Gigabit Industrial Bridge Repeater

VAR1200-H/VAR1200-L/VAR1800-H/

VAR1800-L/VAR600-H/VAR600-L

Quick Setting Guide

Statement

Copyright © 2022 Shenzhen Houtian Network Communication Technology Co., Ltd.

Copyright, all rights reserved

Notice

The parameters used in the screenshots shown in this manual are only for reference of setting examples and may not be completely consistent with the actual situation. Please set the parameters according to your actual needs.

Due to different software versions, the screenshots shown in this manual may not be exactly the same as the web interface of the product you purchased. Please configure your product according to the actual web interface.

Product application and secondary development precautions

1. Problems related to wireless interference:

- 1.1 Use the ping command to test the wireless transmission performance. If it is found that the delay of the ping packet response is extremely uneven, and there are many responses with a large delay, it can basically be judged that the wireless has been strongly interfered;

- 1.2 The product antenna should be kept as far away as possible from sources of interference, such as switching power supplies, antennas of other modules or wireless products, etc.;

- 1.3 If it is too close to the antenna of other wireless products, it will cause mutual interference, resulting in an increase in the transmission bit error rate and a slower transmission rate. At this point, the wireless signal must be properly attenuated. The methods of attenuating the signal include adding obstacles, extending the distance,

and adding a resistor in series between the antenna feed point and the antenna, etc., to meet the actual application requirements;

2. Selecting a suitable power supply is the key to good and stable wireless transmission and stable operation of the product. Improper power supply will cause damage to the product or poor wireless performance. The selected power supply must meet the voltage range and input power requirements of the power supply input, and the ripple must be less than the required maximum power supply ripple (100mV);

3. POE related issues:

- 3.1 If the product has PSE function (POE output), it needs 48V power supply voltage and meets the power requirements of POE output before it can be used;

- 3.2 If the network port of the product has a POE output port, if it is connected to other non-POE network ports, please use it with caution, and ensure that the access network port is isolated from the ground, otherwise it may cause damage to the connected product!

- The safest way is: let the product use a two-pin switching power supply without ground (AC TO DC, AC input is two-pin instead of three-pin).

The adapter power supply in all the schematic diagrams shown in the following figures are externally connected to the power supply.

Transmission distance parameter table (Table 1)				
Model Number	Antenna type	Frequency Band		Barrier-free point-to-point transmission distance(for reference only)	Transmission Rate （Mbps）
VAR1200-H	External	Dual Frequency	2.4GHz	400m--500m	300
			5GHz	400m	900
VAR1200-L	Built in		2.4GHz	300m--400m	300
			5GHz	300m	900
VAR1800-H	External	Single Frequency	5GHz	400m	1800
VAR1800-L	Built in			300m	1800
VAR600-H	External		2.4GHz	500m	600
VAR600-L	Built in			400m	600

Power Supply Parameter Table (Table 2)					
Model Number	Wide voltage power supply		Output Power	Typical power supply	Ripple
VAR1200-H/VAR1200-L VAR1800-H/VAR1800-L VAR600-H/VAR600-L	No POE output power supply	DC12V--48V	≥30W	12V/3A	<100mV
	With POE output power supply	DC48V	≥57W	48V/1.2A	<200mV
The standard kit of this product does not include a power supply, please select the power supply carefully according to "Table 2", otherwise the product may be damaged or the WiFi performance may be degraded.					

Notice:

In the actual application environment, if the POE output port (PSE) is connected to a non-POE network port (PD is an access network port), please use it with caution, and ensure that the access network port is isolated from the power ground, otherwise it may cause the access device to fail. damage! When the power input is 48V (≥57W), the POE output is valid!
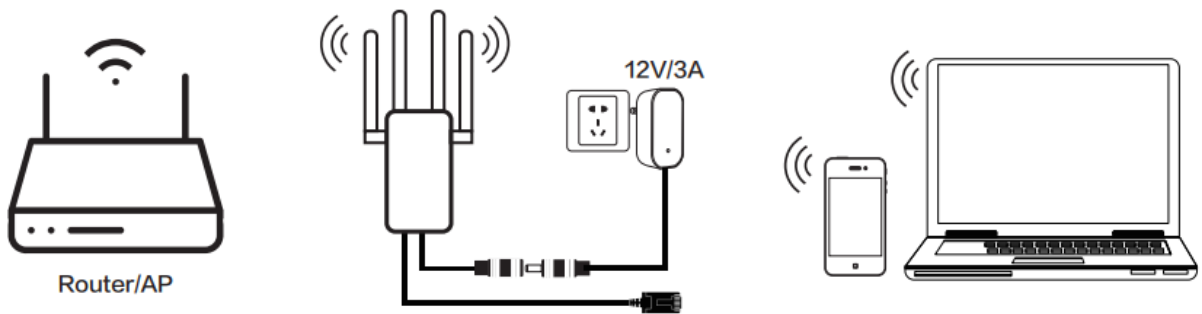
Contents

Chapter 1 Application Mode

1.1 Bridge + Repeater Mode(In the actual application environment, if the POE output port (PSE) is connected to a non-POE network port (PD is an access network port), please use it with caution, and ensure that the access network port is isolated from the power supply ground, otherwise it may cause the access device. damage!)

There are three application modes for the bridge mode of VONETS device: WiFi repeater, WiFi bridge and WiFi AP.
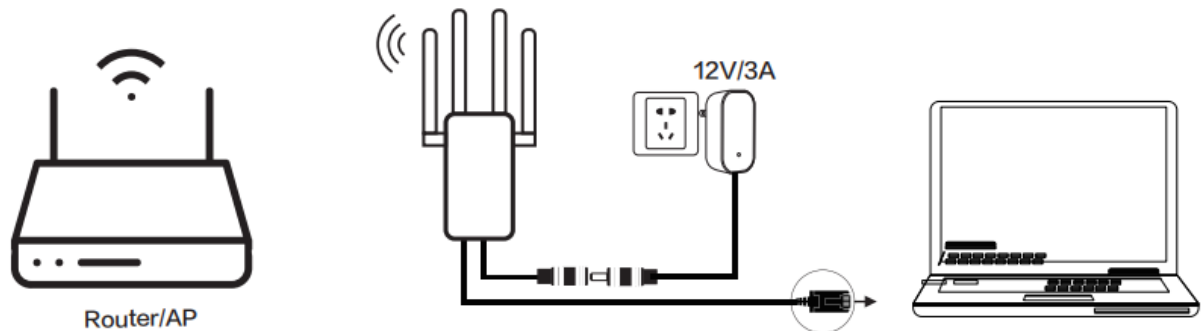
- **WiFi Repeater:**
  VONETS device as WiFi Repeater, it must be configured to source WiFi hostpot parameters, can be used to extend the wireless signal coverage of existing APs or wifi router .
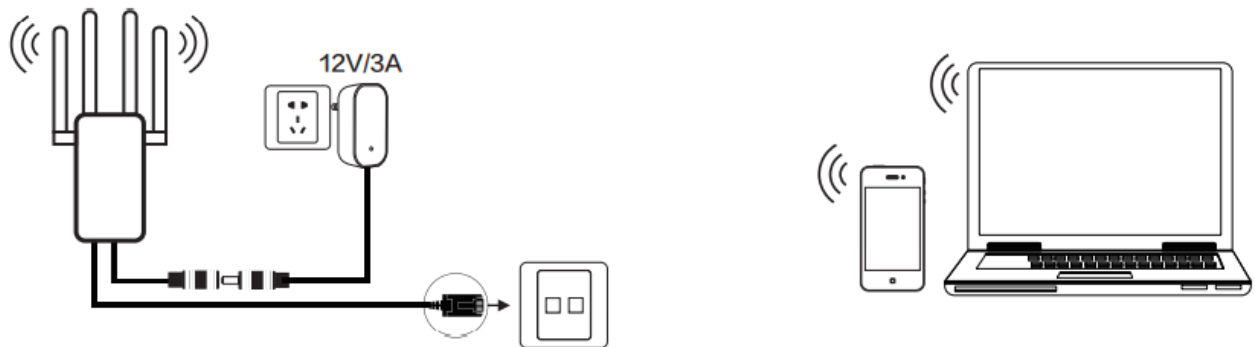

- **WiFi Bridge:**
  VONETS device as WiFi bridge, it must be configured to source WiFi hotspot parameters, can be used for devices only with Ethernet ports to access wireless networks.


- **WiFi AP：**
  VONETS device as WiFi AP, it can achieve wireless access to wired LAN, no configuration required, plug and play.
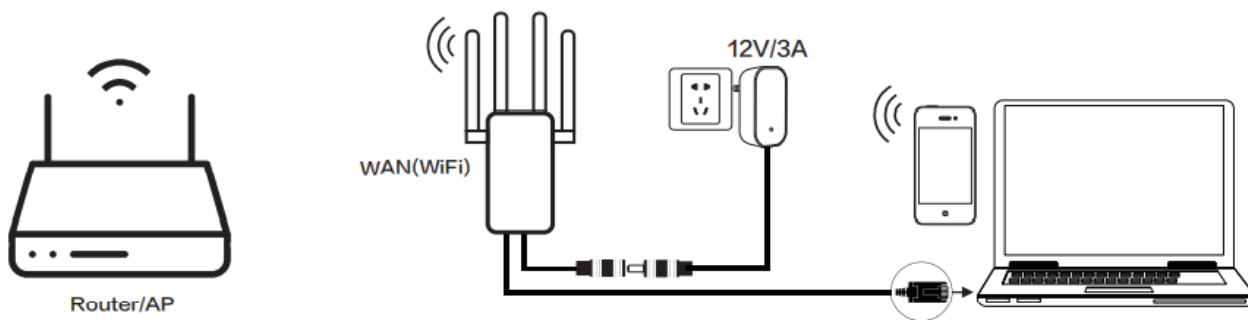
1.2 Router Mode(In the actual application environment, if the POE output port (PSE) is connected to a non-POE network port (PD is an access network port), please use it with caution, and ensure that the access network port is isolated from the power supply ground, otherwise it may cause the access device. damage!)

