

Tozed Kangwei Tech Co., Ltd

VL7M19K

USER MANUAL



Table of Contents

1. Getting Started.....	1
1.1. Power on.....	1
1.2. Connect.....	1
(1) Connect via LAN.....	1
(2) Connect via Wi-Fi	1
1.3. Access the Web Admin Panel.....	1
(1) Language Setting.....	2
(2) Admin Password Setting	2
(3) Bootstrap page	3
(4) Admin Panel.....	3
2. INTERNET	4
2.1. Wired Network Mode.....	4
(1) DHCP	6
(2) Static	6
(3) PPPoE Mode	7
(4) Bridge Mode	7
2.2. Repeater.....	8
(1) 2.4 GHz Wi-Fi Mode	8
(2) 5 GHz Wi-Fi Mode.....	9
(3) 6 GHz Wi-Fi Mode.....	9
3. WIRELESS	9
3.1. Wi-Fi Setting	9
4. CLIENTS.....	11
5. UPGRADE.....	11
6. FIREWALL	12
6.1. DMZ.....	12
6.2. Port Forwards.....	13
6.3. IP MAC Binding.....	14
6.4. URL Filters.....	14
6.4.1. function	14
6.4.2. Add rules.....	14
6.5. Access Control.....	15
7. VPN	15
7.1. OpenVPN.....	15
7.1.1. OpenVPN Client.....	16
(1) Upload your OpenVPN configuration file.....	16
(2) Enter Description, Username and Password	16
(3) Connect to the OpenVPN server	16
(4) Manage configuration files.....	16
7.1.2. OpenVPN Server	17
(1) Server configuration.....	17
(2) Export OpenVPN configuration file	17
(3) Start the OpenVPN server.....	17
7.2. WireGuard	18
(1) Server configuration.....	18
(2) Start the WireGuard server	18
7.3. VPN Configuration	19
7.3.1. VPN L2TP Mode	19

(1) Configuration.....	19
(2) Connect to the VPN server.....	20
7.3.2. VPN PPTP.....	20
(1) configuration.....	20
(2) Connect to the VPN server.....	20
8. APPLICATIONS	21
8.1. Package Management.....	21
8.2. ZeroTier.....	21
8.3. Network Storage	23
8.4. LuCI Page	24
8.5. AdGuard Home.....	24
9. MORE SETTINGS	25
9.1. Revert Firmware	25
9.2. LAN IP	25
9.3. Time Zone.....	25
9.4. Network Mode.....	26
10. Trouble shooting.....	26
10.1. LED Indicators.....	26
10.2. Reset.....	28
10.3. RESTART	28
10.4. WPS.....	28
10.5. Access Web Panel	28
11. Parental Control.....	29
11.1 Parent Mode.....	29
11.2 QOS.....	29
(1) Speed Limit.....	29
(2) High priority	30
12. LOG	30
12.1 User LOG.....	30
12.2 Export LOG	30
13 FCC Statement.....	31

1. Getting Started

Model: VL7M19K

1.1. Power on

Plug the power cable into the power port of the router. Make sure you are using a standard **12V/3A** power adapter. Otherwise, it may cause malfunction.

1.2. Connect

You can connect to the router via Ethernet cable or Wi-Fi.

Note: *This step only connects your devices to the local area network (LAN) of the router. You cannot access the Internet currently. In order to connect to the Internet, please finish the setup procedures below and then follow Internet to setup an Internet connection.*

(1) Connect via LAN

Connect your device to the LAN port of the router via Ethernet cable.

(2) Connect via Wi-Fi

Search for the SSID of the router in your device and input the default password: admin.

Note: *The SSID was printed on the side label of the router with the following formats:*

- **VL7M19K-2.4G-XXX**
- **VL7M19K-5G-XXX**
- **VL7M19K-6G-XXX**

1.3. Access the Web Admin Panel

Open a web browser (we recommend Chrome, firefox) and visit

http://192.168.0.1. You will be directed to the initial setup of the web Admin Panel.

(1) Language Setting

You need to choose the display language of the Admin Panel. Currently, our routers support English, 简体中文, 繁體中文, Français, Español and 日本語, русский, etc.



(2) Admin Password Setting

There is no default password for the Admin Panel. You have to set your own password, which must be at least 8 characters long. Then, click Submit to proceed.





Note: This password is for this web Admin Panel. It will not change your Wi-Fi password.

(3) Bootstrap page

You can set the WIFI country code and time zone according to your country or region on the navigation page.

Set Up Wi-Fi

Complete

2.4G Wi-Fi

SSID: WIRELESS-XXXXXX

Security Key: 1234567890123456

Wi-Fi Country Code: CN

5G Wi-Fi

SSID: WIRELESS-XXXXXX_5G

Security Key: 1234567890123456

5G Wi-Fi

SSID: WIRELESS-XXXXXX_5G

Security Key: 1234567890123456

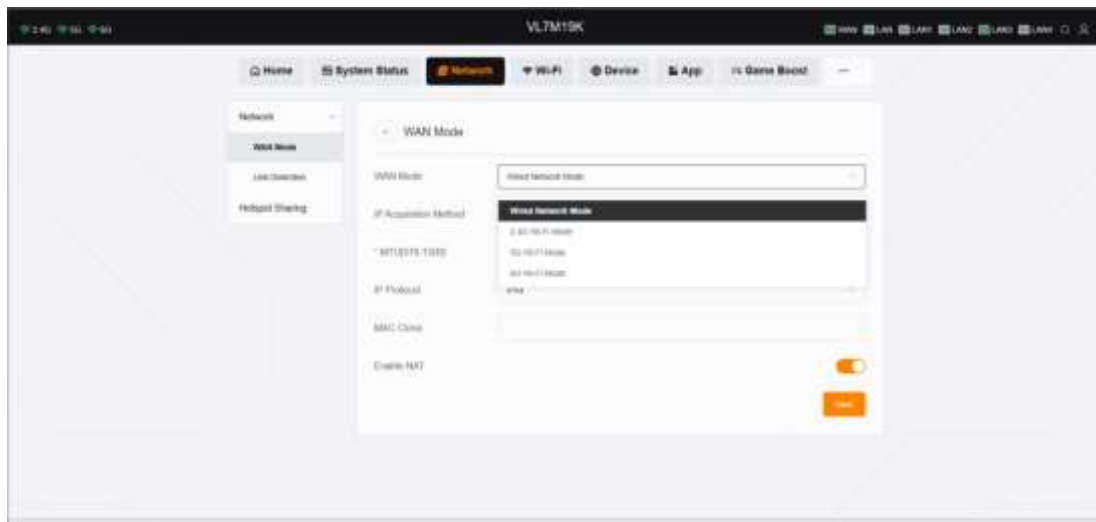
Time Settings

Time Zone: UTC+8

Exit Next Step

(4) Admin Panel

After the initial setup, you will enter the web Admin Panel of the router. It allows you to check the status and manage the settings of the router.

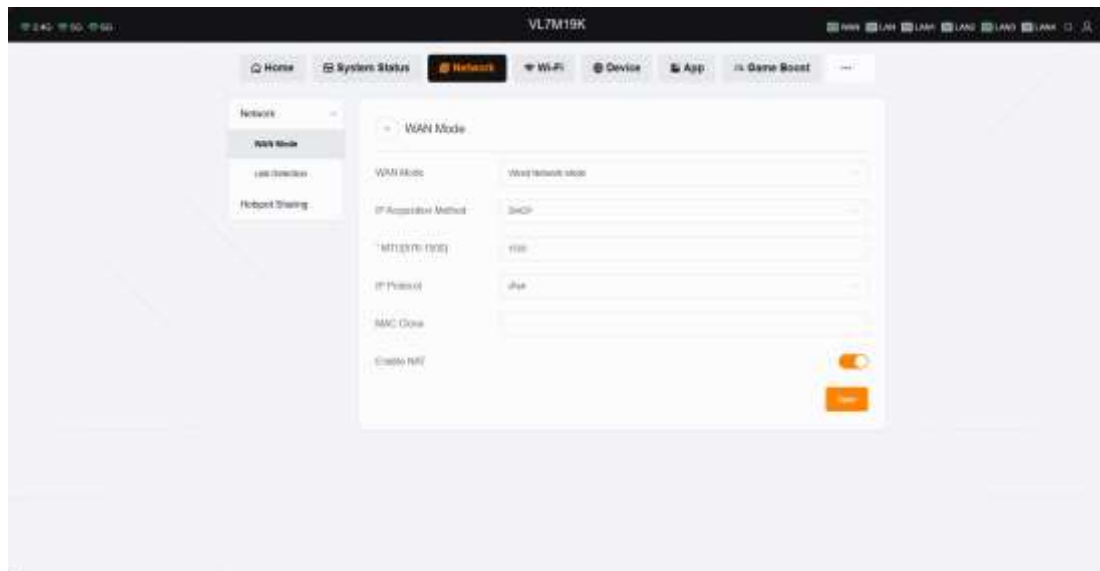


2. INTERNET

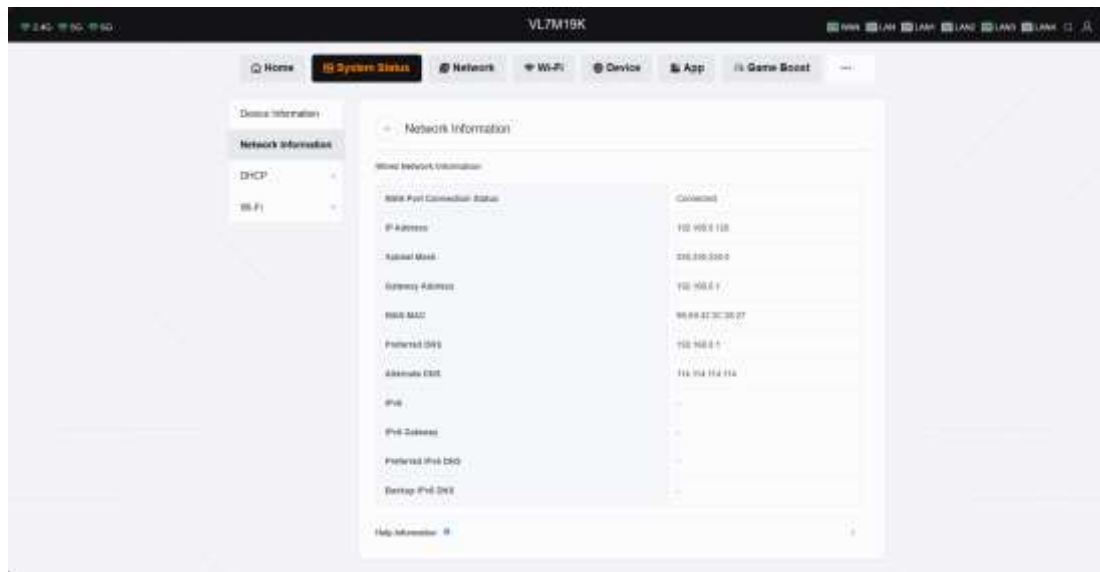
There are total 2 types of connection method that you can use to access the Internet: Wired Network Mode, Repeater(2.4 GHz Wi-Fi Mode, 5 GHz Wi-Fi Mode and 6 GHz Wi-Fi Mode).

2.1. Wired Network Mode

Connect the router to the modem or main router via Ethernet cable to access the Internet.

