



Chengdu Ebyte Electronic Technology Co.,Ltd

# Wireless Modem

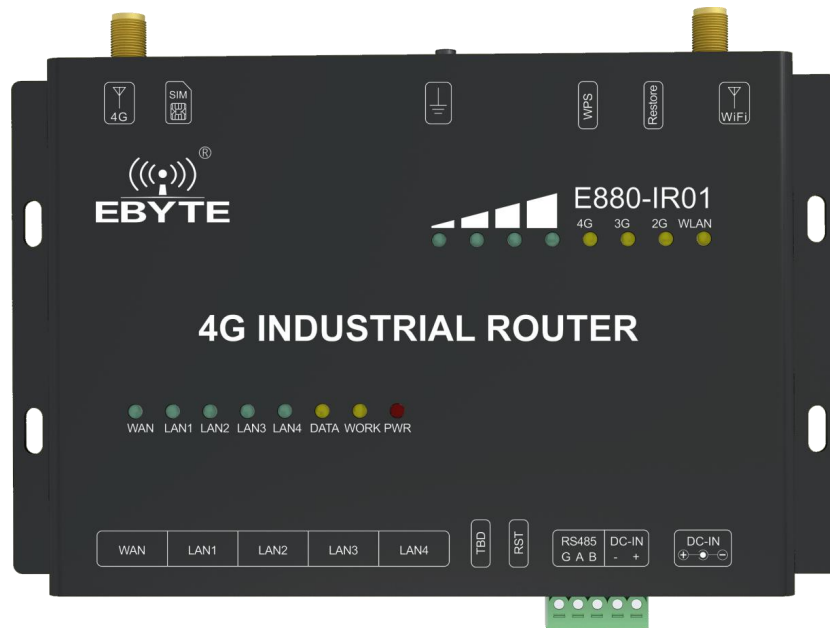
## User Manual



All rights to interpret and modify this manual belong to  
Chengdu Ebyte Electronic Technology Co., Ltd.

## CONTENTS

Functional features.....	2
1. Quick start.....	3
1.1 Preparation.....	3
1.2 Hardware connection.....	3
1.3 Web access.....	4
2. Product Introduction.....	6
2.1 Basic Parameters.....	6
2.2 Size and interface description.....	7
3. Function Set.....	10
3.1 Menu overview.....	10
4. Function description.....	11
4.1 Status.....	11
4.2 System.....	11
4.2.1 Host name and time zone setting.....	11
4.2.2 Username login password setting.....	11
4.2.3 Restore factory reset and upgrade.....	12
4.2.4 Restart.....	13
4.3 Service.....	14
4.3.1 Dynamic DNS.....	14
4.3.2 WIFI Plan.....	15
4.3.3 Frp Intranet penetration.....	15
4.3.4 485 Serial port.....	18
4.3.5 VPN Server.....	20
4.3.6 SIM Card.....	24
4.4 Network.....	26
4.4.1 Interface.....	26
4.4.2 Wireless.....	29
4.4.3 Switch.....	29
4.4.4 Host name.....	30
4.4.5 Static routing.....	30
4.4.6 Load balancing.....	31
4.4.7 Firewall.....	34
4.4.8 Network diagnostics.....	36
4.4.9 Flow control management (Qos) .....	36
5. Device panel identification and function setting.....	38
5.1 LED Indicator.....	38
5.2 Button setting.....	39
5.3 Other identifications.....	39
6. AT SMS command description.....	39
7. Revision history.....	41
About us.....	41



## Functional features

- 4 wired LAN ports and 1 wired WAN port are supported.
- Support 1 WLAN wireless LAN;
- Support LED status monitoring (display power, Work, WAN, LAN, WIFI, 4G network mode and signal strength status);
- Support SSH, Web multi-platform management configuration;
- One key to restore factory Settings;
- The cable network ports all support the 10/100Mbps rate;
- Support APN private network access, SIM card self-test, 2/3 / 4G standard switching, SIM information display
- Support wired wireless simultaneous online, multi-network intelligent switching;
- Support firmware upgrade, firmware configuration backup function;
- Firewall, NAT, DMZ host, access control black and white list, IP speed limit.
- QOS and traffic service can limit the speed according to interface;
- WPS one-key Internet function;
- Support VPN private network access, VPN client and VPN server operating mode;
- Support data transmission between serial port and Ethernet, transparent transmission and MODBUS transmission mode;
- Support load balancing multi-network port flow control settings, with network port priority, enable, flow control ratio and other operating methods;
- Support FRP internal network penetration, remote management of router (status display and parameter setting)

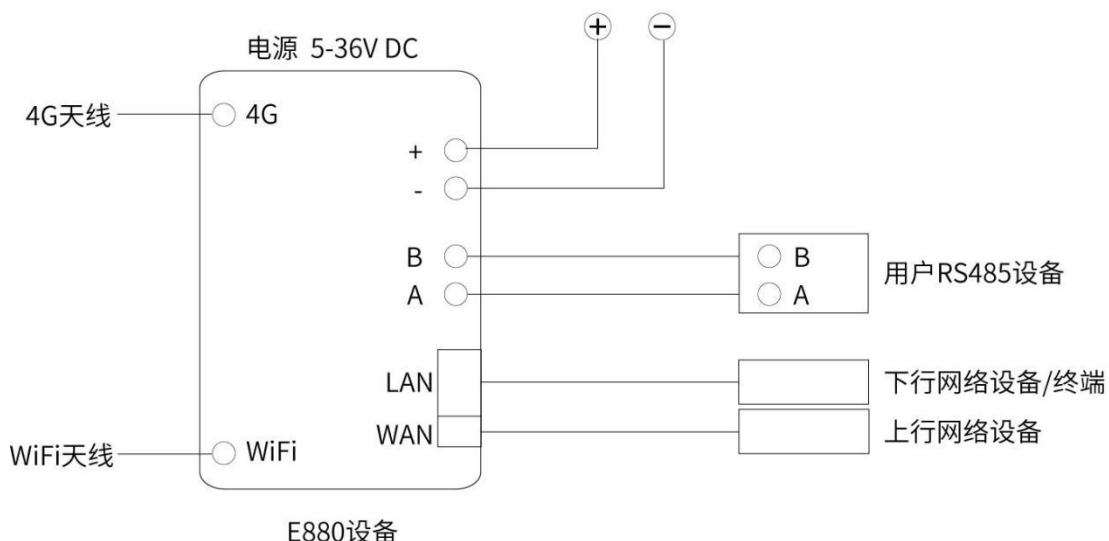
# 1. Quick start

In order to ensure that the products that users get at the first time are qualified, we provide a simple testing process for users to refer to. In the whole process, the customers can get started quickly.

## 1.1 Preparation

Before the 4G router works, users need to prepare at least one PC, one network cable, product supporting devices and a 4G SIM card with traffic.

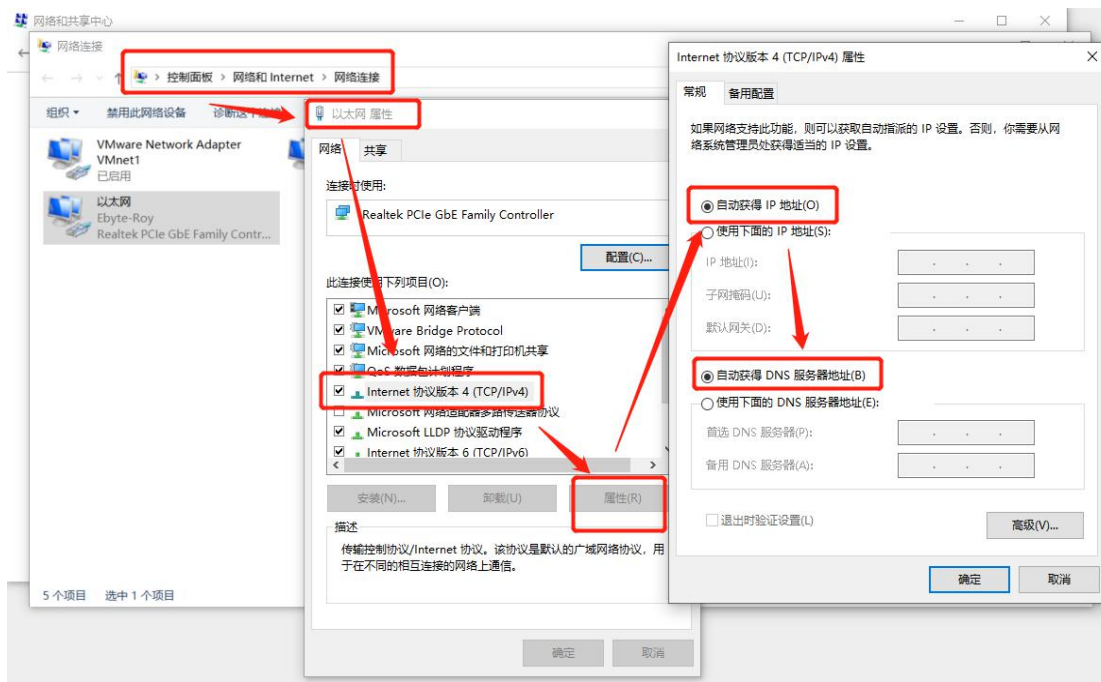
## 1.2 Hardware connection



As shown in the figure above, before charging the device (the charging position has been marked on the panel), the customer must insert the 4G SIM card into the value card slot (chip end up), otherwise the 4G function will not be enabled.

Connect the WIFI antenna and 4G antenna to the SMA interface under the mark of the device panel, and connect the computer to the LAN port of the device (LAN1~LAN4 can be used). In order to detect 4G function, the WAN port cannot be connected to Ethernet.

In order to ensure that the computer can enter the WEB management interface through the LAN, the customer needs to ensure that the computer network property automatically obtains the IP address and automatically obtains the DNS server address, as shown in the figure below.



After completing the above steps, use the power supply of the equipment, and then power up the router.