● The VONETS device is used as a wireless router. The default Ethernet port is the WAN port, and the default Ethernet cable is the LAN port. The WAN and LAN ports are interchangeable (the shell is marked with WAN/LAN ports);
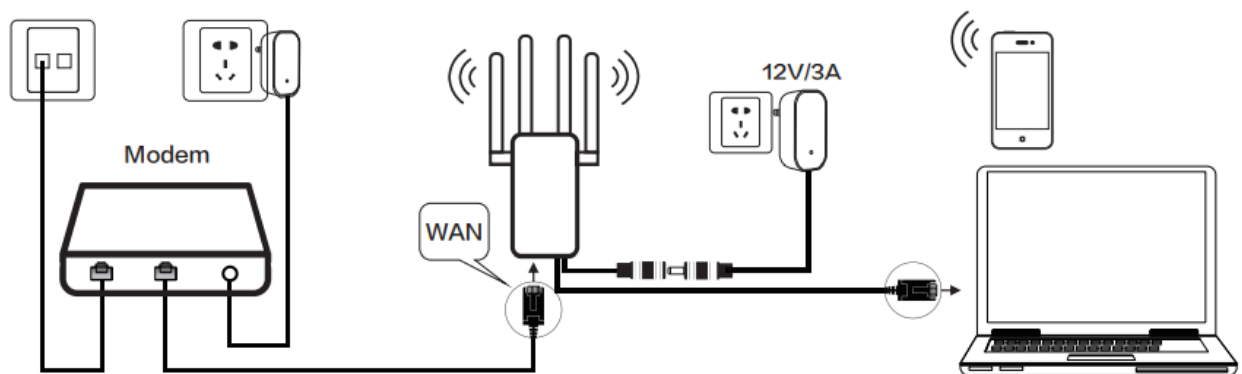
● The VONETS device is used as a wireless router, and the WAN port can be set to connect to a WiFi hotspot and used as a secondary router. Its Ethernet port and Ethernet cable are both LAN ports.

Chapter 2 Bridge+Repeater Mode Configuration Instruction

2.1 Device connect(In the actual application environment, if the POE output port (PSE) is connected to a non-POE network port (PD is an access network port), please use it with caution, and ensure that the access network port is isolated from the power supply ground, otherwise it may cause the access device. damage!)

Power on VONETS device by 12V/3A power supply, then connect to PC, there are two connection ways as below:
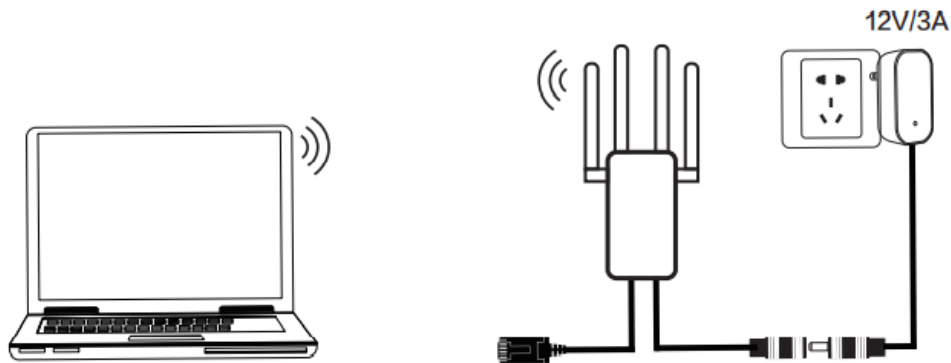   A. Computer is wired connected to LAN port of VONETS device;
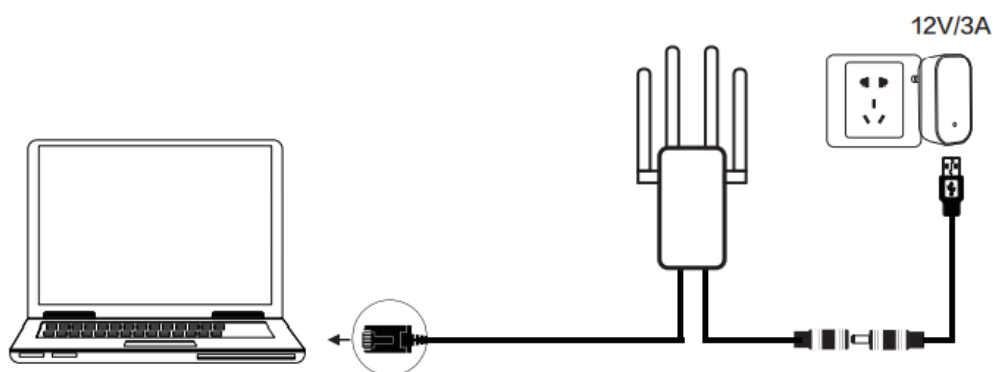
<p align="center">（Recommend Method）</p>

   B. The computer wirelessly connects to the WiFi signal of VONETS device, its default hotspot parameters are as follows:
   WiFi SSID: VONETS_****** (corresponding to VONETS device MAC address)
   WiFi password: 12345678

（After the WiFi parameters are configured, the WiFi will be disconnected, that is normal.）

2.2 Bridge+Repeater Application Configuration

The configuration steps of VONETS device for WiFi repeater and WiFi bridge are basically the same, so this manual combines the configuration instructions of the two application modes.
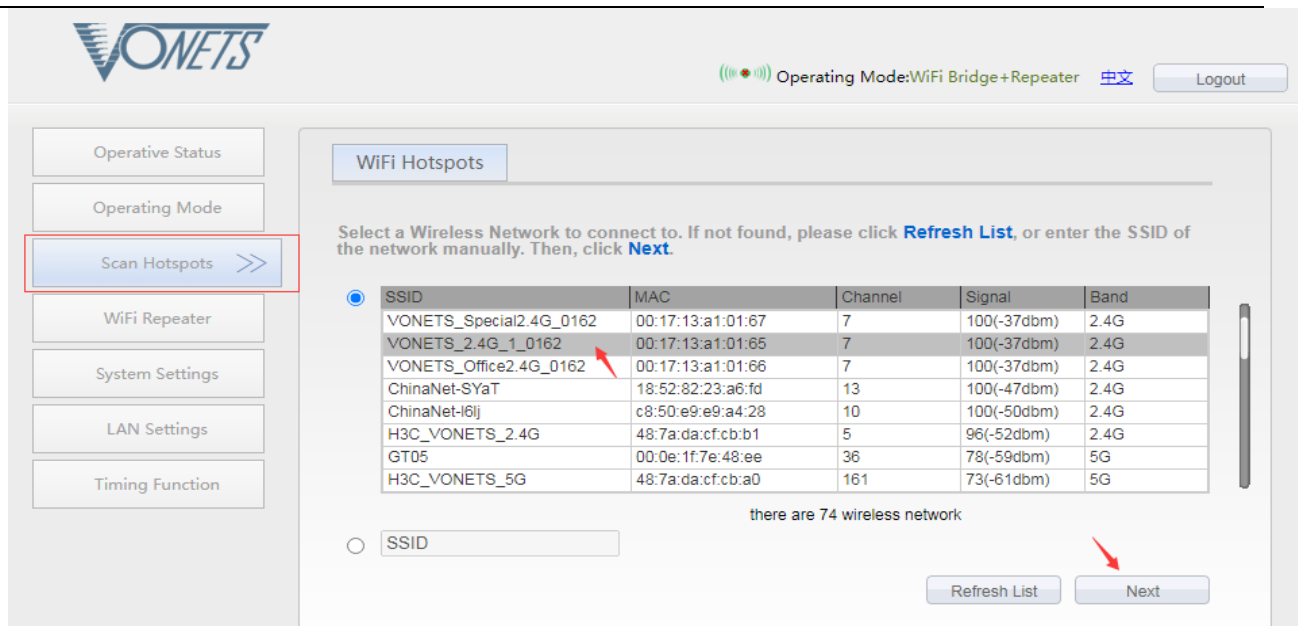
1. After computer is connected to VONETS device, open browser, input configured page: http://vonets.cfg (or IP: 192.168.254.254), then press Enter;
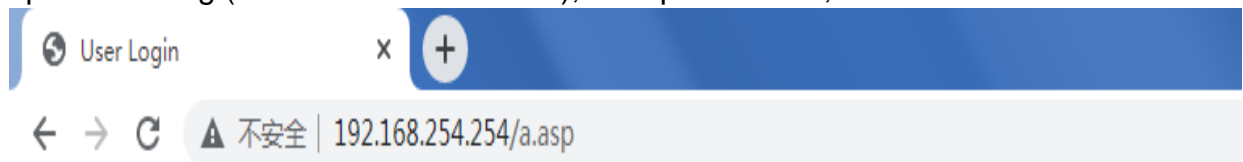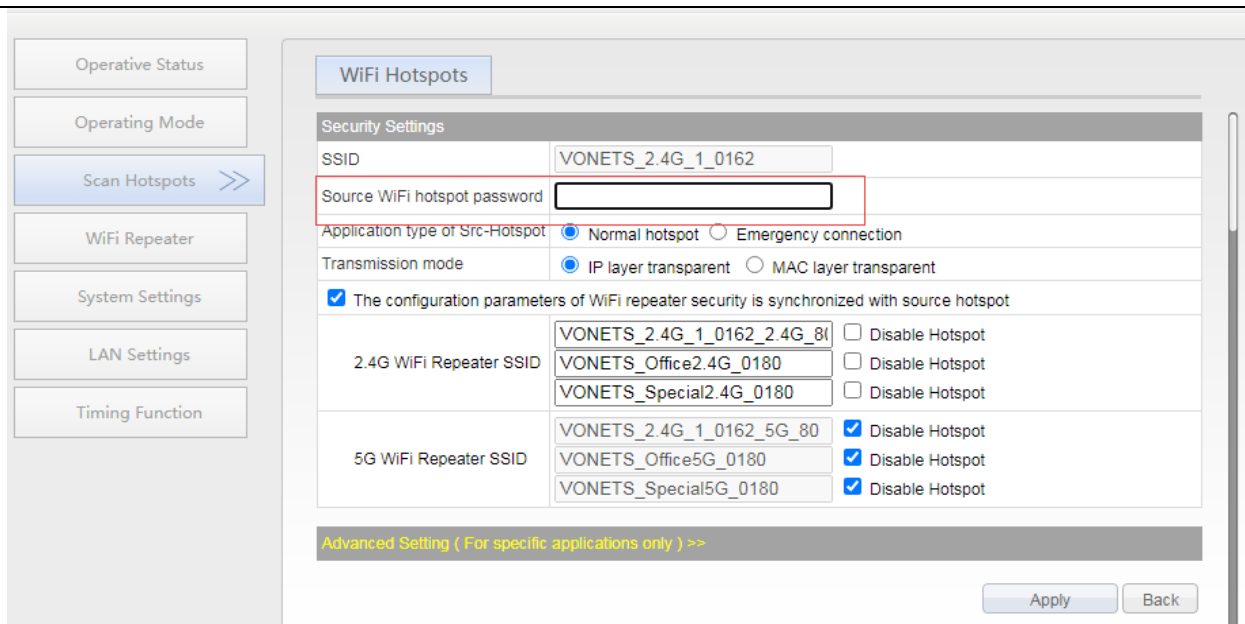

