HAP101 Wi-Fi HaLow Access Point



User Manual

Version: 2.4

© Vantron Technology, Inc. All rights reserved.

Revision History:

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

Table of Contents

Foreword		1
CHAPTER 1	DEVICE INTRODUCTION	5
1.1	Product Overview	6
1.2	Unpacking	6
1.3	Terminologies and Acronyms	7
1.4	Specifications	8
1.5	Interfaces and Indicators	9
1.5.1	Front view	9
1.5.2	Back view	10
1.6	DIP Switches	11
1.7	Pair/Restore Button	11
1.7.1	Button state: HaLow DPP & factory reset	12
1.7.2	Button state in combination with switches & LEDs	13
1.8	LED Indicators	13
1.8.1	WLAN indicator	13
1.8.2	HaLow indicator	14
1.8.3	Up & Down indicators	14
1.8.4	Restore indicator	15
1.8.5	Power indicator	15
1.8.6	System indicator	15
1.8.7	Error indicator	16
1.9	Serial Port	16
CHAPTER 2	GETTING STARTED	17
2.1	Setting up the Device	18
2.2	Pairing Two HAP101 Devices	19
2.2.1	Pairing via station setup on the web portal	19
2.2.2	HaLow DPP pairing via hardware setup	22
2.2.3	HaLow DPP pairing via software setup	23
2.3	Web Login	25
2.3.1	Login via the 2.4GHz WLAN IP	26
2.3.2	Login via the VLAN IP (Windows PC)	28
2.3.3	Login via the VLAN IP (Linux PC)	31
2.3.4	Login via the WAN port IP	33
2.4	SSH Login	34
2.5	Wi-Fi HaLow Mode	35
2.5.1	AP mode	35
2.5.2	Station mode	38
2.5.3	Mesh mode	39
2.6	Network Interface Bridging	41
2.7	Ethernet Port Modification	42
2.7.1	WAN port to LAN port	42
a.	AP-mode HAP101 with 2.4GHz Wi-Fi in Client Mode	42
b.	STA-mode HAP101 with Bridged 2.4GHz Wi-Fi	44

	2.7.2	LAN port back to WAN port47		
	2.8	Password Change		
	2.9	Language Change	.50	
	2.10	Factory Reset the Device	.51	
	2.10.1	Hardware reset	.51	
	2.10.2	Software reset	.51	
CHA	PTER 3	DEVICE SETUP IN VANTRONOS	52	
	3.1	Introduction to VantronOS	.53	
	3.2	Status	.54	
	3.3	Route Management	.55	
	3.3.1	Automatic network routing	.55	
	3.3.2	Static routing	.56	
	3.4	Network	.58	
	3.4.1	Interfaces	.58	
	3.4.1.1	LAN	. 59	
	3.4.1.2	WAN	.61	
	3.4.2	Wireless (WIFI)	.64	
	3.4.2.1	Wi-Fi – AP Mode	.64	
	3.4.2.2	Wi-Fi – Client Mode	.65	
	3.4.3	Wi-Fi HaLow	.66	
	3.4.4	Diagnostics	.66	
	3.4.5	Network capture	.66	
	3.5	Services – DHCP Server	.69	
	3.6	Security – ACL	.70	
	3.6.1	Whitelist ACL rule	.71	
	3.6.2	Blacklist ACL rule	.73	
	3.7	Advanced Features	.75	
	3.7.1	IPK Installer	.75	
	3.8	BlueSphere	.76	
	3.9	User Management	.78	
	3.10	System	.80	
	3.10.1	System	.80	
	3.10.2	Administration	.81	
	SSH Log	;in	.81	
	3.10.3	Log	.83	
	3.10.4	Terminal	.84	
	3.10.5	Backup/Flash Firmware	.85	
	3.10.6	Reboot	.87	
	3.11	Logout	.87	
CHA	PTER 4	USE CASE	88	
	4.1	Application Topology	.89	
	4.2	Wiring	.90	
	4.3	Setup of HAP101-STA	.90	
	4.3.1	HaLow	.90	
	4.3.2	Reconfiguring WAN to LAN	.92	

4.3.3	2.4GHz Wi-Fi	93
4.4	Viewing Camera IPs	94
CHAPTER 5	DEBUGGING THE DEVICE	95
CHAPTER 6	DISPOSAL AND PRODUCT WARRANTY	98
6.1	Disposal	
6.2	Warranty	
Appendix	Regulatory Compliance Statement	101

Foreword

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

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

Intended Users

This manual is intended for:

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

Copyright

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 <u>www.vantrontech.com</u>.

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.

Â	Caution for latent damage to system or harm to personnel
Ì	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.
- \triangle 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
- A Power off and contact Vantron technical support engineer in case of the following faults:
 - The Product is damaged
 - The temperature is excessively high
 - Fault is still not solved after troubleshooting according to this manual
- ⚠ Do not use in combustible and explosive environment:
 - Keep away from combustible and explosive environment
 - Keep away from all energized circuits
 - Unauthorized removal of the enclosure from the device is not allowed
 - Do not change components unless the power cable is unplugged
 - In some cases, the device may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the device before replacement of the components.

CHAPTER 1 DEVICE INTRODUCTION

1.1 Product Overview

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

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

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

1.2 Unpacking

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

Standard accessories:

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

Optional accessories:

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

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

1.3 Terminologies and Acronyms

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

Table 1-1

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

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

7

1.4 Specifications

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

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

1.5 Interfaces and Indicators

1.5.1 Front view



I/O description:

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

1.5.2 Back view



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

1.6 DIP Switches

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

Table 1-2

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

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

1.7 Pair/Restore Button

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

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

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

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

* Refer to table 1-1 in <u>1.3</u> for the details of the mode.

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

1.7.1 Button state: HaLow DPP & factory reset

Table 1-3

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

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

1.7.2 Button state in combination with switches & LEDs

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





1.8 LED Indicators

1.8.1 WLAN indicator

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

- a. 2.4GHz Wi-Fi module not working: OFF;
- b. 2.4GHz Wi-Fi module working: Solid green;
- c. 2.4GHz Wi-Fi communication in progress: Blinking regularly;
- d. Upon a successful 2.4GHz Wi-Fi connection, the indicator blinks regularly. Meanwhile the UP/DOWN indicator (depending on whether the device is a 2.4GHz Wi-Fi AP or client) will blink at 4Hz for 3s, and later turns solid green;
- e. When the device is ready for factory reset, the indicator blinks at 2Hz. After the user confirms the state, the indicator will blink at 4Hz, indicating the device is undergoing a factory reset. Upon successful factory reset, the indicator will turn solid green.

1.8.2 HaLow indicator

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

- a. Wi-Fi HaLow module not working: OFF;
- b. Wi-Fi HaLow module working: Solid green;
- c. Wi-Fi HaLow communication in progress: Blinking regularly;
- d. When short pressing the Pair/Restore pinhole button to enter the HaLow DPP state:
- 1) The device enters the HaLow DPP state upon a short press of the button and the HaLow indicator blinks at a frequency of 1Hz;
- 2) When there is no action within 3 seconds, the device will confirm the HaLow DPP state and the indicator will blink at a frequency of 2Hz;
- 3) When the device is pairing with another device via Wi-Fi HaLow, the indicator will blink at a frequency of 4Hz;
- 4) Upon successful connection, the device will exit the HaLow DPP mode, and the indicator blinks regularly. Meanwhile the UP/DOWN indicator (depending on whether the device is a HaLow AP or station) will blink at 4Hz for 3s and later turns solid green.
- e. When the device is ready for factory reset, the indicator blinks at 2Hz. After the user confirms the state, the indicator will blink at 4Hz, indicating the device is undergoing a factory reset. Upon successful factory reset, the indicator will turn solid green.

1.8.3 Up & Down indicators

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

- 2. Down indicator
- When there is a successful uplink connection via any of Ethernet WAN, 2.4GHz Wi-Fi STA, and HaLow STA of the device: Solid green;
- When the device does NOT establish a successful uplink connection via any of Ethernet WAN, 2.4GHz Wi-Fi STA, and HaLow STA: OFF;
- When Wi-Fi HaLow STA/2.4GHz Wi-Fi STA pairing is completed with success: Blinking at 4Hz for 3s and later transitioning to solid green.
- 3. When the device is ready for factory reset, the Up and Down indicators blink at 2Hz. After the user confirms the state, the indicator will blink at 4Hz, indicating the device is undergoing a factory reset.

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

1.8.4 Restore indicator

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

1.8.5 Power indicator

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

1.8.6 System indicator

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

1.8.7 Error indicator

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

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

1.9 Serial Port



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

Та	b	le	1-4

No.	Signal	Device name	Port	Туре	Description
1	VCC	/dev/ttyS0	60140	Р	5V output
2	GND			Р	Ground
3	А		COIVIO	I/O	RS485 A signal
4	В			I/O	RS485 B signal

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

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

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

CHAPTER 2 GETTING STARTED

2.1 Setting up the Device

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

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



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



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



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



2.2 Pairing Two HAP101 Devices

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

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

2.2.1 Pairing via station setup on the web portal

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

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

- Power on H1 and use an Ethernet cable to connect it to a router that functions as a DHCP server;
- The router is used for network access and unified IP allocation. Connecting to it is not necessary if you just intend to verify the HaLow connection.

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

HaLow WLAN MAC: XX:XX:XX:XX:XX:XX WLAN MAC: XX:XX:XX:XX:XX:XX WAN MAC: XX:XX:XX:XX:XX:XX WLAN Login IP: 172.18. 2.1 User name/Password: admin/XXXXXX WLAN SSID: XXXXXX WLAN Password: XXXXXXX HaLow WLAN SSID: XXXXXX HaLow WLAN Password: XXXXXXXX

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



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

HaLow WLAN MAC: XX:XX:XX:XX:XX:XX WLAN MAC: XX:XX:XX:XX:XX:XX WAN MAC: XX:XX:XX:XX:XX:XX WLAN Login IP: 172.18. 2.1 User name/Password: admin/XXXXXX WLAN SSID: XXXXXX WLAN Password: XXXXXXX HaLow WLAN SSID: XXXXXX
HaLow WLAN SSID: XXXXXX HaLow WLAN Password: XXXXXXXX

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

Super user: root // password: rootpassword

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

		HaLow WIFI	
Status	`	HaLow WIFI Settings	
Route Management	>	General Setting Advanced Setting	
h Network	Y	Status	Mode - Matter BSED - 40-DD 40-C 0: 1B F 83 SSED: DOL - AH-10: 1BF 83 Energyption: UPA3 SAE (CCMP) Channel: 12 (0950: 000 MHz) Tx-Pewer: 21 dBm. Country: US Signal: 0 dBm. Noise: 0 dBm. Birrate: 0.0 Mbits
· Wireless(WIFI)		WIFI mode	AP () Switch Mode (2)
HaLow WIFI		SSID Network Authentication	Mesn
Diagnostics		Key	WPAS-Personal
Network Capture		Bridge Mode	
© Services	>	DPP Push Button	Start DPP Push
1 Security	>	DPP Push Log:	
O Advanced Features	>		
🚺 Users Manage	,	Associated Stations	AC.Address Hest
			No information available
System	>	Back or Refresh	(3) Save & Apply Save Reset

- The LAN IP of the device will change to **172.18.3.1** when the HaLow mode switches to Client.
- 7. Reconnect the host computer to the 2.4GHz Wi-Fi of **H2** and log in to VantronOS using the new WLAN IP: 172.18.3.1;
- 8. Check the device label of **H1** for the HaLow WLAN SSID and password for HaLow connection;



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

Wifi Client Setting		
Select SSID	Mac/Bssid 🔎	Key 🖲
100% ; DGL-AH-101-DEBE	Auto	✓ Ki z
Scan WIFI No connection		

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

Wifi Client Setting			
Select SSID		Mac/Bssid 📍	Key 📍
100% ; DGL-AH-101-DEBE	~	Auto	✓ K z
Scan WIFI Connected: 0h 0m 43s IPaddr: 172.18.1.199			

2.2.2 HaLow DPP pairing via hardware setup

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

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

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

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

Table 2-1

Steps:

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

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

- a. H1 and H2 are successfully connected; or
- b. The Pair/Restore button is briefly pressed during the DDP state; or
- a. The second device does not enable the DDP state in 120 seconds after the first device does or the connection fails.

