
Channel: 12 (908.000 GHz) | **Tx-Power:** 21 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

WIFI mode: AP

SSID: MM6108-AP-D86C

Encryption: SAE

Key: vantron1

Associated Stations

Network	MAC-Address
No information available	

4.3 Setup of H2 and H3 (HaLow STA mode)

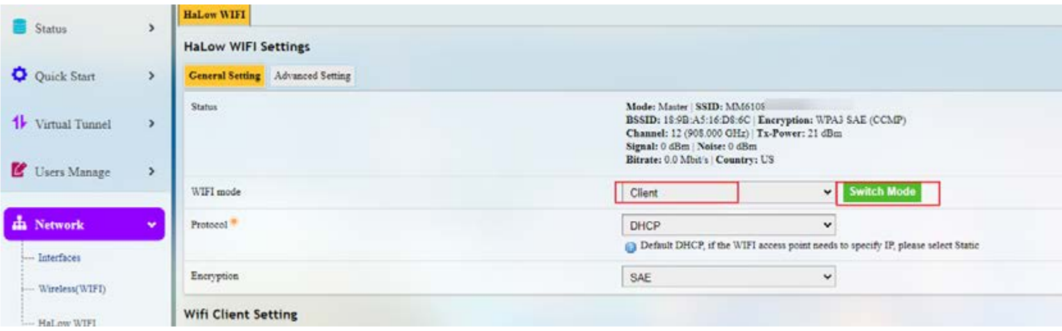
1. Use the WLAN SSID and password provided on the device label to connect PC 2 to H2 via 2.4GHz Wi-Fi;

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**;



HaLow WIFI Settings

Status: **Mode:** Master | **SSID:** MM6108
BSSID: 18:9B:A5:16:D8:6C | **Encryption:** WPA3 SAE (CCMP)
Channel: 12 (908.000 GHz) | **Tx-Power:** 21 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

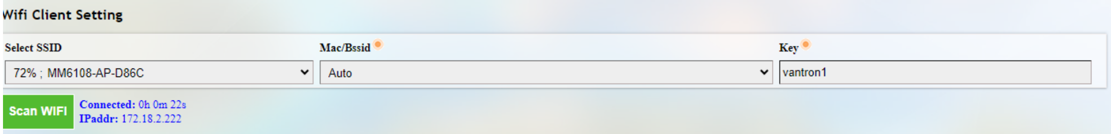
WIFI mode: Client

Protocol: DHCP
Default DHCP, if the WIFI access point needs to specify IP, please select Static

