



MANUAL DE INSTRUCCIONES

CY-LTE102/105

CONTENTS

CONTENTS.....	1
1.Product Description.....	6
2.Device login and system status check	8
2.1Hardware interface	8
2.1.1 Interface Specification	8
2.1.2 Interface Specification	9
2.1.3 Interface Specification	9
2.1.4 Reset Button.....	9
2.2 Indicator status	10
2.3 Web page login	14
3.System Status	16
3.1 Overview	16
3.1.1 Status bar.....	16
3.1.2 Mobile WAN network and wired WAN status view	17
3.1.3 Memory usage and DHCP connection list	17
3.1.4 WiFi Access Point information.....	18
3.1.5 Load Balancing (optional).....	19
3.2 Routing Table	19
3.3 System Log	20
3.4 Kernel Log	20
3.5 Real-time information	21
3.6 Load balancing	21
4. Basic Network.....	23
4.1 Switch	23
4.2 Hostnames	23
4.3 Static Routing.....	24

- 4.4 Wired Network25
 - 4.4.1 WAN Interface25
 - 4.4.1.1 DHCP Client26
 - 4.4.1.2 Static(wan) address.....26
 - 4.4.1.3 PPPoE dial-up.....27
 - 4.4.2 LAN Interface.....28
 - 4.4.3 MGT Interface30
- 4.5 mobile network.....30
 - 4.5.1 DHCP Dial (single modul single SIM)31
 - 4.5.1.1 Auto network (default)32
 - 4.5.1.2 Lock the network (4G/3G/2G).....33
 - 4.5.2 PPP Dial.....34
 - 4.5.2.1 Automatic network35
 - 4.5.2.1 Lock the network (4G/3G/2G).....35
- 4.6 Wireless Network.....36
 - 4.6.1 AP mode.....36
 - 4.6.1.1 Device Configuration37
 - 4.6.1.2 Interface Configuration38
 - 4.6.2 Client Mode.....40
 - 4.6.2.1 Client DHCP (default)42
 - 4.6.2.1 Client static address43
- 4.7 Static address.....45
- 5. Advanced Network45
 - 5.1 QoS45
 - 5.2 DMZ.....46
 - 5.3 Firewall46
 - 5.3.1 Basic Settings46
 - 5.3.2 Communication rules47
 - 5.3.3 Domain name filtering49
 - 5.3.4 Keyword filtering49

5.4 Portal authentication (optional)	49
5.4.1 General arrangement	49
5.4.1.1 Local Upload	50
5.4.1.2 Download file from URL server address	50
5.4.2 counter.....	51
5.4.3 Filter.....	52
5.4.4 other	52
5.5 Repeater	53
5.6 Port forwarding.....	53
5.7 Static NAT.....	54
5.8 Smarmlink	55
5.8.1 General	55
5.8.1.1 Mode configuration	55
5.8.1.2 Connection configuration	56
5.8.1.3 Serial port configuration	57
5.8.2 advanced.....	58
5.8.3 Operating mode	59
5.8.4 Custom protocol.....	59
5.8.5 Configuration example	61
5.8.5.1 TCP server.....	61
5.8.5.2 TCP Client	64
5.8.5.3 UDP Server	66
5.8.5.4 UDP Client	67
5.8.5.5 Real serial port mode.....	67
5.8.5.6 MQTT Client.....	68
5.8.5.7 Modbus RTU to TCP master-slave communication	70
5.8.5.8 Modbus TCP master-slave communication.....	70
5.9 M2M Cloud platform	70
5.10 Load Balancing (optional).....	71
5.10.1 Global.....	72

5.10.2 Interface	73
5.10.3 Member	74
5.10.4 Strategy	75
5.10.4.1 wan_only	76
5.10.4.2 wwan_only	76
5.10.4.3 3gwan_only	76
5.10.4.4 balanced	76
5.10.4.5 balanced_wan	77
5.10.4.6 wan_primary	77
5.10.4.7 wwan_primary	77
5.10.4.8 3gwan_primary	77
5.10.4.9 wan_wwan_4G	78
5.10.5 Rule	78
5.11 Intranet penetration (optional)	79
5.12 Network Monitoring	79
6.Virtual Private Network.....	80
6.1 GRE Client	81
6.2 PPTP Client.....	83
6.3 L2TP Client	86
6.4 IPsec Client	90
6.4.1 IPsec security strategy	90
6.4.1.1 Basic Settings	90
6.4.1.1 Security proposal	91
6.4.2 IPsec Security Alliance	94
6.5 EOIP Client	94
6.6 N2N VPN Client	95
6.7 OPEN VPN	96
7.System Management.....	99
7.1 System	100
7.1.1 System property	100

7.1.1.1 General Settings.....	100
7.1.1.2 Modification of WAN mode	100
7.1.2 Time synchronization.....	102
7.2 Administration	103
7.3 Backup/flush Firmware	103
7.3.1 Generate Archive.....	104
7.3.2 Perform Reset	104
7.3.3 Upload Archive.....	105
7.3.4 Flash Image	105
7.4 System diagnostics	106
7.5 Device Reboot.....	107
7.5.1 Reboot now.....	107
7.5.2 Reboot timer	107
Appendix: Network Abbreviations	108

The content of this document may be updated from time to time due to product version upgrade or other reasons. Unless otherwise agreed, this document is intended as a guide to use only, and all statements, information and recommendations contained in this document do not constitute any warranty, express or implied.

Document Revision Records

Date	Version	Discription	Author
2015-5-15	V1.0	Initial Release	MC
2017-6-6	V1.1	Supplement/Amendment	MC/DHL
2019-10-8	V1.2	Update	MC/DHL
2021-9-18	V2.0	Update	MC/DHL

1.Product Description

Our router series adopts industrial design, adopts high-performance 32-bit embedded MIPS architecture dedicated network processor, embedded with industrial-grade, high-performance, multi-band mobile 3G/4G communication processing module. Support WCDMA, HSPA+, TD/FDD-LTE, EVDO (CDMA 2000), TD-SWCDMA, GSM and other high-speed mobile broadband network, to provide customers with convenient and fast Internet access or private network transmission, optional embedded Wi-Fi module or multi-LAN port. Provide customers with wired fixed network or wireless WLAN sharing high-speed broadband connection; At the same time, we provide customized advanced VPN (OpenVPN, IPSec) functions to build safe tunnels, which are widely used in finance, electric power, environmental protection, oil, transportation, security and other industries.

The Router series provides users with a Web-based configuration interface, making it very easy to configure and manage the Router. At the same time, the M2M terminal product management platform provides users with remote management of all Router terminals. Through the M2M platform, users can monitor the status of all

terminals successfully connected to the platform, and provide remote control, parameter configuration and remote upgrade services.

This instruction manual introduces to the user how to install and configure the industrial grade Router, and guides the user to get started and use our products quickly after correctly installing the hardware and configuring the basic parameters.

2. Device login and system status check

This chapter mainly introduces and instructs the customer how to judge the current network connection of the device through the state of each indicator light outside the device, and at the same time instructs the user how to connect to the routing device through the computer or other wireless terminals to set and view some parameters. The detailed description is as follows:

2.1 Hardware interface

2.1.1 Interface Specification



Figure 1



Figure 2

1) **Aux**: WiFi antenna SMA interface, or the backup network AUX diversity antenna SMA interface;

2) **3G/4G** : SMA interface of the main antenna of the 3G/4G network;

3) **SIM/USIM**: SIM card slot, standard Mini card is supported(Micro/Nano card not supported);

: SIM card magnetic strip face up during installation, place it in the direction of the small triangle below the card seat, and then push it up into the whole card slot. (Note: the SIM card does not support electric plugging and unplugging, so it is recommended to first power off the device before taking and putting the SIM card, so as not to damage the SIM card);

4) **SIM card eject button**: it is necessary to use a card needle or other sharp object to press this button to eject the SIM card holder;

- 5) **WAN/LAN:** the default is WAN port. After modification, it can be changed to LAN port (see 7.1.1.2 "Modification of WAN mode" -- "3G/4G mode" for details);
- 6) **LAN:** Connect to a computer or other user network device;
- 7) **POWER:** Supply DC head access(DC 7.5V~32V), The standard distribution power adapter is DC12V/1.5A;

2.1.2 2ports Interface Specification



Figure 3



Figure 4

Interface description;

2.1.3 4ports Interface Specification



Figure 5



Figure 6

Interface description;

2.1.4 Reset Button

Operation instructions for Reset: Long press this button in the power-on state and

release it for about 10s to complete the factory recovery of the equipment (all indicator lights are on and off);

2.2 Indicator status

1) PWR Light: power indicator, the yellow light, remains on after power on;

2) WiFi Light: After enabling WiFi, the yellow light is always on;

When WiFi is disabled, it goes off; (no WiFi indicator light);

3) WAN Light: The yellow light flashes when there is a device connected to the WAN/LAN network port; When no device is connected or the network cable is abnormal, the network port light goes out;

4) LAN Light: The yellow light flashes when there is a device connected to the WAN/LAN network port; When no device is connected or the network cable is abnormal, the network port light goes out;

5) NET Light: 3G/4G mobile network dial-up status indicator (Note: when the device is working in wired mode,net light goes out).

2ports and 4ports are as follows;

The network dialing indicator light equipment is described in the following table:



Serial Number	Dialing Status	SIM usage	NET indicator status	SIM status	network status
1	Dialing Failed	No SIM	The green light flashes slowly,	SIM not inserted	not connected

2		Invalid or damaged SIM	and finally goes out	Unplugged SIM Or SIM abnormal	
3		SIM installation error			
4	Dialing	SIM is normal	Flashes Quickly	simready	connecting
5	Dialing successfully	1<=Signal value (weak)<=10	Fast flashing at 500ms frequency		connected
6		11<signal value (general)<=20	Fast flashing at 100ms frequency		
7		21<signal value (stronger)<=31	Always On		

2.1.2 Table 1

The following table briefly describes the details of the network dialing status of the device in "3G/4G mode" or "compatible mode". As follows:

The indicator lights of the ZR1000 device during network dialing are as follows:



Serial Number	Dialing Status	SIM usage	NET indicator status	SIM status	network status
1	Dialing Failed	No SIM	The green light flashes slowly, and finally goes out	SIM not inserted	not connected
2		Invalid or damaged SIM		Unplugged SIM Or SIM abnormal	
3		SIM installation error			
4	Dialing	SIM is normal	Flashes Quickly	simready	connecting
5	Dialing successfully	1<Signal value (weak)<=10	Fast flashing at 500ms frequency		connected
6		11<signal value (general)<=20	Fast flashing at 100ms frequency		
7		21<signal value (stronger)<=31	Always On		

2. 1. 2 Table 2

The indicator lights of device during network dialing are as follows:



Serial Number	Dialing Status	SIM usage	NET indicator status	SIM status	network status
1	Dialing Failed	No SIM	The green light flashes slowly, and finally goes out	SIM not inserted	not connected
2		Invalid or damaged SIM		Unplugged SIM Or SIM abnormal	
3		SIM installation error			
4	Dialing	SIM is normal	Flashes Quickly	simready	connecting
5	Dialing successfully	1<Signal value (weak)<=10	1 indicator light		connected
6		11<signal value (general)<=20	2 indicator light		
7		21<signal value (stronger)<=31	3 indicator light		

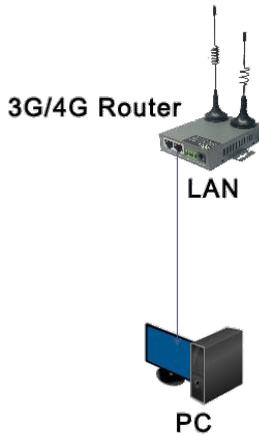
2.1.2 Table 3

2.3 Web page login

The industrial router products support users to view and set relevant product parameters with the login mode of Web terminal. The specific operations are as follows.

Step1: Hardware connection

Connect the router's LAN port to the computer. The computer's LAN card can set the automatic access address (or set the static IP address, but make sure it is on the same network as the router, otherwise you will not be able to log in to the router later. The default LAN address of the router is 192.168.1.1, and the netmask is 255.255.255.0) .



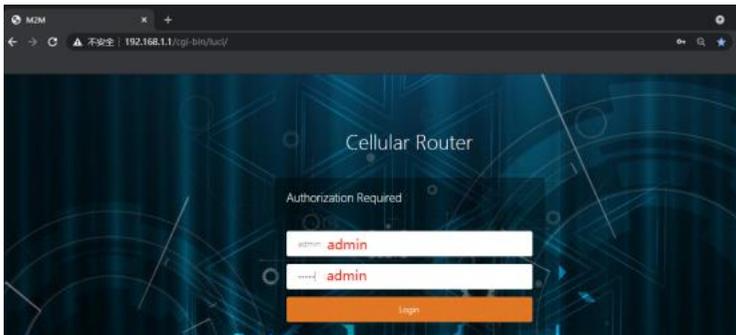
Device connection

Step 2: Check your computer's IP address

Open the computer's local connection and check whether the computer has obtained an IP address.

Step 3: Log on to the router Web using your browser

Open any browser, log in at the default address 192.168.1.1, enter the default user name/password admin/admin (for the safety of the device, it is strongly recommended to change the default password when using the device, please refer to Section 7.2 "Management Rights" for details), and finally press Enter to enter the device Web page. As follows:



3. System Status

This chapter mainly instructs the user how to view the current status information of the routing device through this function, and make a preliminary judgment of the status of the current network access.

3.1 Overview

After logging in the router Web, click "System Status" -- "Overview". Here you can view some detailed information of the product, as follows:

3.1.1 Status bar

Here you can view the product system name, product model, product serial number, firmware version, hardware type (single module single card/dual module dual card), MAC address, WAN mode (wired mode/compatible mode /3G4G mode), load situation and other information.

System Status			
System Name	Product Model	Product ID	Product Version
System Name	10201	Product Model	1020101
Product Model	1020101	Product ID	102010101
Product Version	102010101	Product Name	10201010101
Product Name	102010101	Product Type	10201010101
Product Type	102010101	Product Status	10201010101
Product Status	102010101	Product Mode	10201010101
Product Mode	102010101	Product Load	10201010101
Product Load	102010101	Product Average	10201010101
Product Average	102010101	Product Load Average	10201010101
Product Load Average	102010101	Product Load Average	10201010101

3.1.2 Mobile WAN network and wired WAN status view

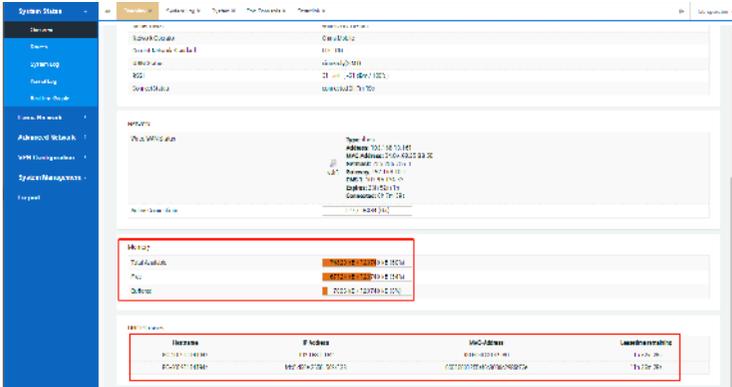
Here you can view the mobile network status details of the device, such as: SIM card insertion status and 3G/4G dialing details, 4G module identification, base station network received signal strength (RSSI) and the current network connection duration, etc.



3.1.3 Memory usage and DHCP connection list

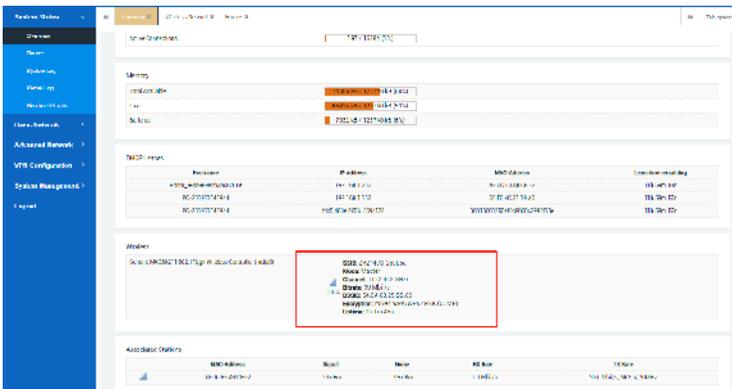
Here you can view the current memory usage of the device, including available memory, unused memory, buffers.

You can also view the list of devices connected to the DHCP server.



3.1.4 WiFi Access Point information

Here you can view the WiFi enabled status and working mode (AP/Client) of the device. At the same time, you can also check which wireless terminals are connected below, such as mobile phones, laptops, etc.



3.1.5 Load Balancing (optional)

Here you can view the load balancing (MWAN3) interface status of the device (3G/4G mobile WAN and wired WAN), such as online or offline.

The screenshot shows the MWAN3 interface status page. It includes a table with columns for Interface, IP Address, WAN Address, and Load Balancing. Below the table, there are three status indicators for WAN1, WAN2, and WAN3, each with a green 'Online' label.

Interface	IP Address	WAN Address	Load Balancing
wan1	192.168.1.101	192.168.1.101	WAN1 WAN
wan2	192.168.1.102	192.168.1.102	WAN2 WAN
wan3	192.168.1.103	192.168.1.103	WAN3 WAN

3.2 Routing Table

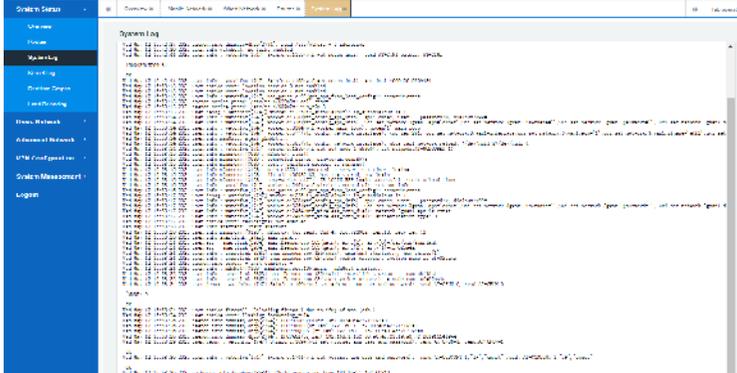
Here you can view the current host address list information through the ARP list; All active IPv4 and IPv6 routing links can be viewed at the same time as follows.