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

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

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

2.2.3 HaLow DPP pairing via software setup

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

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

	HaLow WIFI			
Status	HaLow WIFI Settings			
Route Management >	General Setting Advanced Setting			
Network Interfaces	Status	Mode: Master BSSID: 40:De3:C01:BF:83 SSID: DGL-AH:101:BF83 Encryption: WP Channel: 12 (908:000 MHz) Tx-Power: 21 d Signal: 0 dBm Noise: 0 dBm Bitrate: 0.0 M	A3 SAE (CCMP) Bm Country: US bit/s	
· Wireless(WIFI)	WIFI mode	AP	Switch Mode	
Hal on WIEI	SSID	DGL-AH-101-BF83		
Disposition	Network Authentication	WPA3-Personal		
Network Capture	Key	•••••	2	
Network Capture	Bridge Mode			
Services >	DPP Pash Button	Start DPP Push		
1 Security	DPP Push Log:			

5. Switch the HaLow mode of H2 to Client;

Status	>	HaLow WIFI	
Route Management	>	General Setting Advanced Setting	
Network	•	Status	Mode: Master BSSID: 40:D6:3C:01:BF:83 SSID: DGL-AH:101-BF:83 [Encryption: WPA3 SAE (CCMP) Channel: 12 (908.000 MHz) [Tx-Power: 21 dBm Country: US Signal: 0 dBm Noise: 0 dBm Bitrate: 0.0 Mbit's
Wireless(WIFI)		WIFI mode	Client Switch Mode
HaLow WIFI		Protocol	DHCP DHCP, if the WIFI access point needs to specify IP, please select Static
Diagnostics		Bridge Mode	
Network Capture		DPP Push Button	Start DPP Push
Services	>	DPP Push Log:	
1 Security	>		

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

HaLow WIFI		
HaLow WIFI Settings		
General Setting Advanced Setting		
Status	Mode: Master BSSID: 40:D6/3C:01:BF:83 SSID: DGL-AH-101:BF83 Encryption: WPA3 SAE (CCMP) Channel: 12 (908.000 MHz) Tx-Power: 21 dBm Country: US Signal: 0 dBm Noise: 0 dBm Bitrate: 0.0 Mbit/s	
WIFI mode	AP Switch Mode	
SSID	DGL-AH-101-BF83	
Network Authentication	WPA3-Personal	
Key	······ 2	
Bridge Mode		
DPP Push Button	Start DPP Push	

- 7. Wait for the devices to pair;
- 8. Upon successful connection, the HaLow indicators on both devices will enter the 'netdev' mode. The UP indicator on H1 and the DOWN indicator on H2 will blink at a frequency of 4Hz for 3s and later turn solid green;
- 9. The DPP push log indicates the success or failure state of the connection.

DPP Push Log:				
<pre><2024-12-16 11:34:28> <2024-12-16 11:39:14> <2024-12-16 11:39:36> <2024-12-16 11:40:33> <2024-12-16 11:42:03> <2024-12-16 11:42:03> <2024-12-16 11:42:03> <2024-12-16 11:43:36> <2024-12-16 11:46:56> <2024-12-16 11:47:15></pre>	DPP PUSH Connected. DPP PUSH Exit. DPP PUSH Started. DPP PUSH Started. DPP PUSH Started. DPP PUSH Started. DPP PUSH Started. DPP PUSH Started. DPP PUSH Started.]		
Wifi Client Setting				
Select SSID		Mac/Bssid 🔎	Key 🦲	
52% ; DGL-AH-101-BDA5	~	Auto	~	
Scan WIFI Connected: 0 IPaddr: 172	0h 2m 23s 18.1.107			

2.3 Web Login

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

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

Та	bl	e	2-	·2

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

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

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

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

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

2.3.1 Login via the 2.4GHz WLAN IP

Prerequisites:

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

Steps:

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

HaLow WLAN MAC: XX:XX:XX:XX:XX:XX WLAN MAC: XX:XX:XX:XX:XX:XX WAN MAC: XX:XX:XX:XX:XX WLAN Login IP: 172.18.2.1 User name/Password: admin/XXXXXX WLAN SSID: XXXXXX WLAN Password: XXXXXXXX HaLow WLAN SSID: XXXXXX HaLow WLAN Password: XXXXXXXX

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

HaLow WLAN MAC: XX:XX:XX:XX:XX:XX WLAN MAC: XX:XX:XX:XX:XX:XX WAN MAC: XX:XX:XX:XX:XX:XX WLAN Login IP: 172.18. 2.1 User name/Password: admin/XXXXXX WLAN SSID: XXXXXX WLAN Password: XXXXXXX HaLow WLAN SSID: XXXXXX HaLow WLAN Password: XXXXXXXX



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

HaLow WLAN MAC: XX:XX:XX:XX:XX:XX WLAN MAC: XX:XX:XX:XX:XX:XX WAN MAC: XX:XX:XX:XX:XX:XX WLAN Login IP: 172.18. 2.1 User name/Password: admin/XXXXXX WLAN SSID: XXXXXX
User name/Password: admin/XXXXXX WLAN SSID: XXXXXX WLAN Password: XXXXXXXX HaLow WLAN SSID: XXXXXX
HaLow WLAN Password: XXXXXXXX

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

Super user: root // password: rootpassword

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

Status >	Interfaces					
	Interface Overview					
Quick Start >	LAN	Uprime: 0h 3m 1s MAC-Address: 40:05-3C-B9:50:8B FX: 10(8:30 K7 (1)55 Ftm.)	Restart Edit	Delete		
n Network	ی (منطق کی استان میں اور	TX: 1 53 MB (608 Ptn), IPv4: 172.18.2.1/24		†: 0.26 KB/s ↓: 0.20 KB/s		
Wireless(WIFI)	WAN	Uptime: 0h 0m 0s MAC-Address: 40:D6:3C:B9:50:8D	Restart Edit	Delete		
HaLow WIFI	ge (A) br-wan	RX: 0 B (0 Plets.) TX: 0 B (0 Plets.)		1: 0.00 B/s ↓: 0.00 B/s		
Static Routes						
Diagnostics	Add new interface					

2.3.2 Login via the VLAN IP (Windows PC)

Prerequisites:

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

Steps:

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



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



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



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

Jumbo Mtu Large Send Offload V2 (IPv4) Large Send Offload V2 (IPv6) Maximum Number of RSS Queu Network Address NS Offload Priority & VLAN Receive Side Scaling Speed & Duplex TCP/UDP Checksum Offload (IP TCP/UDP Checksum Offload (IP TCP/UDP Checksum Offload (IP VLAN ID Wake on Magic Packet Wake on Magic Packet Wolc Speed	↑ 1Þ		×
--	------	--	---

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

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



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



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

Super user: root // password: rootpassword

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

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

2.3.3 Login via the VLAN IP (Linux PC)

Steps:

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

	:~\$ ifconfig
enp2s0	flags=4163 <up,broadcast,running,multicast> mtu 1500</up,broadcast,running,multicast>
	inet 192.168.9.195 netmask 255.255.255.0 broadcast 192.168.9.255
	inet6 fe80::23bb:3bb7:bf0:af70
	ether b4:2e:99:0d:07:46 txqueuelen 1000 (Ethernet)
	RX packets 395268 bytes 151085899 (151.0 MB)
	RX errors 0 dropped 3554 overruns 0 frame 0
	TX packets 243915 bytes 22156453 (22.1 MB)
	TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: fl	ags=73 <up,loopback,running> mtu 65536</up,loopback,running>
	inet 127.0.0.1 netmask 255.0.0.0
	inet6 ::1 prefixlen 128 scopeid 0x10 <host></host>
	loop txqueuelen 1000 (Local Loopback)
	RX packets 20696 bytes 2381387 (2.3 MB)
	RX errors 0 dropped 0 overruns 0 frame 0
	TX packets 20696 bytes 2381387 (2.3 MB)
	TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

- The Ethernet interface of the computer is mapped as *enp2s0* as shown above.
- 3. Create a VLAN interface (e.g., vlan10) on the Ethernet interface (enp2s0 in this case) with a VLAN ID (e.g., 10);

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

4. Bring the VLAN interface up;

\$ sudo ifconfig vlan10 up

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

\$ sudo dhclient vlan10

/:~\$	sudo ip link add vlan10 link enp2s0 type vlan id 10
/:~\$	
/:~\$	sudo ifconfig vlan10 up
/:~\$	
/:~\$	sudo dhclient vlan10
6. Check the network interfaces on the host computer and confirm if the VLAN interface receives an IP;

\$ ifconfig



- The VLAN interface is assigned with an IP of 172.18.2.114 by the VLAN gateway (HAP101).
- 7. Run the ip route command to check the IP address of the VLAN gateway (HAP101).



- The IP address of HAP101 is **172.18.2.1** in this case. Please note that when HAP101 switches to the HaLow station mode, its IP will change to 172.18.3.1 accordingly.
- 8. Use above IP address of HAP101 for VantronOS login.
- 9. Use the username and password provided on the device label for authentication.



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

Super user: root // password: rootpassword

2.3.4 Login via the WAN port IP

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

face Overview		
LAN	Uptime: 0h 6m 40s MAC-Address: 40:D6:3C:B9:50:8B PX: 11:214.0F(1070.Phrs.)	Restart Edit Delete
j€ (ﷺ ∰ ∰) br-lan	TX: 1.76 MB (1344 Pkts.) IPv4: 172.18.2.1/24	↑: 0.10 KB/i ↓: 0.04 KB/i
WAN	Uptime: 0h 0m 36s MAC-Address: 40:D6:3C:B9:50:8D RX: 67 53 KB (329 Pbrs.)	Restart Edit Delete
هچ (ع) br-wan	TX: 5.68 KB (55 Pits.) IPv4: 192.168.19.199/24	↑: 0.00 KB/ ↓: 0.84 KB/:

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

← → C	A Not secure 192.168.19.199 cgi/gateway			☆
Vantr	onOS			
10000				
		VantronOS	root	
		The former	Password	
		welcome		
			Login	

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



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

Super user: root // password: rootpassword

2.4 SSH Login

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

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

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

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

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

Security >	SSH Access Dropbear is running	
Advanced Features	Enable Disable	
🕻 Users Manage 🔶	Interface	evice LAN IP login
System V		unspecified either IP address is allowed
System	Port	Listen only on the given interface or, it unspectified, on all
Log	Password authentication	Specifies the listening port of this Dropbear instance
Terminal		Allow <u>SSH</u> password authentication

Refer to 3.10.2 for the specific login steps.

Use the following information for the login.

Port	Account	Password		
22	root	rootpassword		

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



Example SSH login with the WAN port IP of HAP101:

 MobaXterm Personal Edition v22.1 • (SSH client, X server and network tools)
➤ SSH session to root@192.168.19.199
 Direct SSH : SSH compression : (disabled or not supported by server)
 SSH-browser : X11-forwarding : x (disabled or not supported by server)
 For more info, ctrl+click on <u>help</u> or visit our <u>website</u>.
BusyBox V1.36.1 (2024-11-06 12:37:30 UTC) built-in shell (ash)
$\left[\frac{1}{2}\right] \left[\frac{7}{2}, \frac{1}{2}, \frac{7}{2}, \frac{7}{$
│
V200R003.F0000-0B Built at 2024-11-09 09:08:02
root@VantronOS-508D:~#

2.5 Wi-Fi HaLow Mode

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

2.5.1 AP mode

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

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

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

S 5 4		HaLow WIFI	
Status	<i>´</i>	HaLow WIFI Settings	
Route Management	>	General Setting Advanced Setting	
h Network	~	Status	Moder Matter BSSID: 40:D-3C-01:BF-32 SDD DCL-343-01.BF-33 Channel: 0.20000 DH201: Dr. Person: 21:dGm: Country: US Signal: 0.dBm: [Noise: 0.dBm:]Bitrate: 0.0.Mbits
· Wireless(WIFI)		WIFI mode	2) AP v Switch Mode 3
HaLow WIFI	-	SSID (DGL-AH-101-BF83 WPA3-Personal
· Diagnostics		Key	
Network Capture		Bridge Mode	
Services	>	DPP Push Button	8 Start DPP Push
1 Security	>	DPP Push Log:	
O Advanced Features	>	Associated Stations	
🕻 Users Manage	>	Network MAC-Add	ress Host
😍 System	>	Back or Refresh	vo njornation anazave
× Logout	>		

Description of the numbered areas

- 1) Device general status information
- 2) The device operates in the HaLow AP mode by default and you can switch the mode using the drop-down list
- 3) You need confirm the mode change using the **Switch** button
- 4) HaLow SSID of the device
- 5) Authentication method for a HaLow connection
- 6) Default password for a HaLow connection (clicking the refresh button will display the password)
- 7) The HaLow interface is bridged to the Ethernet interface by default. This means that when the device is connected to a DHCP server through the WAN port, station devices connected to it via HaLow will receive an IP address from the DHCP server;
- 8) Pressing the **Start DPP Push** buttons simultaneously on the web portals for the AP mode HAP101 and the station mode HAP101 will initiate a DPP pairing between the devices.