After power on, wait for about 1 minute, and the WORK indicator on the panel starts flashing at a frequency of about 1S, indicating that the startup is completed. In addition, on the panel, the 4G signal indicator and the 4G indicator in network properties also start to WORK normally (the device is connected to 4G network by default). The amount of 4G signal indicator light is determined by the current network signal quality.

### 1.3 Web access

On the PC, open any browser and input 192.168.10.1 to enter our router Web login interface, as shown in the figure below:



Here, our default password is: root

After entering the password, you can enter our web administration interface.

In the bottom right corner of the Web page, you can click the following link to enter our company's official website,

which verifies the success of 4G routing access to the external network.



Well, after the above steps, no failure occurs, which means that the equipment can be used normally. In addition, if customers want to know the current network speed, they can use relevant software to conduct network test.

## 2. Product Introduction

E880-IR01 is a 4G wireless router that provides fast networking and mobile network sharing solutions for user devices. The equipment adopts the industry's commercial high-performance embedded structure, and has a high application advantage in the data transmission fields such as industrial control network, smart grid, industrial control data acquisition, smart home, etc. It supports wired WAN port, LAN port, WLAN network, 4G network interface, SMS AT command and remote control of 4G router.

### 2.1 Basic Parameters

	Project	Index
Wifi Parameters	TDD-LTE	Downstream Rate 130Mbps, Upstream Rate 35Mbps Band 38/39/40/41
	FDD-LTE	Downstream Rate 150Mbps, Upstream Rate 50Mbps Band 1/3/8
	WCDMA	Downstream Rate 42Mbps , Upstream Rate 5.76Mbps Band 1/8
	TD-SCDMA	Downstream Rate 5.2Mbps , Upstream Rate 2.2Mbps Band 34/39
	CDMA2000 1x/EVDO	Downstream Rate 3.1Mbps , Upstream Rate 1.8Mbps BC0
	GSM/GPRS/EDGE	Downstream Rate 236.8kbps , Upstream Rate 236.8kbps 900/1800
Hardware parameters	Size (H*W*D)	172*107*29mm
	Weight	419.5g
	Working Temperature	-20°C~+70°C
	Storage temperature	-40°C~+85°C
	Working humidity	5%~95%
	Storage humidity	1%~95%
	Working voltage	5V~36V
	Current consumption	Under DC12V power supply, average 106mA, maximum 205mA (normal temperature)
	precision	0.2%
	Data interface	RS485: 1200~115200bps

The working mode and power consumption table are shown in the following table:

The power consumption table of E880-IR01 is shown in the following table

Manner of Working	Supply Voltage	Average Current	Max Current	Remarks
4G+Ethernet	DC12V	106mA	205mA	Ethernet Prior
Ethernet	DC12V	99mA	186mA	Without SIM Card
4G	DC12V	141mA	283mA	Without input of

				WAN port
All Stop	DC12V	88mA	163mA	

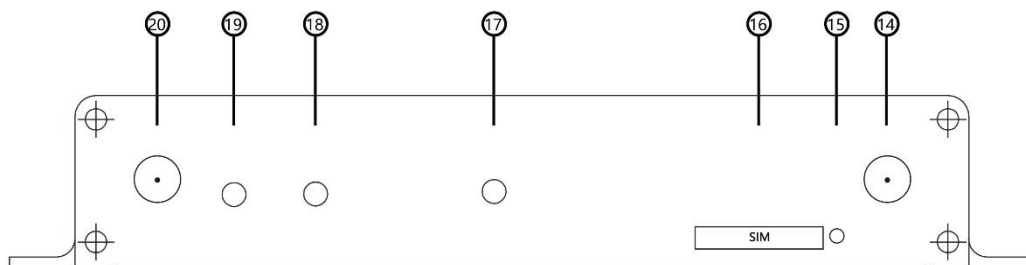
When E880-IR01 is powered at 12V and works simultaneously with 4G and Ethernet, statistics show that: The average power consumption is 1.27w and the maximum power consumption is 2.46w. Average current 106mA, maximum current 205mA;

When E880-IR01 is powered at 12V and works alone in 4G, statistics show that:

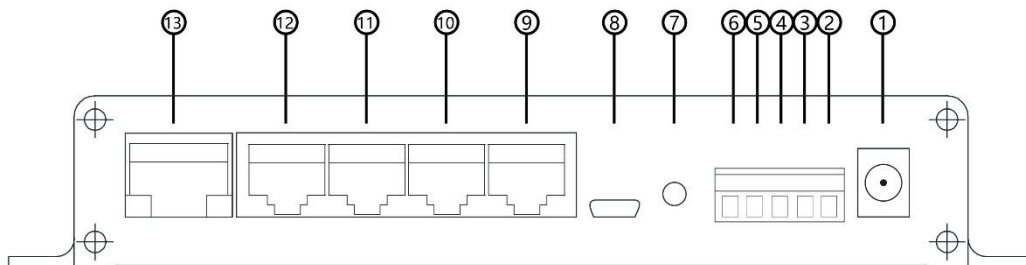
The average power consumption is 1.69w and the maximum power consumption is 3.40w. Average current 141mA, maximum current 283mA.

## 2.2 Size and interface description

SIM Side

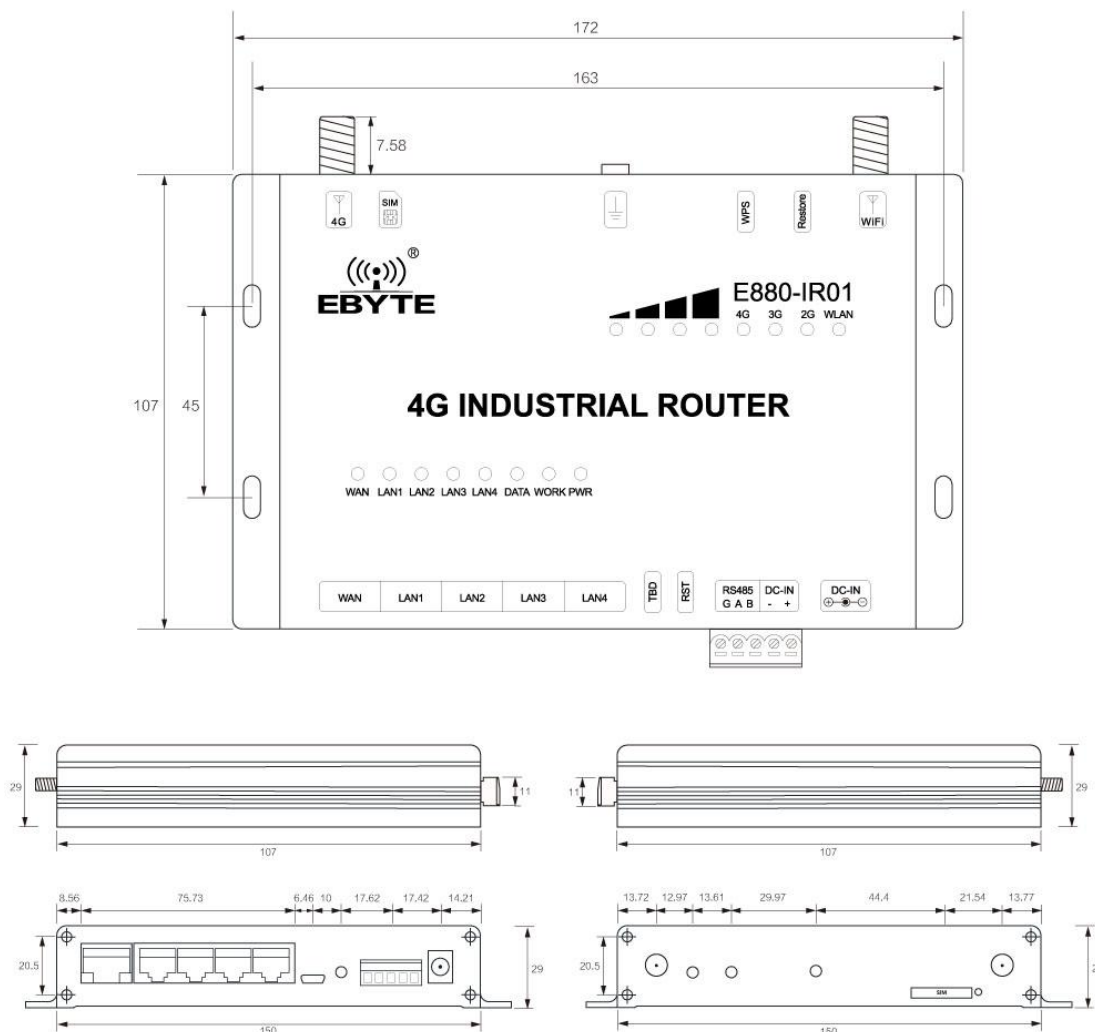


WAN Port Side



Top View





The hardware interface is described below:

Interface No.	Name	Remarks
1	DC5~36V	Voltage Scope DC:5~36V, Standard 5.5*2.1 Power Socket
2	DC-IN+	Voltage Scope DC:5~36V, Power terminal positive
3	DC-IN-	Voltage Scope DC:5~36V, Power terminal negative
4	RS485 B-	RS485 interface B-terminal (standby)
5	RS485 A+	RS485 interface A-terminal (standby)
6	RS485 G	RS485 interface common ground
7	RTS	Press hardware reset to restart
8	TBD	Debugging interface
9~12	LAN (1~4)	LAN Port (1~4), LAN Interface, 10/100Mbps, Support Auto MDI/MDIX
13	WAN	WAN Port, WAN Interface, 10/100Mbps, Support Auto MDI/MDIX
14	4G	4G Antenna SMA Interface
15	Card Withdrawal	Using a sharp object to press, get SIM card out

16	SIM Slot	Where the SIM card is installed
17	GND Self Clinching Studs	Connecting with the earth
18	WPS	Short press to WPS get a no password access to Internet.
19	Restore	Long press 5s and release, and restore factory Settings
20	WIFI Antenna	WIFI Antenna SMA Interface

### 3. Function Set

In this section, we will be according to the function menu on the Web interface, and explain, limited to space, among them, some options, we will emphatically expounded, and some not commonly used and not important functions we can choose an overview, in the whole process, we will be in a certain function, interspersed with some menu with links to other functions.