The screenshot shows the Routing Table page. It includes a table with columns for Interface, IP Address, MAC Address, and Status. The table is divided into IPv4 and IPv6 sections.

Interface	IP Address	MAC Address	Status
wan1	192.168.1.101	08:00:27:16:55:28	WAN
wan2	192.168.1.102	08:00:27:16:55:28	WAN
wan3	192.168.1.103	08:00:27:16:55:28	WAN

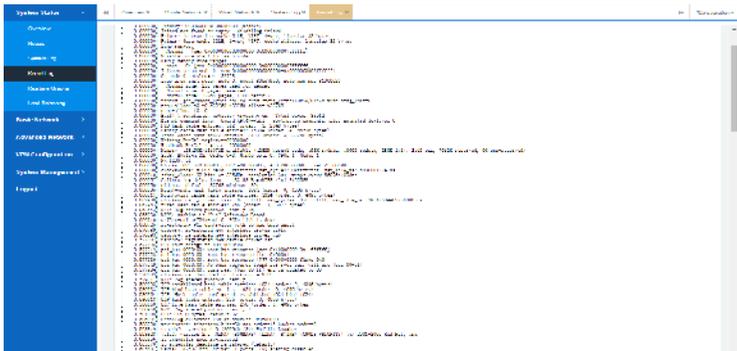
3.3 System Log

Here you can view the log details of the current function modules of the device. When there is an abnormal operation of the device, we can locate the on-site problems of the customer according to the log.



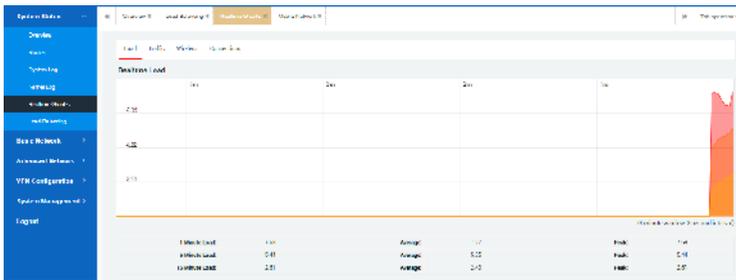
3.4 Kernel Log

Here you can view the device background system driver interface startup information, when there are some device connection or startup abnormalities, you can use these logs to further locate customer field problems.



3.5 Real-time information

Here you can view the device load in real time (such as the load details in the 1st, 5th and 15th minutes), the upstream and downstream real-time traffic situation of different network interfaces, the signal and noise situation of WIFI and the link of other activities.



3.6 Load balancing

1) Interfaces

Here you can check the current online and offline status of each interface (WAN for wired WAN, WWAN for wifi client, 3gwan1 for 3/4G mobile network) of the system after the load balancing function is enabled (the system does not open load balancing by default, if you need to use it, please place an order and comment).

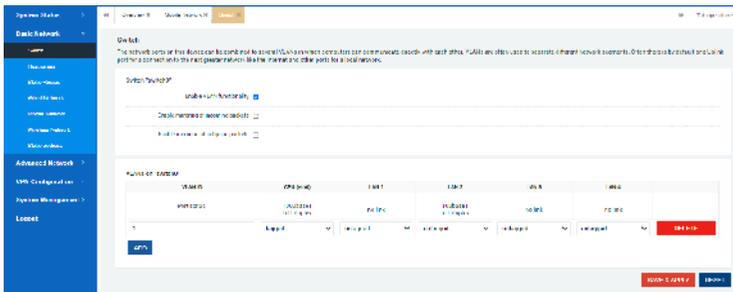


4. Basic Network

This chapter mainly introduces several different external network access scenarios supported by our router, including wired WAN network, WIFI client network, 4G mobile dial up network, etc. The following mainly introduces the use of these specific configuration methods.

4.1 Switch

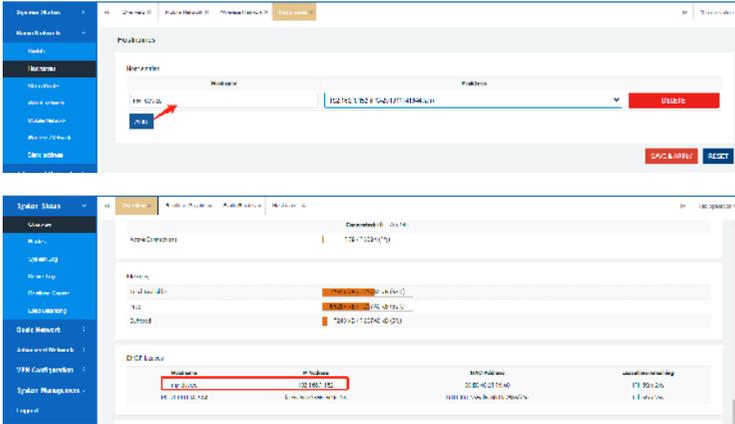
This part can divide the device into VLAN to divide the system network into different network segments. The details are brief.



4.2 Hostnames

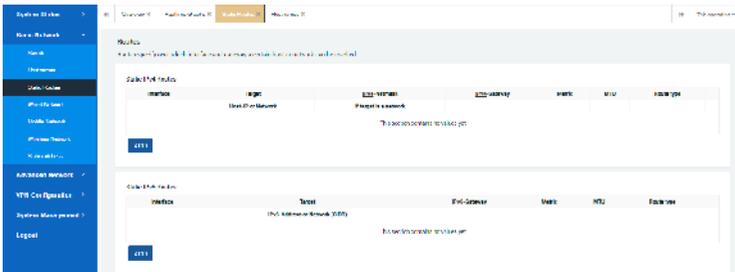
Here, by clicking the "add" button, you can customize the host name of the device connected to the router based on their different IP address.

Example configuration: Customize a host named 'my_device' for the computer with IP address 192.168.1.152 connected to the router. You can see this host information in the System State Overview section.



4.3 Static Routing

This section allows you to view all the current IPv4 / IPv6 dynamic routing tables of the system; You can also create a static routing table (mainly IPv4) by clicking the "Add" button to set up communication with the specified target network.

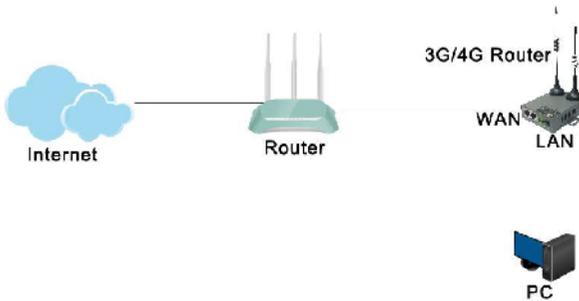


4.4 Wired Network

This chapter mainly introduces several different network configuration modes of wired WAN in routing system, including dynamic WAN address, static WAN address, and PPPOE broadband dial-up mode.

4.4.1 WAN Interface

Cable WAN network mode is to point to by a line bridge connecting mode connect a router's WAN port to another (superior) the router LAN port and make itself has the capability of network access (supervisor should pay attention to union of two router LAN network cannot be completely the same, otherwise result in network conflicts, you can change any of a router LAN address to avoid conflict).



4.4.1.1 DHCP Client

As shown in the figure below, the system defaults to the working mode of "DHCP client", that is, after accessing the superior router network, it will automatically obtain the IP address to access the Internet.

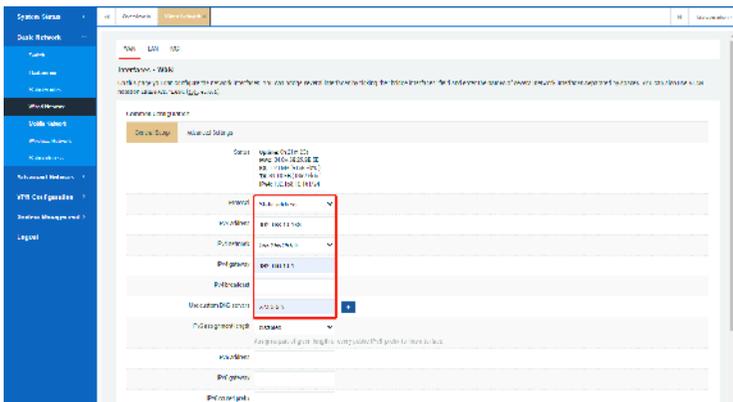
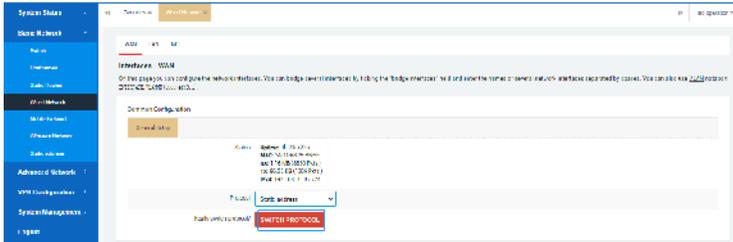


4.4.1.2 Static(wan) address

In addition to automatic WAN access, you can also set the static IP address (must be set to the same network segment as the router above, the mask must be the same, the gateway address and the DNS address also need to be set; For example, the parent router network is 192.168.10.0/24, and the gateway address is 192.168.10.1).

The configuration is as follows:

Select "Basic Network" -- "Wired Network" -- "WAN" -- "General Setup", select the protocol as "Static Address", then switch the protocol and set IP address, subnet mask, gateway address and DNS server, and save the application.

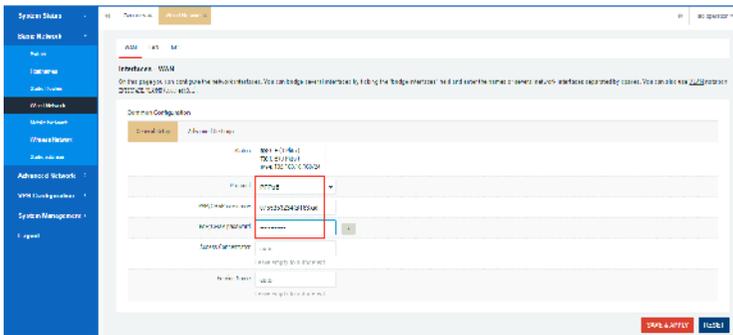
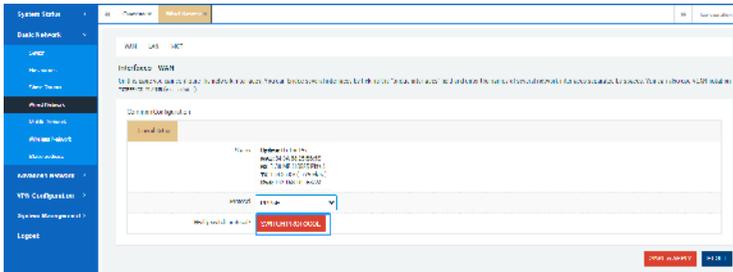


4.4.1.3 PPPoE dial-up

This method mainly refers to using a broadband account assigned by a carrier or other ISP network provider to access the Internet.

Configuration actions:

Select "Basic Network" -- "Wired Network" -- "WAN" -- "General Setup" and select the protocol as "PPPoE". After switching the protocol, fill in the corresponding PAP/CHAP user name and password, and save the application.

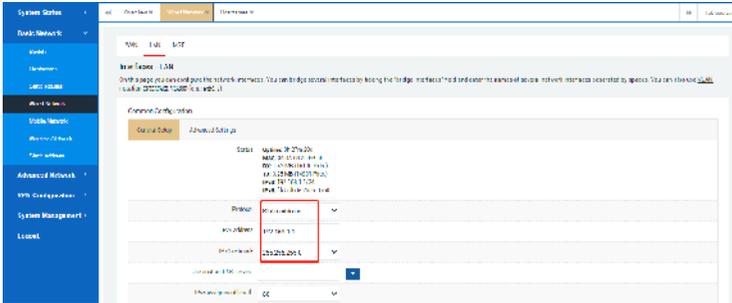


4.4.2 LAN Interface

The router gateway IP address is 192.168.1.1 by default. You can also set the DHCP server configuration here.

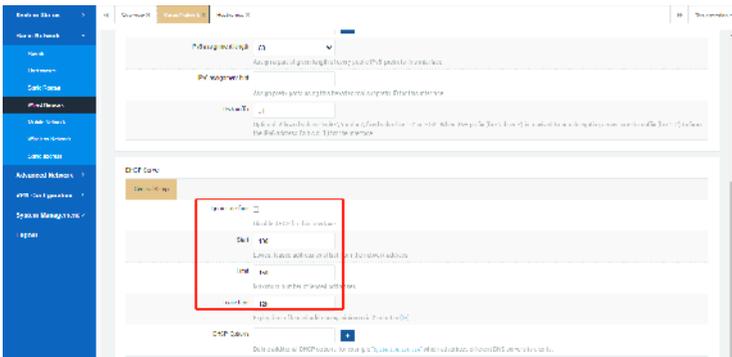
1) LAN address modification

The default router LAN gateway IP address is 192.168.1.1, netmask 255.255.255.0. You can use the image below to change the IP address and netmask and save the application, and then use the new address to access the router configuration page.



2) DHCP server configuration

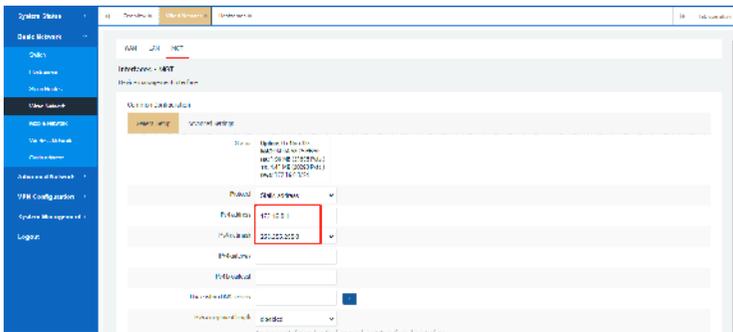
The router DHCP server is enabled by default. You can also set the starting address of the address pool, the maximum number of addresses, the expiration date of the address lease, and the use of specific DNS server addresses. Of course, you can turn it off if you need to.



4.4.3 MGT Interface

This interface is used as an alternate address (usually when the LAN port gateway address is forgotten or the current network address is used in conflict).

After connecting the computer to the router LAN port with a network cable, it is necessary to manually configure the IP with the same network segment as the MGT management address (the default is 172.16.0.1). Then enter 172.16.0.1 in the browser to log in to the router.



4.5 mobile network

3G/4G wireless router is a kind of wireless communication equipment for the Internet of Things, which supports international standard FDD-LTE, TDD-LTE, WCDMA (HSPA+), CDMA2000 (EVDO), TD-Scdma GSM (GPRS/EDGE)/CDMA 2G/ The 3G/4G mobile broadband network standard provides users with convenient and fast high-speed network transmission functions.

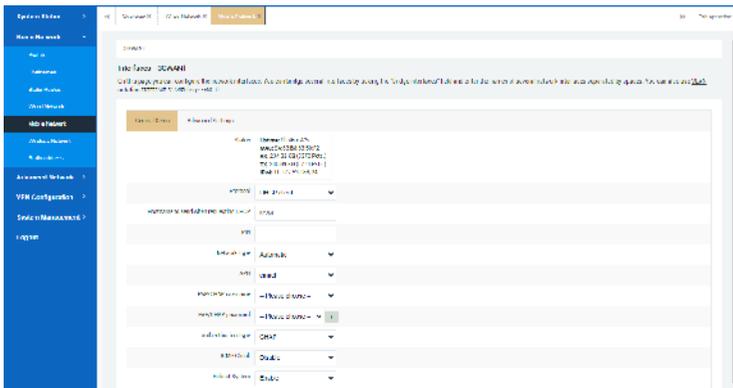
Here we mainly introduce two different dialing methods of mobile network and

the configuration and use of accessing APN and VPDN network. At present, our company's 5-mode and 7-mode full Netcom 3G/4G router equipment supports all operators' network standards. Actually, it depends on the type of router modem selected by the user and the local operator's network support.

4.5.1 DHCP Dial (single modul single SIM)

By default, the device uses DHCP dialing, which is also the preferred module dialing method supported by most module manufacturers. This method has fast dialing speed and strong compatibility. This way of dialing generally does not need to manually configure the SIM card APN information. When dialing, the device will automatically recognize the different APN information of the operator (note that some IoT cards or VPDN private network cards need to manually configure the APN information, user name and password, otherwise the dialing will fail).

Specific operation: select "Basic Network" --- "Mobile Network" --- "3GWAN1" --- "Basic Settings", select "Protocol". as follows:



The main dialing parameters are described as follows:

[Protocol]: Optional DHCP client/PPP mode dialing;

[Host name sent when requesting DHCP]: Default M2M;

[PIN]: SIM card pin code, the default is OK, generally no need to set;

[Network type]: The default is automatic, and the "auto/4G/3G/2G" mode can be manually selected;

[APN]: The network access point required by the operator's SIM card, generally for the Internet of Things card;

[PAP/CHAP Username]: Username authentication required for dialing, fill in according to the specific situation;

[PAP/CHAP password]: The user name authentication required for dialing, fill in according to the specific situation;

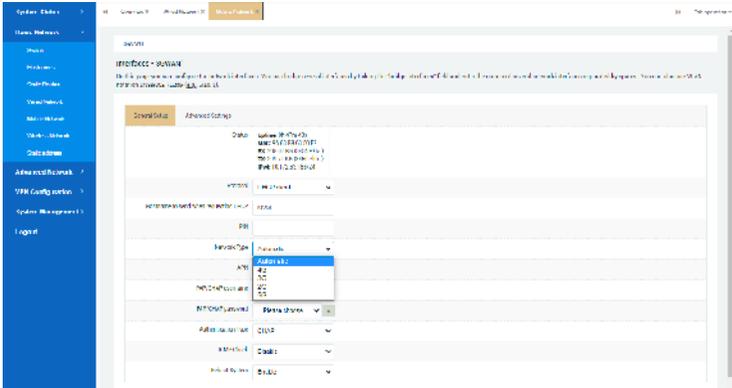
[Authentication type]: including CHAP/PAP authentication;

[ICMP detection]: 4G network detection, disabled by default, fill in according to the specific situation;

4.5.1.1 Auto network (default)

The default network mode of the mobile network of the device is "automatic" mode, that is, the device will automatically identify the matching network according to the overlay network mode, signal strength, and network mode supported by the SIM card used by the surrounding operator base stations. If there is a 4G signal around, it will automatically match the 4G network first; when there is no 4G network, it will automatically recognize and switch to the 3G network; when the 3G network signal is poor or there is no network, it will automatically switch to the 2G network.