2. Input User name and Password in login page (both are "admin"), click "Login" button to enter configured page;
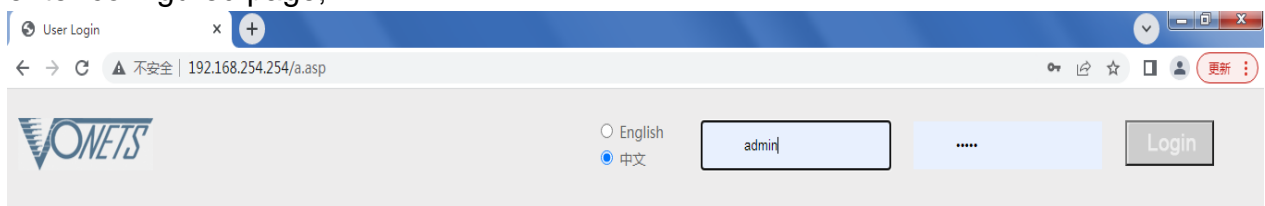
3. "Scan Hotspots", choose the source hotspots, click "Next";

4

4. Input "Source wireless hotspot password", click "Apply";

- **IP layer transparent transmission** (factory default), transparent transmission of IP layer data, can meet most of WiFi bridge applications;
- **MAC layer transparent transmission**, transparent transmission of all data above the MAC layer (link layer) and MAC layer, including IP layer data. MAC transparent transmission can solve some special applications for MAC layer encryption, such as GoPro camera, Cisco AP, Hikvision monitoring system, etc;
- The option "**The configuration parameters of WiFi repeater security is synchronized with source hotspot**" is default ticked, it means the SSID of VONETS repeater is associated with the SSID of the source hotspot, and the WiFi password is the same as the password of the source hotspot;
- **Disable hotspot**, if you select "Disable hotspot" on the right side of the SSID, the device will not transmit the corresponding hotspot and can only be used as a bridge application;
- **Advanced Setting,**include Hot spot authentication match mode, WiFi Signal Motion Detection and SSA Signal strength alarm threshold,these options here can be kept unchanged, for instructions on this option, go to www.vonets.com and download the "V Series WiFi Bridge Advanced Features Instruction";

5. Click "Reboot", VONETS device will connect to the configured WiFi hotspot automatically, if connection is successful, the WiFi LED light will flash quickly;
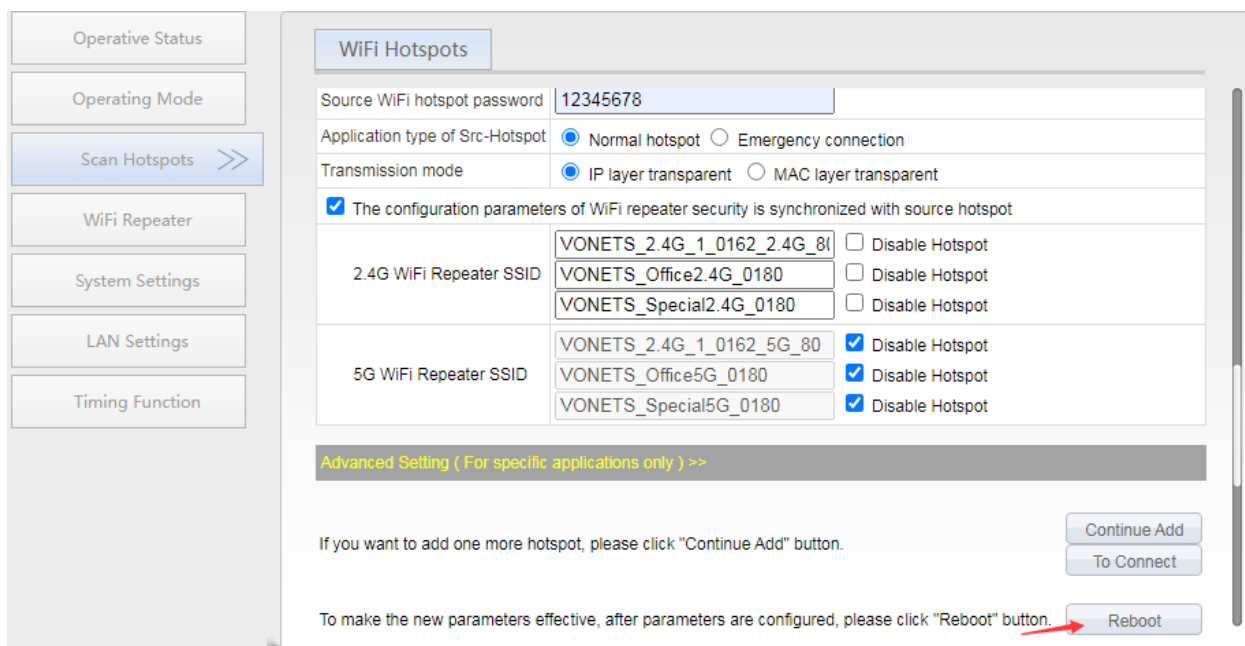

Remark 1:	LED Light Form			
Model	Blue Light	Green Light	Yellow Light	Red Light
VAR1200-H/VAR1200-L	2.4G Connection Status Light	5G Connection Status Light	Ethernet Cable Connection Status Light	POE Output connection light
VAR1800-H/VAR1800-L	/	5G Connection Status Light		
VAR600-H/VAR600-L	2.4G Connection Status Light	/		

① VONETS device is not connected to any hotspot, WiFi connection status light will flash quickly;

② VONETS device is connected to hotspot successfully, but hotspot signal strength　is greater than 50%, WiFi connection status light will quick flash;

③ VONETS device is connected to hotspot successfully, but hotspot signal strength is less than 50% greater than 10%, WiFi status light will pause flash and flash;
VONETS device is connected to hotspot failed, WiFi connection status light will flash slowly.

2.3 AP Application Configuration

VONETS device can be configured as an AP application, the wireless terminal device can connect to VONETS device hotspot to connect to the network; however, it is best to change its WiFi name and password for network security.

1. Log in to the configuration page http://vonets.cfg (or IP: 192.168.254.254you're your computer browser, both user name and password are "admin";
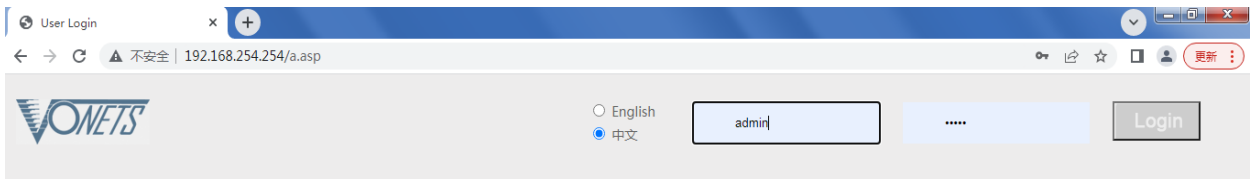