Encryption: SAE

Wifi Client Setting

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

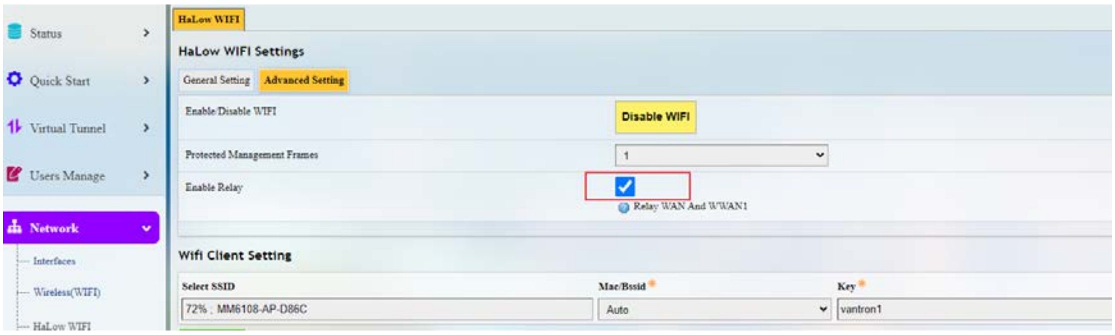


Wifi Client Setting

Select SSID	Mac/Bssid	Key
72% ; MM6108-AP-D86C	Auto	vantron1

Connected: 0h 0m 22s
IPaddr: 172.18.2.222

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



HaLow WIFI Settings

Enable/Disable WIFI: Disable WIFI

Protected Management Frames: 1

Enable Relay: ☑
Relay WAN And WWAN1

Wifi Client Setting

Select SSID	Mac/Bssid	Key
72% ; MM6108-AP-D86C	Auto	vantron1

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

4.4 Setup of the Cameras and Connection Testing

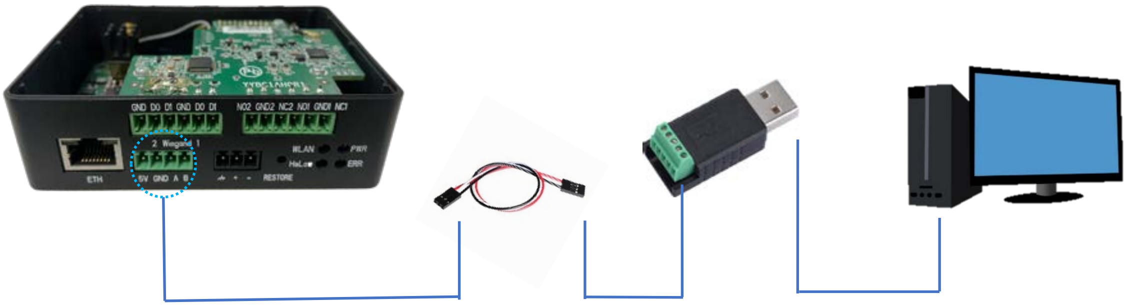
1. Use a USB Type-A to Type-C cable to connect HCAM26 HaLow IP camera to the host computer;
2. Enter the device shell and connect it to H1 via Wi-Fi HaLow using ABD commands;

   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.

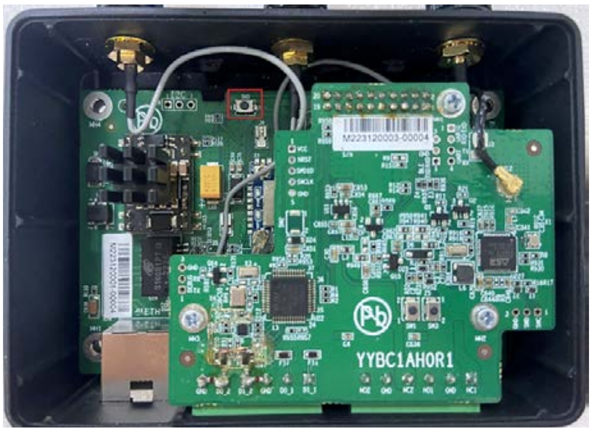
CHAPTER 5 DEBUGGING THE DEVICE

In the event that you need to debug HAP103, please follow the steps below to set up the device.

1. Connect the host computer to a router/switch for Internet access;
2. Connect HAP103 to the same router/switch using an Ethernet cable;
3. Unscrew the bottom screws of the device and remove the top cover;
4. Use an RS485 to USB adapter and DuPont wires or other way to connect HAP103 to the host computer;



