3onedata

ICPE2300 Series
Industrial-grade 5G Router
User Manual

Document Version: 03

Release Date: 7/12/2022

Trademark statement

3onedata , 3onedata and 3One data are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Notice

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	tech-support@3onedata.com
Service hotline:	+86 -880-4496
E-mail:	sales@3onedata.com
Fax:	+86 0755-2670-3485
Website:	http://www.3onedata.com http://www.3onedata.com

Preface

The User Manual of NP series serial device server has introduced:

- Network management method

Note

The screenshot reference model of this manual is 1 Gigabit COMBO + 3 Gigabit Copper Ports + 2 2.4G Antennas + 2 5.8G Antennas + 4 5G Antennas + 2 CAN + 2 RS-232 + 2 RS-485/422 + 4 DI + 4 DO. Except for the following differences, the interface functions and interface operations of other series models basic are the same.

- Interface difference, the device has no CAN Port, serial port, IO port.
- WEB function difference, the device has no configuration of CAN Port, serial port and IO port.

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.”.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.

Format	Description
About this chapter	The section 'about this chapter' provide links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

Symbols

Format	Description
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	11/25/2021	Product release
02	1/11/2022	Document maintenance
03	7/12/2022	Product serialization, adding configuration of CAN port and serial port

Contents

PREFACE 1
CONTENTS I
1 LOGIN THE WEB INTERFACE 1
1.1 SYSTEM REQUIREMENTS FOR WEB BROWSING 1
1.2 SETTING IP ADDRESS OF PC 1
1.2.1 Wired Access Mode 1
1.2.2 Wireless Access Mode 3
1.3 LOG IN THE WEB CONFIGURATION INTERFACE 3
2 SYSTEM INFORMATION 5
3 BASIC NETWORK 9
3.1 WAN MODE 9
3.2 WAN NETWORK SETTINGS 10
3.3 WIFI & 4G/5G ROAMING 15
3.3.1 Policy Status 16
3.3.2 Roaming Policy 17
3.4 MOBILE DETECTION 23
3.5 LINK BACKUP 24
3.6 LOCAL AREA NETWORK 26
3.7 DYNAMIC DOMAIN NAME 27
3.8 ROUTING TABLE SETTINGS 28
4 WLAN SETTINGS 32
4.1 BASIC PARAMETER SETTINGS 32
4.2 WIRELESS CLIENT FILTERING 43
5 ADVANCED NETWORK 46
5.1 PORT FORWARD 46
5.2 PORT REDIRECTION 47
5.3 DMZ SETTINGS 48
5.4 UPNP SETTINGS 49
5.5 MULTICAST NAT 51
5.6 VRRP 52
5.7 RIP 56
5.8 OSPF 57
5.9 STATIC DHCP 59
5.10 DHCP CLIENT 61

5.11 QoS 62
6 CAN SETTINGS 63
7 CAN MODE 68
7.1 TCP SERVER MODE 69
7.2 TCP CLIENT MODE 72
7.3 UDP SERVER MODE 75
7.4 UDP CLIENT MODE 77
7.5 UDP RANG MODE 79
7.6 UDP MULTICAST MODE 82
8 CAN STATUS 85
8.1 CAN PORT COMMUNICATION STATISTICS 85
8.2 NETWORK CONNECTION STATUS 86
9 COMMUNICATION PRARAMETERS 88
10 SERIAL MODE 92
10.1 REALCOM MODE 93
10.2 TCP SERVER MODE 97
10.3 TCP CLIENT MODE 103
10.4 UDP SERVER MODE 109
10.5 UDP CLIENT MODE 113
11 SERIAL STATUS 117
11.1 SERIAL PORT COUNT 117
11.2 SERIAL PORT STATUS 118
11.3 NETWORK CONNECTION STATE 119
11.4 SERIAL PORT ERROR COUNT 121
12 MODBUS UPGRADE 123
12.1 UPGRADE 123
13 FIREWALL 125
13.1 IP FILTER 125
13.2 MAC FILTER 127
13.3 URL FILTER 128
13.4 KEYWORD FILTER 129
13.5 IP ADDRESS BLACK/WHITE LIST 131
14 VPN TUNNEL 133
14.1 GRE SETTINGS 133
14.2 PPTP CLIENT SETTINGS 134
14.3 PPTP SERVER SETTINGS 136
14.4 L2TP CLIENT SETTINGS 138
14.5 L2TP SERVER SETTINGS 140
14.6 IPSEC 141
15 SYSTEM MANAGEMENT 145
15.1 DEVICE ALIAS 145
15.2 TIME SETTINGS 146
15.3 ACCESS SETTINGS 147

15.4 TIMED RESTART 148
15.5 BACKUP RECOVERY 149
15.6 LOG MANAGE 150
15.7 FIRMWARE UPGRADE 151
15.8 SYSTEM SETTINGS 152
16 DIAGNOSTIC TOOLS 153
16.1 SYSTEM LOG 153
16.2 PING TEST 154
16.3 ROUTE TRACKING 155
17 FAQ 157
18 MAINTENANCE AND SERVICE 160
18.1 INTERNET SERVICE 160
18.2 SERVICE HOTLINE 160
18.3 PRODUCT REPAIR OR REPLACEMENT 161

1 Login the WEB Interface

1.1 System Requirements for WEB Browsing

Using this equipment, the system should meet the following conditions.

Hardware and Software	System requirements
CPU	Above Pentium 586
Memory	128MB or more
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 8.0 or above
Operating system	Windows XP/7/8/10

1.2 Setting IP Address of PC

1.2.1 Wired Access Mode

The default management network address of the device as follows:

IP Settings	Default Values
IP address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Please confirm the computer has installed and enabled Ethernet network card.

- Before conducting remote configuration, please confirm the route between computer and device is reachable.
- Before making a local configuration, make sure that the IP address of the computer and the serial server are on the same subnet.

Note:
While configuring the device for the first time, if it's the local configuration mode, first confirm the network segment of current PC is 1.

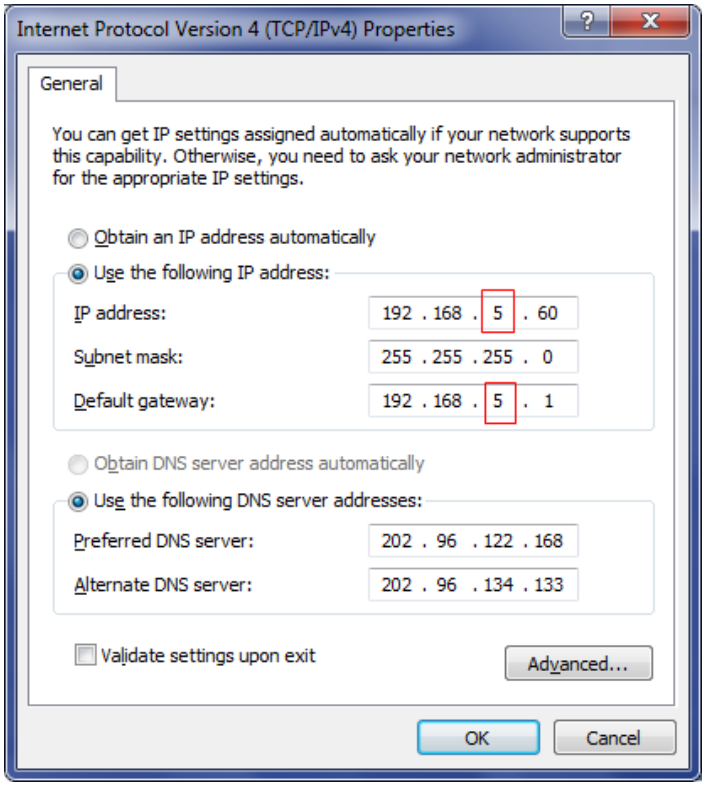
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

Step 1. Open "Control Panel> Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2. Change the selected "5" in red frame of the picture below to "1".



Step 3. Click “OK”, IP address is modified successfully.

Step 4. End.

1.2.2 Wireless Access Mode

The default management network address of the device as follows:

IP Settings	Default Values
IP address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Please confirm the computer has installed and enabled wireless network card.
- Place the computer on wireless network range of the device.
- Please confirm the IP address of computer is in the same subnet to the device.

Notice:

If the computer accesses to the Internet via proxy server, proxy service must be cancelled.

Set the IP address of computer in the same subnet to the device IP address.

Operation Steps

Operation steps of wireless connection as follows.

Note:

This manual takes the wireless network settings function of Windows 7 system for example.

Step 1. Click wireless icon "  " on the lower right corner of the computer, pop up the wireless list box.

Step 2. Choose the device wireless network in the wireless list box, click "Connect" button.

Note:

Default wireless network begins with "3ONE", without encryption.

Step 3. End. After successful connection, wireless network displays "Connected".

1.3 Log in the Web Configuration Interface

Operation Steps

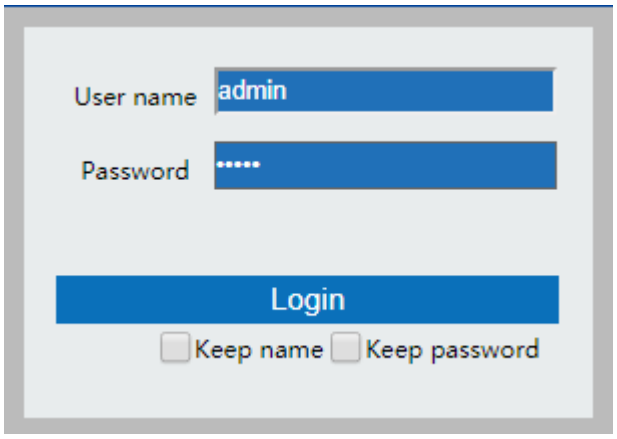
Login in the web configuration interface as follow:

Step 1. Run the computer browser.

Step 2. Enter the address of the device "http://192.168.1.254" in the address bar of the browser.

Step 3. Click the “Enter” key.

Step 4. Pop-up dialog box as shown below, enter the user name and password in the login window.



Note:
The default username and password are “admin”; please strictly distinguish capital and small letter while entering.

Step 5. Click "Login".

Step 6. End.

After successful login, you can configure the relevant parameters and information of the WEB interface as needed.

Note:
After logging in to the device, user can modify the device IP address for convenient usage; if there is no interface operation within 10 minutes, user will need to log in to the device again.

2 System Information

Function Description

On the "System information" page, user can check the following information:

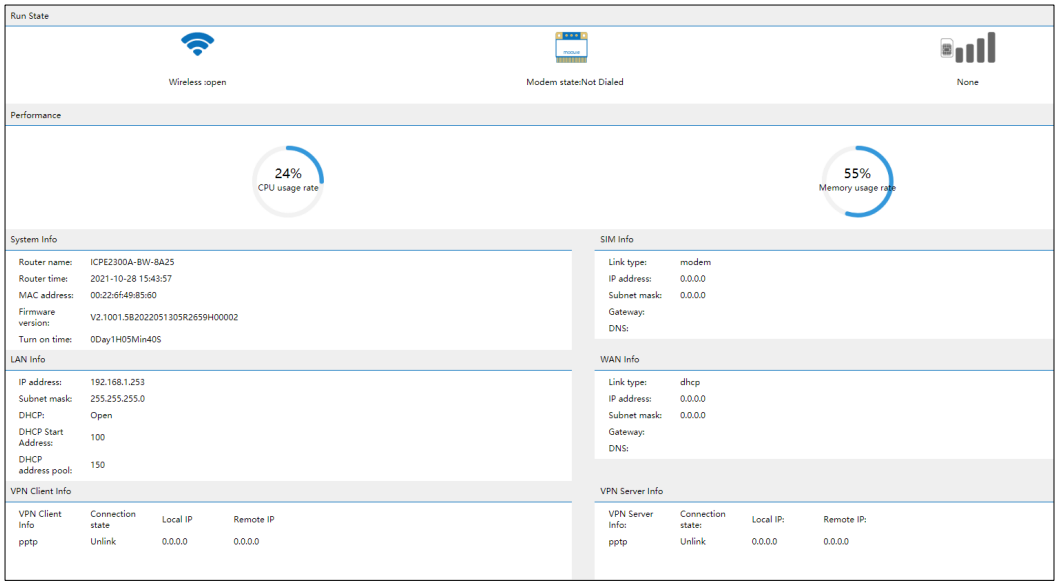
- Running state
- Performance;
- System Information;
- SIM card information;
- LAN information;
- WAN information;
- VPN client information;
- VPN server information.

Operation Path

On the navigation bar, select "System information".

Interface Description

System status interface as follows:



The main element configuration description of system status interface:

Interface Element	Discription
Run state	**The running state bar**
Wireless	The status of device wireless function is displayed as follows: • Open: the wireless WiFi function has been enabled; • Close: the wireless WiFi function hasn't been enabled.
Modem state	The states of 5G module Modem.
SIM card	Information including the existence state of SIM card used by current device, operator's network, network operating mode and signal strength etc.
Performance	**The performance bar**
CPU (%)	Device CPU utilization rate (%).
Memory (%)	Device memory utilization rate (%). Note: The performance of the device would be affected if the application consumes too much memory.
System Info	**System information bar**
Router name	Display the device name.
Router time	The current time displayed by router. Its format is Year-Month-Day Hour: Minute: Second.
MAC address	The MAC Address of this device.
Firmware version	Device firmware version.
Turn on time	The run time after turning on the device
SIM information	**SIM information bar**

Interface Element	Discription
Link Type	SIM connection Type
IP Address	IP address obtained by SIM card from network operator.
Subnet mask	Subnet mask address of SIM.
Gateway	The gateway address of SIM.
DNS	DNS server address of SIM.
LAN info	**The LAN information bar**
IP Address	The IP address information of LAN.
Subnet mask	The subnet mask information of LAN.
DHCP	The state of the DHCP server function.
DHCP start address	The minimum host number of IP address assigned by DHCP address pool, which is 100 by default.
DHCP address pool	The maximum IP address number assigned by DHCP address pool, which is 150 by default
WAN info	**The WAN information bar**
Link Type	The connection type of WAN.
IP Address	The IP address information of WAN.
Subnet mask	The subnet mask information of WAN.
Gateway	The gateway information of WAN
DNS	The DNS information of WAN
VPN client information	**The VPN client information bar**
VPN client info	Related information about VPN client. It displays related information when VPN client is enabled.
Connection status	The connection state of VPN client: • Unlink; • Connected.
Local IP	The IP address of local client.
Remote IP	The IP address of remote server.
VPN server infor	**The VPN server information bar**
VPN server infor	Related information about VPN server. It displays related information when VPN server is enabled.
Connection state	The connection state of VPN server: • Not connected; • Connected.
Local IP	The IP address of local server.

Interface Element	Discription
Remote IP	The IP address of remote client.

3 Basic Network

3.1 WAN Mode

Function Description

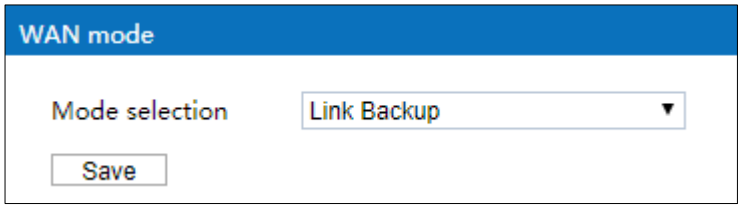
On “WAN Mode” page, users can set network mode. The device can be connected to the network via wired (WAN port), wireless roaming (WiFi), or 5G mobile network (SIM card).

Operation Path

Choose “Basic Network > WAN mode” in the navigation bar.

Interface Description

The WAN mode interface is as follows:



The configuration description of main elements of the WAN Mode interface:

Interface Element	Discription
Mode Selection	Choose drop-down list in WAN network mode, the options as follows: • Link backup: network connection can be switched between wired WAN port network and 5G module mobile network. • WiFi & 4G/5G roaming: network connection can be

Interface Element	Discription
	switched between WiFi wireless network and 5G module mobile network.

3.2 WAN network settings

Note

"WAN network settings" and "link Backup" page are displayed when "WAN Mode" is "link Backup".

Function Description

On the "WAN Network Settings" page, you can set the connection interface of WAN as follows:

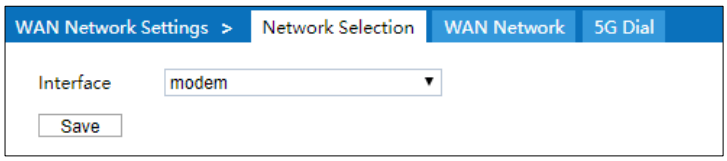
- WAN: connecting WAN through WAN port of the device.
  - Dynamic: the WAN port of the device accesses network address information allocated by network provider or outer network automatically;
  - Static address: configuring the network information of the device WAN port manually;
  - PPPoE: implement PPPoE point-to-point protocol dial-up via wired network WAN port to access network;
  - WAN to LAN: WAN port woks as a LAN port for data exchange.
- MODEM: 5G dialing, connecting to 3G/4G/5G signal via SIM card to access Internet.

Operation Path

Choose "Basic Network > WAN networking settings" in the navigation bar.

Interface Description 1: Network selection

Network selection interface as follows:

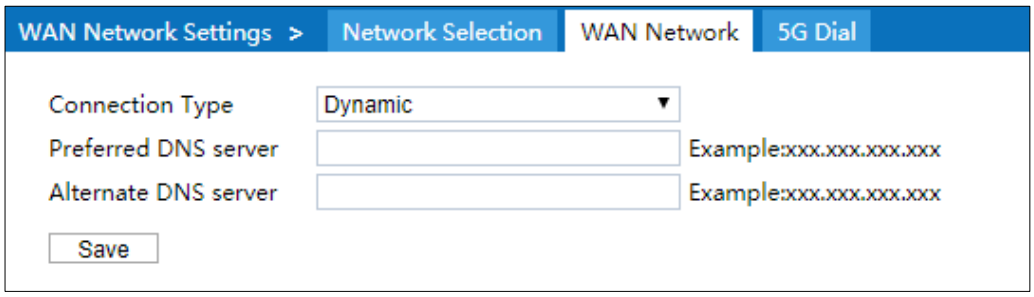


The main elements configuration description of network selection interface:

Interface Element	Discription
Interface	Drop-down list of WAN Network, options as follows: • WAN: obtaining wired network through WAN port. • Modem: obtaining mobile network through SIM.

Interface Description 2-1: WAN Network-Dynamic access

WAN Network-Dynamic interface is as follows:

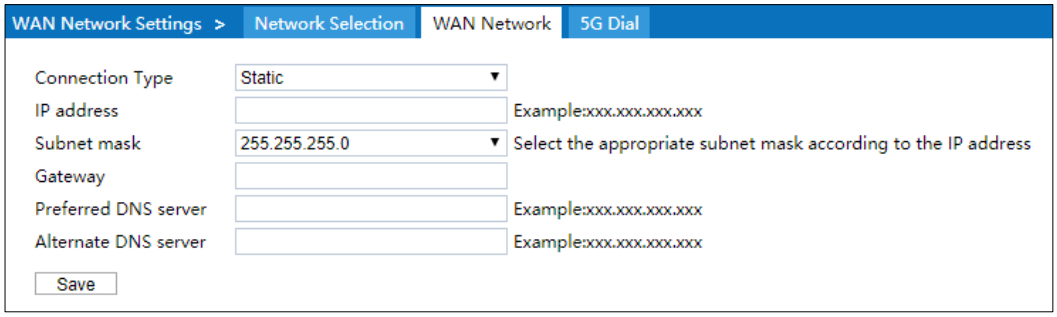


The main elements configuration description of WAN Network-Dynamic interface:

Interface Element	Discription
Connection Type	Dynamic: the WAN port of the device accesses network address information allocated by network provider or outer network automatically.
Preferred DNS server	The DNS server address provided by network provider or extranet.
Alternate DNS server	The backup DNS server address provided by network provider or outer network. This item can be skipped.

Interface Description 2-2: WAN Network-Static Address

WAN Network-Static Address interface is as follows:

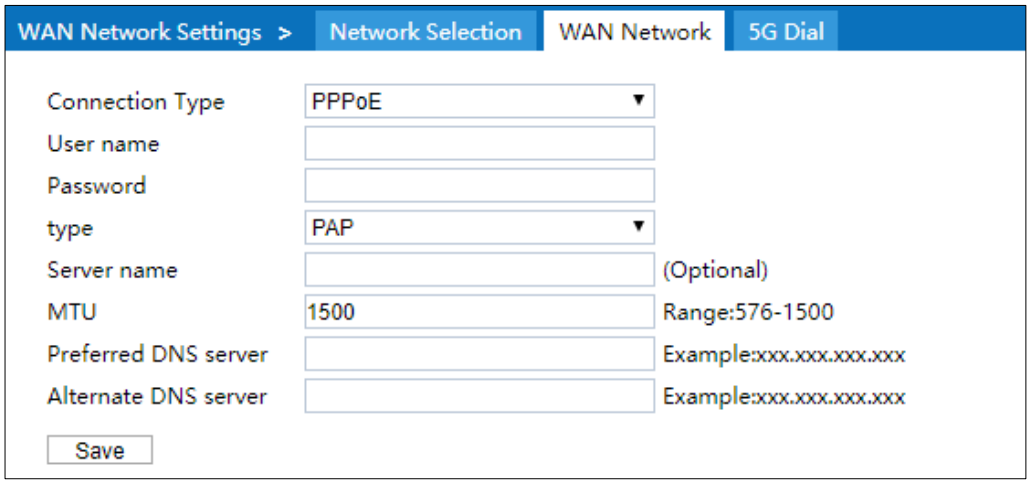


The main elements configuration description of WAN Network-static address interface:

Interface Element	Discription
Connection Type	Static address: the network information configuration of device WAN port.
IP Address	The fixed IP address distributed by network provider or extranet.
Subnet mask	Drop-down list of netmask.
Gateway	Gateway address offered by network provider or WAN.
Preferred DNS server	The DNS server address provided by network provider or extranet.
Alternate DNS server	The backup DNS server address provided by network provider or outer network. This item can be skipped.