2. Change the WIFI name: select "Basic Settings" in "WIFI Relay", enter the new WIFI name in the text box after the SSID, and click the "Apply" button;
Note: There are a total of 6 hotspots in dual-band, you can set the account name and password accordingly;
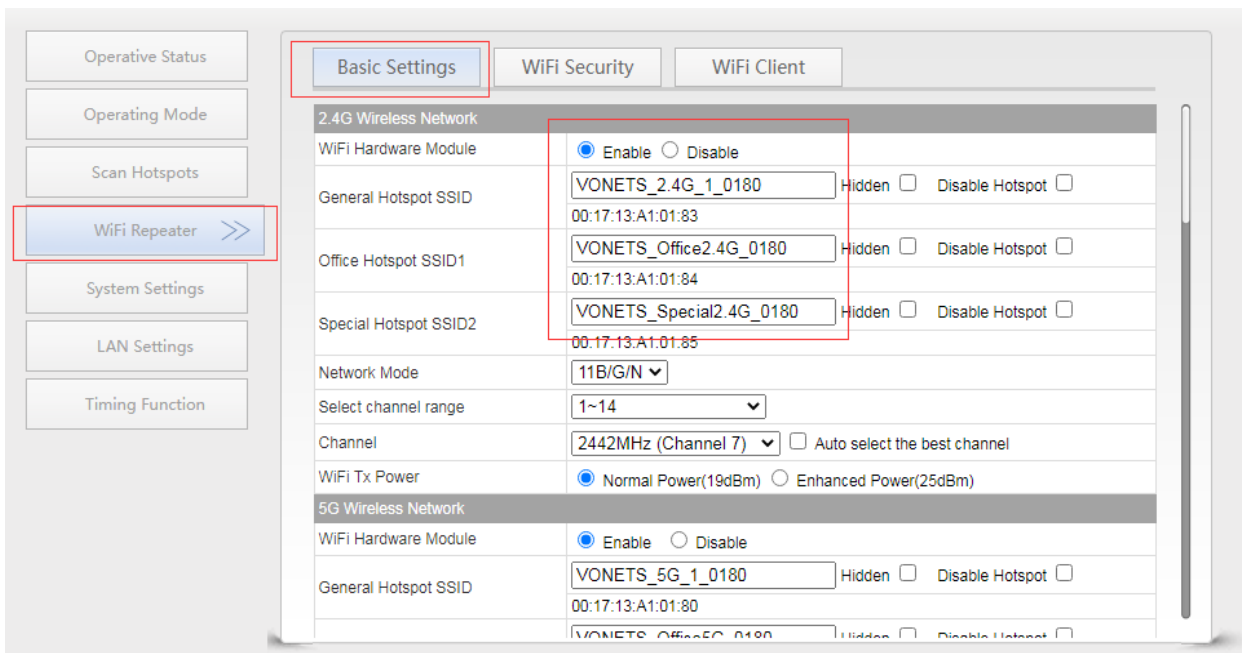
3. Revise WiFi password, in "WiFi Repeater"---"WiFi Security", enter new WiFi password in "Pass Phrase", click "Apply";
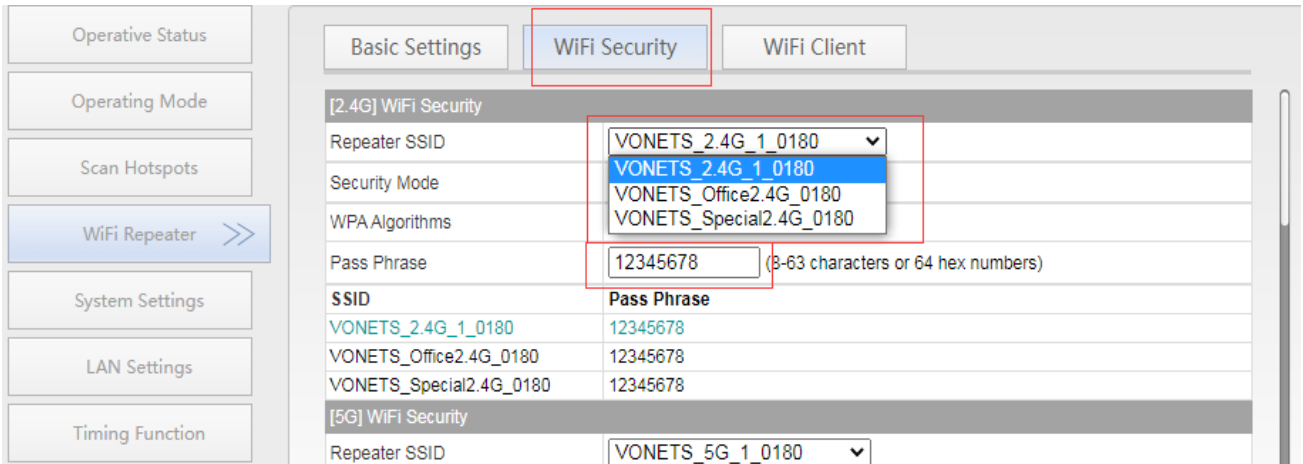
4. "WiFi Tx Power" of VONETS device can be changed, jump to "System Settings"---- "Advance Settings", choose suitable transmit power, then click "Apply";
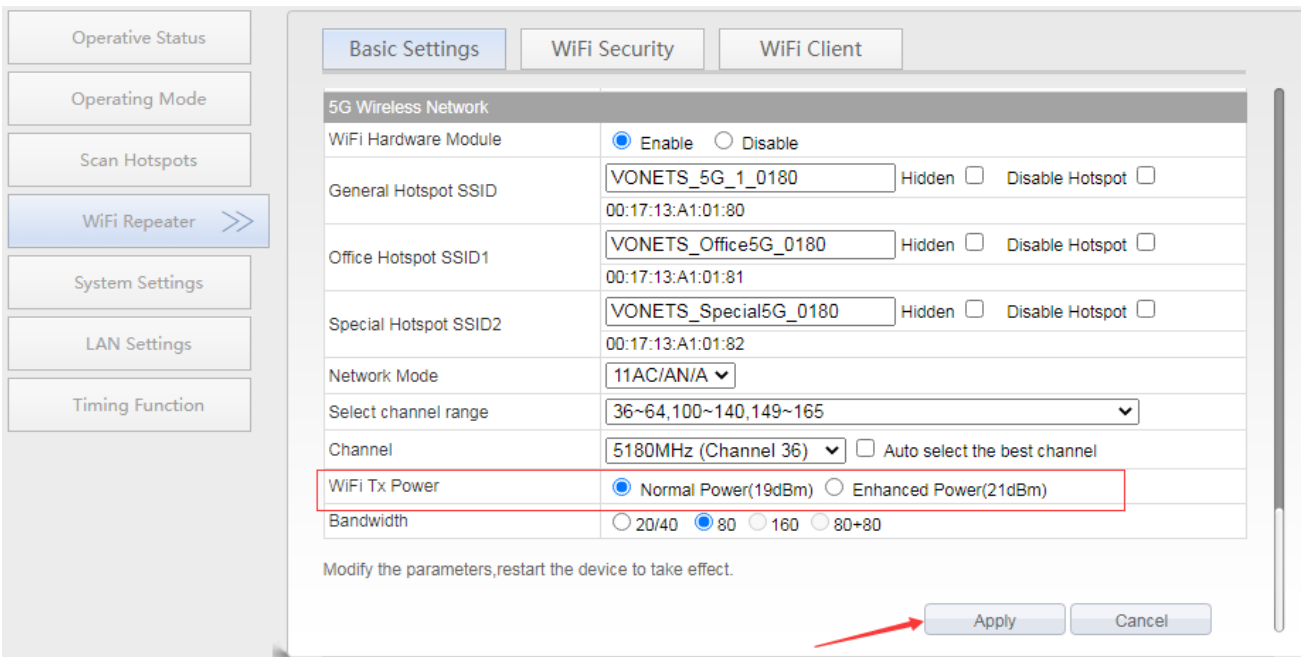
5. Reboot device, jump to "System Settings"---- "Reboot Device", click "Reboot", when it is finished, all revised options will take effort.
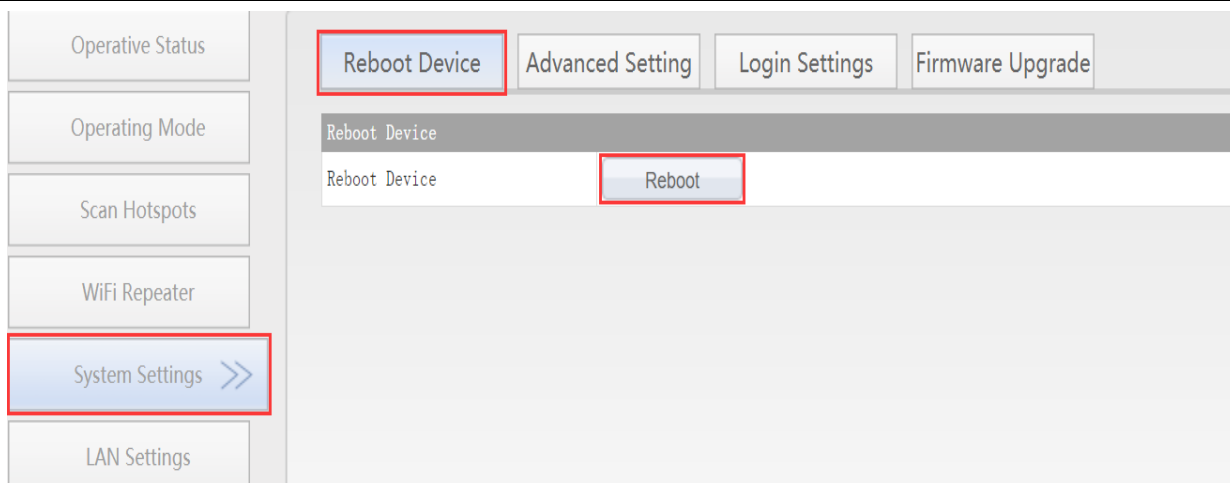
Remark 2: When VONETS device connects to external network, its IP address will be changed. At this time, when log in configured page, we suggest you enter configured domain name: http://vonets.cfg. Or in Windows command window, enter the command: ping vonets.cfg, to get the IP address of the device, then log in configuration page by this IP address

Chapter 3 Router Mode Configuration Instruction

3.1 Change device mode (In the actual application environment, if the POE output port (PSE) is connected to a non-POE network port (PD is an access network port), please use it with caution, and ensure that the access network port is isolated from the power supply ground, otherwise it may cause the access device. damage!)

1. Power on VONETS device by 12V/3A power supply, then connect to PC, there are two connection ways as below:
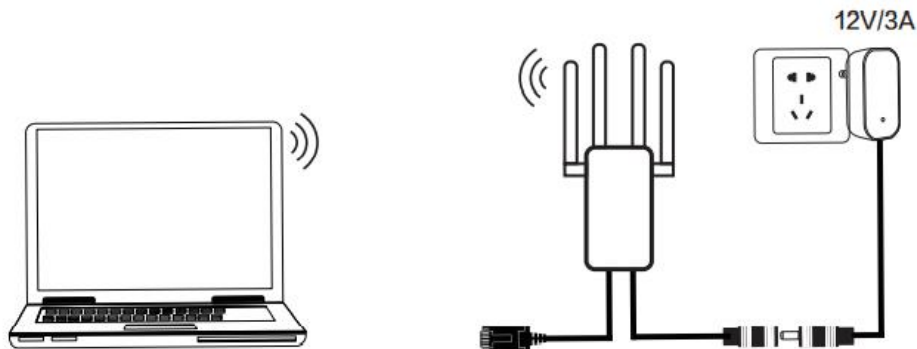   A. Computer is wired connected to LAN port of VONETS device;
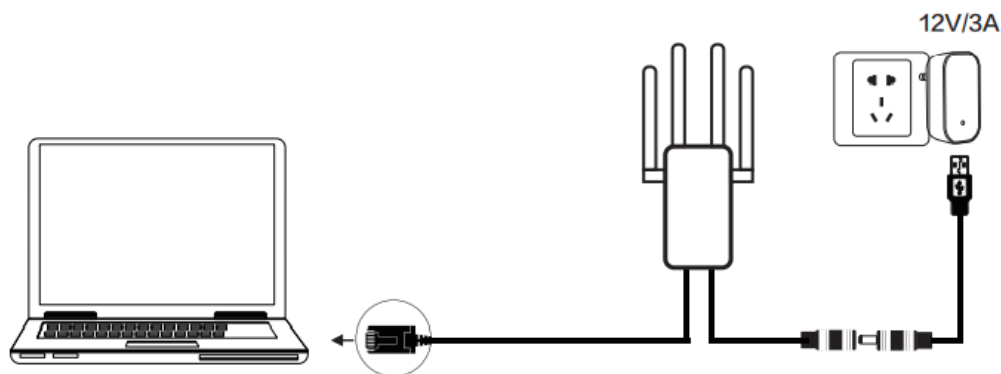
（Recommend Method）