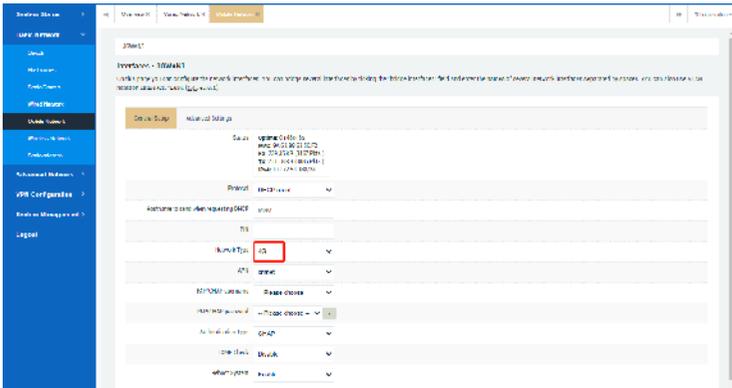
Specific operation: select "Basic Network" --- "Mobile Network" --- "3GWAN1" --- "Basic Settings", select "Network Type", as follows:

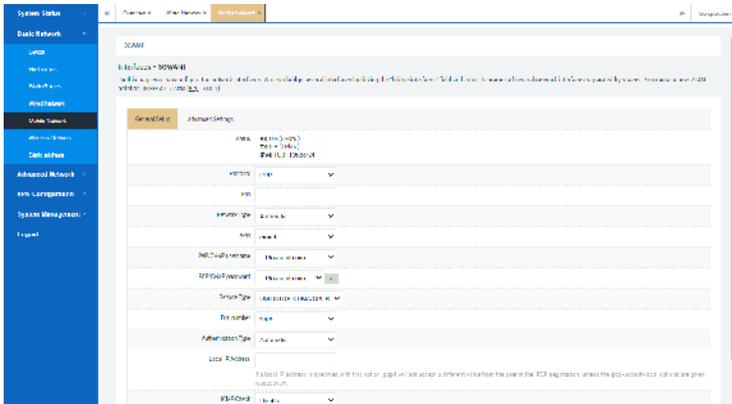


4.5.1.2 Lock the network (4G/3G/2G)

Specific operation: select "Basic Network" --- "Mobile Network" --- "Basic Settings", change the "Network Type" to 4G" mode, and save the dial-up networking information ("System Status" --- "Overview" ---"3G WAN1 (mobile network) status").

As follows:





4.5.2.1 Automatic network

See for details [4.5.1.1](#)

4.5.2.1 Lock the network (4G/3G/2G)

See for details [4.5.1.2](#)

Notice:

- 1) For the use of APN IoT card or VPDN dedicated network card, please fill in the APN access point information and PAP/CHAP user name and password correctly, otherwise the system cannot complete dial-up networking.
- 2) For the VPDN private network card scenario, it is generally not allowed to access the external network. Please log in to the device page and find the "High Level Network"---"Network Monitoring", turn off this function or modify the default ping address to be a valid and connectable other private network address, otherwise it will cause the device to periodically restart about 10 minutes.

4.6 Wireless Network

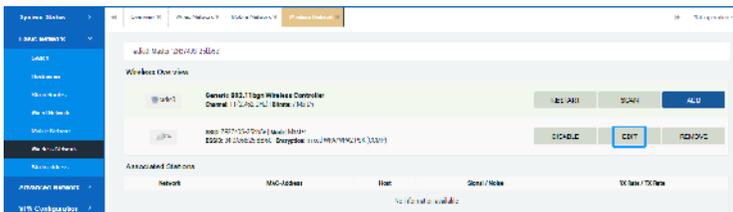
The following mainly introduces two commonly used wireless working modes.

Access point AP mode: This working mode is to use the router as a wireless transmitting point, which can provide mobile phones, laptops or other wireless terminals to connect to the Internet through wireless means (Wi-Fi has no password by default before V2.1, and it is strongly recommended for the safety of the device. Please set the WiFi password when the customer uses the device; after the V2.1 version, the default WiFi password is admin123). Specific operations such as [4.6.1](#).

Client mode: This mode refers to the use of the routing device as a wireless client, which can enable itself to have networking capabilities by searching and joining other wireless hotspots around it, that is, wireless bridging. Specific operations such as [4.6.2](#).

4.6.1 AP mode

Specific operation: select "Basic Network" --- "Wireless Network" --- "Wireless Overview" to check and confirm. as follows:



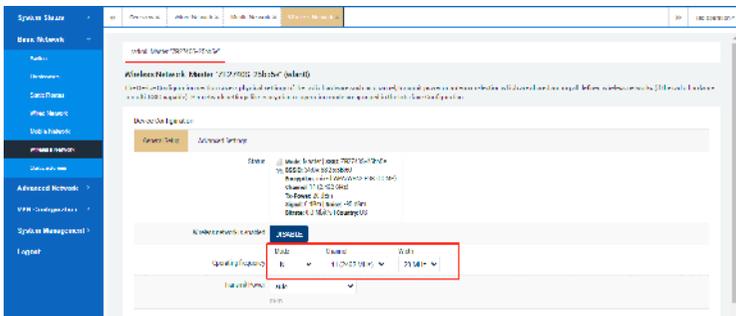
Click the Add button to add a WiFi interface, which can be used to configure the access point AP or client mode.

4.6.1.1 Device Configuration

Click the "Edit" button on the right of "Wireless Profile" and enter "Device Configuration" to configure the basic and advanced settings of wireless WiFi.

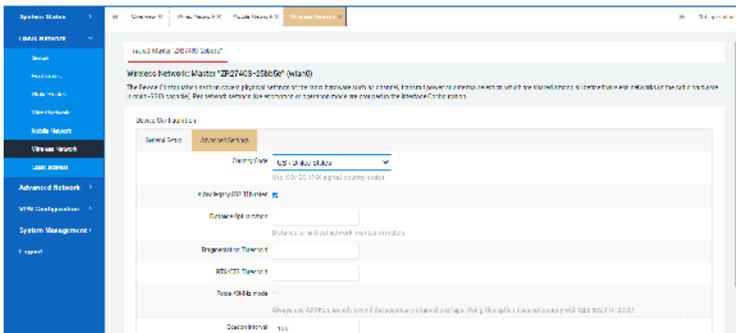
4.6.1.1.1 Basic Settings

Through the "Basic Settings" option, you can configure the wireless network (WiFi) switch, wireless channel selection and radio power adjustment, as follows;



4.6.1.1.2 Advanced Settings

Through the "advanced settings", you can set the country code, distance optimization and other settings, as follows:

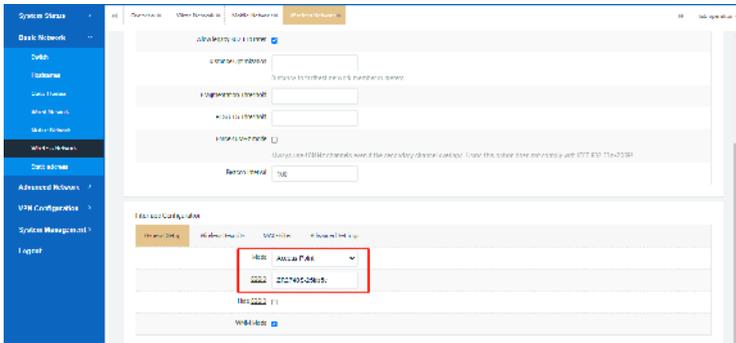


4.6.1.2 Interface Configuration

Click the "Edit" button on the right of the wireless profile and then enter the "Interface Configuration".

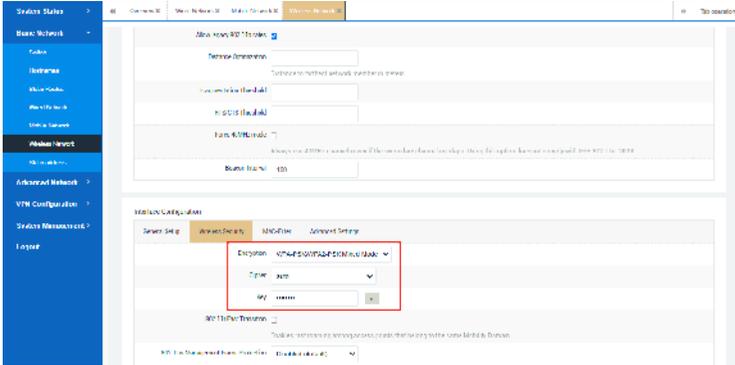
4.6.1.2.1 Basic Settings

Through the "Basic Settings" option, you can set the WiFi mode, wireless ESSID (hotspot name), working mode, whether to hide the ESSID name, and enable WMM mode, etc. as follows:



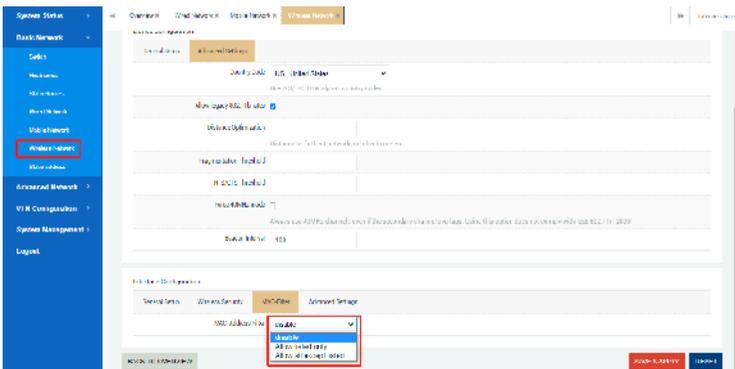
4.6.1.2.1 WiFi Password Setting

Through the "Wireless Security" option, you can set the wireless encryption method (the new version defaults to WPA-PSK/WPA2 Mixed Mode mixed encryption), algorithm and secret key settings, etc. (the password is at least 8 digits, the default is admin123), and the rest of the settings are generally default That's it.



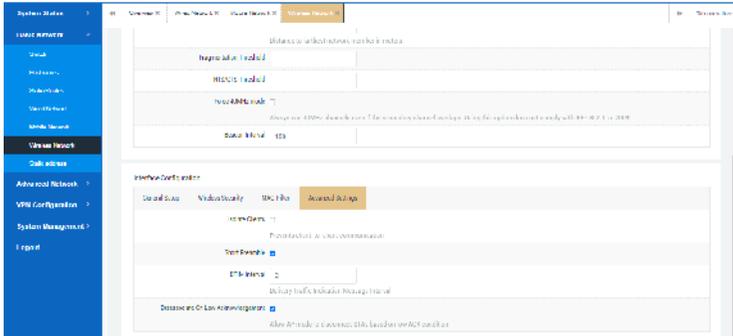
4.6.1.2.3 Black and white list settings

Through the "MAC filtering" option, you can set whether to enable MAC address filtering (disabled by default), "allow only in the list (whitelist: accessible)" or "only allow outside the list (blacklist: no access)". as follows:



4.6.1.2.4 Advanced Settings

Through the "Advanced Settings" option, you can set whether to isolate the client, etc., as follows:



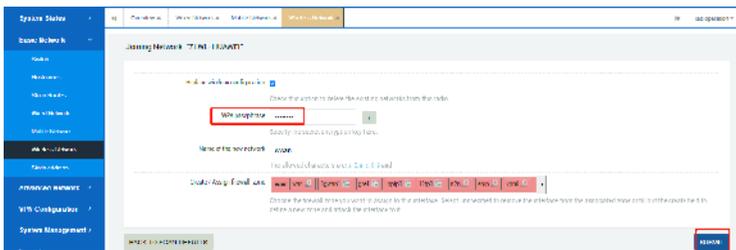
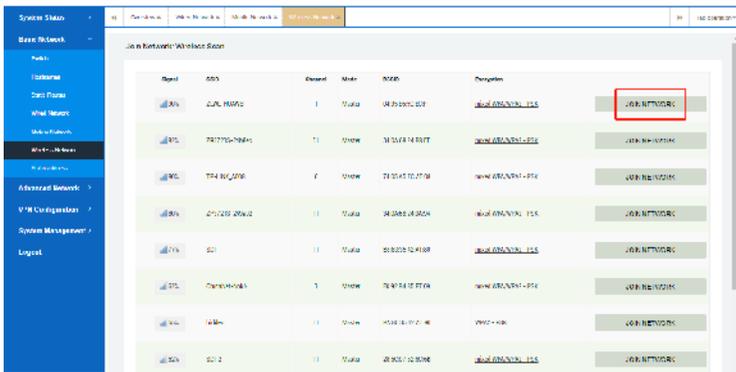
4.6.2 Client Mode

You can scan to join other wireless hotspots and set the method of obtaining an IP address (DHCP (default) or static address). as follows:

1) Specific operation: Select "Basic Network" --- "Wireless Network" --- "Wireless Overview", click the "Scan" button on the right to start searching for other wireless hotspots around, as follows:

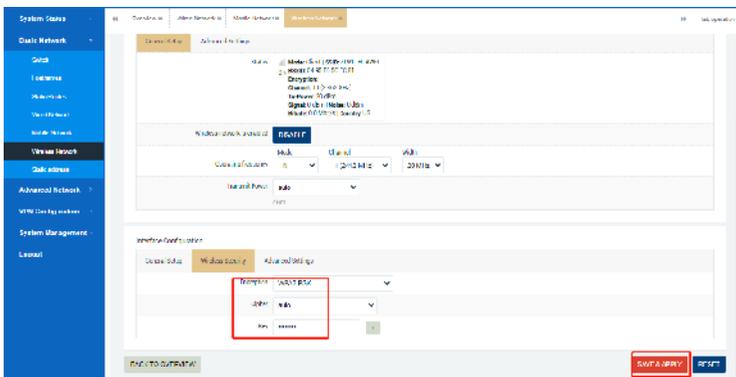
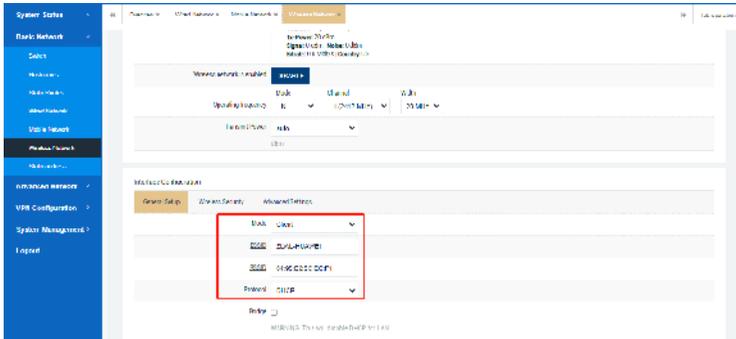


2) Select the wireless hotspot that needs to be connected, click "join network", check "reset wireless configuration" and set the password of the wireless hotspot and the name of the new network (the default is sufficient), and finally click "submit", the page will jump Go to the "Interface Configuration" --- "Basic Settings" page (you can set the protocol (wireless IP address acquisition method) to DHCP (default) or static address method), the rest of the settings can be defaulted, and finally click "Save Application", as follows:

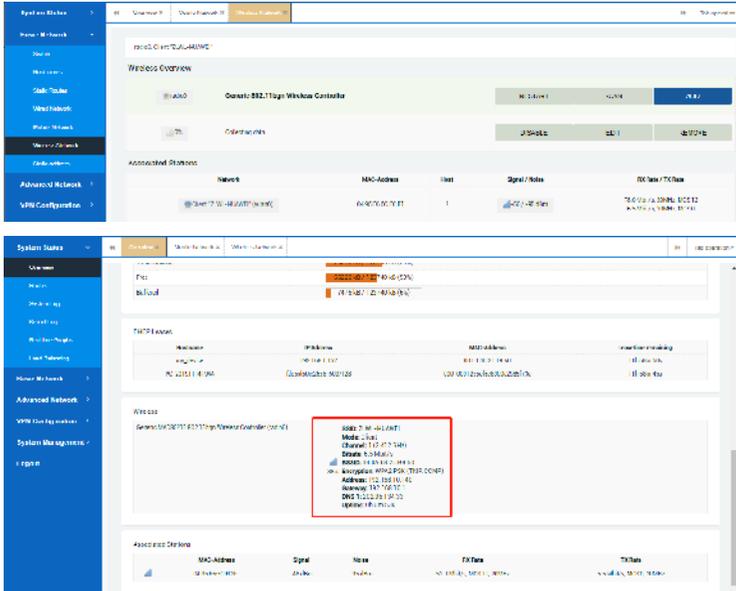


4.6.2.1 Client DHCP (default)

After filling in the password and submitting, jump to the WiFi interface configuration page, "Interface Configuration" --- "Basic Settings", the "Protocol" defaults to "DHCP", and then save the application.

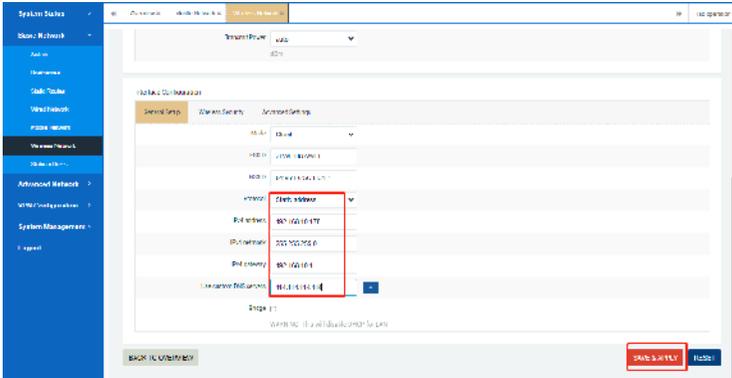


After clicking to save the application, select "System Status" --- "Overview" --- "Wireless" to check that the wireless client mode has been successfully connected at this time, as follows:

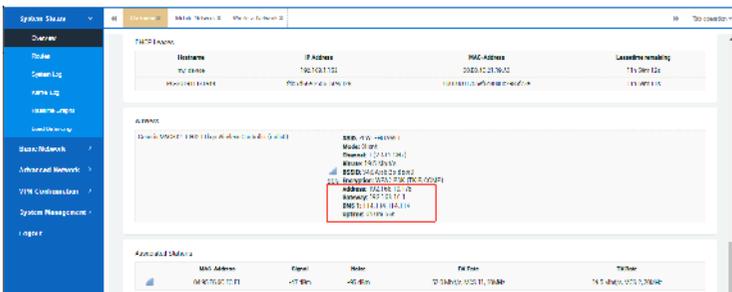
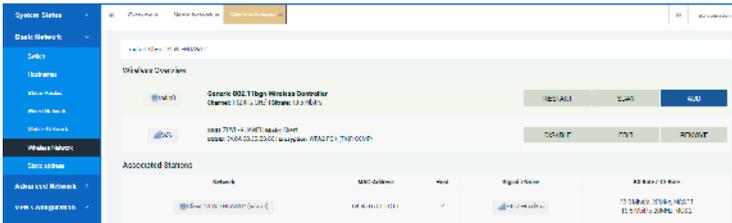


4.6.2.1 Client static address

You can scan to join WiFi, fill in the password and submit it, and then jump to the WiFi interface configuration page. In "Interface Configuration" --- "Basic Settings", select "Protocol" as "Static Address", and then enter the IP address, subnet mask, Save the application after the gateway and DNS server.