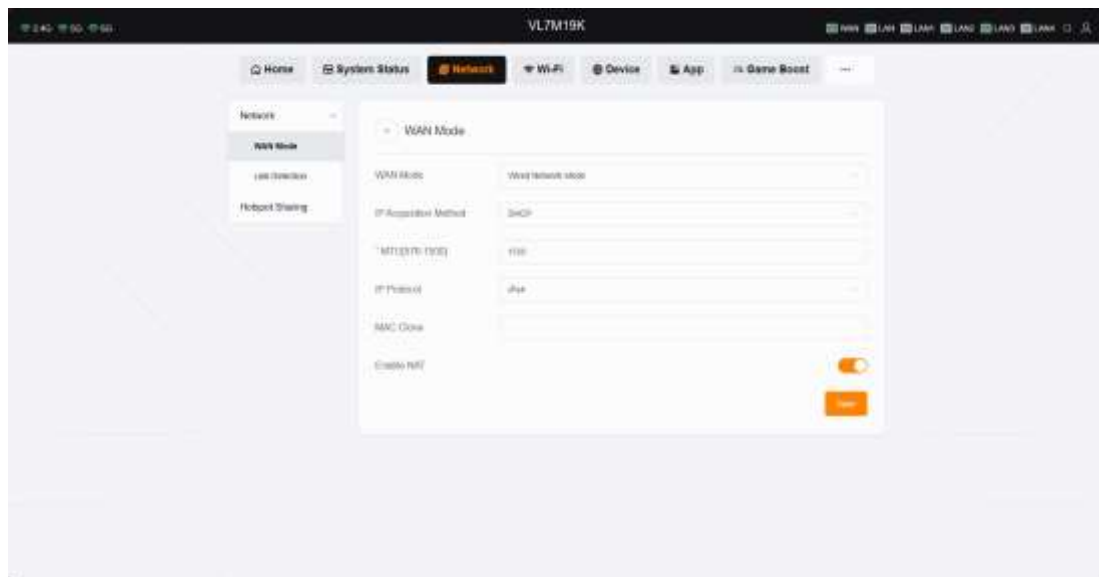


Plug the Ethernet cable into the WAN port of the router. The information of your connection will be shown on the System Status section. DHCP is the default protocol. You can change the protocol in the Network section.



(1) DHCP

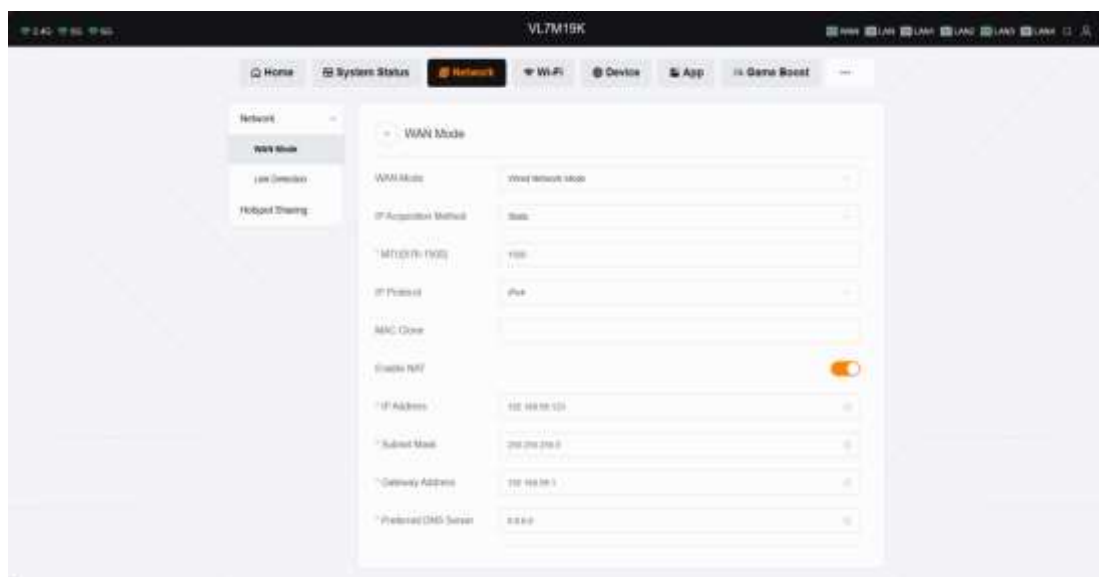
DHCP is the default and most common protocol. It doesn't require any manual configuration.



(2) Static

Static is required if your Internet Service Provider (ISP) has provided a fixed IP address for you or you want to configure the network information such as IP address, Gateway, Netmask manually.

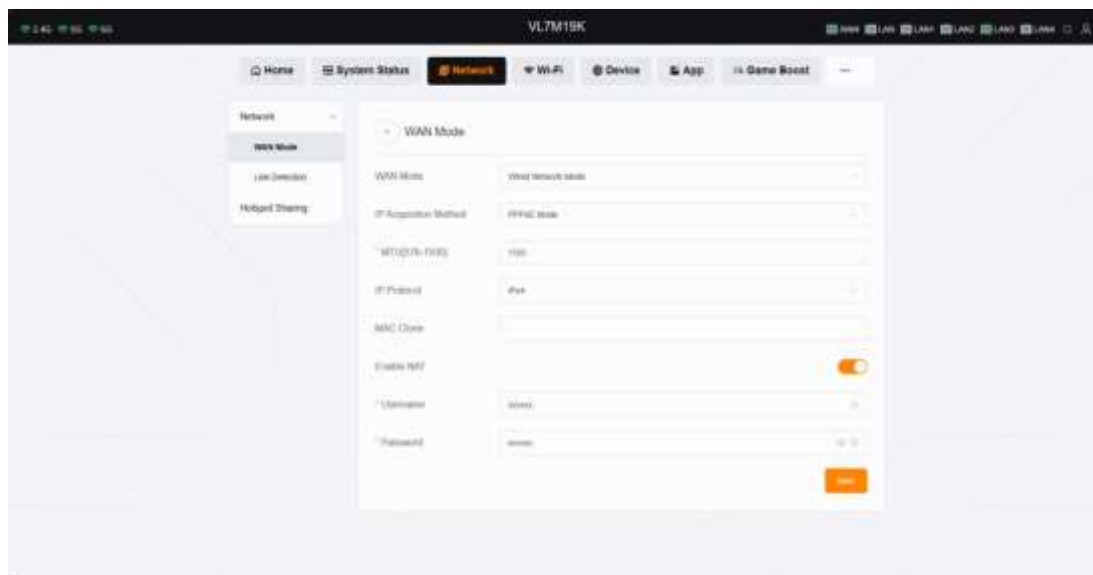
The current settings will be change once you choose Static. Change it according to your needs and then click Save.



(3) PPPoE Mode

PPPoE is required by many Internet Service Providers (ISP). Generally, your ISP will give you a modem and provide you a username & password that you needed when you are creating the Internet connection.

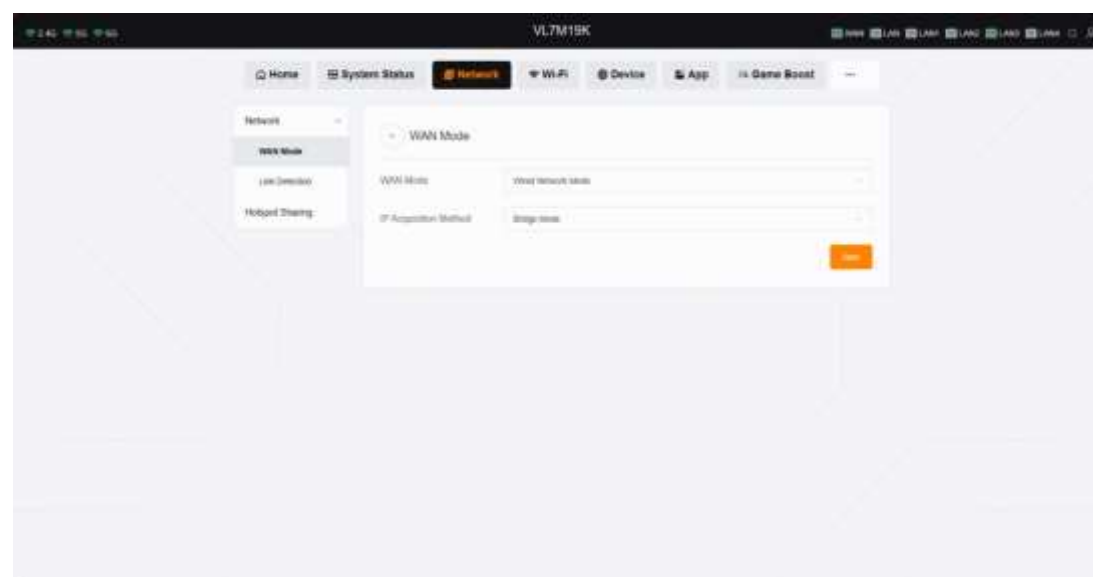
Under PPPoE protocol, enter your username and password, then click Save.



(4) Bridge Mode

Bridge Mode can achieve network expansion. In this mode, the secondary router acts as an extension of the primary router's network, enhancing the signal coverage area, and enabling stable and high-speed interconnection between different devices.

Under Bridge Mode, you only need to click **Save**.



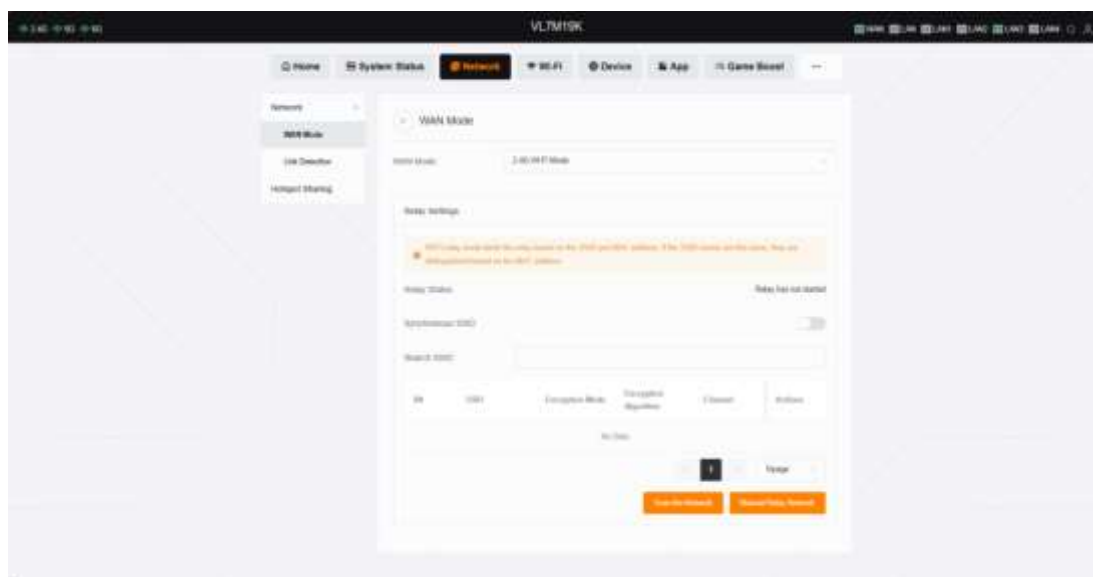
2.2. Repeater

Using Repeater means connecting the router to another existing wireless network, e.g. when you are using free Wi-Fi in a hotel or cafe.