   B. Computer wirelessly connects to the WiFi signal of VONETS device, its default
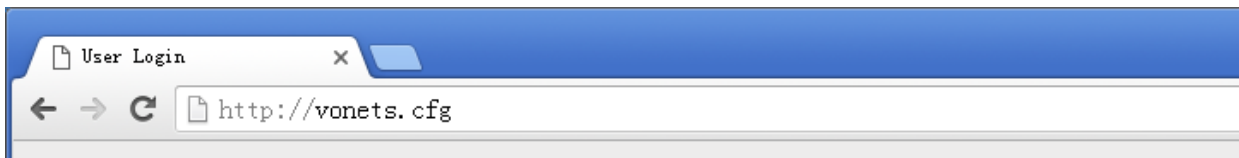
hotspot parameters are as follows:

WiFi SSID: VONETS_****** (corresponding to VONETS device MAC address)

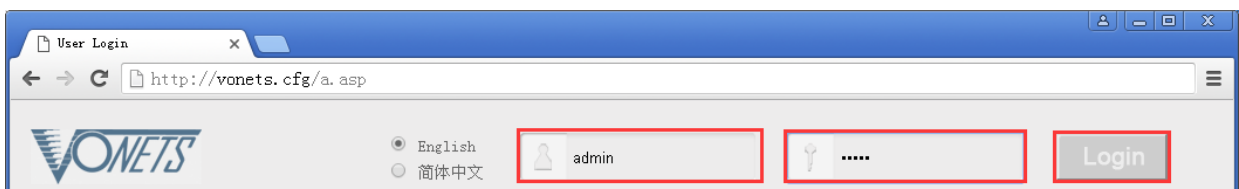WiFi password: 12345678

(After the WiFi parameters are configured, the WiFi will be disconnected, that is normal.)
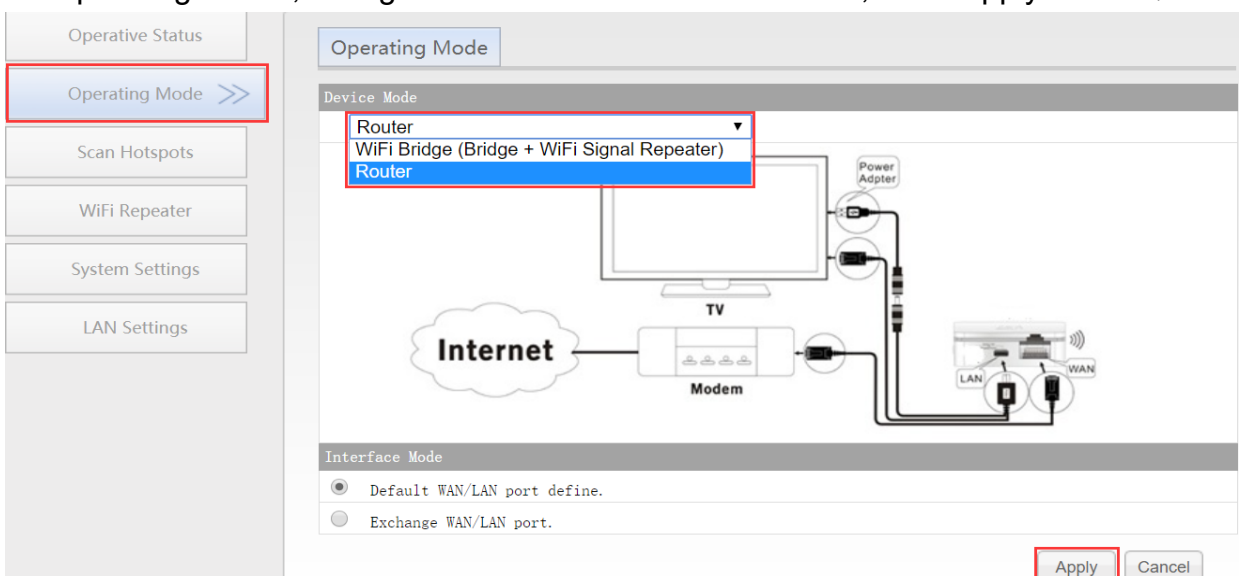
2. After computer is connected to VONETS device, open browser, input configured page domain name: http://vonets.cfg (or IP: 192.168.254.254), then press Enter;
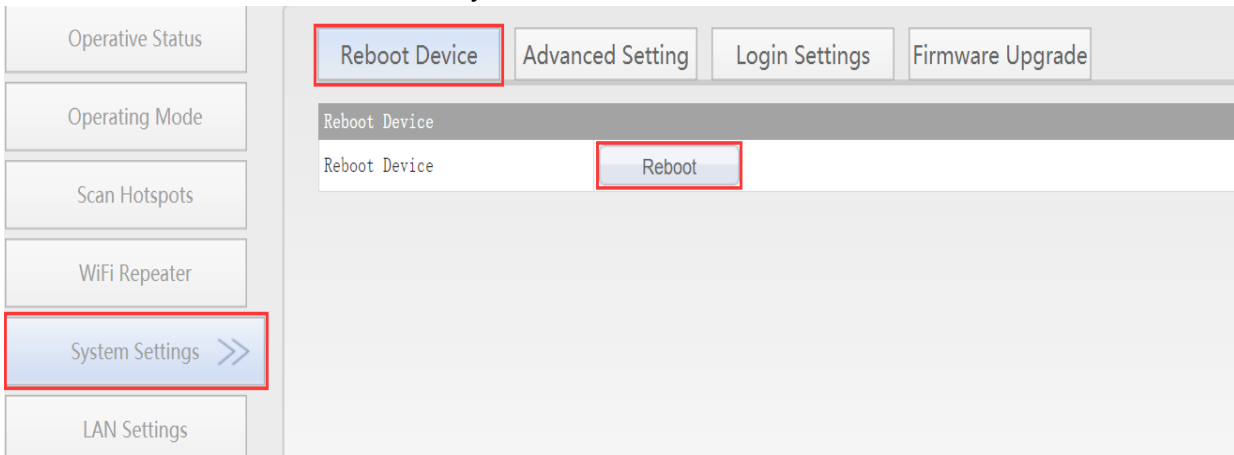

3. Enter User name and Password in login page (both are "admin"), click "Login" button to enter configured page;

4. In "Operating Mode", change Device mode to "Router" mode, click "Apply" Button；

5. Reboot device: go to "System Settings"-- "Reboot device", click "Reboot" button, VONETS device will automatically switch to router mode.

3.2 WAN port settings

3.2.1 WAN/LAN exchange

In routing mode, the WIFI hotspot of the VONETS device is the WAN port and the Ethernet cable is the LAN port, and the WAN/LAN can be interchanged;
The WiFi of the VONETS device is the WAN port by default, and the Ethernet cable is the LAN port by default. If the interface mode is changed to "WAN/LAN interchange", the Ethernet cable is the WAN port, and the WiFi is the LAN port (no modification required);
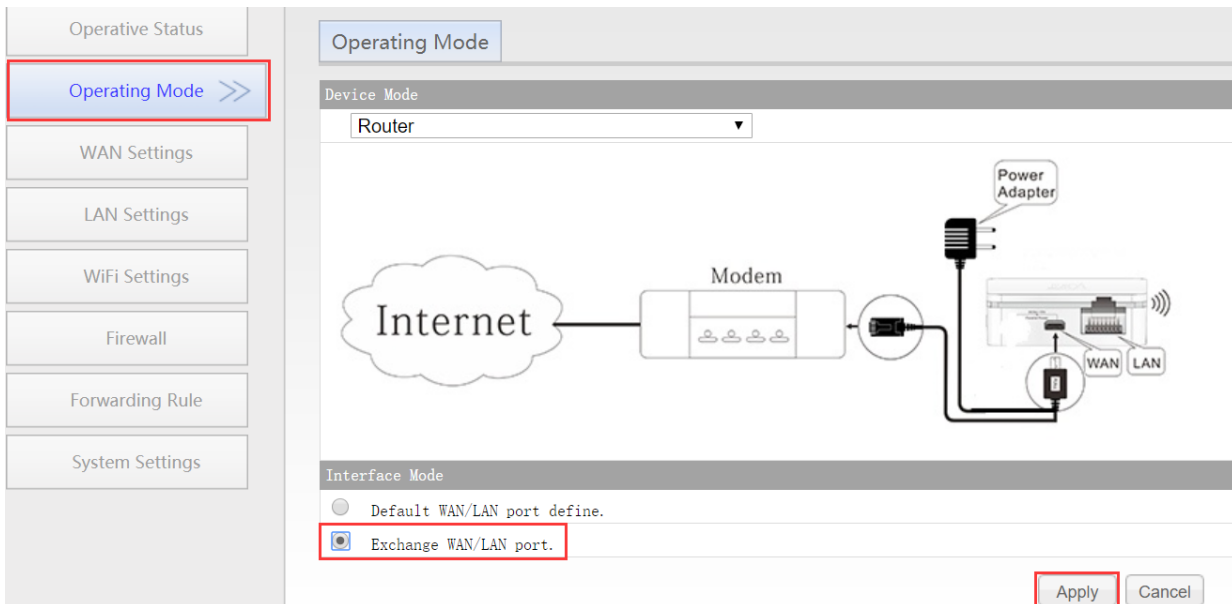
3.2.2 WAN Port connection method

By setting the WAN port of the router, you can change the network connection type according to the actual needs of the individual, there are three types of WAN port connections commonly used in the routing mode of VONETS device: DHCP(Auto Config),

PPPoE(ADSL) and WiFi. DHCP and PPPoE are wired connections, and the WAN port needs to be connected to the source network through a wired connection:

● DHCP(Auto Config): WAN port connection type is selected as **"DHCP(Auto Config)"**, VONETS device will automatically obtain IP address from source network;

● PPPoE(ADSL): WAN port connection type is selected as **"PPPoE"**, that is, ADSL virtual dialing mode requires ISP (Internet Service Provider) to provide Internet account and password;