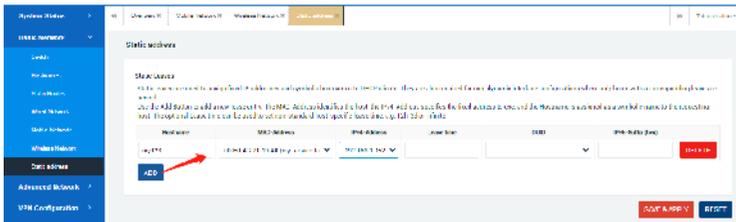
If you used "Protocol" as "DHCP" when scanning and joining before, now you need to change it to a static IP address. Specific operation: Select "Basic Network" --- "Wireless Network" --- "Wireless Profile", click the "Edit" button on the right, enter the interface configuration and select "Protocol" to change to "Static Address". After the configuration is as above:



4.7 Static address

The static address function is used to assign a fixed IPv4 address to a host with a specified MAC address, that is, the host device MAC-IP binding, and it can also customize the device host name.

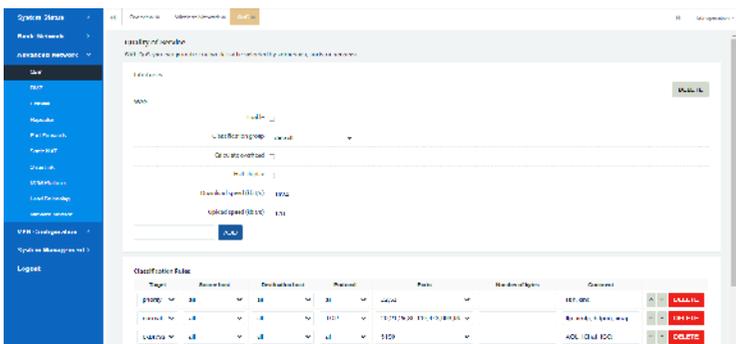
Select "Basic Network" --- "Static Address" and click the "Add" button to set the host name, MAC address, IPv4 address, lease period, etc., as follows:



5. Advanced Network

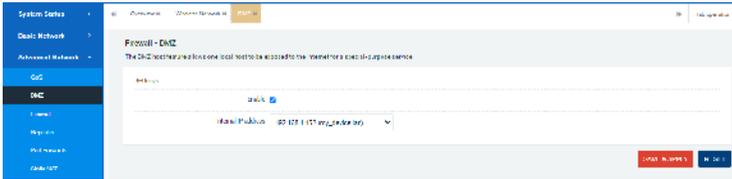
5.1 QoS

Here you can configure some specific QoS service quality rules, such as limiting the rate of each interface of the device or sorting different traffic data packets.



5.2 DMZ

The network attributes used for the WAN interface of the routing device (such as with a public IP address) forward the full port of the external network to the internal network host behind the firewall, so that the internal service resources of the network can be accessed quickly and efficiently. Examples are as follows:



5.3 Firewall

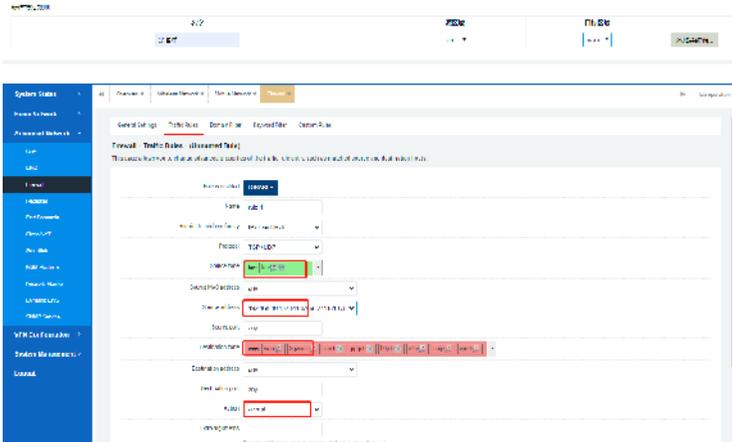
The firewall configuration is used to set certain rules for the inbound and outbound traffic of the routing system so as to effectively protect the security of the system.

5.3.1 Basic Settings

It is mainly used to set the entry and exit data access rules of different interface areas of the routing system and set related SYN-flood defense, etc. It is generally defaulted and does not need to be changed.



For example: create a new forwarding rule "blacklist" to restrict devices connected to the router from being able to access the Internet based on the MAC address, as follows:



The parameters need to be set as follows, and the rest can be defaulted.

[Agreement]: Any;

[Source MAC address]: Access router LAN LAN host device MAC address, the example access router host MAC address is 00-50-56-2B-95-F0 (because the IP address will change directly);

[Action]: Reject;

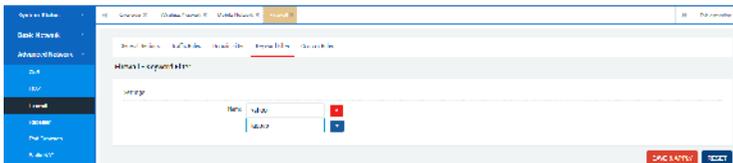
5.3.3 Domain name filtering

Here you can set the black and white list of the network domain addresses to be accessed, thereby denying or allowing the router system to communicate with these addresses, as follows:



5.3.4 Keyword filtering

Here, you can configure keyword filtering to reject the routing system and certain specified network communications, as follows:

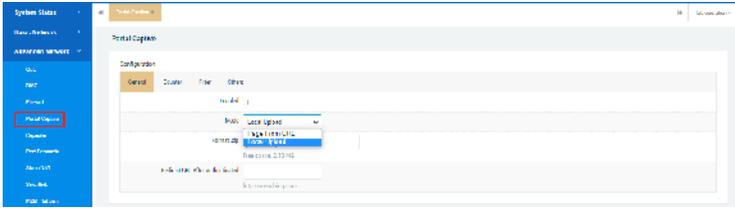


5.4 Portal authentication (optional)

This function is used to set advertising routing authentication parameters. Click "Advanced Network"->"Portal Authentication" to configure as follows:

5.4.1 General arrangement

You can configure whether it is enabled, the mode of obtaining advertisement files, and the redirection address after authentication.



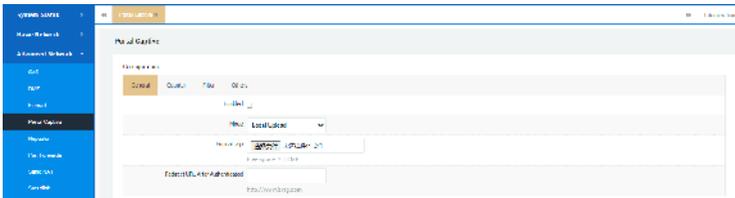
The configuration instructions are as follows:

[Enable] Check whether to enable the advertising routing function.

[Mode] You can choose the authentication file upload mode, which is uploaded locally by default.

[Jump address after authentication] The default is none, you can set it yourself.

5.4.1.1 Local Upload

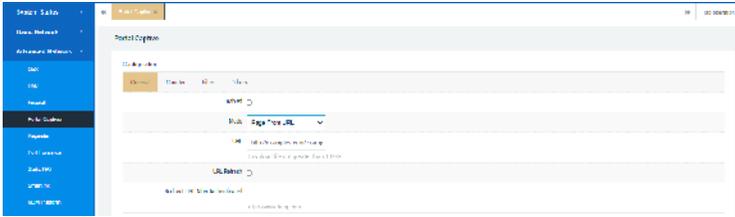


[Format] Upload a compressed package of certification files in *.zip format

5.4.1.2 Download file from URL server address

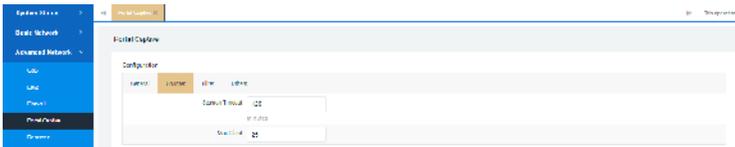
[Address] Fill in the URL server to store the htdocs advertisement file path (support http, https);

[Page update] means that when the htdocs advertisement file of the URL server changes, the advertising router will re-download the new htdocs file from the URL server. It is recommended to check it. After checking, the router background will check the server file every 5 minutes and update it synchronously.



5.4.2 counter

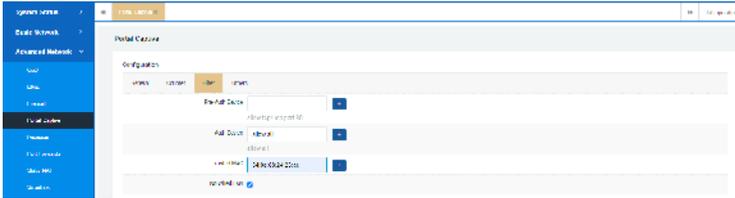
It can be used to set the timeout period of connected devices and the maximum number of device connections.



[Session timeout] refers to the total time that wireless terminals such as mobile phones can connect to the router after WiFi access is authenticated. If this time is exceeded, the terminal will be disconnected and need to be re-authenticated. The default value is 120 minutes, which is 2 hours.

[Maximum number of customers] refers to the number of wireless terminals that support WiFi authentication for connecting to the router. When this value is exceeded, the newly added wireless terminal cannot pass the authentication. The default value is 25.

5.4.3 Filter



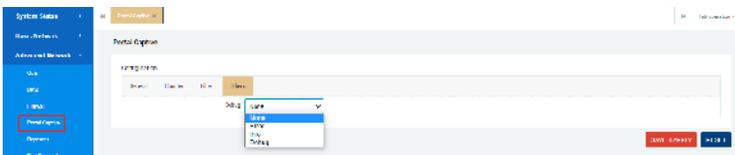
[Uncertified device] refers to a wireless terminal that is not connected to the router with WiFi certification or certification-free, and there are no restrictions on use by default.

[Authenticated device] refers to the network usage restrictions for wireless terminals after connecting to the route WiFi authentication, such as the restriction of the destination ip address or access port, all are allowed by default, and there is no restriction.

[Authentication-free device MAC address] means that after filling in the device's network card mac address, the wireless terminal does not need to be authenticated after connecting to the routed WiFi, and can directly access the network.

[Ignore wired devices] After checking, the system will ignore LAN access devices for authentication, and you can directly access the network.

5.4.4 other



[Debug] Switch to different log debugging sectors (none, error, information,

debugging), the router system log will correspondingly display the corresponding log information;

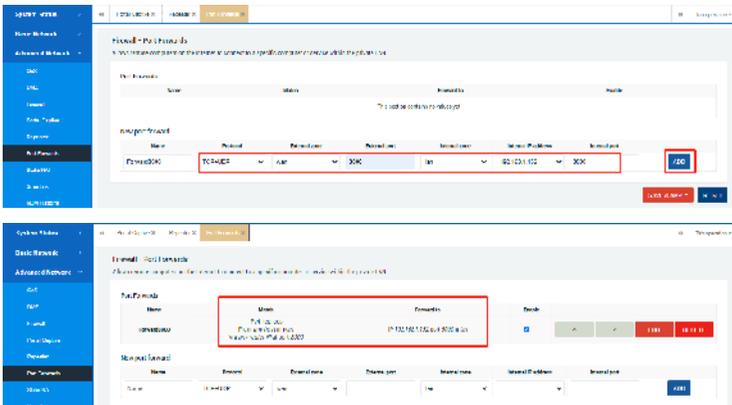
5.5 Repeater

This function is used to forward TCP/UDP to other network locations. as follows:



5.6 Port forwarding

This function is used to map the service resources of the internal host to the external access area of the device (usually a public IP address or an address that can be directly accessed), and at the same time makes the access to the internal service resources more secure. as follows:



[Name]: The name of the custom rule;

[Agreement]: Select rule agreement, generally ALL;

[External area]: select WAN area;

[External port]: Fill in the port for forwarding access to the external area;

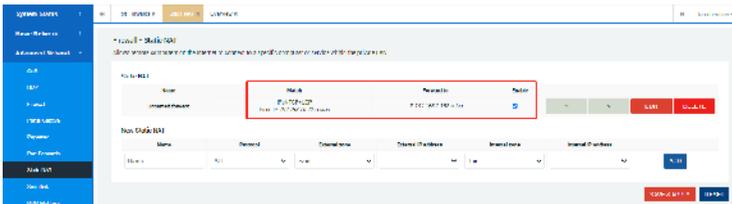
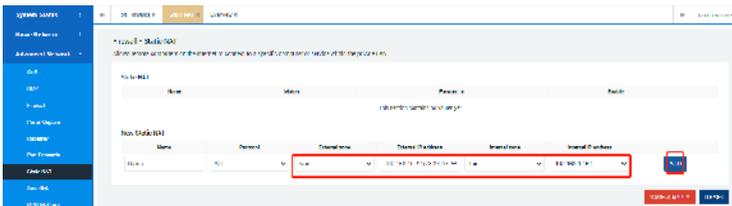
[Internal Area]: Select the area for internal forwarding, here is the LAN area;

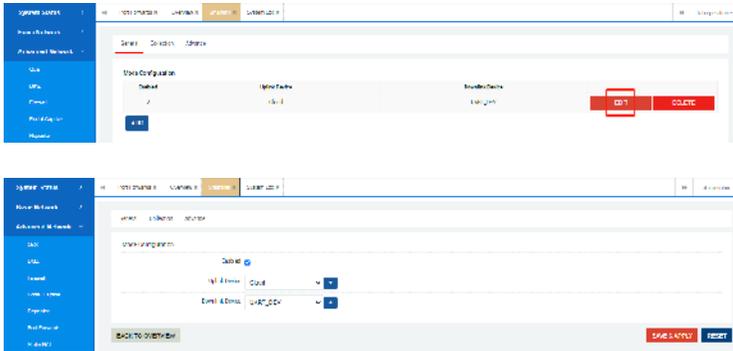
[Internal address]: Fill in the internal host address after forwarding, which can be filled in specifically;

[Internal port]: Fill in the port forwarded and accessed by the internal host, which can be filled in specifically;

5.7 Static NAT

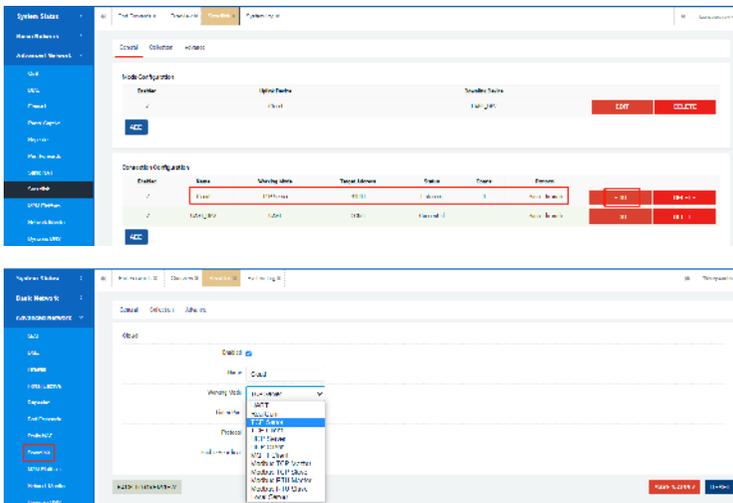
This function allows remote computers on the Internet to connect to specific computers or services in the internal network, and the device supports 1-to-1 or many-to-one static nat functions.





5.8.1.2 Connection configuration

Uplink device settings:



The parameter description is as follows:

[Enable]: After checking, enable the serial port function;

[Name]: It is empty by default and can be named;

[Work Agreement]: Choose the corresponding work mode according to actual needs;

[Monitor port]: TCP port, this item is related to the specific working mode;

[Protocol]: Transparent transmission mode;

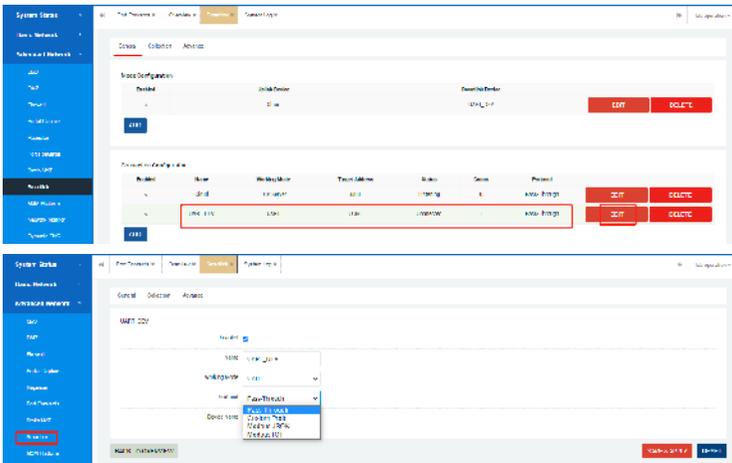
[Heartbeat]: Not checked by default;

[Heartbeat interval]: can be set specifically, the unit is second;

[Heartbeat content]: It can be set specifically, and the heartbeat content in the corresponding format must be filled in;

[Save and apply]: The configuration will take effect after saving and will be displayed in the general interface;

Downstream device settings:



5.8.1.3 Serial port configuration

Click the edit button to enter the COM port configuration interface.