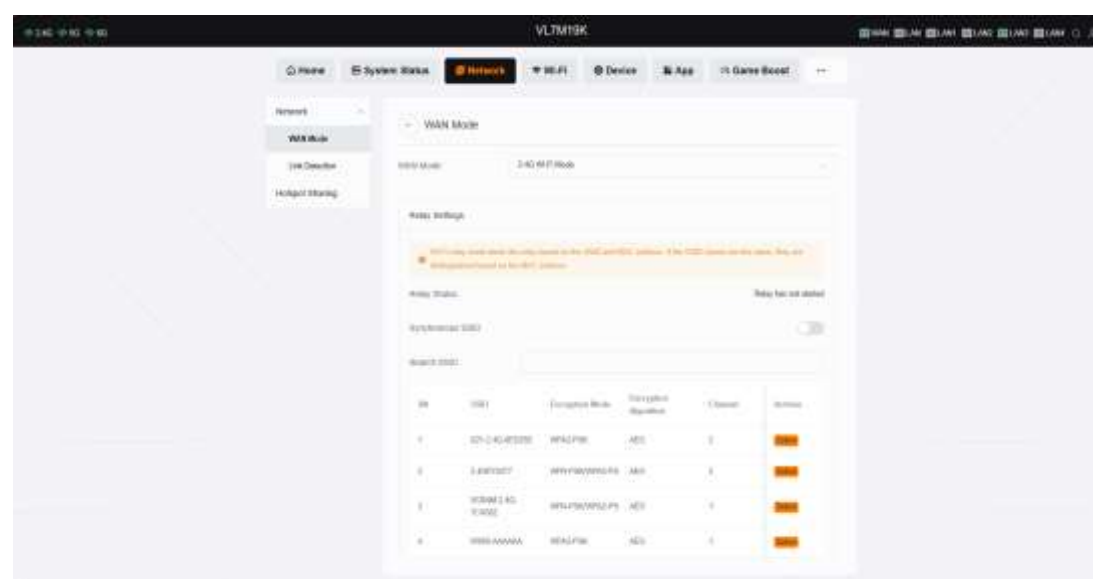
It works in WISP (Wireless Internet Service Provider) mode by default, which means that the router will create its own subnet and act as a firewall to protect you from the public network.

(I) 2.4 GHz Wi-Fi Mode

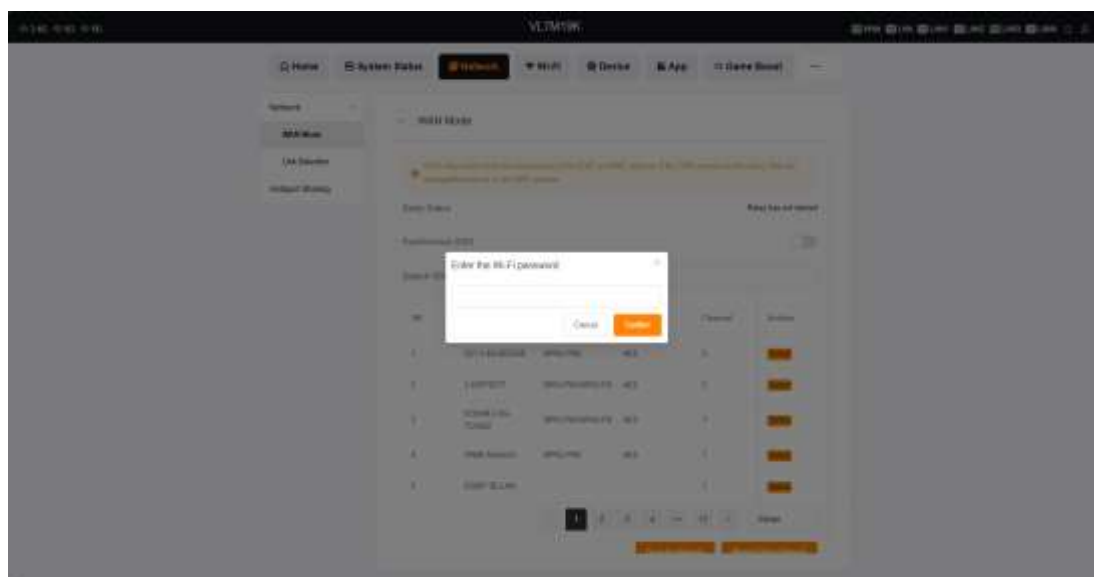
In Network section, choose 2.4 GHz Wi-Fi Mode and click Save.



Click Scan the Network to search for the available wireless networks nearby.



Choose a SSID from the list and enter its password. Finally, click Confirm.



(2) 5 GHz Wi-Fi Mode

Refer to the operation steps for the 2.4 GHz Wi-Fi Mode bridging mode.

(3) 6 GHz Wi-Fi Mode

Refer to the operation steps for the 2.4 GHz Wi-Fi Mode bridging mode.

3. WIRELESS

3.1. Wi-Fi Setting

In Wi-Fi section, you can change the settings of the wireless network created by the router. The wireless network can be turned on or off by switching the ON/OFF button.

Wi-Fi Name (SSID): The name of the Wi-Fi. It is not suggested to use Unicode characters such as Chinese.

Wi-Fi Security: The encryption method of the Wi-Fi.

Wi-Fi Key: The password of the Wi-Fi, which must be at least 6 characters long. We suggest you to change it when you receive the router.

SSID Visibility: Show/hide the Wi-Fi SSID.

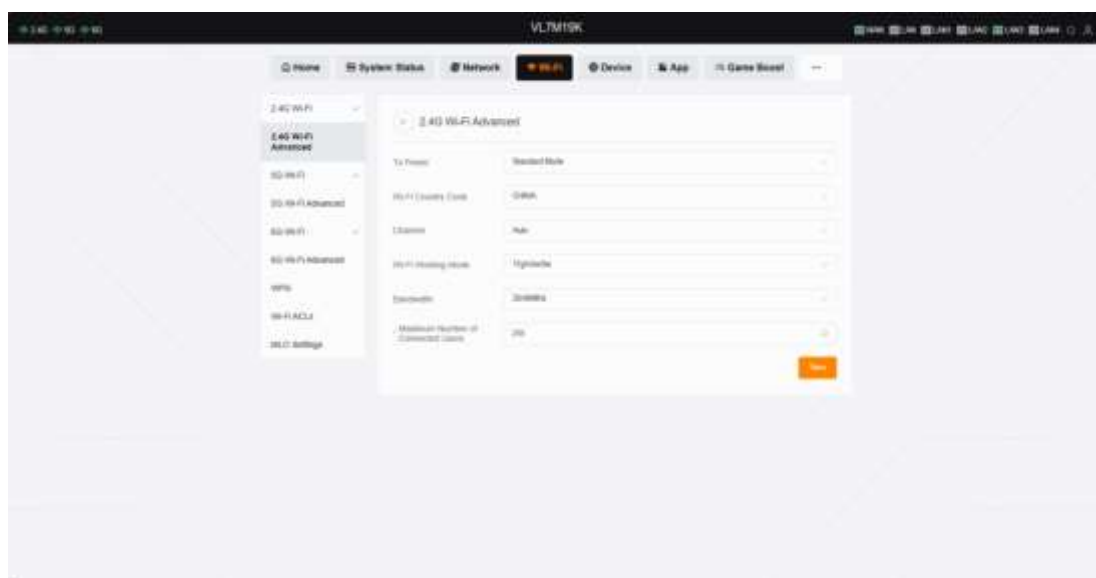
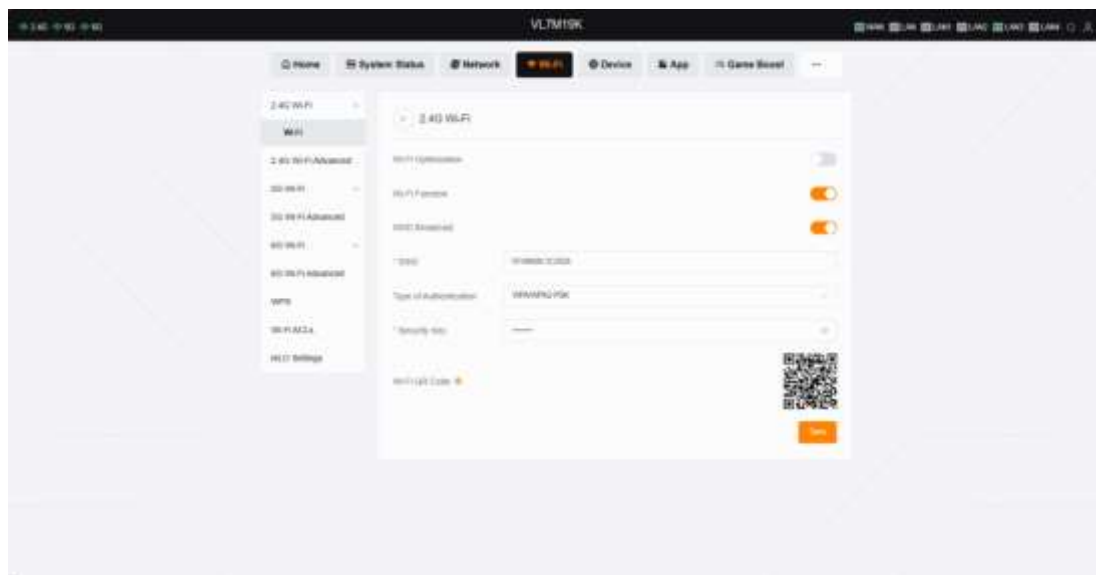
Wi-Fi Mode: The protocol of the Wi-Fi. It is suggested to use default settings (2.4 GHz is b/g/n/ax/be, 5 GHz is a/n/ac/ax/be).

Bandwidth: The channel frequency coverage range of the Wi-Fi. It is suggested to use default parameter.

Channel: The router will choose the best channel itself. You also can choose a channel manually. If your router is used as a Wi-Fi repeater, the channel will be fixed according to the connected wireless network.

TX Power (dBm): It specifies the signal strength.

Wi-Fi Optimization: It will optimize your Wi-Fi signal and channel according to the Wi-Fi environment.



Click Save to change the settings of the wireless network.

3.2. MLO

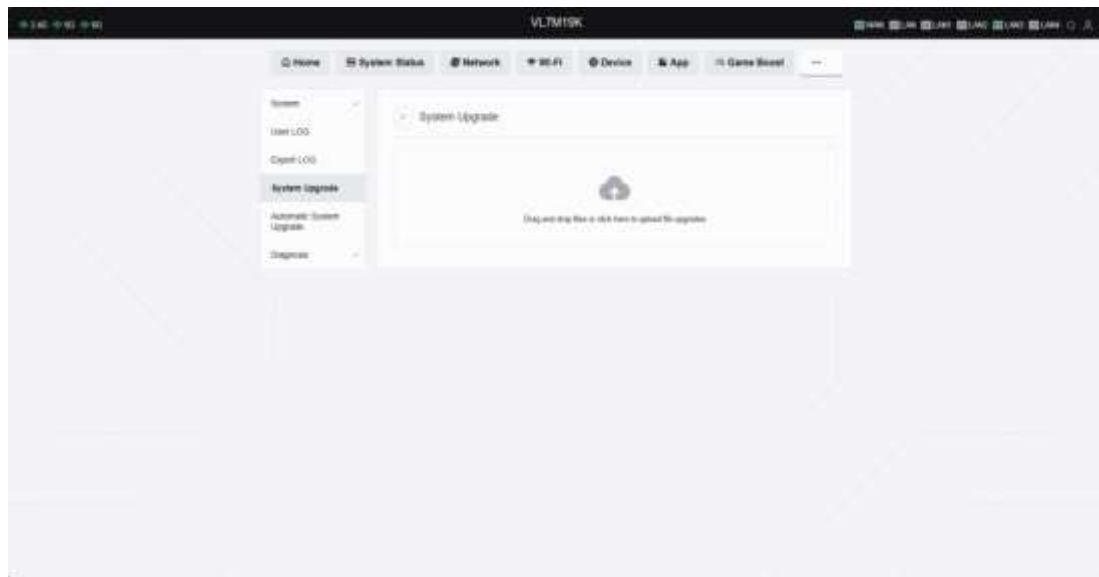
MLO (Multi-Link Operation) is a dark technology in Wi-Fi 7, the latest generation of wireless networking technology. The function is to allow devices

You can see all connected clients in homepage.