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

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

S C C		HaLow WIFI			
Status	<i>′</i>	HaLow WIFI Settings			
Route Management	>	General Setting Advanced Setting			
-		Enable/Disable WIFI HaLow	(1)	Disable WIFI	
A Network	Ľ	Country Code	2	US 🗸]
Wireless(WIFI)		Operating Bandwidth	3	8MHz 🗸	Switch Country and BW
HaLow WIFI	-	Channel	(4)	12 - 908MHz 🗸	
Diagnostics		DCS	5		
Network Capture				Dynamic Channel Selection Based on Quality	y of the Signal
		Associated Stations			
Services	>	Network	MAC-Address		Host
				No information available	
1 Security	>	Desta a Defect			
Advanced Features	>	Back of Refresh			Save & Apply Save Reset
Services Security Advanced Features	> > >	Network Back or Refresh	MAC-Address	No information available	Host Save & Apply Save Reset

Description of the numbered areas

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

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

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

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

2.5.2 Station mode

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

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

Statue	,	HaLow WIFI		
Jiaius		HaLow WIFI Settings		
Route Management	>	General Setting Advanced Setting		
Network	•	Status	Moder: Mater: BSSID: 40.0457.01.BF.83 SSID: 20.04.AF.101.BF.83 [Encrytoles: WPA3 SAE (CCMP) Channel: 12 (906.00.MEz) 17.5.Power: 21 dBm: Country: US Signal: 0 dBm: [Noise: 0 dBm: Bitrate: 0.0.Met/s	
· Wireless(WIFI)		WIFI mode	AP (1) Switch Mode (2)	
Hal on WIFI		SSID	Client Wesn	
Diagnostics	-	Network Authentication	WPA3-Personal	
Network Cantura		Key	······ <i>2</i>	
Network Capture		Bridge Mode		
Services	>	DPP Push Button	Start DPP Push	
1 Security	>	DPP Push Log:		
O Advanced Features	>			
-		Associated Stations		
🖉 Users Manage	>	Network	MAC-Address Host	
🚭 System	>	Back or Refresh	No information analiable	Pasat
× Logout	>		Sure a Appy Sure	e

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

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

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

Wifi Client Setting				
Select SSID	Mac/Bssid 📍	Key 🧕		
100% ; DGL-AH-101-DEBE 🗸	Auto	Ki z		
Scan WIFI No connection				

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

Wifi Client S	etting				
Select SSID		1	Mac/Bssid °	K	ley 💿
100% ; DGL-A	NH-101-DEBE	•	Auto 🗸	ł	< z
Scan WIFI	Connected: 0h 0m 43s Paddr: 172.18.1.199				

2.5.3 Mesh mode

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



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

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

Refer to 2.3 for the login steps.

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

	HaLow WIFI					
Status >	HaLow WIFI Settings					
Route Management >	General Setting Advance	d Setting				
A Network	Status		Mode: 1 BSSID: Mesh II Channe Signal:	Mesh Point 40:D6:3C:01:BF:83 D: DGL-AH-101-mesh Encrypti 4: 12 (908.000 MHz) Tx-Power: 0 dBm Noise: 0 dBm Bitrate: 0	on: WPA3 SAE (CCMP) 21 dBm Country: US .0 Mbit/s	
Wireless(WIFI)	WIFI mode		Mesh		Switch Mode	
	Mesh ID		DGL-A	H-101-mesh		
Diagnostics	Network Authentication		WPA3	-Personal	•	
Diagnostics	Key				2	
Techoix ouplate	Enable AP in Mesh mode					
© Services >	AP Status		Mode: 1 BSSID: SSID: I Channe Signal:	Master 42:D6:3C:01:BF:83 DGL-AH-101-BF83 Encryption: d: 12 (908.000 MHz) Tx-Power: 0 dBm Noise: 0 dBm Bitrate: 0	WPA3 SAE (CCMP) 21 dBm Country: US .0 Mbit/s	
i security	AP SSID		DGL-A	H-101-BF83		
O Advanced Features	AP Network Authentication		WPA3	-Personal	~	
Users Manage	AP Key				2	
	AP Bridge Mode		 Image: A start of the start of			
🔮 System 🔸	Mesh Associated	itations				
X Logout	Network		MAC-Add	ress Io information available		
	AP Associated Sta	tions				
	Network	M	AC-Address			Host
			4	o information available		
	HaLow WIFI					
Status >	HaLow WIFI Settings	_				
Route Management	General Setting Advanced Setting					
A Network	Enable/Disable WIFI HaLow		Disable WIFI			
Interfaces	Country Code		US	~		
Wireless(WIFI)	Operating Bandwidth		8MHz	✓ Switch	Country and BW	
HaLow WIFI	Channel		12 - 908MHz	~		
Diagnostics	Mesh Associated Statio	Ins				
Network Capture	Network	1	MAC-Address			
			No information a	wailable		
Services	AP Associated Stations	MAC Address			Hart	
1 Security >		ALAC-Address	No information a	wailable	nost	
○ Advanced Features →	Back or Refresh				Save & Apply	Save Reset

- 4. After completing above settings, a mesh network is established between the devices (H1, H2, H3), and you can check the connection under the **Mesh associated Stations** tab of the device connected to the DHCP server;
- 5. You can then connect station mode devices (H4, H5, H6) to the mesh mode devices via HaLow using the individual **AP SSID** and **AP key** of the mesh mode devices.

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

2.6 Network Interface Bridging

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



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

	Status	>	Interfaces				
	0.10		Interface Overview				
Ĭ	Quick Start	· _	LAN	Uptime: 1h 30m 54s MAC-Address: 18:9B:A5:17:DE:BD	Restart	Edit	Delete
÷	Network	~	85 (2000) br-lan	RX : 0.0 (0 PRB.) TX : 127 RB (11 PFr.) IPv4 : 172.18.2.1/24		1: 0.00 B/s ↓: 0.00 B/s	
	Interfaces Wireless(WIFI)	-	WAN	Uptime: 1h 30m 44a MAC-Address: 18:9B:A5:17:DE:BD RX: 865.56 KB (6822 Ptts.)	Restart	Edit	Delete
	HaLow WIFI		قﷺ (پیش ایس) br-wan	TX: 2.58 MB (7088 Ptr.) IPv4: 172.18.1.20024 WAN & HaLow AP			↑: 54.0 B/s ↓: 46.0 B/s

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

Status >	Interfaces				
	Interface Overview				
Quick Start >	HALOWRELAY	Uptime: 1h 17m 19s MAC-Address: 18:98:A5:10:11:12	Restart	Edit	Delete
Network Y	篇 (60 金) Relay "halowrelay"	RX: 784.46 KB (7258 Pitts.) TX: 781.80 KB (7038 Pitts.)			†: 0.00 B/s ↓: 0.00 B/s
···· Interfaces ···· Wireless(WIFI)	LAN	Uptime: 1h.24m.23s MAC-Address: 18.59EA5:10:11:12 RX: 2.17 MR (1717) Pits.)	Restart	Edit	Delete
HaLow WIFI	ی (شیسی) br-lan	TX: 2.66 MB (16192 Ptn.) IPv4: 172.18.3.124			†: 54.0 B/s ↓: 40.0 B/s
Static Routes Diagnostics	WAN	Uptime: 0h 0m 0s MAC-Address: 18-98:A5:10:11:12	Restart	Edit	Delete
ACL	gif (2) br-wan	RX: 0 B (0 Plats.) TX: 0 B (0 Plats.)			î: 0.00 B/s ↓: 0.00 B/s
UHCP	WWAN1	Uptime: 1h 17m 19a MAC-Address: 18-98hA5:10:11:13 RX: 764.46 Rt (7258 Pen.)	Restart	Edit	Delete
🕑 Users Manage 🔹 🕨	Client "DGL-AH-101-DEBE"	TX: 751 S0 KB (703 S PAL) IPv4: 172.18.1.199/24 HaLow STA			1: 0.00 B/s ↓: 0.00 B/s

2.7 Ethernet Port Modification

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

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

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

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

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

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

2.7.1 WAN port to LAN port

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

1. Log in to the device's VantronOS via 2.4GHz Wi-Fi as instructed in 2.3.1;

2. Navigate to Network > Interfaces;

Status	>	Interfaces					
- Status		Interface Overview					
Route Management	>	LAN	Uptime: 1h 53m 27s MAC-Address: 40:D6:3C:01:BF:82 RY-1 53 MR (1d:472 Pite.)	Restart	Edit Delete		
h Network	~				1: 54.0 B/s ↓: 40.0 B/s		
Interfaces	-	WAN	Uptime: 0h 0m 0s	Restart	Edit Delete		
···· Wireless(WIFI)			MAC-Address: 40:D6:3C:01:BF:82 RX: 0 B (0 Pkts.)		* 0.22 KD/s		
HaLow WIFI		br-wan	TX: 767.45 KB (2244 Pkts.)		↓: 0.00 KB/s		
Diagnostics		Add new interface					
Network Capture							

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

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

Status	>	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
Route Management	>	separated by spaces. You can also use <u>VLAN</u> notation INTERFACE. VLAWR (<u>e.g.</u> ; eth0.1).
		Common Configuration
the Network	~	General Setup Advanced Settings Physical Settings Firewall Settings
Interfaces	_	Bridge interfaces
Wireless(WIFI)		O creates a bridge over specified interface(s)
		Enable STP
HaLow WIFI		(2) Enables the Spanning Tree Protocol on this bridge
Diagnostics		Interface uncheck 🗾 🖉 Ethemet Adapter: "eth0" (wan)
Network Capture		21 Software VLAN, "eth.10" (an)
		Wireless Network: Master DGL-AH-101-10CA" (van)
O Services	>	add eth0.20 🗹 🖉 Custom Interface: eth0.20
1 Security	>	Back or Refresh Save & Apply Save Reset
0		

- 5. Save and apply the settings, and the system will automatically return to the **Interfaces** page;
- 6. Click the Edit button after LAN, then click the Physical Settings tab to edit the interface;
- 7. Check the box next to "eth0", and check the box next to "eth0.10";

Status	>	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
Route Management	>	separated by spaces. You can also use <u>VLAN</u> notation INTERFACE, VLANIR (e.g., eth0. 1).
		Common Configuration
A Network	~	General Setup Advanced Settings Physical Settings
Interfaces		Bridge interfaces
Wireless(WIFI)		creates a bridge over specified interface(s)
HaLow WIFI		Enable <u>STP</u>
		Bradies the Spanning Tree Protocol on this orage
Diagnostics		Interface Check Z Ethernet Adapter: "eth0"
Network Capture		UNCHECK Software VLAN: "eth0.10" (an)
		Sonware VLAN: emu/20 (wan)
		Wireless Network: "DGL-AH-101-1DCA" (wan)
Services	>	Custom Interface:
4L c h		

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

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

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

Status	, wi	FI Settings					
	En	able/Disabled WIFI			Enable	~	
Route Management	> WI	IFI Mode		1	Client	~	
a Network				2	Save		
Interfaces		Mode: BSSID: Channel:	AP 40:D6:3C:B9:30:8F 1(2:412 GHz)		SSID: Network Authentication: Tx-Power:	DGL-AH-1 psk-mixed 20 dBm	101-308F
Wireless(WIFI)		Signal: Bitrate:	-23 dBm 130 Mbit/s		Noise: Country:	0 dBm 00	
HaLow WIFI	SS	ID			DGL-AH-101-308F		
Diagnostics	Ne	etwork Authentication			WPA/WPA2	~	
Network Capture	Ke	ey.					2
	- A	dvanced Settings					
Services	> Co	ountry Code			00-World	~	
	Hv	vmode			2.4G	~	
Security	> Ch	nannel			1	~	
Advanced Features	> Bri	idge Mode			Bridge 2.4G Wi-Fi to the WAN		
Users Manage	, 3	Apply					

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

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

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

9 0		HaLow WIFI	
Status	1	HaLow WIFI Settings	
ᅌ Route Management	>	General Setting Advanced Setting	
Network	~	Status	Mode: Master BSSID: 1639:-A518:1D-CA SSID: DGL-AH-101-1DCA Encryption: WPA3 SAE (CCMP) Channel: 12 (908:000 MHz) Tx-Power: 21 dBm Country: US Signal: 0 dBm Noise: -86 dBm Bitrate: 0.0 Mbit/s
···· Wireless(WIFI)		WIFI mode	AP 1 Switch Mode 2
HaLow WIFI	_	SSID Network Authentication	Vient
Diagnostics			WPAS-Personal
Network Capture		Key	
		Bridge Mode	
Services	>	DPP Push Button	Start DPP Push
1 Security	>	DPP Push Log:	
Advanced Features	>		
		Associated Stations	
🙋 Users Manage	>	Network MAC-	Address Host
			No information available
👽 System	>	Back or Refresh	3 Save & Apply Save Reset
× Logout	>		

