Wi-Tek
Communication Solution

User Guide
For 4G Router

Release version:V1.0.0

March 2024

Directory

Overview

As one of the product lines of Wi-Tek, 4G routers have the advantages of powerful functionality, flexible deployment, and high cost-effectiveness. They have built-in 4G modules and PoE outputs, which can solve the power supply and networking problems of outdoor monitoring systems. Wi-Tek 4G router can support 4G mode, wireless router mode, 4G mode, and Ethernet backup mode. You can switch between different modes to cope with various environmental challenges: 4G to Ethernet, 4G to WiFi, which can effectively solve problems such as high cost, long duration, and maintenance of outdoor wired networks. Wi-Tek also offers free cloud management services.

Applicable product models are as follows:

WI-LTE113-O, WI-LTE117-O, WI-LTE115-O(v2), WI-LTE110-O(v2), WI-LTE300(v2)

Revision History

Date	Doc Version	Description
March 2024	V1.0	Initial version

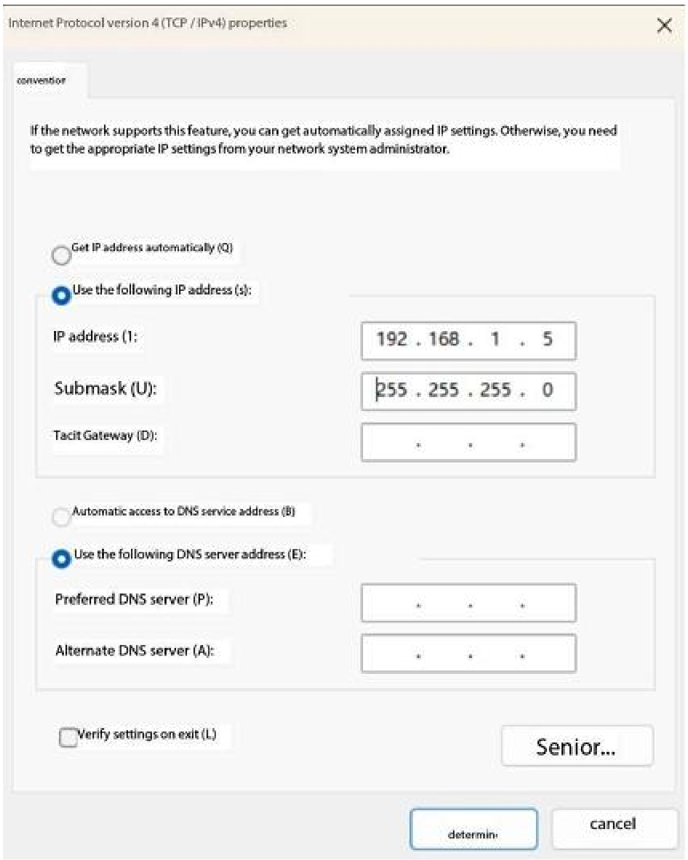
1. Quick Start

1.1. Start the device

Take WI-LTE110-O (V2) as an example, you can use **12v DC** power supply or **24v PoE** power supply, the **default IP address: 192.168.1.1**, and the computer can set a static IP to log in to the web page.

1.2. Log in to the web interface

Step 1 Connect your computer to the LAN port of your 4G router with a network cable.
Step 2 Make sure that the IP address of the management computer is in the same network segment of the 4G router. For example, if the IP address of the 4G router is **192.168.1.1**, the management computer can be configured with an IP address of **192.168.1.5**.



Internet Protocol version 4 (TCP / IPv4) properties

convention

If the network supports this feature, you can get automatically assigned IP settings. Otherwise, you need to get the appropriate IP settings from your network system administrator.

○ Get IP address automatically (Q)

● Use the following IP address (s):

IP address (I: 192 . 168 . 1 . 5

Submask (U): 255 . 255 . 255 . 0

Tacit Gateway (D): . . .

○ Automatic access to DNS service address (B)

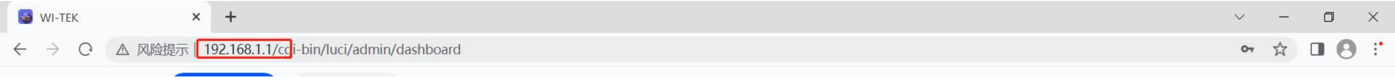
● Use the following DNS server address (E):

Preferred DNS server (P): . . .

Alternate DNS server (A): . . .

□ Verify settings on exit (L)

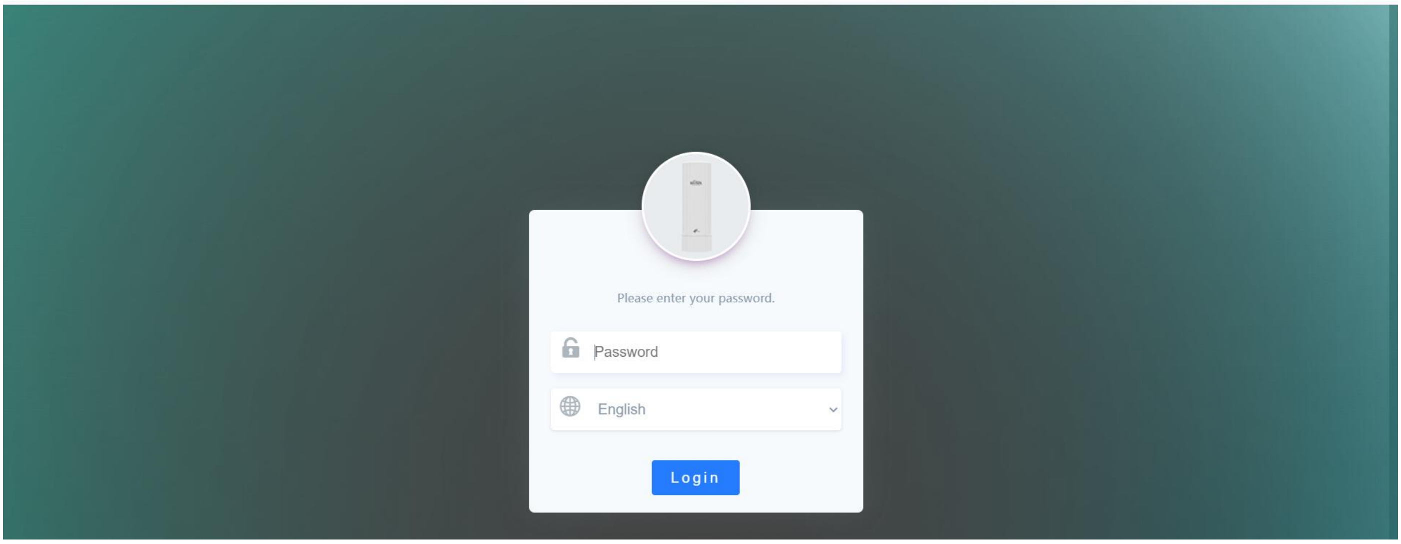
Step 3 Launch a web browser on your computer and enter the IP address of the 4G router(**default:192.168.1.1**) in the address bar.



WI-TEK

风险提示 192.168.1.1/cgi-bin/luci/admin/dashboard

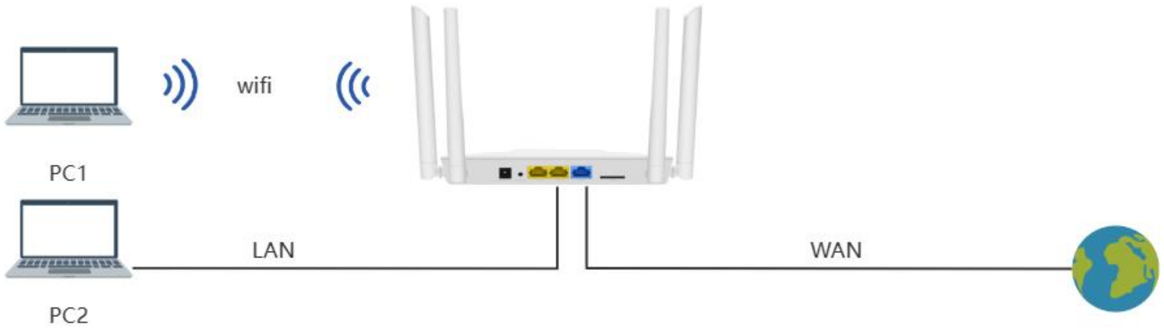
Step 4 Enter the login username and password (**default: admin**) and click the Login button.


Please enter your password.

1. Working mode

1.3. Router mode

Wired is used as WAN (external network) port, wireless is used as LAN (local area network) port, and WAN (external network) port supports PPPOE, fixed IP and automatic acquisition. The following is a schematic diagram of the connection.



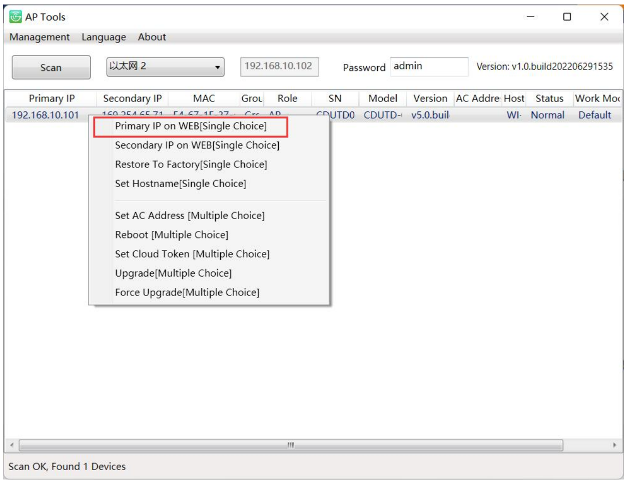
Setup steps

Step 1 Open the Scan Tools on computer.

ScanTools_20210927

Note: Download Link http://www.wireless-tek.com/files_down.php?id=90

Step 2 Click the "Scan" button to query the IP address obtained by the router, and the tool will use the default browser to open the corresponding IP access device. As follows:

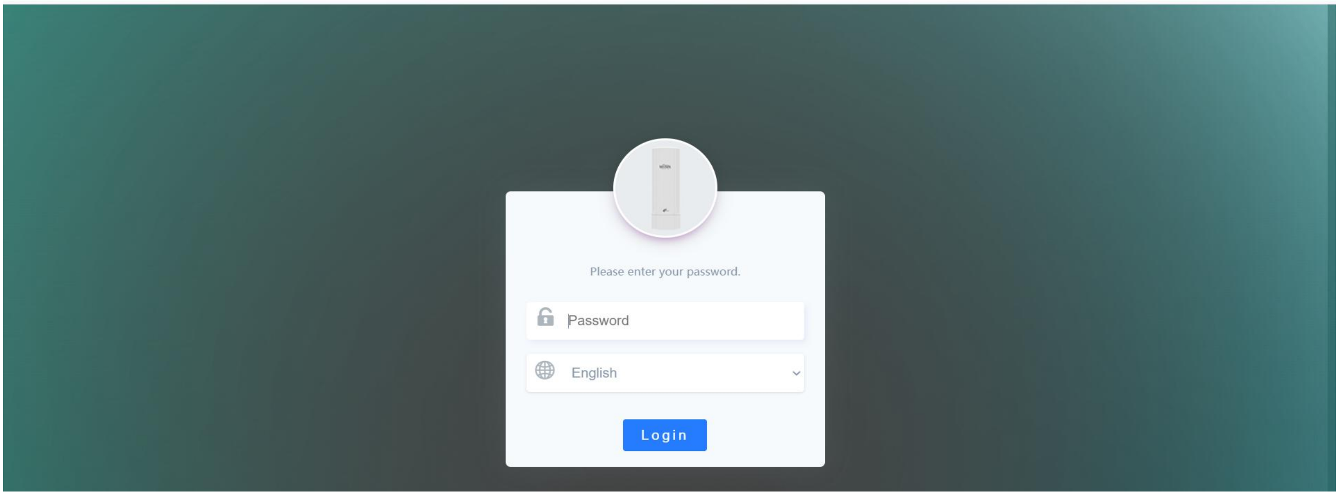

AP Tools
Management
Language
About
Scan
Primary IP on WEB[Single Choice]
Secondary IP on WEB[Single Choice]
Restore To Factory[Single Choice]
Set Hostname[Single Choice]
Set AC Address [Multiple Choice]
Reboot [Multiple Choice]
Set Cloud Token [Multiple Choice]
Upgrade[Multiple Choice]
Force Upgrade[Multiple Choice]

以太网 2 192.168.10.102 Password admin Version: v1.0.build202206291535

Primary IP	Secondary IP	MAC	Grou	Role	SN	Model	Version	AC Addre	Host	Status	Work Moc
192.168.10.101	169.254.65.71	[illegible]	Grc	AP	CDUTD0	CDUTD-	v5.0.buil		WI-	Normal	Default

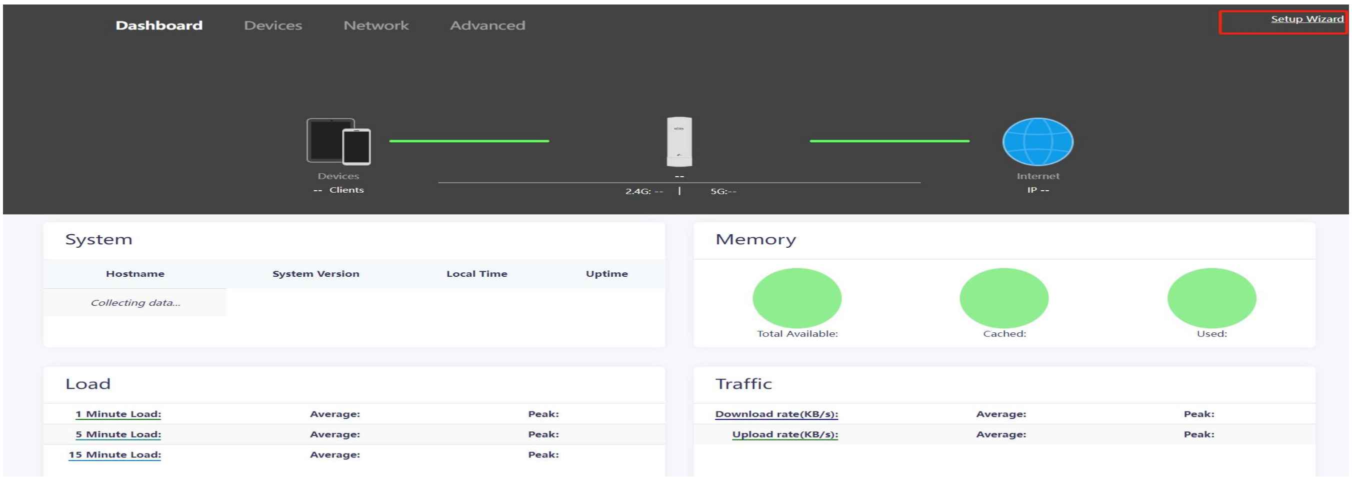
Scan OK, Found 1 Devices

Step 3 After normal access opens, enter the default password admin for Administrator Login,as shown below.



Please enter your password.

Step 4 Click "Setup Wizard" to enter the next step and select the router mode.



System

Hostname	System Version	Local Time	Uptime
Collecting data...			

Memory

Total Available: Cached: Used:

Load

1 Minute Load:	Average:	Peak:
5 Minute Load:	Average:	Peak:
15 Minute Load:	Average:	Peak:

Traffic

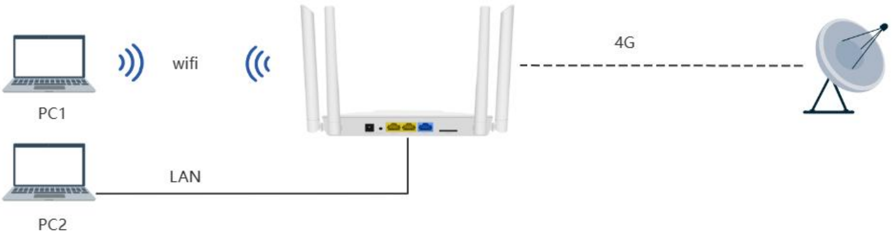
Download rate(KB/s):	Average:	Peak:
Upload rate(KB/s):	Average:	Peak:

Step 5 Choose how you want to access the Internet.

Step 6 After the SSID and password are saved, the router mode takes effect.

1.4. 4G mode (default)

Use a SIM card to access the Internet in 4G mode.The following is a schematic diagram of the connection.



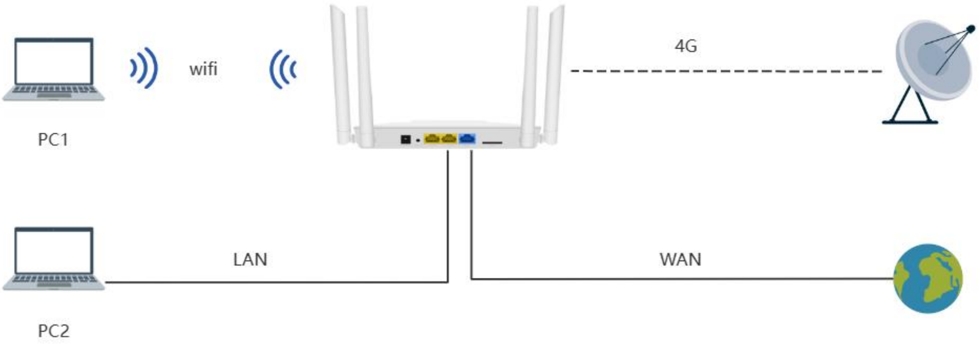
Setup steps

Step1 Click "Setup Wizard" to enter the next step and select the 4G mode.

Step2 After the SSID and password are saved, the router mode takes effect.

1.5. Eth-First Router mode

When there is both Internet and SIM card Internet access, the router mode is preferred.The following is a schematic diagram of the connection.



Setup steps

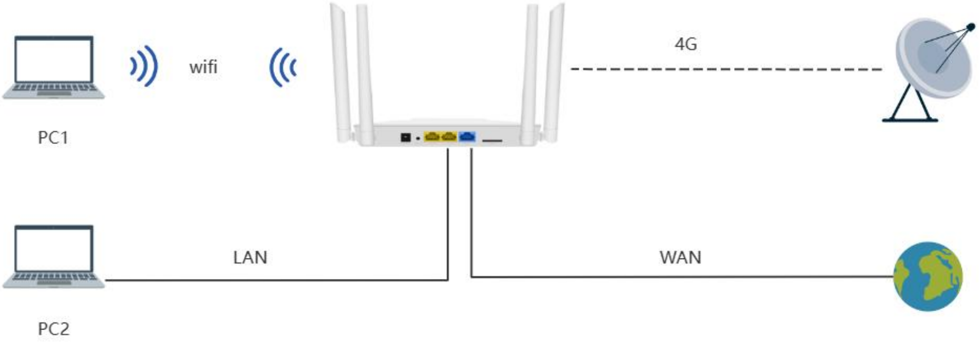
Step1 Click "Setup Wizard" to enter the next step and select the Eth-First Router mode.

Step2 Choose how you want to access the Internet.

Step3 After the SSID and password are saved, the router mode takes effect.

1.6. 4G-First Router

When there is both Internet and SIM card Internet access, the 4G mode is preferred.The following is a schematic diagram of the connection.



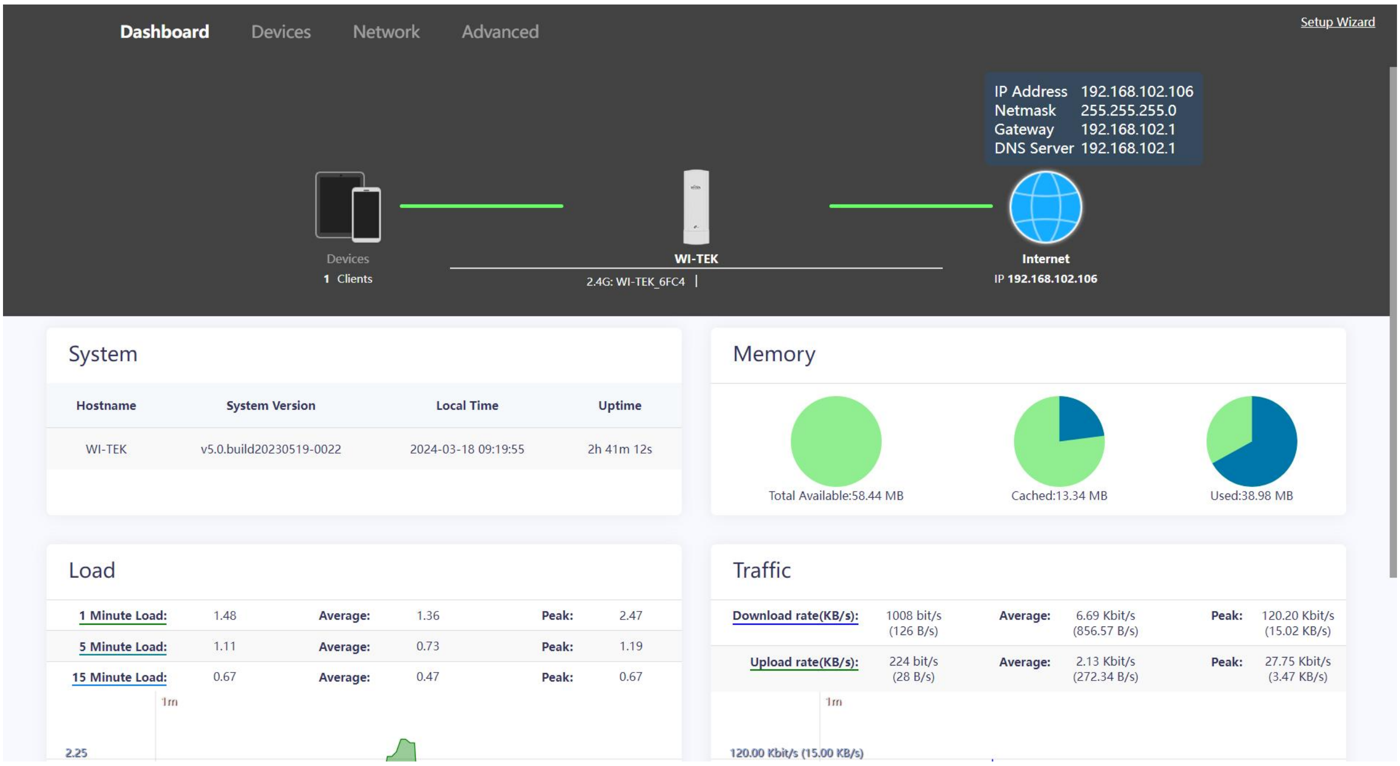
Setup steps

Step1 Click "Setup Wizard" to enter the next step and select the 4G-First Router mode.

Step3 After the SSID and password are saved, the router mode takes effect.

2. Dashboard

The Dashboard page allows you to check current system info of 4G router.



IP Address 192.168.102.106
Netmask 255.255.255.0
Gateway 192.168.102.1
DNS Server 192.168.102.1

System

Hostname	System Version	Local Time	Uptime
WI-TEK	v5.0.build20230519-0022	2024-03-18 09:19:55	2h 41m 12s

Memory

Total Available:58.44 MB

Cached:13.34 MB

Used:38.98 MB

Load

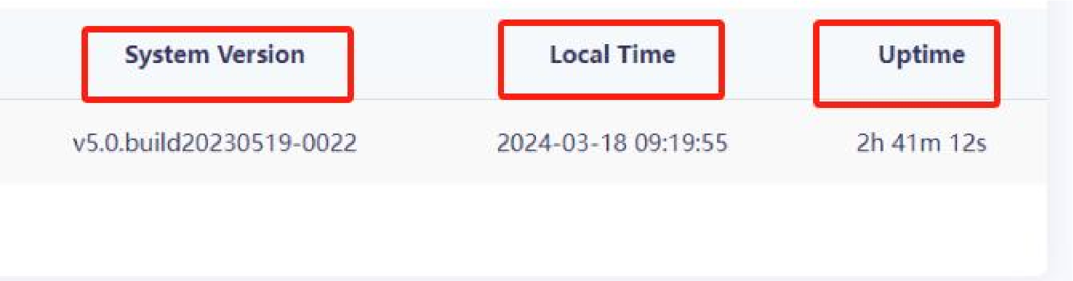
1 Minute Load:	1.48	Average:	1.36	Peak:	2.47
5 Minute Load:	1.11	Average:	0.73	Peak:	1.19
15 Minute Load:	0.67	Average:	0.47	Peak:	0.67

Traffic

Download rate(KB/s):	1008 bit/s (126 B/s)	Average:	6.69 Kbit/s (856.57 B/s)	Peak:	120.20 Kbit/s (15.02 KB/s)
Upload rate(KB/s):	224 bit/s (28 B/s)	Average:	2.13 Kbit/s (272.34 B/s)	Peak:	27.75 Kbit/s (3.47 KB/s)

2.1. System Version,Local Time,Uptime

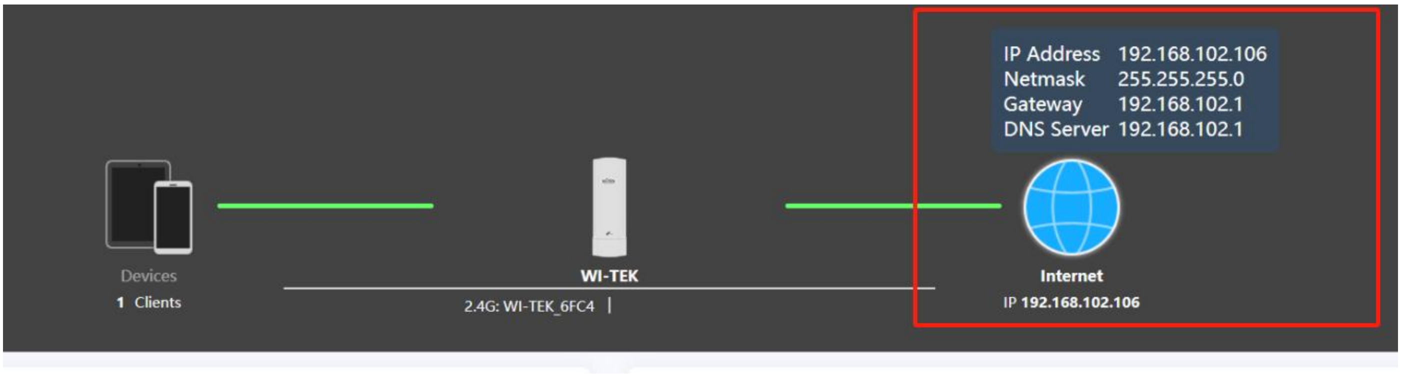
The version information, startup time, and running time of the device software are displayed



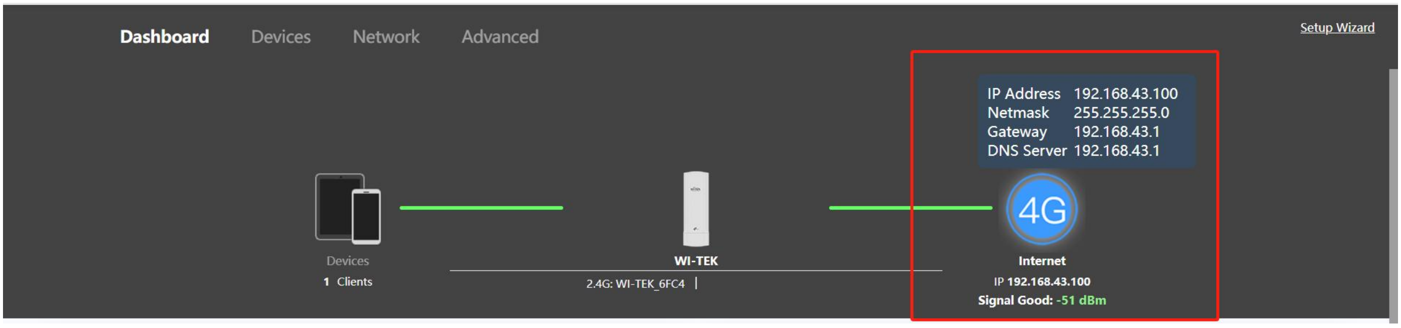
System Version	Local Time	Uptime
v5.0.build20230519-0022	2024-03-18 09:19:55	2h 41m 12s

2.2. Information about the current network

It will display the current Internet access method, and display the IP address, subnet mask, gateway address, and DNS server information of the device.