You can see their name, IP, MAC address and connection type.



Click **System Upgrade** to upload a firmware file to the router. Simply drag and drop your firmware file to the area indicated.



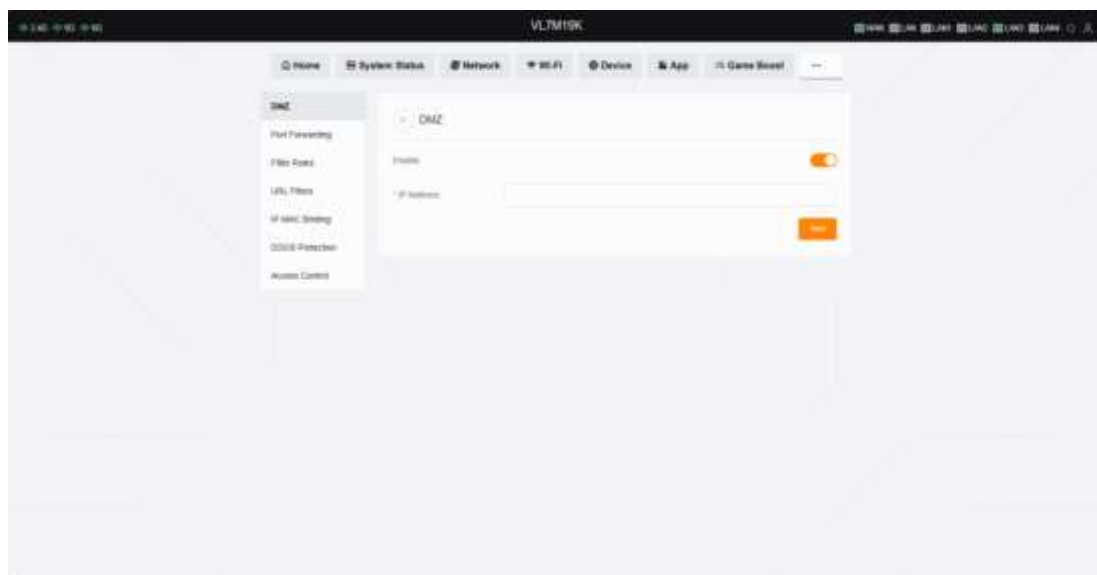
6. FIREWALL

In FIREWALL, you can set up firewall rules like **DMZ**, **Port Forwarding**, **Filter Rules**, **URL Filters**, **IP MAC Binding**, **DDOS Protection**.

6.1. DMZ

DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set.

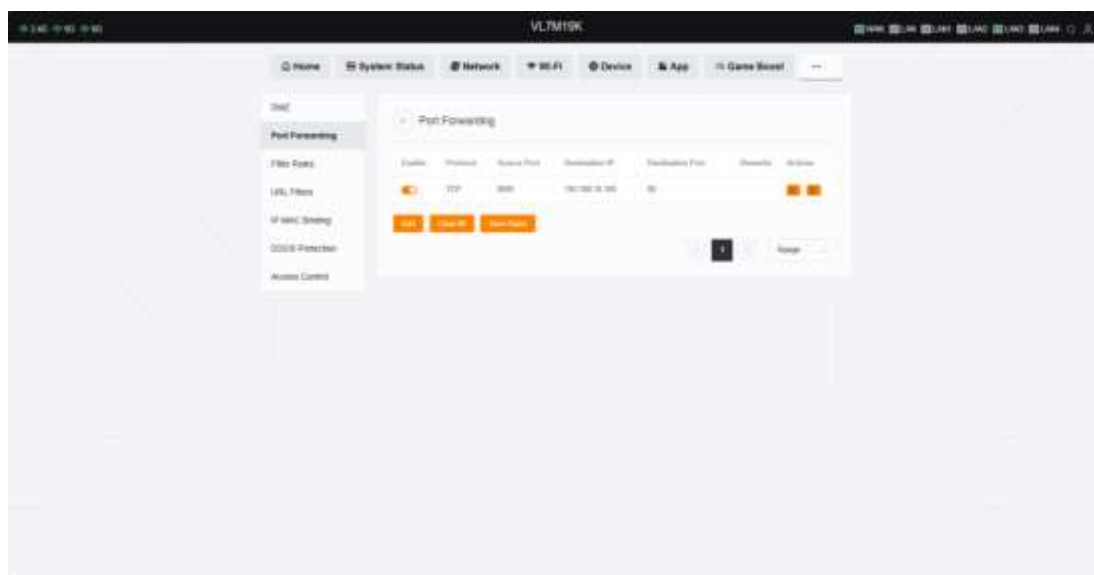
Click DMZ and enable Open DMZ.



6.2. Port Forwards

Port Forwarding allows remote computers to connect to a specific computer or service behind the firewall in the local LAN (such as web servers, FTP servers, etc).

To set up port forwarding, click Port Forwarding and click Add.



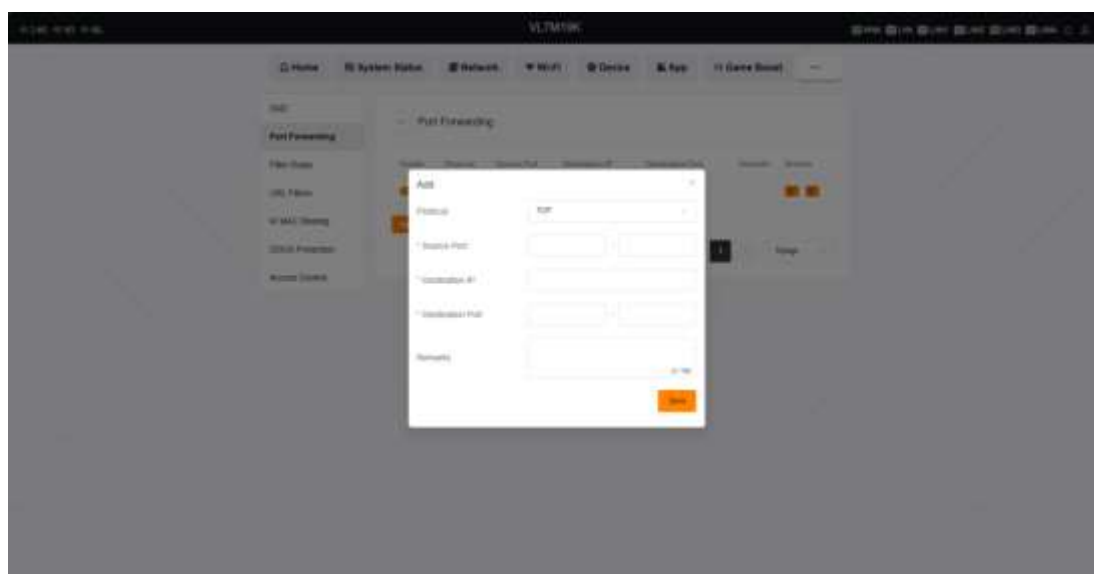
Protocol: The protocol used, you can choose TCP, UDP, or both TCP and UDP.

Source Port: The internal port number of the device. You can enter a specific port number. Leave it blank if it is same as the external port.

Destination IP: The IP address represents the IP assigned by the router to the device that needs remote access.

Destination Port: The numbers of external ports. You can enter a specific port number or a range of service ports (E.g 100-300).

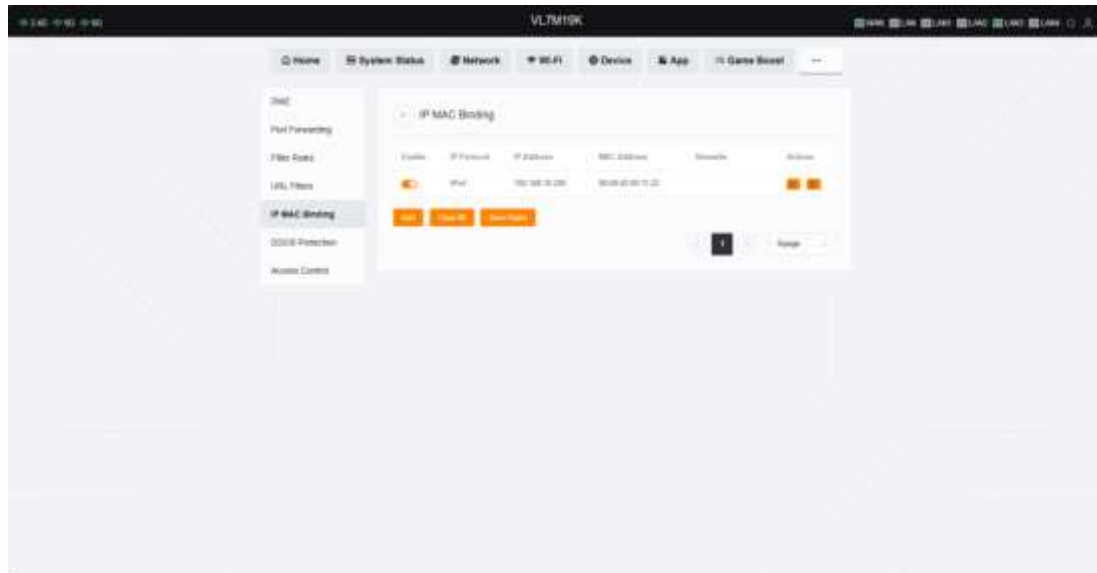
Remarks: You can comment on the port forwarding rule.



The router's services, such as web, FTP and soon, require their respective ports to be opened on the router in order to be publicly reachable.

6.3. IP MAC Binding

Statically bind the MAC address (unique hardware identifier) of a specific device to a specified IP address.



6.4. URL Filters

The URL Filter feature of routers is a technology that restricts devices from accessing specific websites based on the URL or domain name.

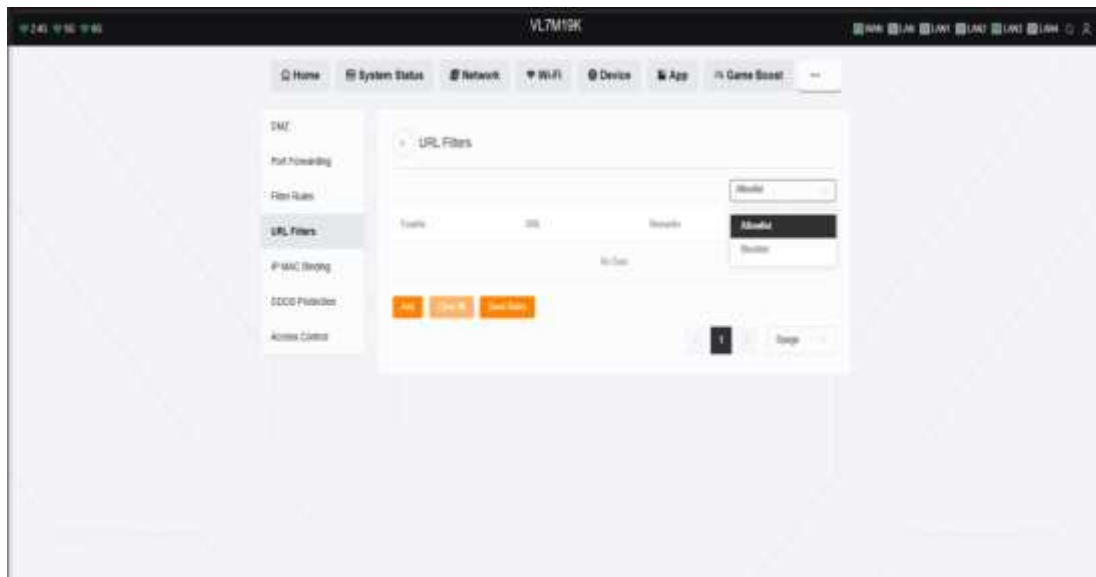
6.4.1. function

It is commonly used for content control, network security or bandwidth management. Block or allow access to specific web pages by analyzing URLs or domain names in HTTP/HTTPS requests.