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

Status	>	Interfaces Interface Overview			
C Route Management	>	HALOWRELAY	Uptime: 0h 0m 0s MAC-Address: 18:9B:A5:18:1D:C9	Restart Edit	Delete
A Network	~	Eelay "halowrelay"	RX: 0 B (0 Pkts.) TX: 13.34 KB (39 Pkts.)		1: 0.00 B/s ↓: 0.00 B/s
···· Interfaces ···· Wireless(WIFI)	-	LAN	Uptime: 0h 6m 27s MAC-Address: 18:9B:A5:18:1D:C9 RX: 178.37 KB (1629 Pkts.)	Restart Edit	Delete
HaLow WIFI		jj⊄ (∰™∰) br-lan	TX: 1.96 MB (1361 Pkts.) IPv4: 172.18.3.1/24		↑: 0.10 KB/s ↓: 0.08 KB/s
Diagnostics		WAN	Uptime: 0h 0m 0s MAC-Address: 18:9B:A5:18:1D:C9	Restart Edit	Delete
· Network Capitire		قری (یے) br-wan	KX: 0 B (0 Pkts.) TX: 13.34 KB (39 Pkts.)		1: 0.00 B/s ↓: 0.00 B/s
Services	>	WWAN1	Uptime: 0h 0m 0s MAC-Address: 18:9B:A5:18:1D:CA	Restart Edit	Delete
1 Security	>	Connect to "DGL-AH-101-1DCA"	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)		1: 0.00 B/s ↓: 0.00 B/s
O Advanced Features	>	Add new interface			

5. Navigate to Network > Interfaces;

- 6. Click the Edit button after WAN, then click the Physical Settings tab to edit the interface;
- 7. Uncheck the box next to "eth0", and add an "eth0.20" interface;

Status	>	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				
Route Management	>	separated by spaces. You can also use <u>VLAN</u> notation INTERFACE. VLANNR (<u>e.g.</u> ; eth0.1).				
		Common Configuration				
n Network	*	General Setup Advanced Settings Physical Settings Firewall Settings				
Interfaces		Bridge interfaces				
···· Wireless(WIFI)		creates a bridge over specified interface(s)				
HaLow WIFI		Enable STP Enables the Spanning Tree Protocol on this bridge				
Diagnostics		Interface uncheck Ethermet Adapter: "eth0" (wan)				
Network Capture		2 Software VLAN: "etho.10" (an)				
		Witeres revolut. state DGL-AH-101-10CA" (unvani)				
Services	>	add eth0.20 Custom Interface: eth0.20				
1 Security	>	Back or Refresh Save & Apply Save Reset				
Advanced Features	>					

- 8. Save and apply the settings, and the system will automatically return to the **Interfaces** page;
- 9. Click the Edit button after LAN, then click the Physical Settings tab to edit the interface;

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

Status	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
Route Management	separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1).
	Common Configuration
th Network	General Setup Advanced Settings Physical Settings
Interfaces	Bridge interfaces
Wireless(WIFI)	Creates a bridge over specified interface(s)
HaLow WIFI	Enable <u>STP</u>
Diagnostics	Interface check 🗾 🖉 Ethemet Adapter: "eth0"
Network Capture	uncheck
	✓ ∰ Wireless Network: Master "DGL-AH-101-308F" (lan) Ø Wireless Network: Master "DGL-AH-101-1DCA" (wan)
Services	Q Custom Interface:
1 Security	

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

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

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

Status	>	WIFI Settings		
OROUTE Management	>	Enable/Disabled WIFI WIFI Mode		Enable AP
network	×			Save
Interfaces Wireless(WIFI)	_	Mode: BSSID: Channel: Signal: Bitrate:	AP 40:D6:3C:B9:30:8F 1(2.412 GHz) -41 dBm 130 Mbit/s	SSID: DGL-AH-101-308F Network Authenticies pul-mixed Tx-Pever: 20 dBm Noise: 0 dBm Country: 00
HaLow WIFI		SSID		DGL-AH-101-308F
Diagnostics		Network Authentication		WPA/WPA2 🗸
Network Capture		Key		#
		- Advanced Settings		
O Services	>	Country Code		00-World
- Surres		Hwmode		2.4G 🗸
1 Security	>	Channel		1 🗸
Advanced Features	>	Bridge Mode		1 (Bridge 2.40 Wi-Fi to the WAN
🕻 Users Manage	>	Apply 2		

- 11. Refresh the page and VantronOS is not accessible because the 2.4GHz Wi-Fi of the device is bridged;
- 12. Connect the host computer to the device via the Ethernet port using an Ethernet cable;
- 13. Log in to VantronOS using the LAN IP of the device: **172.18.3.1**.

2.7.2 LAN port back to WAN port

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

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

		-					
Status	>	WIFI Settings					
		Enable/Disabled WIFI		Enable	~		
Route Management	>	WIFI Mode		AP	~		
A Network	~			Save			
Interfaces		Mode: BSSID: Channel:	AP 40:D6:3C:B9:30:8F 1(2.412 GHz)	SSID: Network Authentica Tx-Power:	DGL-AH-1 tion: psk-mixed 20 dBm	01-308F	
Wireless(WIFI)	-	Signal: Bitrate:	-18 dBm 130 Mbit/s	Noise: Country:	0 dBm 00		
HaLow WIFI		SSID		DGL-AH-101-308F			
Diagnostics		Network Authentication		WPA/WPA2	~		
Network Capture		Key				8	
		- Advanced Settings					
Ö Samiran	,	Country Code		00-World	~		
Services		Hwmode		2.4G	~		
1 Security	>	Channel		1	~		
Advanced Features	>	Bridge Mode		1 Bridge 2:4G Wi-Fi to the W	/AN		
🕑 Users Manage	>	Apply 2	:				
🚭 System	>	Associated Stati	ons	Mac 5475-05-06-1-1-	IP	2 10 2 120	Signal
V T		DESKTOP-DHIONEN		041701901001ea1bc	17	2.18.3.139	-18

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

Status	>	Interfaces			
		Interface Overview			
Route Management	>	LAN	Uptime: 0h 6m 30s MAC-Address: 18:9B:A5:18:1D:C9 RX: 234 22 KB (1970 Ptrs.)	Restart	dit Delete
h Network	~	ق ⁽²⁷ (ه) br-lan	TX: 800.12 KB (1717 Pkts.) IPv4: 172.18.2.1/24		↑: 54.0 B/s ↓: 40.0 B/s
···· Interfaces ···· Wireless(WIFI)	-	WAN	Uptime: 0h 0m 0s MAC-Address: 18:9B:A5:18:1D:C9	Restart	dit Delete
HaLow WIFI		ه (۲۰۰۰ ۲۰۰۰) br-wan	KX: 35.78 KB (110 Pkts.) TX: 43.78 KB (128 Pkts.)		↑: 0.33 KB/s ↓: 0.00 KB/s
Diagnostics		Add pow intorface			
Network Capture		Add new interface			

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

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

Status	>	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
Route Management	>	separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (<u>e.g.</u> , etno.1).
A Network	~	General Setup Advanced Settings Physical Settings
	-	Bridge interfaces
HaLow WIFI		Enable SIP
Diagnostics Network Capture		Interface Check Z Ethernet Adapter "eth" (lan) uncheck Mr Software VLAN: "eth.0.0" (van) Wreless Network: Master "DGL-AH-101.306F" (lan)
© Services	>	Wireless Network: Client "DGL-AH-101-1DCA" (<u>www.ml</u>)
1 Security	>	Back or Refresh Save & Apply Save Reset

- 7. Save and apply the settings, and the system will automatically return to the **Interfaces** page;
- 8. Click the **Edit** button after LAN, then click the **Physical Settings** tab to edit the interface;

Status	>	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
Route Management	>	separated by spaces. You can also use <u>VLAN</u> notation INTERFACE, VLANNR (<u>e.g.</u> : eth0.1).
		Common Configuration
n Network	~	General Setup Advanced Settings Physical Settings
Interfaces		Bridge interfaces
Wireless(WIFI)		(g) creates a bridge over specified interface(s)
HaLow WIFI		Enable <u>STP</u> (2) Enables the Spanning Tree Protocol on this bridge
Diagnostics		Interface 🗾 🖉 Ethernet Adapter: "br-wan" (wan)
Network Canture		uncheck Ethernet Adapter: "eth0" (lan, wan)
remone ouplate		Vireless Network: Master "DGL-AH-101-308F" (lan)
		Wireless Network: Chient "DGL-AH-101-IDCA" (wwani)
Services	>	Custom Interface eth0.10

- 9. Save and apply the settings, and the system will automatically return to the **Interfaces** page;
- 10. If the device is operating in HaLow STA mode, you can optionally switch it to the AP mode and access VantronOS using the IP: 172.18.2.1.

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

LAN	Uptime: 0h 23m 18s MAC-Address: 40:D6:3C:01:BF:82	Restart	Edit	Delet
هه (۲۰۰۰ کی کی) br-lan	RX: 520.17 KB (5351 Pkts.) TX: 2.27 MB (4675 Pkts.) IPv4: 172.18.2.1/24			↑: 0.10 K ↓: 0.12 K
WAN	Uptime: 0h 0m 0s MAC-Address: 40:D6:3C:01:BF:82	Restart	Edit	Delet
gđ (J) br.wan	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)			1: 0.00 ↓: 0.00

- 12. Connect the device to a router or switch through the Ethernet port;
- 13. Restart the WAN port and you will see the WAN port IP allocated by the router or switch.

Interfaces				
Interface Overview				
LAN	Uptime: 0h 25m 23s MAC-Address: 40:D6:3C:01:BF:82 RX: 636 91 KB (5985 Pirs.)	Restart	Edit	Delete
ي (يېسې کې (پې کې	TX: 2.35 MB (5177 Pkts.) IPv4: 172.18.2.1/24			↑: 0.56 KB/s ↓: 0.31 KB/s
WAN	Uptime: 0h 0m 40s MAC-Address: 40:D6:3C:01:BF:82 BX: 122.05 KB (596 Ptrt.)	Restart	Edit	Delete
go (ja) br-wan	TX: 25.20 KB (113 Pirts) IPv4: 192.168.19.167/24	1		↑: 0.48 KB/s ↓: 0.53 KB/s
Add new interface				

2.8 Password Change

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

Status	>	Router Password	
		Changes the administrator password for accessing the device	
Route Management	>	Original Password	<i>d</i>
📩 Network	>	Password	<i>2</i>
		Confirmation	2
Ö Services	>		

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

2.9 Language Change

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

System						
Here you can configu	Here you can configure the basic aspects of your device like its hostname or the timezone.					
System Properties						
General Settings	eneral Settings Language and Style					
Language			auto	~		
Design			auto English			
			简体中文 (Simplified Chinese)			

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

English: English interface

Simplified Chinese: Simplified Chinese interface

2.10 Factory Reset the Device

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

2.10.1 Hardware reset

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

2.10.2 Software reset

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

Status		Firmware Update Backup/Restore Configuration
Status	<i>´</i>	Backup
O Pouto Monogoment	>	Click "Generate archive" to download a tar archive of the current configuration files.
 Route Management 		Download backup: Generate archive
h Network	>	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).
Services	>	Reset to defaults: Perform reset
1 Security	>	Restore backup: Choose File No file chosen Upload archive
		O Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.
O Advanced Features	>	
🙋 Users Manage	>	
🚭 System	~	
System		
Administration		
Log		
· Terminal		
Backup / Flash Firmware		

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

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

CHAPTER 3 DEVICE SETUP IN VANTRONOS

3.1 Introduction to VantronOS

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

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

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

3.2 Status

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



Description of the numbered areas

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

- 9. Address information of clients connected to the device via Ethernet
- 10. Current network connection information of the device
- 11. Default route (gateway) currently used by the device
- 12. Traffic distribution of clients connected to the device displayed by MAC addresses
- Clicking on each MAC address in the table at the bottom page will get the detailed traffic information of the clients.
- 13. Traffic of application layer protocols

3.3 Route Management

3.3.1 Automatic network routing

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

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

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



Description of the numbered areas

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

3.3.2 Static routing

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

Example:

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

Static routing:

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

Routes							
Routes specify over v	which interface and gateway a certain ho	st or network can be reached.					
Static IPv4 Rou	utes						
Interface→ Ta	arget ost-P or Network	IPv4-Netmask if target is a network 3	IPv4-Gateway	Metric 5	MTU 6	Route type	
wan 🗸 1	92.168.0.0/16	255.255.255.255	192.168.9.222	0	1500	unicast 🗸	Delete
Add							

Description of the numbered areas

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

- 6. Set the MTU
- 7. Select a route type (refer to the details next page)
- Be sure to save the settings before you exit the page.