Interface description 2-3：WAN Network-PPPoE Dialing

WAN Network-PPPoE Dialing interface is as follows:

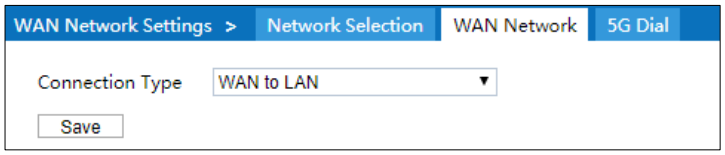


The main elements configuration description of WAN Network-PPPoE Dialing interface:

Interface Element	Discription
Connection Type	PPPoE: realize Internet access via PPPoE point-to-point protocol dialing.
User name	User name of PPPoE connection. Note: User name, password and server name are provided by network provider.
Password	Password of PPPoE connection. Note: User name, password and server name are provided by network provider.
Type	PPPoE dialing authentication type, options as follows: • PAP: Password Authentication Protocol, client transmits username and password in plaintext to for authentication. • CHAP: Challenge Handshake Authentication Protocol, sever transmits “challenge” message to client, then client authenticates sever through “challenge” message, MD5 encryption algorithm and other information. • PAP/CHAP: PAP or CHAP authentication method.
Server name	Server name, not fill if network provider doesn't supply. Note: User name, password and server name are provided by network provider.
MTU	The maximal length of single message that can get through in WAN network communication, the value range is 576-1500 bytes. Note: • MTU (Maximum Transmission Unit), the device will divide the data packet into multiple small packets if the maximum length of single message exceeds the given MTU value; so reasonable setting can optimize network speed; • MTU value is recommended to be same to the one of superior router.
Preferred DNS server	The DNS server address provided by network provider or extranet.
Alternate DNS server	The backup DNS server address provided by network provider or outer network. This item can be skipped.

Interface description 2-4: WAN Network- WAN to LAN

WAN Network- WAN to LAN interface is as follows:

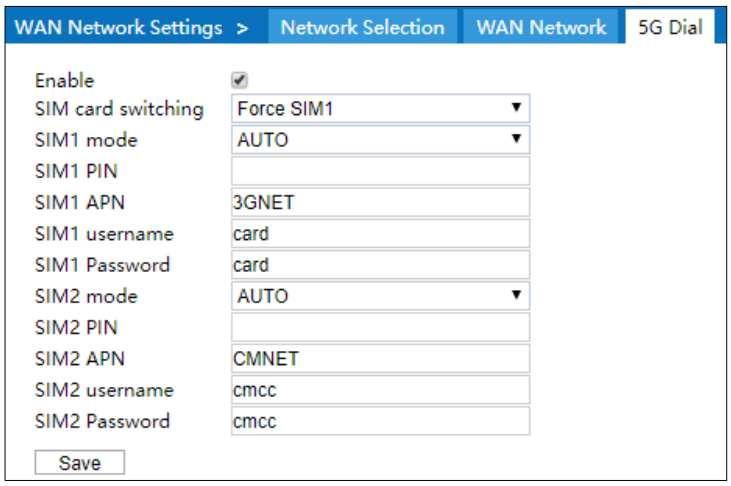


The main elements configuration description of WAN Network-WAN to LAN interface:

Interface Element	Discription
Connection Type	WAN to LAN: WAN port woks as a LAN port for data exchange.

Interface Description 3: 5G dial

5G dial interface as follows:



The main elements configuration description of 5G dial interface:

Interface Element	Discription
Enable	Enable checkbox, check to enable 5G dialing function.
SIM card switching	In the drop-down list of Switch SIM card, user can choose specified SIM card. The options are: • Force SIM1; • Force SIM2.
SIM1 mode	• The drop-down list of SIM1 mode. The options are: • Auto: self-adaptation; • 5G(NR)

Interface Element	Discription
	• LTE(4G) • (WCDMS/TD-SCDMA) • 3G(CDMA/EVDO)
SIM1 PIN	The Personal Identification Number (PIN) of SIM1. Please enter 4 to 8-digit PIN code if the boot PIN code is enabled; It is null by default if not enabled. Notice: When PIN code is enabled, user needs to enter it every time turning on the device. Please be cautious, it would be locked automatically if you enter wrong codes in three times.
SIM1 APN	The SIM1 access point name. It defaults to 3GNET.
SIM1 username	The username of SIM1. It defaults to card.
SIM1 password	The password of SIM1. It defaults to card.
SIM2 Mode	• The drop-down list of SIM2 network mode. The options are: • Auto: self-adaptation; • 5G(NR) • LTE(FDD/TDD) • (WCDMS/TD-SCDMA) • 3G(CDMA/EVDO)
SIM2 PIN	The Personal Identification Number (PIN) of SIM2. Please enter 4 to 8 digits PIN code if the boot PIN code is enabled; It is null by default if not enabled. Notice: When PIN code is enabled, user needs to enter it every time turning on the device. Please be cautious, it would be locked automatically if you enter wrong codes in three times.
SIM2 APN	The SIM2 access point name. It defaults to CMNET.
SIM2 username	The username of SIM2. It defaults to cmcc.
SIM2 password	The password of SIM2. It defaults to cmcc.

3.3 WIFI & 4G/5G roaming

Note

"WIFI & 4G/5G roaming" page is displayed when "WAN Mode" is "WIFI & 4G/5G roaming".

3.3.1 Policy Status

Function Description

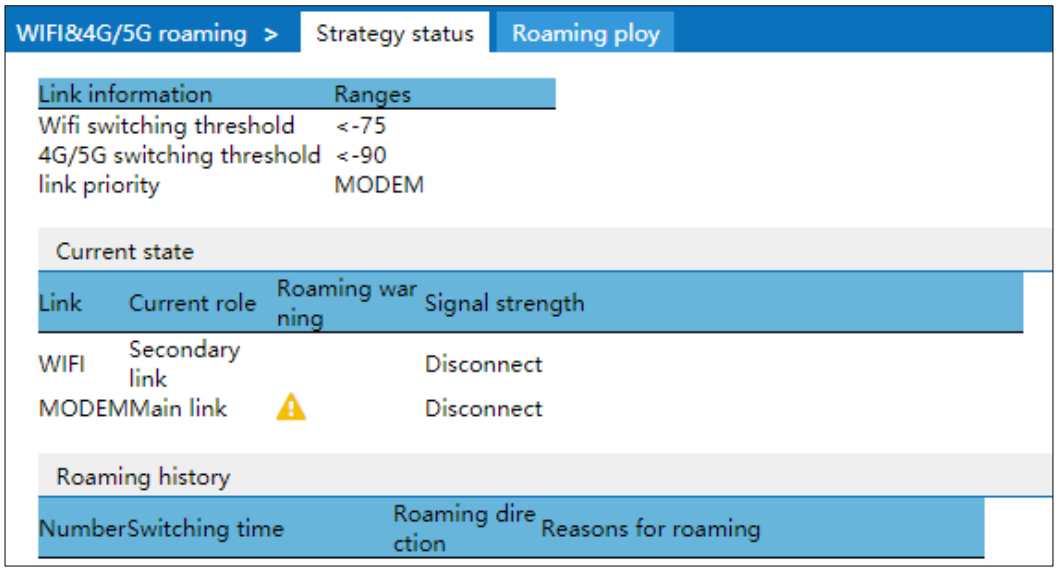
On the "Policy Status" page, users can view link status of current wireless roaming and record of roaming history.

Operation Path

Choose " Basic Network > WIFI & 4G/5G roaming > policy Status" on the navigation bar.

Interface Description

Policy Status interface as follow:



The main elements configuration description of Policy State interface:

Interface Element	Discription
Link Information	The threshold of WiFi and 4G/5G switching signal and the information of priority link are displayed.
Ranges	The threshold and link name corresponding to the link information.
Current state	**Current status display bar**
Link	Display link name information, which can be taken as:

Interface Element	Discription
	• WiFI； • LTE。
Current role	Display the current role of the link, which can be taken as: • Host link: • Deputy link.
Roaming warning	Prompt whether the current roaming conditions have been met and whether the roaming is about to take place, values are: •  :At present, the roaming conditions have been satisfied, and the roaming will happen soon. •  : At present, the roaming conditions are not satisfied, so there is no need for roaming
Signal strength	Displays the strength of the current link signal in dBm.
Roaming history	**Roaming history display bar** Note: Displays only the last 20 roaming records.
Number	Displays the serial number of roaming history record.
Switching time	Show the time of switching link.
Roaming direction	Display the main link after roaming, for example: when the value of roaming direction is WiFi, it means roaming from LTE to WiFi.
Reason for roaming	Shows the specific reason for roaming.

3.3.2 Roaming Policy

Function Description

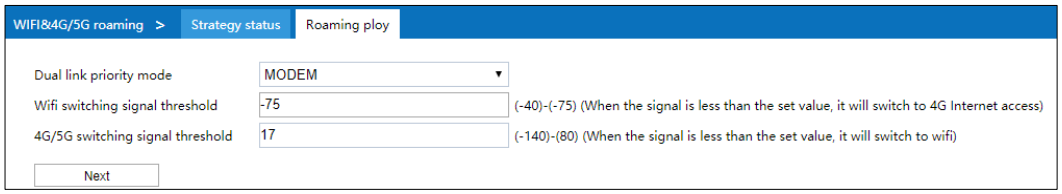
On “Roaming Policy” page, users can configure priority link and link information of WIFI & 4G/5G roaming.

Operation Path

Choose “ Basic Network > WIFI & 4G/5G roaming > Roaming Policy” on the navigation bar.

Interface Description 1: Dual Link Priority Method

The “Roaming Policy - Dual Link Priority Method” interface as below:



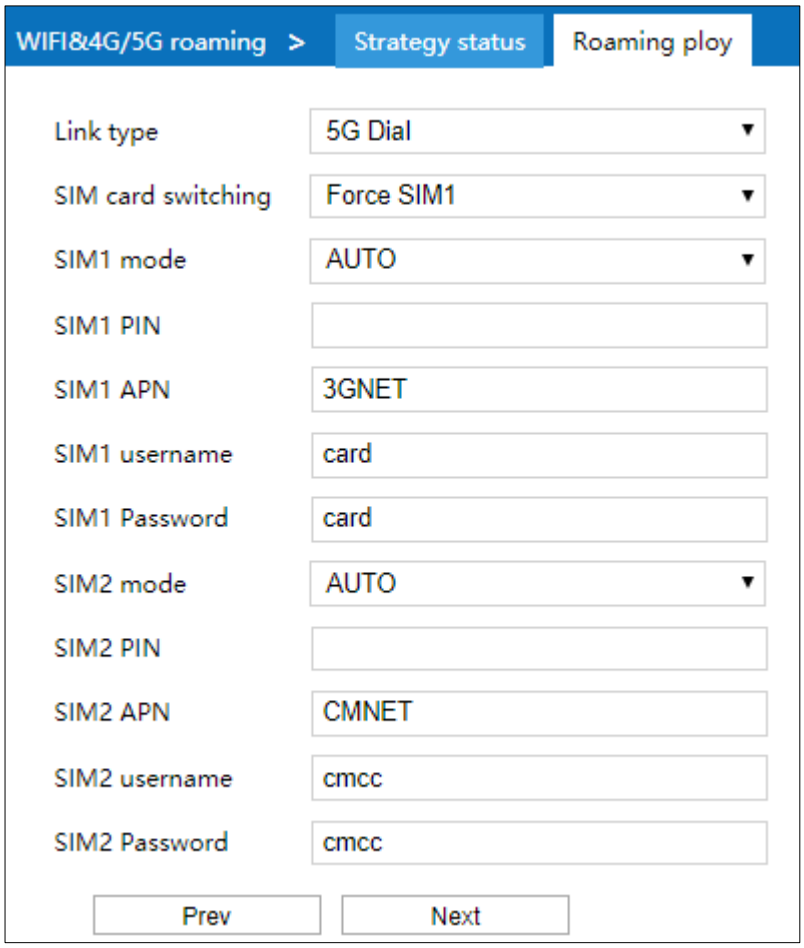
The main element configuration description of “Roaming Policy - Dual Link Priority Method” interface:

Interface Element	Discription
Dual link priority mode	The drop-down list of wireless roaming Link Priority Method, the options are as follows: • MODEN: adopts 4G/5G mobile signal to access network in priority. • WiFi: adopts WiFi wireless signal to access network in priority.
WiFi switching signal threshold	Switch to 4G/5G accessing network when the opposite wireless WiFi signal strength is less than specified threshold.
4G/5G switching signal threshold	Switch to Wi-Fi accessing network when the opposite wireless 4G/5G signal strength is less than specified threshold.

Click “Next” button to configure 4G/5G network parameters.

Interface Description 2: LTE

Roaming Policy-LTE interface as follows:



The main element configuration description of Roaming Policy-LTE interface:

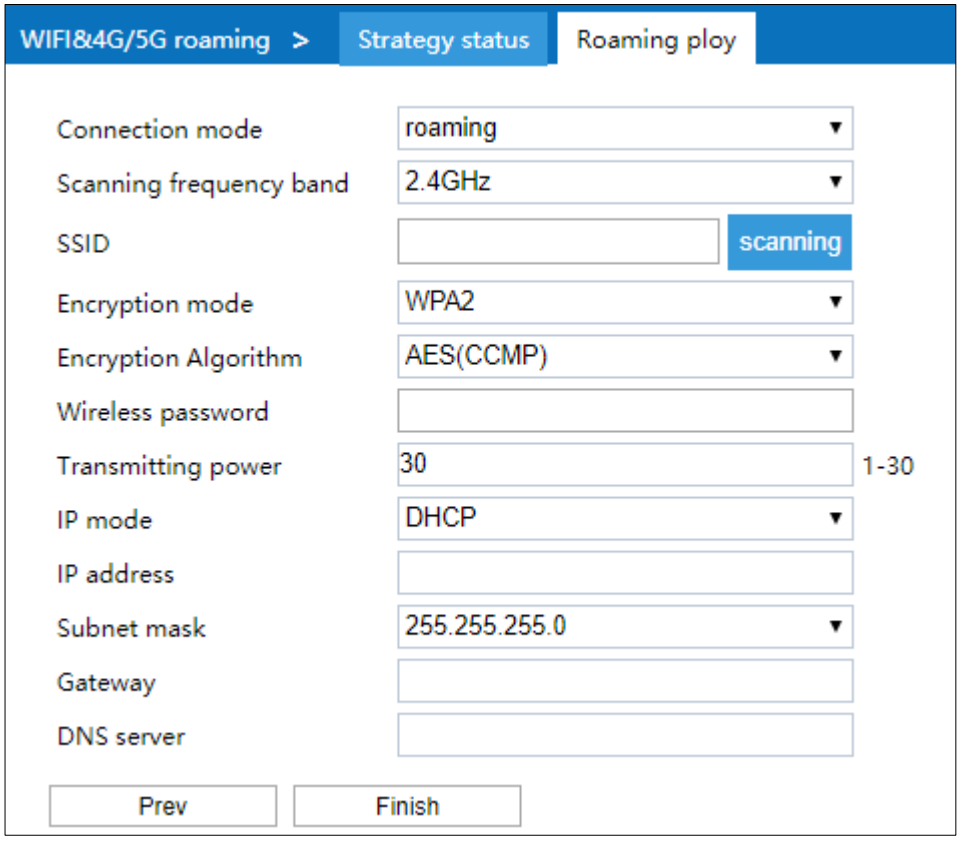
Interface Element	Discription
Link type	The link method of current configuration.
Switch SIM card	In the drop-down list of Switch SIM card, user can choose specified SIM card. The options are: • Force SIM1; • Force SIM2.
SIM1 mode	• The drop-down list of SIM1 mode. The options are: • Auto: self-adaptation; • 5G(NR) • LTE(4G) • (WCDMS/TD-SCDMA) • 3G(CDMA/EVDO)
SIM1 PIN	The Personal Identification Number (PIN) of SIM1. Please enter 4 to 8-digit PIN code if the boot PIN code is enabled; It is null by default if not enabled. Notice:

Interface Element	Discription
	When PIN code is enabled, user needs to enter it every time turning on the device. Please be cautious, it would be locked automatically if you enter wrong codes in three times.
SIM1 APN	The SIM1 access point name. It defaults to 3GNET.
SIM1 username	The username of SIM1. It defaults to card.
SIM1 password	The password of SIM1. It defaults to card.
SIM2 Mode	• The drop-down list of SIM2 network mode. The options are: • Auto: self-adaptation; • 5G(NR) • LTE(FDD/TDD) • (WCDMS/TD-SCDMA) • 3G(CDMA/EVDO)
SIM2 PIN code	The Personal Identification Number (PIN) of SIM2. Please enter 4 to 8 digits PIN code if the boot PIN code is enabled; It is null by default if not enabled. Notice: When PIN code is enabled, user needs to enter it every time turning on the device. Please be cautious, it would be locked automatically if you enter wrong codes in three times.
SIM2 APN	The SIM2 access point name. It defaults to CMNET.
SIM2 username	The username of SIM2. It defaults to cmcc.
SIM2 password	The password of SIM2. It defaults to cmcc.

Click “Next” button to configure WiFi network parameters.

Interface Description 3: WiFi

Roaming Policy-WIFI interface as follows:



The main element configuration description of Roaming Policy-WiFi interface:

Interface Element	Discription
Connection mode	The connection mode between the device and the wireless device on the opposite end is roaming by default: seamless switching between different APS.
Roaming signal threshold	The roaming signal threshold of the backup frequency band for scanning is -70 by default. When the roaming threshold of the backup band is lower than this value, it will scan.
Scannning frequency band	Scanning frequency band. Options are as follows: • 2.4GHz • 5GHz
SSID	SSID name of the opposite device wireless network. Note: User can add the wireless signal needed to connect via scan button.
Encryption mode	Encryption mode of opposite device wireless network, options as follows: • No encryption; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and

Interface Element	Discription
	AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm.
Encryption Algorithm	Wireless network encryption algorithm of the opposite device, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES(CCMP) encryption algorithm is supported.
Wireless password	Password of opposite device wireless network.
Transmitting power	The wireless signal transmission power of device ranges from 1 to 30dBm. Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is. • Different device has different transmitting power range.
IP Mode	The acquisition mode of wireless roaming segment IP, options following: • DHCP: acquires IP address by DHCP protocol. • Static IP: manually configure IP address.
IP Address	The fixed IP address distributed by network provider or extranet.
Subnet mask	Drop-down list of netmask.
Gateway	The default gateway address automatically distributed by network provider or outer network.
DNS server	IP address of DNS server. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

Click “Finish” button to submit wireless roaming configuration information.

3.4 Mobile Detection

ICMP (Internet Control Message Protocol) belongs to network layer protocol, and is mainly used for delivering control message between hosts and routers: including whether the network is connected, the host is reachable and the router is usable, etc. when there are situations in which IP data cannot access the target or the IP router cannot forward data packet at current transmission rate, it would send ICMP message automatically.

Function Description

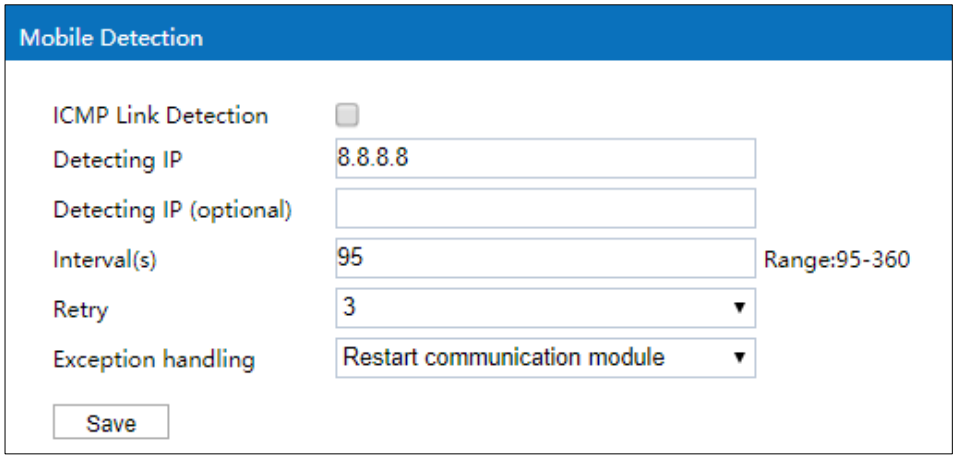
On the “Mobile Detection” page, user can detect the connection status of network and make corresponding operation.

Operation Path

Choose “Basic Network > Mobile Detection” in the navigation bar.

Interface Description

The mobile detection interface as follows:



The main element configuration description of mobile detection interface:

Interface Element	Note
ICMP Link Detection	ICMP Link Detection checkbox, checking to turn on ICMP link detection function, which can detect network connection.

Interface Element	Note
Detecting IP	To detect whether the specified IP address could be connected. It defaults to 8.8.8.8.
Detecting IP (optional)	To detect whether the backup IP address could be connected.
Interval (s)	The time interval of detection, the unit is second. The value range is 95-360.
Retry	To detect the times of retry, the drop-down list of retry. Options are: 2-5.
Exception handling	The corresponding way of handling detected exception. The drop-down list of exception handling, options are: • Restart communication module; • Switch SIM card; • Reboot the system.

3.5 Link Backup

Note

"WAN network settings" and "link Backup" page are displayed when "WAN Mode" is "link Backup".

Function Description

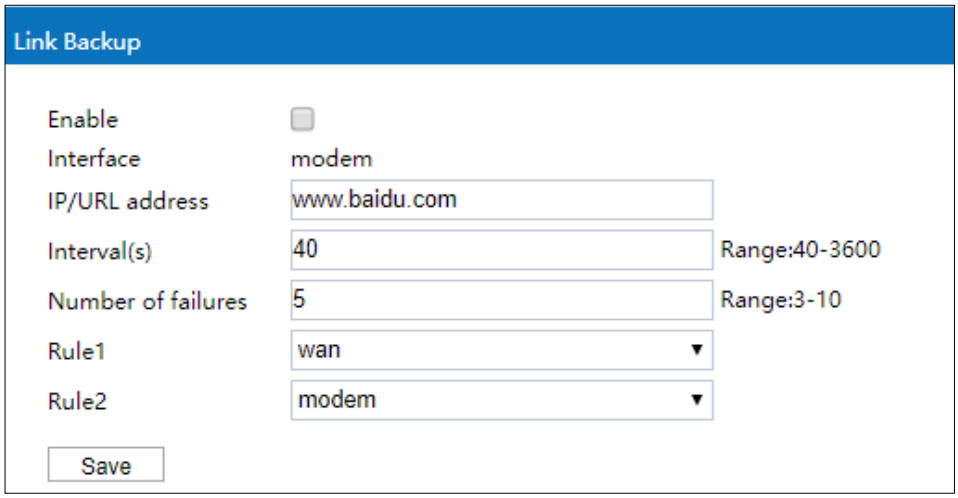
On the "Link Backup" page, user can configure the wired network and the wireless cellular network as link backup network. After Link Backup is enabled, if the current main network is abnormal, network connections can be switched to the backup network; When the main network returns to normal, network connections will automatically switch to the main network.

Operation Path

Choose "Basic Network > Link Backup" in the navigation bar.