The interface parameters are described as follows:

[Baud rate]: The default is 115200, which can be set specifically;

[Data bit]: The default is 8, which can be set specifically;

[Stop bit]: The default is 1, which can be set specifically;

[Check Digit]: The default is NO, which can be set specifically;

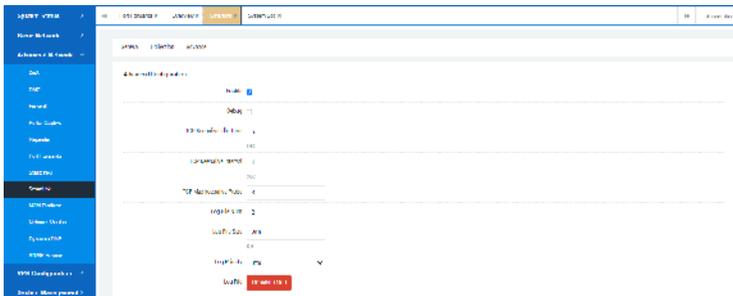
[Flow Control]: The default is NONE, which can be set specifically;

[Sub-packing interval]: The default is 60, which can be set specifically;

[Sub-package length]: The default is 1460, which can be set specifically;

5.8.2 advanced

Mainly configure the opening and closing of the Smartlink function, the opening and closing of debugging, the size, number, priority, download, etc. of log files. as follows:



The advanced parameters are described as follows:

[Open]: Smart IoT switch.

[Debug]: Not checked by default.

[TCP keep-alive idle time]: The default is 60s, which can be set specifically.

[TCP keep-alive detection interval]: The default is 3s, which can be set specifically.

[Maximum times of TCP keep-alive detection]: The default is 3 times, which can be

set specifically.

[Number of retained log files]: The default is 2, which can be set specifically.

[Log file size]: The default is 200KB, and it is recommended not to exceed 3000KB.

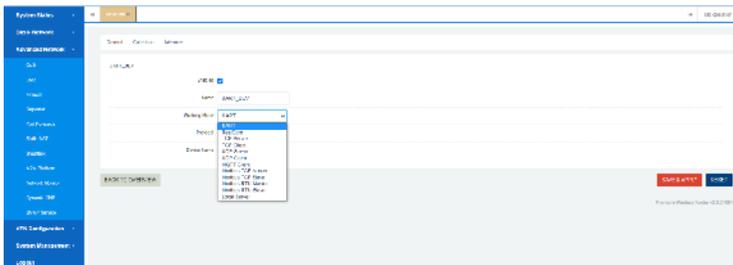
[Log Priority]: Default information, which can be selected specifically.

[Log file]: Download button.

5.8.3 Operating mode

Smartlink supports a total of 12 modes to meet the needs of different scenarios in the project. It can be flexibly configured according to the actual needs of the site. The general serial port mode is the physical COM port of the router.

Select "Advanced Network" --- "Smart IOT" --- "General" --- "Connection Configuration" --- "Edit", select "Work Mode". as follows:



5.8.4 Custom protocol

Smartlink usage protocol supports the use of custom protocols to meet the needs of different scenarios. It can be flexibly configured according to the actual needs of the site.

Select "Advanced Network" --- "Smartlink" --- "General" --- "Connection Configuration" --- "Edit", select "Protocol". as follows:

5.8.5 Configuration example

5.8.5.1 TCP server

Example description

In the TCP server mode, the router configures an IP port number (monitoring the local port) as a TCP server, and passively waits for the remote host to connect. After the remote host initiates a connection request and establishes a connection with the router, the remote host can realize two-way transparent transmission through the network connection and the serial port. The remote host can read or send data to a serial device at the same time.

Example steps

Router (TCP server) parameters:

WAN port IP address: 192.168.10.122

Listening port: 6800

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

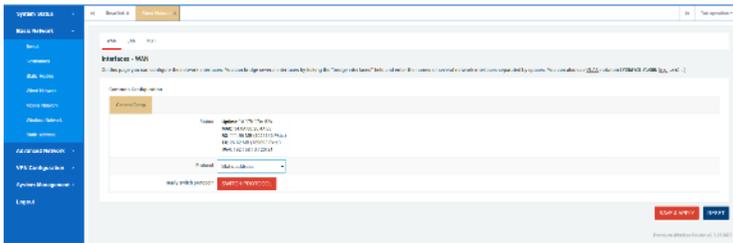
COM1 115200 8 1 None None

Remote PC (TCP client) parameters:

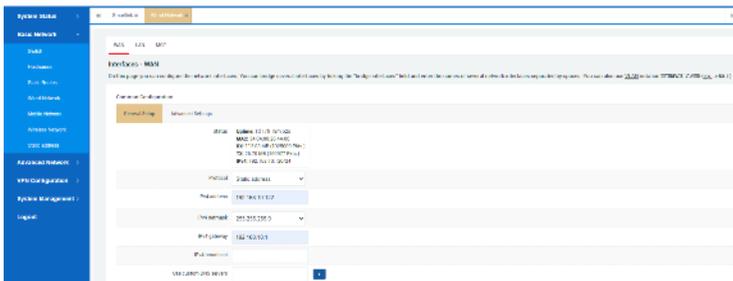
IP address: 192.168.10.192

Step 1: Configure the WAN port IP address

Wired network>WAN>click protocol (select static address)>click to switch protocol

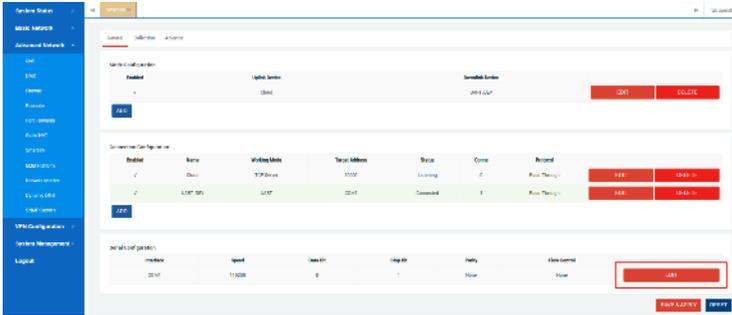


Configure the IPV4 address, subnet mask, and IPV4 gateway, and click the Save and Apply button in the lower right corner to save the configuration.

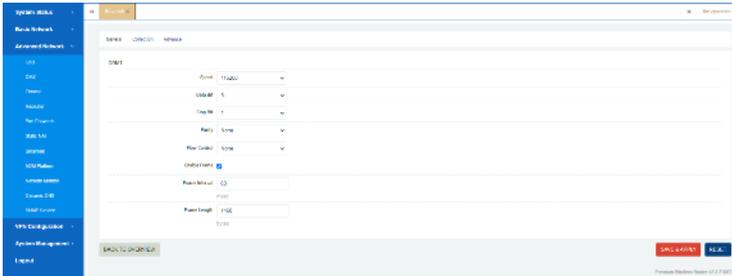


Step 2: Configure the serial port configuration

Smartlink> Click the "Edit" button of COM1. The serial port parameter can be configured.



Enter the configuration interface to modify the baud rate, data bit, stop bit and other parameters according to actual needs. The "Save and Apply" button in the lower right corner will save and take effect.



5.8.5.2 TCP Client

Example description

In the TCP client mode, the router host IP and port number actively establish a TCP protocol connection with the remote PC, and the router can realize bidirectional transmission to the transparent mode through the network connection and the remote PC. The PC can send and receive data to a serial device at the same time.

Example steps

Router (TCP client) parameters:

WAN port IP address: 192.168.10.122

Server address: 192.168.10.192

Server port: 6800

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

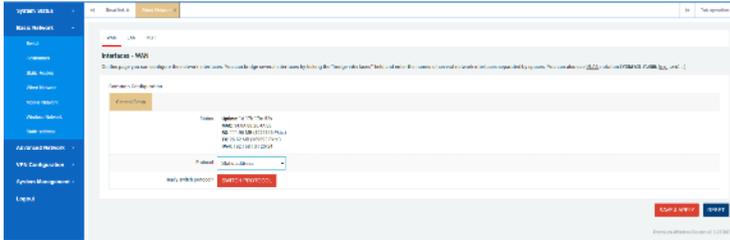
COM1 115200 8 1 None None

PC (TCP server) parameters:

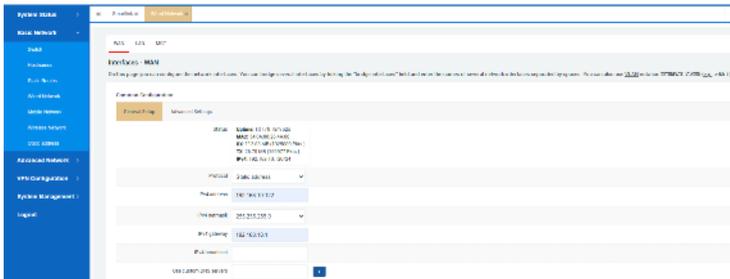
IP address: 192.168.10.192

Step 1: Configure the WAN port IP address

Wired network>WAN>click protocol (select static address)>click to switch protocol

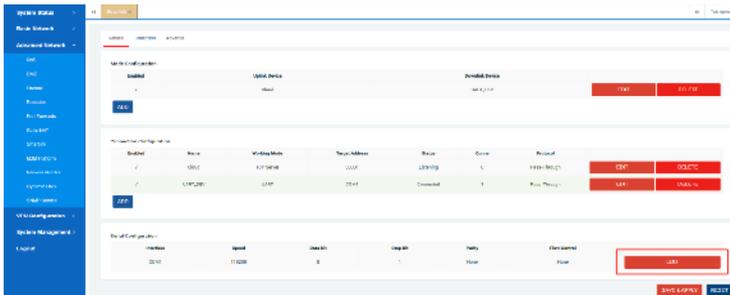


Configure IPV4 address, subnet mask, IPV4 gateway.



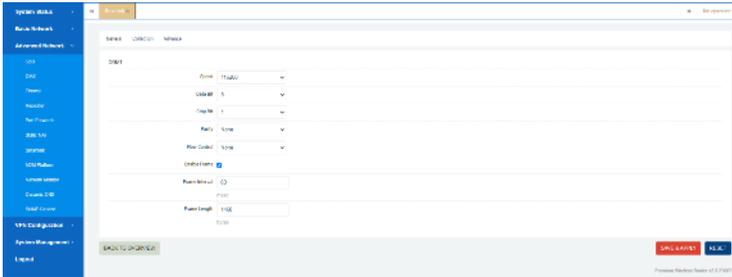
Step 2: Configure the serial port configuration

Smartlink> Click the edit button in the serial port configuration bar. The serial port parameter can be configured.

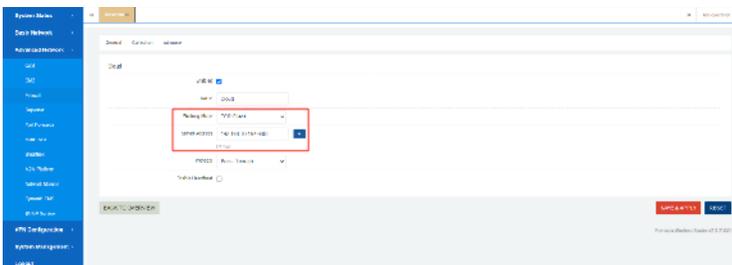
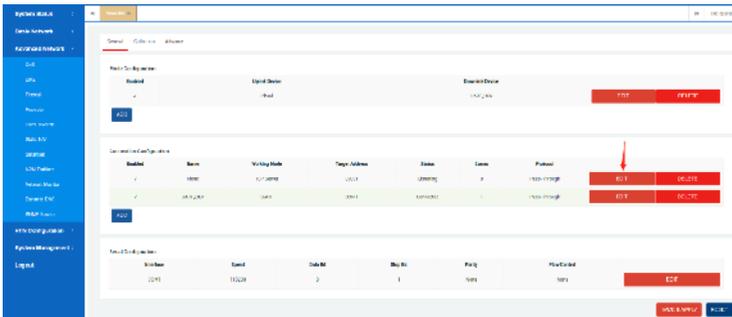


Enter the configuration interface to modify the baud rate, data bit, stop bit and other

parameters according to actual needs.



Step 3: Configure the server address and port for receiving data



5.8.5.3 UDP Server

Slightly (same as TCP server mode, the difference is that UDP server mode uses UDP

protocol to build network connection)

5.8.5.4 UDP Client

Slightly (same as TCP client mode, the difference is that UDP client mode uses UDP protocol to build network connections)

5.8.5.5 Real serial port mode

Example description

In the real serial port mode, the router connects to the virtual serial port of the remote PC. The virtual serial port tool establishes a transparent network transmission connection between the host and the serial device in the operating system, and maps the router's serial port to the host's local virtual serial device according to the parameters such as the router IP address and serial number configured by the user to realize the real serial port and virtual Transparent transmission between serial ports.

Example steps

Router (real serial port) parameters:

WAN port IP address: 192.168.10.122

Router port: 30001 (fixed)

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

COM1 115200 8 1 None None

PC parameters:

IP address: 192.168.10.192

Step 1: Configure the WAN port ip address

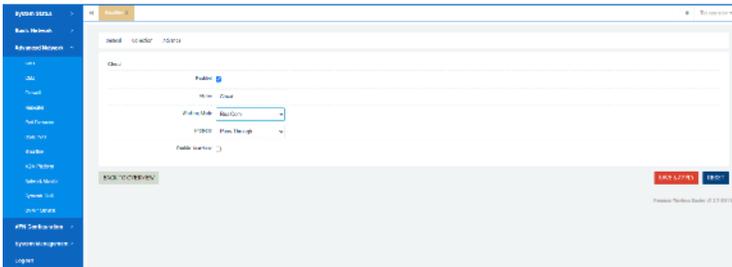
Omit (same as above)

Step 2: Configure the serial port configuration

Omit (same as above)

Step 3: Connection configuration

Configuration Enable check, name (can be empty), working mode selection: real serial port mode



5.8.5.6 MQTT Client

Example description

Two MQTT clients are similar to the process of mailing letters between two people. One party publishes a message, and the other party receives the message after subscribing.

Example steps

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

COM1 115200 8 1 None None

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

COM1 115200 8 1 None None

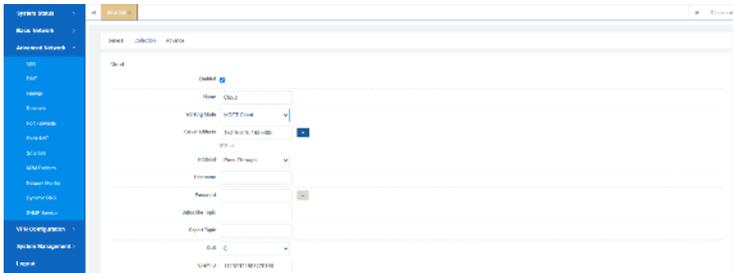
step 1:

Configure serial port configuration

Omit (same as above)

Step 2: Connection configuration

Configuration Enable check, name (can be empty), working mode selection: MQTT client



[Server address] Fill in the MQTT server address and port (server address: port).

[Protocol] The default transparent transmission mode, you can choose by yourself;

[Username/Password] The MQTT server decides whether it is required or not. If there is, it needs to be filled in.

[Subscribe/Report Subject] The subject address for mutual communication can be set by yourself.

[Qos] Quality of service, the default is 0, you can choose to set 1, 2.

[Customer ID] Default device serial number.

[MQTT keep-alive period] MQTT keep-alive period, the default is 60 seconds.

[Device Mode] The default transparent transmission mode can be selected by yourself.

[Heartbeat] Check to enable.

[Heartbeat interval] The unit is second, which can be set by yourself.

[Heartbeat content] ASCII code and hexadecimal string can be set by yourself.

5.8.5.7 Modbus RTU to TCP master-slave communication

Please contact technical support to assist in debugging.

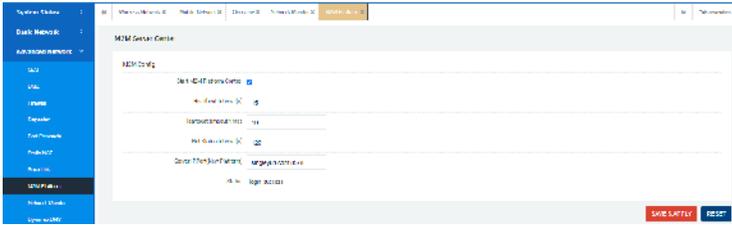
5.8.5.8 Modbus TCP master-slave communication

Please contact technical support to assist in debugging.

5.9 M2M Cloud platform

The user scenario of this function is: the router connects to the cloud server management platform through the Internet, and the user can realize remote view management of the router, remote firmware upgrade, remote configuration, log download and view without going to the site.

The functional parameters are described below:



[Start M2M Platform Control]: Enable or disable the platform connection;

[Heartbeat Interval(s)]: The heartbeat interval between the router client and server platform (default: 15s);

[Heartbeat timeout times]: The router client reports the number of failed heartbeat packets (if it exceeds this number, the router is considered to have failed to connect to the platform). The default is 10 times.

[Net Status Interval(s)]: The interval at which the router reports its online status to the server platform (default 120s).

[Server IP:Port(New Platform)]: Server platform address and port configuration;

[Status]: The status of the router connecting to the cloud platform;

5.10 Load Balancing (optional)

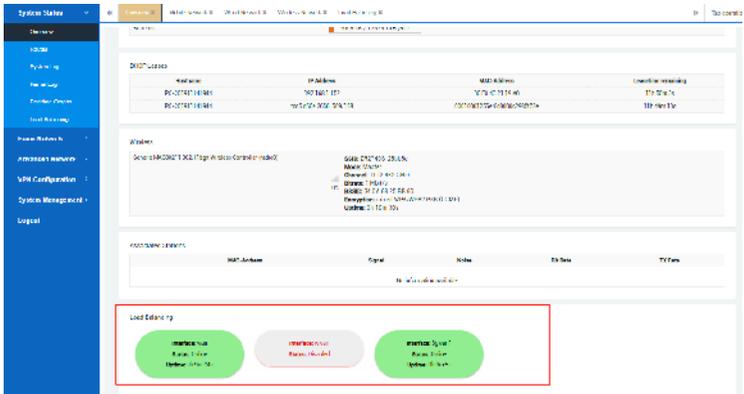
The load balancing function (MWAN3) is mainly to deploy the interface traffic of different network interfaces of the router system (such as wired WAN, 3G/4G mobile network, WiFi client, etc.) according to certain policy rules, mainly including traffic balancing or switching backup.

The overall features of load balancing will be described below.