IP Address 192.168.102.106
Netmask 255.255.255.0
Gateway 192.168.102.1
DNS Server 192.168.102.1

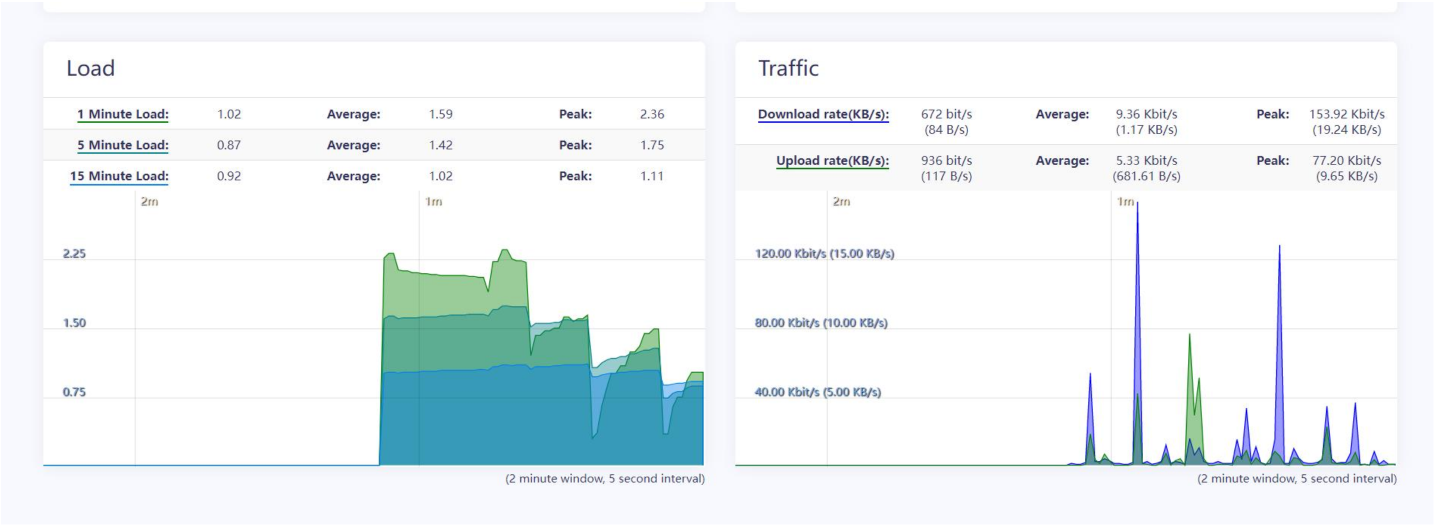


IP Address 192.168.43.100
Netmask 255.255.255.0
Gateway 192.168.43.1
DNS Server 192.168.43.1

Signal Good: -51 dBm

2.3. Load and traffic information

On the web page displays real-time payload information, uplink and downlink traffic informati on.



Load

1 Minute Load:	1.02	Average:	1.59	Peak:	2.36
5 Minute Load:	0.87	Average:	1.42	Peak:	1.75
15 Minute Load:	0.92	Average:	1.02	Peak:	1.11

(2 minute window, 5 second interval)

Traffic

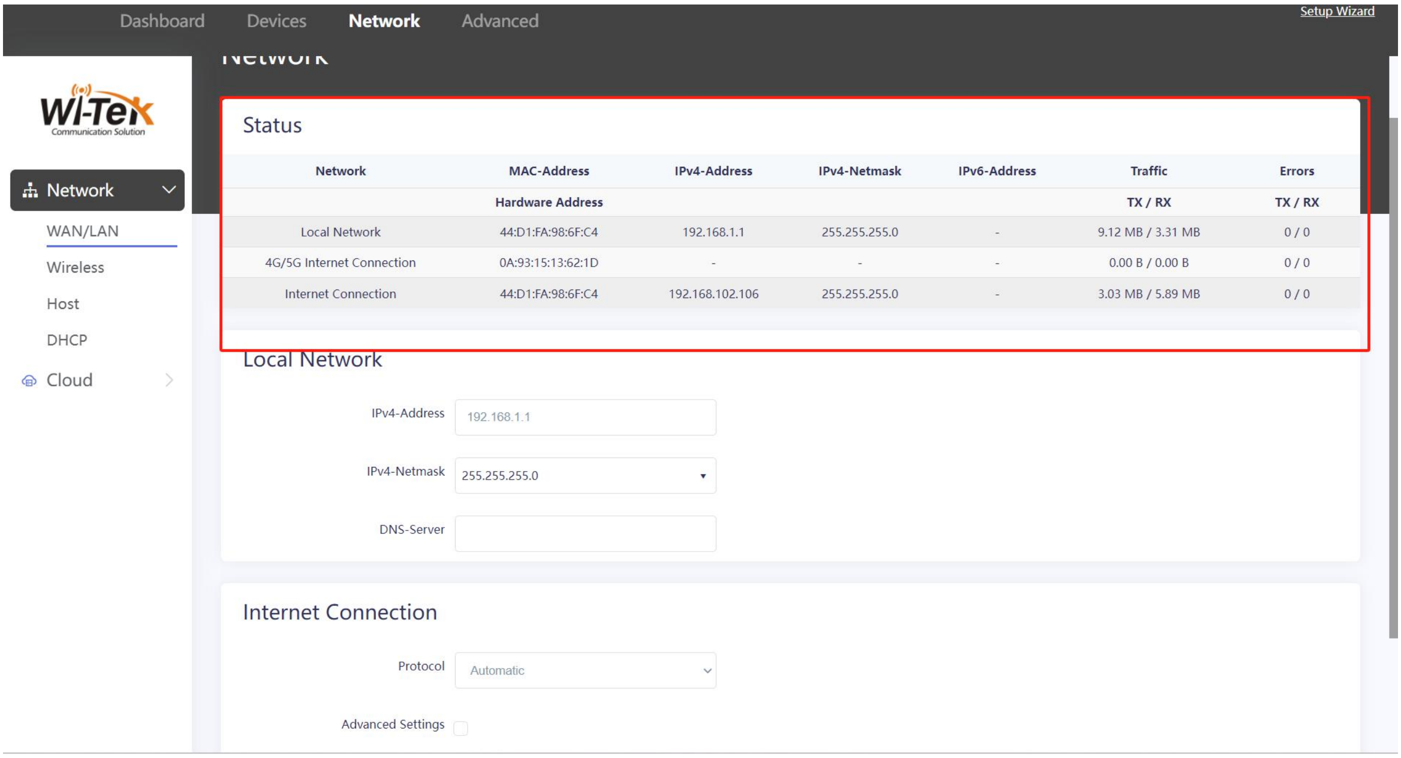
Download rate(KB/s):	672 bit/s (84 B/s)	Average:	9.36 Kbit/s (1.17 KB/s)	Peak:	153.92 Kbit/s (19.24 KB/s)
Upload rate(KB/s):	936 bit/s (117 B/s)	Average:	5.33 Kbit/s (681.61 B/s)	Peak:	77.20 Kbit/s (9.65 KB/s)

(2 minute window, 5 second interval)

3. Network settings

3.1. WAN/LAN Settings

Click “Network”> “WAN/LAN”,in the “Status” section, you can view the network information and local network information that you are currently connected to.



Status

Network	MAC-Address	IPv4-Address	IPv4-Netmask	IPv6-Address	Traffic	Errors
	Hardware Address				TX / RX	TX / RX
Local Network	44:D1:FA:98:6F:C4	192.168.1.1	255.255.255.0	-	9.12 MB / 3.31 MB	0 / 0
4G/5G Internet Connection	0A:93:15:13:62:1D	-	-	-	0.00 B / 0.00 B	0 / 0
Internet Connection	44:D1:FA:98:6F:C4	192.168.102.106	255.255.255.0	-	3.03 MB / 5.89 MB	0 / 0

Local Network

IPv4-Address: 192.168.1.1

IPv4-Netmask: 255.255.255.0

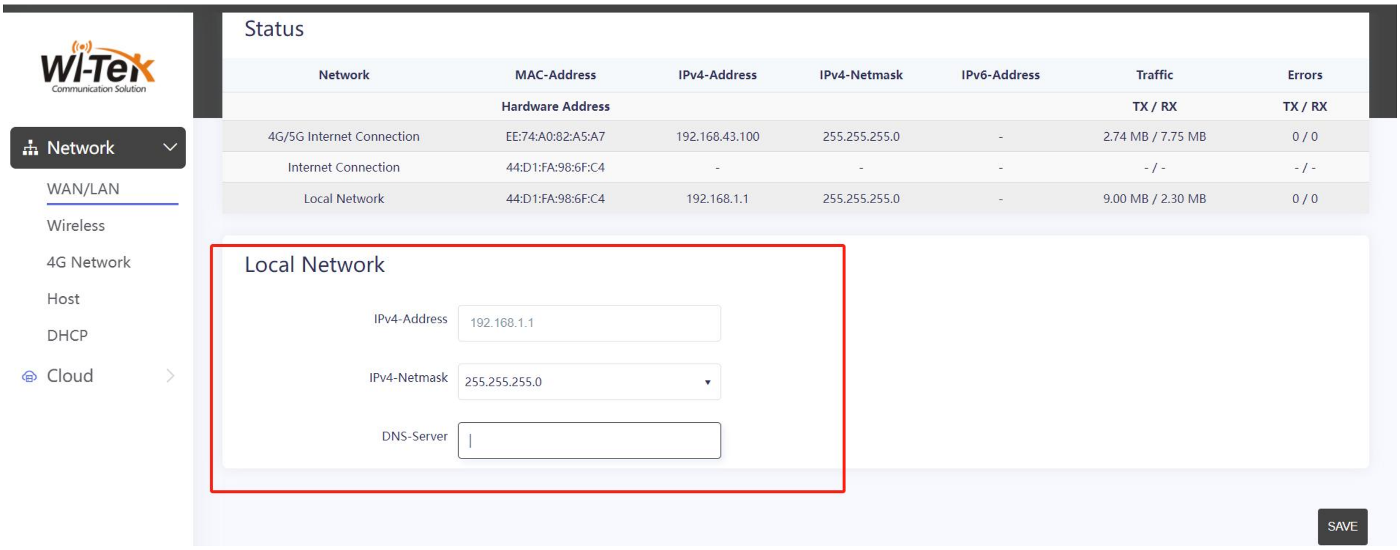
DNS-Server:

Internet Connection

Protocol: Automatic

Advanced Settings □

In "Local Network", you can set the IP address and mask of the local network, as well as the DNS server, and your connection terminal will get the IP address of the same network segment.



Status

Network	MAC-Address	IPv4-Address	IPv4-Netmask	IPv6-Address	Traffic	Errors
	Hardware Address				TX / RX	TX / RX
4G/5G Internet Connection	EE:74:A0:82:A5:A7	192.168.43.100	255.255.255.0	-	2.74 MB / 7.75 MB	0 / 0
Internet Connection	44:D1:FA:98:6F:C4	-	-	-	- / -	- / -
Local Network	44:D1:FA:98:6F:C4	192.168.1.1	255.255.255.0	-	9.00 MB / 2.30 MB	0 / 0

Local Network

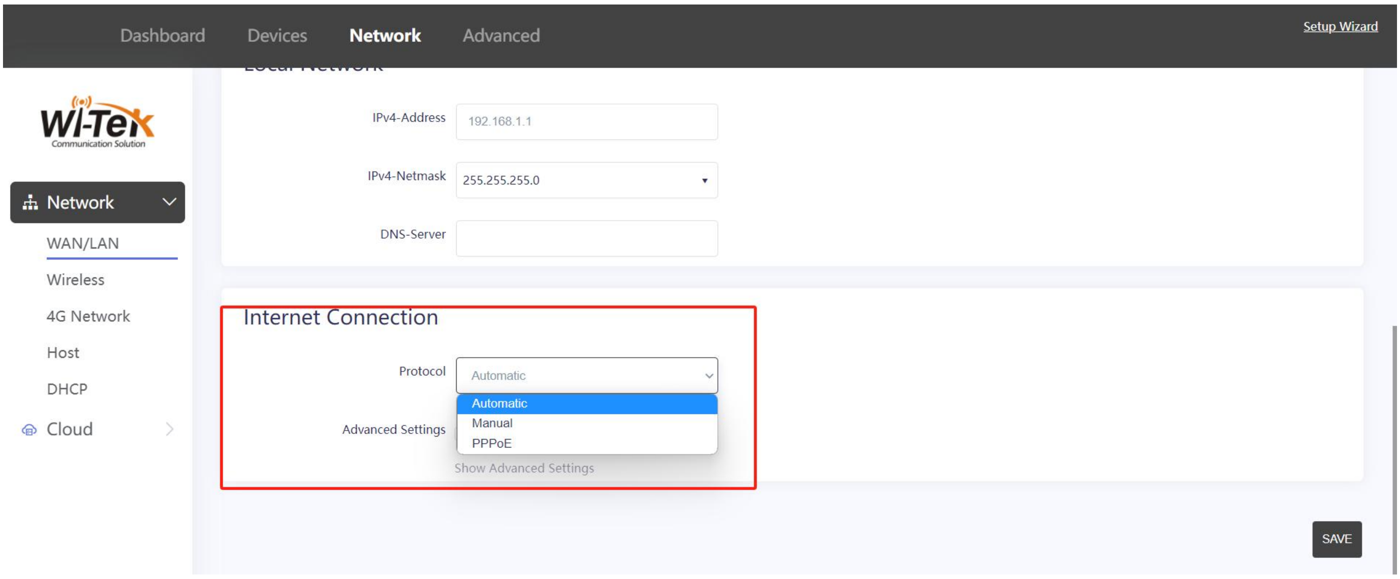
IPv4-Address: 192.168.1.1

IPv4-Netmask: 255.255.255.0

DNS-Server:

You can also set the network connection mode in "Internet Connection", which can set Automatic, Manual, and PPPoE dial-up.

Note:this feature is not supported in 4G mode.



IPv4-Address: 192.168.1.1

IPv4-Netmask: 255.255.255.0

DNS-Server:

Internet Connection

Protocol: Automatic

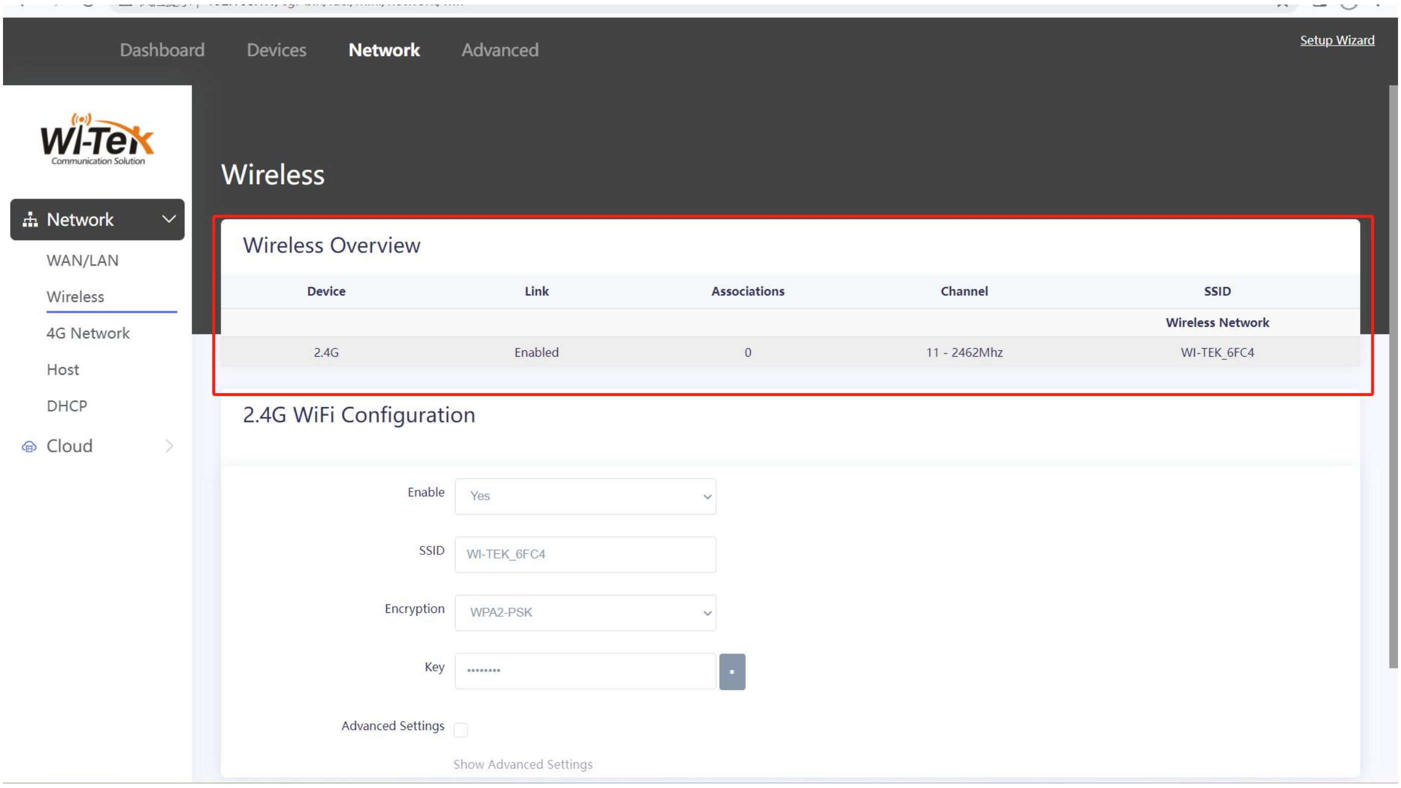
- Automatic
- Manual
- PPPoE

Advanced Settings: Show Advanced Settings

Parameter	Describe
Automatic	Connecting the 4G router to the higher-level router (DHCP server) will automatically obtain information such as IP address, mask, gateway, etc.
Manual	Enter the correct information such as static IP, mask, gateway, DNS, etc. obtained from the upstream network.
PPPoE	When the operator provides a broadband account and password that can access the Internet, you can choose this networking method.

3.2. Wireless

Click “Network”> “Wireless” go to the wireless settings page and view the Wi-Fi information in the "Wireless Overview".



Wireless

Wireless Overview

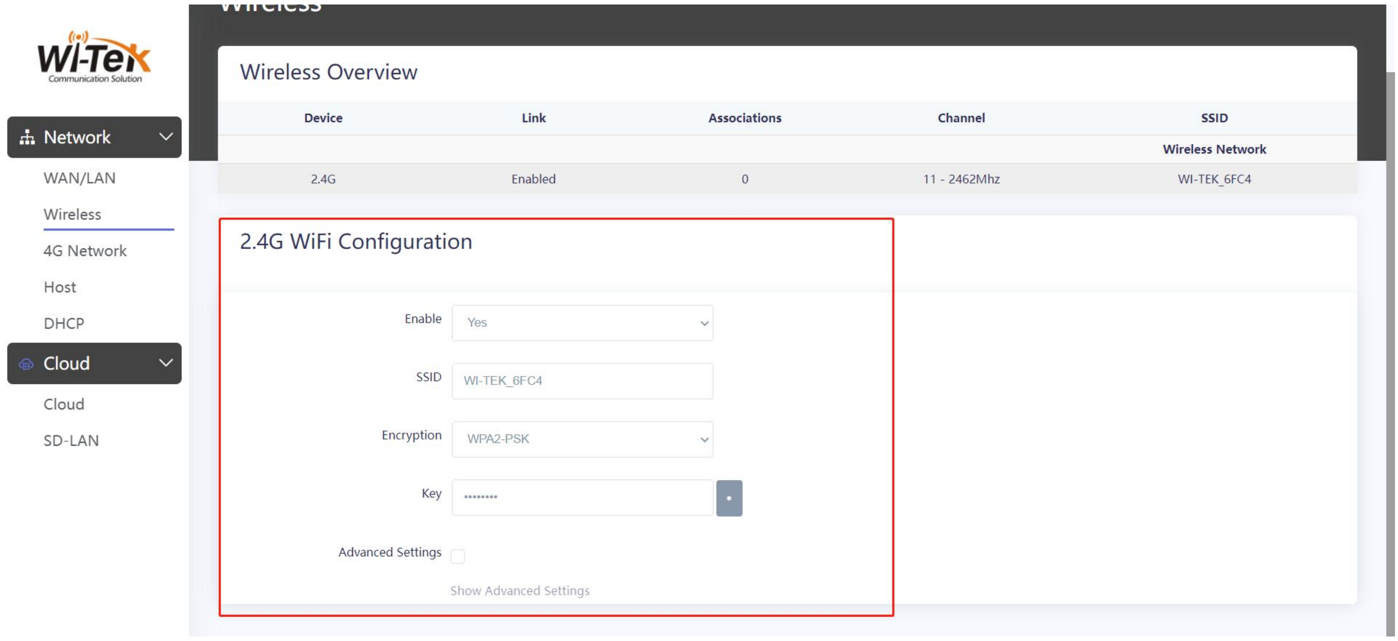
Device	Link	Associations	Channel	SSID
				Wireless Network
2.4G	Enabled	0	11 - 2462Mhz	WI-TEK_6FC4

2.4G WiFi Configuration

Enable	Yes
SSID	WI-TEK_6FC4
Encryption	WPA2-PSK
Key	••••••••
Advanced Settings	□

Show Advanced Settings

You can set Wi-Fi on and off, and when Wi-Fi is turned off, the connected terminal will no receive the Wi-Fi SSID. You can also set the SSID, encryption method, and password.



Wireless Overview

Device	Link	Associations	Channel	SSID
				Wireless Network
2.4G	Enabled	0	11 - 2462Mhz	WI-TEK_6FC4

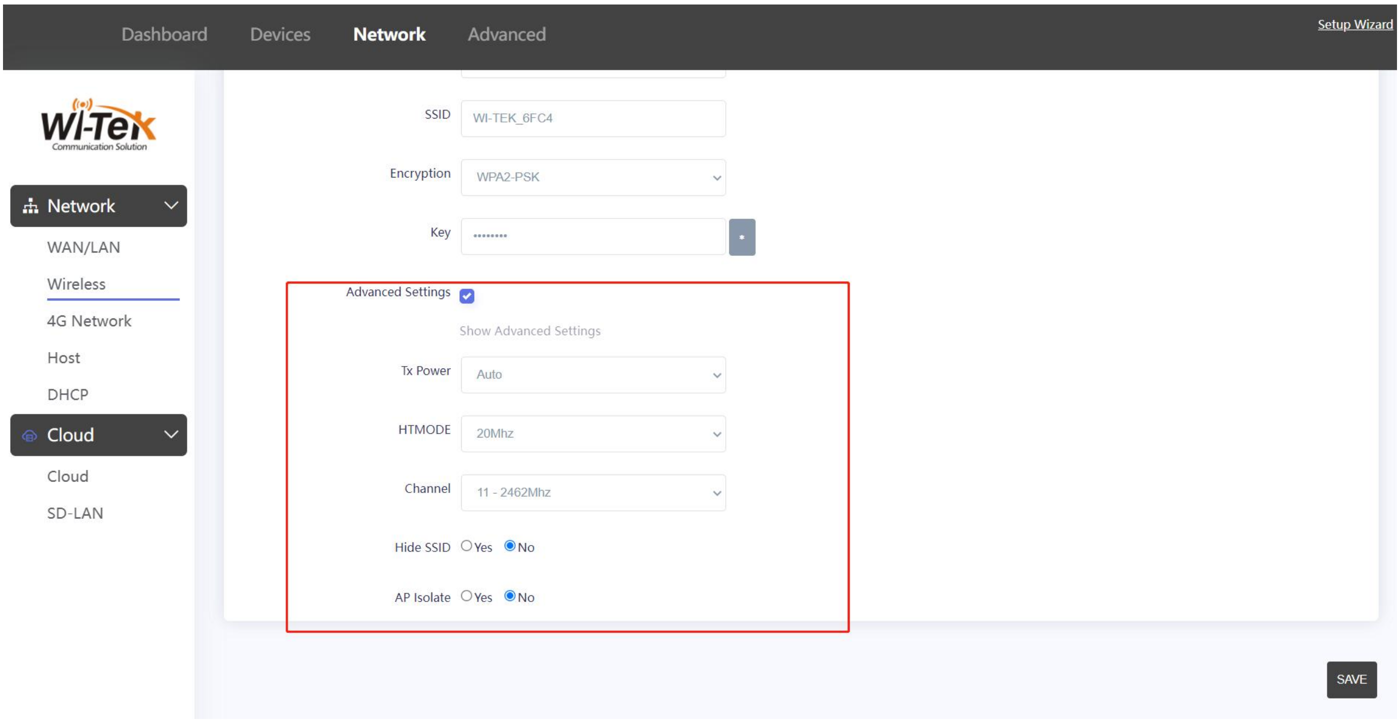
2.4G WiFi Configuration

Enable	Yes
SSID	WI-TEK_6FC4
Encryption	WPA2-PSK
Key	••••••••
Advanced Settings	□

Show Advanced Settings

Parameter	Describe
Enable	Check this option to disable the wireless. If checked, the wireless radio will disable.
SSID	Specify a name for the wireless network.
Encryption	Select the Encryption mode of the wireless network. There are five options: WPA-TKIP, WPA2-AES, WPA1/WPA2-Mixed, WPA-Enterprise and WPA2-Enterprise. The latest WPA2-AES mode is recommended. None: Clients can access the wireless network without authentication.
Key	Specify password for SSID.

Click “Advanced Settings” modify RF parameters.