Description of the route type:

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

3.4 Network

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

3.4.1 Interfaces

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

Status >	Interfaces			
	Interface Overview			
Route Management	HALOWRELAY	2 Uptime: Ih 8m 34s MAC-Address: 40 D05 3C 01:BF:82	Restart Edit	t Delete
A Network	陸山 (武学 愛) Relay "halowelay"	RX: 10.14 MB (51122 Pens) TX: 5.44 MB (17836 Pens)		1: 0.00 B/s 6 4: 0.00 B/s
Wireless(WIFI)	LAN	Uptime: 0b.17m.26s MAC-Address: 40:De3C:01:BF-32 RX: 0.8 (0.97m.)	Restart Edit	t Delete
HaLow WIFI	gjø (ten) br-lan	TX: 0 B (0 Pkts.) IPv4: 172.18.3.124		1: 0.00 B/s ↓: 0.00 B/s
Diagnostics Network Capture	WAN	Uptime: 1b 8m 34s MAC-Address: 49D355:01:157:82 873: 101349: (1024.Pers.)	Restart Edit	t Delete
	gi (j.) braza	TX: 4.36 MB (14939 Ptr.) IPv4: 192.168.19.167/24		↑: 0.94 KB/s ↓: 6.91 KB/s
Services >	WWAN0	Uptime: 00.18m 78s MAC-Address: 42.D53.C01-DF-51 PX7: M0.487 (100 Pers.)	Restart Edit	t Delete
1 Security >	Connect to "Lucius"	Tx: 20.8 K (180 Ptn.) IPv4: 172.20.10.5/28		↑: 0.00 B/s ↓: 0.00 B/s
○ Advanced Features →	WWANI	Updime: 0b.5m 56b MAC-Address: 40D/5/2013BE:83 BX: 11:58(R 09 Rep.)	Restart Edit	t Delete
🗹 Users Manage 🔹 🕨	Connect to "DGL-AH-101-BDA3"	TX: 580.95 KB (287 Pits.) IPv4: 172.18.1.107/24		1: 0.00 B/s ↓: 0.00 B/s
🚭 System 🔸	Add new interface (7)			

The numbered areas are detailed as follows:

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

3.4.1.1 LAN

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

• Common Configurations

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

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 $\underbrace{VLAN}_{notation}$ notation INTERFACE.VLANNR (e.g.: eth0.1).							
Common Configuration							
General Setup Advanced Settings Physical Settings							
Status	1	(j) Device: br-lan Uptime: 0h 0m 34s MAC: 40:d6:3c=01:bf:82 RX: 0 B (0 Pltts.) TX: 0 B (0 Pltts.) IPv4: 172.18.2.1					
Protocol	2	Static address	~				
IPv4 address	3	172.18.2.1					
IPv4 netmask	4	255.255.255.0	▼				

Description of the numbered areas

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

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

	Status	>	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 <u>VLANN</u> notation INTERFACE, VLANN (<u>g.g.</u> , etno. 1).							
	Quick Start	>	Common Configuration							
	1 Virtual Tunnel		General Setup Advanced Settings Physical Settings							
		1	Override MAC address	18:9B:A5:16:14:13						
I	n Network	•	Override MTU	1500						
I	Interfaces		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)

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 (gig: eth0.1).	
Common Configuration	
General Setup Advanced Settings Physical Settings	
Bridge interfaces	 G creates a bridge over specified interface(s)
Enable <u>STP</u>	 Enables the Spanning Tree Protocol on this bridge
Interface	3

Description of the numbered areas

- 1. Enable/Disable the interface for network bridge
- 2. Enable/Disable STP protocol
- 3. Select the interfaces for bridge connection
- Once bridged, the interfaces will be on the same network segment, sharing the same IP. Be sure to save the settings before you exit the page.

• General DHCP server

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

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

DHCP Server	
General Setup Advanced Settings	
Ignore interface	1 Disable <u>DHCP</u> for this interface.
Start	2 2 Lowest leased address as offset from the network address.
Limit	3 253 Maximum number of leased addresses.
Lease time	 4 12h i 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 HAP101.

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

Advanced Settings of DHCP Server:

DHCP Server	
General Setup Advanced Settings	
Dynamic <u>DHCP</u>	O gonamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
Force	O Force DHCP on this network even if another server is detected.
<u>IPv4</u> -Netmask	Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHCP-Options	 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.

3.4.1.2 WAN

• General settings

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

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 <u>VLAN</u> notation							
INTERFACE.VLANNR (e.g.: eth0.1).							
Common Configuration							
General Setup Advanced Settings Physical Settings Firewall Settings							
Status	↓ Device: eth0 Uptime: 0h 37m: 59s MAC: 18.9 ba5: 16:63:69 RX: 13.18 MB (66502 Pkts.) TX: 11.18 SMB (2000 Pkts.) IPv4: 192: 168: 19.128						
Protocol	2 DHCP client						
Hostname to send when requesting DHCP	3 VantronOS-D869						

Description of the numbered areas

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

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 <u>VLAN</u> notation INTERFACE, VL400R (g.g., et no. 1).								
Common Configuration								
General Setup Advanced Settings Physical Settings Firewall Settings								
Bring up on boot	 ☑ 							
Force link	 G Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplag handlers). 							
Use default gateway	 If unchecked, no default route is configured 							
Use DNS servers advertised by peer	 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							
Back or Refresh	Save & Apply Save Rese							

Description of the numbered areas

- 1. Check the box to bring up the port upon device boot
- 2. Force link (once the box is checked, hotplug handlers will not be invoked after a link change)
- 3. Enable/Disable Use default gateway
- 4. Enable/Disable Use DNS server advertised by peer
- ▶ If this option is disabled, you will need to define a DNS server.
- 5. Set a gateway metric
- 6. MAC address cloning
- 7. Set the MTU
- Be sure to save the settings before you exit the page.

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

Interfaces - WAN							
On this page you	can configure the net	work interfaces. You	can bridge several in	iterfaces by tic	king the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation		
INTERFACE.VL	ANNR (e.g.: eth0.1).						
Common Co	onfiguration						
General Setup	Advanced Settings	Physical Settings	Firewall Settings				
Bridge interfac	es			1	© creates a bridge over specified interface(s)		
Enable STP				2	 Enables the Spanning Tree Protocol on this bridge 		
Interface				3	Ethernet Adapter: "erupan0" Setting Software VLAN: "eth0.10" (lan) Ethernet Adapter: "tun0" (vgn) Wirreless Network: Master "MM6108-AP-4131" (lan) Wirreless 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.

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	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 <u>VLAN</u> n	otation INTERFACE.V	/LANNR (<u>e.g.</u> : ethØ.	1).					
Common Co	nfiguration							
General Setup	Advanced Settings	Physical Settings	Firewall Settings					
Create / Assign firewall-zone				lan: lan: 2				
				💿 wan: [wan: []] 🛞 wwan0: []]				
				unzpecified-or-create:				
				Choose the firewall zone you want to assign to this interface. Select <i>unpacified</i> to remove the interface from the associated zone or fill out the <i>create</i> 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.

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

3.4.2 Wireless (WIFI)

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

3.4.2.1 Wi-Fi – AP Mode

WIFI Settings					
Enable/Disabled WIFI		1 Enable	×		
WIFI Mode			•		
			•		
		3 Save			
Mode:	AP 40:D6:3C:01:BE:81	SSID: Network Authentication:	DGL-AH-1	01-BF81	
Channel:	1(2.412 GHz)	Tx-Power:	20 dBm		
Signal: Bitrate:	-47 dBm 115.6 Mbit/s	Noise: Country:	0 dBm 00		
SSID					
		5 DGL-AH-101-BF81			
Network Authentication		6 WPA/WPA2	~		
Key		(7)	<u>a</u>		
- Advanced Settings					
Country Code		8 00-World	~		
Hwmode		9 2.4G	~		
Channel		10 1	~		
Bridge Mode		(1) Bridge 2.4G Wi-Fi to the WAN			
Apply (12)					
Associated Stations					
Host (13)		Mac		IP	Signal
DESKTOP-DHT6NBN		54:75:95:06:ea:bc		172.18.2.139	-47

Description of the numbered areas

- 1. Enable/Disable the Wi-Fi module
- 2. Select a Wi-Fi mode (AP mode by default)
- 3. If you have switched the Wi-Fi mode in the prior step, click Save to apply the change
- 4. Wi-Fi AP information
- 5. Wi-Fi AP SSID
- \square Make sure the name does not contain special characters including \$, `, \.
- 6. Authentication method for the connection
- 7. Wi-Fi password (no less than 8 characters)
- Clicking the refresh icon will display/hide the password
- 8. Country code (00 applies to all regions)
- 9. Wi-Fi frequency band (determined by the hardware)

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

3.4.2.2 Wi-Fi – Client Mode

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

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

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

WIFI Settings						
Enable Disabled WIFI WIFI Mode		1Enable2Client3Sav	e My	•		
Mode:	STA	ss	ID: D	GL-AH-101-BDB3	2 Mars	
♥ VT-5F-PM2 ♥ DGL-AH-101-BDB3 Key:	(4)	5 Connect	۵ ۵	Advanced Settings		Î
♥ VT-5F-PM ♥ VT-5F-PM-Guest			≙			
[™] vt-6f-vpn [™] VT-5F-HW			▲			
WG_2.4G						
vantron_test9 vantron_test3 Vantron-B59634			A			
[⇒] vantron test 33 Scan wifi 6			A			-

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

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

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

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

				_
Mode: BSSID: Channel: Signal: Bitrate: Connected:	STA 40:D6:3C:01:BD:B3 1(2.412 CHz) -64 4Bm 52 Mbit's 0h 2m 26s	SSID: Network Authentication: Tx-Power: Noise: Country: IPaddr:	DGL-AH-101-BDB3 psk-mixed 20 dBm 0 dBm 00 172.18.2.191	
🕈 VT-5F-PM2			<u> </u>	
DGL-AH-101-BDB3			Advance	d Settings
🕈 VT-5F-PM			<u> </u>	
✤ VT-5F-PM-Guest			A	
vantron test8			A	
🐨 vt-6f-vpn			a	
vantron test9			a	
♥ VT-5F-HW			-	

3.4.3 Wi-Fi HaLow

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

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

3.4.4 Diagnostics

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

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

3.4.5 Network capture

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

tart network capto	seconds, packets	Filter	Actions (4)
any 🗸 30	seconds V fi	ter	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 capturing by seconds and by packet counts:

Measurement	Description		
Seconds	To specify a time duration for data capturing. For instance, you can input '10/20/30' for the data capturing, which indicates that the capture will stop in 10/20/30 seconds.		
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 netv	vork capture		
Interface	seconds, packets	Filter	Actions
any 🗸	30 seconds∨	tcp port 80	Start capture
Tue Aug 22 Tue Aug 22 Tue Aug 22 Tue Aug 22 tcpdump: 1: 521 packets 0 packets 0 Tue Aug 22	01:50:05 UTC 2023 vtshark start to capture 01:50:05 UTC 2023 ifname: any 01:50:05 UTC 2023 timeout : 30 seconds 01:50:05 UTC 2023 packages : 500000 01:50:05 UTC 2023 filter : tcp port 80 istening on any, link-type LINUX_SLL (Linux cooked s captured s received by filter dropped by kernel 01:50:35 UTC 2023 vtshark capture finished	d v1), capture size 262144 bytes	
Result			
vtshark.result.	pcap Delete		