Interface Description

The Link Backup interface as follows:



The main elements configuration description of Link backup interface:

Interface Element	Note
Enable	Link Backup function enable checkbox, check to enable Link Backup function.
Interface	Show the current working network interface of the device.
IP/URL address	To detect whether the specified IP address or network address can be accessed.
Interval (s)	The time interval of detection, the unit is second and defaults to 5.
Number of failures.	Number of detection failures, When number of detection failures exceed specified value, the corresponding network interface will be started in turn according to the rules.
Rule1	When number of failures exceed the threshold value due to interface network anomalies, the device will preferentially switch to the network interface specified by Rule 1. Rlue1 drop-down list, options as follows: • wan • modem
Rule2	When the network interface specified by Rule 1 is still abnormal, the device will switch to the network interface specified by Rule 2. Rule2 drop-down list, options as follows: • wan

Interface Element	Note
	• modem

3.6 Local Area Network

DHCP (Dynamic Host Configuration Protocol) is a LAN protocol which uses UDP protocol to allocate IP address to internal network automatically and improve IP address utilization. Client in network environment can acquire dynamic IP address, Gateway address, DNS server address and other information from DHCP server.

Function Description

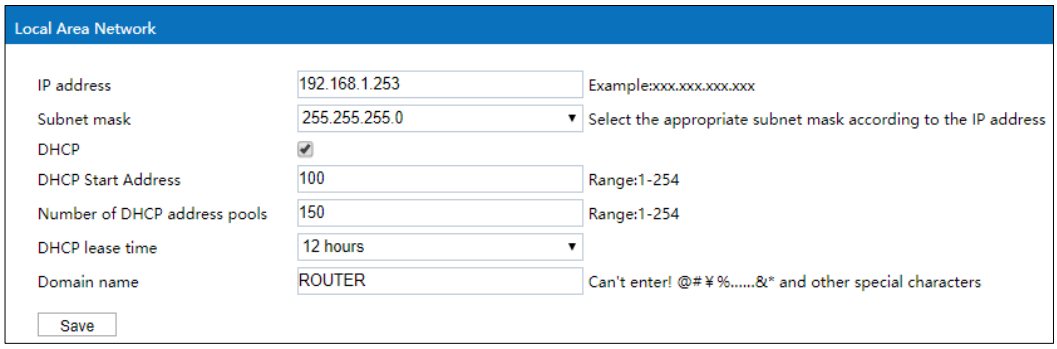
On the “Local Area Network” page, user can turn on DHCP server function and set relevant parameters of gateway.

Operation Path

Choose “Basic Network > Local Area Network” in the navigation bar.

Interface Description

The local area network interface as follows:



The main element configuration description of local area network interface:

Interface Element	Note
IP Address	IP address of the device LAN port.
Subnet mask	Drop-down list of netmask.
DHCP	DHCP function enable checkbox, check to enable DHCP server function.
DHCP start address	The minimum IP address host number allocated by DHCP address pool. Value range is 1-254.
Number of DHCP addresses pools	The maximum IP address number allocated by DHCP address pool. Value range is 1-254.

Interface Element	Note
DHCP lease time	Valid time of IP address distributed by DHCP address pool, it defaults to 12 hours. Drop-down list of time unit, options as follows: • 30 minutes; • 1 hour; • 6 hours; • 12 hours; • 1 day; • 3 days; • 7 days.
Domain name	DHCP domain name is composed of letter, number and underline; it supports 0-32 valid characters.

3.7 Dynamic Domain Name

If the IP address that the router Internet obtained is dynamically allocated by operator, the IP address might be different each time. In this situation, user can use dynamic domain name service. The domain name provider allows registering a domain name, which always corresponds to current dynamic IP address of the router. Therefore, user can visit the latest Internet IP address via visiting domain name.

Function Description

On the “Dynamic Domain” page, user can set relevant information of dynamic domain name.

Operation Path

Choose “Basic Network > Dynamic Domain” in the navigation bar.

Interface Description

The dynamic domain interface as follows:

The main element configuration description of dynamic domain interface:

Interface Element	Note
Enable	Dynamic Domain Name function checkbox, check to enable dynamic domain function.
DDNS supplier	The router supports multiple DDNS suppliers. The options in the DDNS supplier drop-down list are: • no-ip.com • 3322.org • dyndns.org • oray.com • Custom: When user chooses this item, the corresponding DDNS supplier name could be entered in the input box of DDNS supplier.
Domain name info	The relevant information of domain name applied from DDNS supplier.
Username	The user name applied from DDNS supplier.
Password	The password applied from DDNS supplier.
Update Time	Update the time interval of dynamic DNS to server, the unit is second, the value range is 10--360.

3.8 Routing Table Settings

Routing table is a spreadsheet or database stored in router, which has saved the paths to specified network address. The routing table includes topological information of

perimeter network, which mainly aims to implement selection between routing protocol and static routing.

Function Description

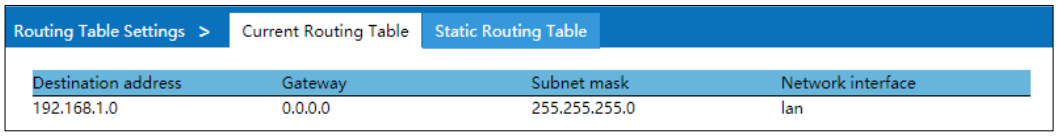
On the “Routing Table Setting” page, user can set relevant information of routing table.

Operation Path

Choose “Basic Network > Routing Table Setting” in the navigation bar.

Interface Description 1: Current Routing Table

The current routing table interface as follows:

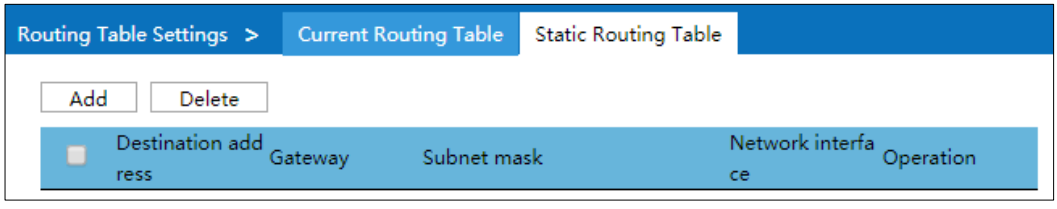


The main element configuration description of current routing table interface:

Interface Element	Note
Destination Address	The destination IP address information of current routing.
Gateway	The destination gateway information of current routing.
Subnet mask	The subnet mask information of current routing.
Network interface	The network interface information of current routing.

Interface Description 2: Static Routing Table

The static routing table interface as follows:



The main element configuration description of static routing table interface:

Interface Element	Note
☐	The check box of static routing entry. Click to check all static routing entries.
Destination Address	The destination IP address information of static routing.

Interface Element	Note
Gateway	The destination gateway information of static routing.
Subnet mask	The subnet mask information of static routing: • 255.255.255.0 • 255.255.255.255 • 255.255.255.254 • 255.255.255.252 • 255.255.255.248 • 255.255.255.224 • 255.255.255.192 • 255.255.255.128 • 255.255.254.0 • 255.255.252.0 • 255.255.248.0 • 255.255.240.0 • 255.255.224.0 • 255.255.192.0 • 255.255.128.0 • 255.255.0.0 • 255.254.0.0 • 255.252.0.0 • 255.248.0.0 • 255.224.0.0 • 255.192.0.0 • 255.128.0.0 • 255.0.0.0 • 254.0.0.0 • 252.0.0.0 • 248.0.0.0 • 240.0.0.0 • 224.0.0.0 • 192.0.0.0 • 128.0.0.0
Network interface	The network interface of static routing: • WAN • LAN • MODEM

Interface Element	Note
	• Manual Input
Operation	Edit: modify static routing table information.
Add	Click the “add” button at the top right corner to add static routing in the pop-up window of “static routing.
Delete select	Check the static routing information to be deleted, and then click the “delete select’ button at the top right corner to delete them.

4 WLAN Settings

4.1 Basic Parameter Settings

Function Description

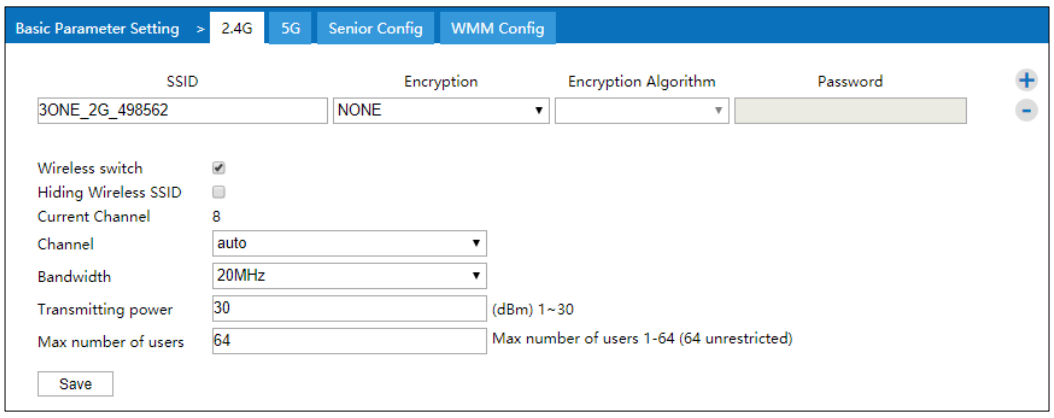
On the “Basic Parameter Settings” page of WLAN settings, user can implement 2.4G/5G basic configuration, senior configuration and WMM Configuration.

Operation Path

Please open in order: “WLAN Settings > Basic Parameter Settings”.

Interface Description 1: 2.4G

The 2.4G interface is as follows:



Main elements configuration descriptions of 2.4G interface:

Interface Element	Note
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE: No encryption; • WPA: Wi-Fi Protected Access. When the wireless

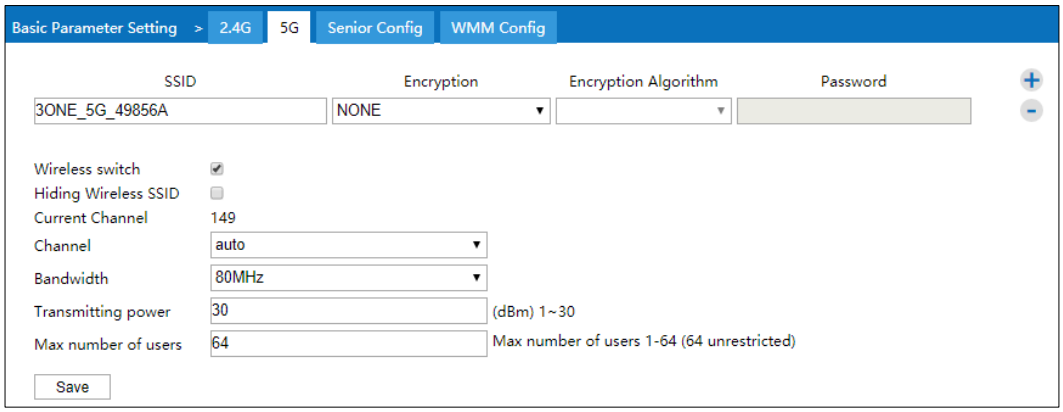
Interface Element	Note
	authentication method is personal edition, encryption method is PSK (pre-shared key); when the wireless authentication method is enterprise edition, encryption method is 802.1X authentication which use RADIUS server and EAP to authenticate. • WPA2: upgrade version of WPA, supports AES (Advanced Encryption Standard), and provides higher security for WLAN. • WPA-MIXED: the mixed-mode of WPA, is compatible with both WPA and WPA2 encryptions.
Encryption algorithm	Wireless network supports different encryption algorithms when it using WPS、WPA2 or WPA-MIXED encryption method, options as follows: • AES(CCMP): CCMP(Counter Mode with CBC-MAC Protocol) uses AES(Advanced Encryption Standard) encryption algorithm. • TKIP: Temporal Key Integrity Protocol, provides more secure protection mechanism than WEP encryption. • TKIP/AES: compatible with both TKIP and AES encryption algorithm.
Password	Password of wireless network, it supports 8-32 characters.
Wireless switch	Wireless Network function enable checkbox, check to enable 2.4G wireless Wi-Fi network.
Hiding Wireless SSID	Hidden wireless SSID enable checkbox, check to enable hidden wireless SSID function. After enabled, name of SSID from the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal first while connecting hidden wireless signal.
Current channel	The working channel of current 2.4G wireless network.
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 1: main frequency band 2412Hz, frequency range 2401~2423Hz; • 2: main frequency band 2417Hz， frequency range 2406~2428Hz;

Interface Element	Note
	• 3: main frequency band 2422Hz，frequency range 2411~2433Hz; • 4: main frequency band 2427Hz，frequency range 2416~2438Hz; • 5: main frequency band 2432Hz，frequency range 2421~2443Hz. • 6: main frequency band 2437Hz，frequency range 2426~2448Hz. • 7: main frequency band 2442Hz，frequency range 2431~2453Hz. • 8: main frequency band 2447Hz，frequency range 2436~2458Hz. • 9: main frequency band 2452Hz，frequency range 2441~2463Hz. • 10: main frequency band 2457Hz，frequency range 2446~2468Hz. • 11: main frequency band 2462Hz，frequency range 2451~2473Hz. • 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in USA, so it's temporarily unavailable; • 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in America, so it's temporarily unavailable; Note: • In order to improve the network performance, please choose unused channel in the device working environment. • Different country opens different channels.
Bandwidth	Channel bandwidth of wireless network, it defaults to 20MHz, options as follows: • 20MHz; • 40MHz. Note: 40MHz bandwidth binds two 20MHz bandwidth channels together to gain the handling capacity more than twice of the 20MHz bandwidth.
Transmitting power	The wireless signal transmission power of device ranges from 1 to 1~30dBm.

Interface Element	Note
	Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is. • Different device has different transmitting power range.
Max number of users	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.

Interface Description 2: 5G

The 5G interface is as follows:



Main elements configuration descriptions of 5G interface:

Interface Element	Discription
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE: No encryption; • WPA: Wi-Fi Protected Access. When the wireless authentication method is personal edition, encryption method is PSK (pre-shared key); when the wireless authentication method is enterprise edition, encryption method is 802.1X authentication which use RADIUS server and EAP to authenticate. • WPA2: upgrade version of WPA, supports AES (Advanced Encryption Standard), provides higher security for WLAN.

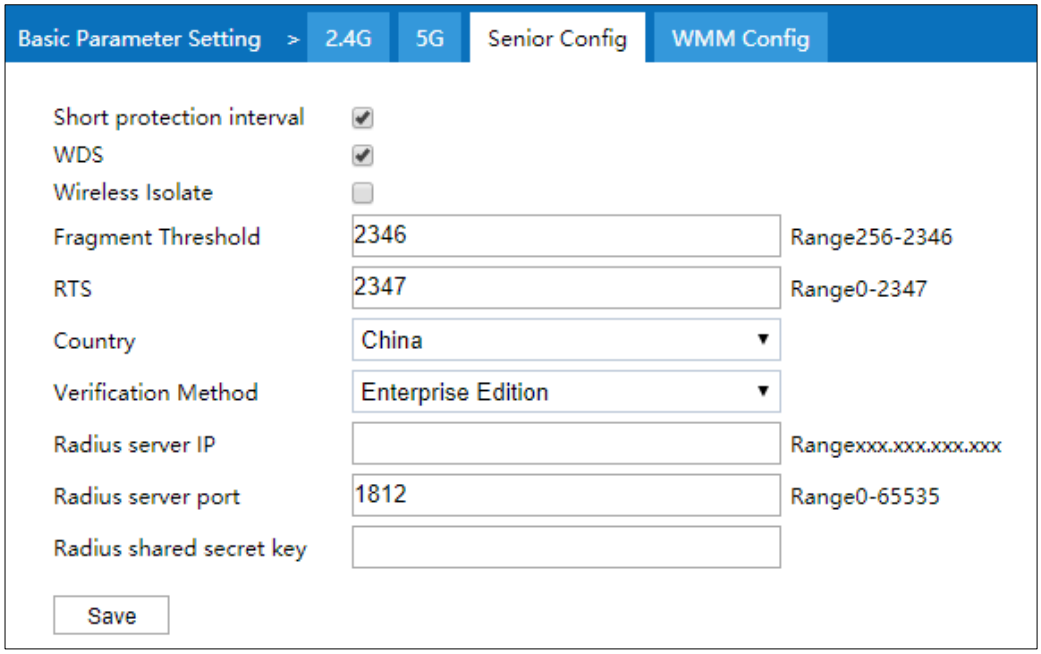
Interface Element	Discription
	• WPA-MIXED: the mixed-mode of WPA, is compatible with both WPA and WPA2 encryptions.
Encryption algorithm	Wireless network supports different encryption algorithms when it using WPS、WPA2 or WPA-MIXED encryption method, options as follows: • AES(CCMP): CCMP(Counter Mode with CBC-MAC Protocol) uses AES(Advanced Encryption Standard) encryption algorithm. • TKIP: Temporal Key Integrity Protocol, provides more secure protection mechanism than WEP encryption. • TKIP/AES: compatible with both TKIP and AES encryption algorithm.
Password	Password of wireless network, it supports 8-32 characters.
Wireless switch	Wireless Network function enable checkbox, check to enable 5.8G wireless WiFi network.
Hiding Wireless SSID	Hidden wireless SSID enable checkbox, check to enable hidden wireless SSID function. After enabled, name of SSID from the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal first while connecting hidden wireless signal.
Current channel	The working channel of current 5.8G wireless network.
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 36: main frequency band 5180Hz, frequency range 5170~5190Hz; • 40: main frequency band 5200Hz，frequency range 5190~5210Hz; • 44: main frequency band 5220Hz, frequency range 5210~5230Hz; • 48: main frequency band 5230Hz，frequency range 5210~5250Hz; • 52: main frequency band 5260Hz，frequency range 5250~5270Hz. • 56: main frequency band 5280Hz，frequency range 5270~5290Hz;

Interface Element	Discription
	• 60: main frequency band 5300Hz，frequency range 5290~5310Hz; • 64: main frequency band 5320Hz，frequency range 5310~5330Hz; • 100: main frequency band 5500Hz, frequency range 5490~5510Hz, this frequency band is not open in China, so it's temporarily unavailable; • 104: main frequency band 5520Hz, frequency range 5510~5530Hz, this frequency band is not open in China, so it's temporarily unavailable; • 108: main frequency band 5540Hz, frequency range 5530~5550Hz, this frequency band is not open in China, so it's temporarily unavailable; • 112: main frequency band 5560Hz, frequency range 5550~5570Hz, this frequency band is not open in China, so it's temporarily unavailable; • 116: main frequency band 5580Hz, frequency range 5570~5590Hz, this frequency band is not open in China, so it's temporarily unavailable; • 120: main frequency band 5600Hz, frequency range 5590~5610Hz, this frequency band is not open in China, so it's temporarily unavailable; • 124: main frequency band 5620Hz, frequency range 5610~5630Hz, this frequency band is not open in China, so it's temporarily unavailable; • 128: main frequency band 5640Hz, frequency range 5630~5650Hz, this frequency band is not open in China, so it's temporarily unavailable; • 132: main frequency band 5660Hz, frequency range 5650~5670Hz, this frequency band is not open in China, so it's temporarily unavailable; • 136: main frequency band 5680Hz, frequency range 5670~5690Hz, this frequency band is not open in China, so it's temporarily unavailable; • 140: main frequency band 5700Hz, frequency range 5690~5710Hz, this frequency band is not open in China,

Interface Element	Discription
	so it's temporarily unavailable; • 144: main frequency band 5720Hz, frequency range 5710~5730Hz, this frequency band is not open in China, so it's temporarily unavailable; • 149: main frequency band 5745Hz，frequency range 5735~5755Hz; • 153: main frequency band 5765Hz，frequency range 5755~5775Hz; • 157: main frequency band 5785Hz，frequency range 5775~5795Hz; • 161: main frequency band 5805Hz，frequency range 5795~5815Hz; • 165: main frequency band 5825Hz，frequency range 5815~5835Hz. Note: • In order to improve the network performance, please choose unused channel in the device working environment. • Different country opens different channels.
Bandwidth	Channel bandwidth of wireless network, it defaults to 80MHz, options as follows: • 20MHz; • 40MHz; • 80MHz.
Transmitting power	The wireless signal transmission power of device ranges from 1 to 1~30dBm. Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is. • Different device has different transmitting power range.
Max number of users	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.

Interface Description 3: Senior Configuration

The advanced interface is as follows:



The main element configuration description of advanced interface:

Interface Element	Note
Short protection interval	Short protection interval checkbox: • Check: enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed. • Uncheck: after disabling the function, the transmission interval of data packet defaults to 800ns. Note: Under high signal strength and low latency, this function can be enabled to improve nearly 10% handling capacity.
WDS	WDS (Wireless Distribution System), this function is used for bridging multiple WLAN. Note: Please enable WDS function while bridging the device and other wireless devices.
Wireless isolate	Wireless user isolation, it's used for isolating the wireless clients connected to the device wireless network with same SSID, defaults to disabled. Note: After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.
Fragment threshold	Fragment threshold of data packet, value range 256-2346, defaults to 2346. Note: • The data frame will be segmented when its length surpasses

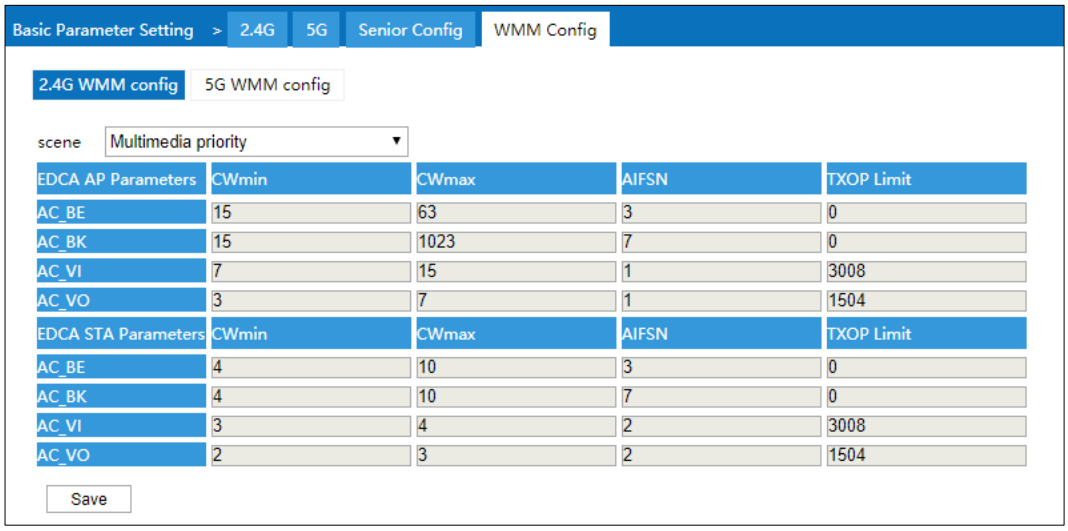
Interface Element	Note
	fragment threshold. • With large interference or high utilization ratio of wireless network, user can adopt smaller fragmentation threshold to increase the transmission reliability; but it is low efficiency. • The wireless network is easy to be interfered while adopting large fragment threshold; but it is high efficiency.
RTS	Data packet RTS (Request to Send) threshold, value range 0-2347, defaults to 2347. • RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will send RTS signal; • 0 < RTS threshold < 2347: when the length of data packet surpasses RTS threshold, the device wireless terminal will send RTS signal to avoid signal conflict; • RTS threshold = 2347: the device wireless terminal won't send RTS signal. Note: • As for the wireless nodes in different wireless detection range of AP range, collision will occur when the nodes send out signals; RTS function can avoid the collision. • The device will send RTS to destination station for negotiation when the length of data packet surpasses RTS threshold. After receiving RTS frame, the wireless station will send a CTS (Clear to Send) frame to response the device, which represents the two stations can conduct wireless communication.
Country	Applied countries and regions of wireless network, Options are as follows: • China • USA Note: Different country opens different channels.
Verification method	Authentication mode of wireless network, options as follows: • Personal edition: wireless network WPA/WPA2 uses WPA-PSK / WPA2-PSK encryption method and pre-shared key. Personal edition is suitable for personal and home users. • Enterprise edition: wireless network WPA/WPA2 uses WPA-802.1X/WPA2-802.1X encryption method. It is necessary to install Radius server to authenticate, and

Interface Element	Note
	suitable for enterprise users with high security requirements. Note: Verification mode can be configured after the wireless network is encrypted.
Radius Server IP	IP address of RADIUS (Remote Authentication Dial In User Service) sever. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.
Radius Server port	The authentication port number of the RADIUS server, value range is 0-65535. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.
RADIUS Shared secret key	Shared key of RADIUS server. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.