6.4.2. Add rules

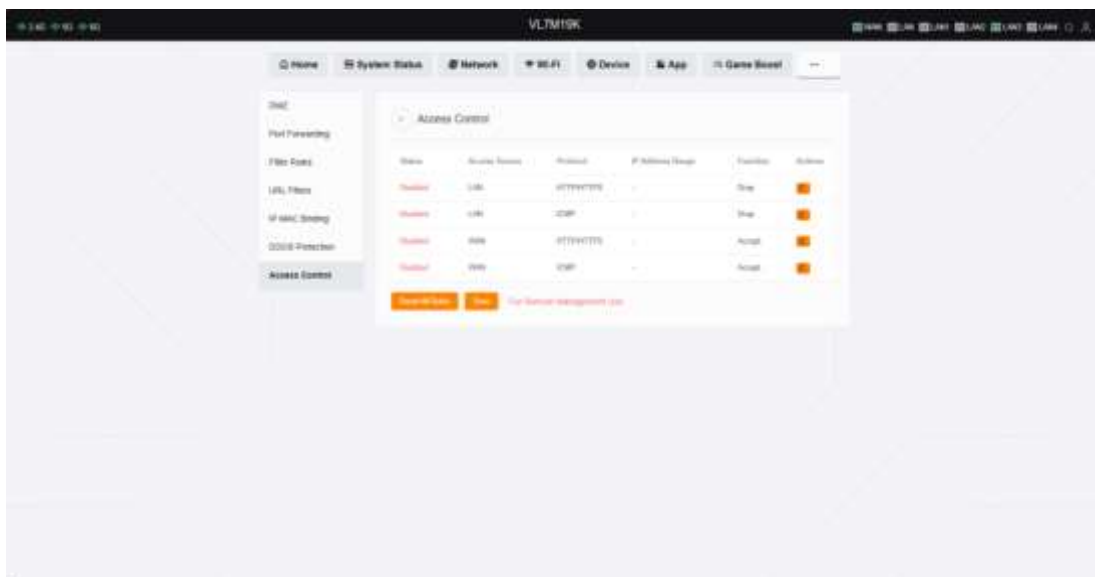
Blacklist mode: Enter the URL or keyword you want to block (such as twitter.com).

Whitelist mode: Only URLs in the list are allowed to be accessed (e.g., the corporate intranet is only open to office websites).



6.5. Access Control

The Access Control feature of a router is a network security mechanism that manages a device's access to network resources. This feature allows administrators to restrict or allow specific devices, users, or applications to access the local area network (LAN) or the Internet (WAN), thereby improving network security and resource utilization.



7. VPN

VL7M19K routers have pre-installed VPN server and client in OpenVPN and WireGuard.

7.1. OpenVPN

VL7M19K routers have pre-installed OpenVPN server and client.

7.1.1. OpenVPN Client

OpenVPN client requires OpenVPN configuration file (.ovpn) to create the OpenVPN connection. If you have your own VPN service provider but you don't know how to get the configuration file, please refer to [Get your configuration file](#). Click + Add a New VPN Configuration to upload the configuration file.

(1) Upload your OpenVPN configuration file

Simply drag and drop your file to the pop up windows. It can be a single .ovpn file or a zip/tar.gz file which contains multiple .ovpn files.

Be careful that some .ovpn files use separated ca, cert, crl files. These files must be zipped together with the .ovpn file before upload.

(2) Enter Description, Username and Password

Enter a description for your OpenVPN configuration file and then click Submit to finish the upload process. In some cases, it will ask you to enter your username and password.

(3) Connect to the OpenVPN server

You can now click Connect to start the OpenVPN connection.

If your configuration file is an archive file, like .zip, you can switch server at the cog icon.

Once connected, you should find your IP address, data received/sent.

Note: It can't running VPN Client and Server at the same time, and also can't running OpenVPN Client and WireGuard Client at the same time.

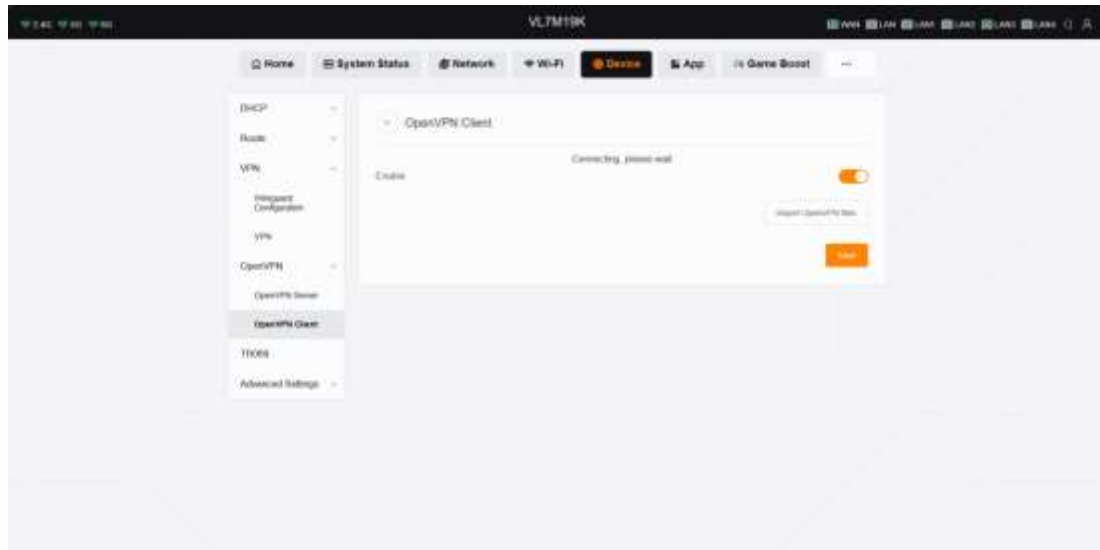
(4) Manage configuration files

Click Management to check the list of configuration files. You can modify the Description, User name or Password of each configuration file. You can also add, delete a configuration file or even purge all your uploaded configuration files.

If your configuration file is a zip/tar.gz file which includes multiple ovpn files, you can choose an individual .ovpn file that you would like to connect in Server.

Get your configuration file.

We have tested different VPN service providers. Therefore, if you don't know how to get the configuration file, you can follow the instruction below. However, you have to contact your service provider for the configuration file if they are not listed below.



7.1.2. OpenVPN Server

You can set up an OpenVPN server on VL7M19K router. Click + Generate a configuration file.

(1) Server configuration

There are preset OpenVPN server configurations. You can also click Modify to change them manually. Click Apply when you finish.

Allow Access Local Network: Enable this will allow every client that connect to this OpenVPN Server be able to access your LAN. Please use with caution.

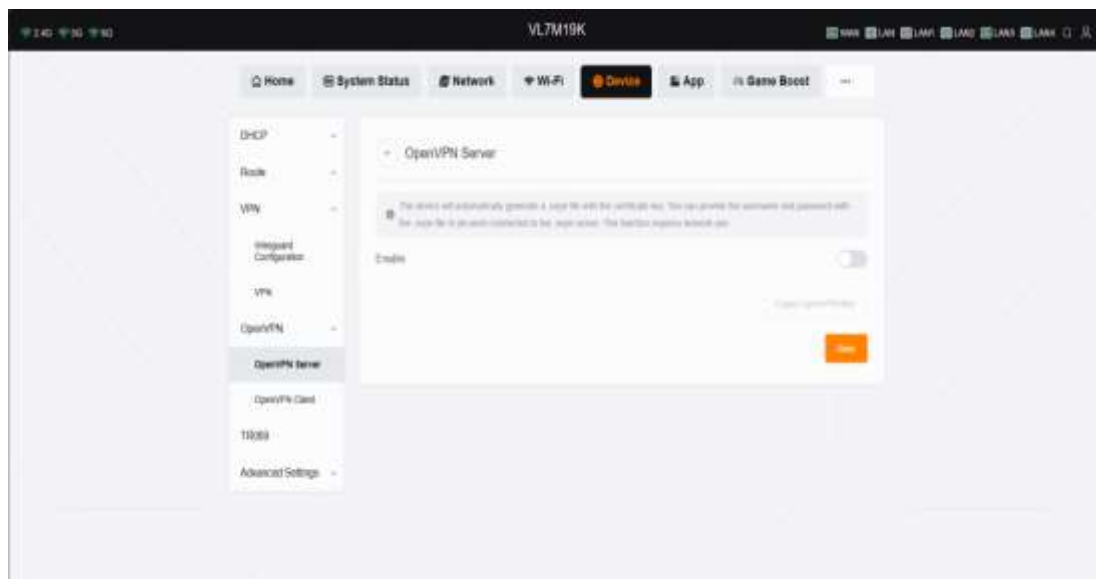
Note that you can't running VPN Client and Server at the same time, and also can't running OpenVPN Client and WireGuard Client at the same time.

(2) Export OpenVPN configuration file

Click Export Config to download the OpenVPN configuration file which you need to upload when you are configuring your OpenVPN client.

(3) Start the OpenVPN server

Click Start to start your OpenVPN server. Otherwise, you will not be able to connect to the OpenVPN server by using its configuration file.



7.2. WireGuard

You can set up a WireGuard server on your VL7M19K router. Here are the steps on how to configure and start a WireGuard server.

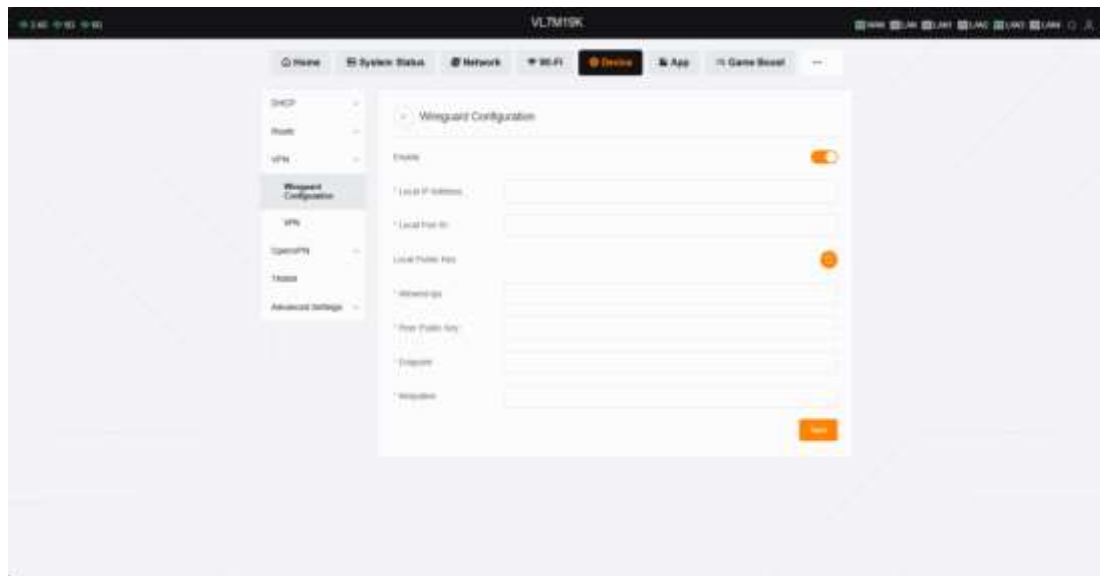
(1) Server configuration

1. In the "Local IP Address" field, enter the server's internal network IP address.
2. In the Local Port ID field, enter the port number of the server monitoring.
3. In the "Local Public Key" field, if the public key does not exist, click the button to generate the public key of the server. This is the server's authentication key and is used to establish a secure connection with the client.
4. In the Allowed-ips field, enter the IP address range that the client is allowed to access.
5. In the "Peer-to-End Public Key" field, enter the public key of the client. This is the client's authentication key that is used to establish a secure connection with the server.
6. In the "Endpoint" field, enter the public IP address and port of the client connecting to the server.
7. In the "Keepalive" field, enter the time interval (in seconds) to keep the connection active. For example: 25.