● WiFi: WAN port connection type is selected as **"WiFi"**, VONETS device uses a built-in WiFi network card (used to connect to the source hotspot) as a WAN port, and all Ethernet ports as LAN ports, while providing WiFi hotspot functions.
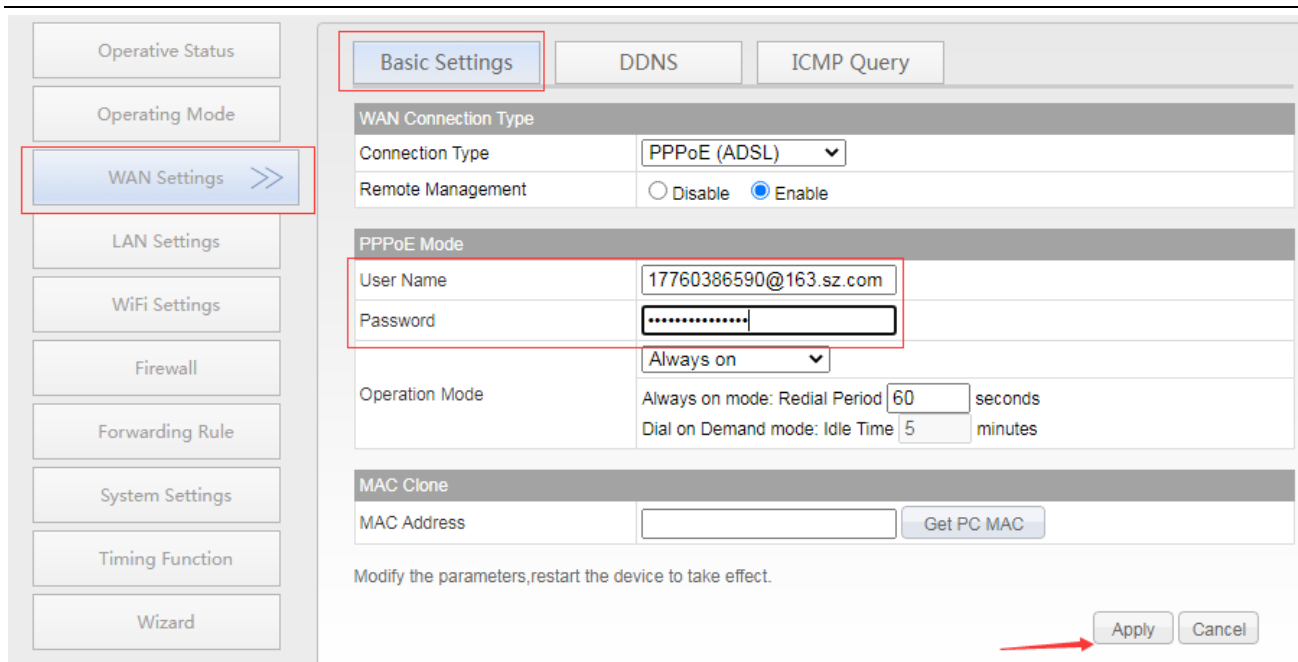
3.2.3 WAN port wired connect network──DHCP

The default WAN port connection method of VONETS device is DHCP.　WAN port can automatically obtain an IP address after connecting to the source network.
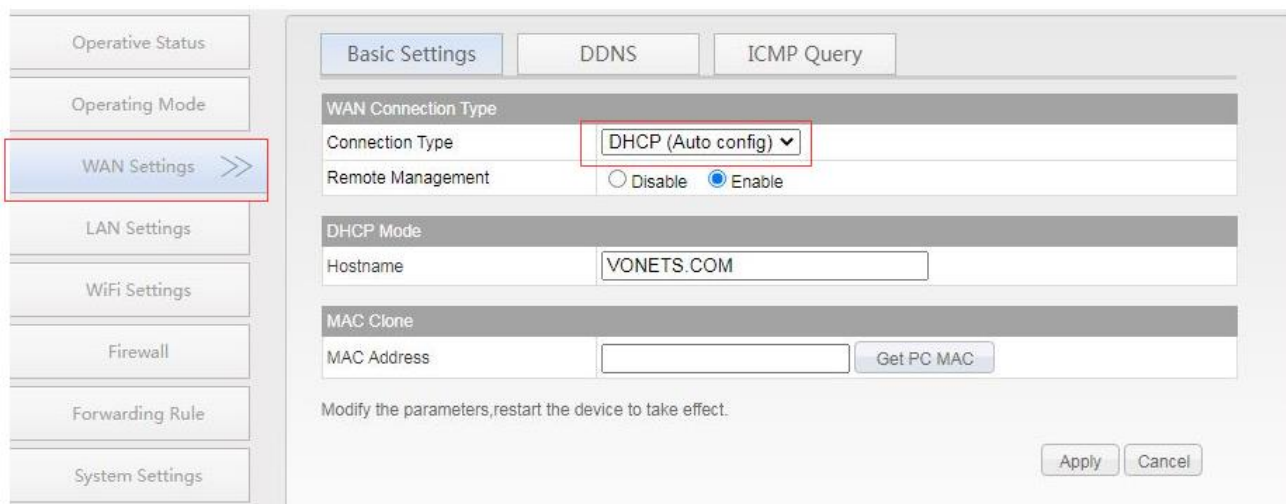

3.2.4 PPPoE WAN port wired connect network──PPPoE

In "WAN settings", select "Basic settings", change the connection type to "PPPoE (ADSL)", then enter the Internet account and password provided by the ISP (Internet Service Provider), click the "Apply" button, and reboot VONETS device, then can access to network.
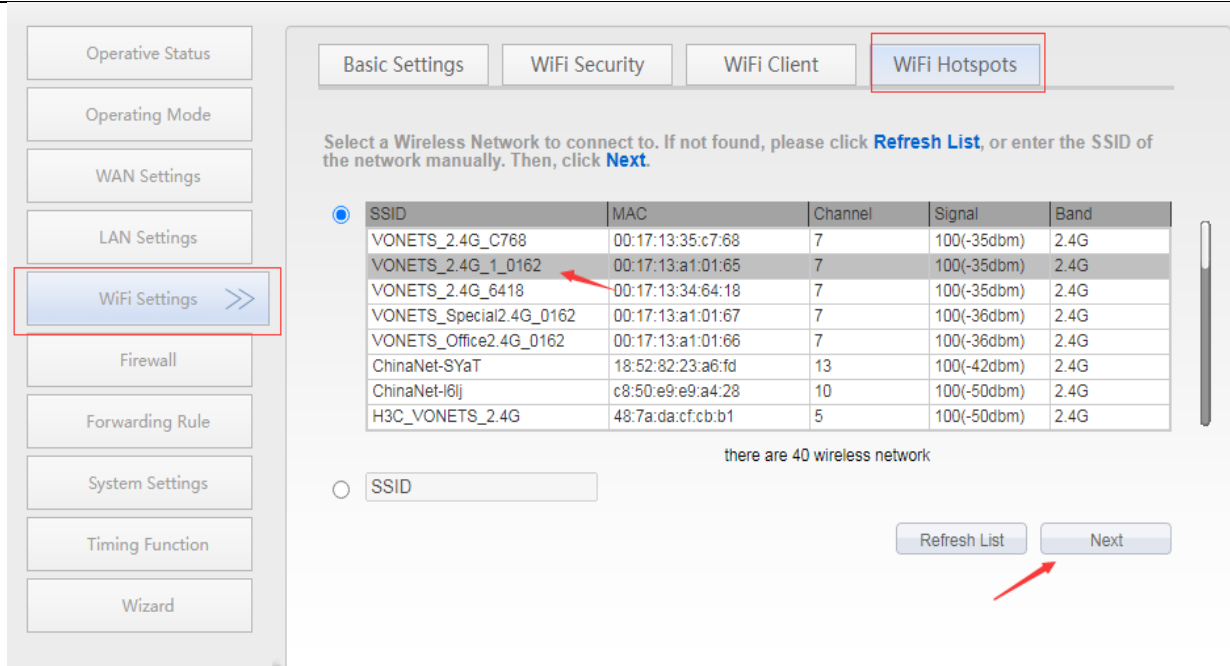
3.2.5 WAN port wireless connect network---- WiFi