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

Image: Construction	
Display a display filter	• +
No. Time Source Destination Protocol Length Rol Protocol Length Rol Destination 1 0.000000 1322.1048.9.214 322.1048.9.214 122.1048.9.214.9.214.9.214.9.214.9.214.9.214.9.214.9.214.9.214.	
16.0000 1922(56,9.17) 192.164,9.241 TCP 66.0000 162.166,9.214 TCP 66.0000 162.0000 162.0000 162.166,9.214 TCP 66.0000 162.0000 162.0000 162.0000 172.166,9.214 TCP 66.0000 162.0000 162.0000 172.166,9.214 TCP 66.0000 162.0000 162.0000 162.0000 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214 172.166,9.214,9.214 172.166,9.214,9.2	_
2 8.00414 123.014.0.21 123.014.0.21 121.014.0.17 127 66 [[19:A004 universis segment]. 5544 - m8 [0.00] 6947.047 Micro8d Lines Table25553127 Tecr-25145531 [3 8.2045 135.204.0.21 123.204.0.21 121.014 124.114.01 101 125.114.01 124.01	_
3 8,254613 142-168,8,214 142,168,9,17 HTTP 515 6ET /cg1/gsteway/admin/network/vthark_check_status?_47,16160060112633 HTTP/1_1 4 6,250586 142-168,5,21 152-168,5,214 169 66 [167 Free2oos segment not capture] 80 - 55468 [AKI] Sequ Activate MuniPD Lumi Toware2501501401 TScree2500504093 6,8 4109 112 142 142 142 142 142 142 142 142 142	_
4 4 0.55555 10.2456.9.37 402.458.9.231 102 651 [102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segment on explored by 1.6551 [Mag] Segme Astronomy Sum Polytophala (2012) 102 (102 Firstings segme as	
5.0.410830 102 168 0 17 102 168 0 214 TCD 137 80 . 56048 ID54 AC41 54m-2 Ark=448 Min=706 1 an=60 T5va1=251047813 T5arr=2550534003 ITCD segment of a ressembled DNI1	
0 0142000 20120000121 20120101214 10 100 0000 [F00] 000-2000000000 [10- 0000000000 [10- 0000000000	
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=251947613	
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 66 56948 - 80 [ACK] Seq=448 Ack=662 Win=501 Len=9 TSval=2559335158 TSecr=251947814	_
9 9.425332 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 192.108.9.17 192.168.9.214 TCP 68 [TCP Keep-Alive] 80 - 56948 [ACK] Seq=606 Ack=448 kin=766 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=666 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#48 Ack=607 Min=501 Lem#0 TSval=2559537165 TSecr=251947819	
15 3.257115 192.168.9.214 192.168.9.17 HTTP 515 EET /cg1/gateway/admin/network/vthark_check_status?_=0.4734152645199634 HTTP/1.1	_
15 3.25/321 192.106 9.17 192.108 9.214 1CP 88 80 - 50448 [ACK] Seq=00/ ACK499 Kaln=76 Leney 1594=25199053 [Sec=259593/094	
1/ 3.424040 TAX108/3/1/ TAX108/3/1/ TAX108/3/1/4 ICA T31.66 - 20346 [A24] VECK_BR2 MTULIAD FELCA 12/31236871 (241-22738361) (241-22738341) (14) Selimetr or a Learsemple Anni	
i Frame: 158 bytes on uirre (4120 bits), 58 bytes captures (122 bits) 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
X statukresit.pop	Profile: Defau

3.5 Services – DHCP Server

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

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

🥃 Status	>	DHCP Server	
Route Management	>	Status	by Devices br-lan Uptime: 037m 5 % Dyaddr: 172.182.1 Netwark: 252.552.50
A Network	>	EnableDisable	2 Enable
A		Start	O Disable DHCP Server. 2
DHCP Server	Ľ	Limit	Orvest leased address as offset from the network address. 253
	-	Lease time(unit: minutes)	Maximum number of leased addresses. 720
1 Security	>	DNS Server	Expiry time of leased addresses, minimum is 2 minutes (2).
O Advanced Features	>		Define additional DHCP options, for example: 192.168.2.3,192.168.2.4.
🕑 Users Manage	>		
🔮 System	>	DHCP Static Leases	
× Logout	>	ID Host Add	MAC IP Action

Description of the numbered areas

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

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

DHCP Static	Leases				
ID	Host	MAC	IP	Action	*
1					
2	*	54:75:95:06:ea:bc 🗸	\$ 172.18.2.139 v \$	Bind	-
Add 1		(2)	3	(4)	

Description of the numbered areas

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

3.6 Security – ACL

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

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

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

Status	>	ACL Rules
		Default Policy 1 Whitelist
Route Management	>	Control Device To WAN 2 Disable 🗸
- Natwork		Control LAN to Device 3 Disable •
Network	ĺ.	(4) Save
Services	>	ACL Type
		WAN - Blacklist - Source IP 5
11 Security	~	Address
ACL		
		Add 7

Follow the steps below to create an ACL rule:

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

- 5. Select an ACL type;
- ▶ If you have selected the whitelist policy, you need to configure the blacklist IP. Otherwise, the rule will not take effect. "Source IP" refers to the IP from which the access requirement is initiated towards HAP101 and "Destination IP" refers to the IP to which the access requirement is initiated from HAP101.
- 6. Enter the addresses that match the rule;
- 7. Click **Add** to create the rule;
- 8. Repeat above steps to add more rules.

3.6.1 Whitelist ACL rule

Example Scenario:

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

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

Network status before IP blocking:

Status	>	ACL Rules			
		Default Policy	1	Whitelist	~
Route Management	>	Control Device To WAN	2	Enable	~
		Control LAN To Device		Disable	~
A Network	>		3	Save	

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

2	Status	,	Diagnostics		
	- Status		Network Utilities		
¢	Route Management		(1-1-) managerale and a de ad		
đ	Network				
	Interfaces		192.168.19.225	www.google.com	www.google.com
	···· Wireless(WIFI)		Ping	Traceroute	Nslookup
	HaLow WIFI		PING 192.168.19.225 (192.168.19.225): 56 data bytes 64 bytes from 192.168.19.225: seq=0 tt]=128 time=0.848 ms 64 bytes from 192.168.19.235: seq=1 tt]=128 time=0.501 ms		
	Diagnostics		64 bytes from 192.168.19.225: seq=2 ttl=128 time=0.540 ms		
	Network Capture		64 bytes from 192.168.19.225; seq=5 t1=128 time=0.525 ms		
~	1 a .	_	192.168.19.225 ping statistics 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.525/0.615/0.848 ms		

Rule setting:

Status	>	ACL Rules
Route Management	>	Default Policy Control Device To WAN Enable
h Network	>	Control LAN To Device Disable
Services	>	ACL Type WAN - Blacklist - Destination IP
1 Security ACL		Address 192.168.19.225 2 Add 3

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

ACL Rules		
Default Policy Control Device To WAN Control LAN To Device	Whitelist ~ Enable ~ Disable ~ Save	
ACL Type WAN - Blacklist - Destination IP v Address Add	WAN Blacklist Destination IP 10 Address 1 192.168.19.225	Action Remote

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

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

Status >	Diagnostics Network Utilities						
Route Management >	C1-1-2 manufacture alle and - C						
📥 Network 🗸 👻							
Interfaces	192.168.19.225	www.google.com	www.google.com				
· Wireless(WIFI)	Ping	Traceroute	Nslookup				
HaLow WIFI	PING 192.168.19.225 (192.168.19.225): 56 data bytes ping: sendto: Operation not permitted						
Diagnostics							
Network Capture							

3.6.2 Blacklist ACL rule

Example Scenario:

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

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

Network status before IP release:

Status	>	ACL Rules			
		Default Policy	1	Blacklist	~
🜻 Route Management	>	Control Device To WAN	2	Enable	~
		Control LAN To Device	_	Disable	~
A Network	>		3	Save	

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

Status >	Diagnostics Network Utilities		
Route Management >			
h Network		MAN C	
Interfaces	192.168.19.225	www.google.com	www.google.com
Wireless(WIFI)	Ping	Traceroute	Nslookup
HaLow WIFI	PING 192.168.19.225 (192.168.19.225): 56 data bytes ping: sendto: Operation not permitted		
Diagnostics			
Network Capture			

Rule setting:

Status	>	ACL Rules
 Route Management Network 	> >	Default Policy Blacklist Control Device To WAN Enable Control LAN To Device Disable Save
Services	>	ACL Type WAN - Whitelist - Destination IP
1 Security ACL	~	Address 192.168.19.225 Add 3

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

ACL Rules				
Default Policy		Blacklist	•	
Control Device To WAN	Ĩ	Enable 🗸	•	
Control LAN To Device		Disable 🗸	•	
	(Save		
ACL Type	WAN Whitelist Destination	IP		
WAY - Whitelist - Desunation IP	ID Address			Action
Address	1 192.168.19.225			Remove
Add				

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

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

Status >	Diagnostics Network Utilities		
Route Management >	CI-1-1-2 managanda		
n Network			
Interfaces	192.168.19.225	www.google.com	www.google.com
Wireless(WIFI)	Ping	Traceroute	Nslookup
HaLow WIFI	PING 192.168.19.225 (192.168.19.225): 56 data bytes 64 bytes from 192.168.19.225: seg=0 ttl=128 time=0.870 ms		
Diagnostics	64 bytes from 192.168.19.225; seq=1 ttl=128 time=0.603 ms 64 bytes from 192.168.19.225; seq=2 ttl=128 time=0.564 ms 64 bytes from 192.168.19.225; seq=2 ttl=128 time=0.599 ms 64 bytes from 192.168.19.225; seq=4 ttl=128 time=0.824 ms		
	192.168.19.225 ping statistics 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.564/0.692/0.870 ms		

3.7 Advanced Features

3.7.1 IPK Installer

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

Status	>	Upload architecture: mipsel_24kc Unload file to jungt TUSER_SPACE/ink/upload/						
Coute Management	>	Choose local file: Choose File No file chosen	Upload	2				
th Network	>							
Services	>	Download Download ipk file in /mnt/USER_SPACE/ipk/upload/, default down	load all ipk file					
11 Security	>	Download file	Downlo	oad 4				
O Advanced Features	~	Upload file list						
IPK installer		File name	Modify time	Attributes	Size	Remove	Install	Stat
BlueSphere		plc_protocol_vantronos-3.5.2.0.ipk	2024-12-17 06:57:25	FW-FF	1.9 MB	Remove	Install	Uninstall
PLC Protocol Service						(3)		

Description of the numbered areas

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

3.8 BlueSphere

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

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

- Log in to BlueSphere GWM at <u>https://gatewaymanager.bluesphere.cloud/#/login</u> with your authorized account and corresponding password;
- 2. Click the user account in the top right corner and select the **User Profile** option after the login;

	💽 Gwm	Device Management						C 15	:00 (UTC+8)	vantrongateway	§vantron.com ∨	Q	0	Ê
BLUESPHERE	🚺 🛗 🔍 Search					Operation + Save	d Search	× Add (levice Q Use	r Profile	vay Pi	LC U	ora	
Ē	은 Provisioning 스	Device Groups	All Devices							E 108	501			
	Device Management	Ungrouped (21)	Device Name	Model *	Device Status *	SN	Lora Gateway ID	Lora	Lora State	Group Name	License 💌	Operat	ion	
	Configuration	VT-M2M-G202 (1)	V202101003-001	VT-M2M-GLR	Offline	V202101003-001	aaaa42d63cb960e1	~		Ungrouped	VTSYS-20			
		VT-M2M-G304 (0)	5102-20241118-000	WIOT-GT-2AI100	Online	5102-20241118-00002		×		Ungrouped	VTSYS-20			
	Software Management	VT-M2M-GLR (2)	5307-24100010-000	VT-DGL-AH-101-GE	Offline	5307-24100010-00012		×		Ungrouped	VTSYS-20			
e	System 🔨	VT-M2M-R105 (0)	5302-23100006-123	VT-M2M-GLR	Offline	5302-23100006-12346	aaaa40d63cb960df	~	Offline	Ungrouped	VTSYS-20			
		VT-M2M-R102 (0)	GLR-NA-R-1	VT-M2M-GLR	Offline	5302-23100006-12345	aaaa40d63cb960ad	~	Never Seen	Ungrouped	VTSYS-20			

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

(U	ser Profile			(
2	Monitoring 🔨		Basic Information			
	Dashboard		E-mail	j		
	Alarm Overview		Name	jin		
	Alarm Routing		Surname	z		
	Device Report		SMS	+1123456		
	Topology Viewer		Description	-		
	MQTT Tracing			5	F 4	
	Data Widgets	<	Language	English		
୍ର	Provisioning 🔨		Last Login	Dec/18/2024 15:34:23		
	Device Management		Customer ID	В		
	Configuration					
	Edge Computing		Account Security			
	Software Management		Password		Change Password	

- 4. Connect HAP101 to internet;
- Refer to <u>2.3</u> for VantronOS login to HAP101 and navigate to Advanced Features > BlueSphere;