(2) Start the WireGuard server

Click Start to start your WireGuard server. Otherwise, you will not be able to connect to the WireGuard server by using its configuration file.

To check if the WireGuard server is working properly, the easiest way is to use a phone with the official WireGuard client app installed, turn off its Wi-Fi connection, and connect to the internet only via 3G/4G/5G. Then open the WireGuard app and import the WireGuard configuration from the QR code. Enable the connection to check if your phone has internet access and if its IP address is the IP address of the WireGuard server.



7.3. VPN Configuration

The VL7M19K router's VPN configuration supports two modes: L2TP and PPTP.

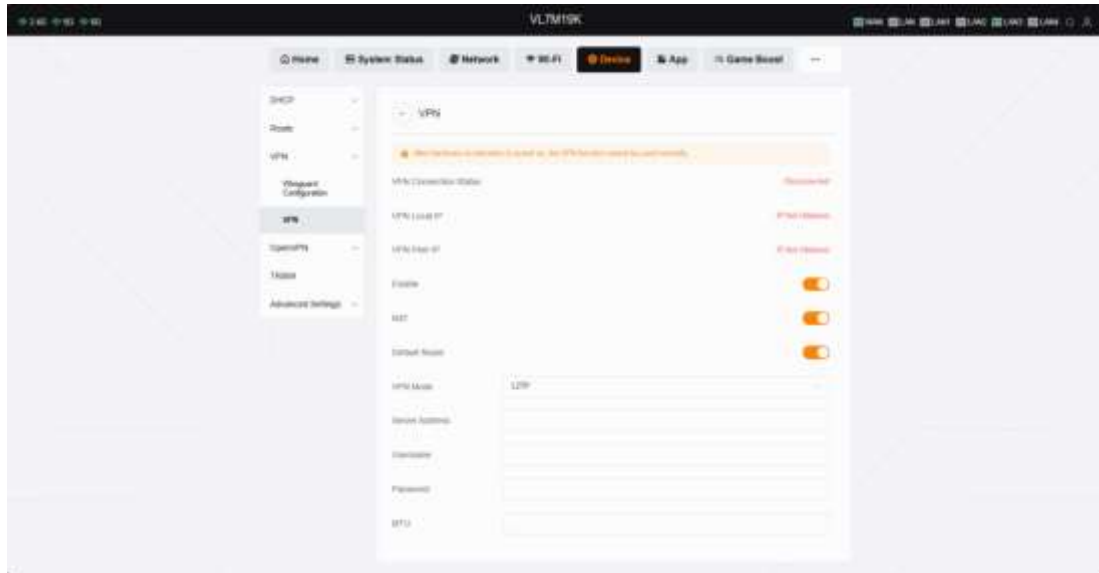
7.3.1. VPN L2TP Mode

(I) Configuration

1. Toggle the "Enable" switch to the right to activate the VPN service.
2. In the VPN Mode drop-down menu, select the VPN mode you want to use as L2TP.
3. Toggle the "NAT" and "Default Routing" switches to the right to enable these functions. This allows the VPN client to access the LAN and route traffic automatically.
4. In the Server Address field, enter the public IP address or domain name of the VPN server.
5. In the "Username" and "Password" fields, enter the credentials provided by your VPN service provider.
6. Enter the maximum transmission cell size in the "MTU" field to optimize network performance.

(2) Connect to the VPN server

Click the Save button to connect to the VPN, if the VPN connection is successful. You can see that the corresponding VPN connection status, VPN local IP, and VPN peer IP are displayed on the page.



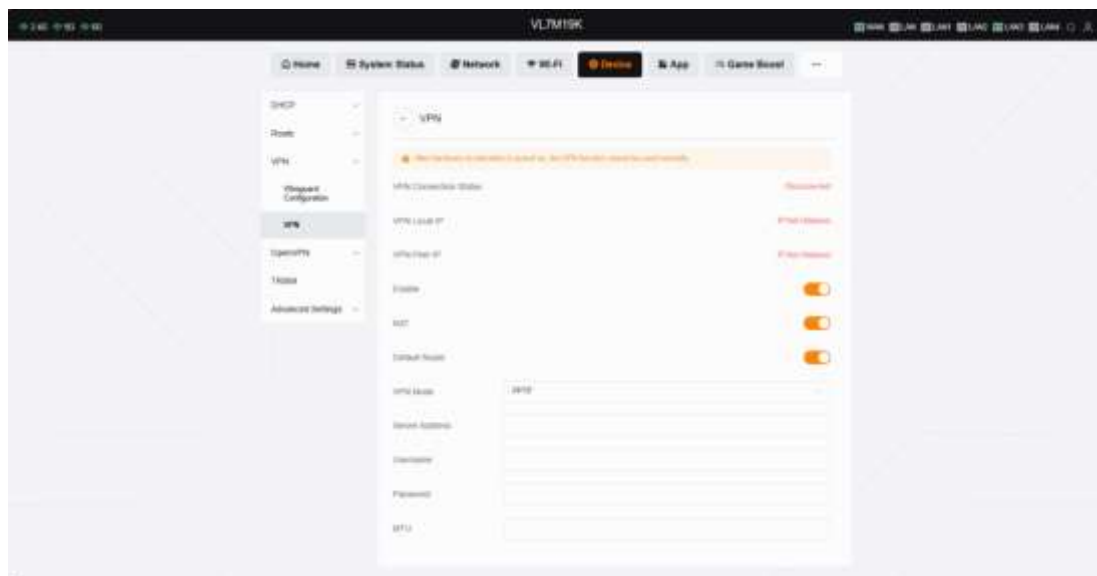
7.3.2. VPN PPTP

(1) configuration

1. Toggle the "Enable" switch to the right to activate the VPN service.
2. In the "VPN Mode" drop-down menu, select the desired VPN mode as PPTP.
3. Toggle the "NAT" and "Default Routing" switches to the right to enable these functions. This allows the VPN client to access the LAN and route traffic automatically.
4. In the Server Address field, enter the public IP address or domain name of the VPN server.
5. In the "Username" and "Password" fields, enter the credentials provided by your VPN service provider.
6. Enter the maximum transmission cell size in the "MTU" field to optimize network performance.

(2) Connect to the VPN server

Click the Save button to connect to the VPN, if the VPN connection is successful. You can see that the corresponding VPN connection status, VPN local IP, and VPN peer IP are displayed on the page.

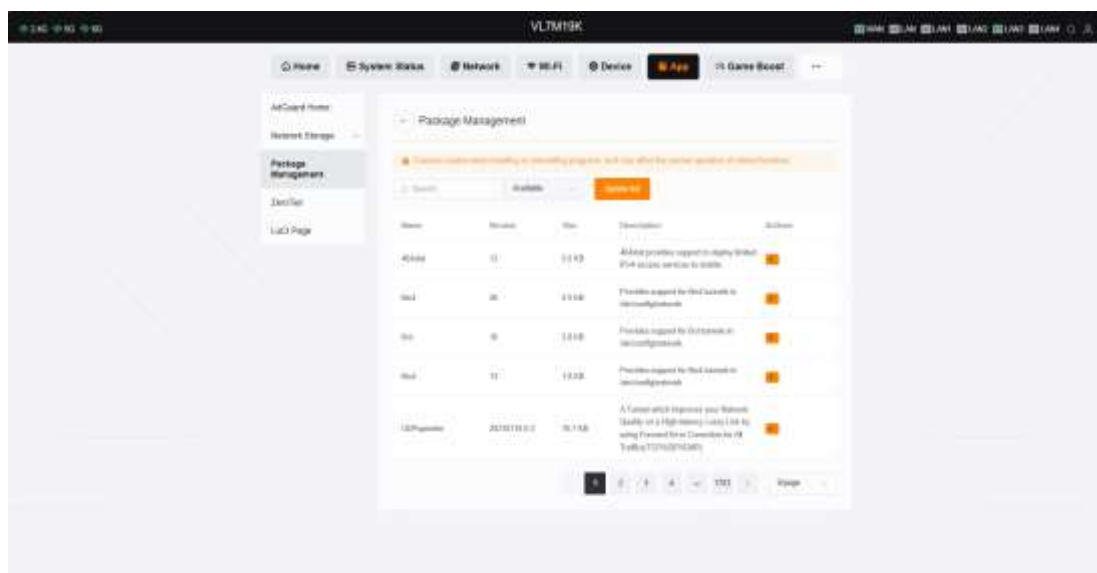


8. APPLICATIONS

8.1. Package Management

Package Management allows you to manage OpenWrt packages. You can install or remove any package.

Remember to click Update whenever you access this packages repository.



8.2. ZeroTier

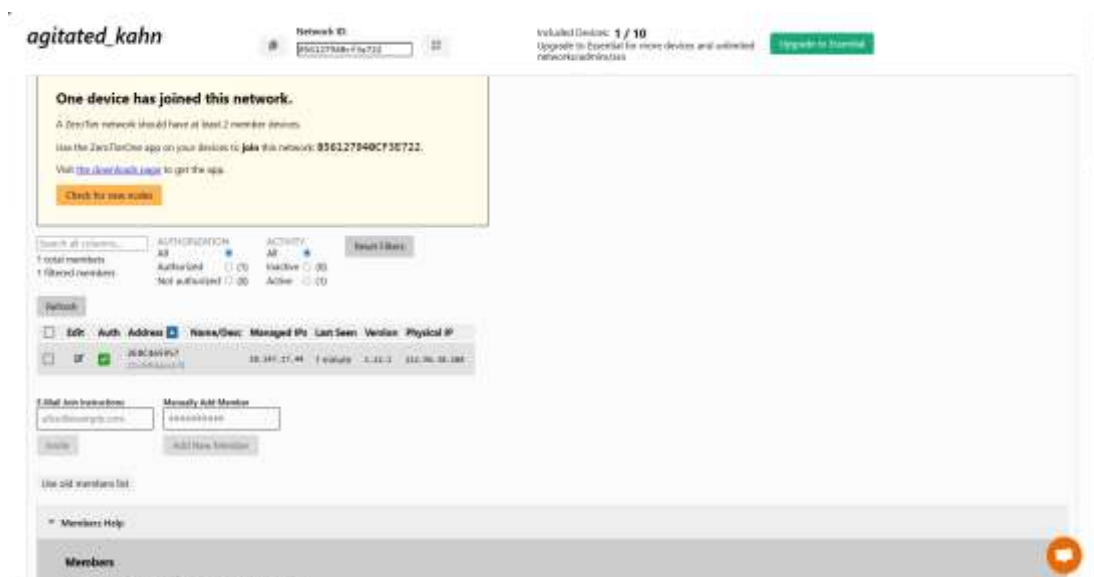
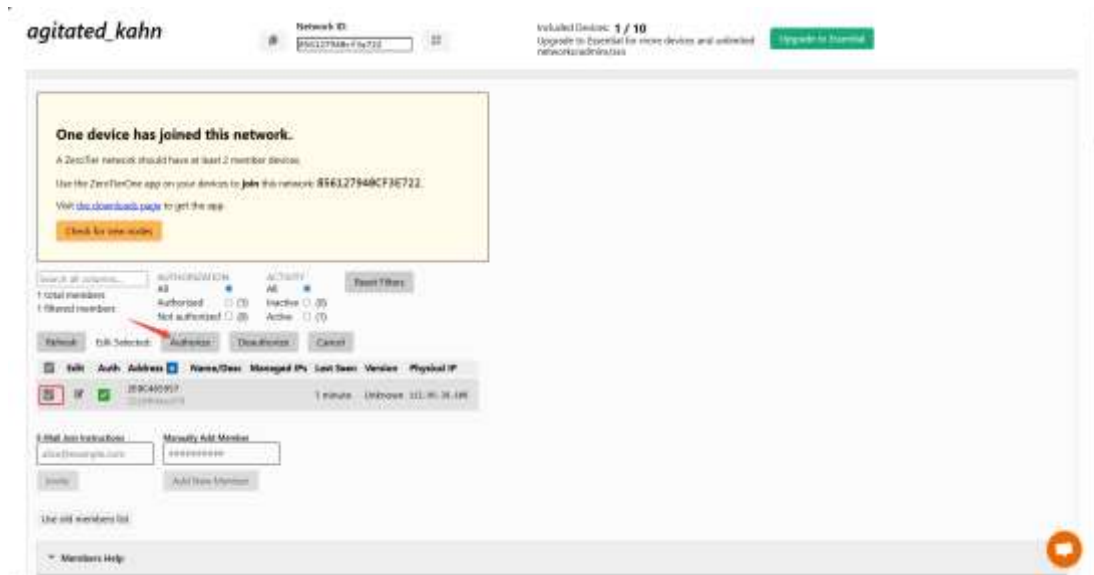
ZeroTier can create a secure point-to-point virtual network, support access to devices such as phones and PCs, and help you remotely access devices or LANs.