#### 3.1 Menu overview

In the web management interface, users can set their desired functions or view relevant states. Through the menu bar on the left of the page, specific functions or information can be set and inquired. Users can see the directory tree structure of the menu as shown in the following table.

Submenu \ menu	Status	System	Service	Internet
1	Overview	System	Dynamic DNS	Interface
2	Firewall	Administration authority	WIFI plan	Wireless
3	Routing table	Scheduled task	FRP Intranet penetration	Interchanger
4	system log	Time synchronization	RS485	DHCP/DNS
5	Real-time Information	Backup/upgrade	VPN server	Hostname
6		Restart	SIM	Static routing
7				SIM
8				Firewall
9				Network diagnosis
10				Qos function

## 4. Function description

### 4.1 Status

In the "Status" menu, users can view the current operating status of the router, including the firewall. Router, system internal operation log, and network related information refreshed in real time, etc. Users cannot set anything in this column. Here, users can query the content of the related sub-menu according to the related needs.

### 4.2 System

In the system bar, we can set the management parameters of the 4G router, etc. These include the login password of the web page, host name, upgrade and other functions.

#### 4.2.1 Host name and time zone setting

In the system-> system properties-> basic settings option, users can set the host name of the 4G module and also modify the time zone. Here, our default host name is: EBYTE, and the time zone uses UTC (if the product is used in China, it can be set to: Asia / Shanghai).

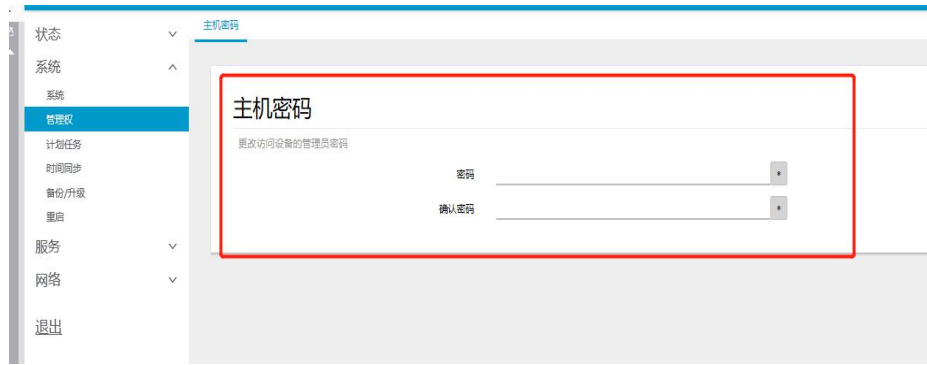
Set the host name as shown below



In addition, users can also set the language (Chinese / English) of the web interface and different style themes. Here, our default language is Chinese, and the style used is our company's technology blue theme

#### 4.2.2 Username login password setting

In the system-> management rights-> host password option, set the web login interface. The host password setting requires at least one character, and then click the Save button. The login password can be set. As shown below.



### 4.2.3 Restore factory reset and upgrade

In the system-> backup / upgrade option, performing a factory reset button to ensure that users can return to the initial state after the wrong operation of the router is set, so that it can be used normally. At the same time, we reserve the upgrade function. When we update the new version of firmware, users can perform the upgrade operation by themselves, so that they can experience more functions. The factory reset and upgrade are as shown below.



What needs to be explained here is that when users upgrades the firmware, please do not power off. After loading the firmware browsed on the page, click to flash the firmware and wait for more than 10 seconds before the next window pops up. After clicking execute, wait a few seconds. A few minutes later, the web page automatically returns to the login interface, and the upgrade is successful.

#### 4.2.4 Restart

In the system-> restart option, you will enter the following interface, click on the execute operation to perform the restart, wait for about 40 seconds, and the WORK indicator on the device panel flashes normally. At this time, the restart is successful.



另外，在面板的侧边（网口位置的右边），有一个 RST 物理按键，短按该按钮，也可以重启该设备。

### 4.3 Service

#### 4.3.1 Dynamic DNS

In the Service-> Dynamic DNS option, users can add a domain name resolution service to achieve the functions of remotely setting up a router, as shown below.



In the dynamic setting interface, some DDNS service providers have been pre-configured in the drop-down menu in the DDNS service provider. If the DDNS service provider selected by the customer is not in the drop-down box, you can choose to customize it.

Dynamic DNS is not enabled by default. Before using this function, please click Enable first.

After modification, please restart the router to ensure normal work.

Customers need to fill in the parameters set by DDNS strictly to ensure that the network matches normally.

With multi-level routing, DDNS is also available.

This function cannot be used if the network where the router is located is not assigned a separate public IP.

If relevant port mapping is set in the firewall, remote access to the router's internal network can be achieved.

The router can add multiple dynamic domain names.

### 4.3.2 WIFI Plan

In the Service-> WIFI plan option, users can set wireless WIFI related events, such as the activation or shutdown of wifi, as shown below.



### 4.3.3 Frp Intranet penetration

For internal users who do not have a public IP, remotely managing routers or other ports on the internal network is an awkward problem. Intranet penetration allows access to devices (such as the local machine) on the internal network through the public network. There are many intranet penetration tools. FRP intranet penetration with its high-performance reverse proxy application not only allows customers to easily perform intranet penetration, provide services to the external network, but also has stable and efficient performance and supports multiple protocol types.

Next, we will demonstrate how to use the intranet penetration tool.



Here, we log in to [www.ngrok.cc](http://www.ngrok.cc), log in to the homepage of a frp server provider's official website, and then purchase the frp server. Of course, the platform also provides a free server (if users have their own public IP, he can set up his own frp server, here we use a third-party provider).

After purchasing the frp server, create a server tunnel in your account (the creation process is very simple and the platform is a detailed tutorial). After the tunnel is created, you can see the following information .



Here we will get: 1. Tunnel domain name; 2. Tunnel name; 3. FRP authorization code; 4. Server address; 5. Server port; 6. Tunnel protocol; 7. Local port. These parameters need to be used in the frp client setting parameters in our router later.

In the service-> Frp intranet penetration-> basic settings option, we get the following setting interface.



Server parameter name	Client parameter name	Description
	Software version	Client software version, select the default 0.16.1

	Download source address	Software download source, select the default source address -2
Server address	Server address	Fill in the obtained server address with this option
Server port	Port	7000
FRP authorization code	Privilege token	Fill the server's authorization code into this option

In the basic settings, we enable the frp function and perform the following parameter correspondence:

For other options, select the default.

In the service-> Frp intranet penetration-> service list option (this option is at the bottom of the page), we click the add button to go to the following interface and the setting interface as follows.

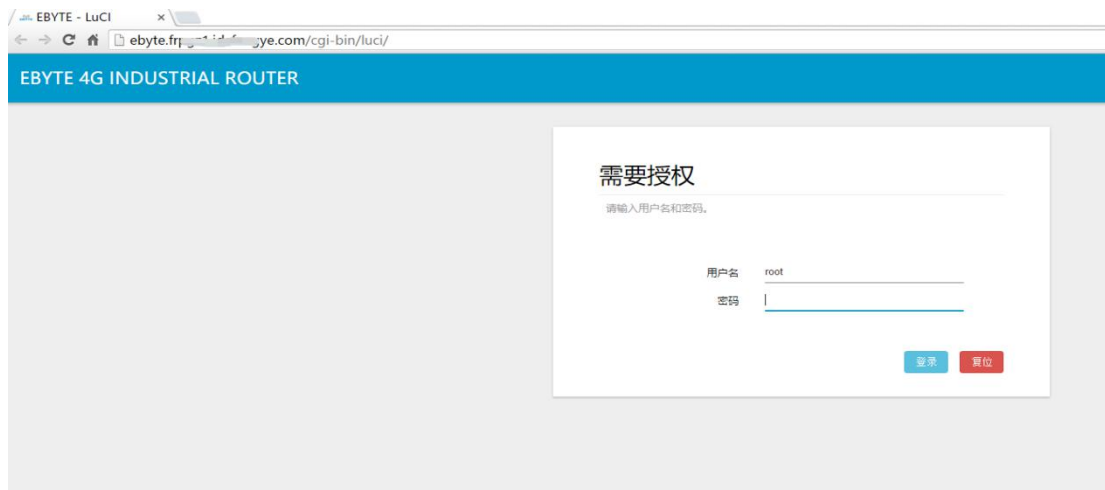


In this setting interface, we need to change the enabled state from disabled to enabled, and then set the relevant parameters corresponding to the server, as shown in the following table.

Server parameter name	Client parameter name	Description
Tunnel protocol	Frp protocol type	http
	Domain type	Select subdomain
Tunnel domain name	Subdomain	ebyte
Local port	Intranet host address	192.168.10.1
	Intranet host port	80 (router web port)
Tunnel name	Service note name	test-ebyte-324717

Other selections default, and then click the Save and Apply button in the lower right corner. And restart the router.

After our intranet penetration function is successfully enabled, enter the Frp public network address in the browser, as shown below. At this time, our management interface appears on the web page, indicating that our intranet penetration start-up was successful.



### 4.3.4 485 Serial port

485 serial port function has the data conversion between local RS485 serial port and Ethernet. Users can send the local serial port data to the remote data receiving port through the network protocol (TCP / IP). Users can also send it to the local serial port. We will explain the RS485 function below.

In Service-> 485 Serial Port Option, you can configure related options for serial port services, as shown below.



As shown in the figure above, the general configuration options include enabling serial port services and related services that enable heartbeat packets. We do not enable them by default here, but if users enable serial port services, in order to prevent the link from breaking, we recommend that users enable the heartbeat packet function at the same time. In the registration packet, you can choose the registration method. Here we provide ICCID and IMEI of SIM card as the registration packet. Of course, users can also customize the registration package content or registration method. In addition, the registration packet and heartbeat need to be explained.