SSID: WI-TEK_6FC4

Encryption: WPA2-PSK

Key: ••••••••

Advanced Settings ☑

Show Advanced Settings

Tx Power: Auto

HTMODE: 20Mhz

Channel: 11 - 2462Mhz

Hide SSID ○Yes ●No

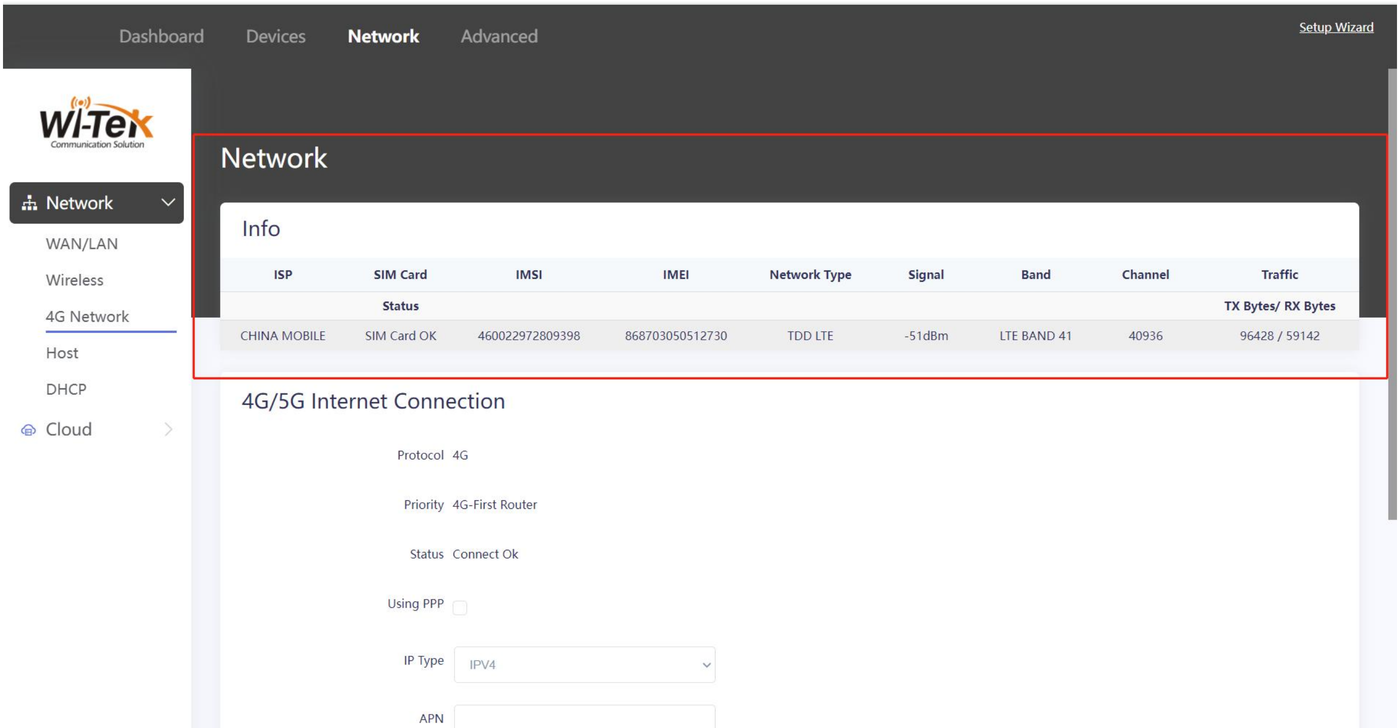
AP Isolate ○Yes ●No

Parameter	Describe
AP Isolation	With this function enabled, the device isolates all the connected clients within the same wireless network from each other.
Hide SSID	Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.

Channel	Select the channel used . For example, 1/2412MHz means that the channel is 1 and the frequency is 2412MHz. By default, the channel is automatically selected, and we recommend that you keep the default setting.
Tx Power	Specify the transmit power value. If this value is set to be larger than the maximum transmitted power that is allowed, the regulated maximum transmit power will be applied. Note: In most cases, it is unnecessary to use the maximum transmit power.Specifying a larger transmit power than needed may cause interference to the neighborhood.
HTMODE	For 4G router of different specifications, there is different bandwidth.Its available options include 20MHz, 20MHz/40MHz. Note: The greater the bandwidth, the greater the throughput, and the shorter the transmission distance, the more susceptible to interference.

3.3. 4G Network

Click “Network”>“4G Network”.The status information of the 4G/5G network can be observed, including carrier information, SIM card connection status, IMEI, network type, signal strength, frequency band, channel, traffic and other information.



Network

Info

ISP	SIM Card Status	IMSI	IMEI	Network Type	Signal	Band	Channel	Traffic TX Bytes/ RX Bytes
CHINA MOBILE	SIM Card OK	460022972809398	868703050512730	TDD LTE	-51dBm	LTE BAND 41	40936	96428 / 59142

4G/5G Internet Connection

Protocol 4G

Priority 4G-First Router

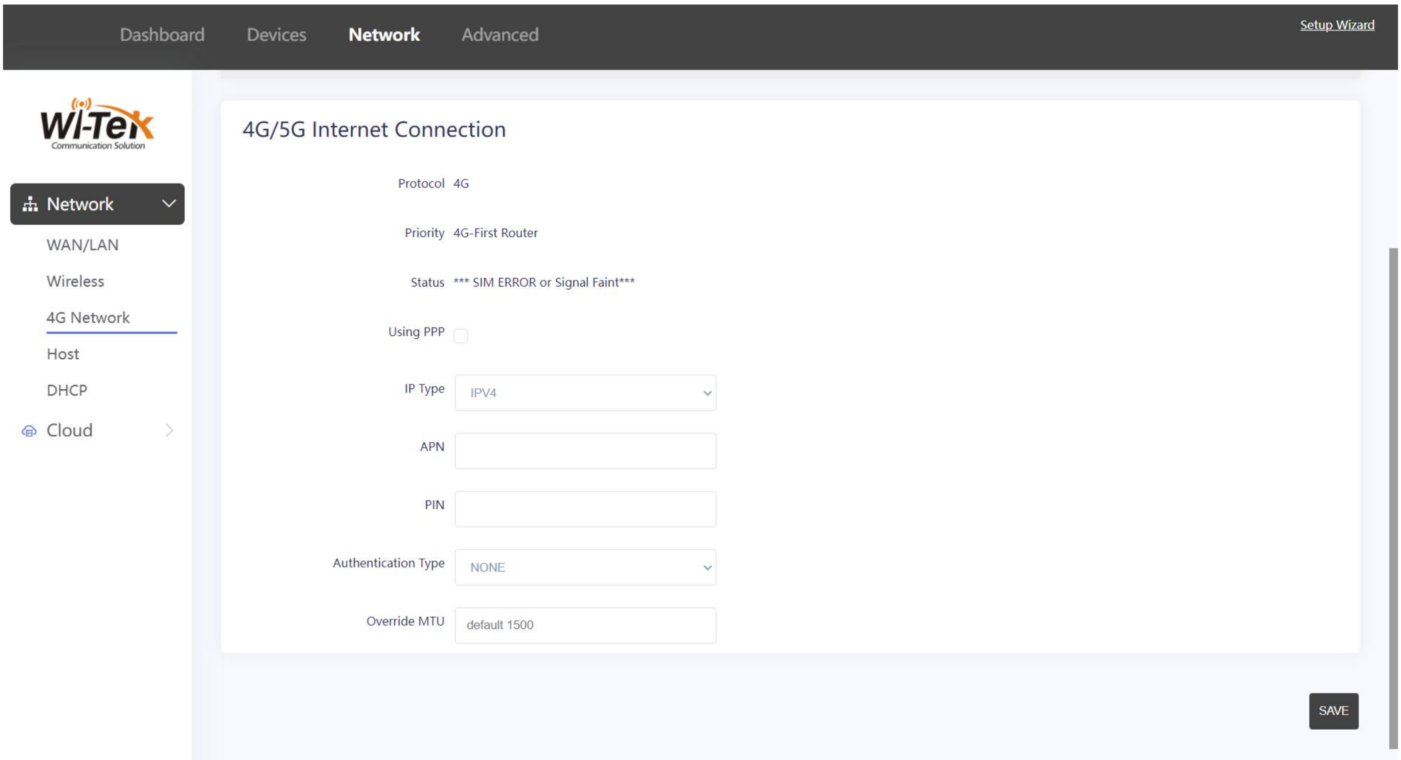
Status Connect Ok

Using PPP □

IP Type IPV4

APN

4G/5G Internet Connection



4G/5G Internet Connection

Protocol 4G

Priority 4G-First Router

Status *** SIM ERROR or Signal Faint***

Using PPP □

IP Type IPV4

APN

PIN

Authentication Type NONE

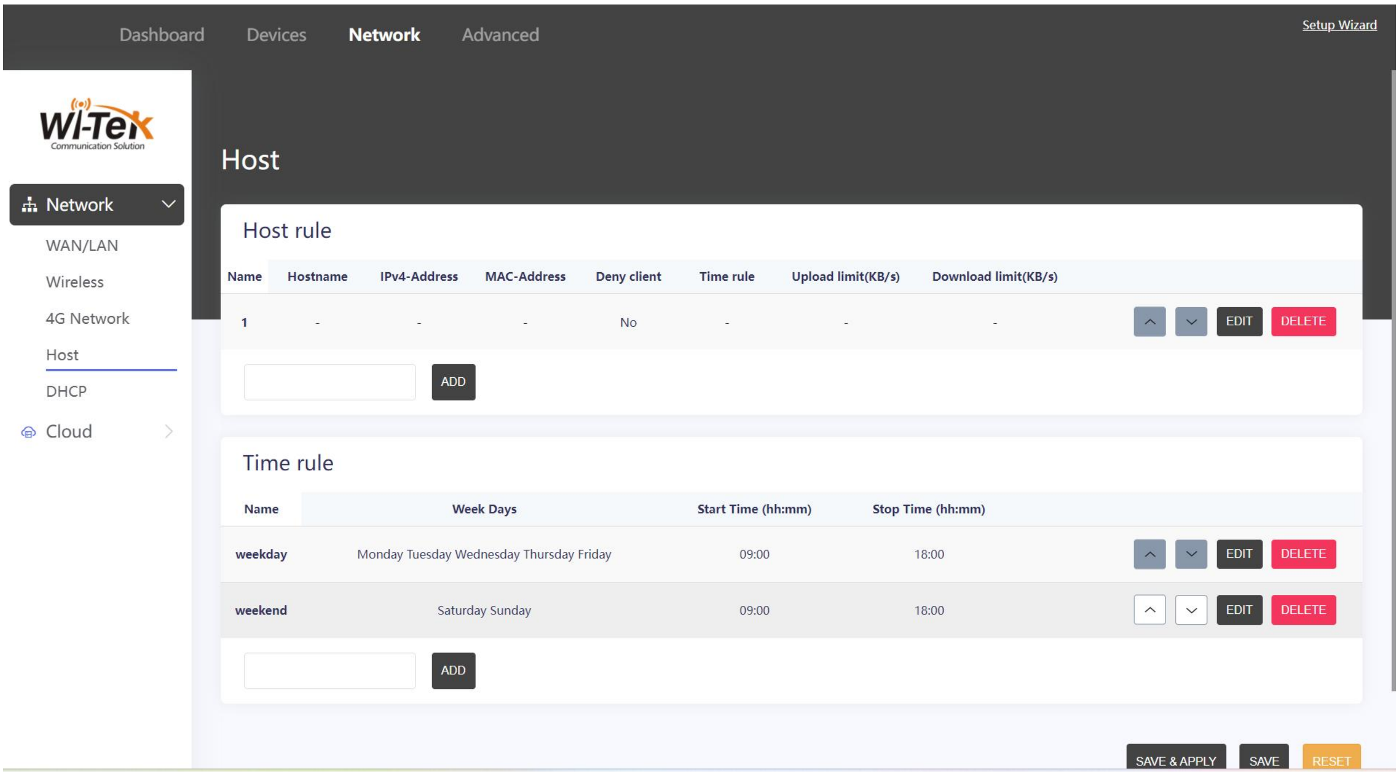
Override MTU default 1500

Parameter	Describe
Protocol	Displays the protocol of the SIM card 4G or 5G.
Priority	Shows the working mode of the 4G router.
Status	Displays the signal status of the SIM card.
Using PPP	When you enable PPP dial-up Internet access, you need to contact the network operator to provide relevant data.
APN	Normally, after inserting the SIM card, the 4G wireless data terminal will automatically recognize and configure the APN parameters to access the internet. If the 4G wireless data terminal does not automatically recognize the APN parameters, you can manually add the APN configuration file for dial-up Internet access. Please contact your carrier for the relevant parameters
PIN	PIN (Personal Identification Number) is used to protect the SIM card from e mbezzlement. PIN Management allows you to easily change the PIN setting s of your SIM card as needed.
Authentication Type	The authentication methods include PAP/CHAP, PAP, CHAP, and NONE.

Override MTU	The maximum packet size that the network is capable of transmitting, in bytes. The size of the MTU determines the maximum number of bytes that the sender can send at one time. If the MTU exceeds the maximum value that the receiver can bear, packets will be fragmented or even dropped, increasing the burden on network transmission. If it is too small and affects the transmission efficiency, it is recommended to use the default value of 1500.

3.4. Host

You can limit the Internet access time of the connected terminal in the client settings.



Host

Host rule

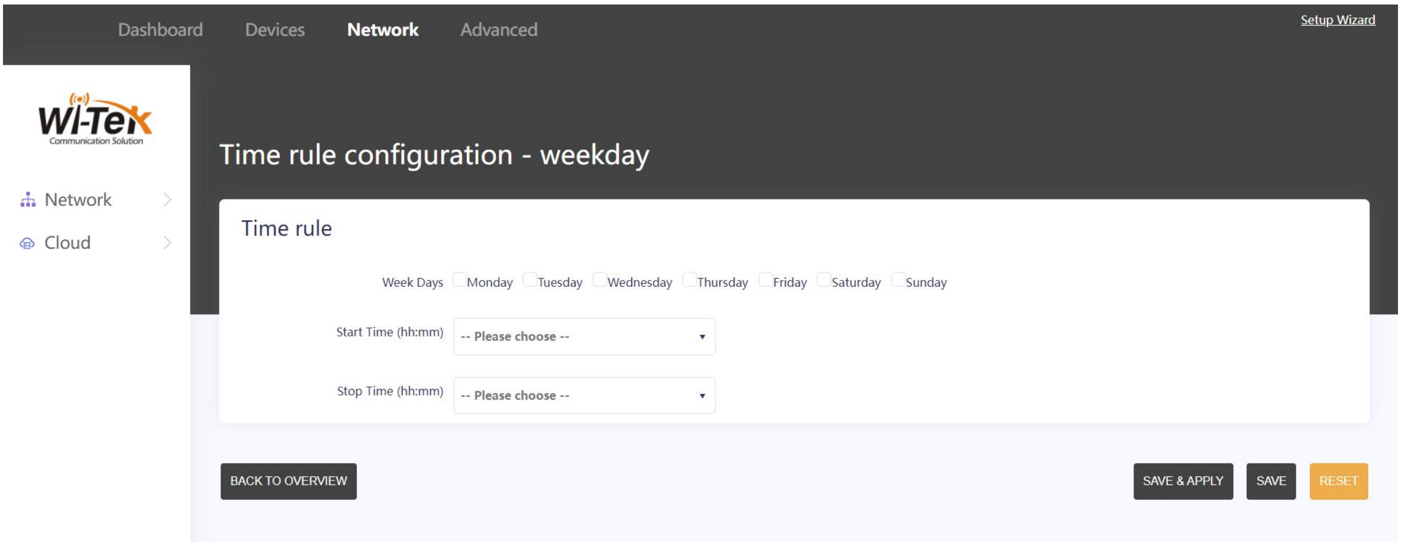
Name	Hostname	IPv4-Address	MAC-Address	Deny client	Time rule	Upload limit(KB/s)	Download limit(KB/s)
1	-	-	-	No	-	-	-

Time rule

Name	Week Days	Start Time (hh:mm)	Stop Time (hh:mm)
weekday	Monday Tuesday Wednesday Thursday Friday	09:00	18:00
weekend	Saturday Sunday	09:00	18:00

Setup steps

Setup1 Edit time rules, and by default, there are two time rules: "weekday" and "weekend" Click "Edit" to set the time rules you want.



Time rule configuration - weekday

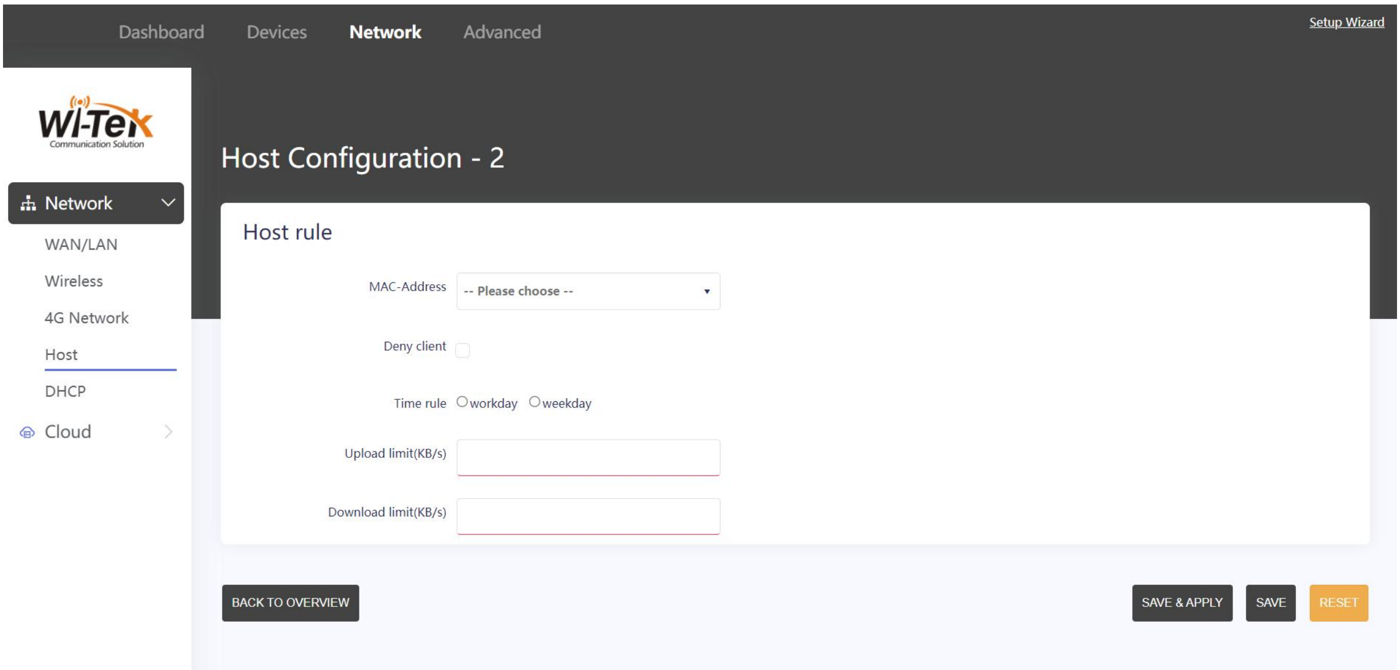
Time rule

Week Days □Monday □Tuesday □Wednesday □Thursday □Friday □Saturday □Sunday

Start Time (hh:mm) -- Please choose --

Stop Time (hh:mm) -- Please choose --

Setup2 Edit the Internet access rules of the connected terminal.



Host Configuration - 2

Host rule

MAC-Address -- Please choose --

Deny client □

Time rule ○workday ○weekday

Upload limit(KB/s)

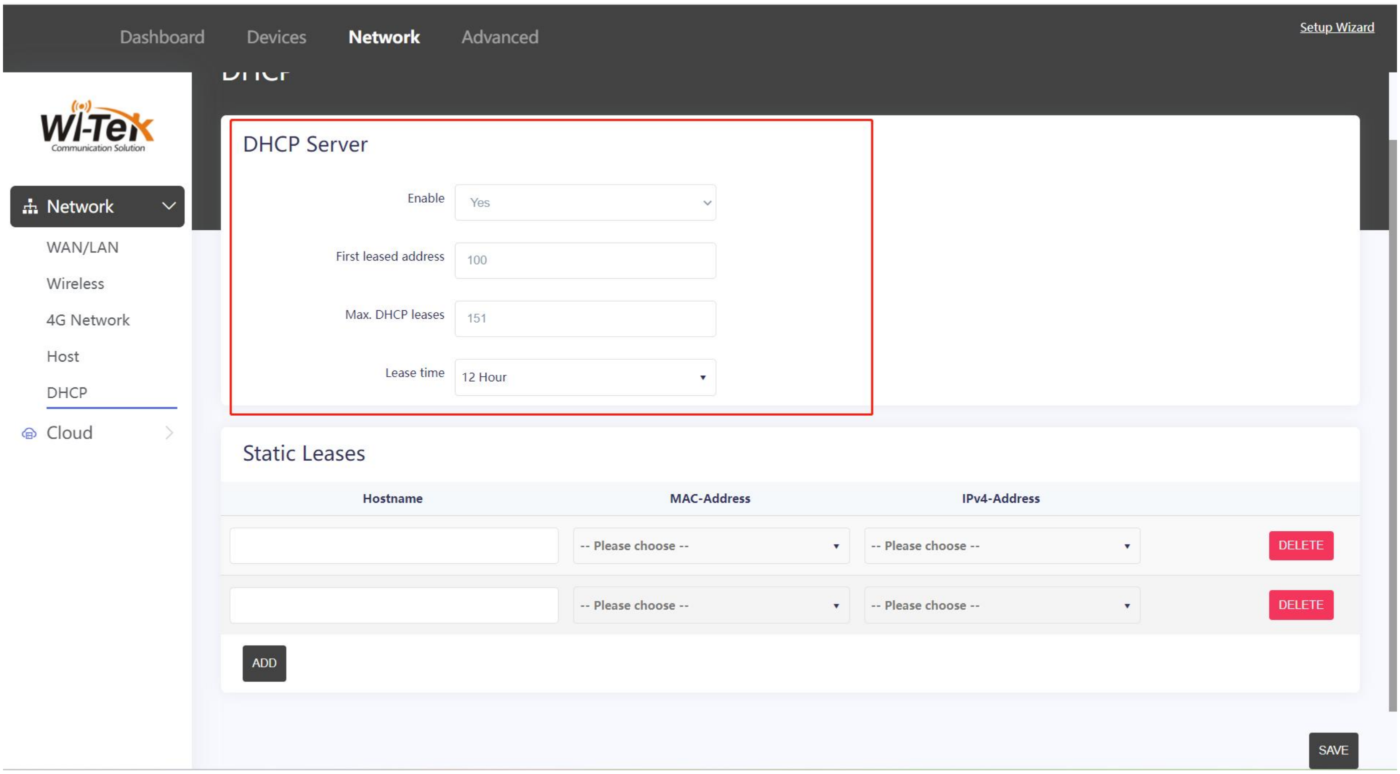
Download limit(KB/s)

Parameter	Describe
MAC-Address	Select the connected terminal device based on the MAC address.
Deny client	When "Deny client" is enabled, the end device will not be able to access the Internet during the time rule you selected. When the time is not within the time limit of the rule, the terminal device can access the Internet.
Time rule	Select a time rule.

Upload limit(KB/s)	The maximum uplink rate is limited in KB/s, and the number "0" indicates that the limit is not required.
Download limit(KB/s)	The maximum downlink rate is limited in KB/s, and the number "0" is set to indicate that the limit is not limited.

3.5. DHCP

On the“DHCP Server”DHCP Server page, you can set the parameters of the DHCP server.



DHCP Server

Enable: Yes

First leased address: 100

Max. DHCP leases: 151

Lease time: 12 Hour

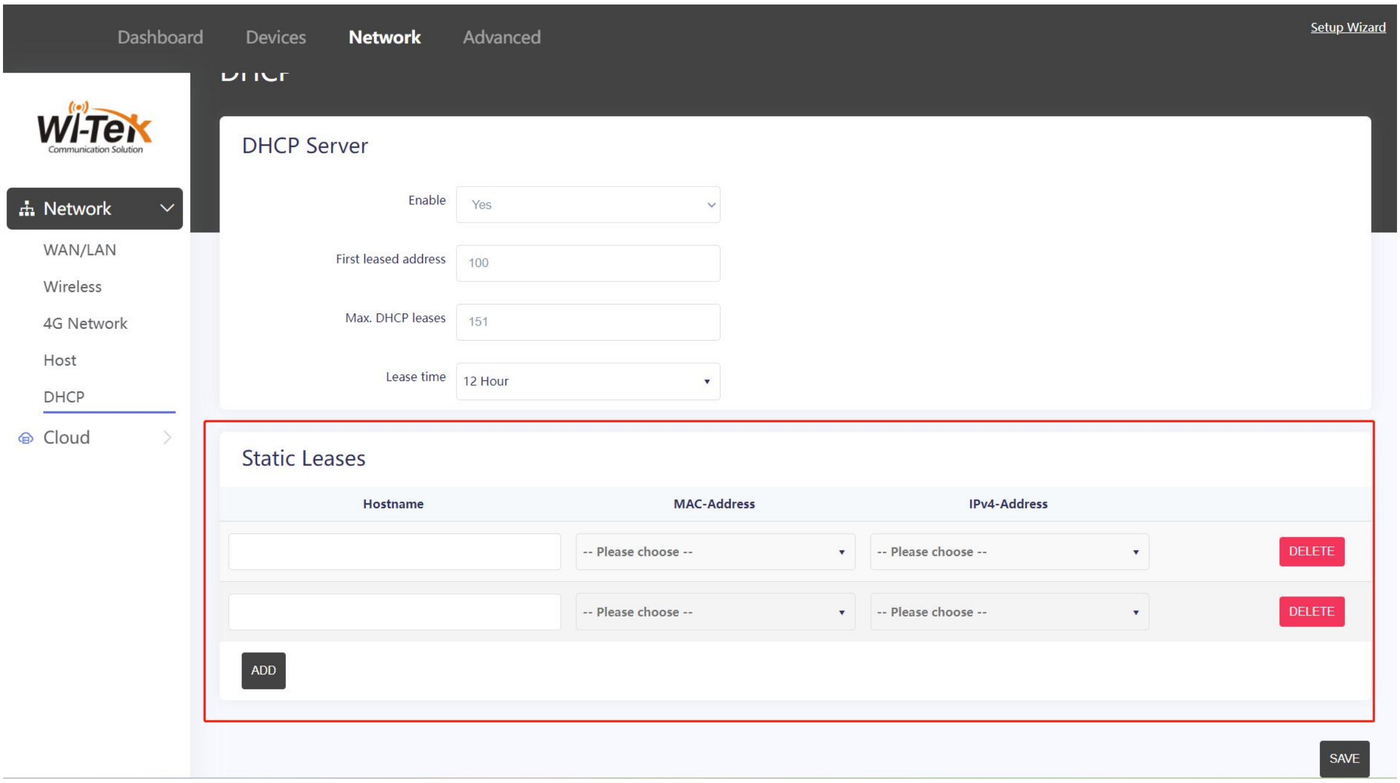
Static Leases

Hostname	MAC-Address	IPv4-Address	
	-- Please choose --	-- Please choose --	DELETE
	-- Please choose --	-- Please choose --	DELETE

Parameter	Describe
Enable	Enable or disable the DHCP server.It is enable by default.
First leased address	Specify an IP address for the DHCP Server to start with when assigning IP addresses.