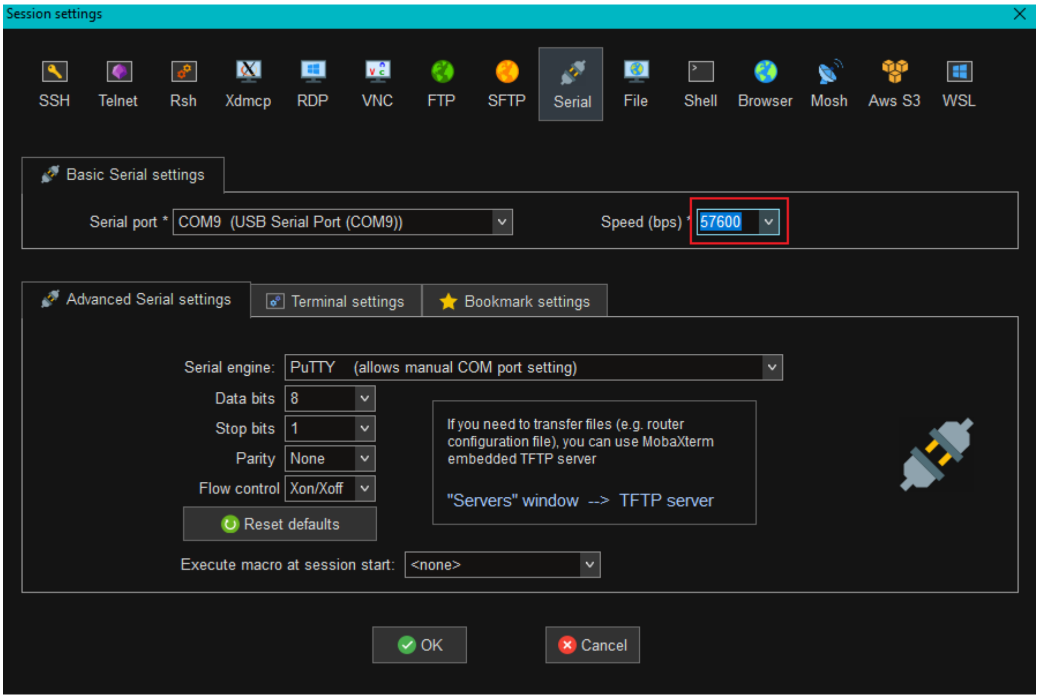
5. Press the SW3 button inside the device and do **NOT** release;



6. Power on HAP103 and release the SW3 button;

7. Open a serial communication program and launch a serial session for HAP103 using the parameters below.

Baud rate	Data bit	Polarity	Stop bit
57600	8	None	1



Serial port * COM9 (USB Serial Port (COM9))

Speed (bps) * 57600

Serial engine: PuTTY (allows manual COM port setting)

Data bits 8

Stop bits 1

Parity None

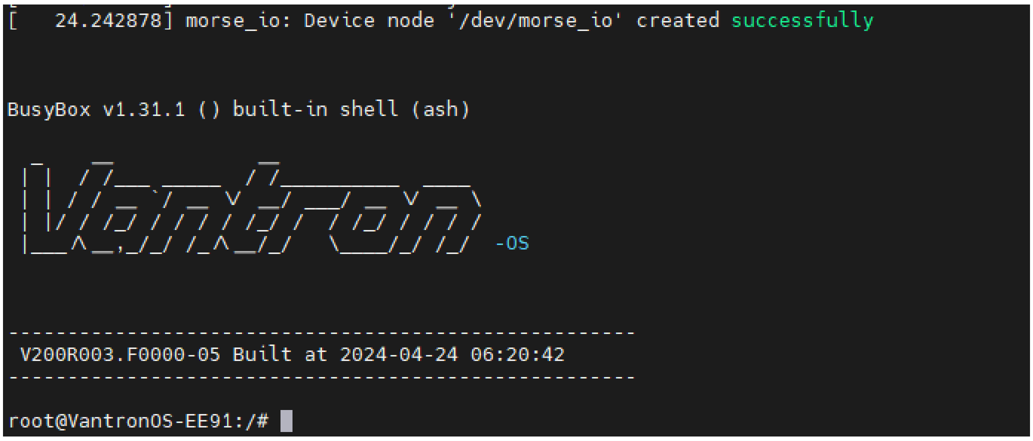
Flow control Xon/Xoff

Execute macro at session start: <none>

If you need to transfer files (e.g. router configuration file), you can use MobaXterm embedded TFTP server

"Servers" window --> TFTP server

8. Wait for the printing process of the device information;
9. When the message for successful device creation appears, press **Enter** and proceed with the debugging operations.



```
[   24.242878] morse_io: Device node '/dev/morse_io' created successfully


BusyBox v1.31.1 () built-in shell (ash)

  _    __            __
 | |  / /___ _____  / /__________  ____
 | | / / __ `/ __  V __/ ____/ __  V __ \
 | |/ / /_/ / / / / / /_/ /  / /_/ / / / /
 |___^__,_/_/ /_^__/_/  \____/_/ /_/  -OS


-----------------------------------------------------
 V200R003.F0000-05 Built at 2024-04-24 06:20:42
-----------------------------------------------------

root@VantronOS-EE91:/#
```

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.