

# **VM3G** WiFi Bridge

## Quick Setting Guide

## Declaration

**Copyright © 2014 Shenzhen HouTian Network Communication Technology Co., Ltd**

All rights reserved, with retained ownership

Without Shenzhen HouTian Network Communication Technology Co., Ltd written authorization, any company or personal can't copy, writer or translation part or all contents. Can't do commodity distribution for any commercial or profitable purposes by any ways (electricity, mechanical, photoprint, record or other methods).

**VONETS** is the registered trademark of Shenzhen HouTian Network Communication Technology Co., Ltd. The other all trademarks or registered trademarks mentioned in this documents are belong to the individual owners. The product specifications and information technology mentioned in this manual are just for reference, if any updates, without other notice. Except for special agreements, this manual is just for user guidance, any statements, information and so on in this manual can't constitute the warranty of any forms.

## Chapter 1 Quick Setting Guide of Bridge Mode

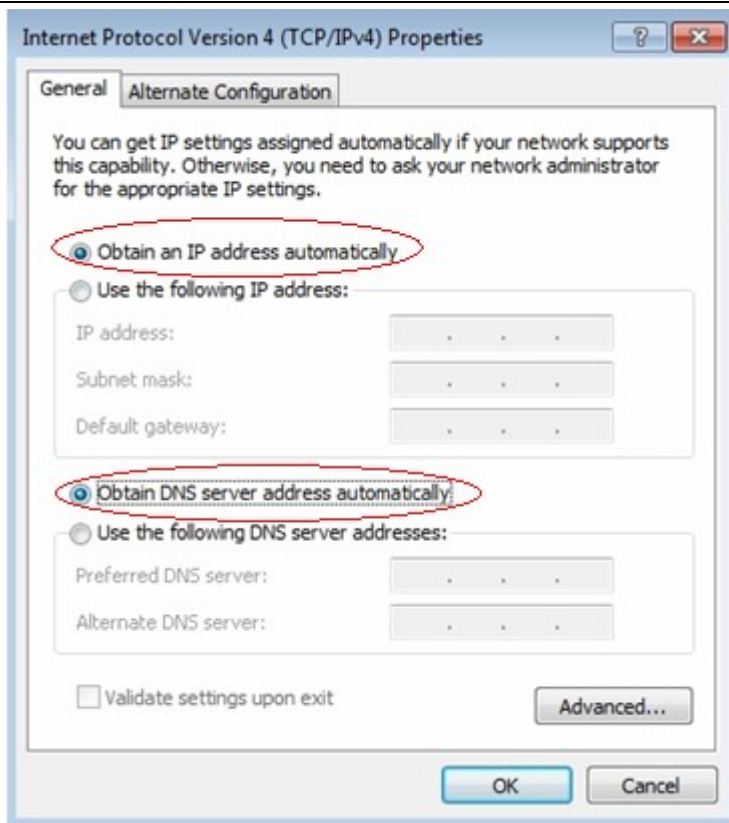
1. Connect USB power of VM3G to USB port.



Open the Wireless connection of the computer, search the device SSID.

**Note:** The SSID of the device is VONETS\_ the last two characters of the MAC of the product.

Set IP address of the computer to automatically, please see the words in the red circle of the following picture:



2. Open the IE browser, enter <http://vonets.cfg> virtual domain name setting (VDNS).



Remark:

Enter domain name, then Enter, the login page will appear, the default admin and password is admin.

### 3. Scan Hotspots

After entering the IE browser, the WiFi hotspots window will appear, can search the WIFI hotspots signal that opened SSID broadcast around, please see the following:

## VONETS—VM3G WiFi Bridge

WiFi Hotspots

Select a Wireless Network to connect to. If not found, please click **Refresh List**, or enter the SSID of the network manually. Then, click **Next**.