In the serial port configuration options, as shown in the figure below.



Here, the user can set the parameters related to the serial port, no unnecessary details are given here.

In the network configuration, configure the relevant parameters of the network, such operating mode, IP address and port, and the related settings of the transmission mode, as shown in the figure below.



Next, we will show a demo for users' reference.

In the general configuration, we set the following parameters.



In the serial port configuration, we choose the default parameters, namely:

Baud rate: 115200;

Data bits: 8;

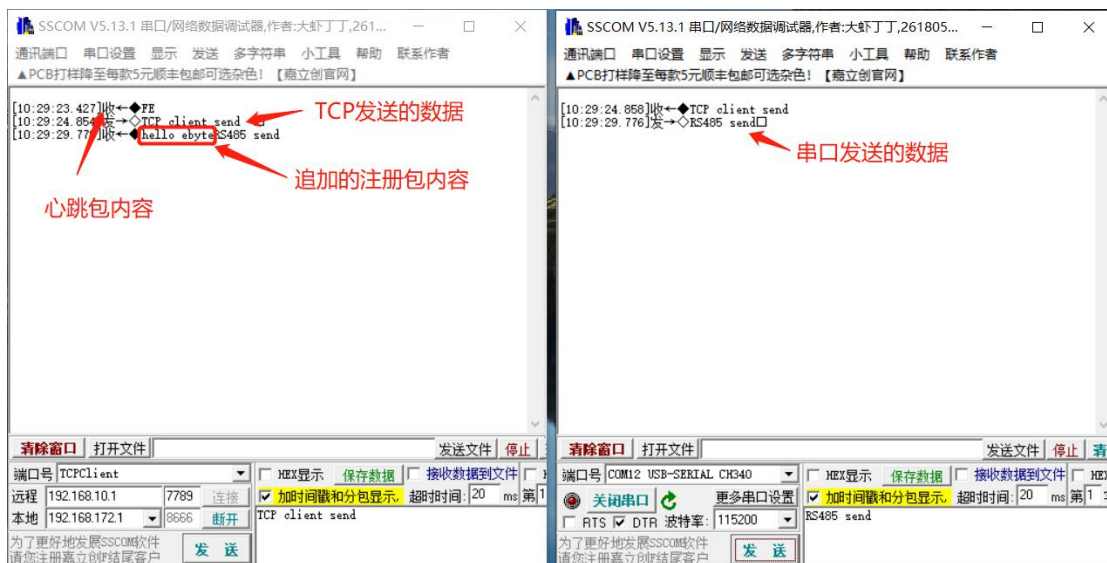
Parity digit: None;

Stop bit: 1;

In network configuration, we do the following configuration.



Now we press the save and apply button (no need to restart the router here).



What needs to be explained here is that when the registration packet is enabled, the registration packet is added only when the serial port data is sent to the Ethernet. No registration packet added when the data sent by the Ethernet to the serial port .

At the same time, RS485 function not only supports the transparent transmission mode, but also supports the Modbus protocol (Modbus RTU and Modbus TCP protocol conversion).

In our demo, the router operates in TCP Server mode and is accessed by LAN. Users can choose relevant network operating mode and remote IP and port according to their needs.

In addition, it should be noted that if users does not connect to the server within 2 to 3 minutes after booting and self-starting in client mode, it will be automatically disconnected. When users confirm that the server is ready, they need to restart the serial-to-Ethernet service (that is, click the Save and Apply button again).

### 4.3.5 VPN Server

The E880-IR01 router supports both VPN client and server mode. Here, we will explain the VPN server (based on the PPTP protocol).

In order to make it easier for users to understand and correctly use VPN functions, we first explain the related concepts of VPN.

VPN (Virtual Private Network) is a virtual private network. It is a remote access technology. It uses the public network to establish a private network of its own. The VPN gateway implements remote access by encrypting data

packets and converting the destination address of the data packets. We can take an application scenario, Xiao Wang of a company is on a business trip in Beijing, he wants to access the intranet server of the company located in Chengdu. At this time, if the company's VPN server is connected through VPN, then Xiao Wang can be assigned a local IP by the server to obtain server resources, or form a "LAN" with other clients (colleague's computers) under the server to achieve remote data interaction.

In the service-> VPN server option, there is the following interface. Among them, in the basic settings, set the gateway IP and client IP (or IP range) of the VPN server and some related operating methods of the VPN.



In the user management settings, set the authentication password and user name of the VPN server. The option column Online Users can view the access information of related clients.

Below we will demonstrate the creation of a VPN server and related considerations.

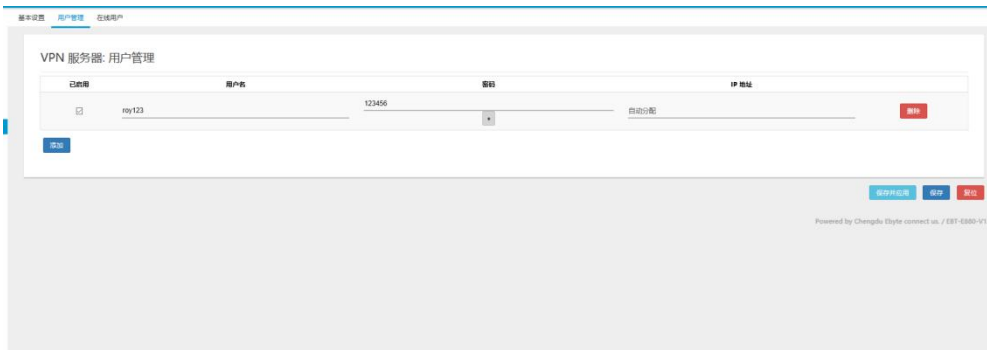
In the basic settings, we set it as follows:



In user management, we set our own password and username, as follows;

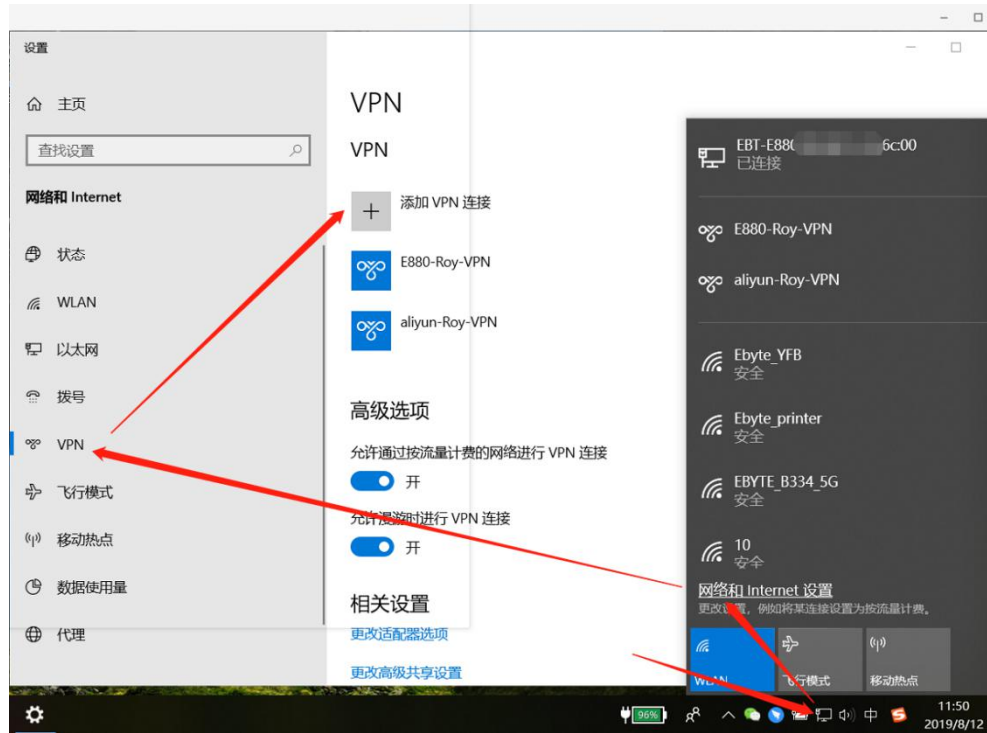
Password: 123456

User name: roy123

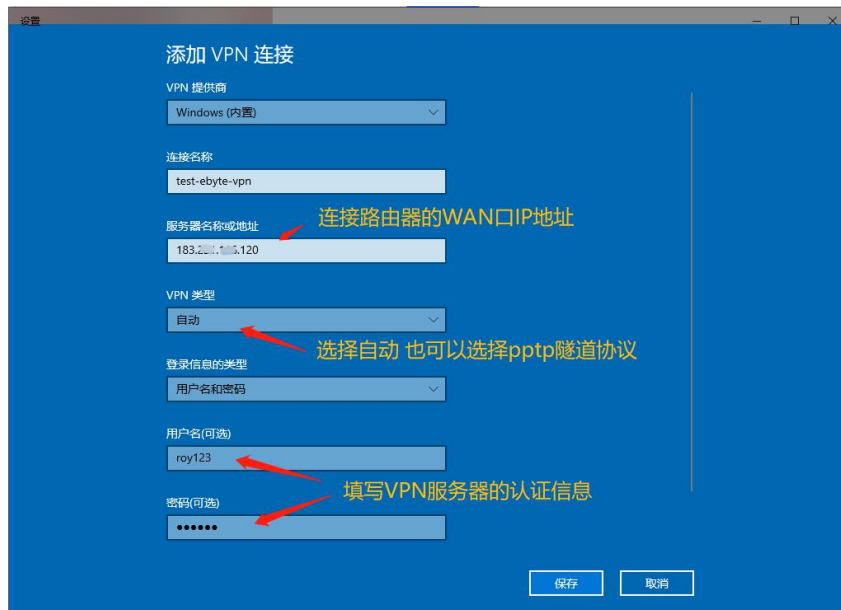


After the setting is completed, we need to restart the router. And after that, our VPN server function starts to work.