Interface Description 4: WMM Configuration

802.11 network provides wireless access services based on competition, but different application requirements have different requirements on the network, and the original network cannot provide access services of different quality for different applications, so it's unable to meet the needs of practical applications. IEEE 802.11e adds QoS features to WLAN system based on 802.11 protocol, which has been standardized for a long time. In this process, the Wi-Fi organization defines WMM (Wi-Fi Multimedia) standard in order to ensure interoperability between devices provided QoS by different WLAN vendors. The WMM standard enables WLAN networks to provide QoS services. WMM is a wireless QoS protocol, which is used to ensure that high-priority messages have the priority of sending, so as to ensure the better quality of voice, video and other applications in wireless networks.

WMM configuration interface is as follows:



Main elements configuration description of WMM configuration interface:

Interface Element	Discirption
WMM Configuration Tab	• 2.4G WMM Configuration • 5G WMM Configuration
Scene	WMM scene settings, options: • No priority; • Multimedia First; • User-defined. Note: • The default scenario is no priority. At this time, data stream and video voice stream have the same priority, and no one has the priority. • After selecting WMM function, the device can process the data packet with priority level, improving the data transmission performance of WMM and ensuring the service quality of voice, video and other services with high real-time requirements. • To select user-defined functions, users need to set their own parameters.
EDCA AP Parameters	WMM priority queue, options: • AC-BE (best effort streaming); • AC-BK (background streaming); • AC-VI (video streaming); • AC-VO (voice streaming).
CWmin	Minimum competition window, available values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767.
CWmax	Maximum competition window, available values: 1, 3, 7, 15,

Interface Element	Discirption
	31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767, and the value of maximum competition window must be larger than the value of the minimum competition window.
AIFSN	AIFSN, Arbitration Inter Frame Spacing Number WMM can configure different idle waiting time for different AC. The larger the value of AIFSN, the longer the idle waiting time of users will be. Value range: 1-255.
TXOP Limit	Transmission Opportunity Limit The maximum length of time the user can occupy the channel after a successful competition The larger this value is, the longer the user can occupy the channel at a time. If it is 0, only one message can be sent after occupying the channel at a time. The value of this parameter must be positive and modification is not recommended.
EDCA STA Parameters	The EDCA(Enhanced Distributed Channel Access) parameters of terminal device(namely workstation STA) supporting 802.11 standard, such as CWmin, CWmax, AIFSN, TXOP Limit.

4.2 Wireless Client Filtering

Function Description

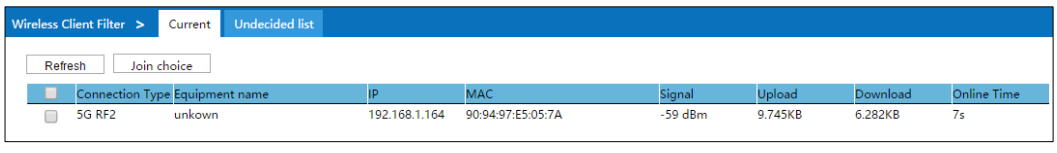
On the “Wireless Client Filtering” page, user can check current connecting devices and manage wireless user connection.

Operation Path

Please open in order: “WLAN Settings > Basic Parameter Settings”.

Interface Description 1: Current connected device

The interface of the current connected device is as follows:

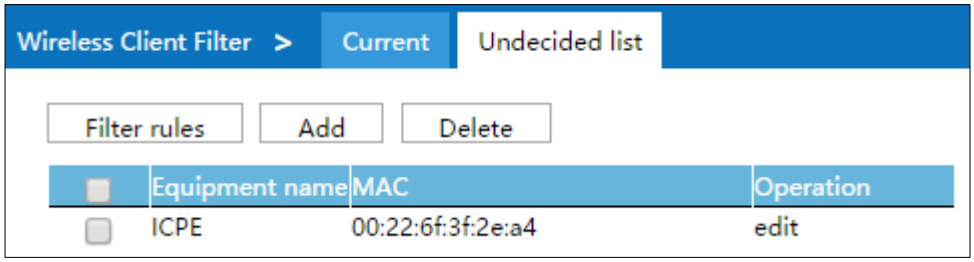


Configuration of the main elements of the current connected device interface:

Interface Element	Discription
Connection Type	The connection type of wireless client connected to this device currently.
Equipment name	The equipment name of wireless client connected to this device currently.
IP	The IP address of wireless client connected to this device currently.
MAC	The MAC address of wireless client connected to this device currently.
Signal	The signal strength of wireless client connected to this device currently. The unit is dBm, the larger the value, the stronger the signal.
Upload	The upload flow of wireless client connected to this device currently.
Download	The download flow of wireless client connected to this device currently.
Online Time	The online time of wireless client connected to this device currently.

Interface Description 2: Undecided List/Black List/White List

Undecided list interface as follows:



The main element configuration description of undecided list interface:

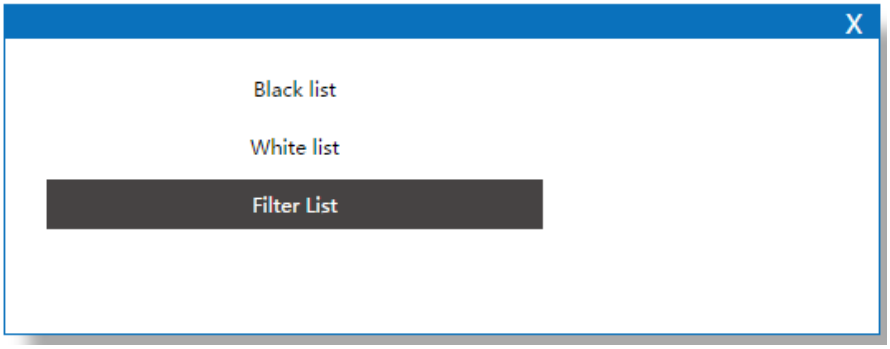
Interface Element	Discription
Device name	The device name of wireless client in filter list. Note: • Click “add” to add device to list manually. • Click “Filter rule” button, you can switch current list between black List, white List and undecided list, to filter wireless Client.
MAC	MAC address of wireless client in filter list.

Interface Element	Discription
Operation	Edit wireless client information.

Interface Description 3: Filter Rule

Click the “Filter Rule” button to switch lists.

The filter rules interface as follows:



The main element configuration description of filter rules:

Interface Element	Discription
Black List	The list of wireless client banned from visiting wireless device.
White List	The list of wireless client allowed to visit wireless device.
Filtered List	The pending list of wireless client visiting wireless device.

Note

Only the current list takes effect after switching the list via filter rules.

5 Advanced Network

5.1 Port Forward

The Port Forward function enables user to set public service on his own network, such as Web server, FTP server, E-mail server or other applications that run only through internet. When user sends those types of requests to your network via internet, the router would forward them to the corresponding client via port forward function.

Function Description

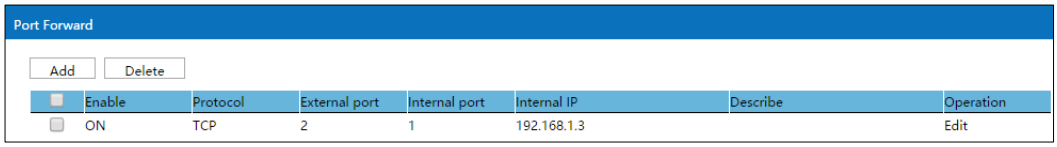
On the “Port Forward” page, user can check or add port forward entry. It allows outer network client to visit specified device via specified port.

Operation Path

Please open in order: "Advanced Network > Port Forward”

Interface Description

The port forward interface as follows:



The main element configuration description of port forward interface:

Interface Element	Discription
☐	The port forwarding entry checkbox, click to check all the port forward entries.
Enable	Enable port forward or not: • ON Status • OFF

Interface Element	Discription
Protocol	The protocol type used by port forward data package: • TCP • UDP. • TCP/UDP
External port	The external port number used by external network.
Internal port	The internal port number used by internal network.
Internal IP	The IP address of device specified by internal network
Describe	Remarks of port forward entries.
Operation	Edit: modify port forwarding entry information
Add	Click the “Add” button to add new port forwarding entry in the pop-up window of “Port Forwarding”.
Delete	Check the port forwarding information that needs to be deleted, then click “delete” button to delete it.

5.2 Port Redirection

Function Description

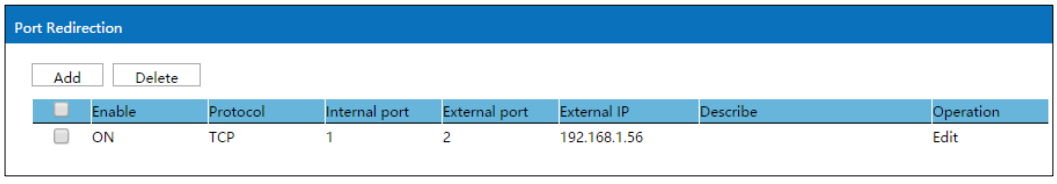
On the “Port Redirection” page, user can check or add port redirection entry, which allows client in LAN to visit the specified port of device with IP address specified by external network via specified port.

Operation Path

Please open in order: "Advanced Network > Port Redirection".

Interface Description

The port redirection interface as follows:



The main element configuration description of port redirection interface:

Interface Element	Discription
☐	The checkbox of port redirection entry. Click to check all port

Interface Element	Discription
	redirection entries
Enable	Enable port redirection or not: • ON Status • OFF
Protocol	The protocol type used by port redirection data package: • TCP • UDP. • TCP/UDP
Internal port	The internal port number used by internal network
External port	The external port number used by external network
External IP	The device IP address specified by external network
Describe	The remark information of port redirection entry
Operation	Edit: modify port redirection entry information
Add	Click the “add” button at the top right corner to add new port redirection in the pop-up window of “Port Redirection”
Delete	Check the port redirection information that needs to be deleted, then click “delete” button at the top right corner to delete it

5.3 DMZ Settings

DMZ(Demilitarized Zone） is a isolation area, it is a buffer built between non-safety system and safety system for solving the problem that visitor from external network cannot visit internal network server.

Function Description

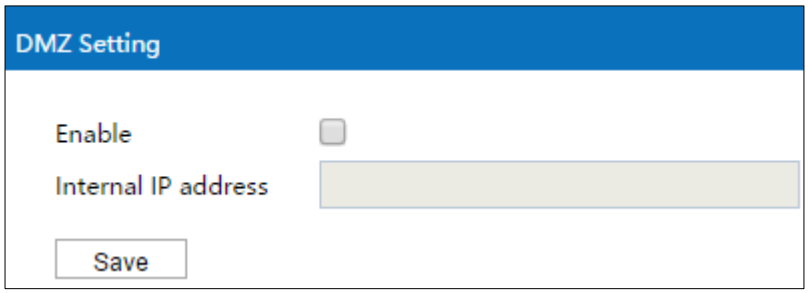
On the page of firewall “DMZ Settings”, user can enable or disable DMZ function. The client can visit the specified LAN client via WAN.

Operation Path

Please open in order: “Advanced Network > DMZ Setting”.

Interface Description

DMZ filter interface as follows:



The main element configuration description of DMZ setting interface:

Interface Element	Discription
Enable	DMZ Settings enable checkbox, check to enable DMZ settings function.
Internal IP address	The IP address of LAN client, for example: 192.168.1.123.

5.4 UPnP Settings

Universal Plug and Play (UPP) is a network structure used for common peer-to-peer network connection (P2P) of computers and smart devices (or instruments). Based on Internet standards and technologies (such as TCP/IP, HTTP and XML), UPnP enables devices to automatically connect and work with each other.

When the router enables UPnP function, if the software on the user's computer also supports UPnP protocol, the router will open the corresponding virtual server port according to the requirements of user software. Based on the UPnP protocol, hosts on the LAN can request routers to perform specific ports translation, allowing external hosts to access resources on internal hosts when needed. Devices that support UPnP can be automatically discovered by the UPnP service application on the LAN. UPnP also allows supported devices to automatically leave the network without negatively impacting the device itself or other devices on the network.

Function Description

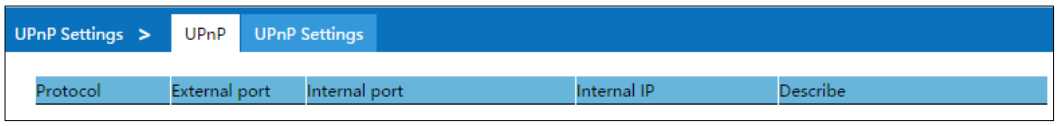
On the page of "UPnP Settings", user can view internal ports translation information and configure UPnP parameters.

Operation Path

Open in order: "Advanced Network > UPnP Settings".

Interface Description 1: UPnP

UPnP settings interface as follows:

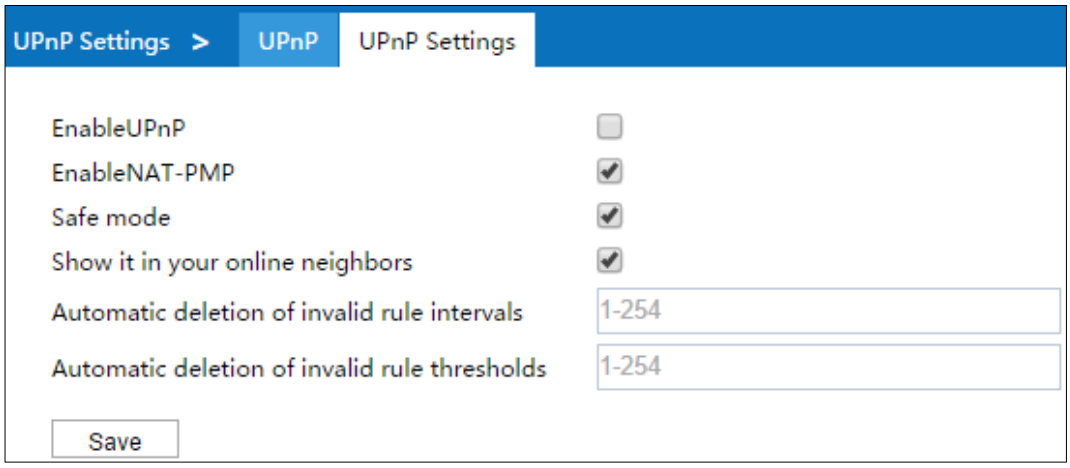


The main elements configuration description of UPnP settings interface:

Interface Element	Discription
Protocol	The type of protocol that adopts UPnP port translation, such as TCP or DUP.
External port	The router port number used for port translation is the external port number.
Internal port	The port number of local LAN host that needs to be converted.
Internal IP	The IP address of local LAN host that needs to be converted.
Describe	The description of the application when it requests port translation from the router via UPnP.

Interface description 2: UPnP settings

UPnP settings interface as follows:



The main element configuration description of UPnP settings interface:

Interface Element	Discription
Enable UPnP	UPnP enable checkbox, check to enable UPnP function.
Enable NET-PMP	The NET-PMP function enable checkbox, check to enable NET-PMP function, and the router will allow the LAN host to communicate with external devices to automate port

Interface Element	Discription
	conversion.
Safe Mode	Safe mode enable checkbox, after the safe mode is enabled, the client can only forward an input port to itself.
Show it in your online neighbors	Show the enable check box in Online neighbors, after checked, the device can be found in the PC Online neighbors or network devices.
Automatic deletion of invalid rule intervals	The system automatically deletes the invalid UPnP rules list after the specified interval, unit: second.
Automatic deletion of invalid rule thresholds	The system automatically deletes the invalid UPnP rules list after the quantity of invalid UPnP rules reaches the threshold.

5.5 Multicast NAT

Function Description

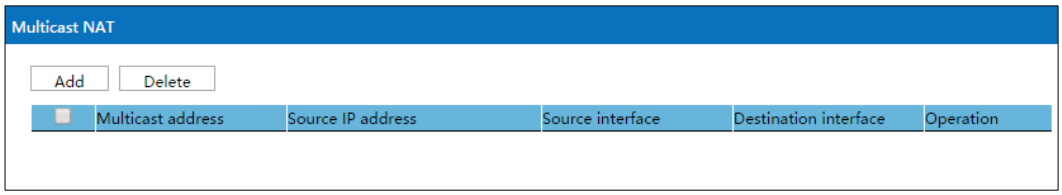
On the "Multicast NAT" page, you can configure specified multicast transparent transmitting between various network.

Operation Path

Open in order: "Advanced Network > Multicast NAT".

Interface Description

Multicast NAT interface as follows:



The main element configuration description of multicast NAT interface:

Interface Element	Discription
Multicast address	Destination IPv4 address of multicast. Note:

Interface Element	Discription
	The multicast address range is 224.0.0.0~239.255.255.255, addresses in different ranges have different functions.
Source IP address	Source IPv4 address of multicast
Source Interface	The device interface to receive multicast data, such as lan, wan or modem.
Destination interface	The device interface to send multicast data, such as lan, wan or modem.
Operation	Click “Edit” button to modify the information of current entry.

5.6 VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. In general, all hosts in a network will set a default route, when the destination address of the message sent by host isn't in the network segment; the message will be sent to the Router A via default router, achieving the communication between the host and external network. When the Router A breaks down, all hosts that takes Router A as default router in the network segment will disconnect communication to the outside, generating single point of failure. VRRP is proposed to solve the problem above, and it's designed for the local area network (such as: Ethernet) with multicast or broadcast capability.

VRRP organizes a set of routers (including a Master, that is the active router and several Backup, that is the standby router) in the local area network into a virtual router, which is called a backup team. The virtual router possesses its own IP address 10.100.10.1 (The IP address can be same to a router interface address in the backup team, it's called IP owner), routers in the backup team have their own IP address (such as IP address of Master is 10.100.10.2, IP address of Backup is 10.100.10.3). Hosts in the local area network only knows the virtual router IP address is 10.100.10.1, it doesn't know that the specific Master router IP address is 10.100.10.2 and Backup router IP address is 10.100.10.3. Hosts set their own default router next hop address to the virtual router IP address 10.100.10.1. Thereupon, hosts in the network start to communicate with other networks via the virtual router. If the Master router in backup team breaks down, Backup router will elect a new Master router via election strategy and provide router service for hosts in the network. Therefore, hosts in the network can uninterruptedly communicate with outside network.

Principle of realization

A VRRP router has the only identification: VRID, range is 0-255. The router has only one virtual MAC address, and the address format is 00-00-5E-00-01-[VRID]. Master router is responsible for replying the ARP request by MAC address. Regardless of the switching, it's ensured to give the only consistent IP and MAC address to the terminal device, declining the switching influence to terminal device.

VRRP control message includes only one type: VRRP announce (advertisement). It's packaged by IP multicast data packet, the multicast address is 224.0.0.18, issue range can be only in the same local area network. It has ensured that VRID can be repeatedly used in different network. In order to decrease the network bandwidth consumption, only the master router can periodically send VRRP announce message. Backup router will start new VRRP election if it can't receive VRRP in three consecutive announce intervals or receives announce with 0 priority.

In the VRRP router group, the master router is elected by priority. The priority range in VRRP protocol is 0-255. If VRRP router IP address is the same to virtual router interface IP address, then the virtual router is called IP address owner in VRRP group; IP address owner automatically has the highest priority: 255. Priority 0 is usually used when IP address owner forwardly gives up the master role. Configurable priority range is 1-254. Priority configuration principle is set according to the link speed and cost, router performance and reliability, and other management strategies. In the election of master router, virtual router with high priority wins; therefore, if there exists IP address owner in VRRP group, it will appear as the master router. Candidate router with the same priority can be elected according to IP address size order. VRRP has also provided priority preemption strategy, if the strategy is configured, backup router with high priority will deprive current master router with low priority and become the new master router.

Function Description

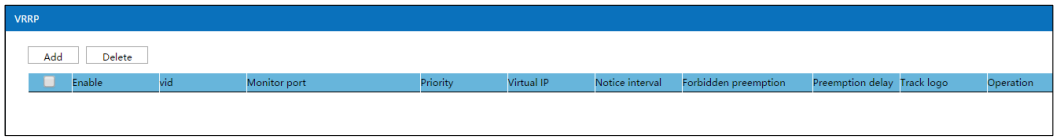
On the "VRRP Configuration" page, user can configure VRRP parameters.

Operation Path

Open in order: "Advanced Network > VRRP".