Max. DHCP leases	Specify the range of IP addresses assigned by DHCP server.
Lease time	Specify the lease time of the IP address assigned to the user.When time is up, the router will automatically assign the same IP address to the user.The default value is 12 hour.

On the “Static Leases ” page, you can select the device that needs to be bound to a static IP address according to the MAC address, and after binding a static IP address, the corres ponding host will obtain the bound IP address every time you connect.



DHCP Server

Enable: Yes

First leased address: 100

Max. DHCP leases: 151

Lease time: 12 Hour

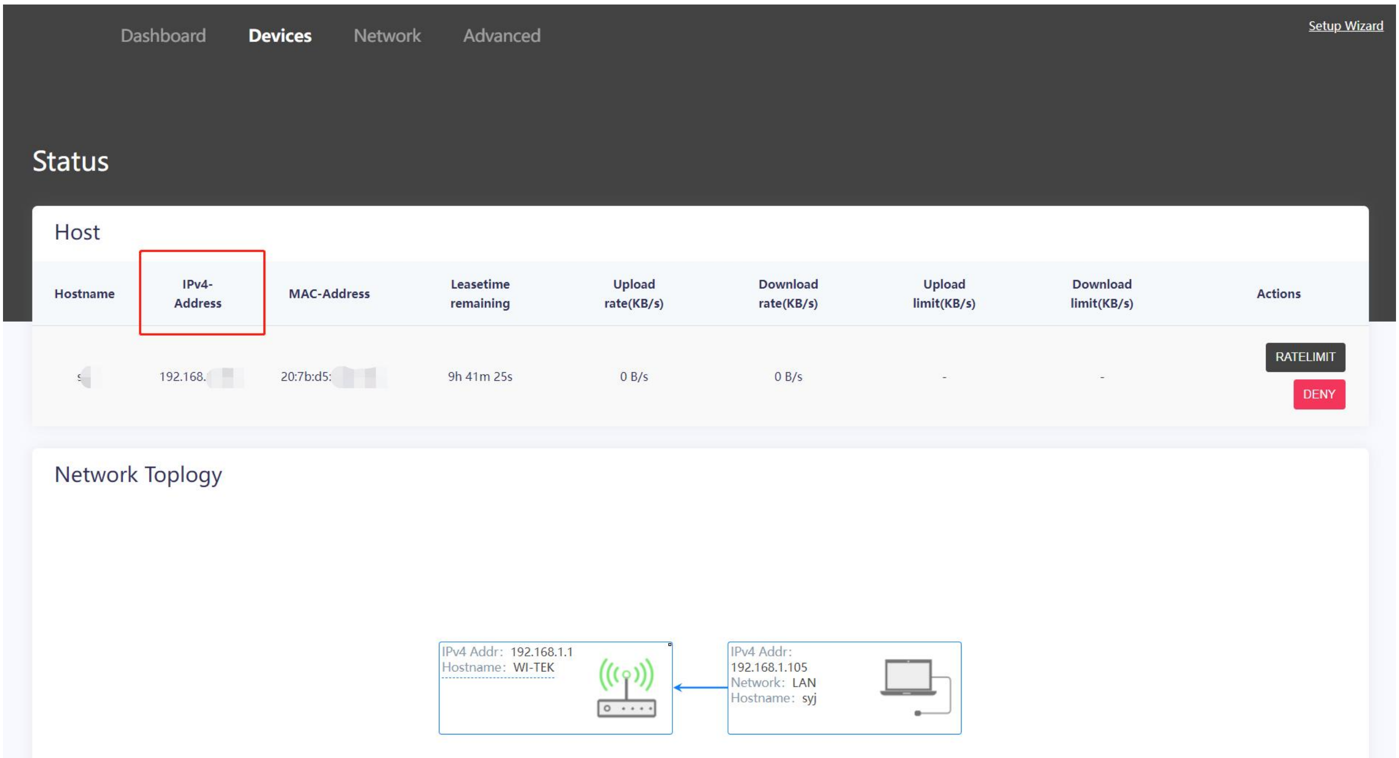
Static Leases

Hostname	MAC-Address	IPv4-Address	
	-- Please choose --	-- Please choose --	DELETE
	-- Please choose --	-- Please choose --	DELETE

ADD

SAVE

Click "Devices" to view the IP information of the connected terminal and the connection diagram.



Status

Host

Hostname	IPv4-Address	MAC-Address	Leasetime remaining	Upload rate(KB/s)	Download rate(KB/s)	Upload limit(KB/s)	Download limit(KB/s)	Actions
s[redacted]	192.168.[redacted]	20:7b:d5:[redacted]	9h 41m 25s	0 B/s	0 B/s	-	-	RATELIMIT DENY

Network Toplogy

IPv4 Addr: 192.168.1.1
Hostname: WI-TEK

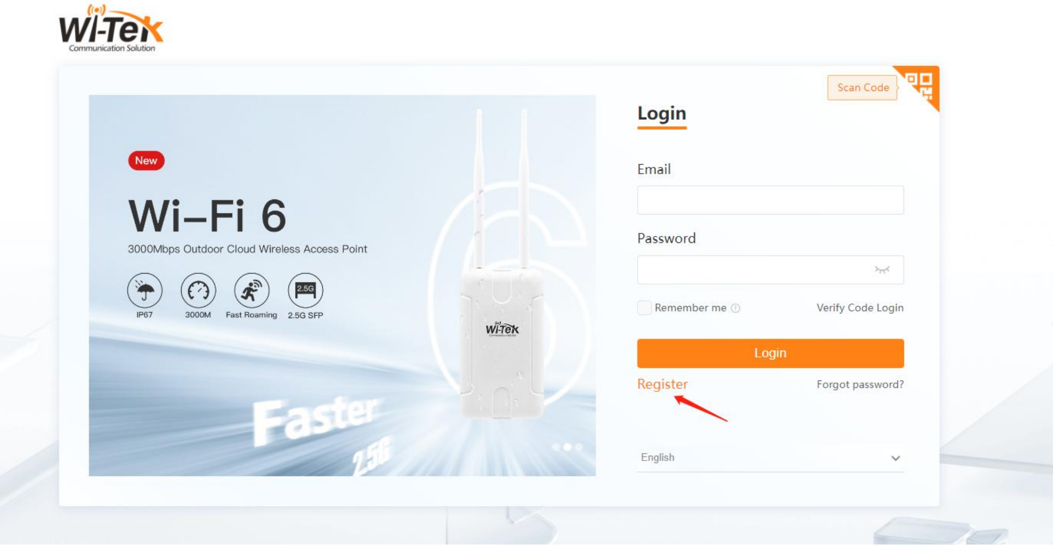
IPv4 Addr: 192.168.1.105
Network: LAN
Hostname: syj

3.6. Cloud management

The 4G router can be bound to the Wi-Tek cloud platform for management, and functions such as configuration delivery and intranet penetration can be realized on the cloud platform, which is convenient for centralized management.

Setup steps

Step1 Open the Wi-Tek cloud platform link cloud2.wireless-tek.com



Login

Email

Password

□ Remember me

Verify Code Login

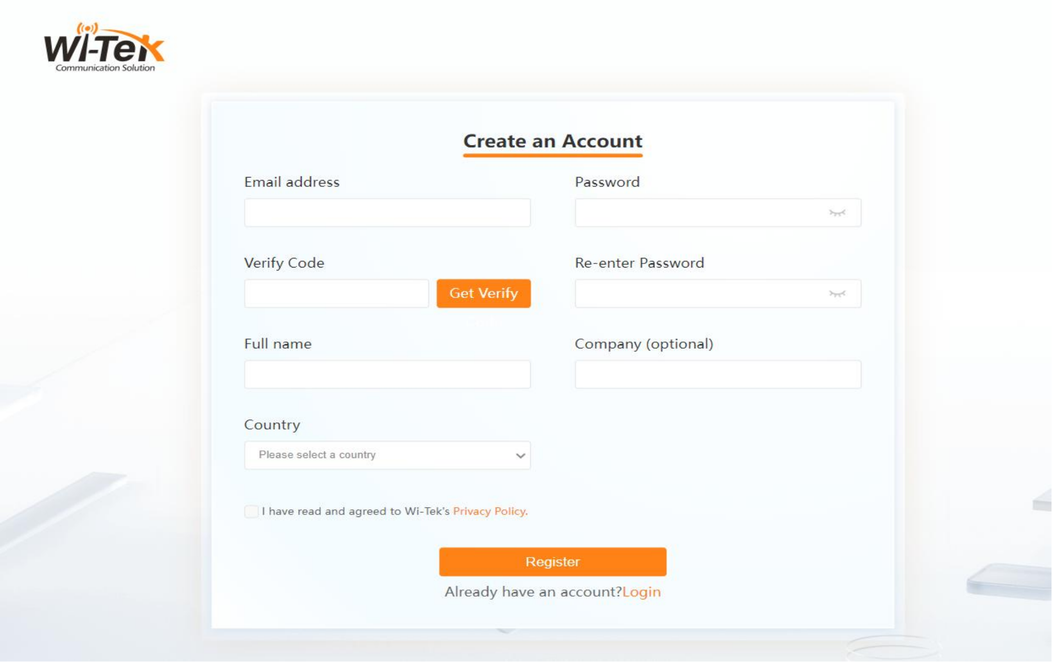
Login

Register

Forgot password?

English

Step2 Sign up for a Wi-Tek cloud account.



Create an Account

Email address

Password

Verify Code

Re-enter Password

Full name

Company (optional)

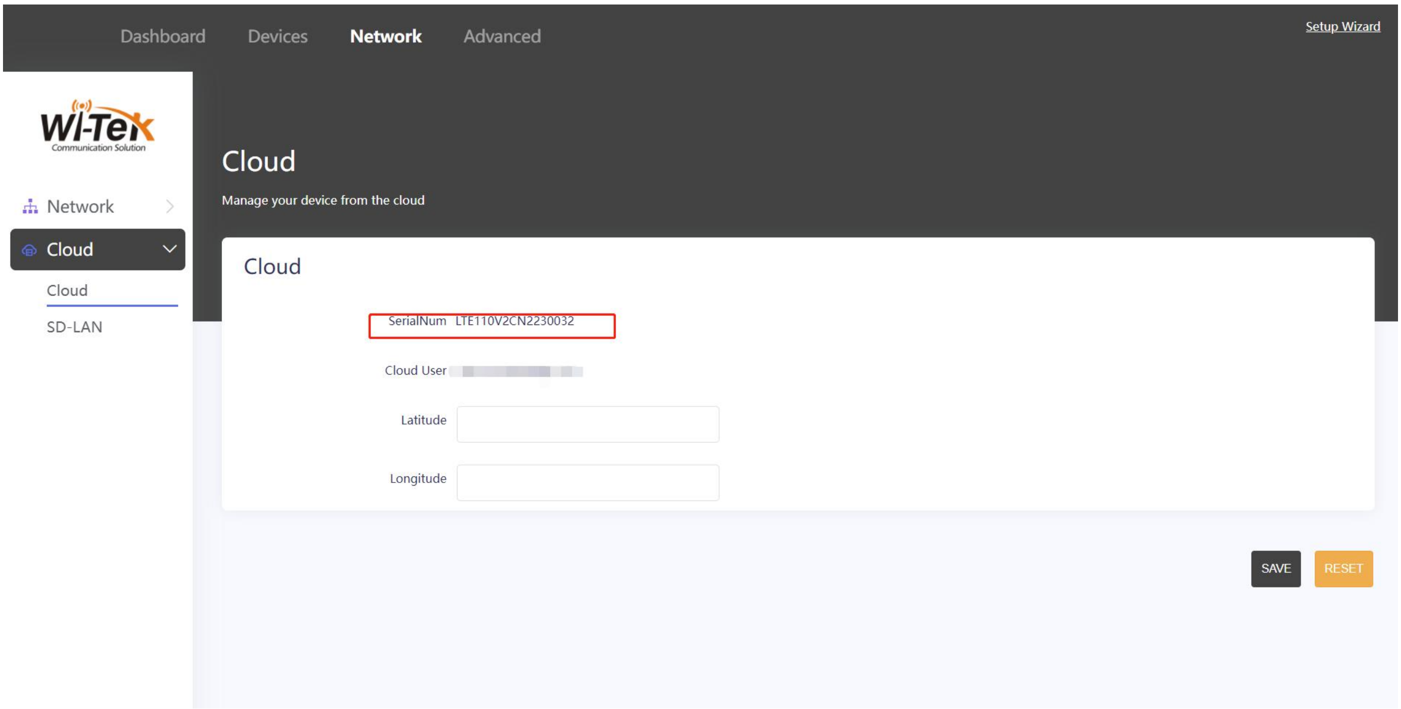
Country

Please select a country

□ I have read and agreed to Wi-Tek's Privacy Policy.

Already have an account?Login

Step3 Copy the SN code of the 4G router on the web page.



Cloud

Manage your device from the cloud

Cloud

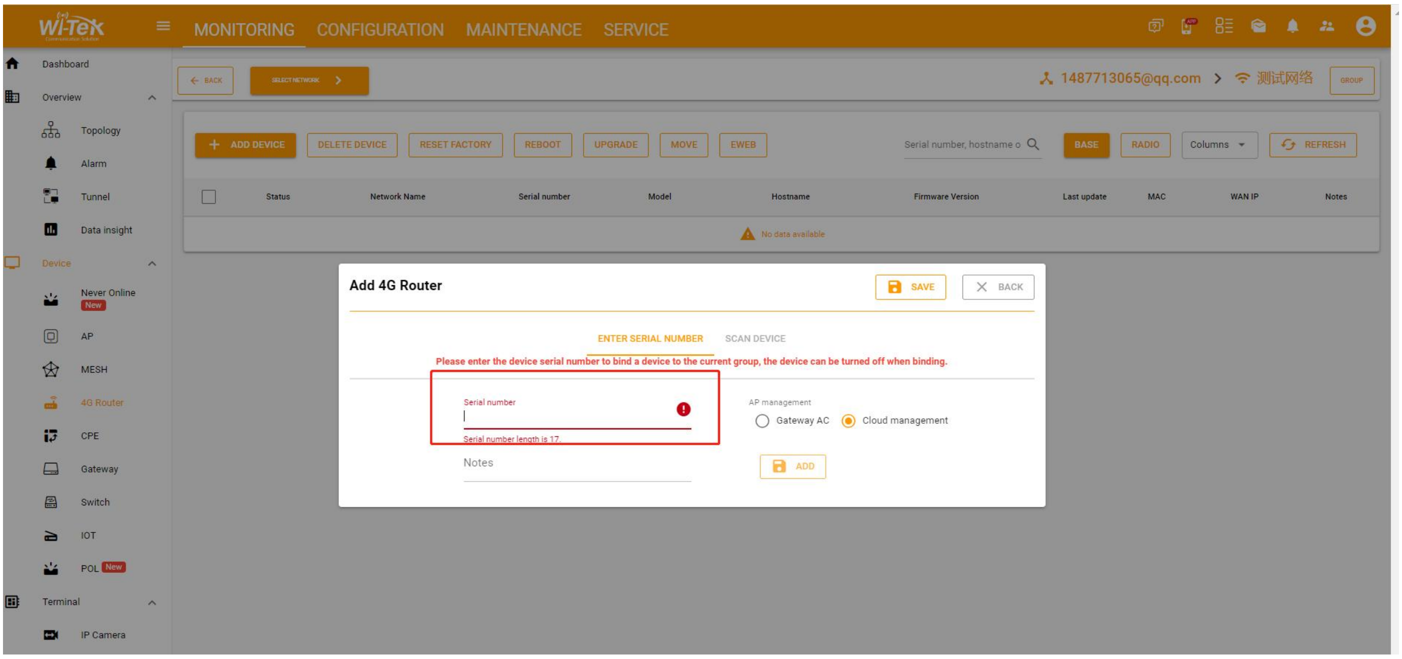
SerialNum LTE110V2CN2230032

Cloud User [redacted]

Latitude

Longitude

Step4 Paste the SN code on the cloud platform to bind the device(For detailed steps, please refer to the Wi-Tek cloud platform user manual).



Add 4G Router

Please enter the device serial number to bind a device to the current group, the device can be turned off when binding.

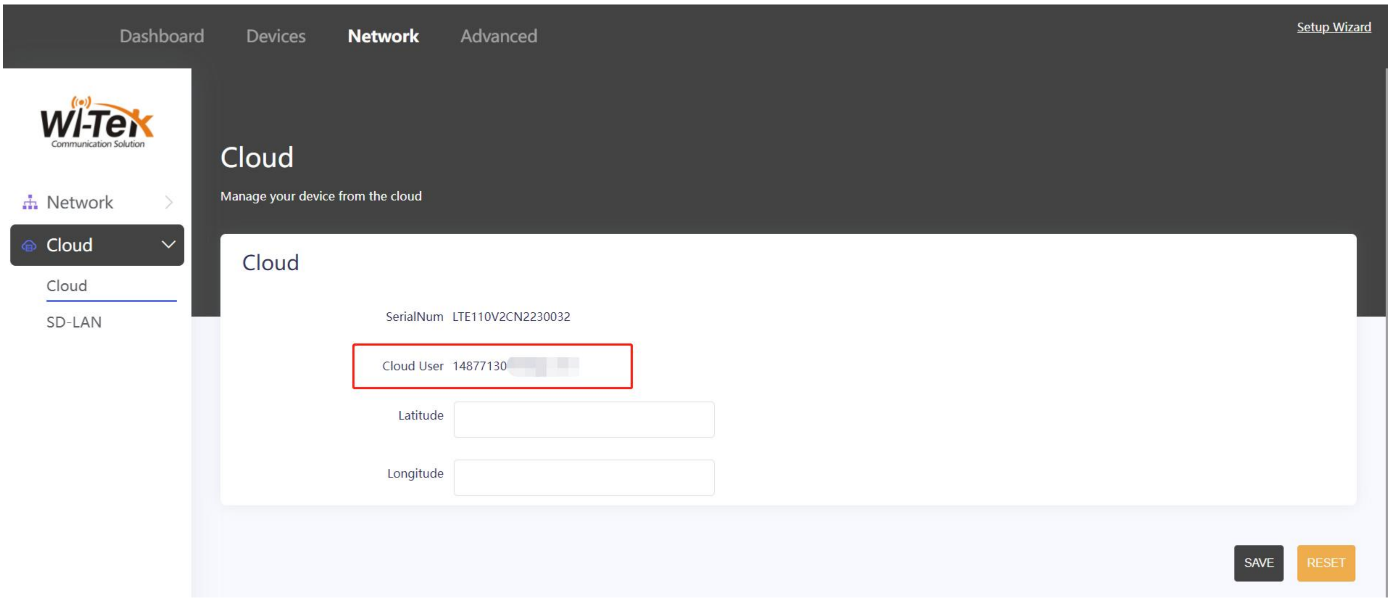
Serial number

Serial number length is 17.

Notes

AP management: ○ Gateway AC ● Cloud management

Step5 After the binding is successful, you can view the bound cloud platform account on the web page (After the binding is successful, the web page login account of the 4G router will be changed to the management account set on the cloud platform).



Cloud

Manage your device from the cloud

Cloud

SerialNum LTE110V2CN2230032

Cloud User 14877130[redacted]

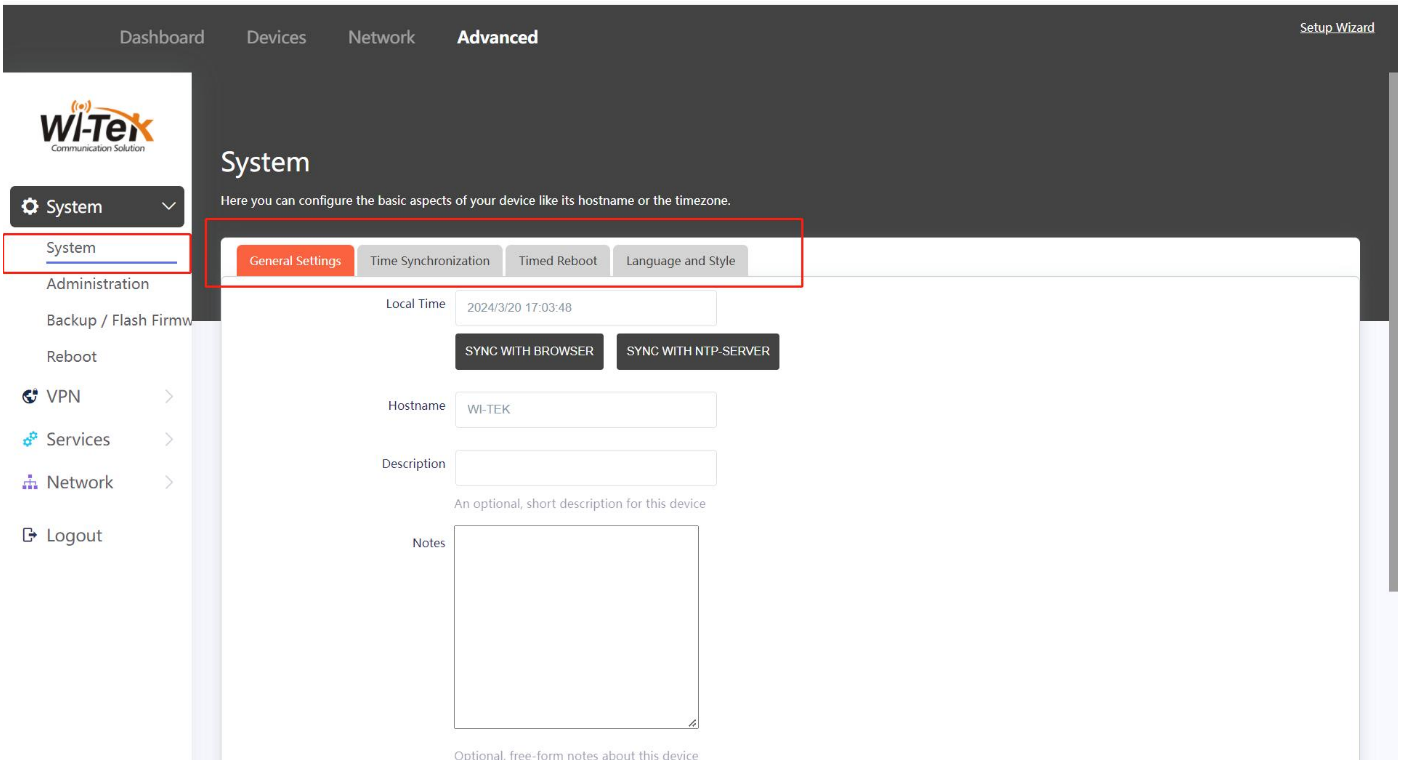
Latitude

Longitude

4. System

4.1. System

Click “Advanced”> “System”>“General Settings”. Here you can configure the basic aspects of your device like its hostname or the timezone.



System

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

Local Time: 2024/3/20 17:03:48

Hostname: WI-TEK

Description:

An optional, short description for this device

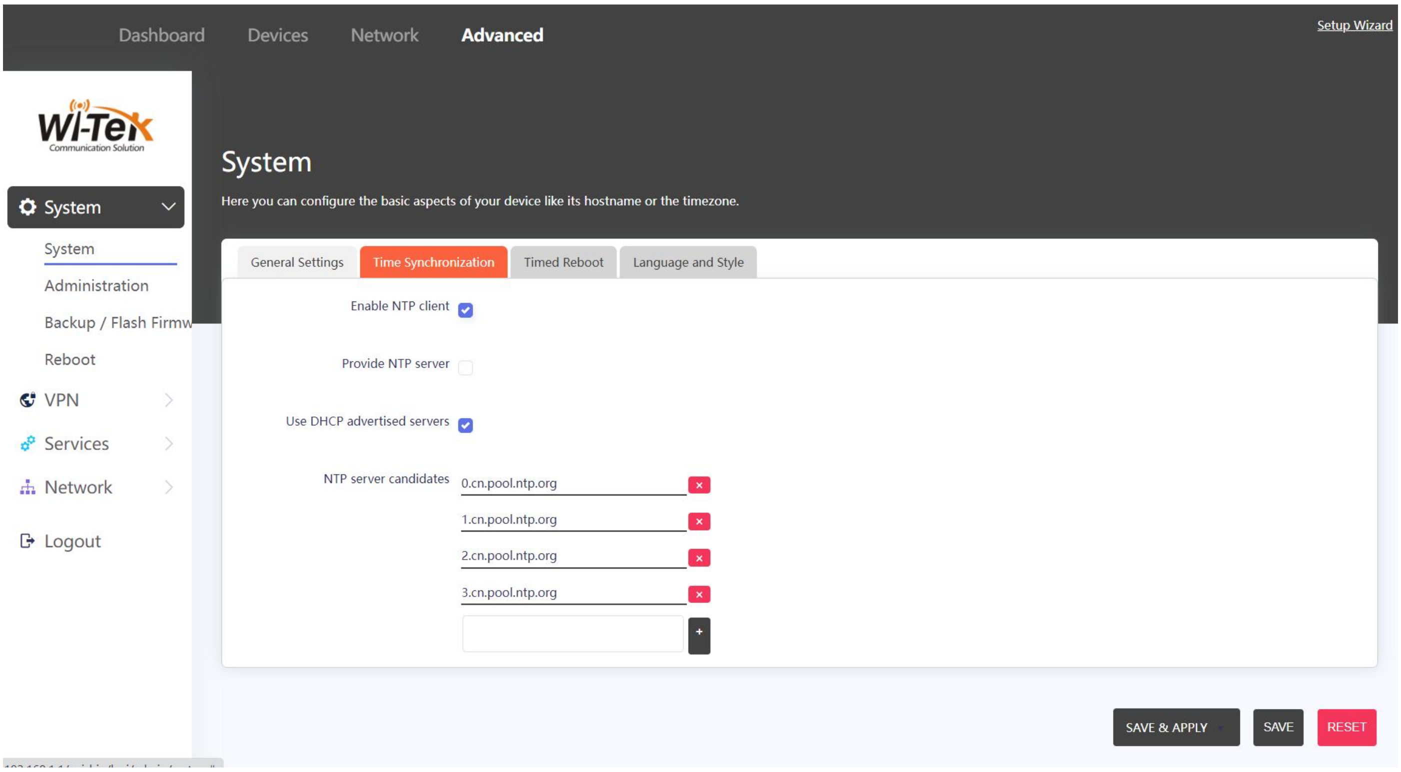
Notes:

Optional, free-form notes about this device

Parameter	Describe
Local Time	Displays the time of the device, you can choose the time to synchronize the browser or the time to synchronize the NTP server.
Host name	You can set the name of the device, which is WI-TEK by default.
Description	An optional, short description for this device.