At this point, we can set up a VPN client on our computer, and authenticate to the username and password we set up before, and then we can access our VPN server.



As shown in the figure above (win10), we click Add VPN Client and get the following interface.



Then click Save. At this point, we will see one more VPN client.



We click Connect and then the VPN client connects to the routing VPN server.





At this point, when the connection is successful, we open the windows console and enter ipconfig, we will see the following adapter.



Now, our computer has been assigned a remote IP address by the VPN server. We can check the current situation of our router as follows:



Similarly, the clients of other operating systems are roughly the same as those of windows. Users should note that the IP address of the VPN server is the same as the address mapped on the WAN port. When users use the VPN client to connect to the server and fill in the server name, they should fill in the IP address of the WAN port instead of 192.168.30.1 IP in the figure above. In addition, users need to know that when the VPN private network is established on the public network, the public network is disconnected, and the private network is immediately disconnected as well.

### 4.3.6 SIM Card

In the network-> SIM card option, you can configure the network access mode of 4G SIM card and query basic information of current SIM, as shown in the figure below.

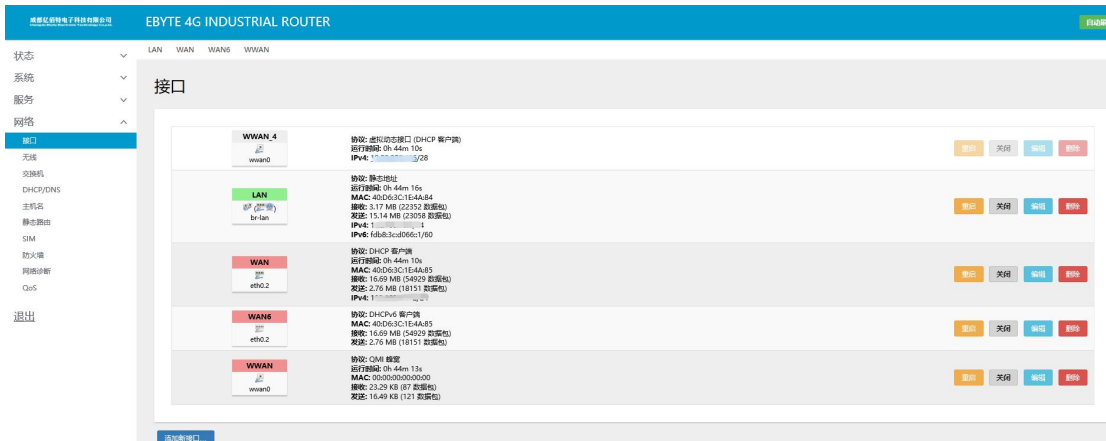


## 4.4 Network

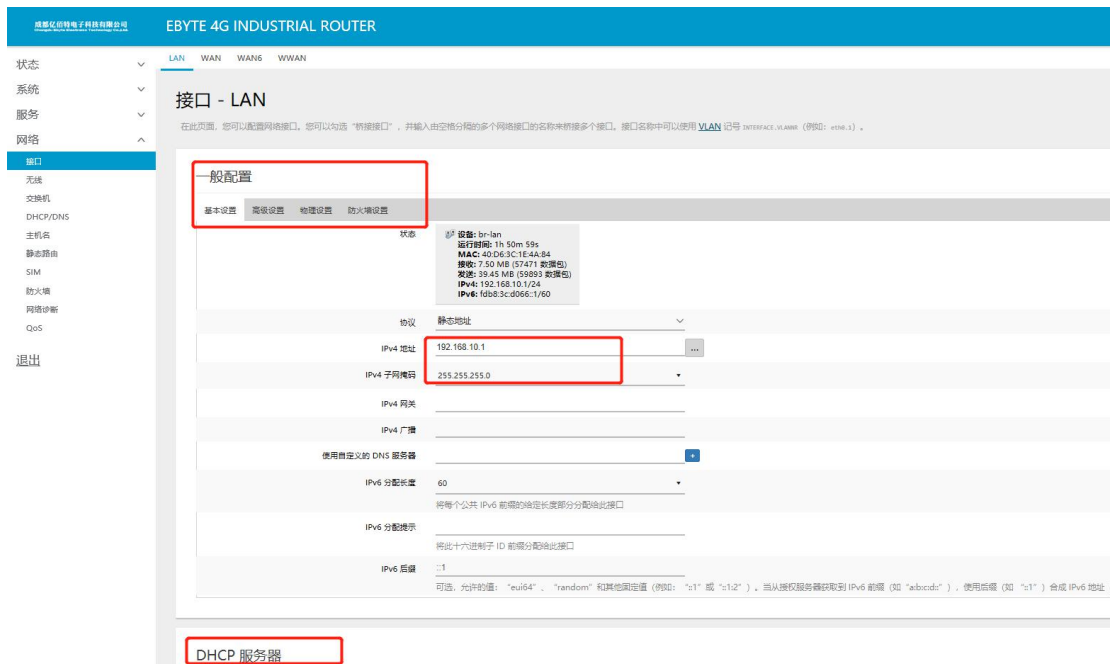
In the network settings column, users can set and query network related parameters, such as login gateway settings, wifi settings, SIM card attributes, firewalls, etc. The following describes some of the commonly used setting options for users.

### 4.4.1 Interface

In Network-> Interface, users can set LAN port, WAN port, 4G network related settings, as shown in the figure below:



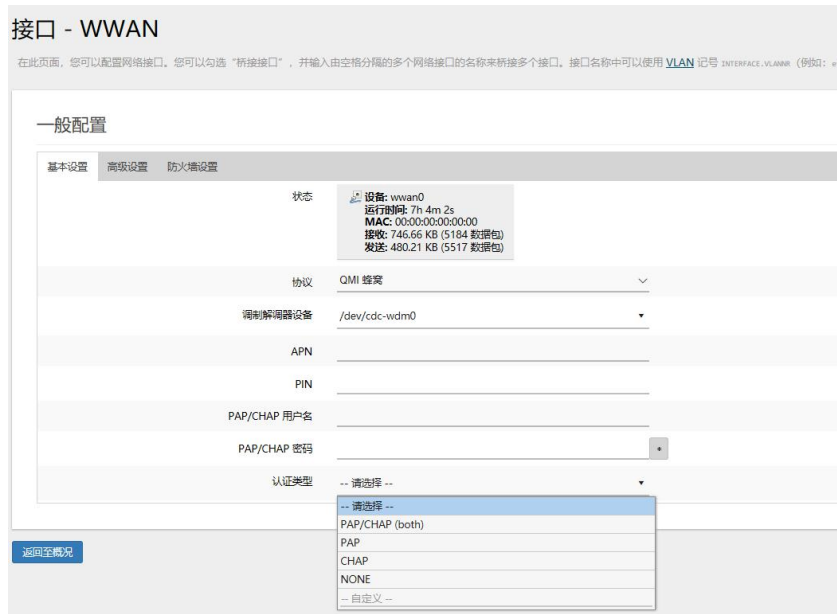
In LAN option, you can set the gateway, subnet mask, etc. of the 4G router and the related settings of the DHCP function, as shown in the figure below.



Users can set the login IP of the 4G router, DHCP IP pool, number of customers, and lease duration, etc. in the general configuration. The default DHCP allocation IP range is 192.168.10.100 ~ 192.168.1.250, and the lease

duration is 12h by default. Dynamic DHCP IP allocation is enabled by default. Users can choose to disable it or not according to their needs.

For the 4G network interface, if users uses an ordinary mobile phone card, it is not necessary to set the relevant APN information. If users use an APN dedicated network card which has a special APN address, when creating a 4G interface, they also need to fill in the relevant APN information in the figure below.



This device also supports VPN clients (pptp, l2tp protocol type). Next, a demo of the VPN client will be given.

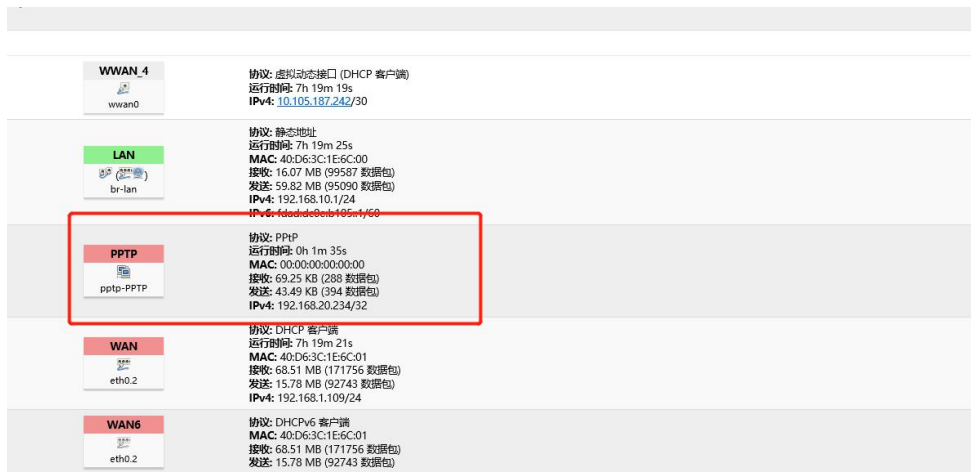
First, we click to add a new interface and get the following information. Here, we set the name to PPTP and the protocol to PPTP.