Interface Description

The VRRP interface as follows:



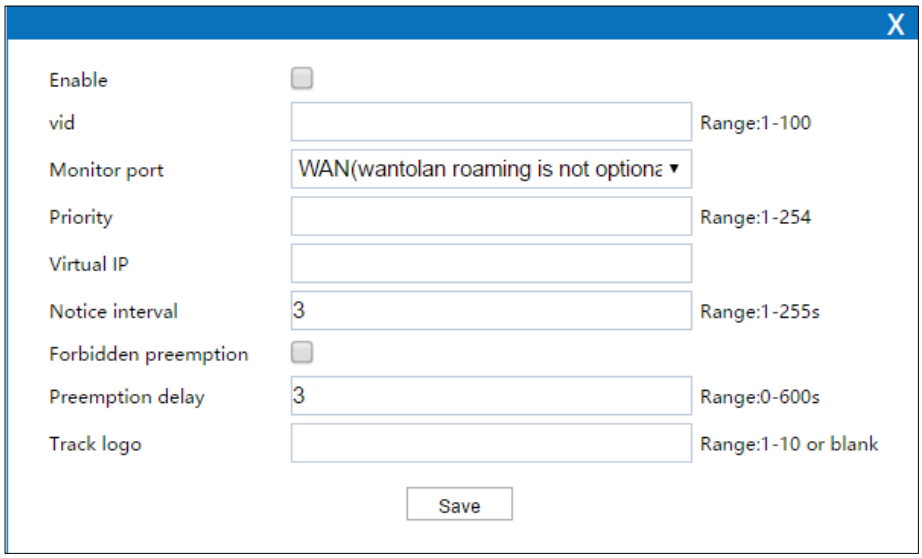
The main elements configuration description of VRRP interface:

Interface Element	Discription
Enable	VRRP function status is displayed, options include: • ON Status • OFF
Vid	Identity of the virtual router is displayed.
Monitor port	Monitor ports of the device is displayed, options include: • LAN • WAN
Priority	Priority of the device. The priority is used for the election of Master device. The greater the value, the higher the priority.
Virtual IP	The IP address of the virtual router is displayed.
Notice interval	Interval at which Master device sends VRRP notice messages, unit: second.
Forbidden preemption	Status display of forbidden preemption, options include: • ON Status • OFF
Preempt Delay	The delay time of switching from Backup device to Master device.
Track logo	Trace and probe Track ID.
Operation	Edit the VRRP entry.

Interface Description: VRRP-Add

Click the "Add" button to add virtual route.

The VRRP-Add interface as follows:



The main elements configuration description of VRRP-Add interface:

Interface Element	Discription
Enable	VRRP enable check box, check it to enable the VRRP function.
Vid	Identity of the virtual router, the valid range is 1-100. Virtual routers consisting of one master device and multiple backup devices have the same identity.
Monitor port	Drop-down list of VRRP monitor port, options as follows: • LAN: LAN port as the listening port; • WAN: WAN port as the listening port.
Priority	Priority of the device. The priority is used for the election of Master device. The greater the value, the higher the priority. The more likely it is to become Master device; the valid range is 1-254.
Virtual IP	IP address of the virtual router, such as 192.168.1.1. A virtual router can have one or more IP addresses.
Notice interval	Annunciate time interval, valid range is 1-600 seconds. Master device periodically sends VRRP notice messages to announce its operating status.
Forbidden preemption	Disable preemption check box of VRRP, check it to disable preemption. • Non-preemptive mode. When the priority of Backup device is higher than the one of Master device, Backup device won't become the Master device;

Interface Element	Discription
	• Preemptive mode. When the priority of Backup device is higher than the one of Master device, Backup device will actively switch to Master device.
Preemption delay	The delay time of switching from Backup device to Master device, the valid range is 1-600 seconds. Note: If the preemption delay time is too short, the device status will be frequently switched; so increasing the preemption delay time can effectively solve this problem.
Track logo	Trace and probe Track ID, the ID range is 1-10, optional.

5.7 RIP

RIP (Routing Information Protocol) is a simple Interior Gateway Protocol (IGP) and mainly used in small network, such as Campus Network and Local Area Network with simple structure. RIP isn't used in more complex environment and large network.

RIP is simple to achieve and easier in configuration and maintenance than OSPF or IS-IS, so it's widely used in actual networking.

Function Description

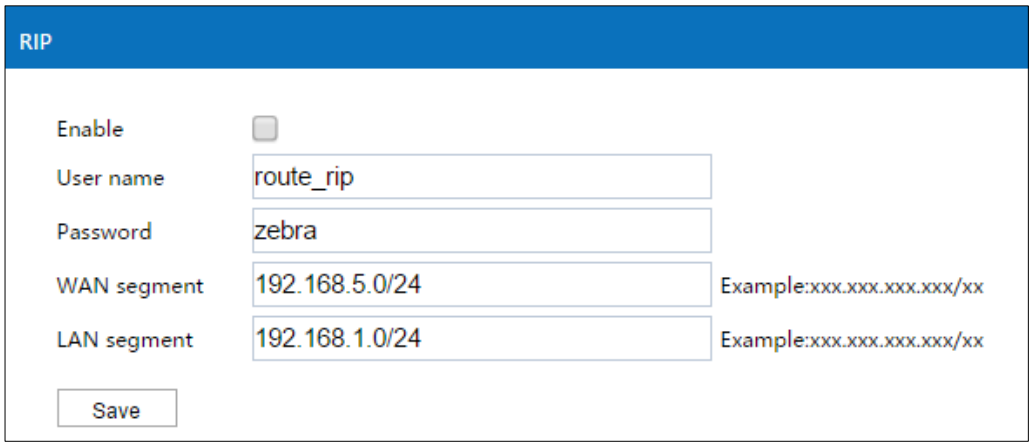
On the page of "RIP", user can configure the RI related parameters.

Operation Path

Open in order: "Advanced Network > RIP".

Interface Description

The RIP interface as follows:



The main elements configuration description of RIP interface:

Interface Element	Discription
Enable	RIP Enable checkbox, check to enable the RIP default configuration.
Username	User name used to log in to the RIP command line configuration.
Password	Password used to log in to the RIP command line configuration.
WAN segment	WAN segment information.
LAN segment	LAN segment information.

5.8 OSPF

OSPF (Open Shortest Path First), its characteristics include:

- It's a kind of routing protocol of link status and adopts the metric value based on bandwidth;
- It adopts SPF algorithm to calculate the route, and the SPF algorithm can avoid routing loop.
- Maintain routes through neighbor relationship to avoid the consumption of bandwidth by regular updates;
- The routing update is efficient with fast network convergence, which is suitable for large and medium-sized networks.

Function Description

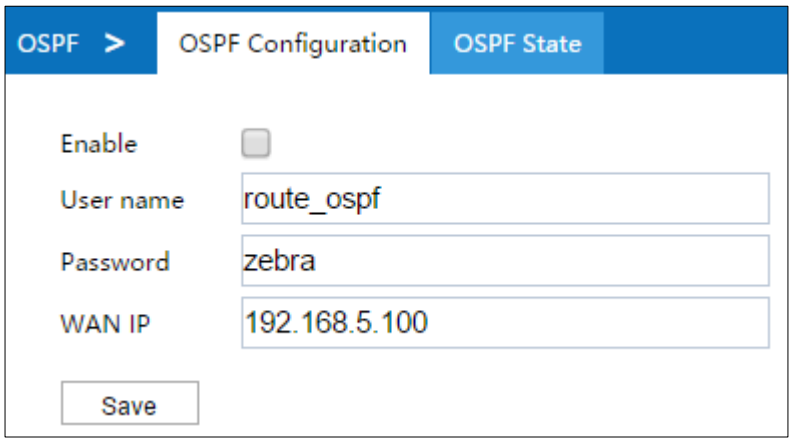
On the page of "OSPF", user can configure the OSPF parameters.

Operation Path

Open in order: "Advanced Network > OSPF".

Interface Description 1: OSPF Configuration

OSPF configuration interface is as follows:

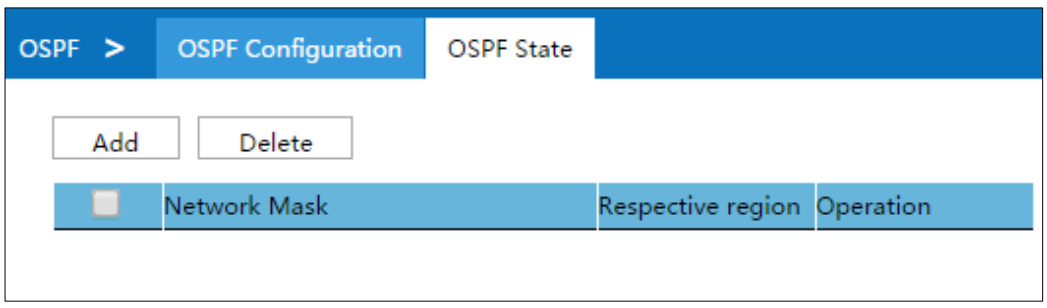


Main elements configuration description of OSPF configuration interface:

Interface Element	Discription
Enable	OSPF enable checkbox, check to enable OSPF protocol.
Username	User name used to log in to the OSPF command line configuration.
Password	Password used to log in to the OSPF command line configuration.
WAN IP	The router ID number, similar to the IP address format, is the unique identification of router in the autonomous system.

Interface Description 2: OSPF State

OSPF State interface as follow:

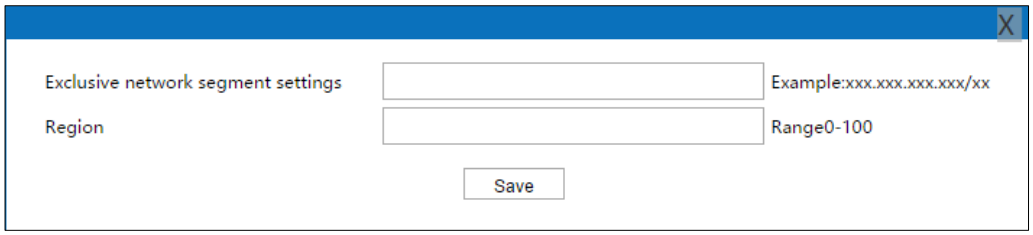


The main elements configuration description of OSPF State interface:

Interface Element	Discription
Network mask	The network segment where the IP address of interface running OSPF protocol is located. A network segment can only belong to one area.
Respective region	The area number of the device. OSPF protocol divides the autonomous system into different areas.
Operation	Edit the OSPF network segment and region information.

Interface Description 2-1: OSPF State-Add

The OSPF State-Add interface as follows:



The main elements configuration description of OSPF State-Add interface:

Interface Element	Discription
Exclusive network segment settings	The network segment where the IP address of interface running OSPF protocol is located. A network segment can only belong to one area, such as 10.1.1.1/24.
Region	The area number of the device. OSPF protocol divides the autonomous system into different areas, the valid range is 0-4294967295.

5.9 Static DHCP

Function Description

On the page of "Static DHCP", user can add, delete, and view the configuration information of static clients. Bind the client's MAC address to the specified IP address

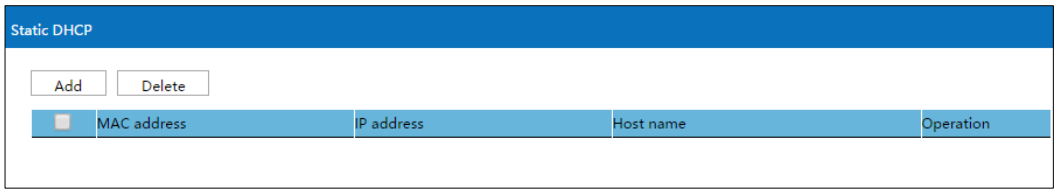
to ensure that the address that the client obtains from the server each time is the binding IP address.

Operation Path

Open in order: "Advanced Network > Static DHCP".

Interface Description

Static DHCP interface as follows:

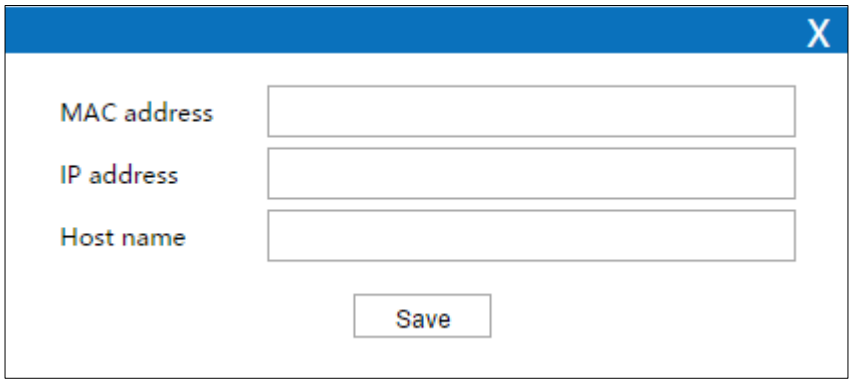


The main elements configuration description of static DHCP interface:

Interface Element	Discription
MAC address	MAC address of DHCP client.
IP Address	IP address bound to the MAC address of DHCP client.
Host name	The name of DHCP client.
Operation	Edit the static DHCP list.

Interface Description: Static DHCP - Add

Static DHCP-Add interface as follows:



The main elements configuration description of static DHCP-Add interface:

Interface Element	Discription
MAC address	MAC address of the DHCP client, the format is

Interface Element	Discription
	XX:XX:XX:XX:XX:XX.
IP Address	IP address bound to the MAC address of DHCP client, such as 192.168.1.1.
Host name	Name or remarks of the DHCP client.

5.10 DHCP Client

Function Description

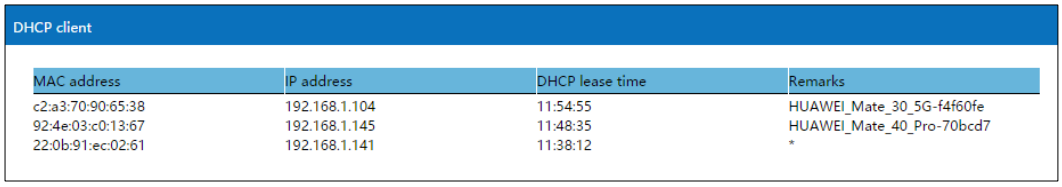
On the “DHCP Client" page, user can view the information of DHCP clients that have obtained valid leases from devices.

Operation Path

Open in order: "Advanced Network > DHCP Client".

Interface Description

The DHCP client settings interface is as follows:



Interface Element	Discription
MAC address	MAC address of DHCP client.
IP Address	IP address of DHCP client.
DHCP lease time	Valid lease of DHCP client.
Remarks	Name or remarks of the DHCP client.

5.11 QoS

Function Description

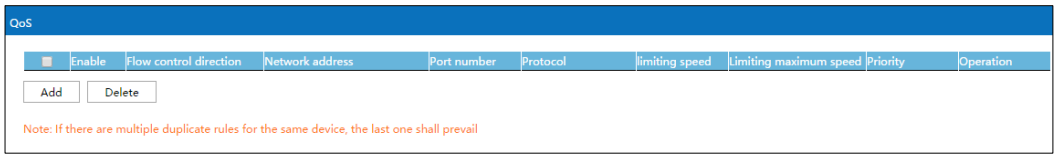
On the “QoS” page, users can configure QoS policy to limit the rate and priority of specified IP data.

Operation Path

Open in order: "Advanced Network> QoS".

Interface Description

The QoS Strategy interface as follows:



The main element configuration description of QoS classification interface:

Interface Element	Discription
Enable	Enable QoS strategy or not.
Flow Control Direction	Flow control direction, such as upload and download.
Network address	Source IP address and subnet mask of the packet.
Port number	Corresponding network port number of the network address.
Protocol	Protocols used by IP data scheduling. • TCP • UDP. • BOTH
Limiting speed	Limit average rate value, the value range of the threshold is 1-1000000bps.
Limiting maximum speed	The maximum Limit rate value, the value range is 1-1000000bps.
Priority	The priority of IP data scheduling, a smaller value indicates a higher priority. The value range is 0-10.
Operation	Click "Edit" button to modify this QoS strategy.

6 CAN Settings

Function Description

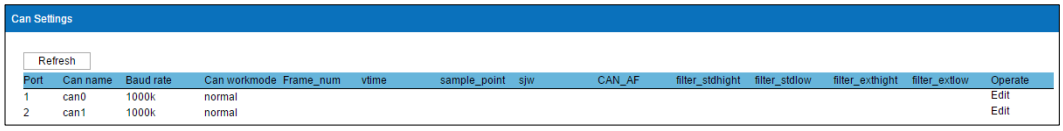
Users can check and configure baud rate, woke mode, subcontract frame number, CAN frame limit and other parameters of each CAN port of the device on “CAN Settings“ page.

Operation Path

Open: "CAN Settings”.

Interface Description

CAN settings interface as follows:



The main element configuration description of CAN settings interface:

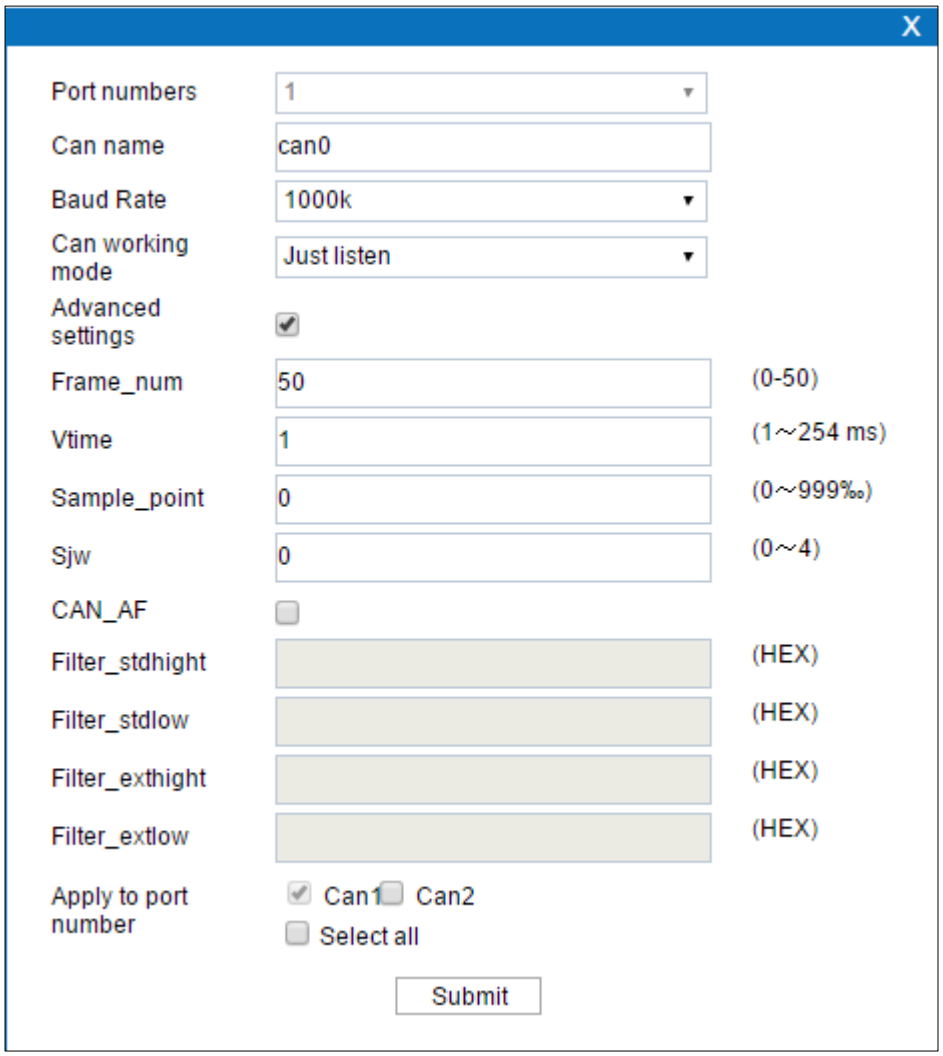
Interface Element	Discription
Port	Display the CAN port number of the device.
CAN name	Displays the name of the device’s CAN port.
Baud Rate	Display the baud rate of the device’s CAN port.
Can Workmode	Display the work mode of the device‘s CAN port. • Normal: the device is in normal operating status. • Just Listen: CAN server is in interception status and can't send data. • Self Test: the device is in the self-transmitting and receiving operation status.
Frame_num	Display the number of CAN frames received when the device

Interface Element	Discription
	CAN port encapsulates Ethernet packets.
vtime	Display the time interval of CAN frames received when the device CAN port encapsulates Ethernet packets.
Sample point	Display the value of sampling point of the device's CAN port, unit is "‰".
sjw	Display the resynchronized jump width of the device's CAN port.
CAN_AF	Display acceptance and filtering status of the device's CAN port. • Enable • Disable
Filter_stdhight	Display the upper limit of standard frame received by the device's CAN port.
Filter_stdlow	Display the lower limit of standard frame received by the device's CAN port.
Filter_exthight	Display the upper limit of extended frame received by the device's CAN port.
Filter_extlow	Display the lower limit of extended frame received by the device's CAN port.
Operate	Click "Edit" to modify the parameters of corresponding CAN port.

Click "Edit" in the CAN entry to modify the current CAN port parameters.

Interface Description: Edit

Edit interface is as follows:



Configuration description of main elements of the Edit interface:

Interface Element	Discription
Port numbers	The port number of the device's CAN port edited currently.
CAN name	Set the name of the device's CAN port which supports up to 1-32 letters or numbers.
Baud Rate	CAN baud rate drop-down list, options as follows: 5K/10K/20K/50K/100K/125K/250K/500K/800K/1000K
Can Working Mode	The drop-down list of CAN work mode, the options are as follows: • Normal: the device is in normal operating status. • Listening: the device is in interception status and can't send data. • Self Test: the device is in the self-transmitting and receiving operation status.

Interface Element	Discription
Advanced Settings	Advanced Settings Check box, click to configure more function parameters.
Frame_num	When the CAN port continuously receives data and the received CAN frame number reaches "Frame Number", the received data is packaged as an Ethernet packet and sent out, settable value is 0-50.
vtime	When the CAN port doesn't receive the new data frame within defined time of "Frame Wait Time", the received data that hasn't been sent out is packaged to an Ethernet packet sent to the Ethernet port, settable value is 1-254ms.
Sample point	Sampling point is the sample of bus state at the end of phase buffer section 1 when the bus level is read and converted into the corresponding bit value. The desired value is the percentage of the time from the beginning of a bit to the sampling point to the total time of a complete bit, which ranges from "0-999‰". Note: When there is a phase difference on the bus, you can adjust the sampling point for resynchronization.
sjw	SJW (reSynchronization Jump Width) specifies the upper limit of the extension or shortening of the phase buffer section. The value ranges from 1 to 4.
CAN_AF	CAN_AF check box, click to enable CAN port acceptance and filtering function. After enabled, the data will be eliminated if the standard frame and the extended frame ID received by CAN port are not in the restricted range.
Filter_stdhight	The upper limit of standard frame received by the device's CAN port, which is hexadecimal and the valid value range is 000-7FF.
Filter_stdlow	The lower limit of standard frame received by the device's CAN port, which is hexadecimal and the valid value range is 000-7FF.
Filter_exthight	The upper limit of extended frame received by the device's CAN port, which is hexadecimal and the valid value range is 00000000-1FFFFFFF.
Filter_stdlow	The lower limit of extended frame received by the device's CAN port, which is hexadecimal and the valid value range is

Interface Element	Discription
	00000000-1FFFFFFF.
Apply to the port number	Check the CAN port check box to apply the current settings to the specified CAN port.