Notes	Optional, free-form notes about this device.
Timezone	You can select the time zone in which the device is located.
Country	Different countries can be selected.

Click “Advanced”> “System”>“Time Synchronization”.You can set the device as an NTP client to synchronize the time on the NTP server.



System

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

Enable NTP client ☑

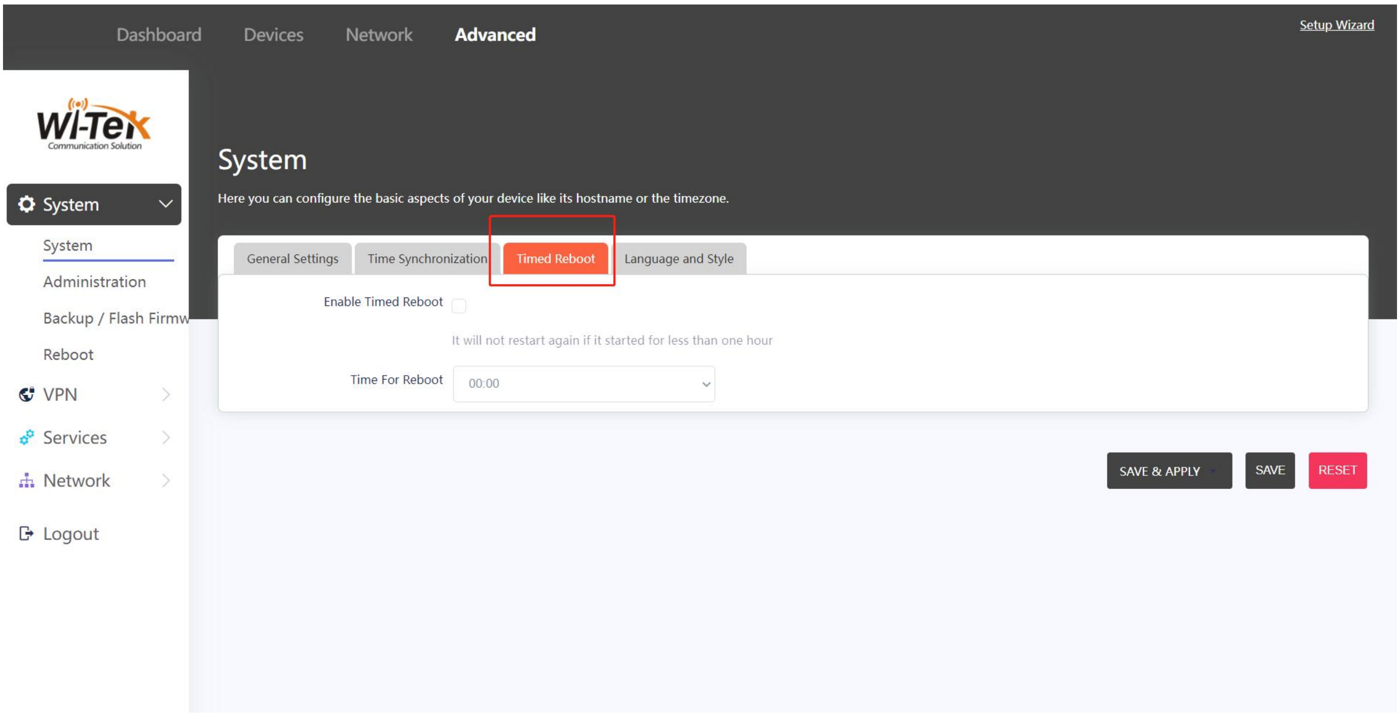
Provide NTP server □

Use DHCP advertised servers ☑

NTP server candidates
- 0.cn.pool.ntp.org
- 1.cn.pool.ntp.org
- 2.cn.pool.ntp.org
- 3.cn.pool.ntp.org

Click “Advanced”> “System”>“Timed Reboot”.Enable the scheduled restart function and set the time to restart every day, and the device will restart at this time every day.

Note :It will not restart again if it started for less than one hour.



System

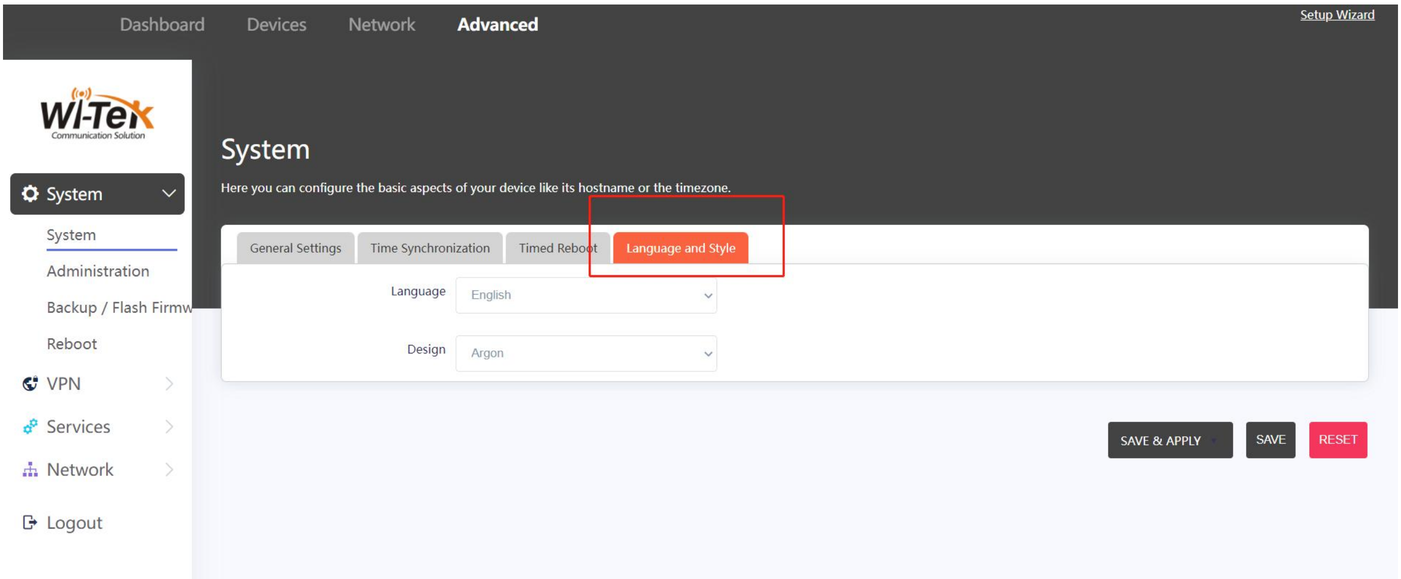
Here you can configure the basic aspects of your device like its hostname or the timezone.

Enable Timed Reboot □

It will not restart again if it started for less than one hour

Time For Reboot 00:00

Click “Advanced”> “System”>“Language and Style”. Set the language of the web page, there are three options: automatic, English, and Chinese.



System

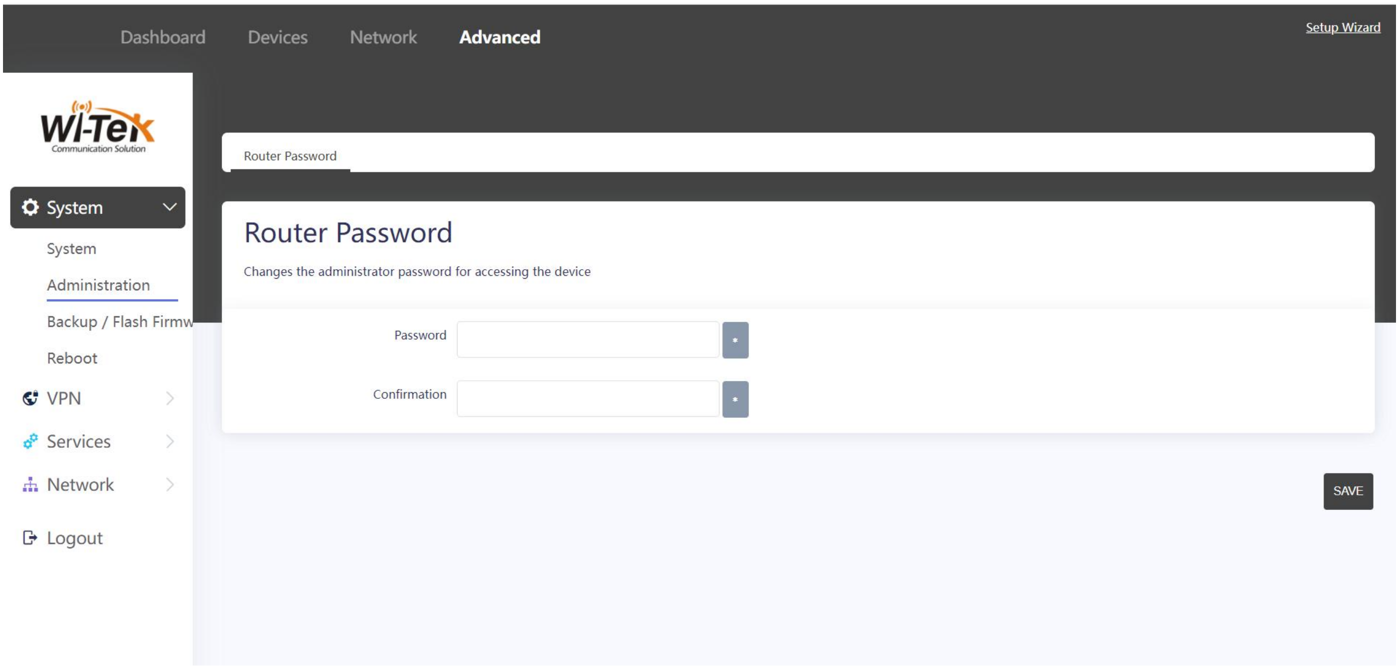
Here you can configure the basic aspects of your device like its hostname or the timezone.

Language English

Design Argon

4.2. Administration

Click “Advanced”> “System”>“Administration”,here you can change your login password.



Router Password

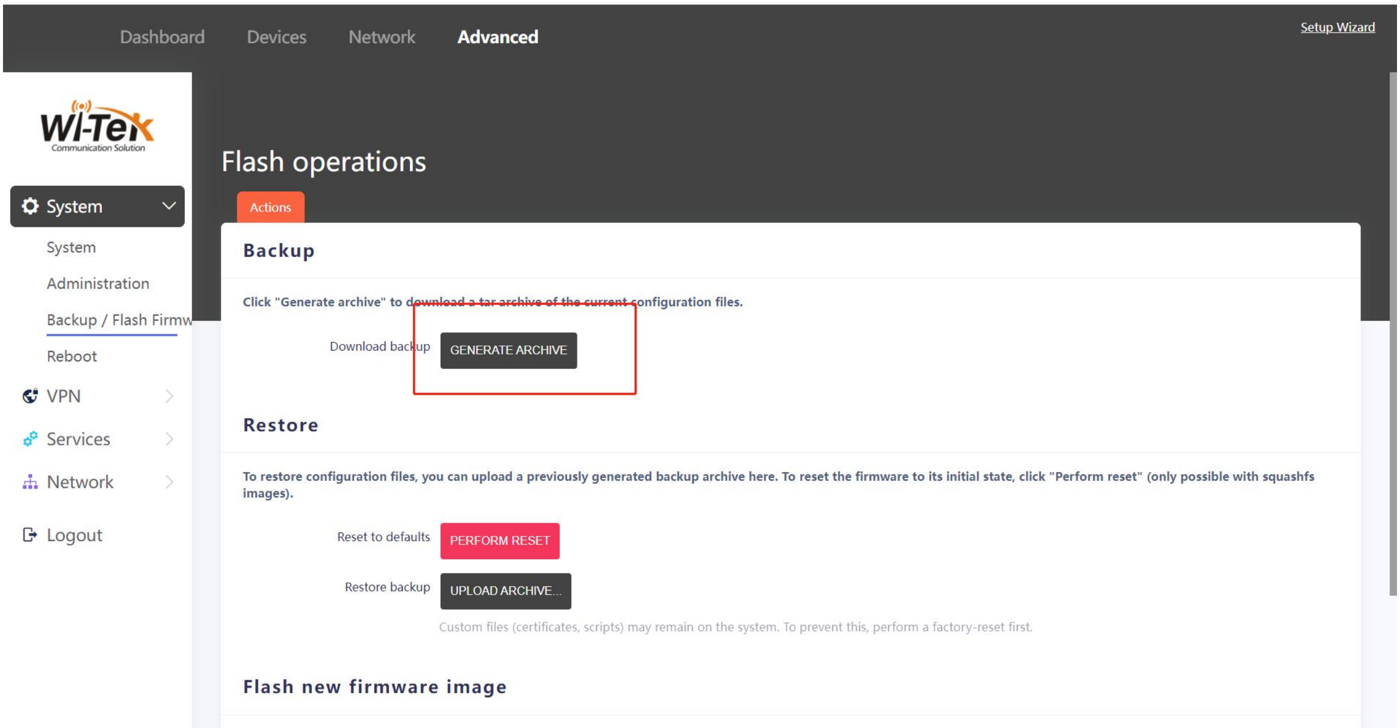
Changes the administrator password for accessing the device

Password

Confirmation

4.3. Backup/Flash firmware

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



Backup

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

Download backup

Restore

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

Reset to defaults

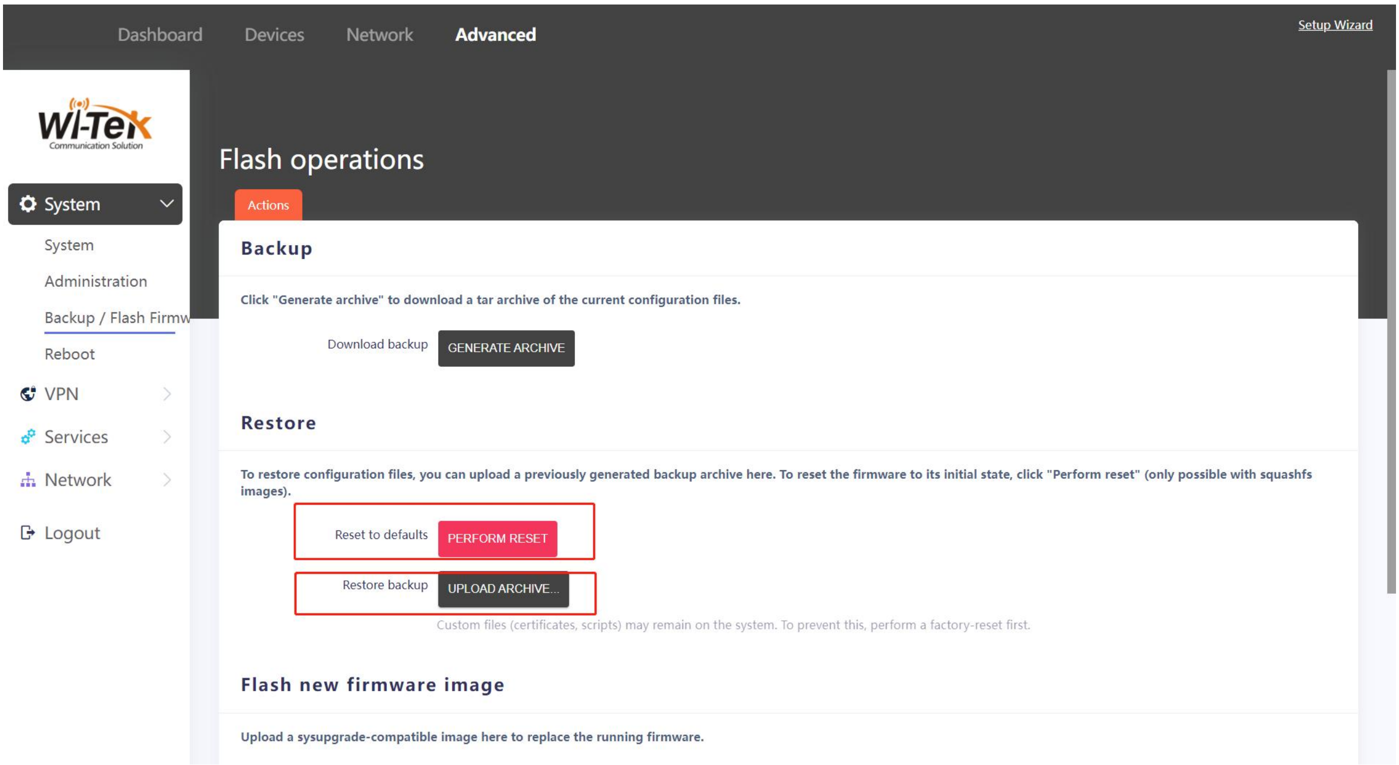
Restore backup

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

Flash new firmware image

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 im ages).

Note: When you upload a configuration document, custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory reset first.



Flash operations

Backup

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

Download backup

Restore

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

Reset to defaults

Restore backup

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

Flash new firmware image

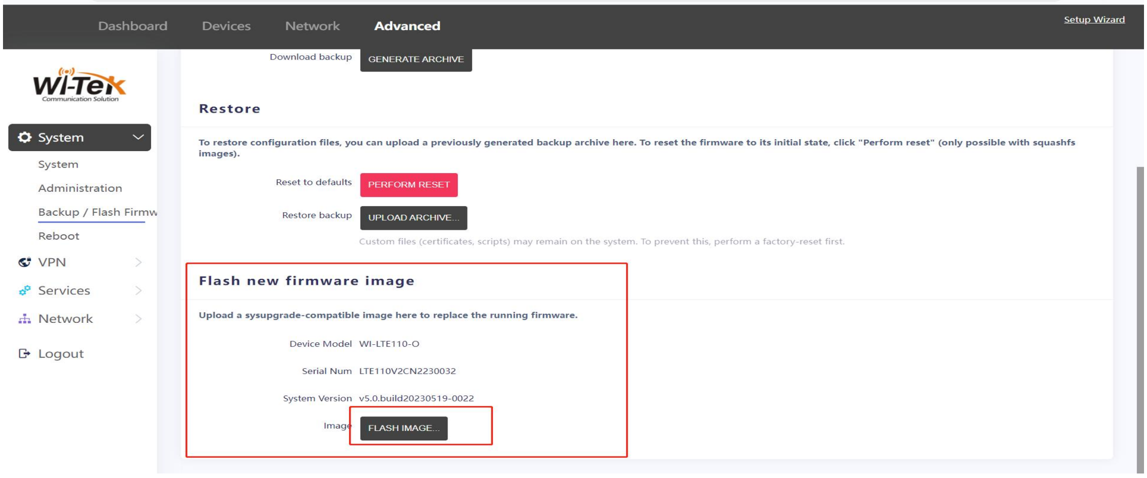
Upload a sysupgrade-compatible image here to replace the running firmware.

On the "**Flash new firmware image**" page, you can view the device model, SN code, and firmware version. The firmware of the device can also be upgraded.

Steps to perform a firmware upgrade.

Step1 Download the latest firmware from Wi-Tek official.

Step2 Click "FLASH IMAGE" >“BROWSE” Select the firmware you downloaded from the official website.



Download backup

Restore

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

Reset to defaults

Restore backup

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

Flash new firmware image

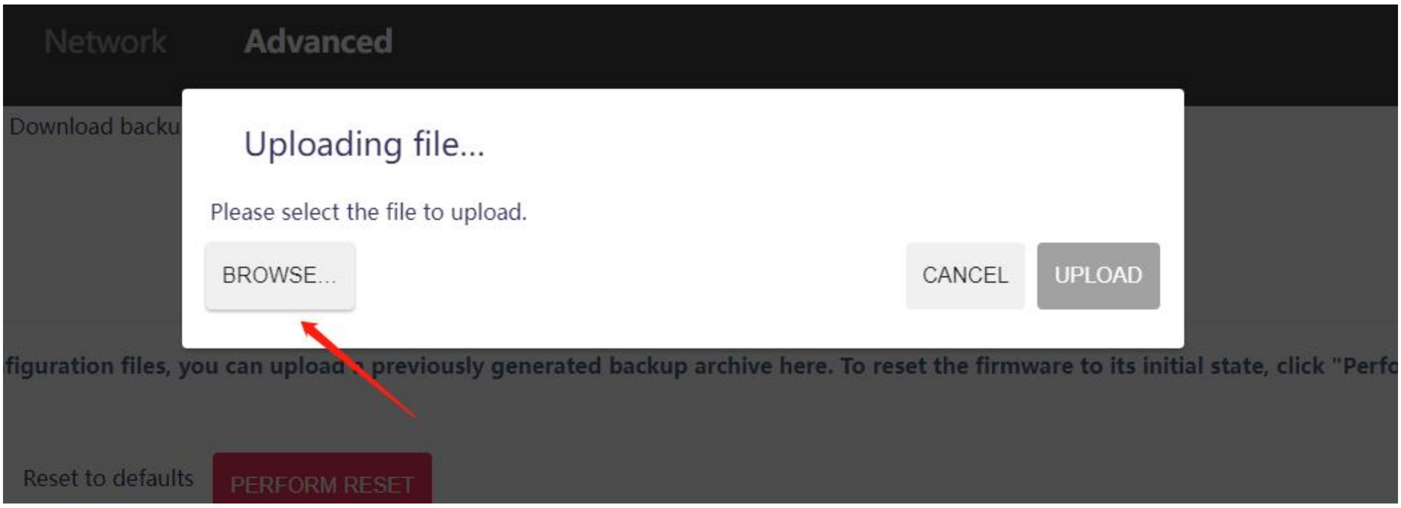
Upload a sysupgrade-compatible image here to replace the running firmware.

Device Model WI-LTE110-O

Serial Num LTE110V2CN2230032

System Version v5.0.build20230519-0022

Image

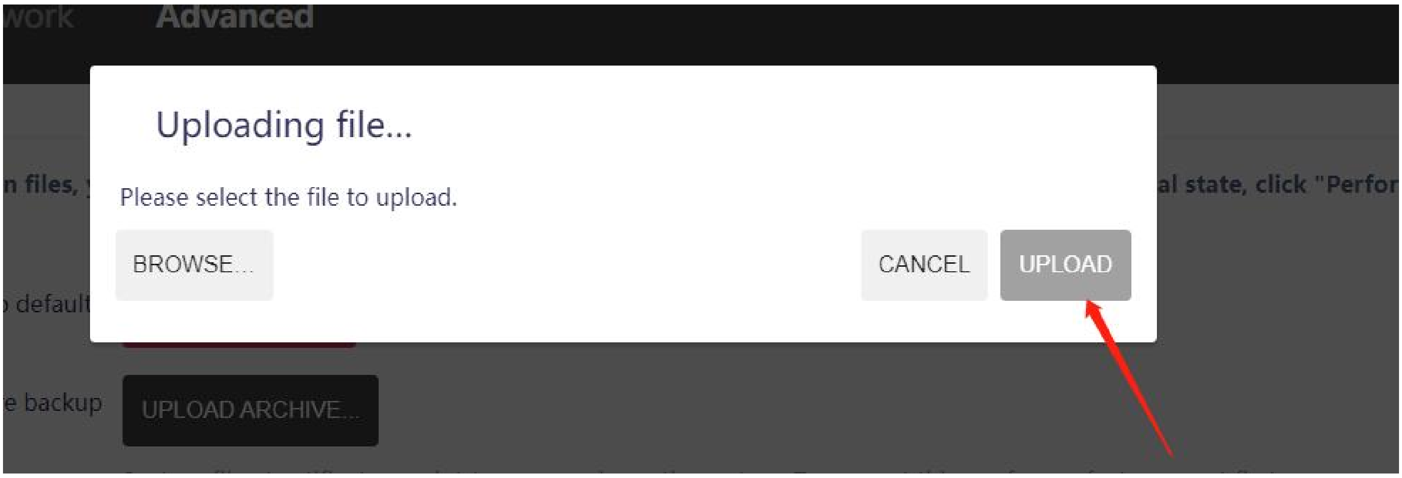


Network
Advanced
Download backu
figuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perfo
Reset to defaults
PERFORM RESET

Uploading file...

Please select the file to upload.

Step 3 Click “**UPLOAD**” Wait for about a minute before the firmware upgrade is successful.

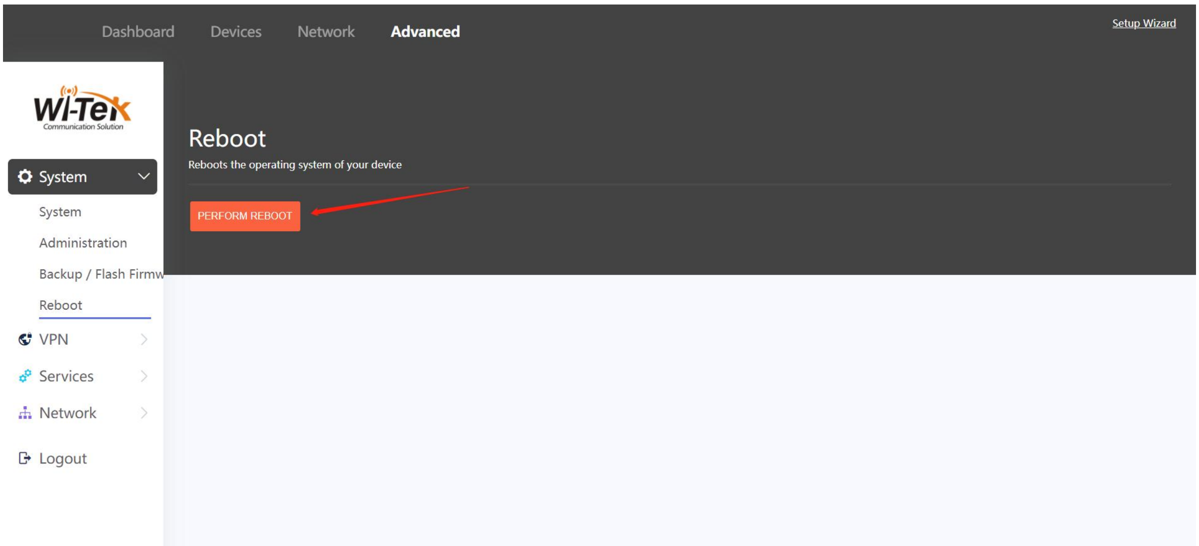


Uploading file...

Please select the file to upload.

4.4. Reboot

Click “Reboot” there will be a restart button, click on it and the device will restart.