1. In "WAN Settings", select "Basic Settings", change Connection type to "WiFi", then click "Scan Hotspots" to enter the scanning hotspot list.
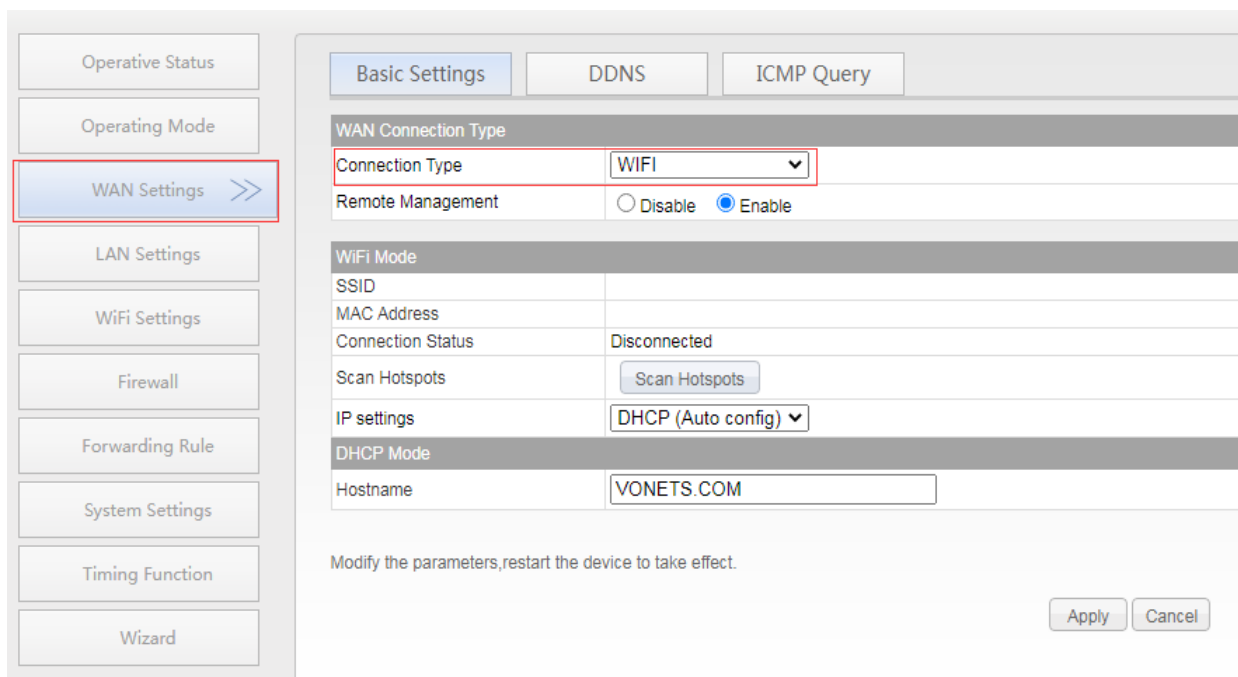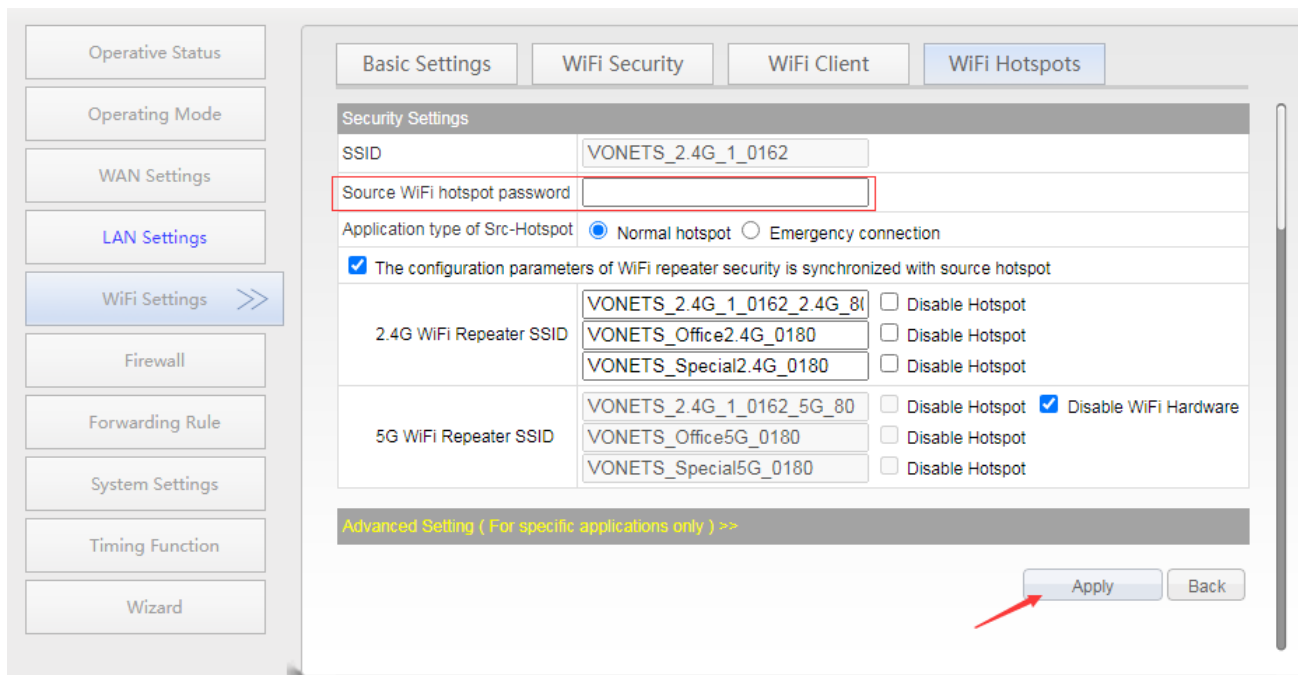

2. Choose the source hotspots, click "Next";

3. Input "Source wireless hotspot password", click "Apply"
   - The option "**The configuration parameters of WiFi repeater security is synchronized with source hotspot**" is default ticked, it means the SSID of VONETS repeater is associated with the SSID of the source hotspot, and the WiFi password is the same as the password of the source hotspot;
   - **Disable hotspot**, if you select "Disable hotspot" on the right side of the SSID, the device will not transmit the corresponding hotspot and can only be used as a bridge application;
   - **Advanced Setting**,include Hot spot authentication match mode, WiFi Signal Motion Detection and SSA Signal strength alarm threshold,these options here can be kept unchanged, for instructions on this option, go to www.vonets.com and download the "V Series WiFi Bridge Advanced Features Instruction";

4. Click "Reboot", VONETS device will connect to the configured WiFi hotspot automatically, if connection is successful, the WiFi LED light will flash quickly;(Please refer to Remark 1 for the description of the LED light.)
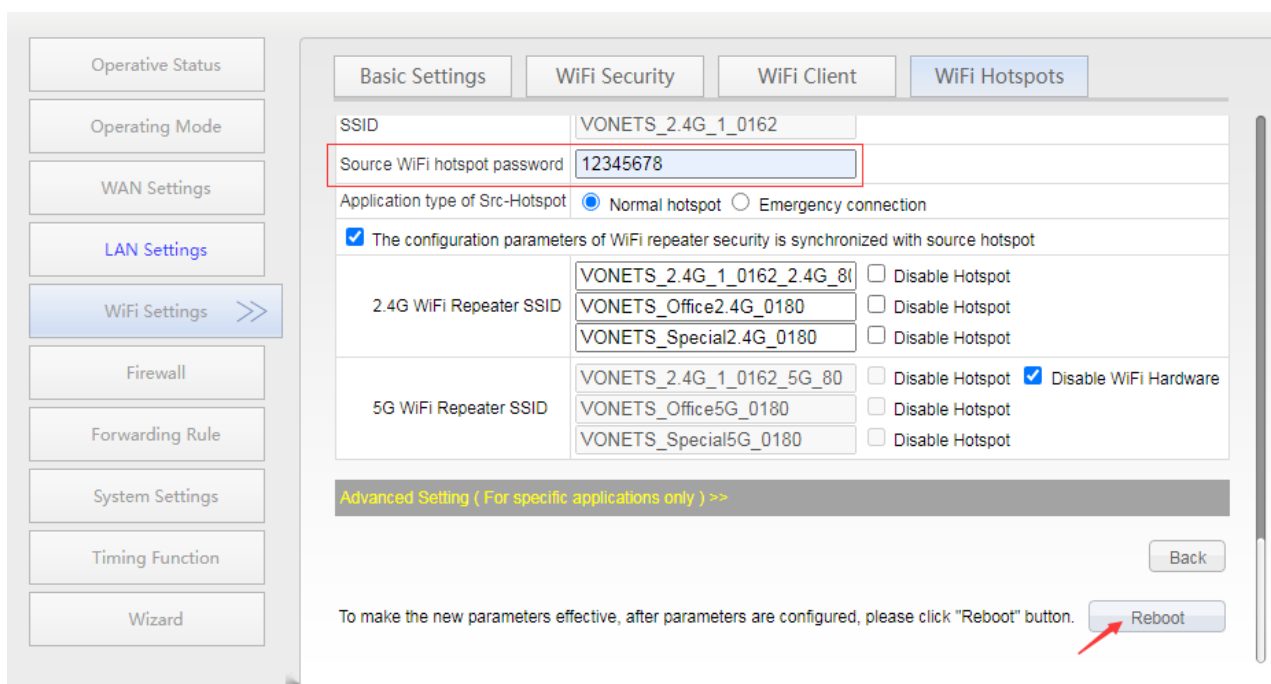
Remark 3: After VONETS device sets the WAN port to access the WiFi hotspot in the routing mode, its LAN port IP is still 192.168.254.254, and the terminal device also obtains the IP address of the same network segment, can login configuration page by 192.168.254.254 or http://vonets.cfg.