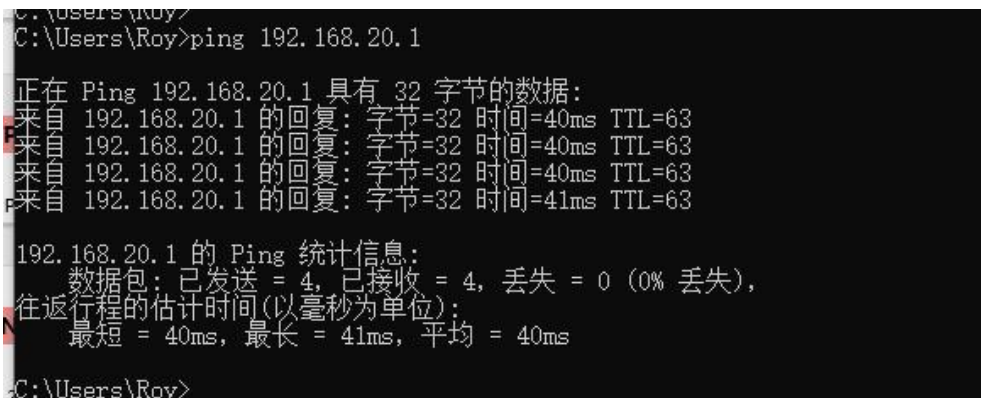
In the basic settings, we enter the corresponding server IP, username and password, and add the interface to the firewall, and save and apply.



Wait for a little while, then, the VPN interface is assigned an IP address by the server, indicating that the remote VPN server is connected.



At this time,our intranet IP of ping server can be pinged.

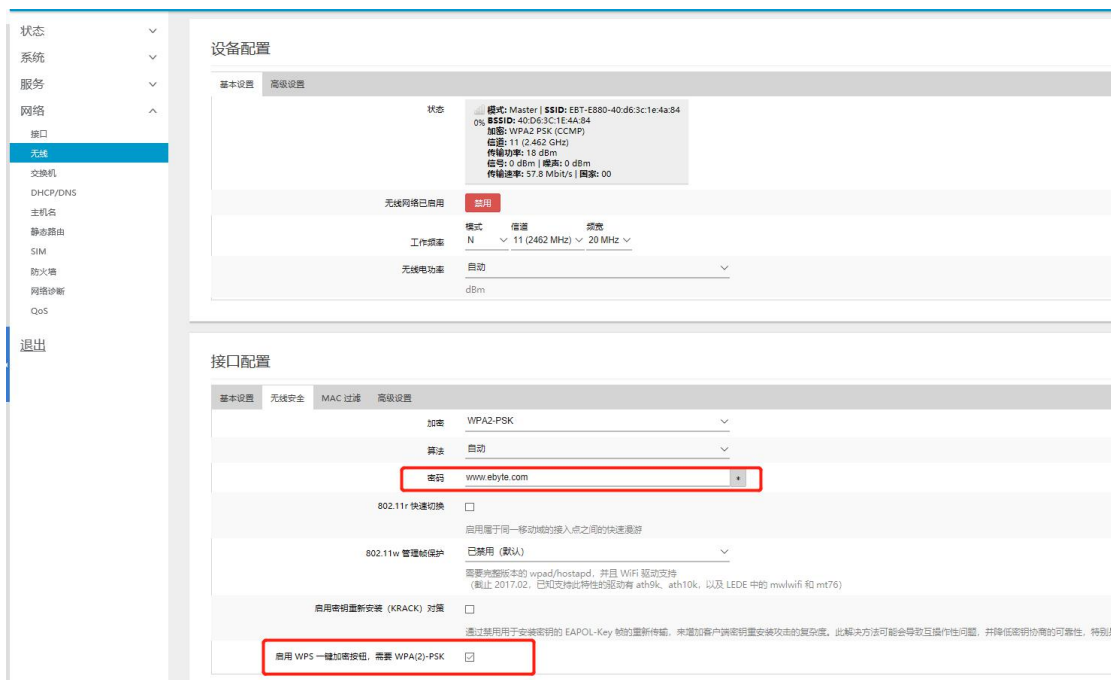


Similarly, the VPN and PPTP settings of the L2TP method are roughly the same.

Here, we do not give an overview of other interfaces. At the same time, we also recommend that customers who do not have special needs or are not professionals, try not to set the relevant parameters of other interfaces. If customers have related questions, please call us for consultation.

### 4.4.2 Wireless

In the network-> wireless-> wireless overview option, click the edit option and users can set and query wireless related parameters, such as setting wireless password, operating mode, MAC filtering, etc., as shown in the figure below.



In wireless WIFI, the default WIFI name is: EBT-E880-XX: XX: XX: XX: XX: XX

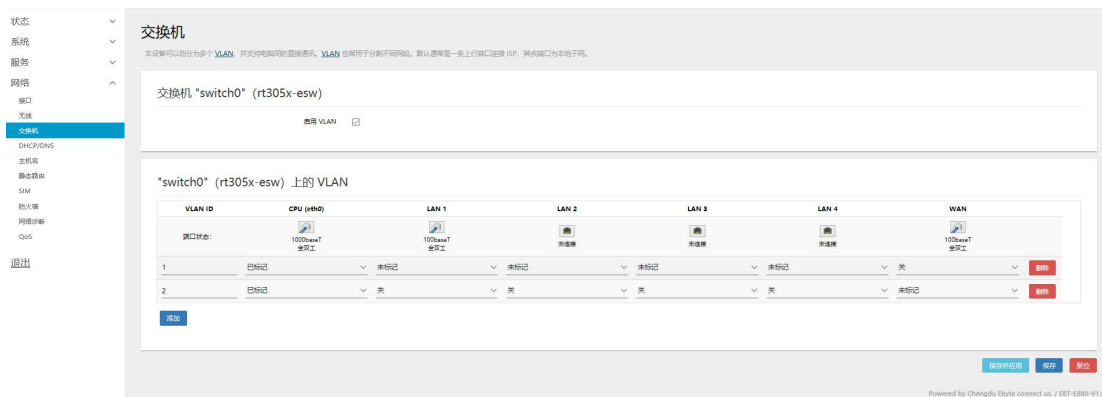
The characters after EBT-E880- are the MAC address of the device.

WIFI default password is: www.ebyte.com

In addition, the 4G router has the WPS one-click Internet access function, which is turned on by default. If users want to connect to the device wirelessly, they need to turn on the WPS button function of the WIFI device, and then short press the WPS button on the side of the device and easily connect to WIFI without entering password.

### 4.4.3 Switch

In the network-> switch option, users can combine the network-> interface to set the type of network port (such as LAN port and WAN port) or enable / disable the network port. In later versions, The relevant settings will be combined with load balancing. The setting interface is shown in the figure below.



#### 4.4.4 Host name

In the network-> host name option, custom domain name resolution can be implemented. Users can fill in any host name (domain name) they want. Here we set "EBYTE-4G-ROUTER" as the host name, corresponding IP address is 192.168.10.109. In this way, the mapping between the host name and the IP address is realized. When the local resolution EBYTE-4G-ROUTER actually resolves the 192.168.10.109 address.



然后，我们在 windows 命令行 ping 一下主机名如下：



#### 4.4.5 Static routing

Static routing can realize the setting communication of two different network segments. Assume the following configuration:

The WAN port address of router R1 is 192.168.0.112, and the LAN port gateway is 192.168.10.1;

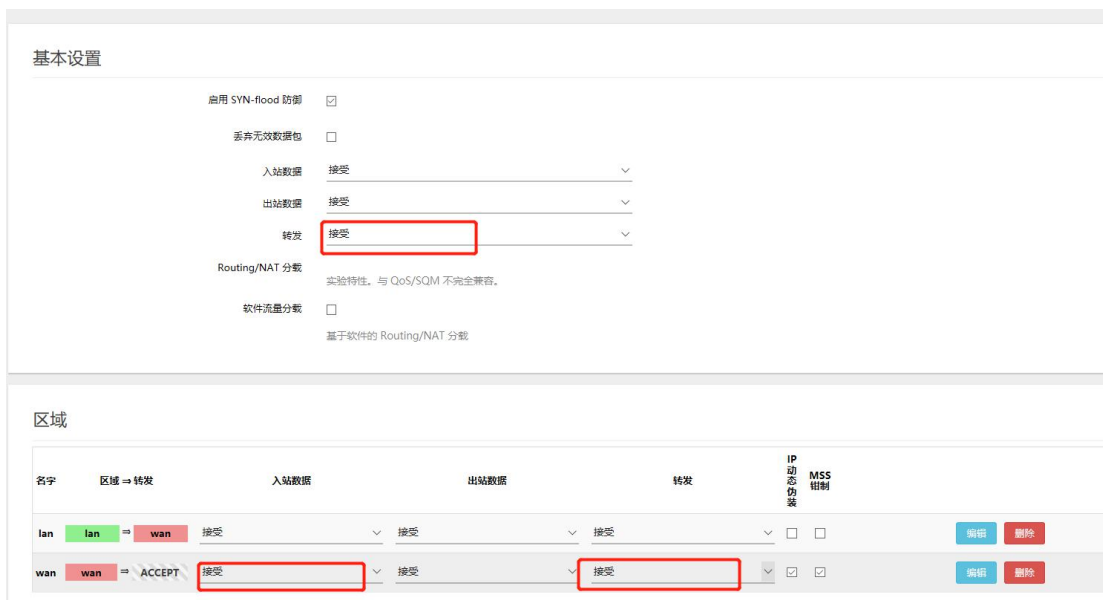
The WAN port address of router R2 is 192.168.0.147, and the LAN port gateway is 192.168.20.1;

If users want to realize that the PC under the R1-LAN port on the LAN accesses the PC under the R2-LAN port to

implement communication functions on different network segments, a static route can be added to R1 to implement it. First set a static route on R1, and set up on R2 with the same principle, as shown in the figure below:



After adding, forwarding option should be changed from Deny to Accept in Network-> Firewall-> Basic Settings, as shown in the figure below.



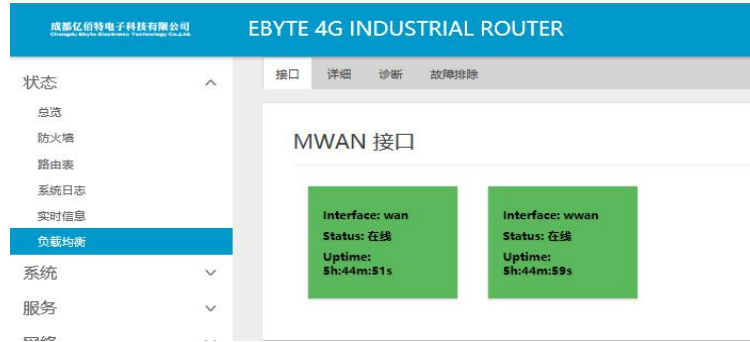
No static routing function is added by default.