	Status	>	BlueSphere Configration Connecting to the Vantor's next-generation Internet of Things gateway management system (BlueSphere). It provides flexible and practical topology management, comprehensive network status monitoring, powerful
			alarm management, diversified report generation, and strict and flexible security management functions.
1	Route Management	>	Enable Configration Enabled V
	Network	•	Customer ID (2)
	Samian		Pownload Log 3
	Services	1	24-12-18 08:56:47 [DEBUG] 19188 broker.c:302: broker publish to client: /udmp/agent/ota/rpc/# - { "method": "udmpState", "params": { "state": true } } 24-12-18 08:56:48 [DEBUG] 19216 ota_client.c:10: ota_client arrived topic: /udmp/agent/ota/rpc/#
1	Security	>	24-12-18 08:56:48 [DEBUG] 19216 ota_client.c:111: ota client arrived payload: { "method": "udmpState", "params": { "state": true } } 24-12-18 08:56:48 [DEBUG] 19216 ota business.c:112: ota model method: udmoState
	, occurry		24-12-18 08:56:48 [INFO] 19216 ota_business.c:28: udmpStateonline
			24-12-18 08:56:48 [DEBUG] 19296 mqtt_client.c:41: async mqtt subscribe success callback: [1]
	N		24-12-16 V8:505:48 [DEBUG] 19296 mdt_client.c:41: async mdt subscribe success callback: [2] 24-12-18 08:55:49 [DEBUG] 19296 mdt_client.c:41: async mdt subscribe success callback: [3]
	Advanced Features	×.	24-12-18 08:56:49 [DEBUG] 19296 matt client.c:41: async matt subscribe success callback: [4]
		_	24-12-18 08:56:49 [DEBUG] 19296 mqtt_client.c:41: async mqtt subscribe success callback: [5]
	IPK installer		24-12-18 08:55:49 [DEBUG] 19296 mgtt client.c:41: async mgtt subscribe success callback: [6]
			2+-12-10 00:00:00 [DEBUG] 19296 mgttc[Lient.c:41 async mgtt subscribe success callback: [7]
	BlueSphere		24-12-18 08:57:07 [ERROR] 19296 mgtt_client.c:121: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
			24-12-18 08:57:07 [ERROR] 19296 mgtt_client.c:122: async mgtt connect lost callback, case: (null)
	PLC Protocol Service		24-12-18 08:57:07 [ERROR] 19296 mgtt client.c:123: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
			24-12-18 08:5/:0/ [DEBUG] 19188 proker.c:302: proker publish to client: /udmp/agent/ota/rpc/# - { "method": "udmpState", "params": { "state": false } }

- 1) Paste the customer ID;
- 2) Enable the configuration;
- 3) The device log will be automatically printed and you can click the link to download.
- 6. Wait for the UDMP Agent to download and install;
- The UDMP Agent is the application that allows HAP101 to interface with BlueSphere GWM.
- 7. When the UDMP agent is online, it indicates the device is enrolled to BlueSphere GWM with success;

	Status	,	BlueSphere Configration
			Connecting to the Vantrov's next-generation Internet of Things gateway management system (BlueSphere). It provides flexible and practical topology management, comprehensive network status monitoring, power and the state of the
ł	Route Management	>	ainin mangemen, oreismeo teport generation, and strict
			Enabled
	Network		Customer ID E
	INCLWOIK	´	
			Download Log
5	Services	>	24-12-18 08:58:57 [DEBUG] 19216 ota_client.c:111: ota client arrived payload: { "method": "udmpState", "params": { "state": false } }
			24-12-16 00:50:57 [INFO] 19216 Ota_business.c:28: udmpState
1	Security	>	24-12-18 08:59:19 [INFO] 19296 mqtt_cilent.c:130: 24-12-18 08:59:19 [INFO] 19296 mqtt_cilent.c:131: async mqtt reconnected success callback, case: automatic reconnect, start sub
			24-12-18 08:59:19 [INFO] 19266 mgtt_client.c:132: ************************************
C.	N		24-12-18 08:59:20 [DEBUG] 19216 ota_client.::10: ota client arrived topic://dm//agent//ta/rpc/#
A.	Advanced Features	Ľ	24-12-18 08:59:20 [DEBUG] 19216 ota_cilent.c:111: ota cilent arrived payload: { "method": "udmpState", "params": { "state": true } } 24-12-18 08:59:20 [DEBUG] 19216 ota_cilent.c:112; ota model methodu udmpState
	IPK installer		24-12-18 08:59:20 [INFO] 19216 ota business.c:28: udmpState
			24-12-18 08:59:20 [DEBUG] 19296 mqtt_client.c:41: async mqtt subscribe success callback: [2]
	BlueSphere		24-12-18 08:59:20 [DEBUG] 19296 mqtt_client.c:41: async mqtt subscribe success caliback: [3] 24-12-18 08:59:21 [DEBUG] 19296 mqtt_client.c:41: async mqtt subscribe success caliback: [4]
	DI C Destanal Service		24-12-18 08:59:21 [DEBUG] 19296 mgtt_client.c:41: async mgtt subscribe success callback: [5]
	1201100001001000		24-12-18 08:59:21 [DEBUG] 19296 mtt_client.c:41: async mqt subscribe success caliback: [7]
			4 24-12-18 08:59:21 [DEBUG] 19296 mott client c:41: async mott subscribe success callback; [8]

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

Gwm	Device Management				(16:56 (UTC+8)		s 🗸	û 0
BLUESPHERE	🔋 🖮 🔍 Search		Operatio	n 👻 Saved Se	arch 👻 Add Device	1= ±	Gateway	y PLC Lora
Monitoring ^	Device Groups	All Devices						
Dashboard								
Alarm Overview	Ungrouped (8)	Device Name	Model -	Device Status 👻	SN	Group Name	U .	Operation
Alarm Routing	🗆 🖿 Loop (2) 🛛 😶	12345678 New	VT-DGL-AH-101-GE	Online	12345678	Ungrouped	V	
Device Report	🗆 🖿 DEMO (5)	HAP 101 AP-1	VT-DGL-AH-101-GE	Offline	5302-24080016-00001	DEMO	V	
Topology Viewer		HAP 101 AP 2	VT-DGL-AH-101-GE	Offline	5302-24080016-00004	DEMO	v	
MQTT Tracing		HAP 101 STA-2	VT-DGL-AH-101-GE	Offline	5302-24080016-00003	DEMO	V	
Data Widgets	<	HAP101 STA-1	VT-DGL-AH-101-GE	Offline	5302-24080016-00002	DEMO	v	
Provisioning ^		test_gateway_wyj_1	VT-M2M-G335	Offline	test_gateway_wyj_1	Ungrouped	v	
Device Management		HAP101_1	VT-M2M-MM6108-AP	Offline	5300-24010140-00013	Ungrouped	V	

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

Gwm	Configuration	• 17	':09 (UTC+8)	• Q Q û
всоезрнене	Q Search			Remote Access
Monitoring ^	Davice Groups	VantronOS Config		(1) Remote Terminal
Dashboard	Device droups			Remote Desktop
Alarm Overview	 Ungrouped (8) 		Open device terminal	
Alarm Routing	• V5106-202107015-17			
	v5106-202301004-004		Log into vantionOS	
Device Report	test_gateway_wyj_1			
Topology Viewer	• 12345678			
MQTT Tracing	* HAP101 1			
Data Widgets	<			
Provisioning	* HAP101_2			
	• R105-001			
Device Management	· 5300-24010140-00016			
IConfiguration	 Loop (2) 			
Edge Computing	DEMO (5)	Oops not applicable to selected device, please use Remote Access.		

3.9 User Management

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

ADMIN			
Users			
Users Overview			
ADMIN	SSH Access: Disabled Group: users Data bilded Ext Data 12 (5:11:18 2024	Edit	Delete
2	Date Added: Fri Dec 13 05:11:18 2024 Last Entry: Fri Dec 13 05:11:18 2024		
Add New User			

Key information of the current user:

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

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

Status	>	Add New User					
O Route Management	•	lefault password vantron			0		
		User Name	User	~	(2)		
A Network	>	SSH Access	Enabled	~	(4)		
Services	>	Enable Network Menus			J		
1 Security	>	Interfaces Wireless(WIFI) V Halow WIFI Diagnostics Network Capture					
Advanced Features	>	PLC Protocol Service BlueSphere V IPK installer					
		Enable Services Menus	~	C			
Users Manage	*	DHCP Server		9			
Edit Users		Static Routing Automatic Network Routing	-				
🔮 System	>	Enable Security Menus					
× Logout	>	ACL Enable System Menus	V				
		🗸 Log 🗸 System 🗌 Administration 🗸 Backup / Flash Firmware 🗸 Reboot ✔ Ter	minal				
						6	
		Back or Refresh				Save & Apply	Save Reset

1. Default password of the new user is "vantron";

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

ADMIN USERI Users			
Users Overview			
USERI	SSR Access: Enabled Group: user. News patients Turn Dec 12.00-14.00, 2021	Edit	Delete
2	Last Entry: Tue Dec 17 08:44:00 2024		
ADMIN	SSH Access: Diabled Group: usen Deta bidded Ec Dec 12 051118 2024	Edit	Delete
2	Last Entry: Fri Dec 13 05:11:18 2024		
Add New User			

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

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

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

3.10 System

3.10.1 System

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

Status	>	System		
		Here you can configure the basic aspects of your device like its hostname or the timezone.		
Q Route Management	>	System Properties		
📥 Network	>	General Settings Language and Style		
A		Local Time	Tue Dec 17 08:30:35 2024 Sync with browser	1
Services	>	Hostname	VantronOS-BF82	2
1 Security	>	Timezone	UTC 🗸	3
O Advanced Features	>	Time Synchronization		
		Enable NTP client	✓ ④	
🕻 Users Manage	>	NTP server candidates	0.centos.pool.ntp.org ×	
			1.openwrt.pool.ntp.org ×	G
🚭 System	~		2.cn.pool.ntp.org ×	0
System			us.pool.ntp.org +	
Administration	-	Provide NTP server	6	

Description of the numbered areas

- 1. Synchronize the device time with the browser (local) time upon a click of the button
- 2. Host name of the device displayed when logging in to the device terminal
- 3. Device time zone
- 4. Enable/Disable NTP online time adjustment
- 5. NTP server candidates that can be used to synchronize the internal clock of the device with an accurate time source
- 6. Enable/Disable the NTP online time server
- HAP101 is used as an NTP server.

For language settings, please refer to 2.8.

3.10.2 Administration

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

SSH Login

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

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

	SSH Access	
	Dropbear is running	
	Enable/Disable	
	Interface	
		vps.davn.d
		war ter
🚭 System 🗸		Listen only on the given interface or, if unspecified, on all
-	Port	22 ⁽²⁾ Specifies the listening port of this Dropbear instance
	Password authentication	Allow <u>SSF</u> password authentication
Administration	SSH-Keys (4) Here you can paste public SSH-Keys (one per line) for SSH public-key authent	cation.
-		

- Depending on the connectivity of the host computer and HAP101, select a port to access (When "unspecified" is selected, SSH login is available through both ports);
- 2) Specify a port number for monitoring (port 22 by default)
- 3) Enable SSH password authentication
- 4) Optionally, add SSH-Keys for public key authentication
- 3. Open a terminal emulator (PuTTY or MobaXterm recommended) on the Windows computer;
- 4. Launch an SSH session on the terminal emulator;

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

Session settings						×
SSH Telnet Rsh	Xdmcp RDP	VNC FTP		🧕 🎽 File Shell	🌏 🔊 Browser Mosh	🧐 🔳 Aws S3 WSL
Sasic SSH settings						
Remote host * 172.18.	2.1	🗹 Spec	ify username root		× 🔈	Port 22 🛟
Advanced SSH settin	age Terminal	sattings N	letwork settings	+ Bookmark se	ttings	
	Sec	cure Shell (SSH	I) session			
		S OK	😣 Ca	incel		

- 6. Click **OK** to start the session;
- 7. Input the password (rootpassword) to log in.