7 CAN Mode

Function Description

Configure the work mode of corresponding device CAN port on "CAN Mode Settings" page.

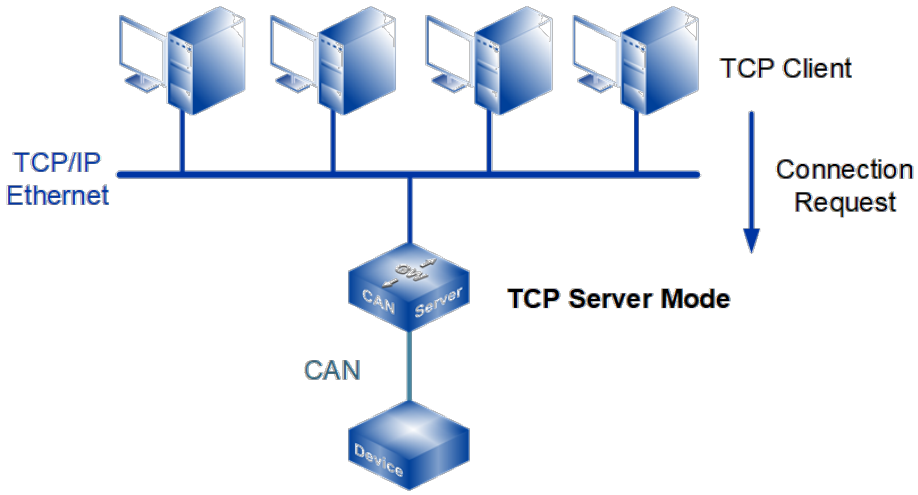
The working modes supported by the device are:

- CAN TCP Server Mode
- CAN TCP Client Mode
- CAN UDP Server Mode
- CAN UDP Client Mode
- CAN UDP Rang Client Mode
- CAN UDP Muliticast Mode

Operation Path

Open in order “CAN Mode > CAN1”. Under the menu of "CAN Mode", the corresponding CAN port information can be configured by entering different CAN ports. The configuration operation mode of all CAN ports' WEB interfaces is the same.

7.1 TCP Server Mode



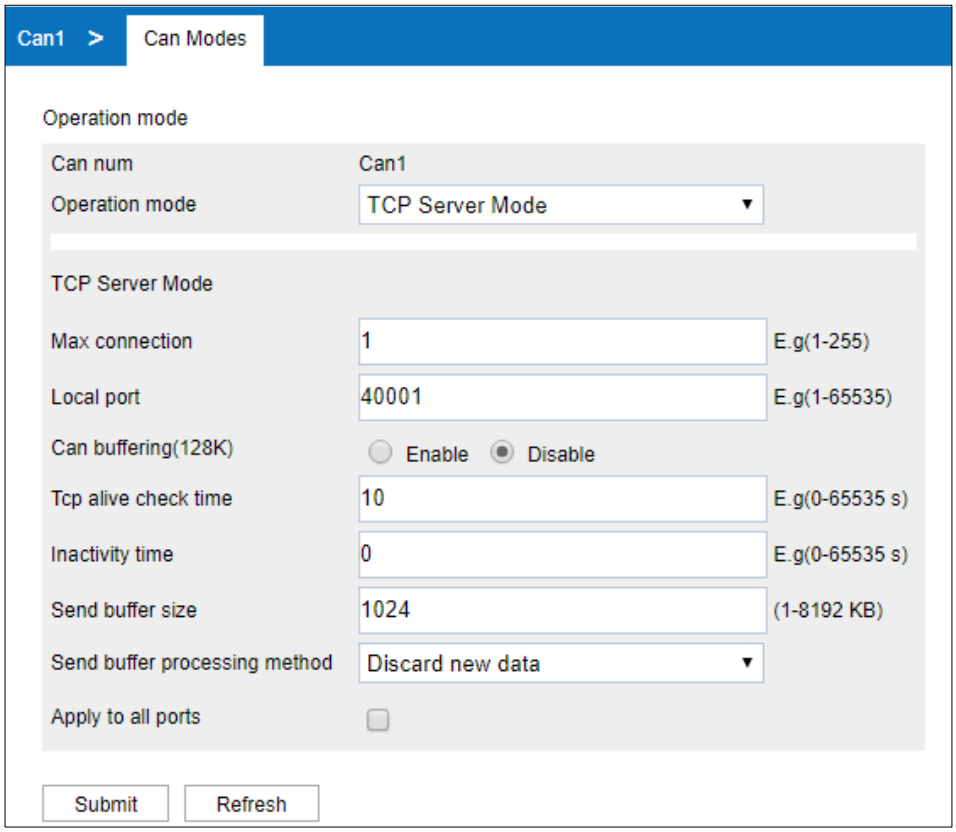
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or interface type is subject to the device obtained.

In CAN TCP server mode, the device is assigned an IP port number and passively waits for the host to connect. After the host initiates connection request and establish connection to the device, the host can realize the data transmission via network connection and CAN port. CAN TCP Server Mode supports multiple session connection at the same time, so that multiple hosts can read or send Ethernet data to a CAN port device at the same time.

Interface Description

TCP server mode interface is as follows:

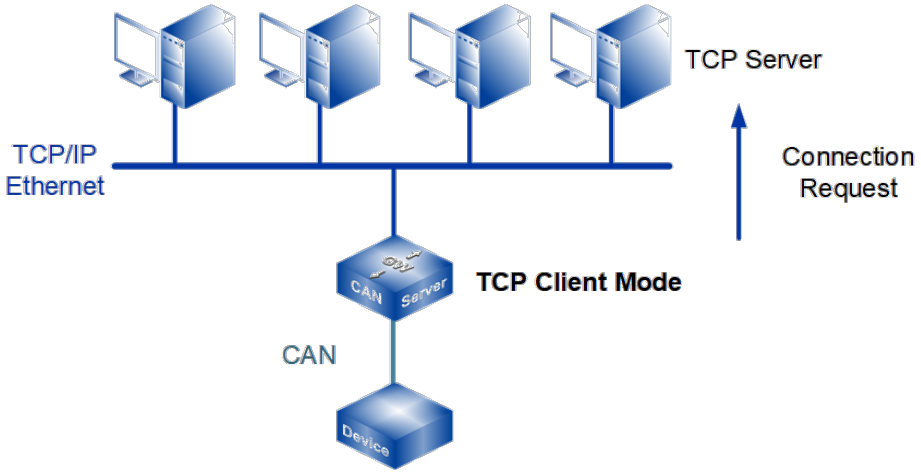


The main element configuration description of TCP Server Mode interface:

Interface Element	Discription
Working mode	**Working Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The working modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
TCP Server Mode	**TCP Server Mode Configuration bar**
Max connection	The maximum session number supported by the device's CAN port. Note: Session refers to the process the device transmits data received from CAN port to Ethernet via socket connection. More than one session number represents the device transmits the data received from CAN port to Ethernet via more than one socket.
Local port	Local port of the device, effective range is 1-65535. Note:

Interface Element	Discription
	TCP port provided by the device that can be connected by other TCP/IP nodes, which is associated with the corresponding CAN port of the device.
CAN buffering (128k)	Port data cache, which can cache CAN port data up to 128K after the network is abnormal. When the network returns to normal, the cached data is forwarded. Options are as follows: • Enable; • Disable.
TCP Alive check Time	If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If the reply packet of opposite side hasn't been received after sending probe packet for 3 times, system will regard the opposite side as down and forwardly close the communication connection. If set TCP Alive Time to "0", the function will be disabled. Effective time range 0~65535s.
Inactivity time	The idle time of device's communication link, valid time range 0~65535s. • TCP Timeout > 0: If there is no data communication between the server and client, the server and client will break connection. • TCP Timeout = 0: When there is no data communication between the server and client, the server and client will keep in connection status.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

7.2 TCP Client Mode



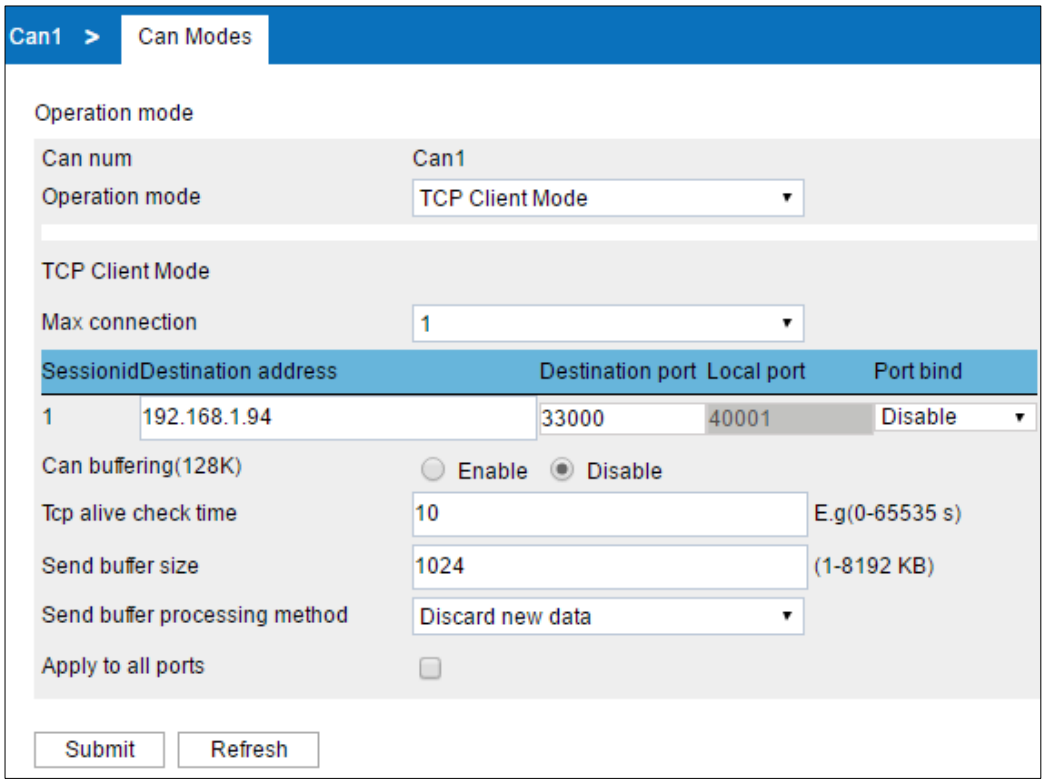
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or interface type is subject to the device obtained.

In CAN TCP client mode, the device can actively establish a network connection with the host specified by the user when the CAN port data arrives. After the data transmission is completed, the device will automatically close the network connection according to TCP keep-alive time/idle timeout and other parameters. CAN TCP Client Mode supports multiple session connection at the same time, so that multiple hosts can read or send Ethernet data to a CAN port device at the same time.

Interface Description

TCP Client mode interface is as follows:

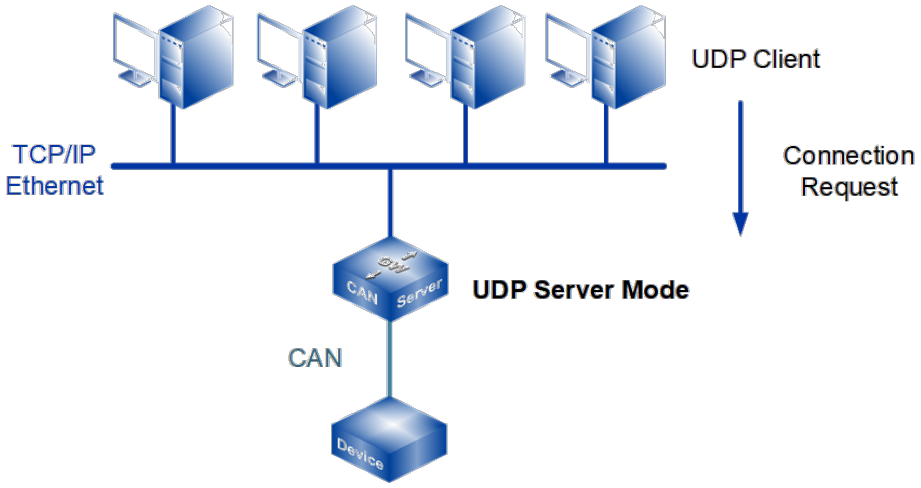


TCP client mode interface main element configuration instructions:

Interface Element	Discription
Working mode	**Working Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The working modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
TCP Client Mode	**TCP Client Mode Configuration Bar**
Max connection	The session number of the device's CAN port. Note: Session refers to the process the device transmits data received from CAN port to Ethernet via socket connection. More than one session number represents the device transmits the data received from CAN port to Ethernet via more than one socket.
Destination address	The IP address of the server to which the device needs to connect.
Destination port	Enter the TCP port number of the server to which the device needs to connect.

Interface Element	Discription
Local port	A local port number assigned by the device for TCP connection, which can provide service or connection to the outside world, is used to connect and communicate with the server.
Port bind	Local port fixed, options are as follows: • Disable: the system automatically selects the idle local port to establish a connection with the server; • Enable: connect to the server using a manually configured local port.
CAN buffering (128k)	Port data cache, which can cache CAN port data up to 128K after the network is abnormal. When the network returns to normal, the cached data is forwarded. Options are as follows: • Enable; • Disable.
TCP Alive check Time	If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If the reply packet of opposite side hasn't been received after sending probe packet for 3 times, system will regard the opposite side as down and forwardly close the communication connection. If set TCP Alive Time to "0", the function will be disabled. Effective time range 0~65535s.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

7.3 UDP Server Mode



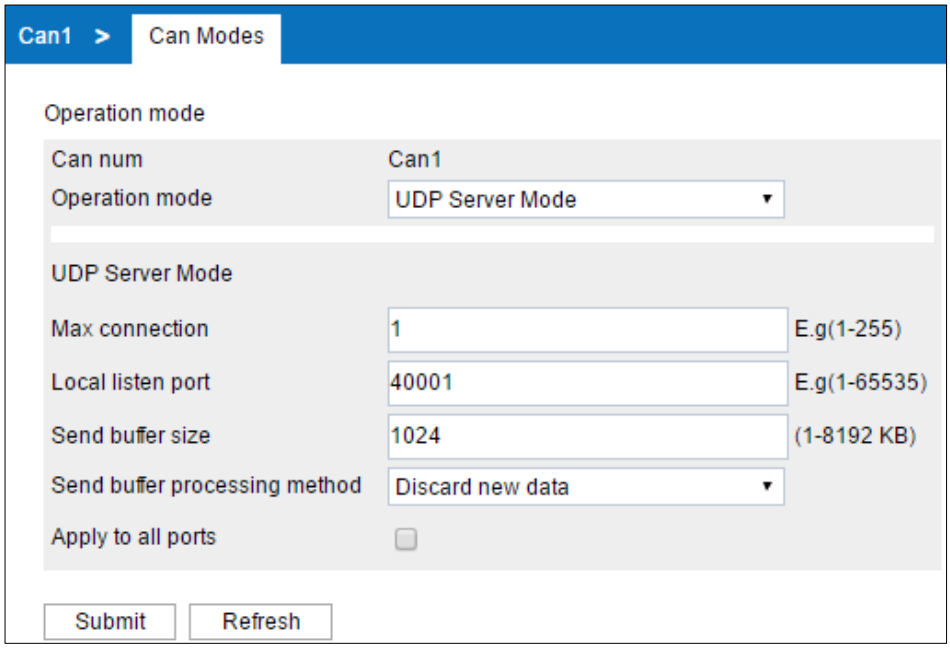
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or interface type is subject to the device obtained.

Under CAN UDP Server Mode, the device can be a server, and it can transmit data with the host user appointed under the UDP protocol. Under CAN UDP Server Mode, the device can transmit the data from CAN device to one or multiple hosts, and CAN device can also receive the data from one or multiple hosts.

Interface Description

TCP Server Mode interface is as follows:

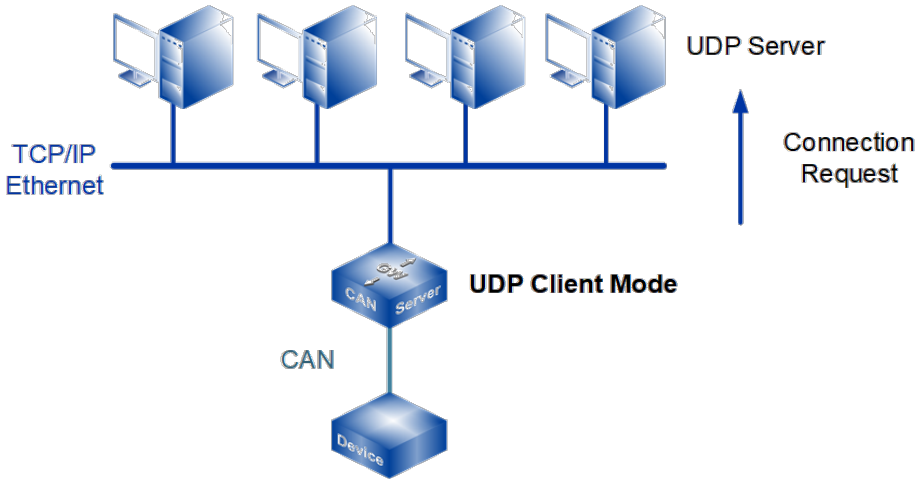


UDP Server Mode interface main element configuration instructions

Interface Element	Discription
Working mode	**Working Mode Configuration Bar**
CAN number	Displays the CAN number of the device currently configured.
Operation mode	The working modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Server Mode	**TCP Server Mode Configuration Bar**
Max connection	The maximum session number supported by the device's CAN port.
Local Listen port	The device is used as the listening port of UDP server for receiving UDP data. Note: User must allot the only listening port to each CAN port, then the system can normally receive UDP data.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer	When sending cache data overflows, the data can be

Interface Element	Discription
processing method	processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

7.4 UDP Client Mode



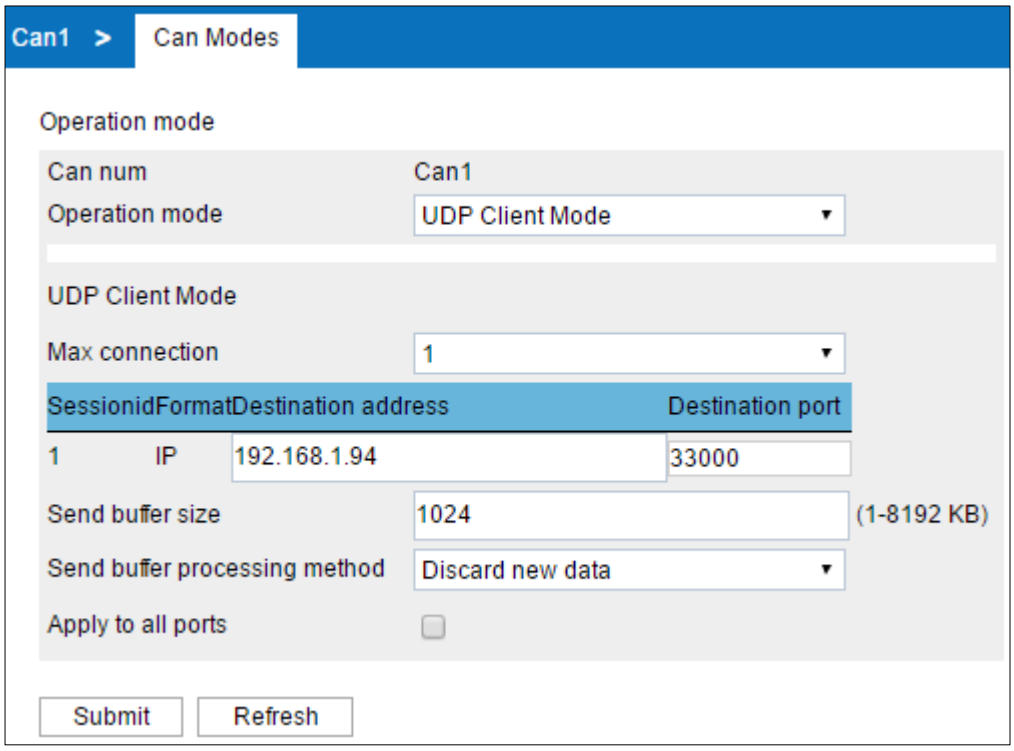
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or interface type is subject to the device obtained.

Under CAN UDP Client Mode, the device can be a client, and it can transmit data with the host user appointed under the UDP protocol. Under CAN UDP Client Mode, the device can transmit the data from CAN device to one or multiple hosts, and CAN device can also receive the data from one or multiple hosts.