#### 4.4.6 Load balancing

Load balancing function can dynamically assign the router's multiple network interfaces (such as wired Ethernet and 4G wireless) to the priority of use of each network, enable, and even the proportion of flow between network ports. It enables users to make relevant allocation mechanisms based on the actual network environment. In the following, we will explain the load balancing function.

On our router, two network interfaces connected are wan (wired Ethernet) and wwan (4G wireless). After we power on, we can check the operating status of the two interfaces in the status-> load balancing option.





Users can handle exceptions in some interfaces or set some parameters through other sub-options.

In the option Network-> Load balancing, users can set the relevant parameters of load balancing, as shown in the figure below.



In this device, we have set two load balancing configurations for multiple network ports by default for users. Next, we will give a brief description of the relevant sub-options of this function for the load balancing formed by these two interfaces. Users can learn to configure their own rules after understanding it.

**Interface:**

It is used to add, delete or configure all external network access interfaces that need to be load balanced, and configure related parameters for interface status definition and detection.

Via the edit button, you can view the related settings between each interface. Some parameters are described below.

[Tracking IP]: Check whether the external network access of the device is normal by detecting and tracking the pinged destination host, which is usually the public IP.

[Tracking Reliability]: Specify how many IP addresses can be connected when the interface is considered online.

[Ping count]: Number of pings on the external network.

[Ping timeout]: When the ping of the external network is unreachable or there is no response, it is considered timeout.

[Ping interval]: How often ping the destination host IP.

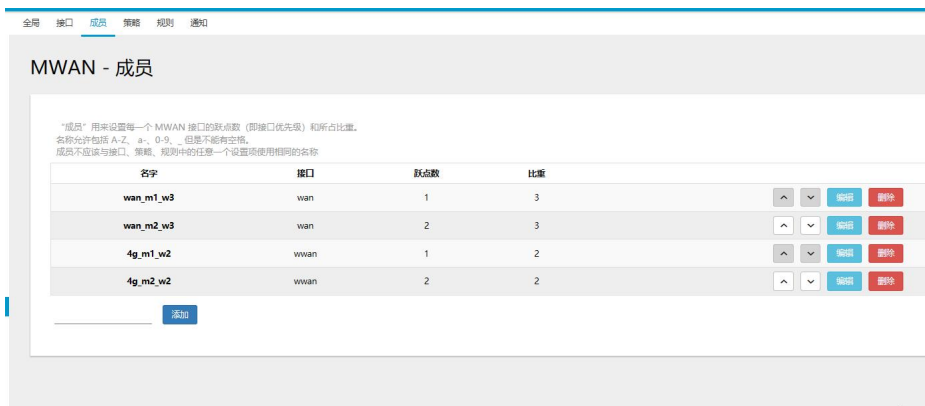
[Interface offline]: When the number of ping failures reaches this value, the interface will be considered offline.

[Interface online]: When the number of successful pings reaches this value, the interface that is considered offline will be online again.

[Hop number]: It shows the priority configured by this interface in multiple interfaces (the smaller the hop value, the higher the priority). It cannot be modified here.

**Members:**

It is used to set the number of hops (that is, the interface priority) and the proportion of each MWAN interface. The member naming rule is generally: "interface name\_hop number\_weight ratio". As shown in the figure below.



The above defines four members, each with different hop counts and weight combinations, which provide services for the subsequent strategies.

**Strategies:**

Used to group members and tell MWAN how to distribute rate of flow using this policy in "rules". Members with lower hops will be used first. Members with the same number of hops divide the flow proportionally according to the weight. Members with a higher proportion of load balancing members will be allocated more flow. This device has 5 default strategies, as shown in the figure below.



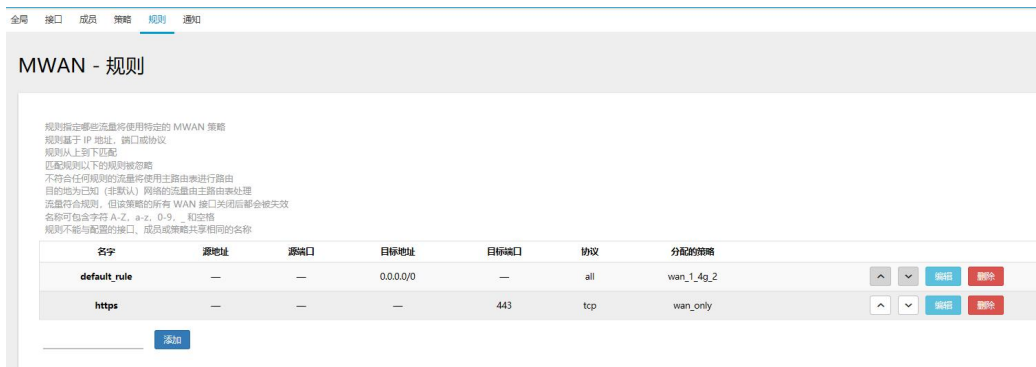
The explanation is shown in the following table:

Name	Description
wan_only	Only use flow from the wired Ethernet interface
balanced	Use Flow from both Ethernet and 4G wireless interfaces and is obtained at a ratio of 3: 2
4g_only	Only use flow from the 4G wireless interface
wan_1_4g_2	Wired priority, 4G backup
4g_1_wan_2	4G priority, wired backup

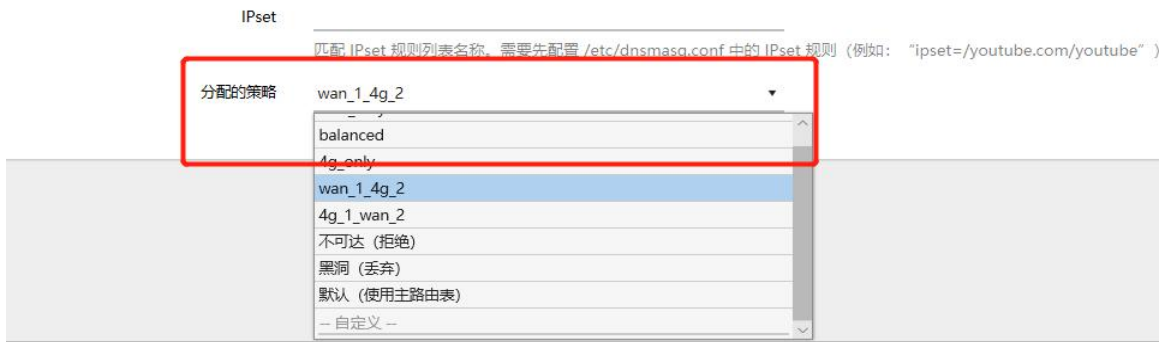
**Rule:**

It divides flow into specified "policies" based on IP addresses, protocols, and ports. Rules are matched in order from top to bottom. Except for the first rule that matches a communication, the other rules are ignored. Communication that does not match any rules will be performed by the system default routing table.

As shown in the figure below, it represents the policy that all target addresses or protocols follow wan\_1\_4g\_2, that is, the wired network data is preferentially used. When the wired Ethernet fails or there is no data flow, flow is obtained from the 4G interface. When the first rule is not satisfied, the next one is matched, otherwise it will be ignored.

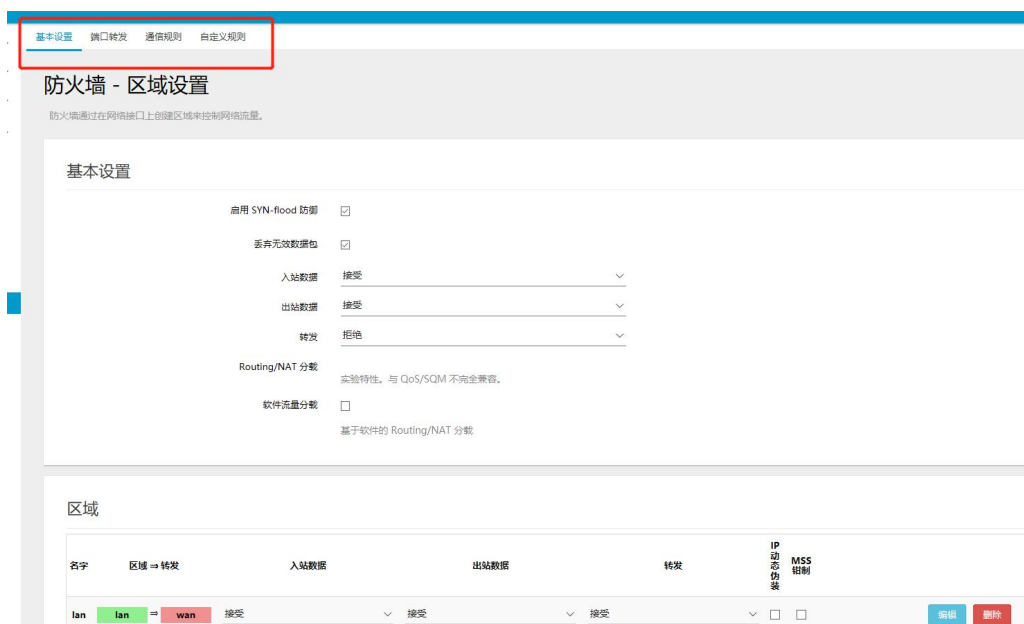


If the current policy type meets the needs of users, users need to click the edit button in the above figure, default\_rule rule, and modify the corresponding policy.



#### 4.4.7 Firewall

In the Network-> Firewall option, set the related settings of network security and communication rules, as shown in the figure below.



### 4.4.7.1 IP Dynamic masquerade (MASQ)

MASQ is MASQUREADE. Address masquerading converts the source IP of the outgoing packet into the IP address of an interface on the router. As shown in the figure, if IP masquerading is checked, the system will modify the source IP address of the data packet out of the router to the WAN port IP address, here, the default method is to enable IP dynamic masquerading.