Note: For scenarios that use virtual private network functions (such as PPTP/2LTP/IPSEC, etc.), please turn off the device load balancing

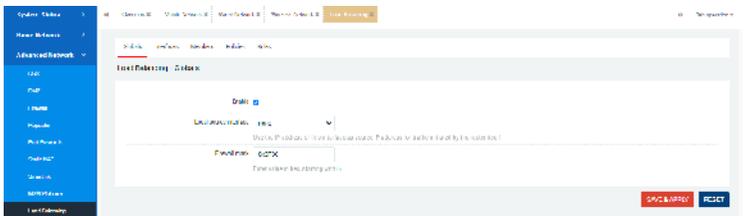
function to avoid causing the virtual private network to fail.

Load balancing is enabled by default in the system (different versions, different), select "System Status" --- "Overview" to view the real-time status of load balancing, as follows:



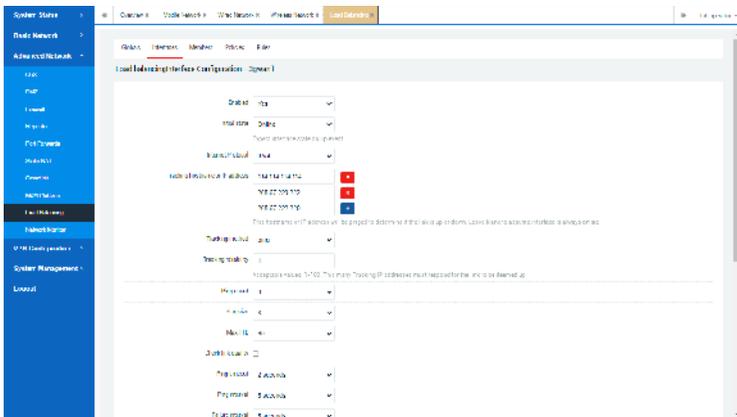
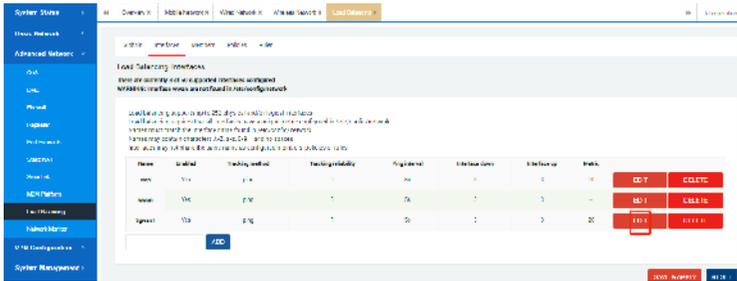
5.10.1 Global

Click the "Advanced Network" --- "Load Balancing" --- "Global" tab, which can be used to enable or disable the load balancing function (not enabled by default), as follows:



5.10.2 Interface

Click the "Advanced Network" --- "Load Balancing" --- "Interface" tab to configure specific interface parameters. You can also add other interfaces by clicking the "Add" button in the lower left corner. After clicking "Edit", you can configure and modify the parameters as follows:



[Enable]: Whether to enable interface detection, it is enabled by default.

[Initial state]: Select the state of the interface during initial detection, such as online or offline.

[Internet Protocol]: Optional IPv4, IPv6, default IPv4.

[Tracked host or IP address]: Use ping to detect the destination host to determine whether the device's external network access is normal, and then to

further determine whether the interface is online or offline, which is generally a public network or a valid IP.

[Tracking mode]: Ping mode is selected by default.

[Tracking reliability]: Specify how many IP addresses can be pinged when the interface will be considered online, and the default is one.

[Ping count]: the number of times of ping detection.

[Ping size]: The size of the data packet detected by ping, the default is 8 bytes.

[Ping timeout]: How long does it take to ping the external network or there is no response when it is considered as a timeout.

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

[Fault detection interval]: The ping interval during fault detection, the default is 5s.

[Failure Recovery Interval]: The ping interval during failure recovery, the default is 5s.

[Interface offline]: When the number of Ping failures reaches this value, the interface will be considered offline, 3 times by default.

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

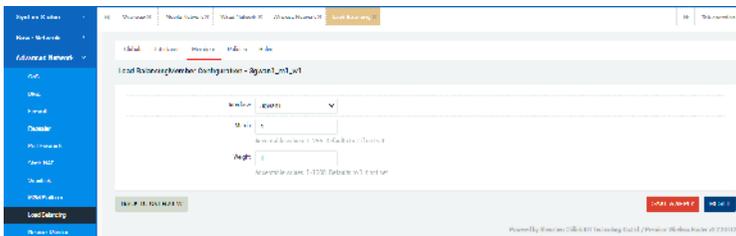
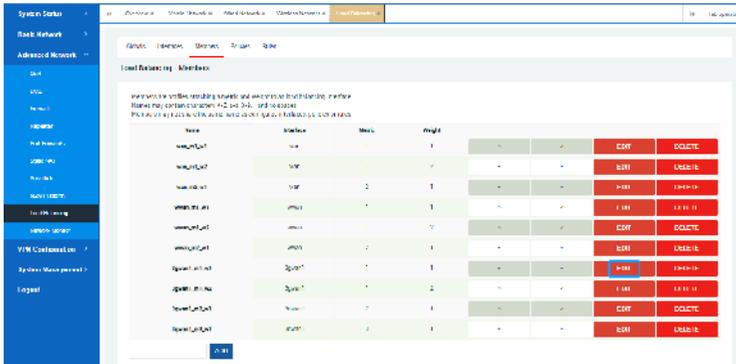
Go online again, 3 times by default.

[Refresh Interval Connection Table]: Refresh the global firewall connection tracking table when an interface event is triggered, which is enabled by default.

[Metrics]: Shows the metric of this interface in the configuration.

5.10.3 Member

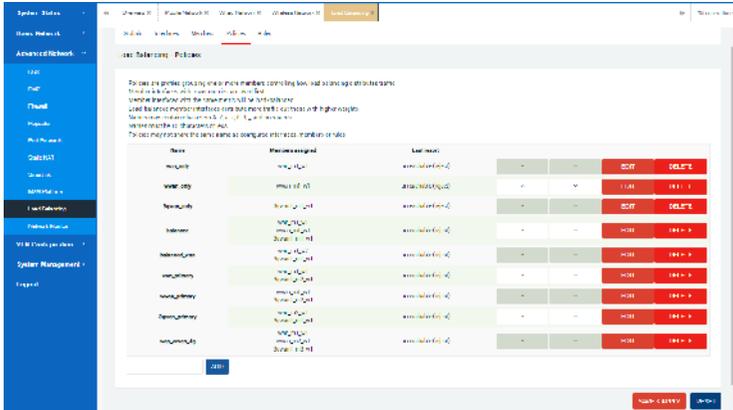
Click the "Members" tab to view or add the members corresponding to each interface and configure different metric and weight. The system presets 6 member properties by default, as follows:



5.10.4 Strategy

This function is used to group members and tell MWAN how to distribute the traffic that uses this strategy in the "rule". Members with a lower metric will be used first, members with the same metric will load balance traffic, and members with a higher proportion will be allocated more traffic.

Click the "Strategy" tab to configure different policy rules based on the "Members" set in the previous step. There are 9 preset policies by default in the system, which are described as follows:



5.10.4.1 wan_only

Refers to using only the wan wired network (ignoring whether the 3G/4G SIM card or wireless WiFi network is normal);

5.10.4.2 wwan_only

Refers to only using WiFi network (no matter whether the wan wired network, 3G/4G SIM card is normal or not, it is ignored);

5.10.4.3 3gwan_only

Refers to dial-up network using only 3G/4G SIM card (ignoring whether the wired wan network or wireless WiFi is normal);

5.10.4.4 balanced

Refers to the simultaneous use of wan wired network, wireless WiFi network and 3G/4G SIM card dial-up network; the default traffic ratio of the three is 1:1:1, which can be modified in detail;

5.10.4.5 balanced_wan

Refers to the simultaneous use of wan wired network and 3G/4G wireless SIM card dial-up network; the default traffic ratio between the two is wan:3gwan1=2:1, which can be modified in detail;

5.10.4.6 wan_primary

Refers to wan wired network priority, 3G/4G wireless SIM card dial-up network backup; when the wan cable is abnormal or faulty, the network automatically detects and switches to the 3G/4G wireless network, and after the wan network is restored, the network traffic is automatically detected and switched to wan cable .

5.10.4.7 wwan_primary

Refers to the wireless WiFi network priority, 3G/4G SIM card dial-up network backup; when the wireless WiFi is abnormal or faulty, the network automatically detects and switches to the 3G/4G network, and when the WiFi network is restored, the network traffic automatically detects and switches to the wireless WiFi.

5.10.4.8 3gwan_primary

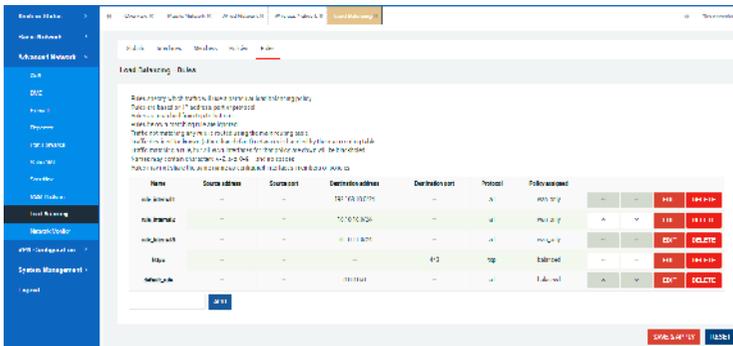
Refers to 3G/4G wireless dial-up network priority, wan wired network backup; when the 3G/4G dial-up network is abnormal or faulty, the network will automatically detect and switch to the wan wired network, and when the 3G/4G dial-up network is restored, the network traffic will automatically detect and switch again go back.

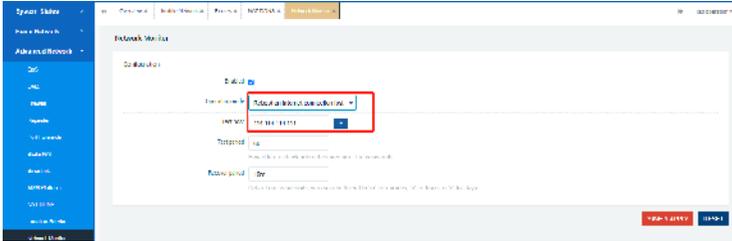
5.10.4.9 wan_wwan_4G

Refers to the wan wired network first, wireless WiFi backup, 3G/4G dial-up second; when the wan wired network is abnormal or faulty, the network automatically detects and switches to the wireless WiFi network, and when the wireless WiFi network is also abnormal or faulty, the network automatically detects and switches to 3G/4G dial-up network. At the same time, when the wireless WiFi network is restored, the network traffic is automatically detected and switched back, and when the wan wired network is also restored, the network traffic is automatically detected and switched back.

5.10.5 Rule

Click the "Rule" tab, the system will take effect according to the "policies" set in the previous step. The system default rule default_rule is balanced, that is, the wired WAN network and the 3G/4 wireless dial-up network can access traffic at the same time. Set other default_rule rules in the actual situation (6 strategies preset by the system can be selected. After selection, the 2 parameter allocation strategies shown below need to be modified to the selected strategy at the same time). as follows:

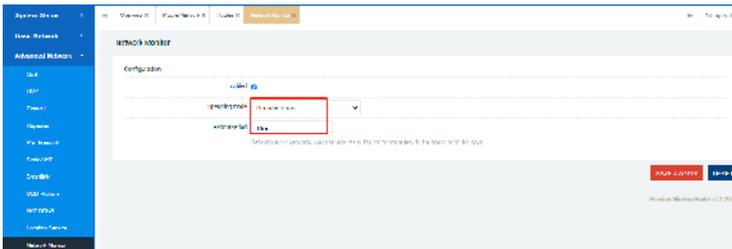




Note: For the scenario where the VPN private network is used or the device's own network is not allowed to access the external network, you need to modify the ping host address to be a valid address, or disable the network monitoring function, otherwise the device will periodically restart abnormally.

2) Periodic restart

Set periodic/timed restart for the device (default is 10min).



6.Virtual Private Network

This chapter mainly introduces several different virtual private network functions and simple configuration and use. The virtual private network function is generally used to build a remote local area network between the user's field device network

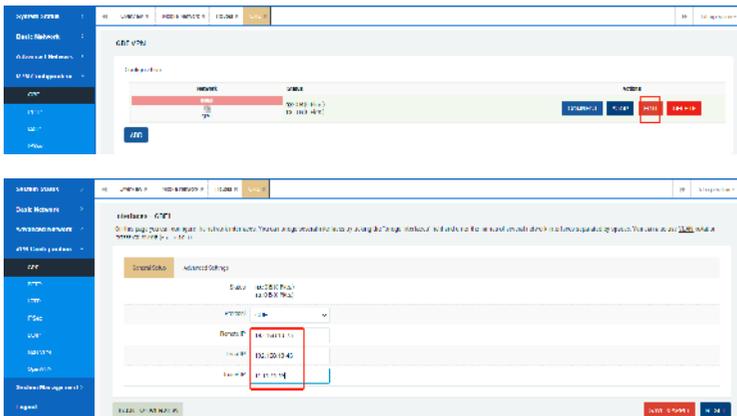
and the server network or different device network with different data transmission methods (such as PPTP/L2TP) or encryption strength (such as IPSec/Openvpn) , To facilitate better and faster remote access and control of remote devices.

Note: For scenarios that use virtual private network functions (such as PPTP/2LTP/IPSEC, etc.), please turn off the device load balancing function to avoid causing the virtual private network to fail.

6.1 GRE Client

The premise of the main use scenario of the GRE network is that different nodes with access attributes of the public network or VPDN private network can realize mutual access communication between the subnet devices under the different nodes through the establishment of virtual tunnels.

1) Select "Virtual Private Network" --- "GRE" --- "GRE Tunnel", click the "Edit" button to proceed GRE related configuration, including tunnel source address, tunnel destination address, tunnel address, etc., are as follows:

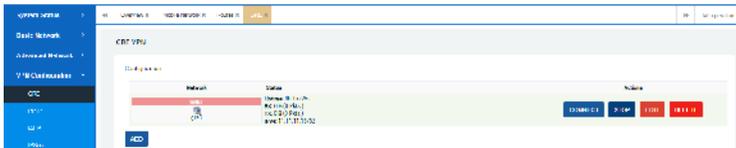
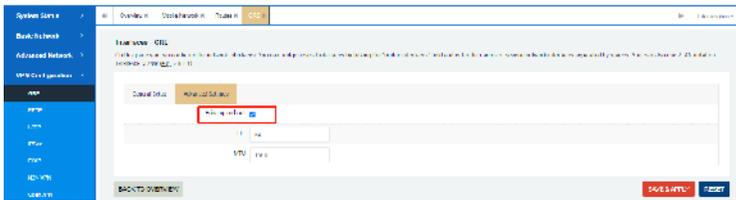


Among them, the description of each parameter is as follows:

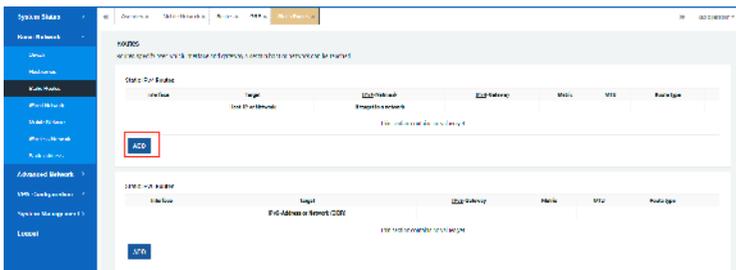
[Tunnel destination address]: Fill in the public network IP address of the opposite

router, this example is the LAN WAN port address 192.168.10.23;
 [Tunnel source address]: Fill in the public network IP address of the local router, this example is the local LAN WAN port address 192.168.10.45;
 [Tunnel Address]: Fill in the virtual tunnel IP address of the local router, here is 11.11.11.13 (the opposite tunnel address is 11.11.11.14) as an example;

2) Set up the "Autostart" service as follows:



3) Take the local router subnet (192.168.3.0/24 as an example) to add the static routing table of the peer router network segment (take 192.168.4.0/24 as an example), as follows:



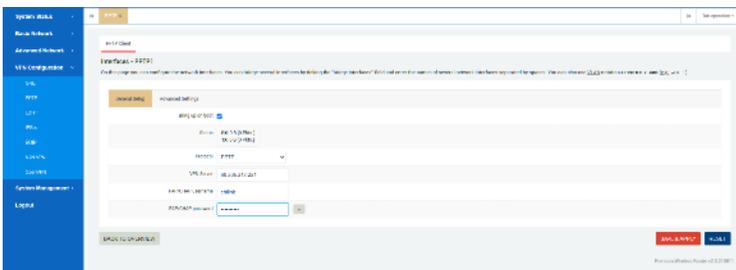
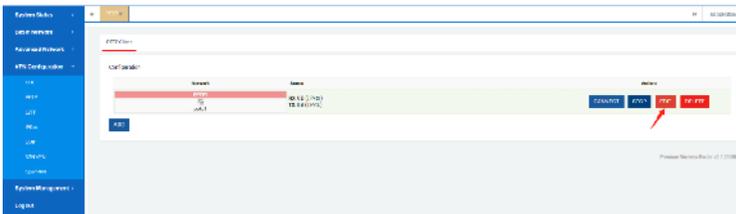
Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

The schematic diagram is as follows:

Specific operation: Select "Virtual Private Network" --- "PPTP" --- "PPTP Client", click the "Edit" button to configure specific parameters, as follows:

1) Select "Basic Settings" to start configuring server parameters and client account, password and other information, as follows:

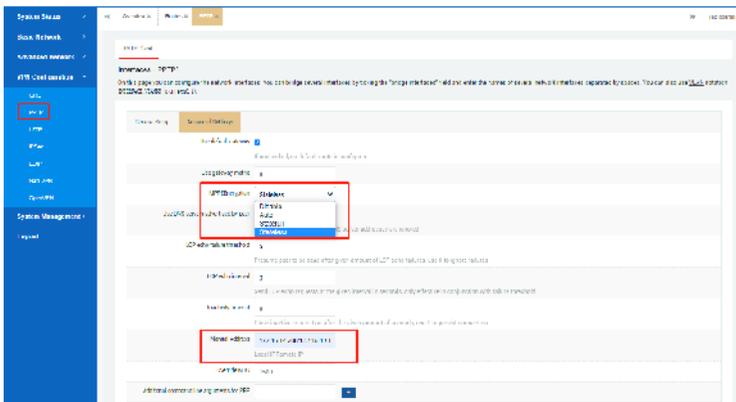


[Startup]: After checking, the router will automatically start and connect to the PPTP service every time it restarts