Interface Description

UDP Client Mode interface is as follows:

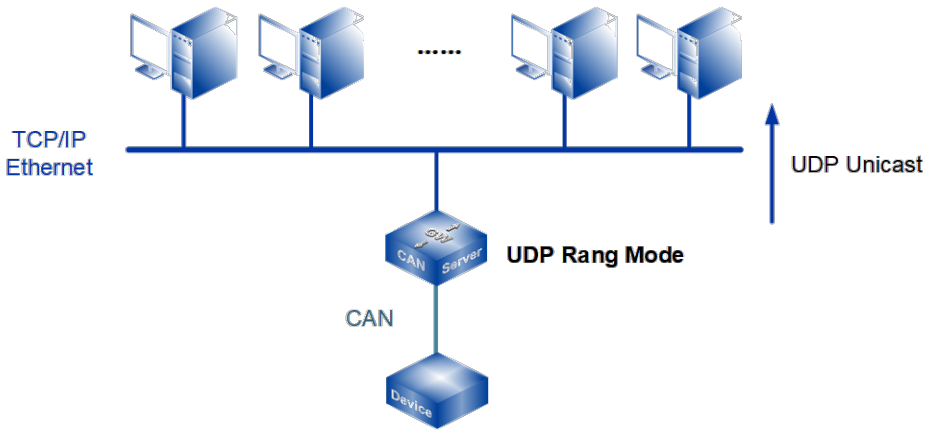


UDP Client Mode interface main element configuration instructions:

Interface Element	Discription
Working mode	**Working Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The working modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Client Mode	**UDP Client Mode Configuration Bar**
Max connection	The maximum session number supported by the device's CAN port.
Format	The Server address format that CAN as the UDP client needs to connect: • IP: IP address format, eg. 192.168.1.254;
Destination address	Enter the IP address of the server to which the device needs to connect.
Destination port	The listening port number of the server that the device need

Interface Element	Discription
	for session.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

7.5 UDP Rang Mode



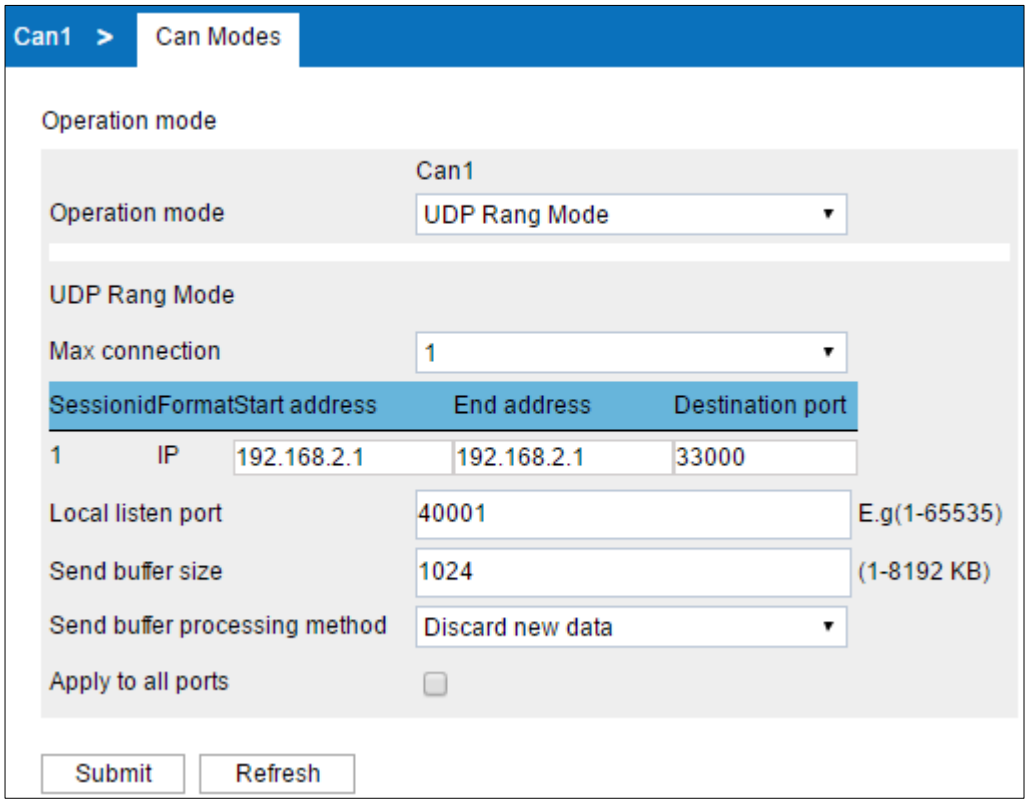
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or interface type is subject to the device obtained.

When the router, switch and other devices do not support multicast function, the device can realize the multicast function under the CAN UDP Rang Mode. In this mode, the device transmits data with multiple hosts in the same network segment designated by the user through UDP protocol, to achieve point to multipoint data communication. Under CAN UDP Rang Mode, CAN device can receive the data from one or multiple hosts.

Interface Description

UDP Rang Mode interface as follows:



UDP Rang Mode interface main element configuration instructions:

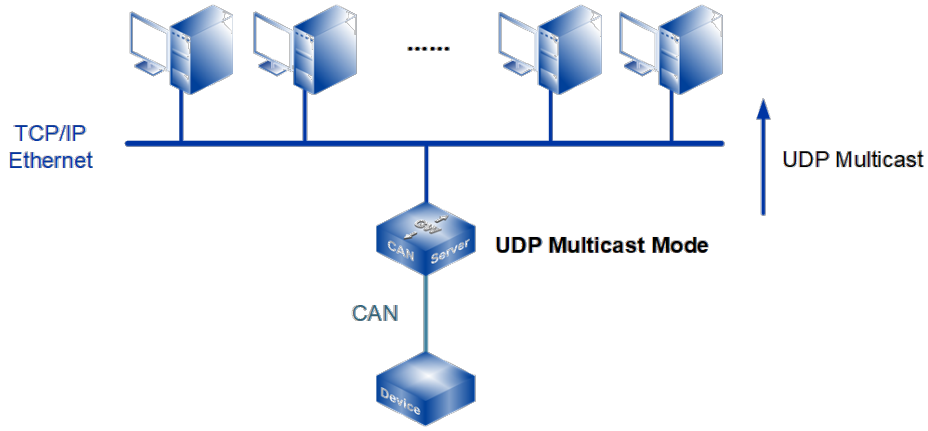
Interface Element	Discription
Operation mode	**Working Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The working modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Rang Mode	**UDP Rang Mode Configuration Bar**
Max connection	The maximum session number supported by the device's CAN port, options include: • 1/2/3/4
Format	The format of UDP Rang address.

Interface Element	Discription
Start Address	Start IP address of UDP Rang destination address.
End address	End IP address of UDP Rang destination address.
Destination port	The listening port number of the server that the device need for session.
Local Listen port	The listening port of the device to receive UDP data Note: User must allot the only listening port to each CAN port, then the system can normally receive UDP data.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

 Notice

- Rang address only supports IP addresses of Class B and Class C. The start address value and end address value of the Rang address need to be the same network segment.
- The start value of Rang address must be less than or equal to the end address value.
- In order to ensure the normal operation of communication, the rang address range needs to be small as much as possible because each IP will cost 20ms.

7.6 UDP Multicast Mode



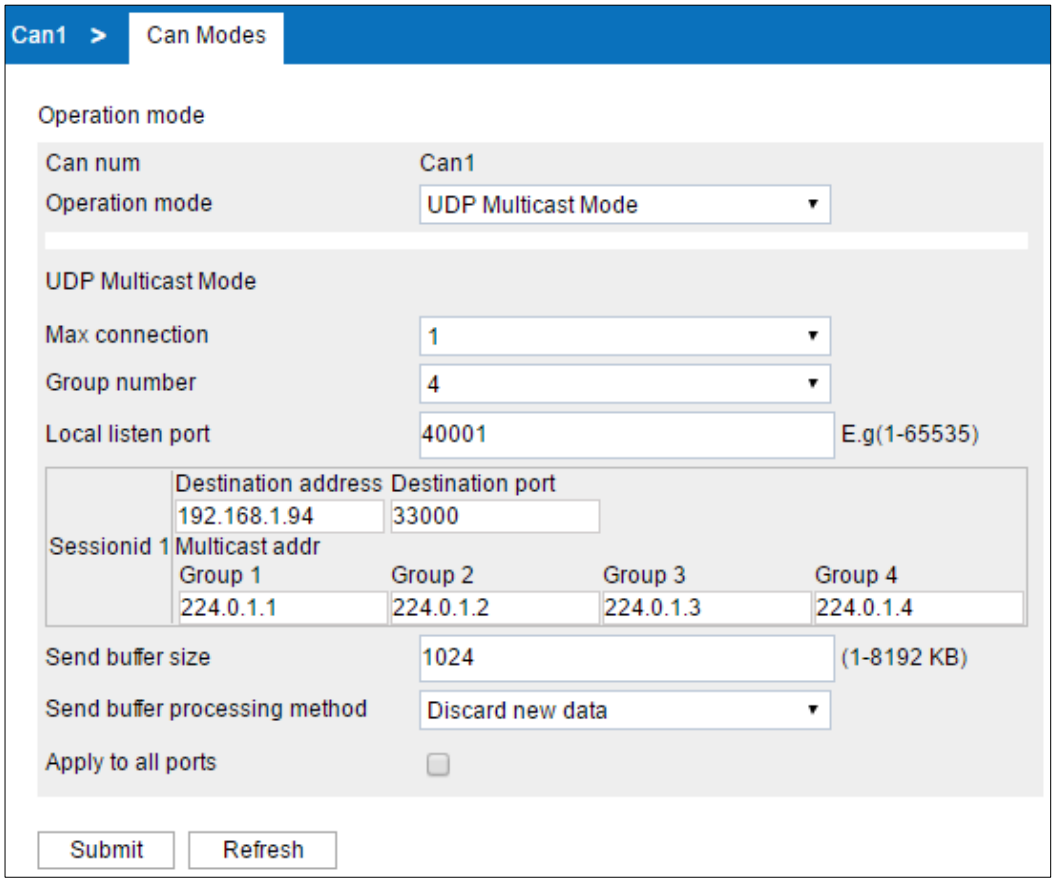
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or interface type is subject to the device obtained.

Under CAN UDP multicast mode, devices can unicast or multicast the data of CAN device to one or more hosts designated by users through UDP protocol, and can also receive unicast and multicast data from one or more devices, thus realizing many-to-many communication.

Interface Description

UDP Multicast Mode interface as follows:



UDP Multicast Mode interface main element configuration instructions:

Interface Element	Discription
Working mode	**Working Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The working modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Multicast Mode	UDP Multicast Mode Configuration Bar
Max connection	The maximum session number supported by the device's CAN port.
Group Number	The multicast number supported by one session, it supports maximum 4 multicasts.

Interface Element	Discription
Local Listen port	The listening port of the device to receive Multicast Note: User must allot the only listen port to each CAN port, and then the system can normally receive the multicast.
Destination address	The IP address of the opposite host that the device needs to connect.
Destination port	Enter the port number of the opposite host that the device needs to connect.
Multicast addr	Group address is used for identifying an IP multicast group, multicast address range is: 224.0.0.0 ~ 239.255.255.255. The device can send or receive group data to or from multiple hosts.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

8 CAN Status

8.1 CAN Port Communication Statistics

Function Description

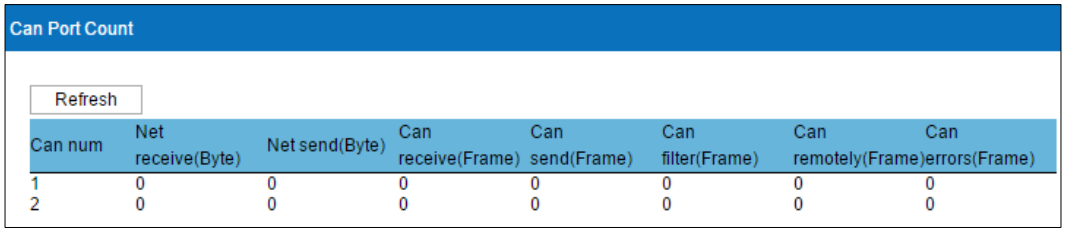
On the "CAN Port Count" page, you can view the statistics of the number of bytes received and sent during the conversion between each CAN port and the network.

Operation Path

Open in order: "CAN Status> CAN Port Count" .

Interface Description

The interface of CAN Port Count is as follows:



The main element configuration description of CAN Port Count interface:

Interface Element	Discription
CAN num	Display the corresponding CAN port number of the device.
Net receive (Byte)	Number of bytes received by the device network interface.
Network transmit (Bytes)	Number of bytes sent by the device network interface.
CAN receive (Frame)	The number of data frames received by the device CAN port.

Interface Element	Discription
CAN send (Frame)	The number of data frames transmitted by the device CAN port.
CAN filter (Frame)	The number of data frames filtered by the device's CAN port.
CAN remotely (Frame)	The number of remotely frames transmitted by the device's CAN port.
CAN errors (Frame)	The number of error frames transmitted by the device's CAN port.

8.2 Network Connection status

Function Description

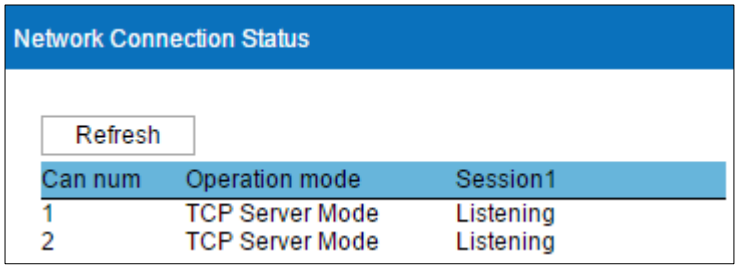
On the "Network Connection Status" page, you can view the working mode and network session connection status of each CAN port of the device.

Operation Path

Open in order: "CAN Status > Network Connection Status".

Interface Description

The network connection status interface is as follows:



The main elements configuration descriptions of the network connection status interface:

Interface Element	Discription
CAN num	Display the corresponding CAN port number of the device.
Operation mode	The operation mode of current serial port are as follows: • TCP Server Mode • TCP Client Mode

Interface Element	Discription
	• UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
Session1	The current connection state of network connection of the CAN port can be displayed as follows: • Connected • Connecting • Listening • (None): the session is not enabled or UDP is not connected

9 Communication Prarameters

Function Description

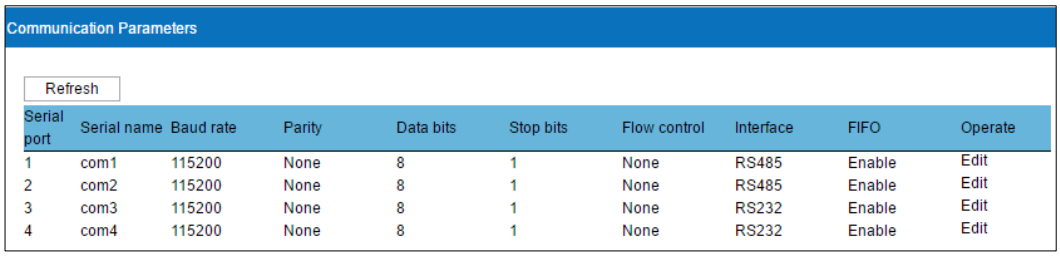
On the "COM Settings" page, you can view and configure the baud rate, parity bit, data bit, stop bit, flow control, interface type, FIFO function and other parameters of each serial port of the device.

Operation Path

Open: “Communication parameters”.

Interface Description

COM setting interface as follows:



The main element configuration description of serial port setup interface:

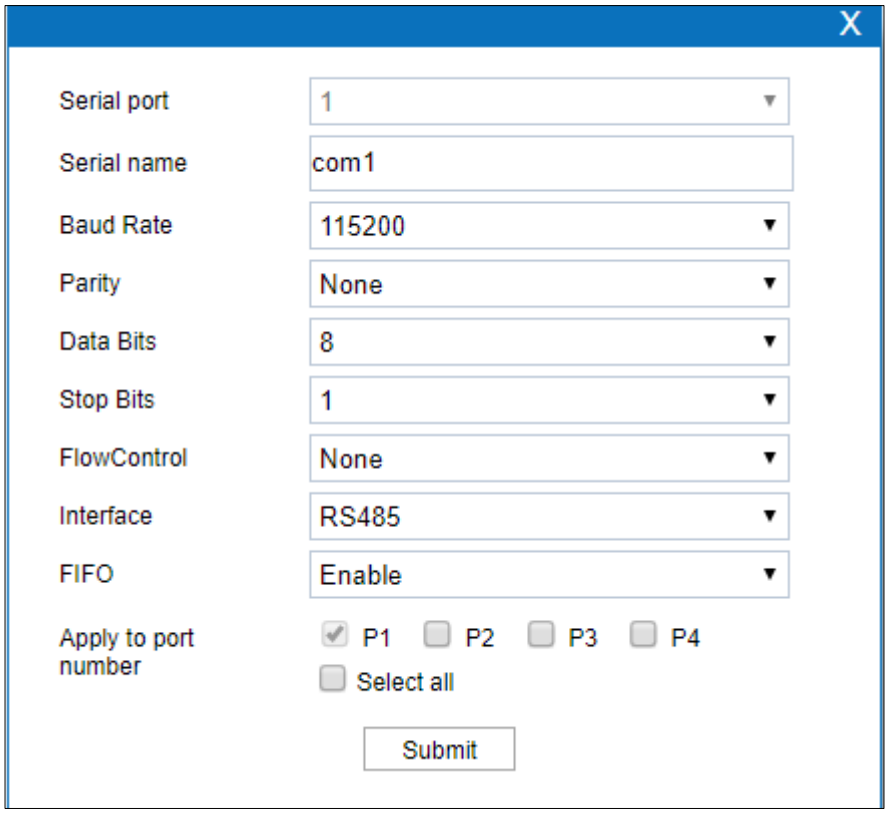
Interface Element	Discription
Serial port	Display the serial port number of the device.
serial name	Displays the name of the device.
Baud rate	Displays the baud rate of the device’s serial port.
Parity	Displays the parity bits of the device's serial Port.
Data Bits	Displays the data bits of the device’s serial port.
Stop Bits	Displays the stop bits of the device’s serial port.
Flow control	Displays whether the flow control function of the device’s serial

Interface Element	Discription
	port is enabled.
Interface	Displays the interface mode of the device's serial port.
FIFO	Display whether the FIFO function of the device's serial port is enabled.
Operate	Click Edit to modify the parameters of the device's serial port.

Click Edit in the serial port entry to modify the current serial port parameters.

Interface Description: Edit

Edit interface is as follows:



The main element configuration description of the Edit interface:

Interface Element	Discription
Serial port	Display the serial port number of the device.
serial name	The text box of serial port name, which supports 1-32 letters or numbers input, and can customize the name of the current serial port.
Baud Rate	Choose baud rate of corresponding serial port. Unit: bps.

Interface Element	Discription
	Options: 110/300/600/1200/2400/4800/9600/19200/38400/57600/115200/230400/460800/921600
Parity	Select parity bits of corresponding serial number. Options: • None • Odd • Even • Mark • Space
Data Bits	Select data bits of corresponding serial number. Options: • 5 bits • 6 bits • 7 bits • 8 bits
Stop Bits	Select stop bits of corresponding serial number. Options: • 1 bits • 2 bits Note: When the data bit is 5bits, stop bit is 1bits and 1.5bits optional.
FlowControl	Flow control is used in two data transmission speed of different devices in the control of data flow technology to ensure that two devices communicate with each other to avoid data loss. Click the "flow control" drop-down list box, select the flow control parameters, the options are: • None • RTS/CTS • DTR/DSR • XON/XOFF
Interface	Determined by both hardware and software, options are as follows: • RS232 • RS422 • RS485
FIFO	Enable or disable the FIFO function, if the serial device does not support data transceiver cache FIFO, FIFO function can be disabled to avoid data transmission errors.

Interface Element	Discription
Apply to the port number	Check the serial port check box to apply the current settings to the specified serial port.

10 Serial Mode

Function Description

On the "Seiral Mode" page, you can configure the working mode of the corresponding serial port number of the device.

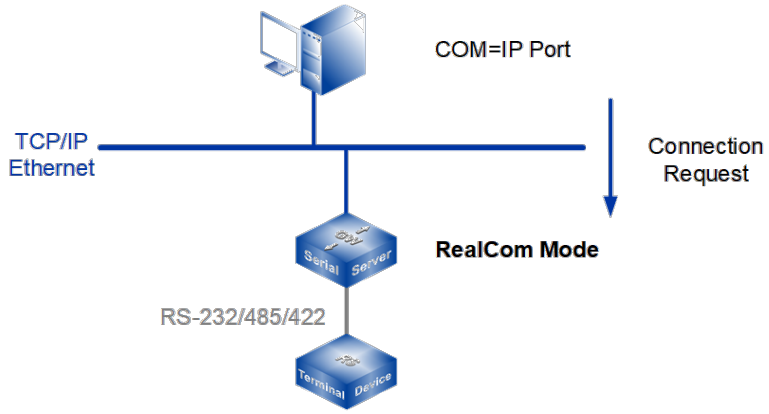
The working modes supported by the device are:

- RealCom Mode
- TCP Server Mode
- TCP Client Mode
- UDP Server Mode
- UDP Client Mode
- Disable Mode

Operation Path

Open in order “COM Mode > Port1”. Under the menu of "COM Mode", the corresponding serial port information can be configured by entering different serial ports. The configuration operation mode of all serial ports' WEB interfaces is the same.

10.1 RealCom Mode



Note:

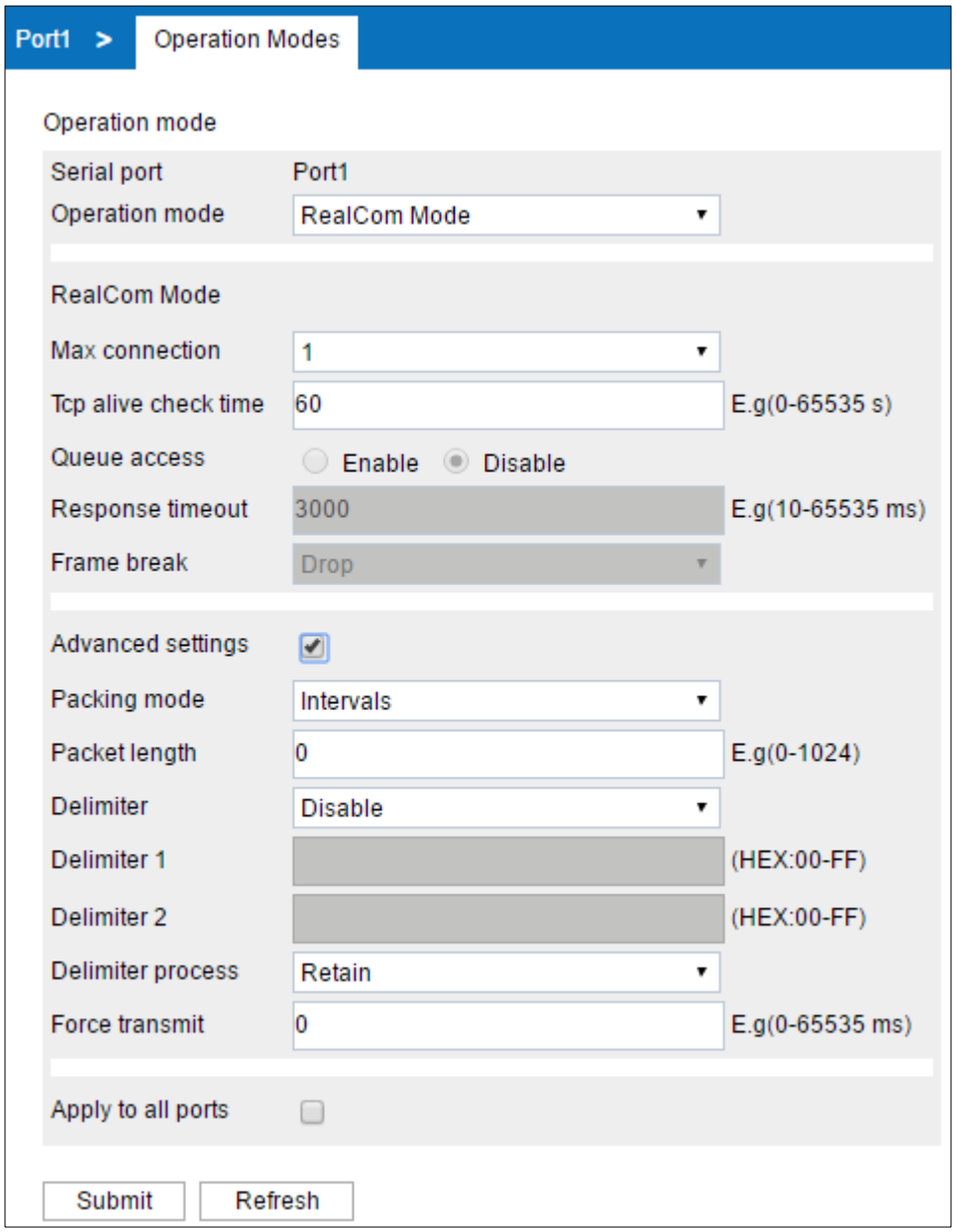
The device picture mentioned in above figure is only an example , and the actual appearance of the device or serial port type is subject to the device obtained.