1. Please go to the official website URL: <https://www.zerotier.com>, apply for a Network ID.
2. On the ZeroTier page of the device, enter the Network ID.



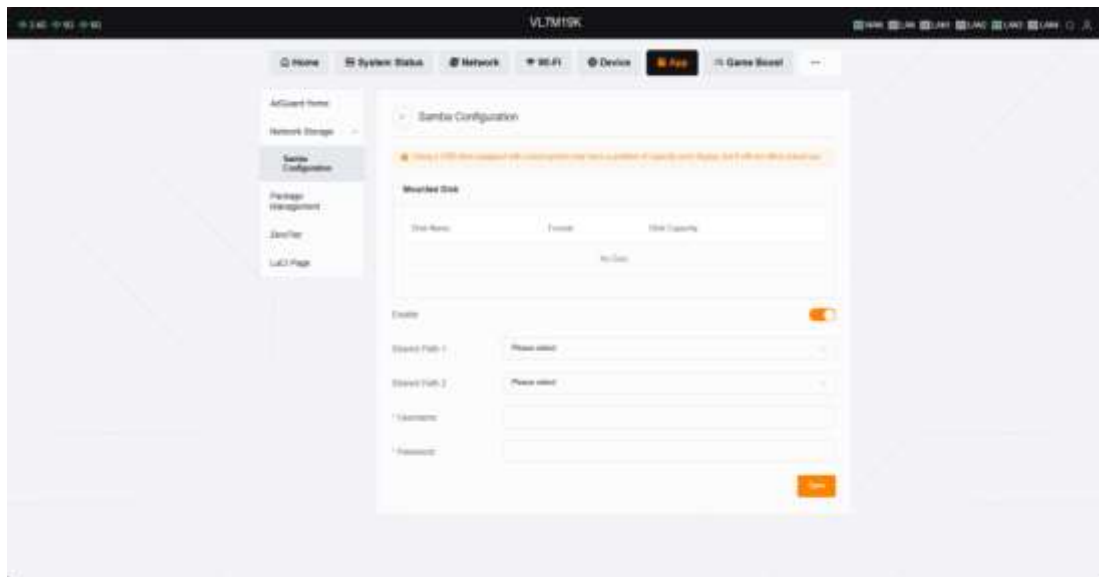
3. Select Activate the device that requires you and get the "Managed IPs" of the device.



4. You can install the official zeroTier tool on your mobile phone or computer, install the above operation to connect to the Network ID, to achieve remote access to the router.

8.3. Network Storage

You can use VL7M19K routers with external storage device such as USB stick, MicroSD card, etc., thus the contents can be shared among all your connected clients. You can easily read or modify its contents.



Note: The power consumption of USB hard drive is quite high. You should use it with an external power supply. Otherwise, it may cause malfunction.

8.4. LuCI Page

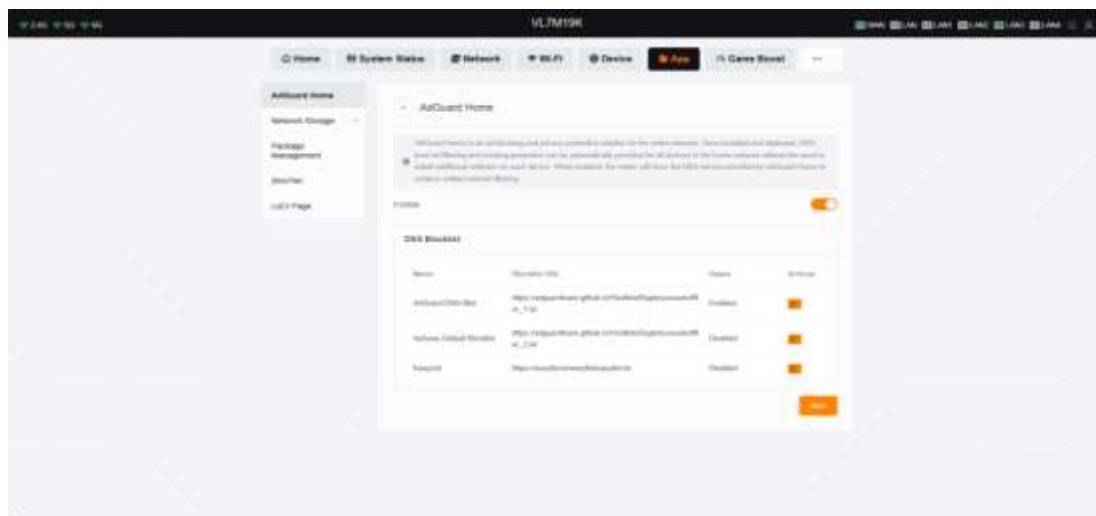
You can use OpenWrt's default user interface LuCI to manage your device. LuCI is an open source standalone project officially maintained by OpenWrt. Click this button to enter the native LuCI page.



8.5. AdGuard Home

AdGuard Home is an ad blocking and privacy protection solution for the entire network. Once installed and deployed, DNS-level ad filtering and tracking protection can be automatically provided for all devices in the home network without the need to install additional software on each device. When

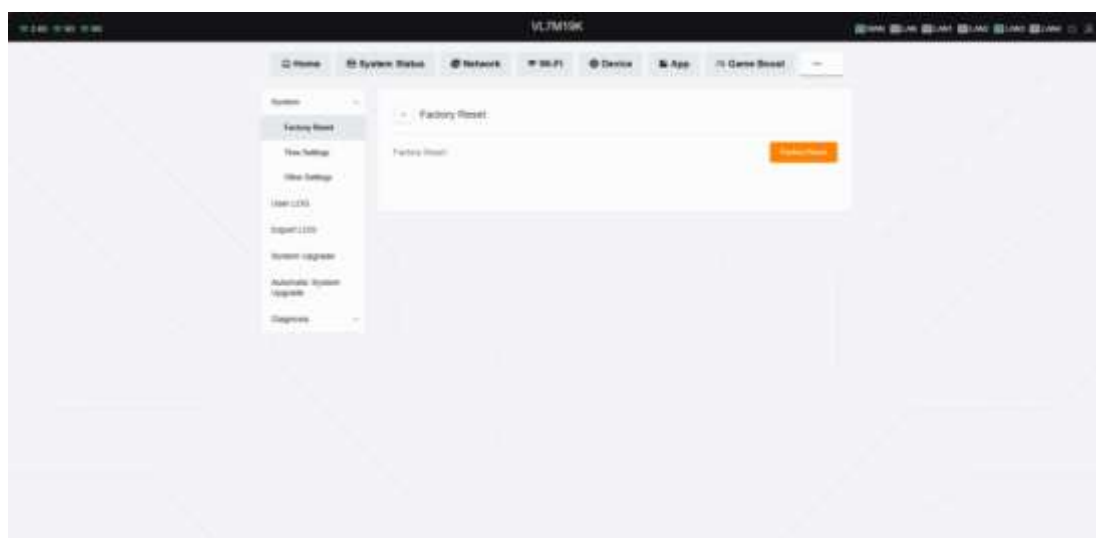
enabled, the router will force the DNS service provided by AdGuard Home to achieve unified network filtering.



9. MORE SETTINGS

9.1. Revert Firmware

Revert the router to factory default settings. All your settings, applications and data will be erased.

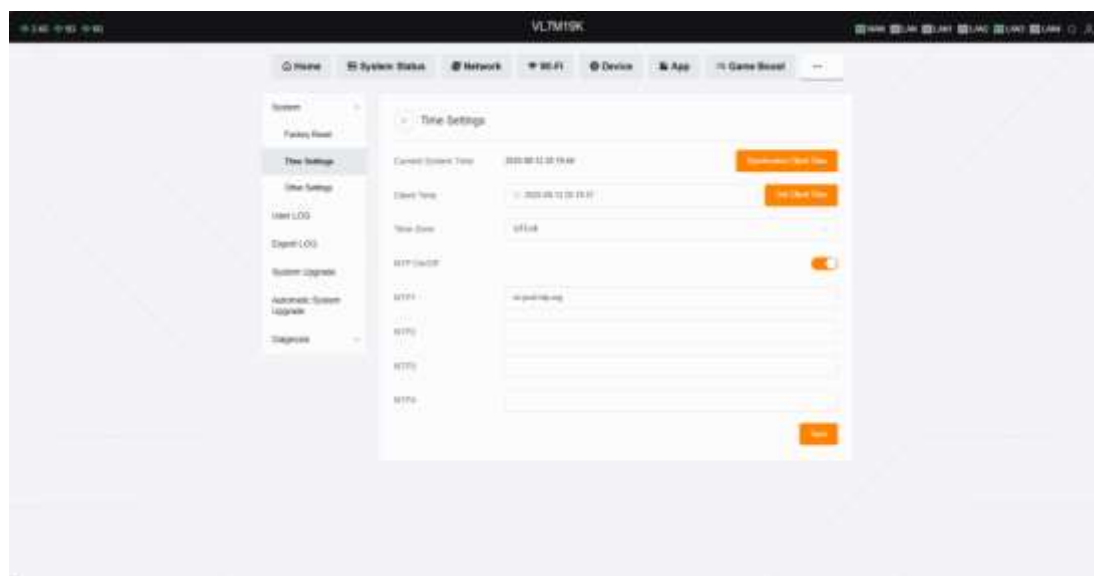


9.2. LAN IP

LAN IP is the IP address that you use to connect to this router. The default IP address of VL7M19K router is 192.168.0.1. If it conflicts with the IP address of your main router, you can change it.

9.3. Time Zone

The time of the router's activities will be recorded according to the router time. Therefore, choosing the time zone of your location is recommended.



9.4. Network Mode

Change the network mode to cater your usage scenario. You may need to reconnect your client device whenever you change the network mode of the router.

Be aware that you may not be able to access the web Admin Panel with the default IP 192.168.0.1 if you use the router in **Access Point**, **Extender** or **WDS** mode. If you want to access the web Admin Panel in this case, you have to use the IP address assigned by the main router to the VL7M19K router.

Router: Create your own private network. The router will act as NAT, firewall and DHCP server.

Access Point: Connect to a wired network and broadcast a wireless network.