SSID	Channel	Signal	Authentication	Encryption	Wifi Mode
ABC	1	96	WPA2-PSK	AES	11b/g/n
VONETS_wxs	1	91	WPA-PSK	TKIP	11b/g/n
ChinaNet-pvby	6	91	WPAPSK-WPA2PSK	AES	11b/g/n
VAR11N_SSID_F0	7	86	WPA-PSK	AES	11b/g/n
VONETS_YF	9	86	WPA-PSK	AES	11b/g/n
houtian@123	10	81	WPA-PSK	TKIP	11b/g
VONETS	1	70	WPA2-PSK	AES	11b/g/n
VONETS_010470	1	70	WPA2-PSK	AES	11b/g/n

there are 26 wireless network

Refresh List

SSID  channel 1  11b/g/n

Next  Exit

- Choose a correct WiFi signal, then click Next, the following interface will appear:

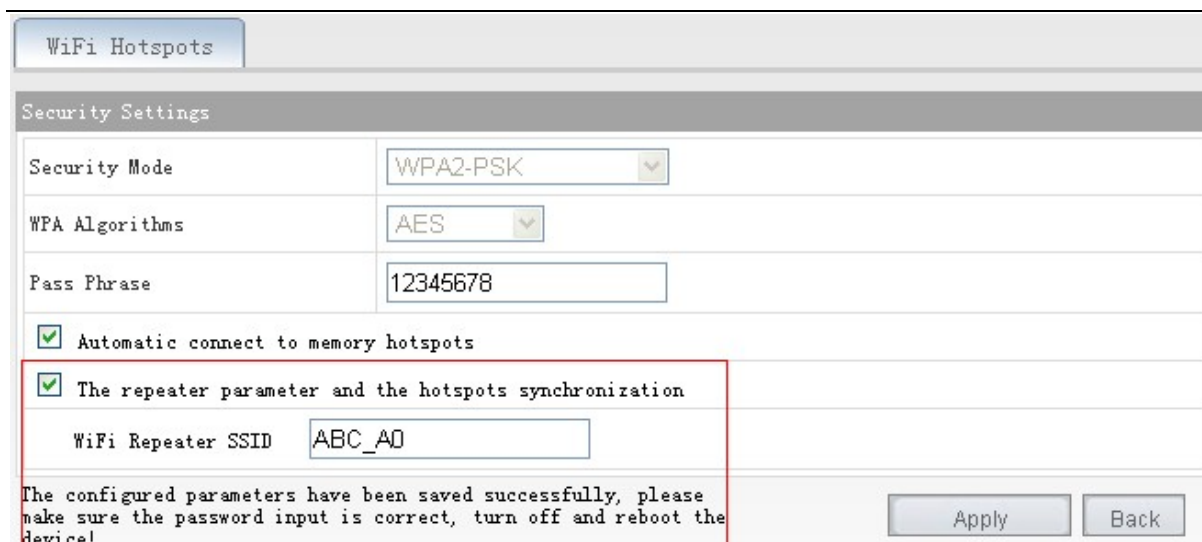
WiFi Hotspots

Security Settings

Security Mode	WPA2-PSK
WPA Algorithms	AES
Pass Phrase	12345678
<input checked="" type="checkbox"/> Automatic connect to memory hotspots	
<input checked="" type="checkbox"/> The repeater parameter and the hotspots synchronization	
WiFi Repeater SSID	ABC_AD

Apply  Back

- Input the correct password, confirm it is correct one, then click Apply button.



- Click Apply button, the above interface will appear, the configured parameters have been saved successfully, please make sure the password input is correct, turn off and reboot the device.

Remark: After configured successfully, the WiFi name of the device is the source hotspot's name add \_the last two characters of the MAC of the product, the password is the same as the source hotspot's parameters, users can go to WiFi Repeater menu to change SSID and password.

#### FCC STATEMENT

1. 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.
  - (2) This device must accept any interference received, including interference that may cause undesired operation.
2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

#### Radiation Exposure Statement:

This equipment complies with FCC radiation exposure requirement. The device can be used in portable exposure condition without RF striction

The module must not be modified in any way. Coupling of external circuitry must not bypass the provided connectors. End product must be externally labeled with “Contains FCC ID: 2AARM-VM3G” The integrator must not provide any information to the end-user on how to install or remove the module form the end-product.

This radio module should not be installed and operating simultaneously with other radio.