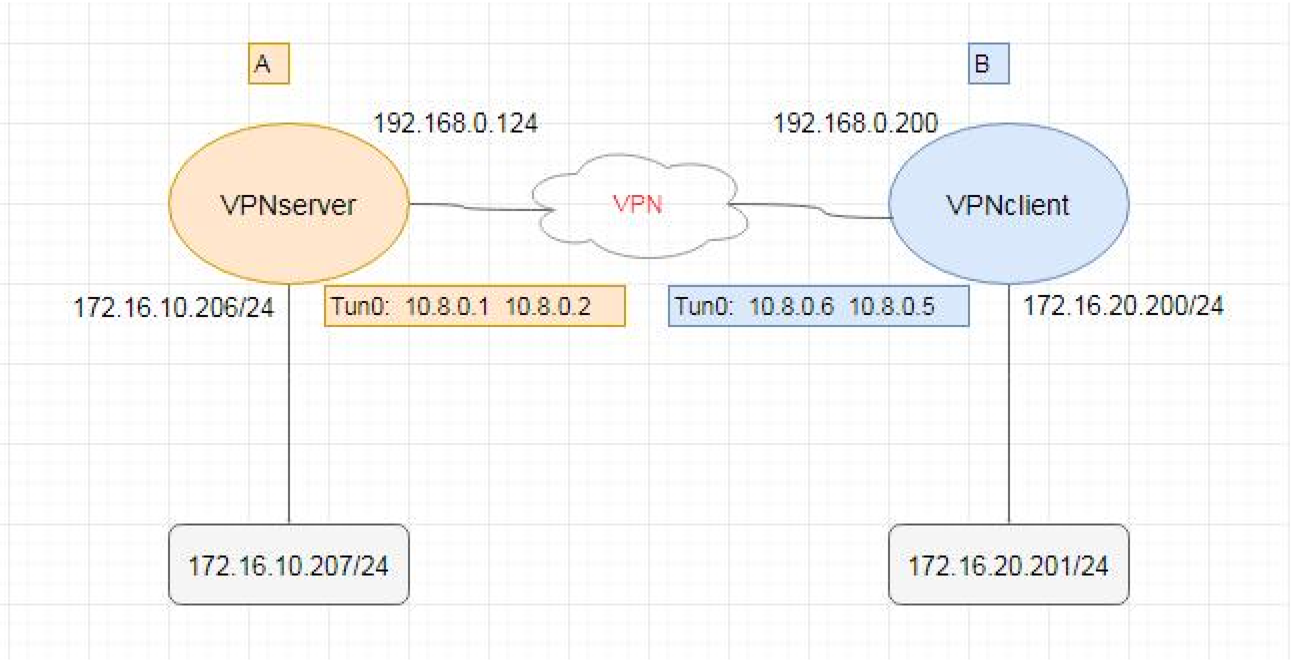
Reboot

Reboots the operating system of your device

5. Open VPN

VPN (Virtual Private Network) is a private network established across the public network, generally via the internet. However, the private network is a logical network without any physical network lines, so it is called Virtual Private Network.

Examples of use cases:
Use Open VPN to build a VPN server to connect two remote networks, A and B, so that segment 172.16.10.0/24 in LAN A and segment 172.16.20.0/24 in LAN B can communicate with each other, just like in a LAN.



Description of the environment:

Use the AC500 gateway as the Open VPN server:
192.168.0.124/24 (Simulated Internet)
172.16.10.206/24 (Intranet)
10.8.0.1 10.8.0.2 (VPN Virtual NIC Address)

Using a 4G router as an Open VPN client:
192.16.0.200/24(Simulated Internet)
172.16.20.201/24 (Intranet)
10.8.0.6 10.8.0.5 (VPN Virtual NIC Address)

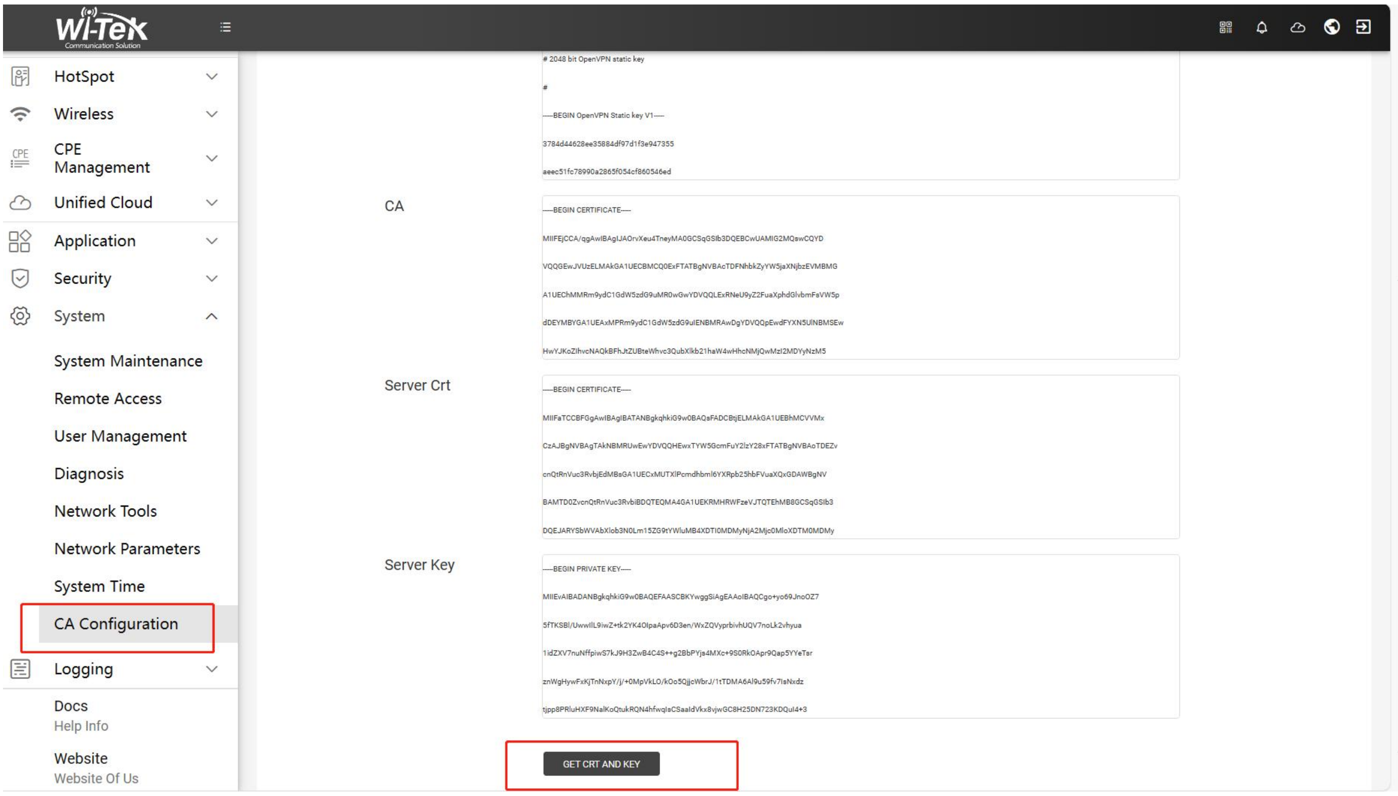
A LAN host 172.16.10.207/24

B LAN host 172.16.20.201/24

Setup steps

Step1

Generate CA certificates, static keys, server certificates, and secret keys according to the gateway's user manual, and the certificates will be automatically configured into the corresponding files after generation, and no manual copy is required.



```
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
3784d44628ee35884df97d1f3e947355
aeec51fc78990a2865f054cf860546ed
```

CA

```
-----BEGIN CERTIFICATE-----
MIIFEjCCA/qgAwIBAgIJAOrvXeu4TneyMA0GCSqGSIb3DQEBCwUAMIG2MQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExFTATBgNVBAcTDFNhbkZyYW5jaXNjbzEVMBMG
A1UEChMMRm9ydC1GdW5zdG9uMR0wGwYDVQQLExRNeU9yZ2FuaXphdGlvbmFsVW5p
dDEYMBYGA1UEAxMPRm9ydC1GdW5zdG9uIENBMRAwDgYDVQQpEwdFYXN5UlNBMSEw
HwYJKoZIhvcNAQkBFhJtZUBteWhvc3QubXlkb21haW4wHhcNMjQwMzI2MDYyNzM5
```

Server Crt

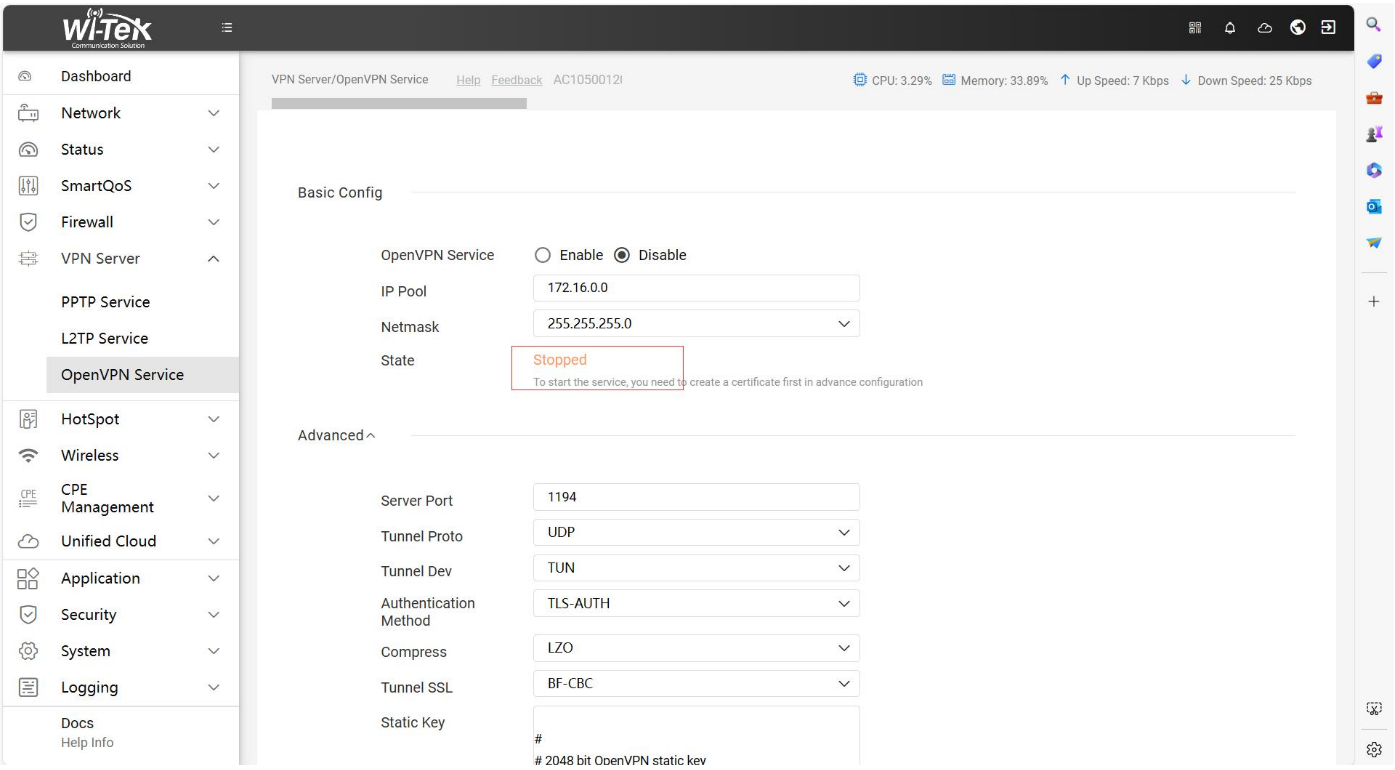
```
-----BEGIN CERTIFICATE-----
MIIFaTCCBFGgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBtjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRUwEwYDVQQHEwxTYW5GcmFuY2lzY28xFTATBgNVBAoTDEZv
cnQtRnVuc3RvbjEdMBsGA1UECxMUTXlPcmdhbml6YXRpb25hbFVuaXQxGDAWBgNV
BAMTD0ZvcnQtRnVuc3RvbiBDQTEQMA4GA1UEKRMHRWFzeVJTQTEhMB8GCSqGSIb3
DQEJARYSbWVAbXlob3N0Lm15ZG9tYWluMB4XDTI0MDMyNjA2Mjc0MloXDTM0MDMy
```

Server Key

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCgo+yo69JnoOZ7
5fTKSBl/UwwlIL9iwZ+tk2YK4OIpaApv6D3en/WxZQVyprbivhUQV7noLk2vhyua
1idZXV7nuNffpiwS7kJ9H3ZwB4C4S++g2BbPYjs4MXc+9S0RkOApr9Qap5YYeTsr
znWgHywFxKjTnNxpY/j/+0MpVkLO/kOo5QjjcWbrJ/1tTDMA6Al9u59fv7IsNxdz
tjpp8PRluHXF9NalKoQtukRQN4hfwqIsCSaaldVkx8vjwGC8H25DN723KDQuI4+3
```

Step2

Configuring the Open VPN Server (please refer to the gateway configuration manual for detailed steps).The push route is based on the actual internal CIDR block of the server, IP: 172.16.10.0, mask: 255.255.255.0. Fill it out. If there are more than one, add them one after the other.Enter the intranet CIDR block in LAN B in the client , and the client name is entered according to the name entered when creating the client certificate, IP: 172.16.20.0 mask: 255.255.255.0. If there are more than one, add them one after the other.

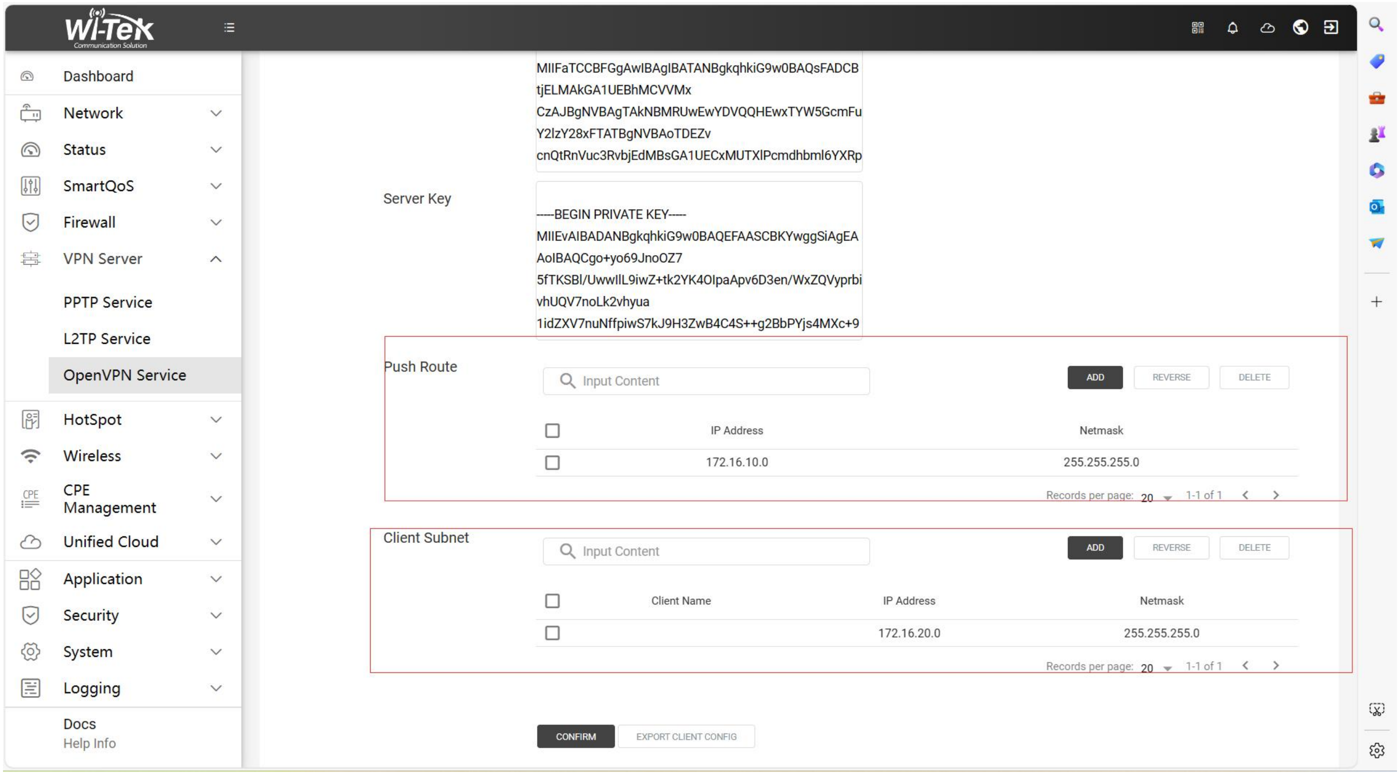


Basic Config

OpenVPN Service	○ Enable ● Disable
IP Pool	172.16.0.0
Netmask	255.255.255.0
State	Stopped To start the service, you need to create a certificate first in advance configuration

Advanced

Server Port	1194
Tunnel Proto	UDP
Tunnel Dev	TUN
Authentication Method	TLS-AUTH
Compress	LZO
Tunnel SSL	BF-CBC
Static Key	# # 2048 bit OpenVPN static kev



```
MIIFaTCCBFGgAwIBAgIBATANBgkqhkiG9w0BAQsFADCB
tjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRUwEwYDVQQHEwxTYW5GcmFu
Y2lzY28xFTATBgNVBAoTDEZv
cnQtRnVuc3RvbjEdMBsGA1UECxMUTXlPcmdhbml6YXRp
```

Server Key

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEA
AoIBAQCgo+yo69JnoOZ7
5fTKSBl/UwwIlL9iwZ+tk2YK4OlpaApv6D3en/WxZQVyprbi
vhUQV7noLk2vhyua
1idZXV7nuNffpiwS7kJ9H3ZwB4C4S++g2BbPYjs4MXc+9
```

Push Route

□	IP Address	Netmask
□	172.16.10.0	255.255.255.0

Records per page: 20 1-1 of 1

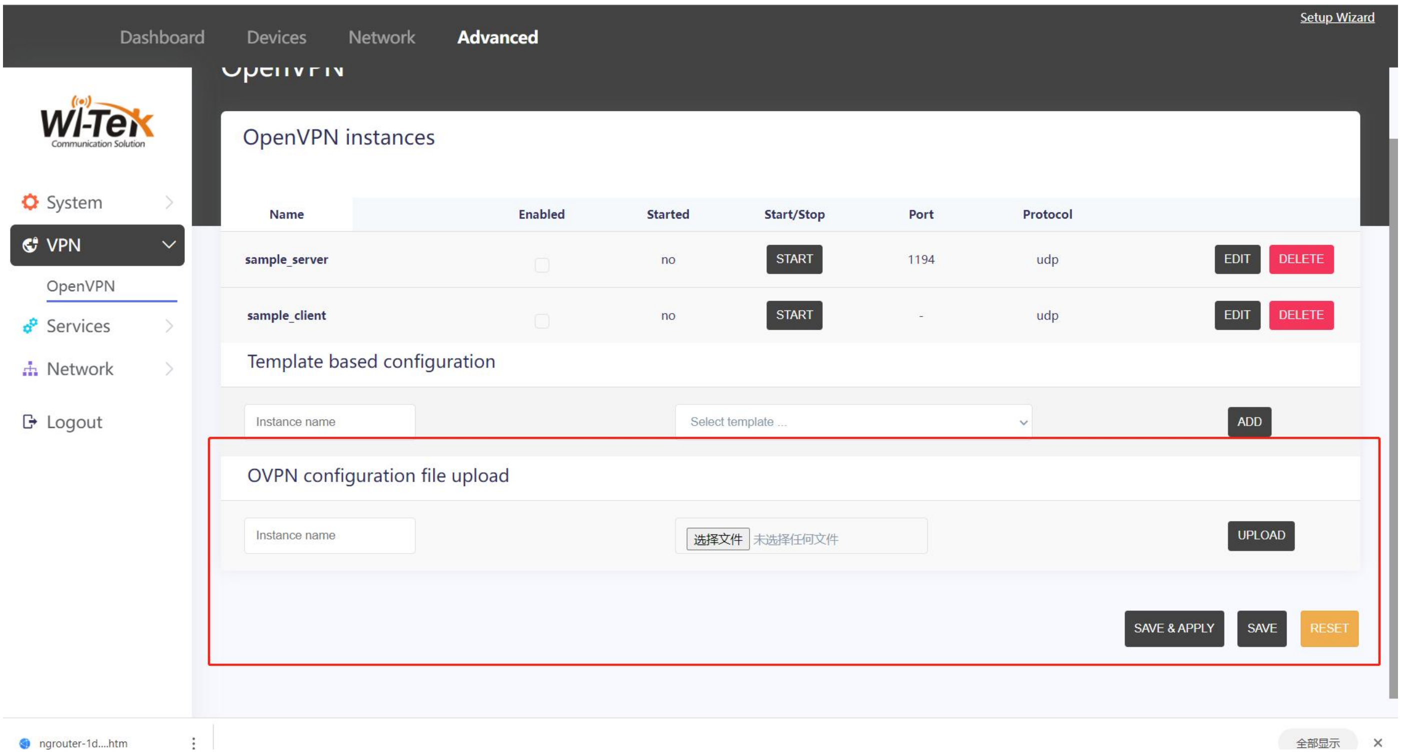
Client Subnet

□	Client Name	IP Address	Netmask
□		172.16.20.0	255.255.255.0

Records per page: 20 1-1 of 1

Step3

Go to the web page of the 4G router and configure the Open VPN client. Select Open VPN configuration file upload, enter the client name, then upload the configuration file downloaded above, and click the upload button.



OpenVPN

OpenVPN instances

Name	Enabled	Started	Start/Stop	Port	Protocol		
sample_server	□	no	START	1194	udp	EDIT	DELETE
sample_client	□	no	START	-	udp	EDIT	DELETE

Template based configuration

Instance name | Select template ... | ADD

OVPN configuration file upload

Instance name | 选择文件 未选择任何文件 | UPLOAD

SAVE & APPLY | SAVE | RESET

Step4

After the configuration is successful, the gateway can communicate with the 4G router.

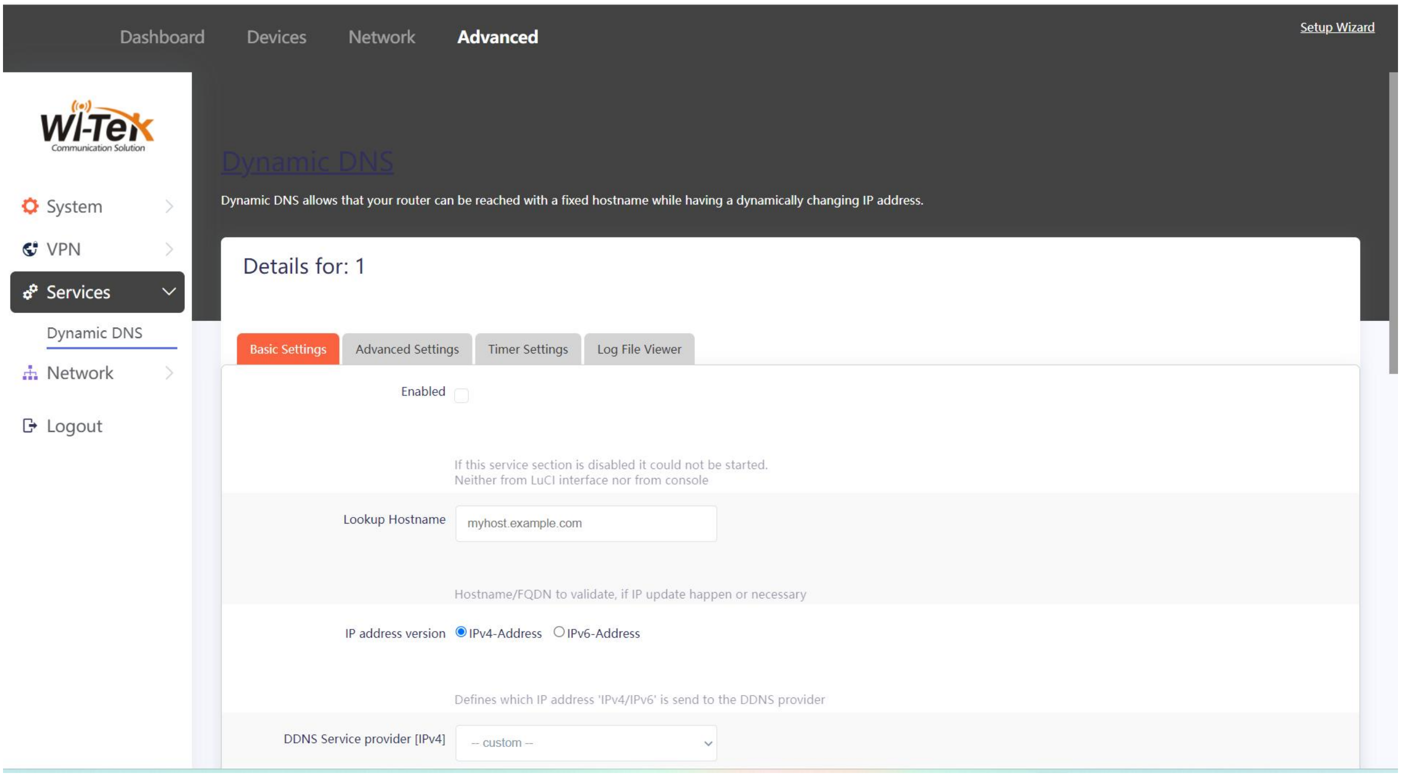
6. Dynamic DNS

Most ISP (internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don’t know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on the router to allow you to access your router and local servers using domain name, in no need of checking and remembering the IP address.

Setup steps

Step1 Register a domain name with a DDNS service provider and obtain a DDNS account.

Step2 Click “Advanced”> “Services”>“Dynamic DNS”>“ADD”, enter the registered domain nae and the account password provided by the service provider, and complete the corresponding configuration as prompted.