[VPN server]: Fill in the IP address of the remote server, generally the public network IP address;

[PAP/CHAP username, password]: Fill in the client account and password assigned by the VPN server;

2) Select "Advanced Settings" to configure some specific advanced parameters, as follows:



[Use default gateway]: After checking, the router can automatically address the server terminal network;

[MPPE encryption]: Fill in the encryption type consistent with the VPN server, otherwise you may not be able to connect to the server;

[LCP response failure threshold]: LCP response times, the default is 5;

[LCP response interval]: LCP response interval, the default is 3s;

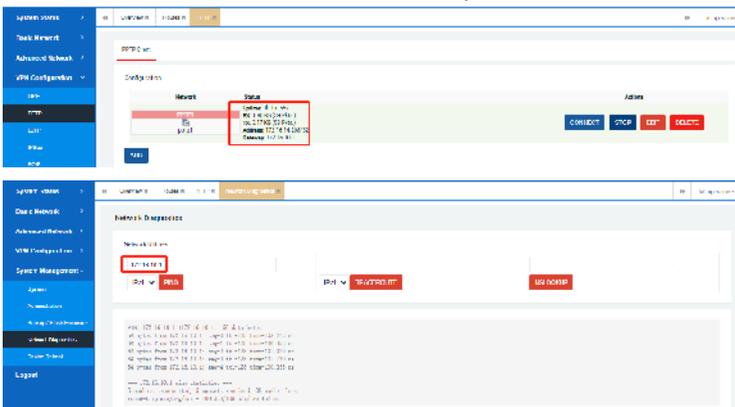
[Activity timeout]: Inactive connection control with the server, the default is 0, which means that continuous connection is supported;

[Manually assign address]: You can specify the VPN address; set the format

172.16.100.2 (client virtual IP): 172.16.100.1 (server gateway virtual IP);

[Additional parameters for PPP]: Customize PPP parameters, such as filling in the debugging command (debug) or specifying the client VPN IP address, etc. (If you need to specify the VPN address, the setting format: 172.16.100.2 (client virtual IP): 172.16.100.1 (server gateway virtual IP));

3) The PPTP client connects to the server successfully, as follows:



6.3 L2TP Client

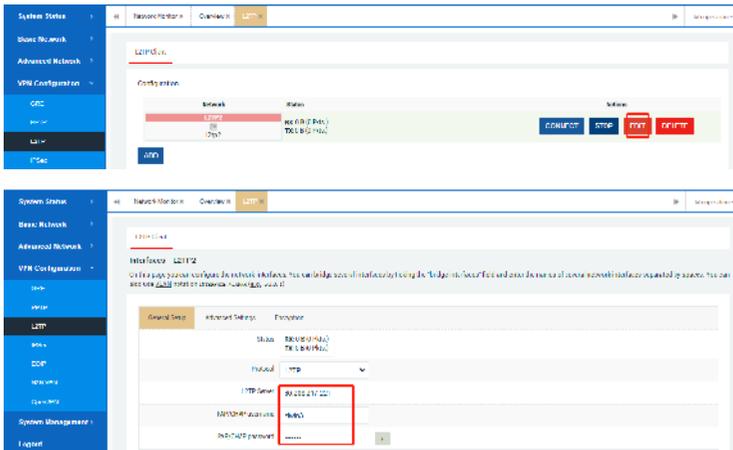
The L2TP network is also mainly used to connect different client router devices or PC computers to the VPN server through the L2TP protocol dial-up configuration to achieve the following two main usage scenarios.

Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

The specific configuration is as follows:

1) Select "Virtual Private Network" --- "L2TP" --- "L2TP Client", click the "Edit" button to perform "Basic Settings", and begin to configure server parameters and client account and password information, as follows:

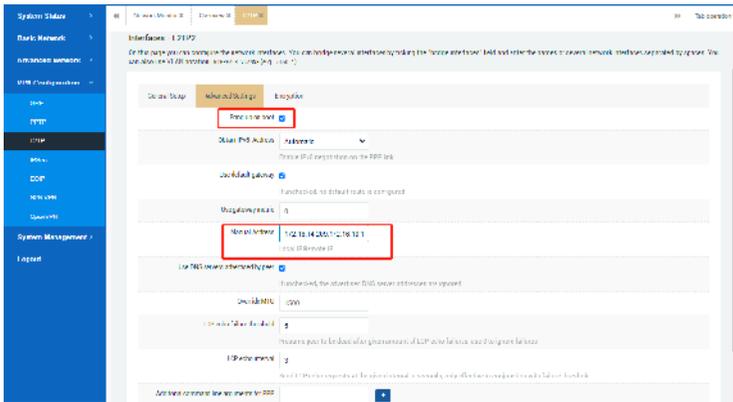


[Protocol]: Default protocol type: L2TP;

[VPN server]: Fill in the IP address of the remote server, generally the public network IP address;

[PAP/CHAP username, password]: Fill in the client account and password assigned by the VPN server;

2) Select "Advanced Settings" to configure some specific advanced parameters, as follows:



[Startup]: After checking, the router will automatically start and connect to the L2TP service every time it restarts;

[Obtain IPv6 address]: The default is automatic, you can choose to disable or manually;

[Use default gateway]: After checking, the router can automatically address the server terminal network;

[Manually assign address]: You can specify the VPN address; set the format 172.16.100.2 (client address): 172.16.100.1 (VPN server gateway address);

[MPPE encryption]: Fill in the encryption type consistent with the VPN server, otherwise you may not be able to connect to the server;

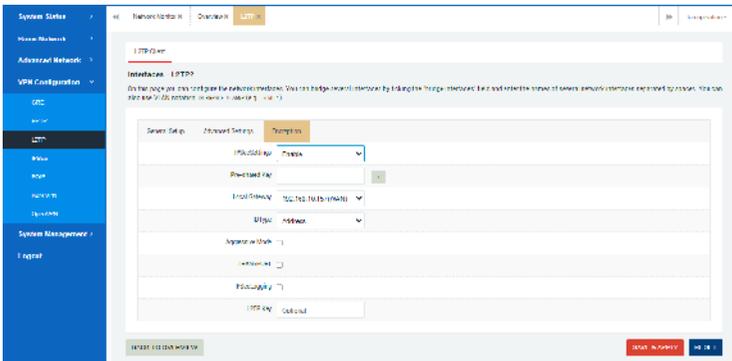
[LCP response failure threshold]: LCP response times, the default is 5;

[LCP response interval]: LCP response interval, the default is 3s;

[Response timeout]: Inactive connection control with the server, the default is 0, which means continuous connection is supported;

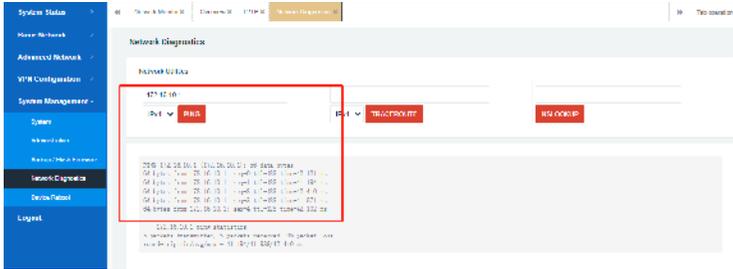
[Additional parameters for PPP]: Customize PPP parameters, such as debug, etc.;

3) Select "Encryption Method" to set whether IPsec configuration is enabled (default is none), and the L2TP key is as follows:



4) The L2TP client connects to the server successfully, as follows:





6.4 IPsec Client

The IPsec network is mainly used to connect different client router devices to the IPsec server through the IPsec protocol dial-up configuration so that the client router subnet devices and the server terminal network devices can communicate with each other at will.

The specific configuration is as follows:

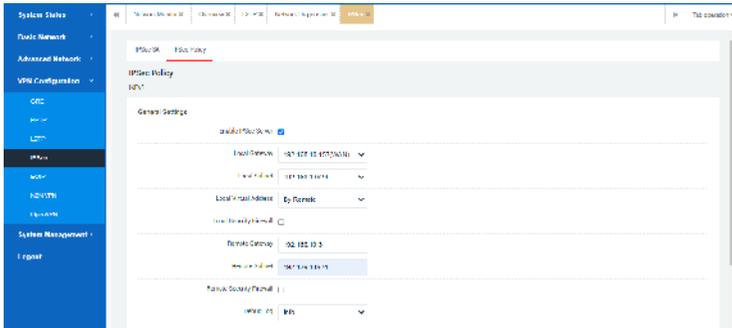
6.4.1 IPsec security strategy

The IPsec security strategy is mainly to set the server-related parameters, and configure the IKE/ESP security proposal, encryption algorithm, national secret SM3 algorithm and other parameter settings of phases 1 and 2 of the entire IPSEC communication.

6.4.1.1 Basic Settings

Select "Virtual Private Network" --- "IPsec" --- "IPsec Security Policy" --- "Basic

Settings" to configure specific parameters. Examples are as follows:



[Enable IPsec service]: Check whether to enable;

[Local Security Gateway]: Fill in the local 4G dial-up IP interface (3GWAN1), the example is the local interface WAN;

[Local Subnet Range]: Fill in the client's local subnet range;

[Local virtual address]: The default is assigned by the opposite end (you can also choose to customize);

[Local security firewall]: Device local client security firewall parameters, check whether to enable;

[Peer End Security Gateway]: Fill in the server-side gateway IP (usually the public network or domain name address);

[Range of terminal network]: Fill in the range of server terminal network;

[Peer-end security firewall]: Device server-side security firewall parameters;

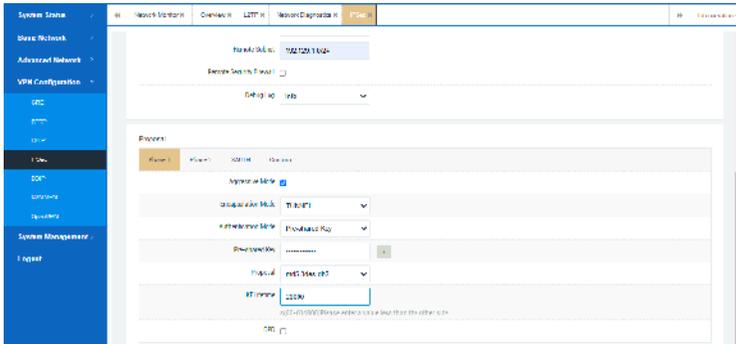
[Debug log]: After opening, you can view the specific connection debug log;

6.4.1.1 Security proposal

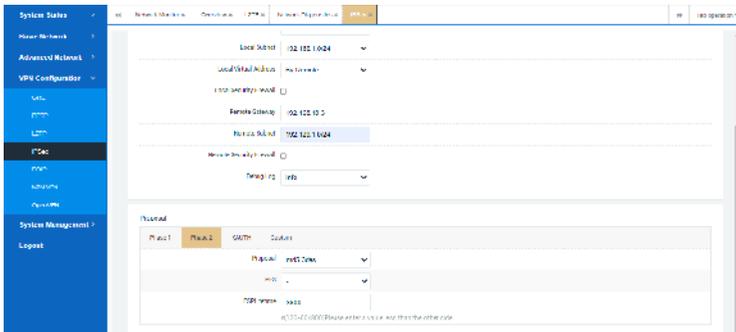
Select "Virtual Private Network" --- "IPsec" --- "IPsec Security Policy" --- "Basic

Settings" drop down to "Security Proposal" to configure specific parameters, as follows:

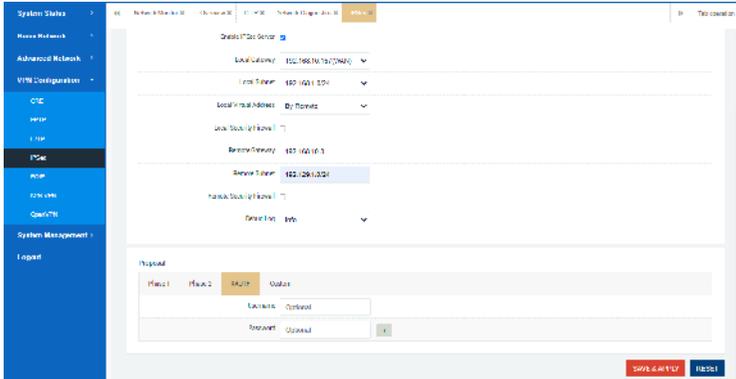
Phase 1 configuration: Mainly configure parameters such as working mode (aggressive mode/main mode), encapsulation mode (tunnel/transmission mode), pre-shared key, security proposal, IKE lifetime, and DPD peer detection.



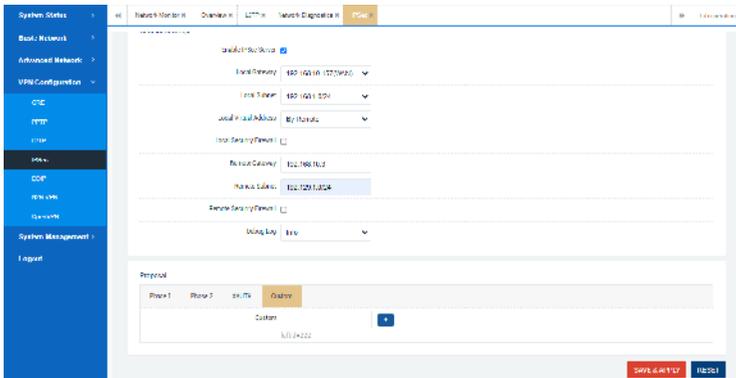
Phase 2 configuration: Mainly configure the security proposal, PFS parameters, and ESP lifetime of this phase.



XAUTH (extended authentication) configuration: User name/password can be set.



Custom settings: If both ends of the server-side settings are based on FQIN name ID authentication, you can configure specific authentication parameters, such as leftid (client authentication ID name) and rightid (server authentication ID name).



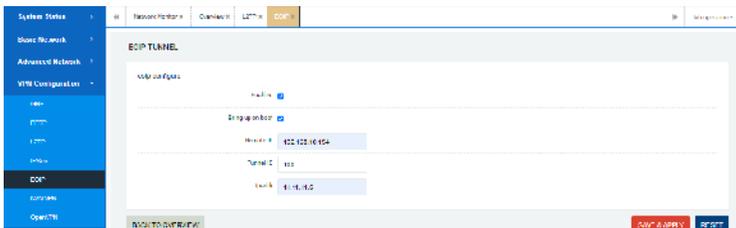
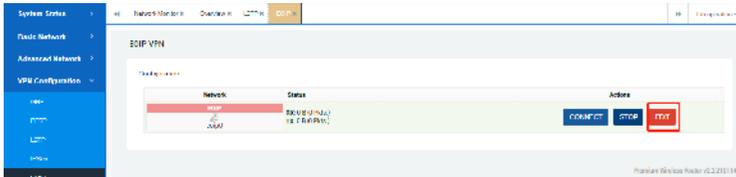
6.4.2 IPSec Security Alliance

Here you can view the tunnel establishment status and data flow at both ends of the IPSec. After the tunnel is successfully established, the following is as follows:



6.5 EOIP Client

This function is similar to that used by the GRE VPN client, but the authentication parameter here is the tunnel ID (0-500), and the specific configuration refers to the use of GRE VPN. as follows:



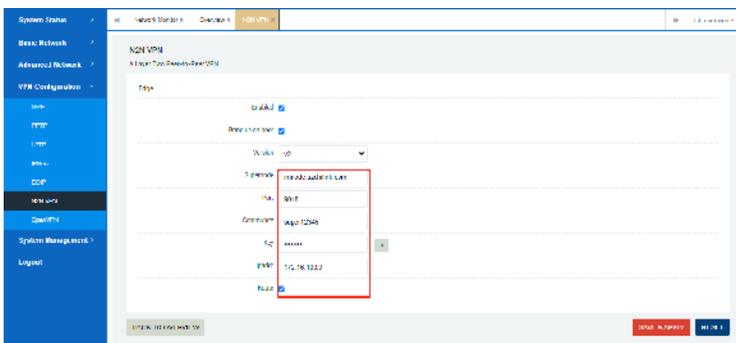
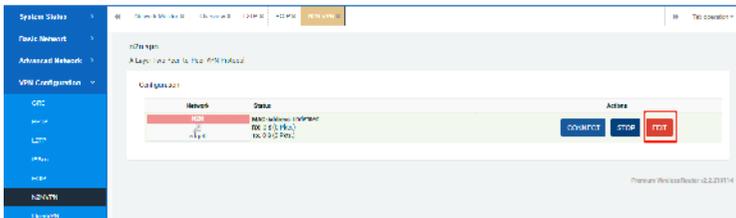
6.6 N2N VPN Client

The N2N network is mainly used to connect different client router devices or PC computer clients to the N2N super node server through the N2N protocol dial-up configuration to achieve the following two main usage scenarios.

Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

The specific configuration is as follows:





[Version]: Super node server optional protocol version V1 and V2;

[Super Node]: Fill in the IP address of the remote central server, generally the public network IP address;

[Port]: The service port of the super node server;

[Community]: N2N constitutes a point-to-point network identification name. Note: The names and passwords of the two client nodes must be exactly the same;

[Secret Key]: The verification password of the child node community network, the passwords of different nodes must be consistent;

[Address]: The virtual IP address in a peer-to-peer network, usually a private network;

[Routing and forwarding]: Used to automatically forward and access different sub-node routing networks;

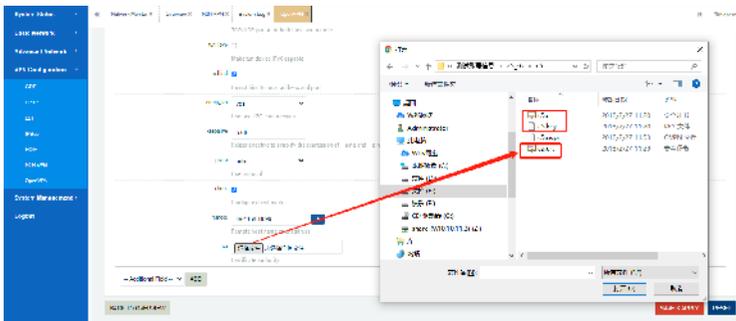
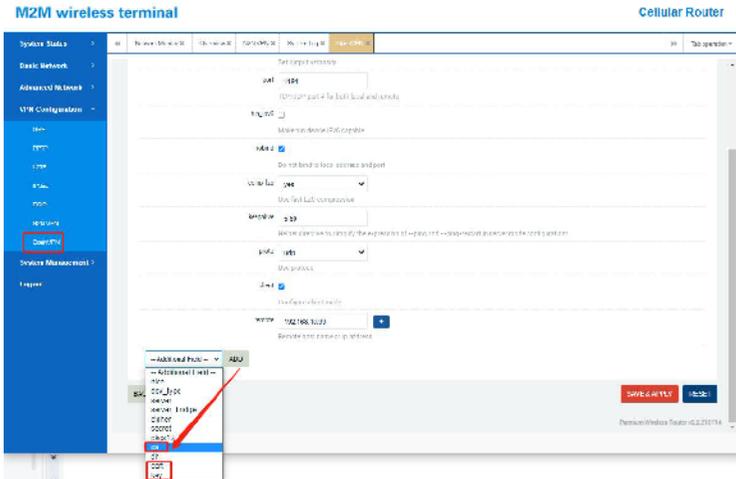
6.7 OPEN VPN

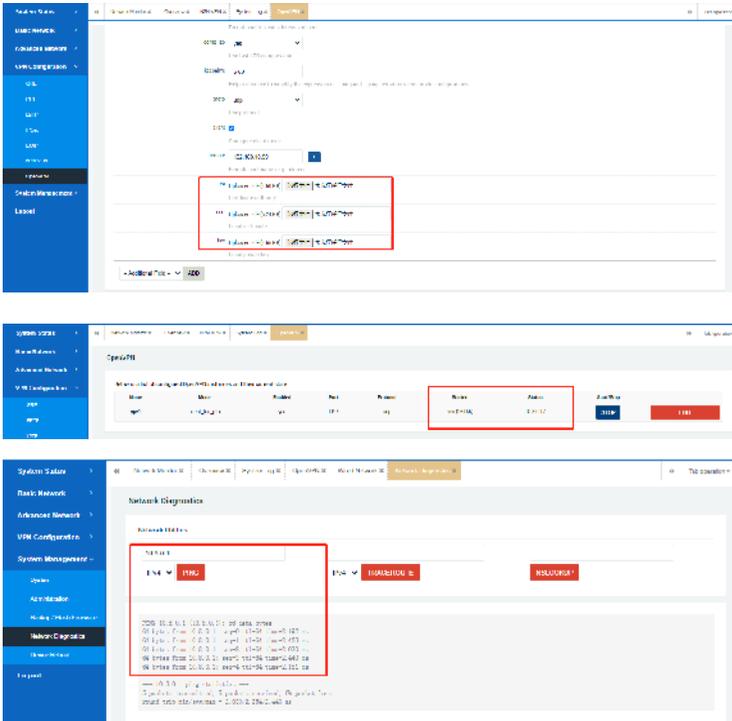
The OPEN VPN network is mainly used to connect different client router devices to the OPEN server after dialing through a specified protocol, so as to realize the following two main usage scenarios.

Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

2) Then click the "Add" button to add the openvpn client CA certificate, cert certificate, and key key certificate generated in advance on the server side one by one, and correctly configure the server IP address and port number, use protocol (default is udp), etc., and save the application The post-connection conditions are as follows:





7. System Management

This chapter mainly introduces some system Settings of the router, such as system language, time zone, NTP server Settings and configuration of several network access modes.

At the same time, you can modify some system default management, such as login user name, password, shell background login access, etc. Finally, you can

perform instant/timed restarts, firmware updates, configuration file backups, and more.

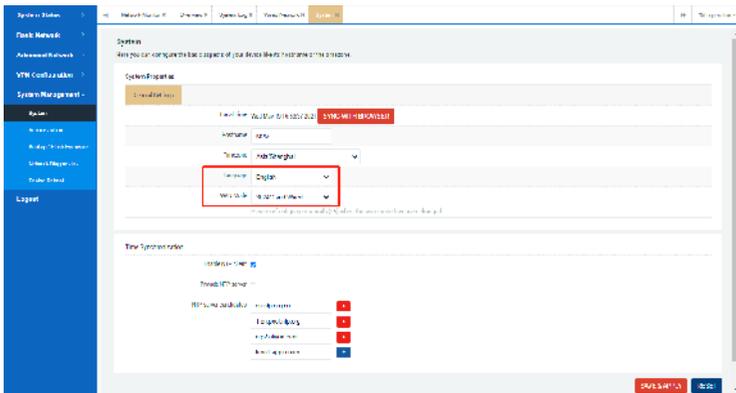
7.1 System

7.1.1 System property

In this section you can configure the system host name, time zone and language Settings, or change the WAN mode Settings, etc. You can also update the system local time by clicking "Synchronize Browser Time".

7.1.1.1 General Settings

As shown in the figure below, you can change the host name (M2M by default), time zone, language, etc.



7.1.1.2 Modification of WAN mode

The router supports three different "WAN modes", as described below:

7.1.1.2.1 3G/4G and Wired (default)

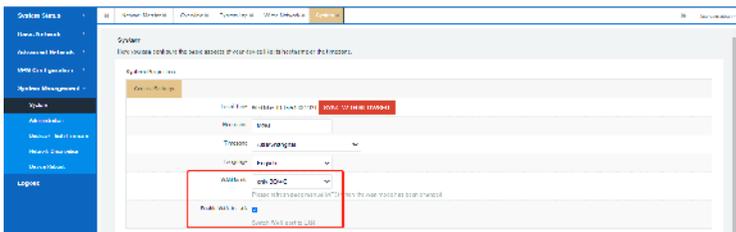
It means that the device supports both WAN port network access (cascaded to the LAN port of the upper router, and the network segment of the two routers cannot be the same) and 3G/4G mobile network.



7.1.1.2.2 only 3G/4G

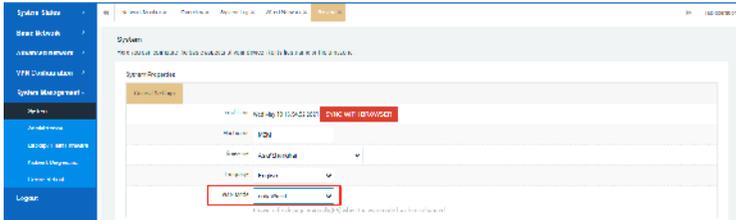
It means that the router only supports the SIM card mobile network and no longer supports the WAN network access (even if the WAN is connected to the superior network, it does not work);

You can further switch the WAN port to LAN by checking "WAN to LAN", so that you can connect to two user devices at the same time.



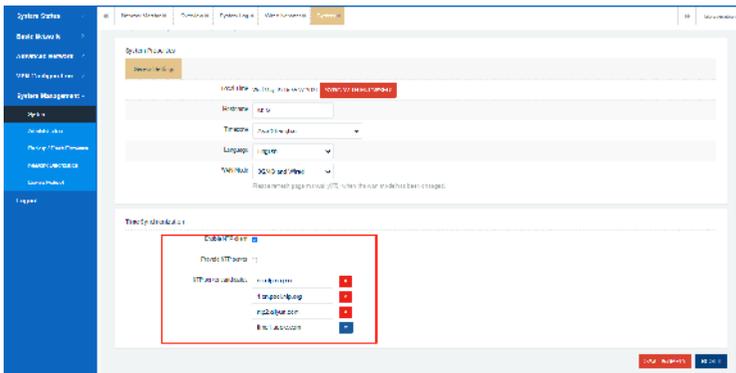
7.1.1.2.3 Only Wired

It means that the router only supports wired WAN network access and no longer supports SIM card mobile network (it will not work even if the SIM card is inserted and the network is successfully connected).



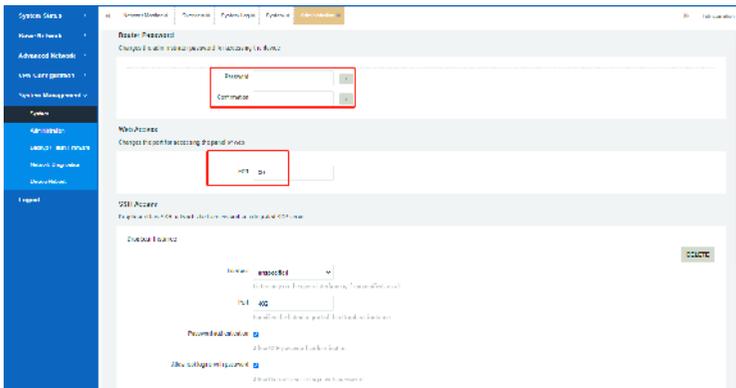
7.1.2 Time synchronization

The router system supports the NTP network timing service, and the device has several default NTP servers. You can also customize to add or modify other NTP servers.



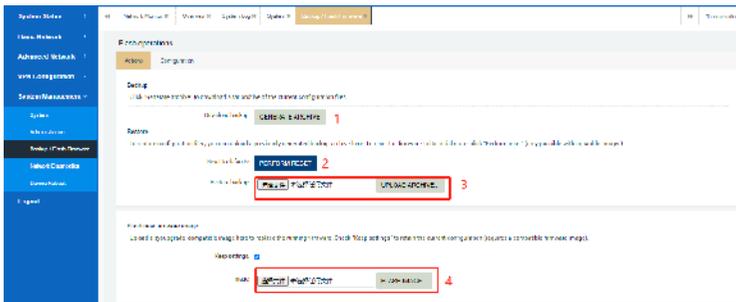
7.2 Administration

In this chapter, you can modify the system's Web login password (default admin), Web access port (default 80), background SSH access (default LAN access, port 402) and other management permissions (in order to use the device safely, it is suggested that customers should change the default parameters when using the device).



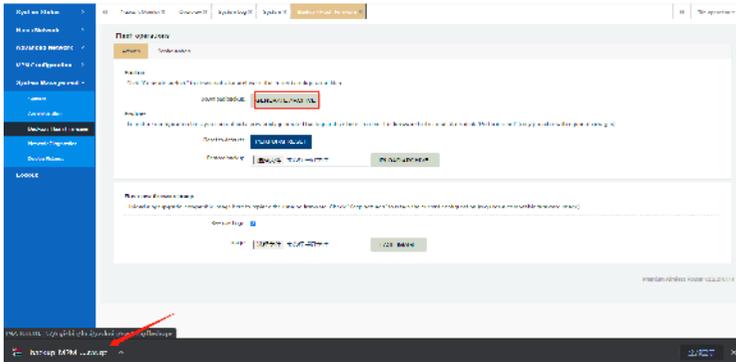
7.3 Backup/flush Firmware

In this chapter, you can perform the following operations on the device system, such as firmware upgrade, backup parameters, reset, etc.



7.3.1 Generate Archive

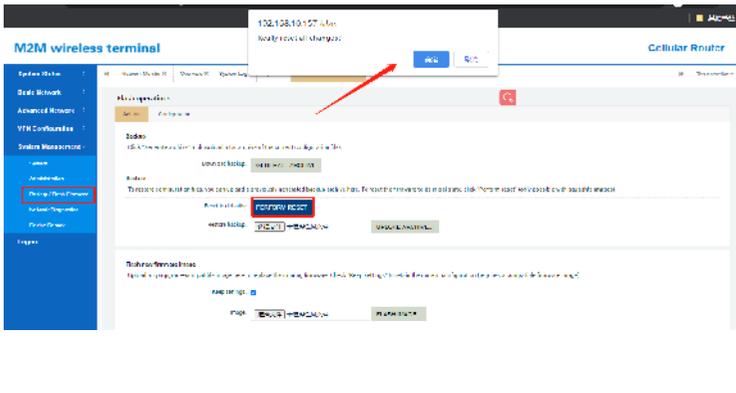
For this part, you can download some of the current configurations by clicking the 'Generate Archive' button of the router for backup so that you can use it for the next time.

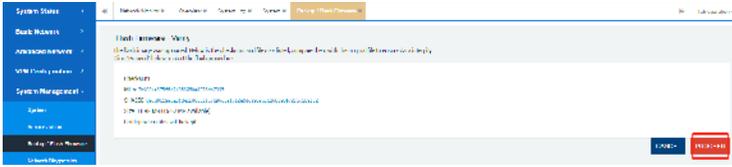


7.3.2 Perform Reset

The router system supports two ways to reset. Refer to the following instructions.

Method 1: Log in to the device Web page, and click "Execute Reset" to restore the routing system to the factory Settings. Please perform this operation carefully.



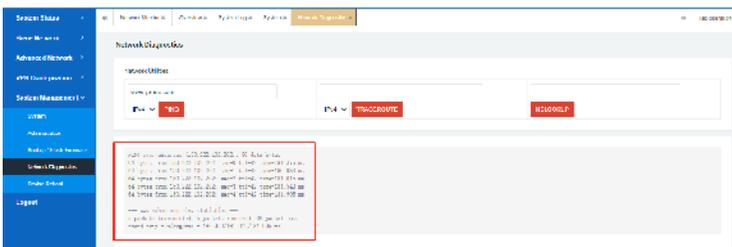


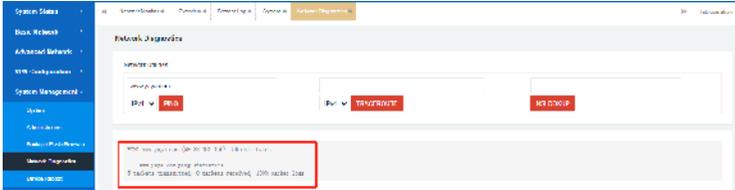
Note: Select the "Keep settings" button, and the system will retain the user's original configuration parameters after upgrade. When upgrading firmware across versions, it is recommended not to check this option to prevent incompatible use of some system functions.

7.4 System diagnostics

This chapter mainly introduces and instructs users how to confirm whether the router network is unblocked by using 'ping'(to test whether the Internet is accessible) and 'traceroute' (to track and view the network routing table) tools.

In particular, if you can ping an external network address (such as www.yahoo.com) successfully, the network is reachable. Otherwise, it indicates that the current network is abnormal and cannot be connected to the Internet, which requires further investigation and processing.





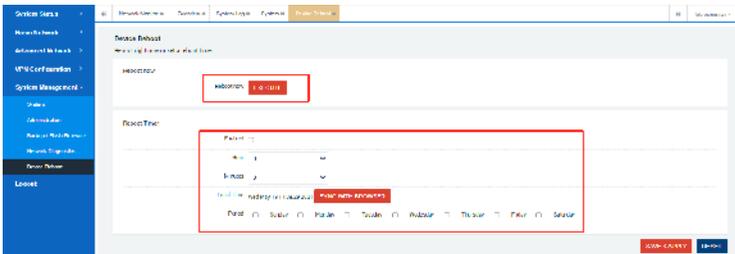
7.5 Device Reboot

7.5.1 Reboot now

Here you can restart the router immediately by clicking the Execute button if you need to.

7.5.2 Reboot timer

With this feature, you can set a specific time to restart the router system by date, hour, or minute.



Appendix: Network Abbreviations

The following abbreviations are only listed based on the current router system (the order is not limited), and hope to provide basic help for you to understand some network terms.

abbreviation	describe
Host network access related:	
M2M	Machine to Machine
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control Address
TTL	Time To Live
MTU	Maximum Transmission Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ARP	Address Resolution Protocol
Device/SIM card identification:	
IMEI	International Mobile EquipMent Identity
IMSI	International Mobile Subscriber Identity
ICCID	Integrate Circuit Card Identity
USIM	Universal Subscriber Identity Module
SIM	Subscriber Identity Module
APN	Access Point Name
Operator network standard:	
LTE	Long Term Evolution
TDD	Time Division Duplexing
TD-SCDMA	Time Division-Synchronous Code Division MultiPle Access

GSM/GPRS/EDGE	Global System for Mobile Communications General packet radio service Enhanced Data Rate for GSM Evolution
FDD	Frequency Division Duplexing
CDMA2000/HDR	Code Division Multiple Access 2000 High Data Rate
CDMA	Code Division Multiple Access
WCDMA/HSDPA/ HSUPA/HSPA+	Wideband Code Division Multiple Access High Speed Downlink Packet Access High Speed Uplink Packet Access Enhanced High-Speed Packet Access
Common network domains:	
WAN	Wide Area Network
LAN	Local Area Network
VLAN	Virtual Local Area Network
MGT	Management
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network
3GWWAN1	3G/4G Wide Area Network
PPPoE	Point-to-Point Protocol Over Ethernet
PPP	Point to Point Protocol
Common network protocols:	
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over SecureSocket Layer
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
PING	Packet Internet Groper
Wireless WiFi use and encryption:	
AP	Access Point
STA	Station
SSID	Service Set Identifier
ESSID	Extended Service Set Identifier
BSSID	Basic Service Set Identifier
WMM	Wi-Fi Multi Media
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA-PSK	WPA-Preshared Key
WPA2-PSK	WPA2-Preshared Key
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
Firewall related use:	
QoS	Quality of Service
DMZ	Demilitarized Zone
NAT	Network Address Translation
SNAT	Source Network Address Translation
DNAT	Destination Network Address Translation
UpNp	Universal Plug and Play
ACL	Access Control Lists
Positioning/timing service:	
GPS	Global Positioning System
LBS	Location Based Services
MCC	Mobile Country Code
MNC	Mobile Network Code

LAC	Location Area Code
CID	Cell ID
SID	System ID
NID	Network ID
BID	Base station ID
BD	BeiDou
NTP	Network Time Protocol
Virtual private network use:	
VPN	Virtual Private Network
VPDN	Virtual Private Dial Network
GRE	Generic Routing Encapsulation
PPTP	Point-to-Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
IPSec	Internet Protocol Security
EoIP	Ethernet over IP
N2N	Node to Node
LCP	Link Control Protocol
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
MPPE	Microsoft Point-to-Point Encryption
Algorithm and verification protocol:	
MD5	Message-Digest Algorithm
DES	Data Encryption Standard
3DES	TriPle Data Encryption Algorithm
SHA	Secure Hash Algorithm
DH	Diffie-Hellman
SM3	/
IKE	Internet Key Exchange

DPD	Dead Peer Detection
PFS	Perfect Forward Secrecy
ESP	Encapsulating Security Payload
XAUTH	Extended Auth

CYGNUS
electronics