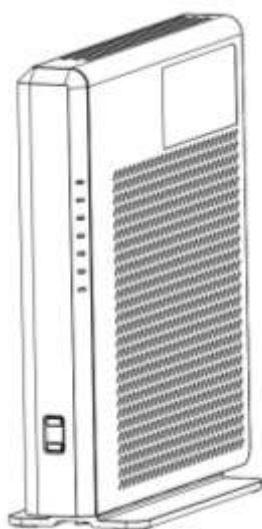
Extender: Extend the Wi-Fi coverage of an existing wireless network.

WDS: Similar to Extender, please choose WDS if your main router supports WDS mode.

10. Trouble shooting

10.1. LED Indicators

LED Status Indication



Category	Status	Description
POWER	Green (Always on)	Power on.
	Orange flashing slowly	When the restart button is pressed for 5 seconds.
	Light off	NO Power.
STATUS	Green (Always on)	Connecting to the Internet.
	Red flashing	Initializing or during firmware update.
	Light off	Not connected to the Internet.
2.4 GHz Wi-Fi	Green (Always on)	2.4 GHz Wi-Fi is enabled.
	Light off	2.4 GHz Wi-Fi is disabled.
5 GHz Wi-Fi	Green (Always on)	5 GHz Wi-Fi is enabled.
	Light off	5 GHz Wi-Fi is disabled.
6 GHz Wi-Fi	Green (Always on)	6 GHz Wi-Fi is enabled.
	Light off	6 GHz Wi-Fi is disabled.
WPS/MESH	Green (Always on)	Mesh network successfully established.
	Green flashing	Activate WPS/MESH scanning.
	Light off	Mesh disabled.
STORAGE	Green (Always on)	USB device mounted successfully.
	Light off	No USB device mounted.

10.2. Reset

All VL7MI9K routers have reset buttons, you can use them to repair your network or reset your routers to factory default settings. If you can neither access the web-based setup page nor the router, you can press the reset button: Press and hold for **6 seconds** then release to reset the router to factory settings. All user data will be cleared.

10.3. RESTART

Press and hold for more than 5 seconds to restart the device.

10.4. WPS

1. If the device supports the mesh function and the mesh switch is enabled, the mesh scan will start when the button lasts for 3 seconds.
2. When the mesh function is off, press and hold the WPS button for 1 to 6 seconds to enable the 5G Wi-Fi WPS feature.

10.5. Access Web Panel

Sometimes you may be unable to access 192.168.0.1 to login web admin panel, please follow the guide below to solve this problem.

Check connection/router's IP address

Make sure your WAN/LAN port connection is correct. WAN port is connected to an internet source and LAN port is connected to devices. If connected by Wi-Fi, make sure the SSID is correct.

Then follow the steps below to check the router's IP address.

Windows 7 / Windows 10 / Windows 11

Your IP address results determine the next step.

Your IP address is incorrect

1. Check your connection again.
2. Try [Reset](#) to back to factory default.

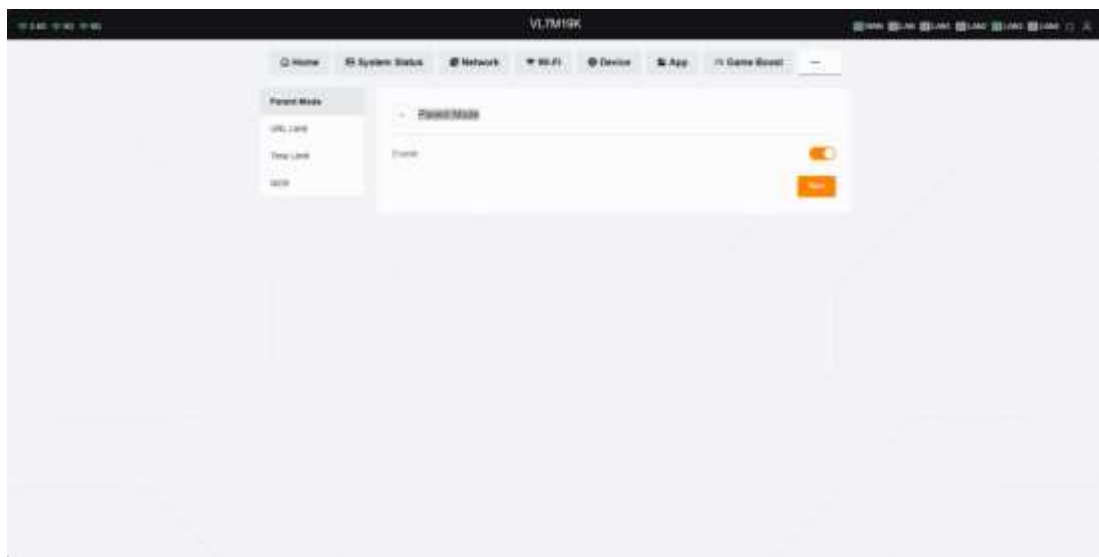
Your IP address is correct

1. Make sure you are using Chrome/Firefox, then try to access 192.168.0.1 again.
2. In order to avoid problems caused by the cache, press the hotkey ctrl+shift+n in Chrome to enter the incognito mode. Then try to access 192.168.0.1 again.

11. Parental Control

11.1 Parent Mode

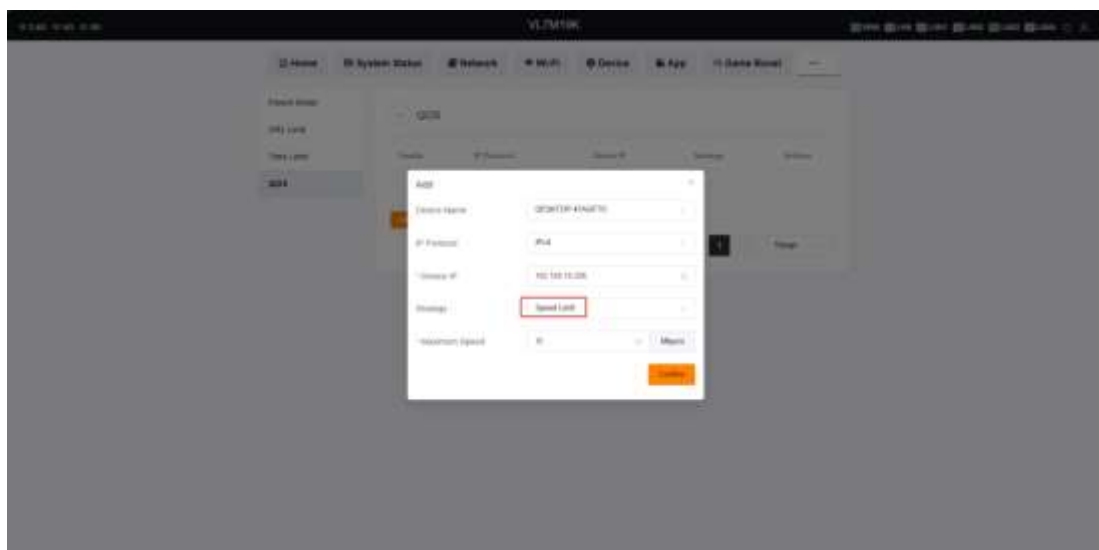
On this page, you can turn on the "Parental Controls" function master switch.



11.2 QOS

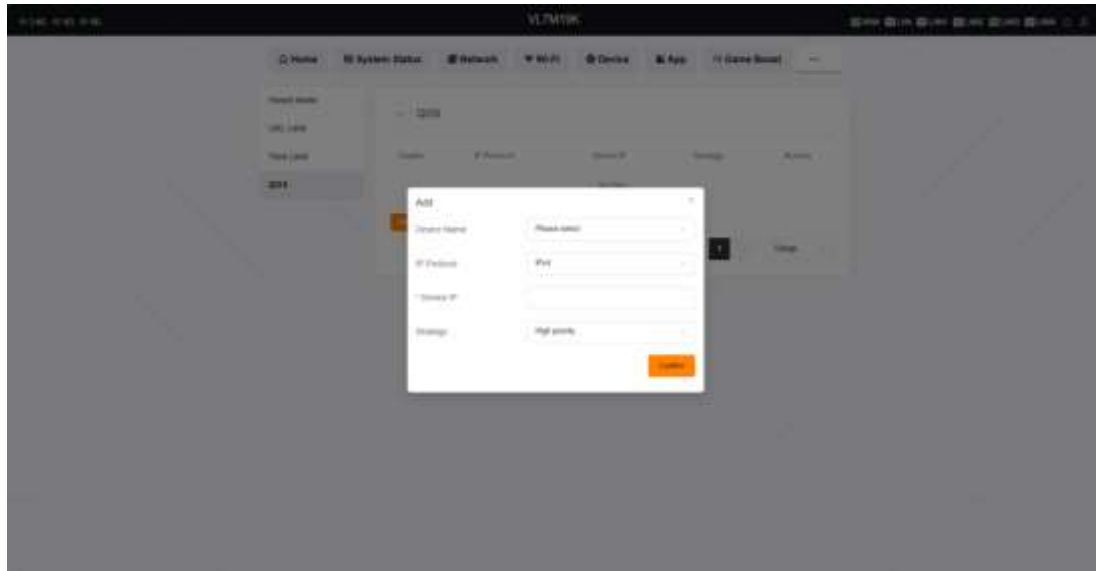
(I) Speed Limit

You can limit the network rate for specified devices.



(2) High priority

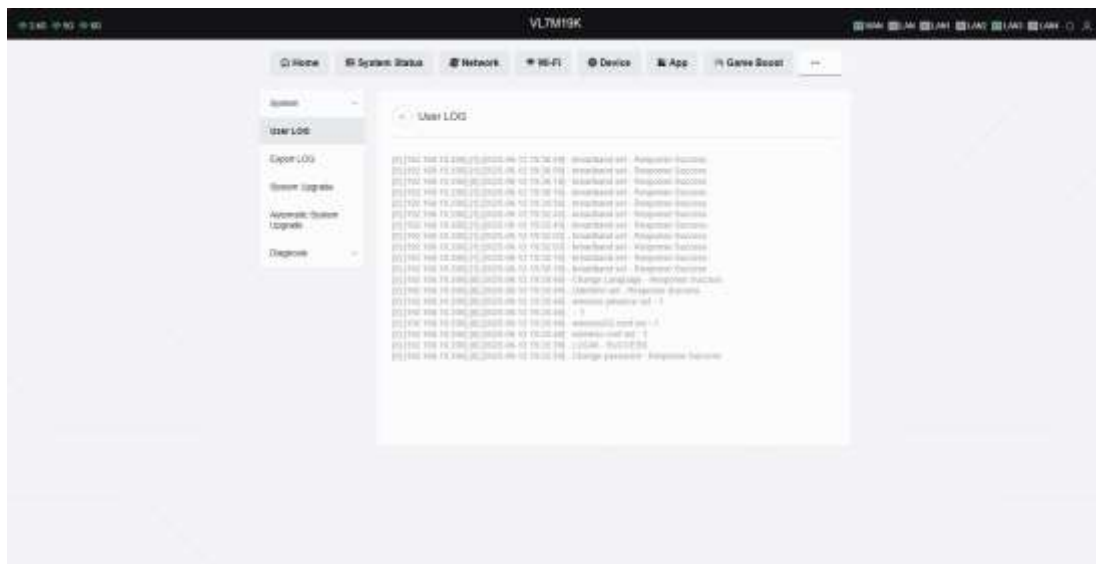
You can specify that a device has the highest preferred level for the current network.



12. LOG

12.1 User LOG

You can check the web logs.



12.2 Export LOG

Export system logs, kernel logs, crash logs, and cloud platform logs.



13 FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of 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.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be

provided with antenna installation instructions and consider removing the no-collocation 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.

Caution!

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

FCC regulations restrict the operation of this device to indoor use only.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.