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Details for: 1

Enabled □

If this service section is disabled it could not be started.
Neither from LuCI interface nor from console

Lookup Hostname: myhost.example.com

Hostname/FQDN to validate, if IP update happen or necessary

IP address version ● IPv4-Address ○ IPv6-Address

Defines which IP address 'IPv4/IPv6' is send to the DDNS provider

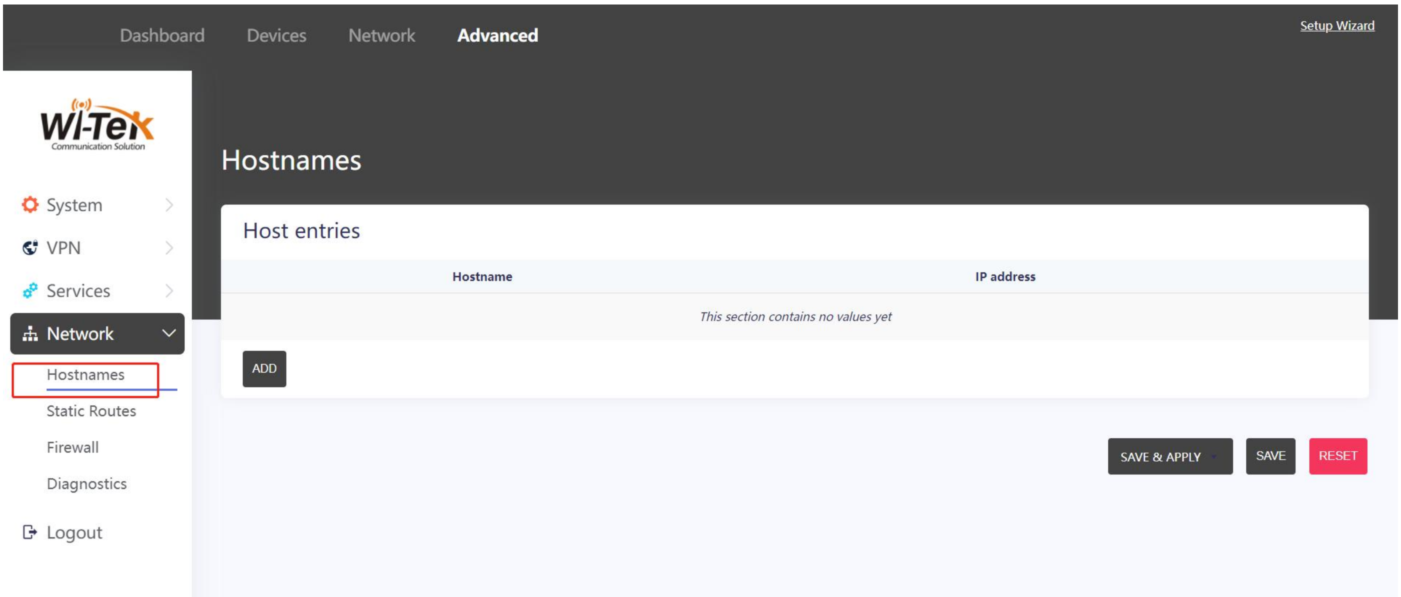
DDNS Service provider [IPv4]: -- custom --

7. Host names

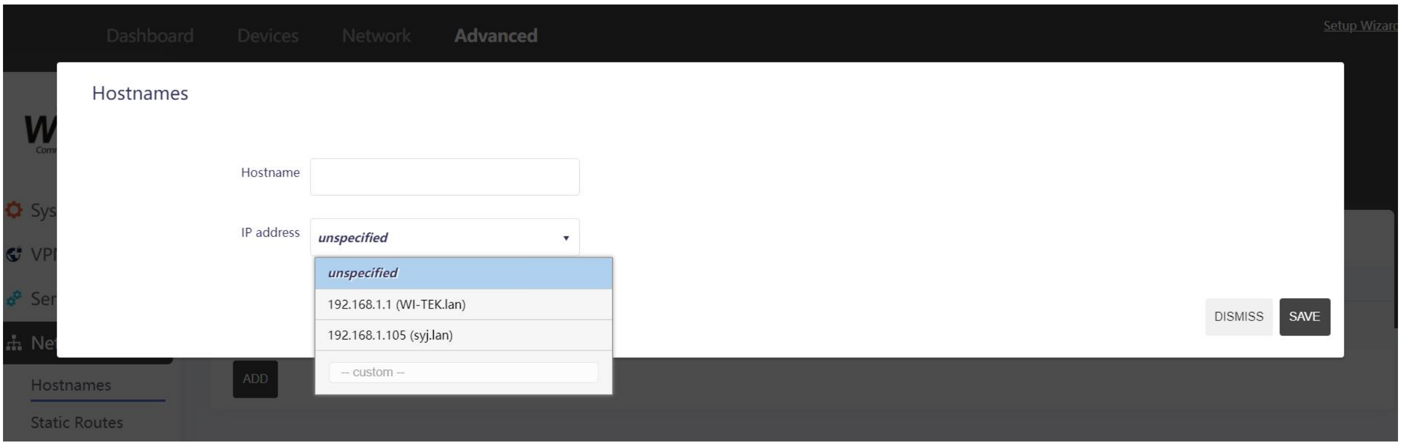
You can associate the IP address of the connected terminal with a custom domain name,within the local area network, the connection terminal can be accessed by domain name.

Setup steps

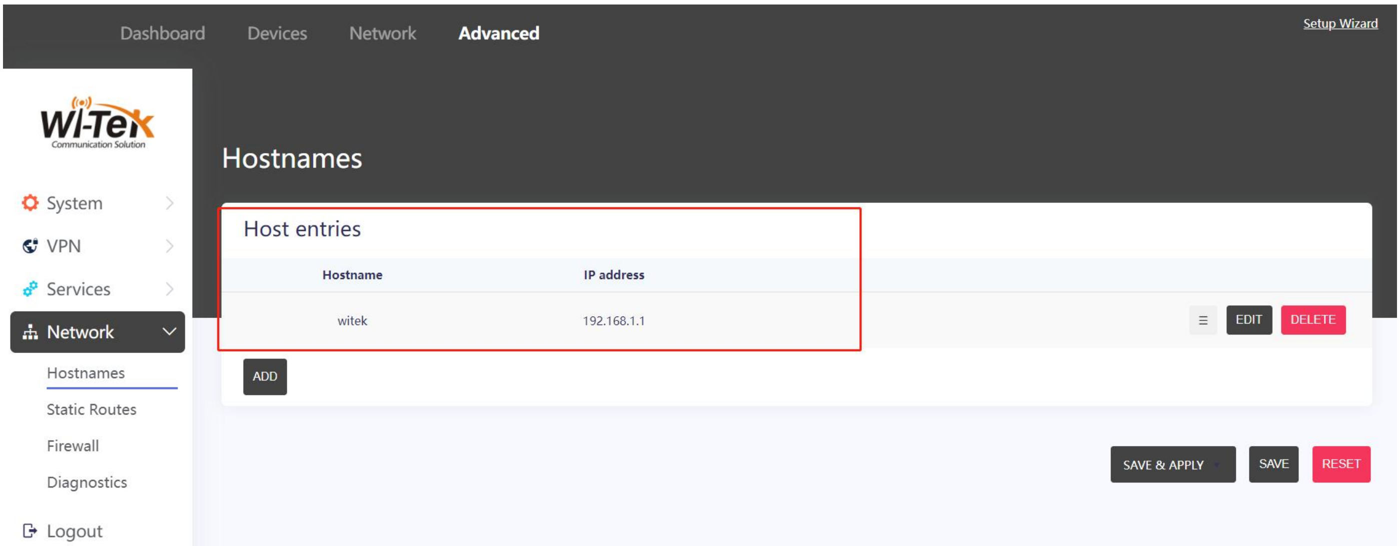
Step1 Click “Advanced”> “Network”>“Host names”>“ADD”



Step2 Click “IP address”,Select the IP address of the connected terminal and customize a domain name.



Step3 Click "SAVE" to see the domain mappings you set up in the list.



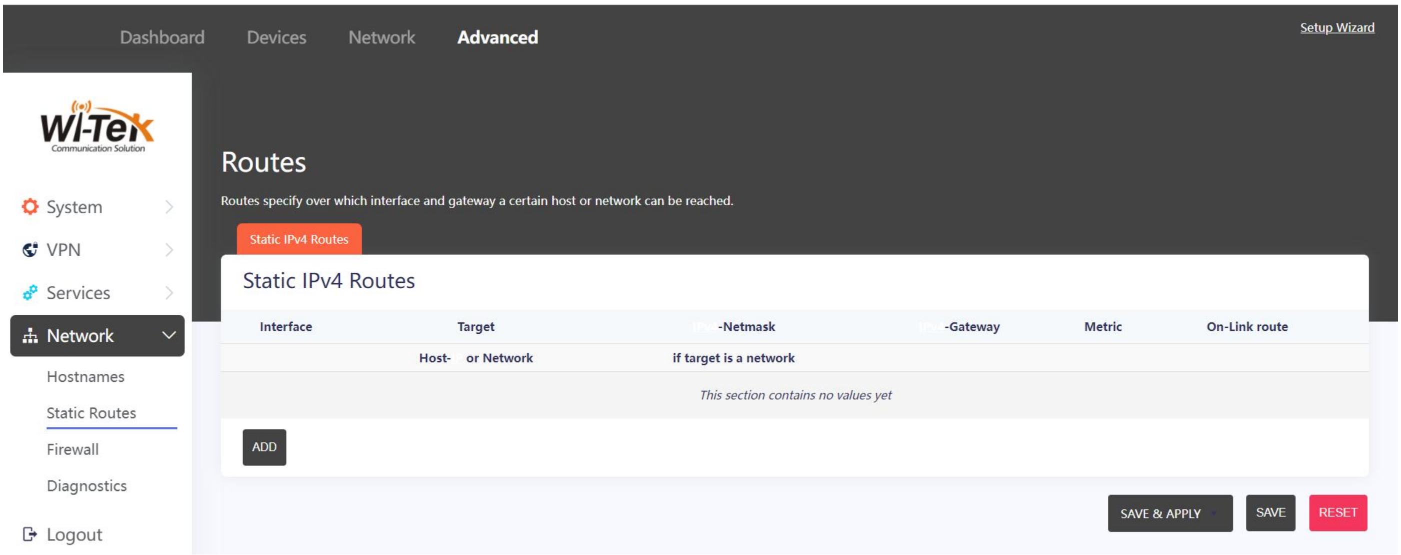
Host entries

Hostname	IP address
witek	192.168.1.1

8. Static Routes

A static route is a pre-determined path that network information must travel to reach a specific host or network. Data from one point to another will always follow the same path regardless of other considerations. Normal internet usage does not require this setting to be configured. It can also be set up according to your network needs, and the steps are as follows.

Step1 Go to the web page of your device. Click “Advanced”> “Network”>“Static Routes”>“A DD”



Routes

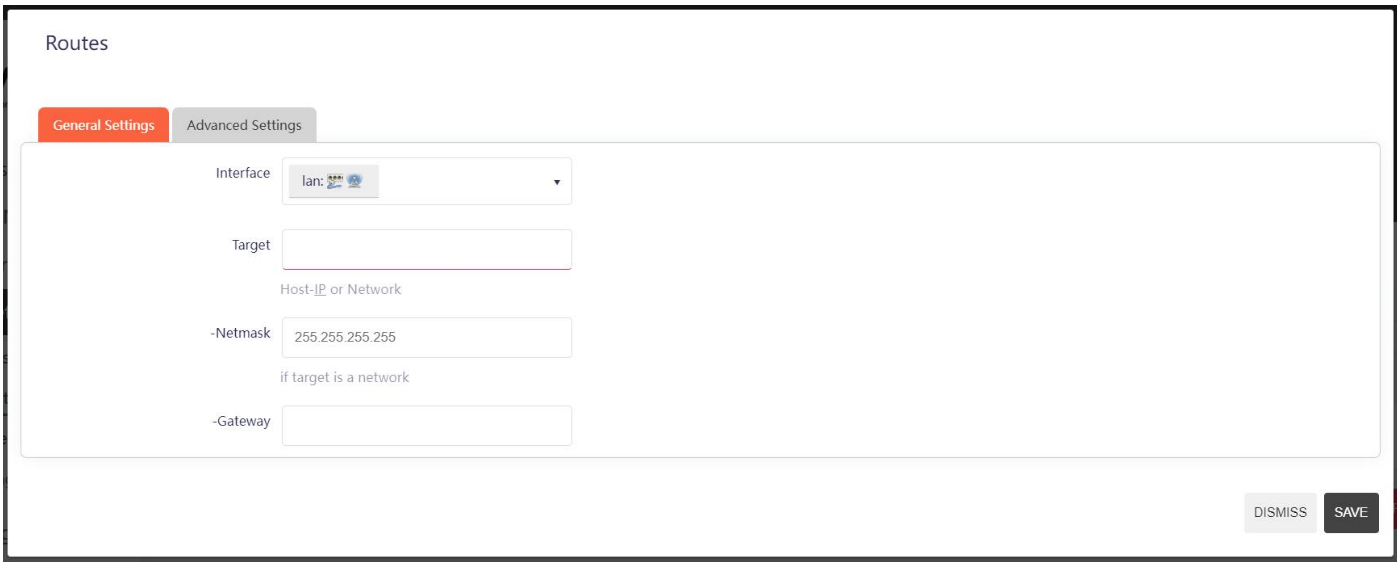
Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	-Netmask	-Gateway	Metric	On-Link route
	Host- or Network	if target is a network			

This section contains no values yet

Step2 Make general settings.



Routes

Interface: lan:

Target:

Host-IP or Network

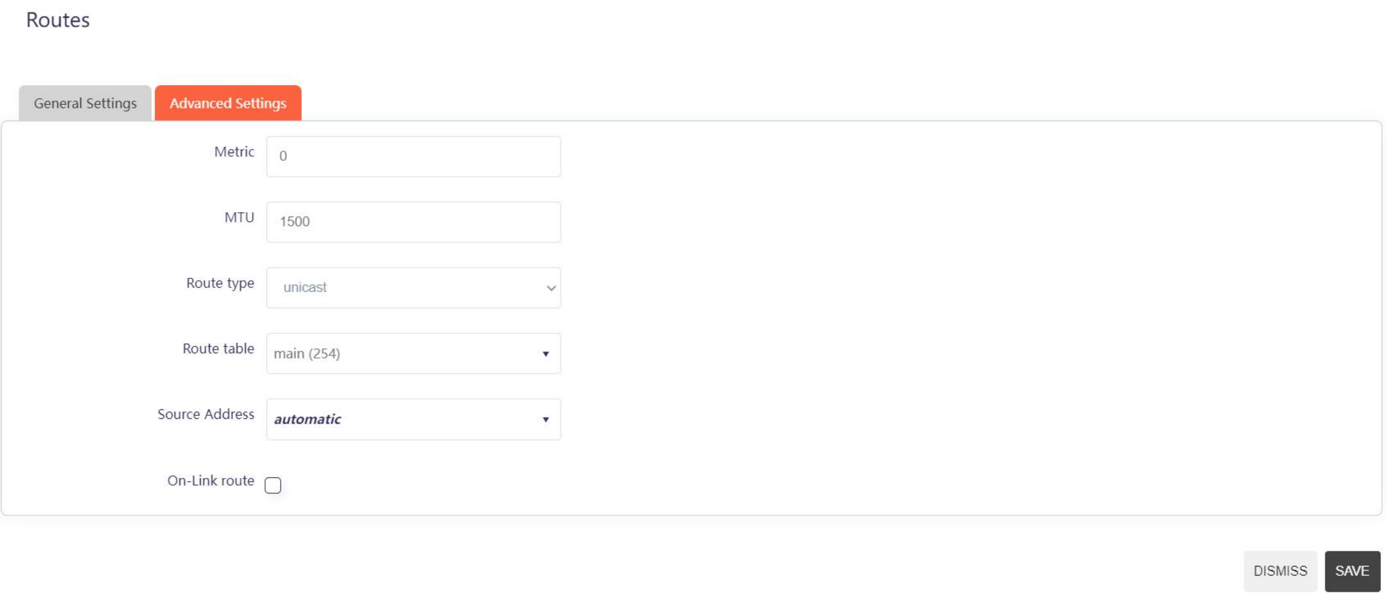
-Netmask: 255.255.255.255

if target is a network

-Gateway:

Parameter	Describe
Interface	Determined by the port that sends out the data packets.
Target	The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of the router.
Netmask	Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the mask of the corresponding network IP.
Gateway	The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the routers IP which sends out the data.

Step3 Advanced settings are available upon request.



Routes

Metric: 0

MTU: 1500

Route type: unicast

Route table: main (254)

Source Address: *automatic*

On-Link route: □

Parameter	Describe
Metric	The number of hops is an accumulator of how many hops have passed, in order to prevent unwanted packets from being scattered over the network. Specify an integer value for the desired number of hops for the route (in the range of 1 ~ 9999),
MTU	The maximum packet size that the network is capable of transmitting, in bytes. The size of the MTU determines the maximum number of bytes that the sender can send at one time. If the MTU exceeds the maximum value that the receiver

	can bear, packets will be fragmented or even dropped, increasing the burden on network transmission. If it is too small and affects the transmission efficiency, it is recommended to use the default value of 1500.
Route type	Select a route type based on your requirements.
Route table	Specify the routing table based on your requirements.
Source Address	Select Automatically obtain or then WAN port address.

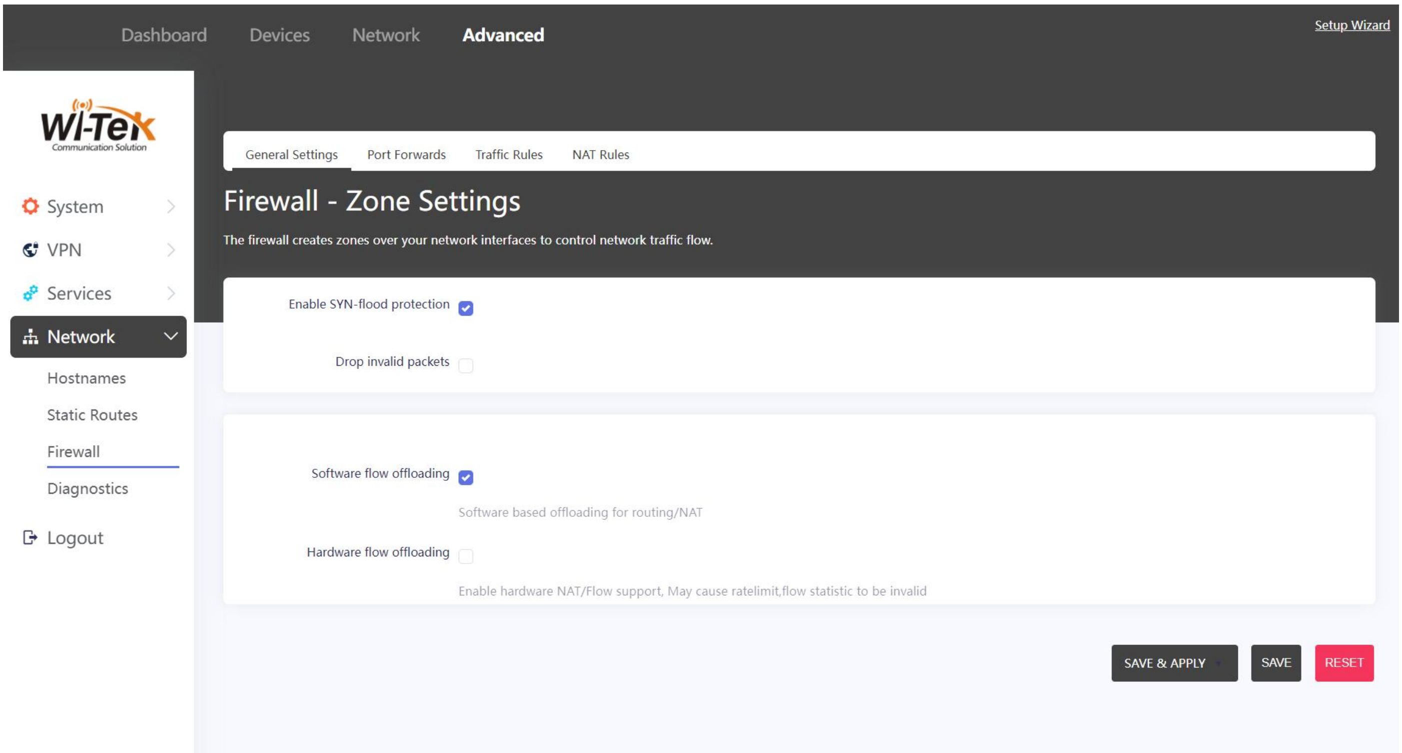
9. Firewall

9.1. General Settings

For the general settings of the firewall, you can set the firewall partition setting feature, which works by creating zones on your network interface by the firewall to control network traffic.

Setup steps

Click “Advanced”> “Network”>“Firewall”>“General Settings”.Enable the firewall features you need.



Firewall - Zone Settings

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

Enable SYN-flood protection ☑

Drop invalid packets □

Software flow offloading ☑

Software based offloading for routing/NAT

Hardware flow offloading □

Enable hardware NAT/Flow support, May cause ratelimit,flow statistic to be invalid

Parameter	Describe
Enable SYN-flood protection	SYN Flood (Semi-Open Attack) is a denial-of-service (DDoS) attack whose goal is to make a server unavailable for legitimate traffic by consuming all available server resources. Pass by repeatedly sending Initial Connection Request (SYN) packets, the attacker is able to overwhelm all available ports on the target server's machine, causing the target device to not respond to legitimate traffic at all.Enabling SYN-flood protection will effectively protect your network devices.
Drop invalid packets	Enabling this feature will result in the firewall dropping invalid packets. Invalid packets include: All station packets from an unauthorized source address with a firewall address. The source address is the address of the internal network for all station packets.

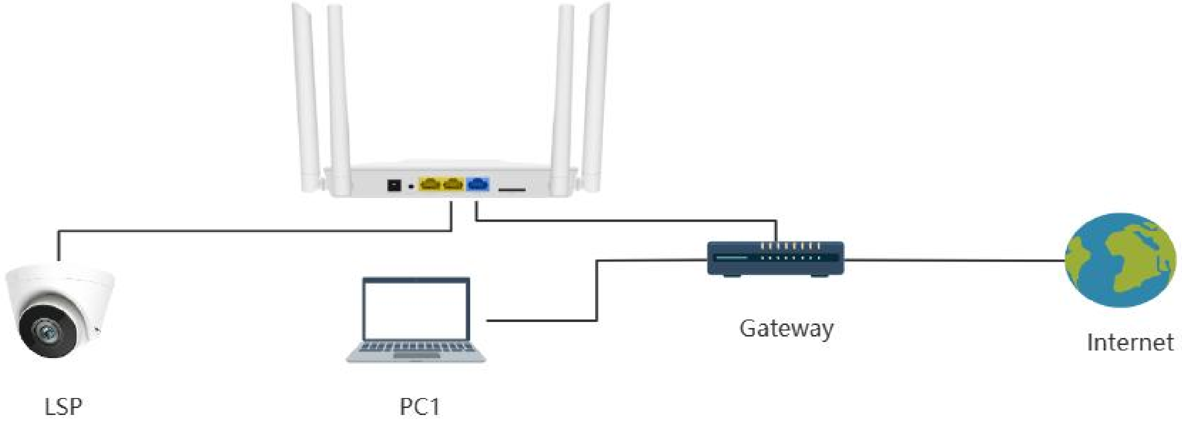
	All station packets from an unauthorized source address containing SNMP. All in-station and outbound packets that contain the source route.
Software flow offloading	Software based offloading for routing/NAT.
Hardware flow offloading	Enable hardware NAT/Flow support, May cause ratelimit,flow statistic to be invalid.

9.2. Port Forwards

In the LAN, users in the LAN can access the terminals connected to the 4G router by configuring port forwarding.

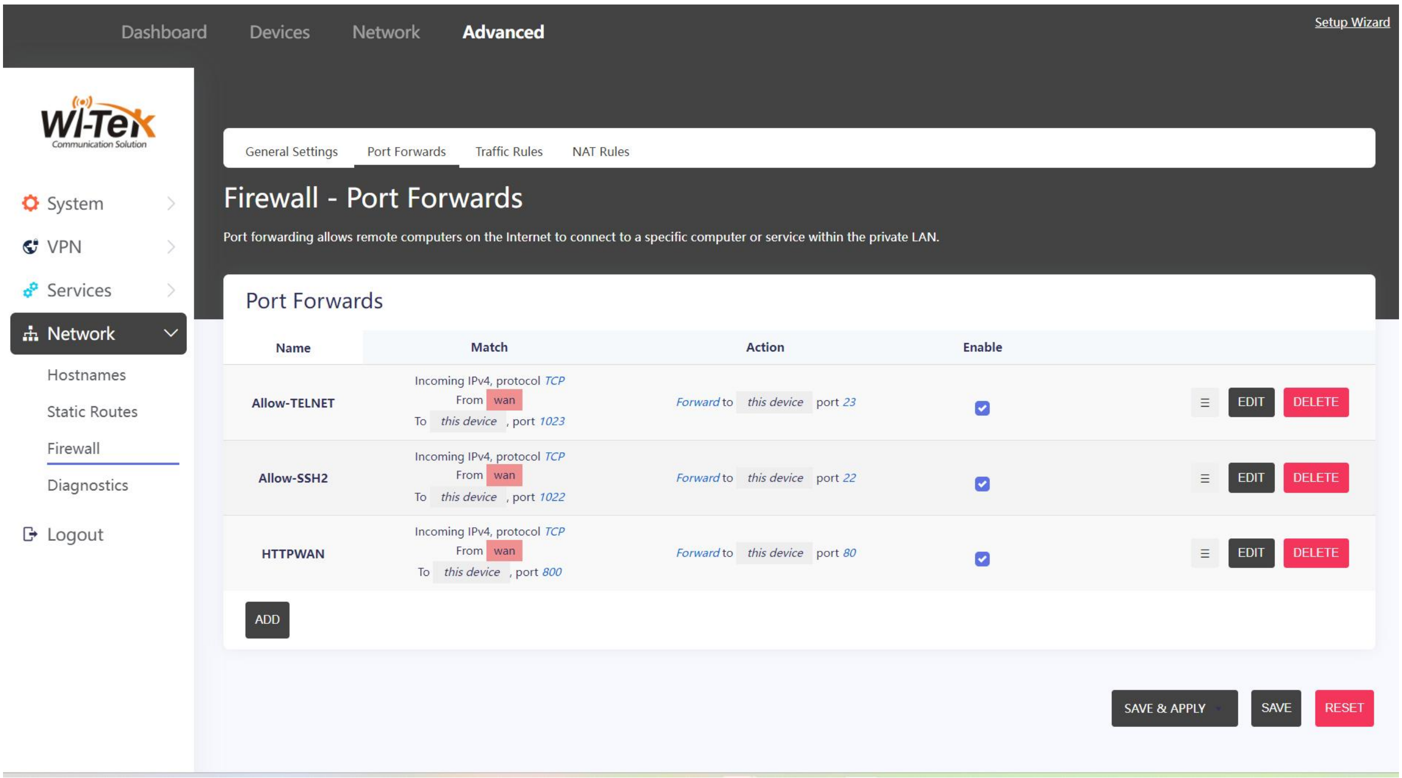
Examples of use cases:

The PC and the 4G router are within the same LAN, and port forwarding is configured within the 4G router to enable the PC to access the IPC web pages.Assume that the IP address of the IPC is 192.168.10.1 and the IP address of the WAN port of the 4G router is 192.168.20.1



Setup steps

Step1 Click “Advanced”> “Network”>“Firewall”>“Port Forwarding”> “ADD”, establish port forwarding.