3.3 Set WiFi hotspot parameters

1. Change the WIFI name: select "Basic Settings" in "WIFI Settings", enter the new WIFI name in the text box after the SSID, or select the WiFi transmit power according to the actual application scenario, and then click the "Apply" button;
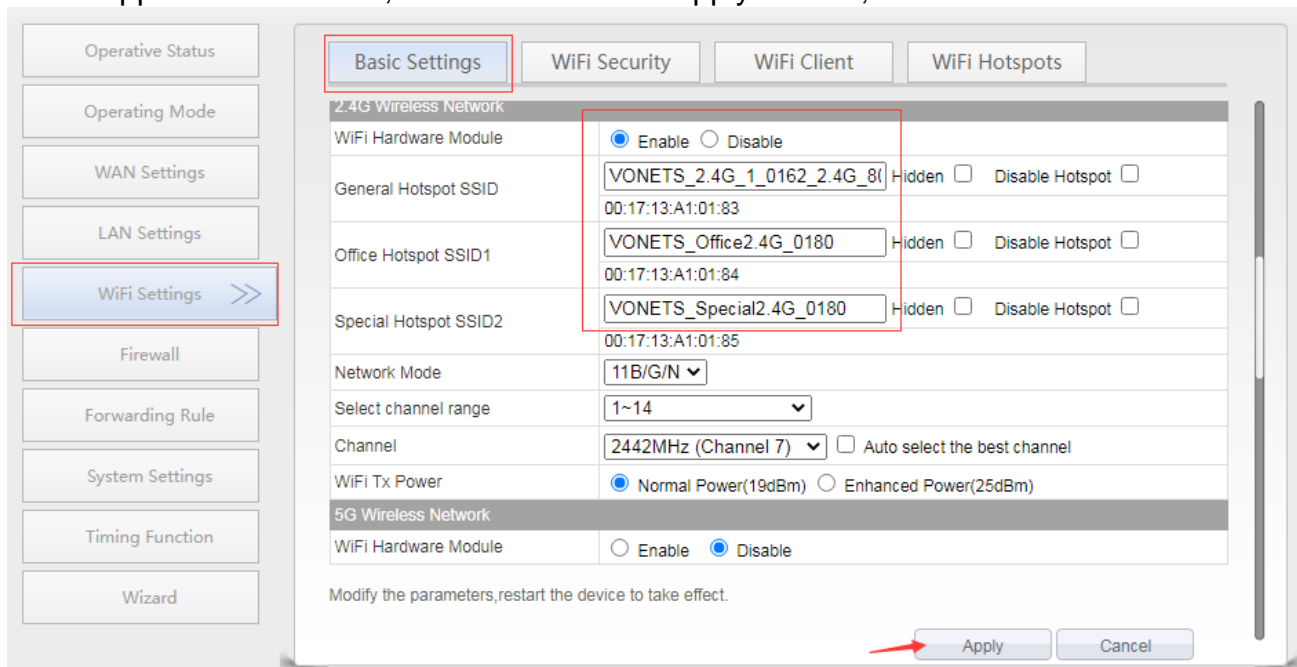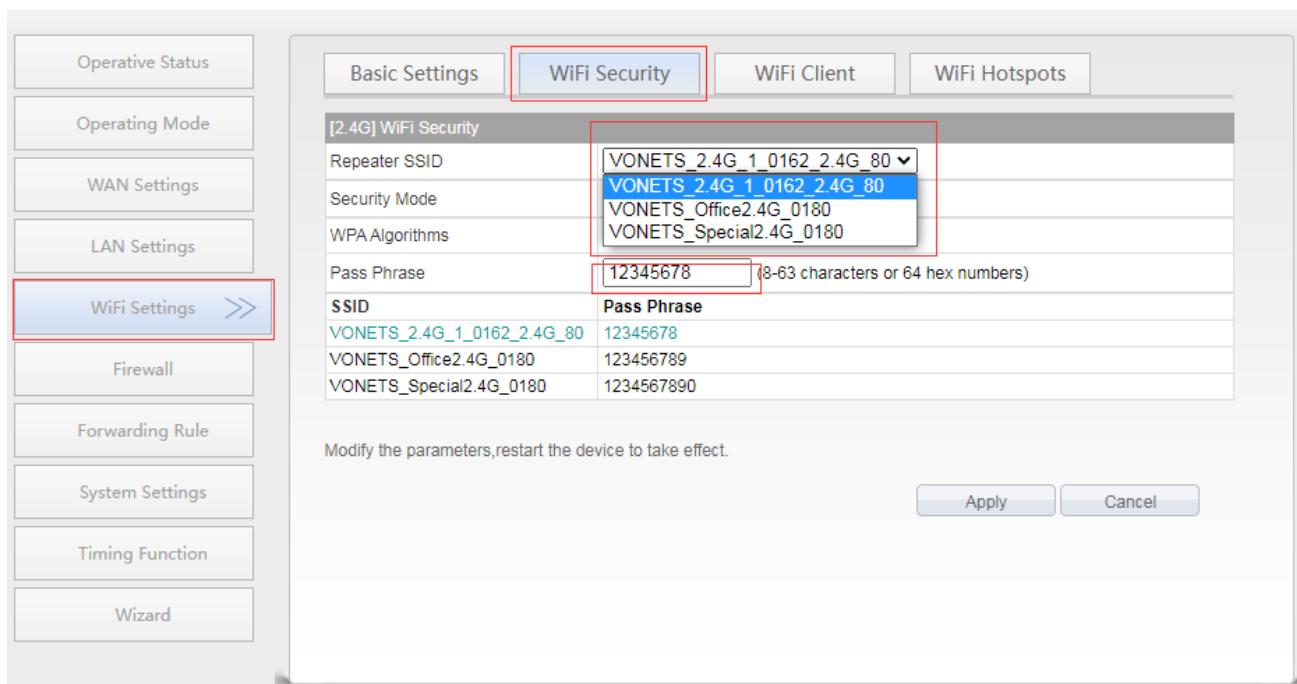

2. Change WIFI password: select "WIFI Security" in "WIFI Settings", enter a new WIFI password in the text box after the key, you can set different passwords for different hotspot names, and then click the "Apply" button;

3. Reboot device, jump to "System Settings"---- "Reboot Device", click "Reboot", when it is finished, all revised options will take effort.

Operative Status	Reboot Device	Advanced Setting	Login Settings	Firmware Upgrade
Operating Mode				
WAN Settings	Reboot Device			
LAN Settings	Reboot Device	Reboot		
WiFi Settings				
Firewall				
Forwarding Rule				
System Settings 》》				
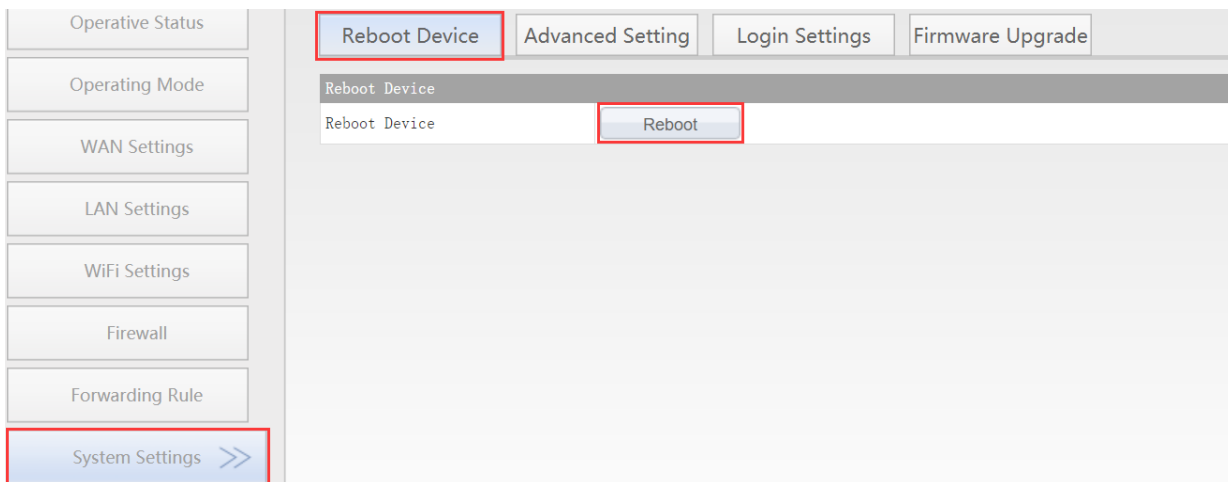
Chapter 4 Other components and installation method

4.1 Other components

1、 Power Adapter (POE option)（48V/1.2A）	2、 Power Adapter (No POE option)（12V/3A）
3、 DC terminal block (Standard Accessories)	4、 2.4G/5G Antenna (-H Series Standard Accessories)

4.2 Industrial chassis rail hook kit installation

1. Snap the VONETS device to the chassis rail

Appendix Frequently Asked Questions

1. How to reset to the factory default parameters?
   Power on the device, after 60 seconds, long press Reset button until 5 seconds, the blue light will flash a few, then the device will automatically reset to the factory default parameters (it will take about 80 seconds to reset the 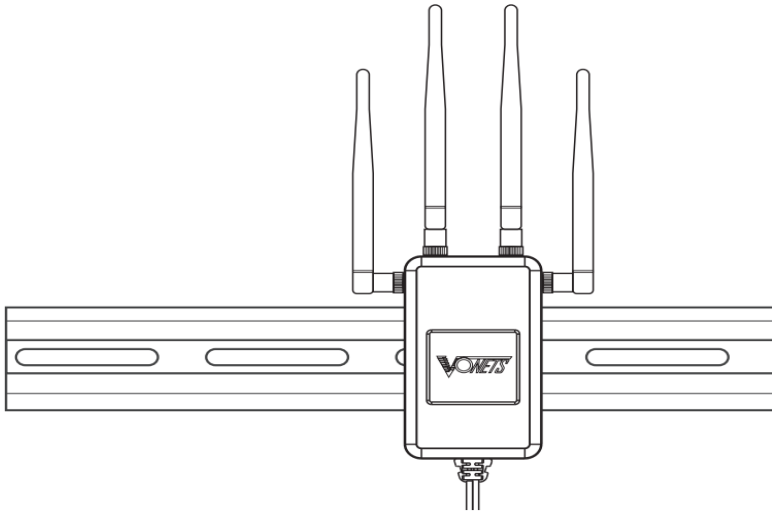device), during the recovery of the factory operation, the product can't be powered off, otherwise it may cause the product to damage.

2. Do VONETS device support firmware upgrade, how to upgrade?
   VONETS devices support firmware upgrade, and support online upgrade, please visit website: www.vonets.com to refer to the related documents

3. The device WiFi hot spot can be found, but the smart phone or PC can't connect to this device hotspot?
   - Reason 1. Due to some unexpected operation or power down, caused the destroy of device parameters. At this time, just need to reset the device to factory default parameters;
   - Reason 2. The device WiFi doesn't work at the best channel, make the performance worse. At this time, you can try to change the source WiFi hot spot and this device WiFi channel to make the performance better;
   - Reason 3. The smart phone or PC haven't configured the correct WiFi password.

4. The device has been configured the source WiFi hot spot parameters, the smart phone

or PC has connected to the device WiFi hot spot, but still doesn't get internet?

- Reason 1. The distance between the device and source WiFi hot spot is too long, cause the communication performance degradation, finally effect the user's access to the Internet. At this time, just need shorten the distance between the device and source WiFi hot spot to solve this problem;

- Reason 2. Due to some unexpected operation or power down, caused the destroy of device parameters. At this time, just need to reset the device to factory default parameters;

- Reason 3. The device WiFi doesn't work at the best channel, make the performance worse. At this time, you can try to change the source WiFi hot spot WiFi channel to make it the same as the default channel of the device, the reboot the device, the device will automatically exchange to the same channel as the source WiFi hotspot, to make the performance better;

- Reason 4. There are several WiFi hot spot around the device, WiFi channel mutual interference, make the performance worse. At this time, you can try to change the source WiFi hot spot and this device WiFi channel to make the performance better;

- Reason 5. The configured source WiFi hot spot parameters are not correct. At this time, just need to configure the correct parameters then reboot.

5. The smart phone or PC has been connected the device by WiFi or Ethernet cable, but user can't log in the device WEB page, or after log in the WEB it shows error?

- Reason 1. The users don't use the browser recommended by VONETS(IE,Google Chrome, Safari, the mobile phone browser);

- Reason 2. The smart phone or PC installed the firewall, the security level is set too high, caused the above problem. At this time, only need to close the firewall;

- Reason 3. The security level of browser is too high, it will also cause the above problem. At this time, just need to reduce the browser's security level, then log in again;

- Reason 4. The IP address of the device input error. For the new device from the factory, user only need input the correct IP address according to the instruction guide; for the device that has connected the source hot spot, user only operate according to <Remark 2>.