### 4.4.7.2 Communication rule (SNAT&DNAT)

In Network-> Firewall-> Communication Rules, there is a column called Source NAT. Source NAT is a special form of packet masquerading. It changes the source address of packets leaving the router. For example, the source IP address of the packet that leaves the router is fixedly changed to 192.168.1.1(real IP: 192.168.10.1). The setting interface is as shown below. The name is EBYTE, which is the display interface after the setting. The name is TEST, which is the display interface when adding.



In this device, Source NAT is not added by default. When using this function, users can make related settings according to related requirements.

DNAT is the replacement of the destination address. The destination IP address of the packets entering the router with the destination address being the IP of the WAN port is replaced with the IP address set by users.

### 4.4.7.3 Port forwarding

Port forwarding allows computers from the Internet to access computers or services in the private LAN. For example, if you forward TCP data on port 82 on the external network to port 82 on the internal network 192.168.10.119, you will have the following settings.

### 端口转发

名字	匹配规则	转发到	启用
----	------	-----	----

尚无任何配置

### 新建端口转发

名字	协议	外部区域	外部端口	内部区域	内部 IP 地址	内部端口
Forward	TCP+U	wa	82	lan	192.168.10.119	82

## 4.4.8 Network diagnostics

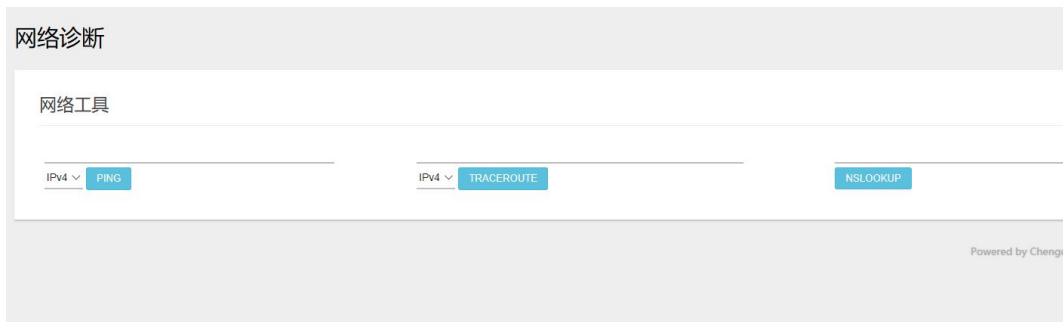
In Network-> Network Diagnostics option, support online diagnostic function:

Ping tool directly operates ping test of specific address on the router.

Router resolution tool, goes through routing when accessing the address.

DNS viewing tool that resolves domain names into IP addresses.

As shown in the figure below.



## 4.4.9 Flow control management (Qos)

In the Network-> Qos option, you can sort data packets based on the network address, port, or service, and perform network speed limit functions on an interface. As shown in the figure below.

接口

WAN

启用

分类组 默认

计算开销

半双工

下载速度 (kbit/s) 1024

上传速度 (kbit/s) 128

添加

删除

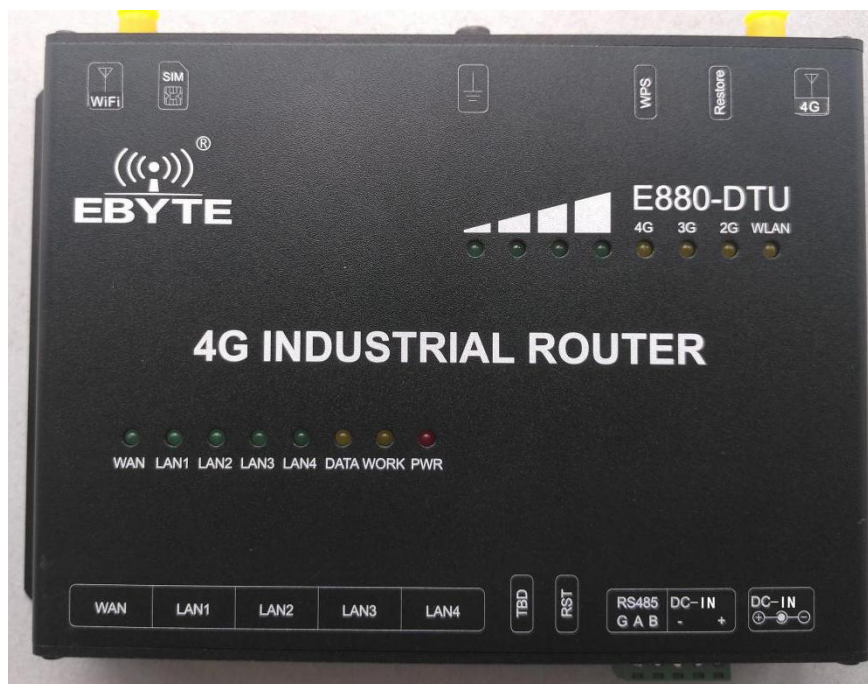
分类规则

目标	源主机	目的主机	协议	端口	字符数	注解			
最高	全部	全部	全部	22,53		ssh, dns	^	v	删除
普通	全部	全部	TCP	20,21,25,80,110,443,993,995		ftp, smtp, http(s), imap	^	v	删除
高	全部	全部	全部	5190		AOL, iChat, ICQ	^	v	删除

添加

## 5. Device panel identification and function setting

The physical picture of the device panel (front view) is shown below



### 5.1 LED Indicator

In the panel, the description of each LED indicator is shown in the following table.

Name	Description
Power	Always on after power on
WORK	After booting, it flashes at a frequency of 1S
WAN	WAN port network cable is plugged in and the other end of the network cable is connected to a device, the light is always on
LAN1-4	LAN port network cable is plugged in and the other end of the network cable is connected to a device, the light is always on
WLAN	when the WIFI network is successfully started, it is always on, and it flashes when there is device access or data interaction.
2G/3G/4G	Current network attribute indicator, all lights off when there is no service, one is on at most
Signal strength 1-4	Indicates the signal quality of the current network attributes. The more the light is on, the stronger the signal is.
DATA	Reserves

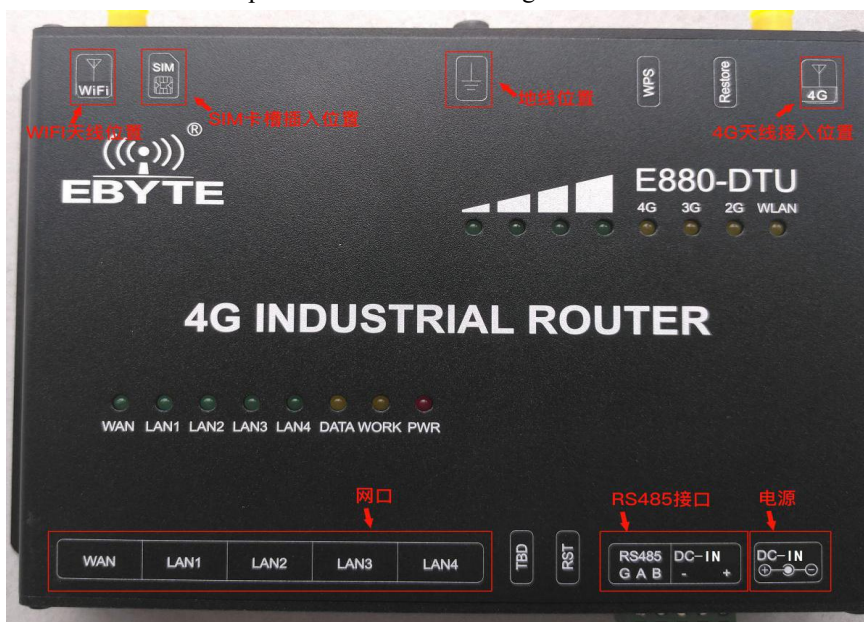
## 5.2 Button setting

In the panel, the functions and instructions of each physical button are shown in the table below.

Name	Description
RST	Hardware reset, short press this button to realize the restart function.
WPS	WPS Internet access function, short press this button, and use WPS button function on the access device to achieve secret-free Internet access
Restore	Long press the button for more than 5s to execute the factory reset function

## 5.3 Other identifications

In the panel, other identifications are explained as shown in the figure below.



## 6. AT SMS command description

This device supports sending AT commands via SMS to remotely control the 4G router. The following are sending instructions and function descriptions.

AT SMS content	Function description
EBYTESMSAT+ATI	Version query
EBYTESMSAT+QCCID	Query 4G module QCCID / ICCID number
EBYTESMSAT+IMEI	Query IMEI Number
EBYTESMSAT+CSQ	Query the current 4G signal quality
EBYTESMSAT+RELD	Restart settings receive message reply + RLAD RUN
EBYTESMSAT+REBT	Restore factory settings receive message reply + RLBT RUN
EBYTESMSAT+QNWINFO	Network attributes currently connected
EBYTESMSAT+CIMI	SIM Card CIMI number



EBYTESMSAT+CNUM	Query the current 4G module number
EBYTESMSAT+QSPN	Query the current telecommunications provider

## 7. Revision history

Version	Date	Description	Issued by
1.0	2019-06-3	Initial version	Blue
1.1	2019-08-18	Added VPN, APN, intranet penetration, load balancing, serial port to Ethernet function descriptions	Xu
1.2	2019-8-20	Format adjustment	Lyl

## About us

Technical support: [support@cdebyte.com](mailto:support@cdebyte.com)

Documents and RF Setting download link: [www.ebyte.com](http://www.ebyte.com)

Thank you for using Ebyte products! Please contact us with any questions or suggestions: [sales@cdebyte.com](mailto:sales@cdebyte.com)

-----  
 Fax: 028-64146160 ext. 821

Web: [www.ebyte.com](http://www.ebyte.com)

Address: Innovation Center D347, 4# XI-XIN Road, Chengdu, Sichuan, China