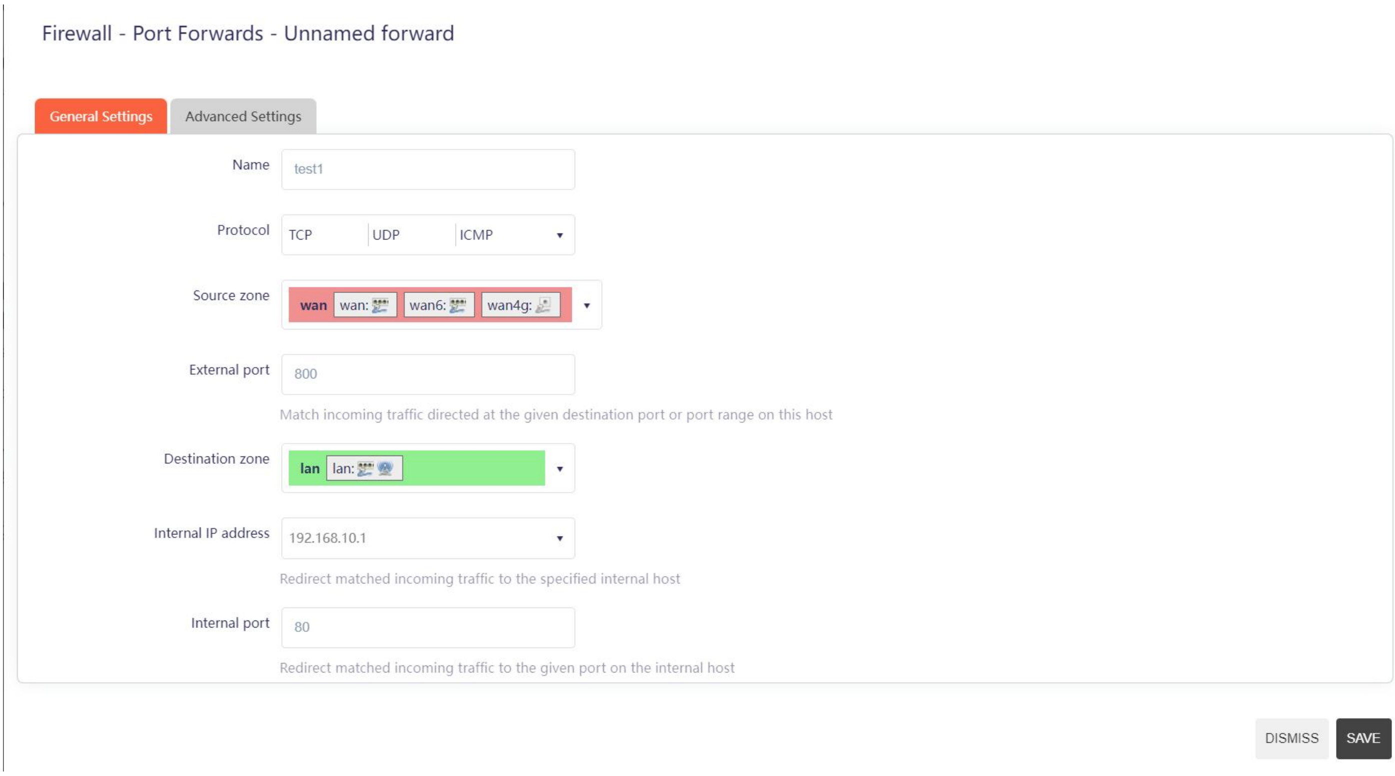
Firewall - Port Forwards

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

Port Forwards

Name	Match	Action	Enable	
Allow-TELNET	Incoming IPv4, protocol TCP From wan To this device , port 1023	Forward to this device port 23	☑	≡ EDIT DELETE
Allow-SSH2	Incoming IPv4, protocol TCP From wan To this device , port 1022	Forward to this device port 22	☑	≡ EDIT DELETE
HTTPWAN	Incoming IPv4, protocol TCP From wan To this device , port 800	Forward to this device port 80	☑	≡ EDIT DELETE

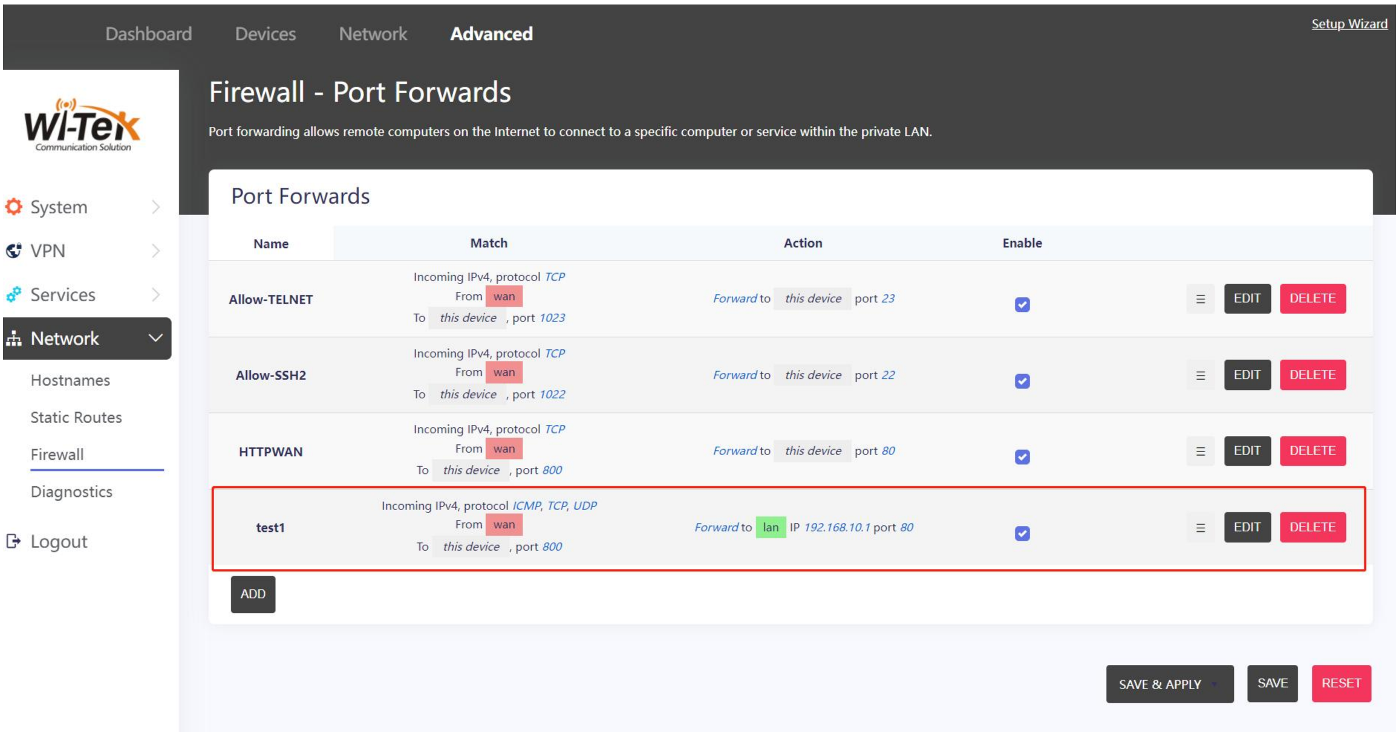
Step2 Click "General Settings" enter the corresponding parameters.


Firewall - Port Forwards - Unnamed forward

Name	test1
Protocol	TCP UDP ICMP
Source zone	wan wan: wan6: wan4g:
External port	800 Match incoming traffic directed at the given destination port or port range on this host
Destination zone	lan lan:
Internal IP address	192.168.10.1 Redirect matched incoming traffic to the specified internal host
Internal port	80 Redirect matched incoming traffic to the given port on the internal host

Parameter	Describe
Name	Set a name.
Protocol	Select the filtered protocol, TCP, UDP, ICMP, or all of them.
Source zone	Select the source area, and in this example,the WAN port is used as the source area.
External port	Match incoming traffic directed at the given destination port or port range on this host,in this example, take 800.
Destination zone	Select the destination area, and in this example, the LAN port is used as the destination area.
Internal IP address	Redirect matched incoming traffic to the specified internal host,in this example, the IP address of the IPC is 192.168.10.1.
Internal port	Redirect matched incoming traffic to the given port on the internal host,in this example, take 80.

Step3 After the configuration is complete, click Save to exit the configuration page, and you will see the configured port forwarding rules in the list, and you can enable or stop the po rt forwarding rules in the list.



Firewall - Port Forwards

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

Port Forwards

Name	Match	Action	Enable	
Allow-TELNET	Incoming IPv4, protocol *TCP* From wan To *this device* , port *1023*	*Forward* to *this device* port *23*	☑	☰ EDIT DELETE
Allow-SSH2	Incoming IPv4, protocol *TCP* From wan To *this device* , port *1022*	*Forward* to *this device* port *22*	☑	☰ EDIT DELETE
HTTPWAN	Incoming IPv4, protocol *TCP* From wan To *this device* , port *800*	*Forward* to *this device* port *80*	☑	☰ EDIT DELETE
test1	Incoming IPv4, protocol *ICMP, TCP, UDP* From wan To *this device* , port *800*	*Forward* to lan IP *192.168.10.1* port *80*	☑	☰ EDIT DELETE

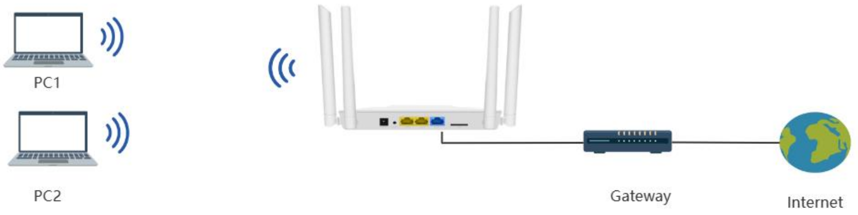
Step4 On a PC, open a browser and type: 192.168.12.107:800 to access the IPC web interface.

9.3. Traffic Rules

You can customize filter rules to flexibly control the access permissions of connected devices to the Internet.

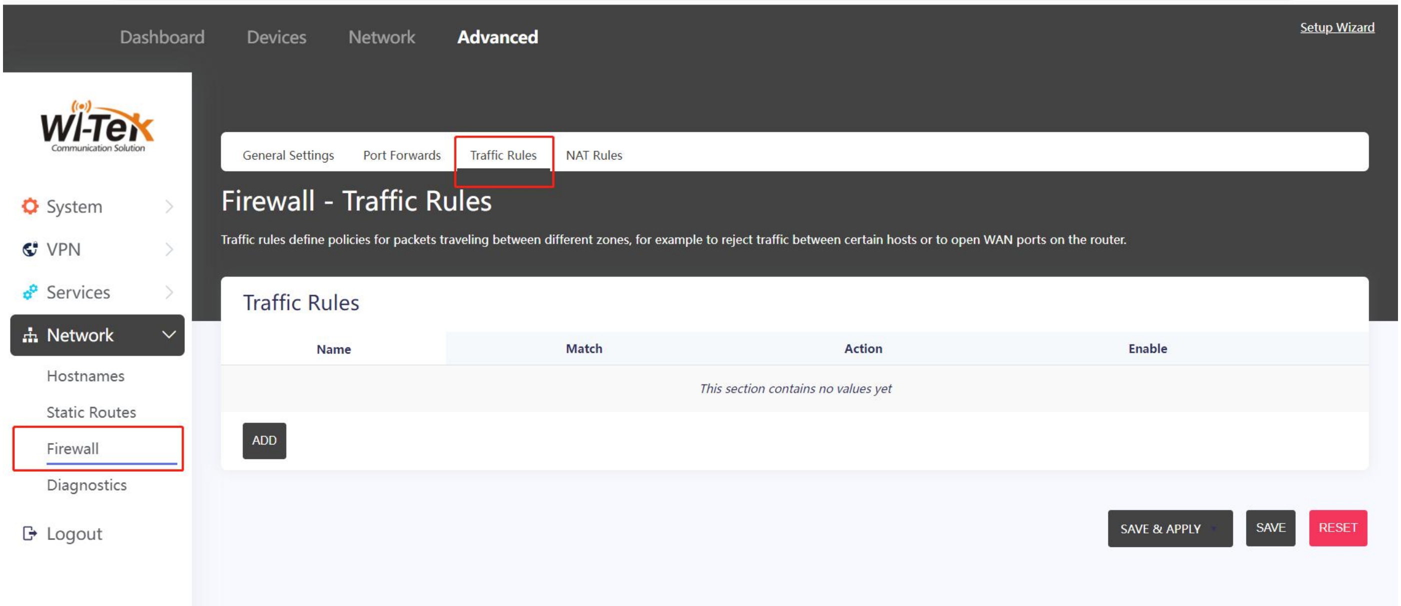
Examples of use cases:

There are two computers connected to the 4G router, the IP address of pc1: 192.168.10.1, the IP address of pc2: 192.168.20.1 now you need to create a filter rule to make pc1 can access the Internet, and pc2 can't.



Setup steps

Step1 Click "Advanced"> "Network">"Firewall">"Traffic Rules"> "ADD", establish filter rules.



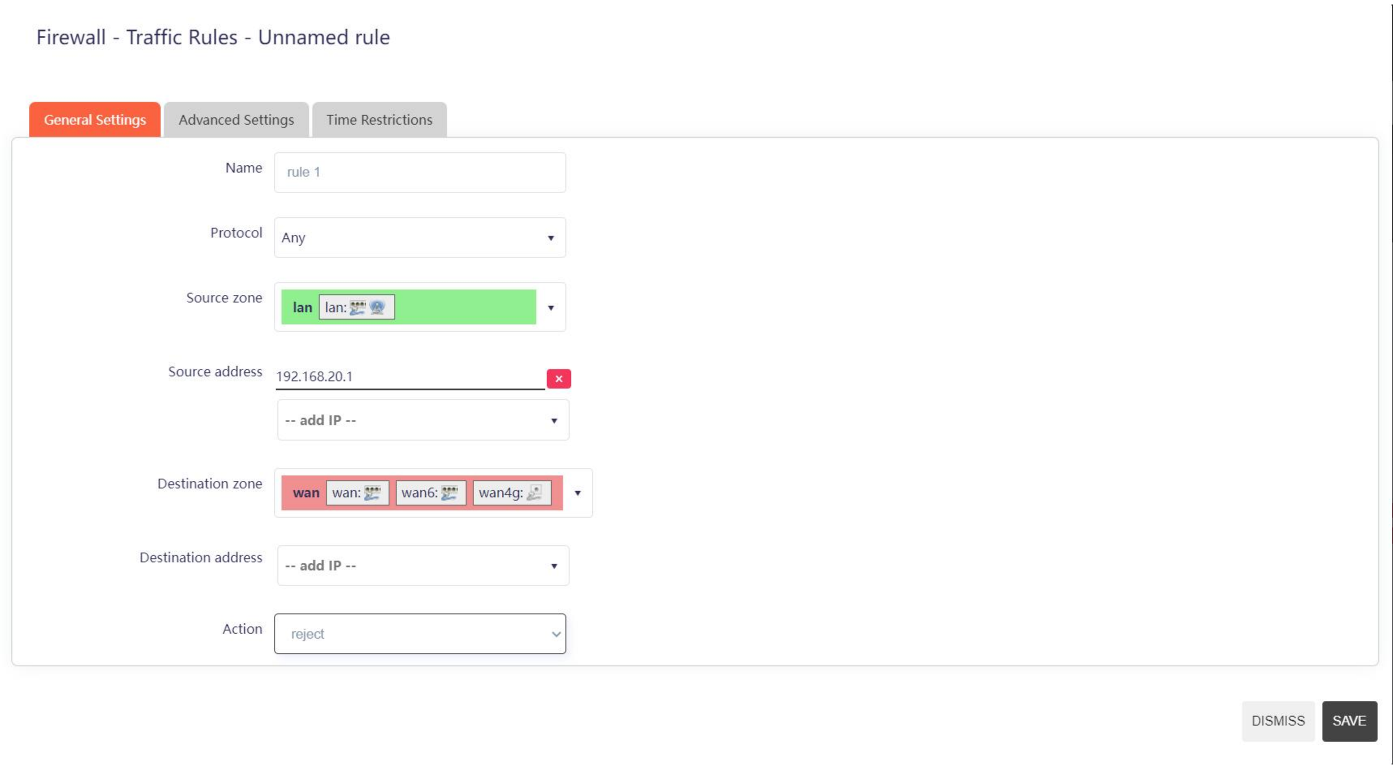
Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable
This section contains no values yet			

Step2 Click “General Settings” enter the corresponding parameters.



Firewall - Traffic Rules - Unnamed rule

Name: rule 1

Protocol: Any

Source zone: lan lan:

Source address: 192.168.20.1
-- add IP --

Destination zone: wan wan: wan6: wan4g:

Destination address: -- add IP --

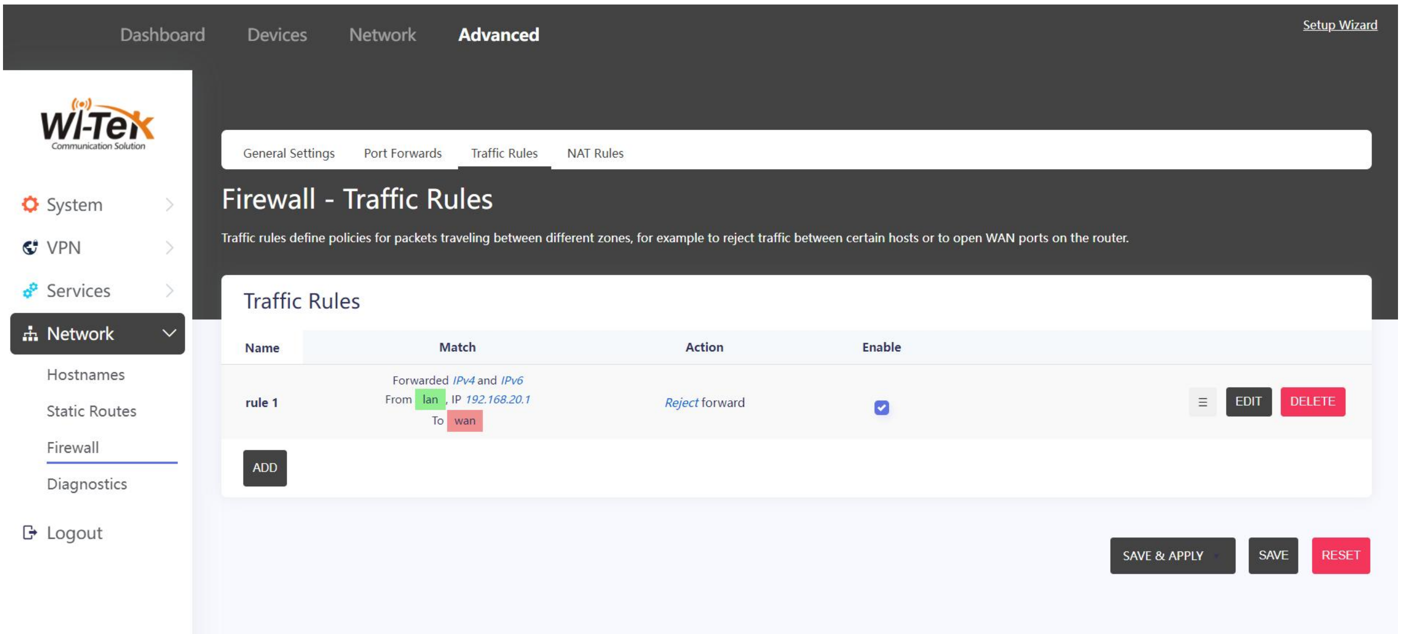
Action: reject

Parameter	Describe
Name	Give the filter a name.
Protocol	Select the filtered protocol, TCP, UDP, ICMP, or all of them.

Source zone	Select the source area, and in this example, select the LAN port to which the PC is connected as the source area.
Source address	Enter the IP address in the source region, in this case the IP address of PC2: 192.168.20.1.
Destination zone	Select the destination area, and in this example, the WAN port is used as the destination area.
Destination address	You can enter the IP address as needed to make the filtering rules more precise, and select Leave blank in this example.
Action	Select the actions of the filter rule, the common actions are "Reject" and "Accept". In this example, you need to select "Deny" to prevent PC 2 data from accessing the Internet from the WAN port.

Step3 After the configuration is complete, click "Save", and after exiting the configuration page, you will see the configured filter rules in the filter rule list, where you can enable or stop the filter rule.

Note: When there are multiple filter rules, they are executed from top to bottom in the order of the list.



Firewall - Traffic Rules

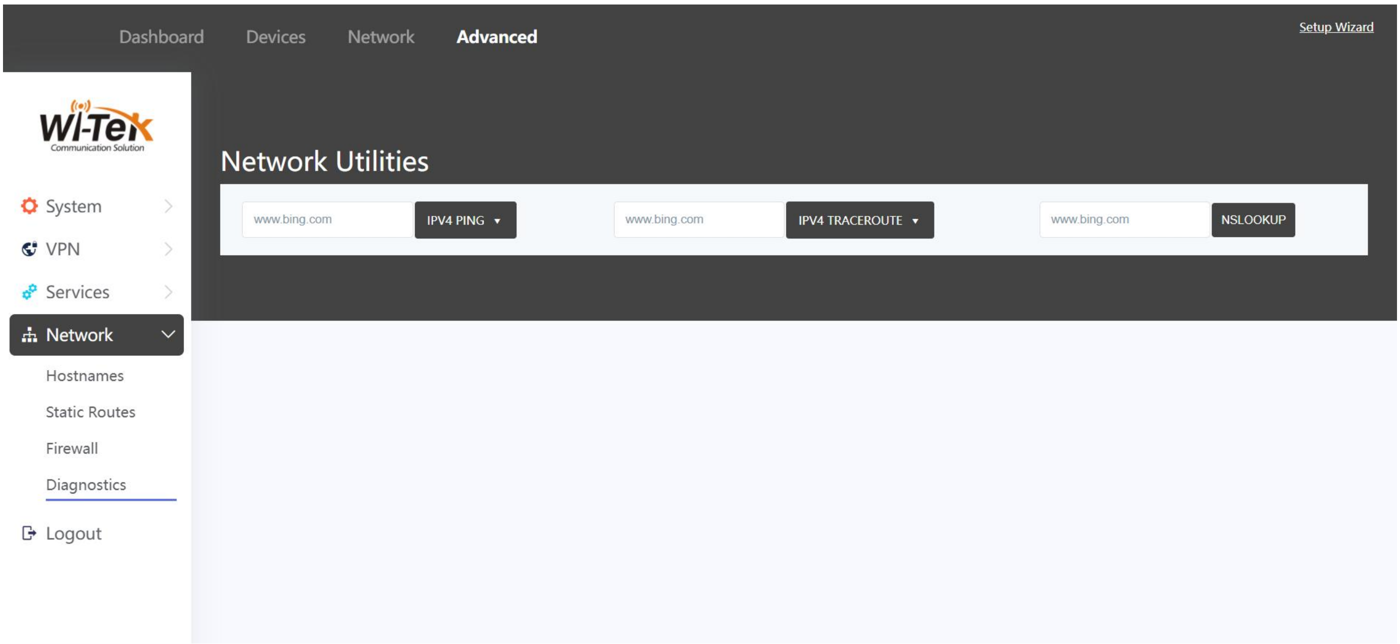
Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	
rule 1	Forwarded IPv4 and IPv6 From lan, IP 192.168.20.1 To wan	Reject forward	☑	≡ EDIT DELETE

10. Diagnostics

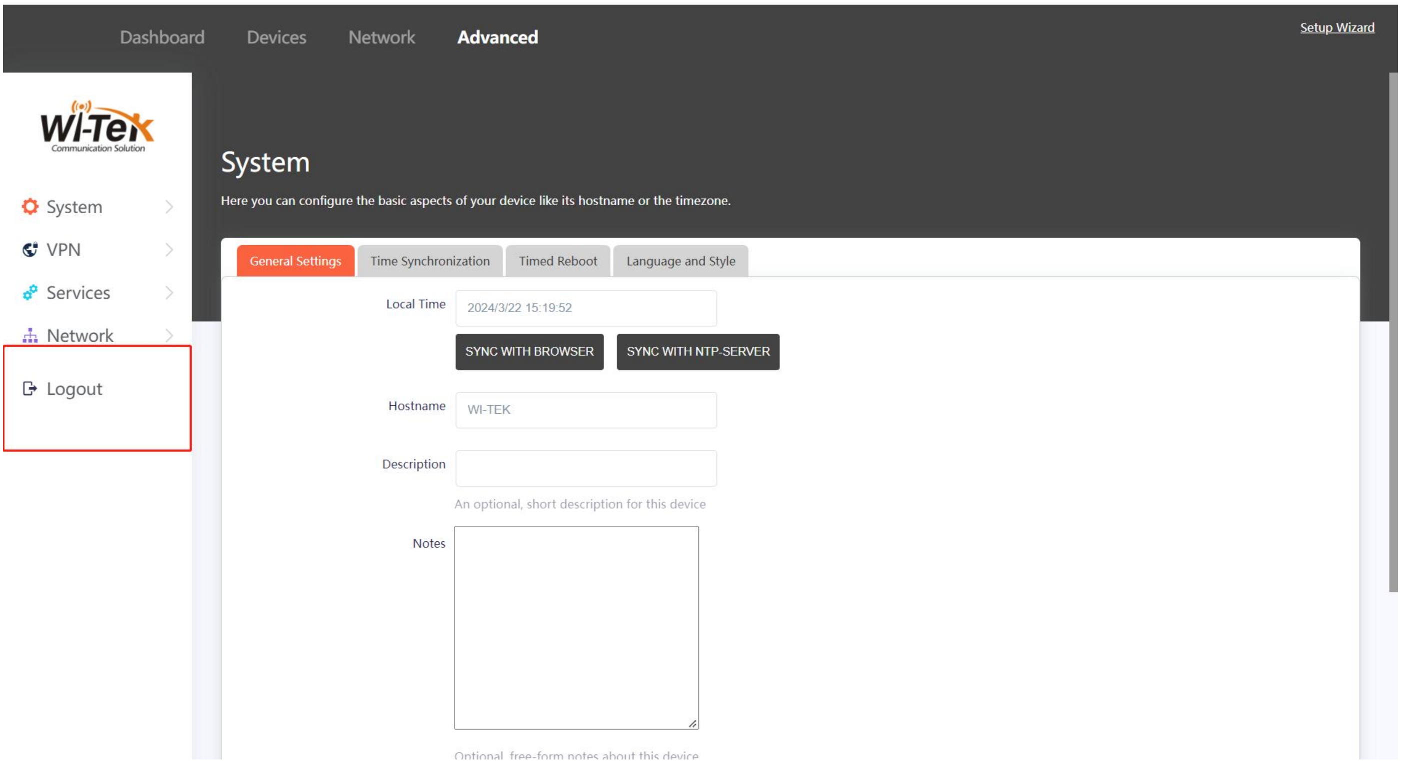
In the built-in network diagnosis tool, you can check the connection of the device to a certain IP address or a certain domain name, and better assist you in troubleshooting network faults.



Parameter	Describe
PING	Specify the IP or domain name of the reachable network.This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
TRACERT	Specify the IP or domain name of the reachable network. This diagnostic tool tests the performance of a connection.
NSLOOKUP	It is used to query DNS records to check whether the domain name resolution is normal, and to diagnose network problems in case of network failures.

11. Logout

Click “Advanced”> “Network”>“Logout” the device's web page will be exited.



System

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

Local Time: 2024/3/22 15:19:52

Hostname: WI-TEK

Description:

An optional, short description for this device

Notes:

Optional, free-form notes about this device