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

 MobaXterm Personal Edition v22.1 • (SSH client, X server and network tools) 					
 SSH session to root@172.18.2.1 Direct SSH : . SSH compression : x (disabled or not supported by server) SSH-browser : . X11-forwarding : x (disabled or not supported by server) 					
➤ For more info, ctrl+click on <u>help</u> or visit our <u>website</u> .					
BusyBox v1.36.1 (2024-12-13 05:11:18 UTC) built-in shell (ash)					
V200R003.F0000-05 Built at 2024-12-13 09:16:15					
root@Vantron0S-BF82:~#					

3.10.3 Log

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

Status	>	Log	
O Route Management	,	View syslog Basic Setting Remote syslog	
 Route Management 	í	The EO Band Jan anthony. However, anthony and at the and -	
h Network	>	Last de trait leg entries, memosi entries sontee at the end .	
Services	>	Tup Dec 17 08:45:08 3824 deemon.notics trd(1723): [2824/12/17 08:458:09:1724] H: _hs	
1 Security	>	Two Dec. 17 09/0016 3804 deemon.notic try0[173]; 1284/12/17 09/0016/68(7) N:wiLtr_g: ++ [usign/4]dested (2) Two Dec. 17 09/0016 3804 deemon.notic try0[173]; 1284/12/17 09/0016/68(7) N:wiLtr_g: ++ [usign/4]dested (2) Two Dec. 17 09/0016 3804 deemon.notic try0[173]; 1284/12/17 09/0016/68(7) N: is /_wiLtr_g: 128.129, clients: 1 Two Dec. 17 09/0016 3804 deemon.notic try0[173]; 1284/12/17 09/0016/68(7) N: started process, pid: 594 Two Dec. 17 09/0016 3804 deemon.notic try0[173]; 1284/12/17 09/0016/68(7) N: started process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/68(7) N: started process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/68(7) N: started process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/67(7) N: started process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/67(7) N: tstretd process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/67(7) N: tstretd process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/67(7) N: tstretd process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/001 N: tstretd process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/001 N: tstretd process, pid: 594 Two Dec. 17 09/0012 1804 deemon.notic try0[173]; 1284/12/17 09/0016/001 N: tstretd process, pid: 594	
O Advanced Features	>	ue Dec 17 09:01112 224 deemon.Hrv untpol_1990]; sn: bad number Tue Dec 17 09:0114 2024 deemon.Hrv untspol_2973]; read /tct/nsts - 4 addresses Tue Dec 17 09:0114 2024 deemon.Hrv untspace/strojenter (strojenter); strojenter (strojenter); strojenter (strojenter); Tue Dec 17 09:0114 2024 deemon.Hrv untspace/strojenter); strojenter (strojenter); strojenter (strojenter); strojenter Tue Dec 17 09:0114 2024 deemon.Hrv untspace/strojenter); strojenter (strojenter); strojenter); strojenter (strojenter); strojenter); strojenter); strojenter Tue Dec 17 09:0114 2024 deemon.Hrv untspace/strojenter); strojenter); strojenter; strojenter); strojenter); strojenter; strojenter); strojenter; strojenter; strojenter); strojenter; s	
🕼 Users Manage	>	Two Dec. 17 0501316 3080 demon.netics try012733) [2304/12/7 05013167325] N process writed with code 0, atts 5044 Two Dec. 17 0501316 3080 demon.netics try012733) [2304/12/7 05013167325] N process writed with code 0, atts 504 Two Dec 17 0501316 3020 demon.netics try012733) [2304/12/7 05013167359] Ni _lws_lc_untag: [wsisrv[4]edopted] (0) 1.000min Two Dec 17 050143 3020 demon.ner untig01999] sin bad number	
System	Ľ	Tue Dec 17 09:01:46 2024 daemon.info dinsmaq[6673]: read /ttc/hosts - 4 addresses Tue Dec 17 09:01:46 2024 daemon.info dinsmaq[6673]: read /tmp/hosts/dhcp.cfg01d1c - 1 addresses Tue Dec 17 09:01:46 2024 daemon.info dinsmaxe(Mon(6673): read /tmp/hosts/dhcp.cfg01d1c - 4	
· System		Tue Dec 17 09:01:49 2024 authoriv.info dropber(6576): Not backgrounding Tue Dec 17 09:05:14 2024 deenon.err unittpd[1990]: shi bad rumber Tue Dec 17 09:05:15 2004 unittpd] info dropber[87031: Oil to comparing from 172 18 2 180:5003	
Administration		tue ber 17 06/05/27 2024 deam info inspecific [24:29]. Nilai Cumerci Lini (1997). 21:20-21	
Log		Tue Dec 17 09:05:29 2024 authoriv.info dropbear[6876]: Early exit: Terminated by signal Tue Dec 17 09:05:29 2024 authoriv.info dropbear[6876]: Not backgrounding Tue Dec 17 09:05:39 2024 authoriv.und rodpear[6929]: Not backgrounding for 'roct' from 172 18.2 130:5003	
Terminal		Tue Dec 17 09:05:38 2024 deemon.err unttpd[1990]: shi bad number	

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

	Status	>	Log		
0	Route Management	,	View syslog Basic Setting Remote syslog		
 Route Management 	Í	Write system log to file	1	/var/log/syslog.log	
đ	Network	>	System log buffer size	2	1024
					() KB
ç	Services	>	Console log output level	3	Error
1	Security	>	Cron Log Level	4	Warning

Description of the numbered areas

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

3.10.4 Terminal

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

Web Terminal			
Enable/Disable	disable	∼	
Interface	enable		
Back or Refresh		(2	Save & Apply Save Reset
Web Terminal			
Enable/Disable		enable	~
Interface		All	~
Terminal	3	Please click here to open Web Term	inal

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)
[−] / [−] / _− , , , , , , , , , , , , , , , , , , ,
V200R003.F0000-03 Built at 2024-01-30 12:45:27
root@VantronOS-D869:~#

3.10.5 Backup/Flash Firmware

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

Firmware Update

Firmware Update Backup/Restore Configuration				
Flash new firmware image				
Upload a sysupgrade image here to replace the running firmware form local.(Device model: V	T-M2M-MM6108-AP)			
Keep settings:	1 • 🗸			
Image:	2 Choose File XOS_WebU000-03.xos Upload image 3			
Uploading 17% 3.2M/19.1M				

Description of the numbered areas

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

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



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

System - Flashing
The systems in fluctures in the lattice sour DO NOT FOURE ROFF THE DEVICE! Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

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

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

Firmware Update Backup/Restore Configuration	
Backup	
Click "Generate archive" to download a tar archive of the current configuration files.	
Download backup:	Generate archive
Restore	
To restore configuration files, you can upload a previously generated backup archive here. To rese	t the firmware to its initial state, click "Perform reset" (only possible with squashfs images).
Reset to defaults:	Perform reset (2)
Restore backup:	3 Choose File No file chosen Upload archive (4)
	② 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 (including only the configuration files and preset files other than user files or programs)
- 2. Factory reset the device (user configurations will be cleared)
- 3. Select a backup package from the local directory
- 4. Upload the backup package to restore the settings

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

Backup file list		
Firmware Update Backup Restore Configuration		
This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modif	fied files in /etc/config/ and certain other configurations are automatically preserved.	
Show current backup file list	Open list 3	
<pre>## This file contains files and directories that should ## be preserved during an upgrade.</pre>		
# /etc/example.conf (1) /etc/bootscript/		
		11
	2 Submit Re	set

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

86

3.10.6 Reboot

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

3.11 Logout

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

CHAPTER 4 USE CASE

4.1 Application Topology

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



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

- 5. PC1 can manage all devices that obtain IP addresses from the DHCP server, while PC2 manages HAP101-AP. When PC3 connects to HAP101-STA via 2.4GHz Wi-Fi, it receives an IP address from the DHCP server but cannot access HAP101-STA's VantronOS. However, if the Ethernet port of HAP101-STA is reconfigured from WAN to LAN, HAP101-STA's VantronOS becomes accessible via an Ethernet connection using the device's LAN IP address.
- After the setup, to view the IP of the cameras, you will need:
 - Log in to HAP101-STA's VantronOS via an Ethernet connection using the device's LAN IP address;
 - 2. Check the IP address of the clients on the 2.4GHz Wi-Fi connection page.

4.2 Wiring

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

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

Refer to steps 2 through 4 in 4.3.1 if you are not sure about steps 1 and 2.

3. Navigate to **Network > Interfaces > WAN** to check the IP information.

4.3 Setup of HAP101-STA

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

4.3.1 HaLow

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

HaLow WLAN MAC: XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
WAN MAC: XX:XX:XX:XX:XX:XX
WLAN Login IP: 172.18. 2.1
User name/Password: admin/XXXXXX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXXX
HaLow WLAN SSID: XXXXXX
HaLow WLAN Password: XXXXXXXX

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

HaLow WLAN MAC: XX:XX:XX:XX:XX:XX WLAN MAC: XX:XX:XX:XX:XX:XX WAN MAC: XX:XX:XX:XX:XX:XX WLAN Login IP: 172.18. 2.1 User name/Password: admin/XXXXXX WLAN SSID: XXXXXX WLAN Password: XXXXXXX HaLow WLAN SSID: XXXXXX HaLow WLAN Password: XXXXXXXX

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



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

Super user: root // password: rootpassword

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

Status 🔪	HaLow WIFI		
Jaius -	HaLow WIFI Settings		
Quick Start >	General Setting Advanced Setting		
A Network	Status	Model: Manter BSSID: 1509-554:10:1113 SSID: DOL. AH3-101-1113 (Eneryption: WPA3 SAE (CCMP) Channel: 22 (916 500 MH2) (TsPower: 21 dBmir Country: US Signal: -53 dBm; Voise: -23 dBm Bitters 25 35 MH2	
Wireless(WIFI)	WIFI mode	AP (1) Switch Mode (2)	
HaLow WIFI	SSID	Client Mesh	
Static Routes	Encryption	SAE 🗸	
Diagnostics	Key		
ACL	Bridge ETH(WAN)		
DHCP	Associated Stations		
🕑 Users Manage 🔹 🕨	Network @ (Master "DGL-AH-101-1113")	MAC-Address 0C:BF:74:A6:C6:F4	Host ?
O Customization >	Back or Refresh		Save & Apply Save Reset

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

- 6. Save the settings and wait a few seconds to allow the change to apply;
- Reconnect the host computer to the 2.4GHz Wi-Fi of HAP101-STA and log in to VantronOS using the new WLAN IP: 172.18.3.1;

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



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

Wifi Client Setting		
Select SSID	Mac/Bssid 🔎	Key 🤎
100% ; DGL-AH-101-DEBE	✓ Auto	✓ Ki z
Scan WIFI No connection		

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

Wifi Client Setting									
Select SSID	Mac/Bssid •	Key 💿							
100% ; DGL-AH-101-DEBE 🗸	Auto	✓ K z							
Scan WIFI Connected: 0h 0m 43s IPaddr: 172.18.1.199									

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

4.3.2 Reconfiguring WAN to LAN

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

4.3.3 2.4GHz Wi-Fi

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

Status	>	WIFI Settings				
		Enable/Disabled WIFI		Enable	~	
Quick Start	>	WIFI Mode		AP	~	
1 Virtual Tunnel	>			Save		
A Network	×	Mode: BSSID: Channel:	AP 1(2.412 GHz)	SSID: Encryption: Tx-Power:	Vantron-B940A1 none 20 dBm	
Interfaces		Signal: Bitrate:	0 dBm 300 Mbit/s	Noise: Country:	-95 dBm US	
Wireless(WIFI)		SSID		Vantron-B940A1		
HaLow WIFI		Encryption	1	OPEN	~	
···· Static Routes		+ Advance Settings				
Firewall		Apply				

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

WIFI Settings				
Enable/Disabled WIFI		Enable	▼	
WIFI Mode		AP	~	
		Save		
Mode: BSSID: Channel: Signal: Bitrate:	AP 1(2.412 GHz) 0 dBm 300 Mbit/s	SSID: Encryption: Tx-Power: Noise: Country:	Vantron-B940A1 none 20 dBm -95 dBm US	
SSID		Vantron-B940A1		
Encryption		OPEN	~	
- Advance Settings				
Country Code		00-World	~	
Hwmode		2.4G	▼	
Channel		1	~	
Bridge ETH(WAN)				
Apply				

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

4.4 Viewing Camera IPs

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

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

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

CHAPTER 5 DEBUGGING THE DEVICE

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

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

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



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



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

Baud rate	Data bit	Polarity	Stop bit
57600	8	None	1

Session se	ttings														\times
SSF	N Telnet	<mark>⊮</mark> Rsh	Xdmcp	The second secon	VNC	🍪 FTP	SFTP	serial	ile) Shell	🌏 Browser	🔊 Mosh	🍄 Aws S3	III WSL	
<i>\$</i>	Basic Serial	settings													
	Serial por	t * COM	9 (USB S	erial Port	(COM9))		~		Speed (bp	s) ¹ 5760)0 ~				
<i>\$</i> 7	Advanced Se	rial settir	ngs 💣] Terminal	settings	🔶 🕇 E	Bookmark	settings							
		Seri	al engine:	PuTTY	(allows r	nanual C	OM port s	etting)			v				
			Stop bits Parity	o 1 None	× × ×	lf yo con em	ou need to t ifiguration f bedded TF	transfer file: île), you cai TP server	s (e.g. rou n use Mob	ter baXterm				,	
		FI	ow control	Xon/Xoff defaults	~	"Se	ervers" wi	indow>	• TFTP	server					
		Exec	cute macro	at sessio	on start: [<none></none>		~							
					•	OK		🙁 Can	icel						

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



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

CHAPTER 6 DISPOSAL AND PRODUCT WARRANTY

6.1 Disposal

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

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

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

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

6.2 Warranty

Product warranty

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

Out-of-Warranty Repair

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

Returned Products

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

Appendix Regulatory Compliance Statement

FCC Compliance Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

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

Exposure to radio frequency energy:

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

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

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

IC Statement

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

(1) This device may not cause interference, and

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

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

Exposure to radio frequency energy:

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

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

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

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

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

L'exposition à l'énergie radiofréquence:

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