In RealCom mode, the serial port server and Windows / Linux operating system with the RealCOM drive work cooperatively. RealCom COM/TTY driver establishes a transparent or secure network transmission connection between the host and the serial device in the operating system. Map the serial port of the serial port server to the local COM/TTY device of the host according to the user configured serial server IP address and serial port number and other parameters. The original serial device software or communication module without modification can be used directly without modification.

The RealCom driver gets the data be sent to the local COM / TTY device of the host, then sends it over Ethernet in the form of TCP / IP packet. At the other end of the transmission, the serial server will receive the TCP / IP packet and analyse the packet, and after unpacking send the original data to the serial device through the corresponding serial port, and vice versa.

Interface Description

The interface of RealCom Mode is as follows:



Main element configuration instructions in RealCom Mode interface

Interface Element	Discription
Operation mode	**Working Mode Configuration Bar**
Serial port	Displays the serial number of the device currently configured.
operation mode	The working modes of serial port of the device are as follows: • RealCom Mode • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • Disable Mode

Interface Element	Discription
RealCom Mode	**RealCom Mode configuration bar**
Max connection	The number of host that one serial port connects to. • Each host communicates with serial port in the order of first-in first-out; • The system supports up to 4 connections.
TCP Alive Check Time	If there isn't any TCP activity within schedule time, the system will automatically send connection detection message and check whether the TCP connection is valid. If the reply packet of opposite side hasn't been received after sending probe packet for 3 times, system will regard the opposite side as down and forwardly close the communication connection.
Queue access	With multiple host connections, the command mode only supports one request and one response from each host, and one response data can be cached in response to other same requests. Options are as follows: • Enable; • Disable; Note: Command mode is enabled when the number of connections is greater than 1.
Response timeout	Time interval that allows the serial server to respond to each host's request, the communication between serial server and host is deemed to be completed after schedule time, serial server continues to deal with the next host request.
Frame break	The processing mode of serial port data with no request and automatic response of serial port equipment is as follows: • Drop: discard the unrequested serial data; • Transmit to the last communication connection: transmit the unrequested serial port data to the last communication connection; • Transmit to all open connection: transmit the unrequested serial port data to all open connection;
Advanced Settings	**Advanced Settings Configuration Bar**
Packing mode	Serial port data packaging Ethernet data time, the options are as follows: • Interval: after sending the last Ethernet packet for some

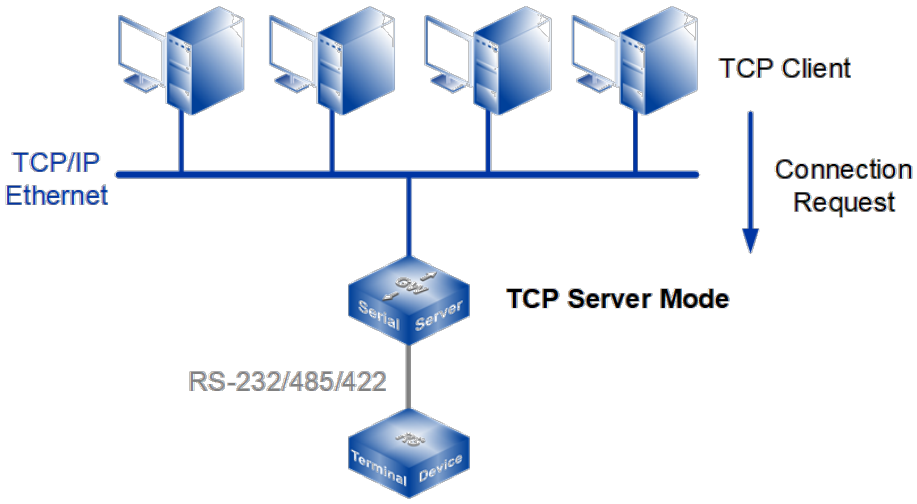
Interface Element	Discription
	time, the system packages the received serial port data into Ethernet packets and sends them out; • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them.
Packing length	The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1024. It means no limit on data transmission length when it' set to 0. Note: There are some slight deviations between the actual package length value and the set value.
Delimiter	Select the number of delimited characters, the options are as follows: • Disable: disable delimiter function; • 1: enable delimiter 1; • 2: enable Delimiter 2. Note: If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network.
Delimiter 1	The Delimiter 1 is expressed in hexadecimal, value range is 00-FF.
Delimiter 2	The Delimiter 2 is expressed in hexadecimal, value range is 00-FF.
Delimiter processing	Select the delimiter processing method. Options: • Retain: the system would send out the received delimiter and other data via network. • Delimiter+1: the system transfers data after receiving a delimiter and an extra byte. • Delimiter+2: the system transfers data after receiving a delimiter and 2 extra byte. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.
Forec transmit	If the transmission time is greater than 0, the system sends the

Interface Element	Discription
	serial data received within the specified time through a packet, in the range of 0 to 65535 ms. When the transfer time is 0, it means that the data transmission interval is not restricted.
Apply to All Ports	Check the “Apply to all port” check box to apply the current settings to all serial ports.

Notice

When the maximum number of connections is greater than 1, set the parameters to be consistent when multiple hosts are connected to the same serial port, otherwise it will cause communication error.

10.2 TCP Server Mode



Note:

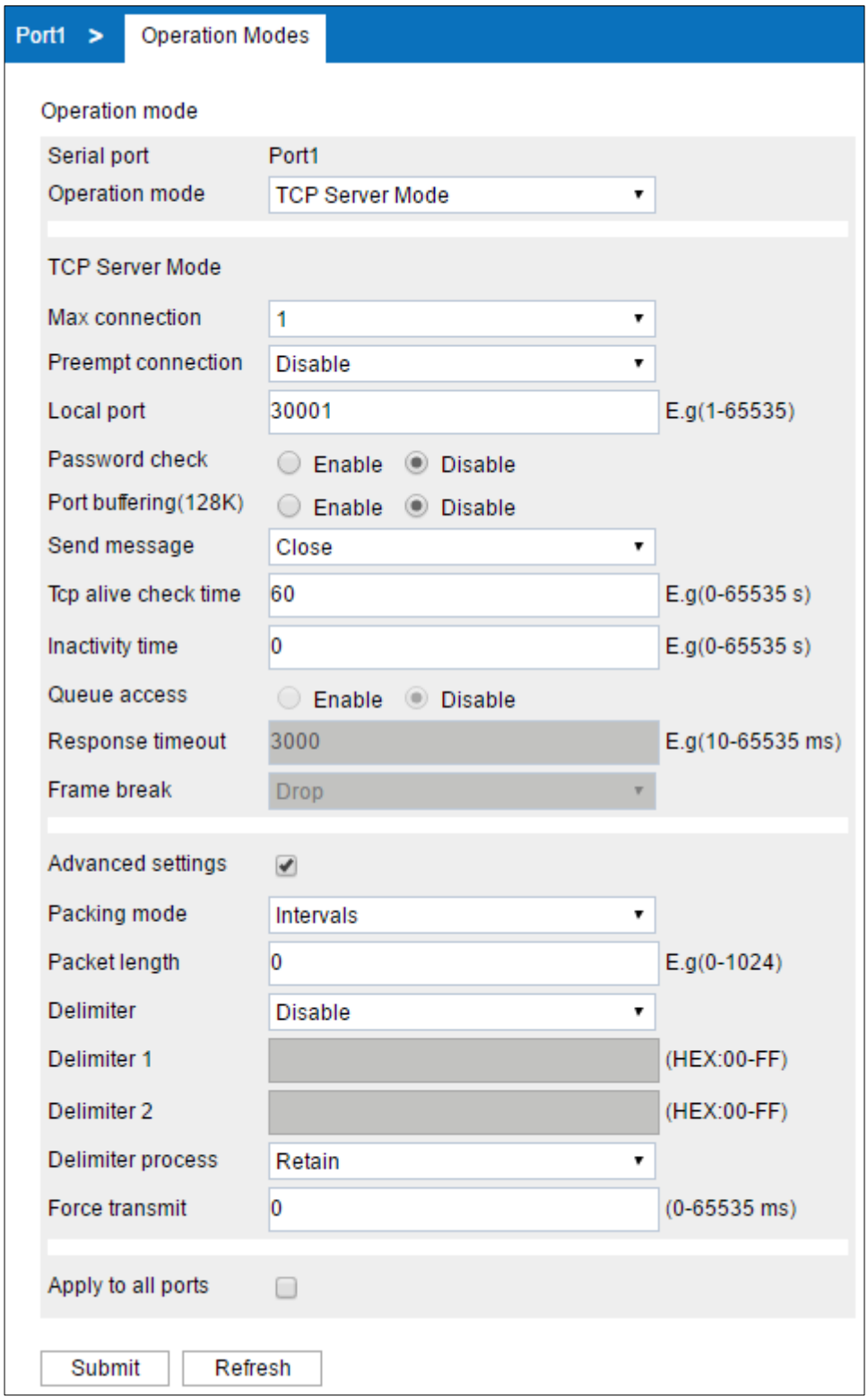
The device picture mentioned in above figure is only an example , and the actual appearance of the device or serial port type is subject to the device obtained.

In TCP server mode, the device is assigned an IP port number and passively waits for the host to connect. When the host initiates a connection request and establishes a connection with the device, the host can realize bidirectional transparent or encrypted data transmission through network connection and serial port. The TCP server mode

supports up to four session connections simultaneously, allowing multiple hosts to simultaneously read or send Ethernet data to a serial device.

Interface Description

TCP server mode interface is as follows:



TCP server mode interface main element configuration instructions:

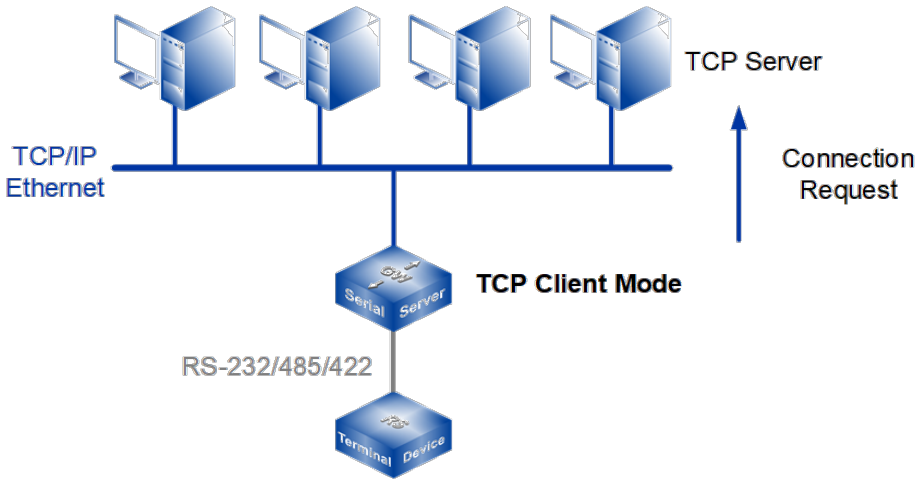
Interface Element	Discription
Operation mode	**Working Mode Configuration Bar**
Serial port	Displays the serial number of the device currently configured.
operation mode	The working modes of serial port of the device are as follows: • RealCom Mode • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • Disable Mode
TCP Server Mode	**TCP Server Mode Configuration bar**
Max connection	The number of host that one serial port connects to. • Each host communicates with serial port in the order of first-in first-out; • The system supports up to 4 connections.
Preempt Connection	When exceed the maximum number of connection request, the number of sessions that have established TCP connections can be preempted, options are as follows: • Disable: established TCP link are not allowed to be preempted; • First connection: the TCP link that first establishes will be preempted; • Longest uncommunicated: the longest uncommunicated TCP link will be preempted.
Local port	The destination connection port of TCP client.
Password check	After the device is connected with the opposite end, the opposite end needs to send the authentication password to the device. If the authentication password is verified, the device and the opposite end can start communication. Options: • Disable: disable password authentication function. • Enable: enable password authentication function. Note: When password authentication is enabled, only users with administrator privileges can send / receive messages using this device. • The first data sent by the opposite end to the device defaults to the authentication password.

Interface Element	Discription
	• The authentication password is a hexadecimal data with 64 bytes. The first 32 bytes are the administrator account, fill with 0 if less than 32 bytes; the last 32 bytes are the administrator password, fill with 0 if less than 32 bytes. • If the authentication password is entered incorrectly, the connection will be broken. After re-establishing the connection with the opposite end, you can re-enter the authentication password. Take the administrator whose account and password are "admin" as an example. The hexadecimal data corresponding to "admin" is "61 64 6D 69 6E", then the check code of the first and the last 32 bytes are "61 64 6D 69 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00", the authentication password is "61 64 6D 69 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 61 64 6D 69 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00".
Port Buffering(128k)	Port data cache, which can cache COM port data up to 128K after the network is abnormal. When the network returns to normal, the cached data is forwarded. The tick options are as follows: • Enable • Disable
Send_message	The information sent after the device is connected to the peer client. Options: • Ipaddr: After the connection is successful, send the IP address of the device to the remote client. • Devicename: After the connection is successful, send the devicename of the device to the remote client. • turnoff: After the connection is successful, no information is sent to the peer client.
TCP Alive check Time	If there isn't any TCP activity within schedule time, the system will automatically send connection detection message and check whether the TCP connection is valid. If the reply packet of opposite side hasn't been received after sending probe packet for 3 times, system will regard the opposite side as down and forwardly close the communication connection.
Inactivity time	Set the idle time of current data communication link of the device. If the idle time-out during communication is larger than 0, the system would close the TCP connection without any

Interface Element	Discription
	data transmission activity occurring in the specified time automatically. 0 means the free TCP connection would not be closed automatically.
Queue access	With multiple host connections, the command mode only supports one request and one response from each host, and one response data can be cached in response to other same requests. Options are as follows: • Enable; • Disable; Note: Command mode is enabled when the number of connections is greater than 1.
Response timeout	The time it allowed for the device to respond to the request of each host. When the specified time arrives, the communication between the device and the host is considered complete, and the request of the next host continues to be processed.
Frame break	The processing mode of serial port data with no request and automatic response of serial port equipment is as follows: • Drop: discard the unrequested serial data; • Transmit to the last communication connection: transmit the unrequested serial port data to the last communication connection; • Transmit to all open connection: transmit the unrequested serial port data to all open connection;
Advanced Settings	**Advanced Settings Configuration Bar**
Packing mode	Serial port data packaging Ethernet data time, the options are as follows: • Interval: after sending the last Ethernet packet for some time, the system packages the received serial port data into Ethernet packets and sends them out; • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them.
Packet length	The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1024. It means no

Interface Element	Discription
	limit on data transmission length when it' set to 0. Note: There are some slight deviations between the actual package length value and the set value.
Delimiter	Select the number of delimited characters, the options are as follows: • Disable: disable delimiter function; • 1: enable delimiter 1; • 2: enable Delimiter 2. Note: If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network.
Delimiter 1	The Delimiter 1 is expressed in hexadecimal, value range is 00-FF.
Delimiter 2	The Delimiter 2 is expressed in hexadecimal, value range is 00-FF.
Delimiter process	Select the delimiter processing method. Options: • Retain: the system would send out the received delimiter and other data via network. • Delimiter+1: the system transfers data after receiving a delimiter and an extra byte. • Delimiter+2: the system transfers data after receiving a delimiter and 2 extra byte. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.
Force transmit	If the transmission time is greater than 0, the system sends the serial data received within the specified time through a packet, in the range of 0 to 65535 ms. When the transfer time is 0, it means that the data transmission interval is not restricted.
Apply to All Ports	Check the "Apply to all port" check box to apply the current settings to all serial ports.

10.3 TCP Client Mode



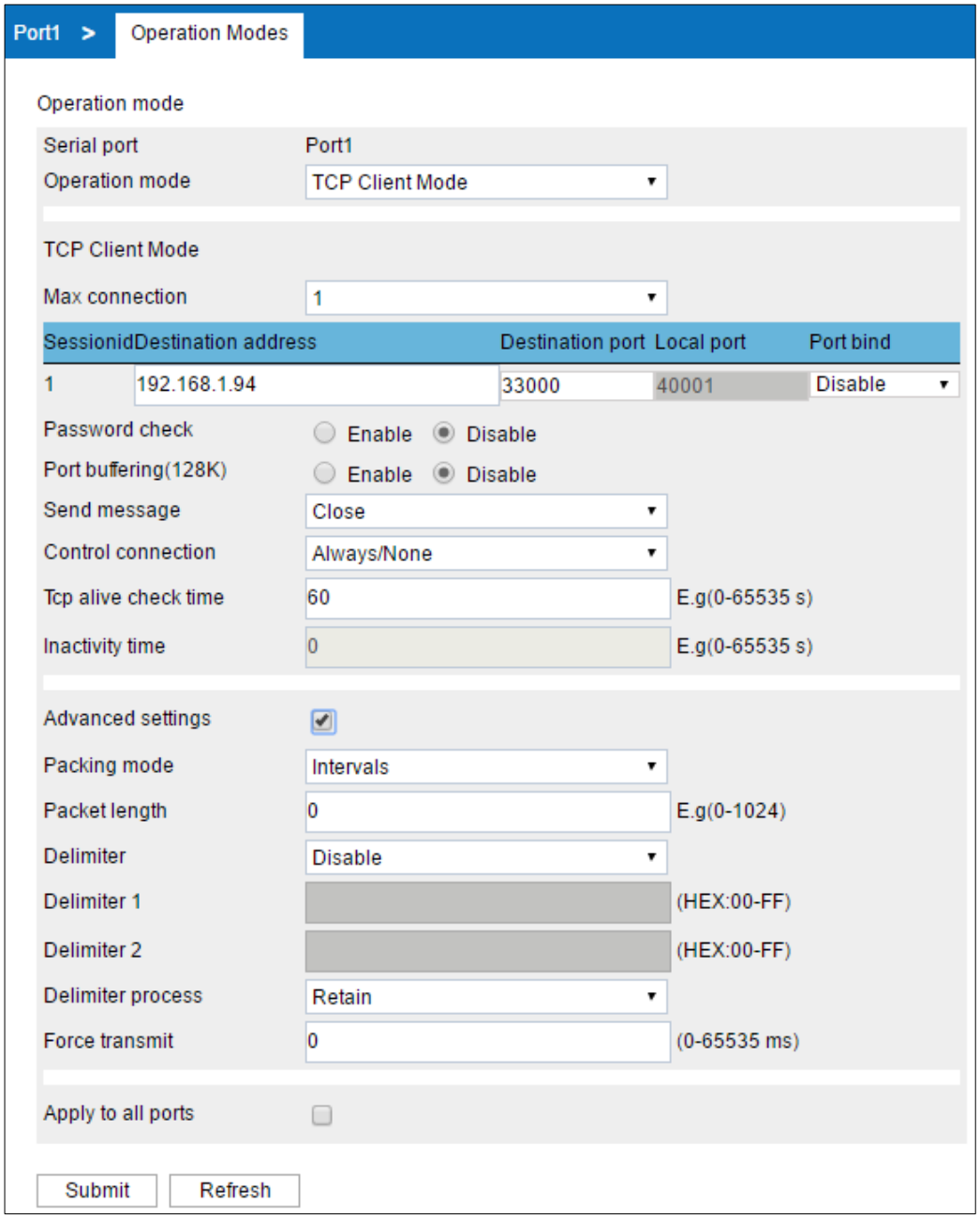
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or serial port type is subject to the device obtained.

In TCP client mode, the device can actively establish a network connection with the host specified by the user when the serial port data arrives. After the data transmission is completed, the device will automatically close the network connection according to TCP keep-alive time/idle timeout and other parameters. Similarly, TCP client mode can support up to four session connections at the same time, so that multiple hosts can simultaneously read or send Ethernet data to a serial device.

Interface Description

TCP Client mode interface is as follows:



TCP client mode interface main element configuration instructions:

Interface Element	Discription
operation mode	**Working Mode Configuration Bar**
Serial port	Displays the serial number of the device currently configured.
operation mode	The working modes of serial port of the device are as follows: • RealCom Mode • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode

Interface Element	Discription
	• Disable Mode
TCP Client Mode	**TCP Client Mode Configuration Bar**
Max connection	The number of host that one serial port connects to. • Each host communicates with serial port in the order of first-in first-out; • The system supports up to 4 connections.
session	The number of TCP connection sessions corresponds to the maximum number of connections.
Destination Address	Enter the IP address of the server to which the device is connected.
Destination Port	Enter the TCP port number of the server to which the device is connected.
Local Port	A local port number assigned by the device for TCP connection, which can provide service or connection to the outside world, is used to connect and communicate with the server.
Port bind	Local port fixed, options are as follows: • Disable: the system automatically selects the idle local port to establish a connection with the server; • Enable: connect to the server using a manually configured local port.
Password check	After the device is connected with the opposite end, the opposite end needs to send the authentication password to the device. If the authentication password is verified, the device and the opposite end can start communication. Options: • Disable: disable password authentication function. • Enable: enable password authentication function. Note: When password authentication is enabled, only users with administrator privileges can send / receive messages using this device. • The first data sent by the opposite end to the device defaults to the authentication password. • The authentication password is a hexadecimal data with 64 bytes. The first 32 bytes are the administrator account, fill with 0 if less than 32 bytes; the last 32 bytes are the administrator password, fill with 0 if less than 32 bytes.

Interface Element	Discription
	• If the authentication password is entered incorrectly, the connection will be broken. After re-establishing the connection with the opposite end, you can re-enter the authentication password. Take the administrator whose account and password are "admin" as an example. The hexadecimal data corresponding to "admin" is "61 64 6D 69 6E", then the check code of the first and the last 32 bytes are "61 64 6D 69 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00", the authentication password is "61 64 6D 69 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 61 64 6D 69 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00".
Port Buffering(128k)	Port data cache, which can cache COM port data up to 128K after the network is abnormal. When the network returns to normal, the cached data is forwarded. The tick options are as follows: • Enable • Disable
Send message	The information sent after the device is connected to the peer client. Options: • Ipaddr: After the connection is successful, send the IP address of the device to the remote client. • Devicename: After the connection is successful, send the devicename of the device to the remote client. • turnoff: After the connection is successful, no information is sent to the peer client.
control Connection	Select how the device initiates a connection request and disconnectsit. Options: • Always/None – Always: Immediately tries to establish a connection with the target host after the system is started and automatically reconnects the target host after the connection is disconnected. – None: Never shut down the network connection automatically. • Char/None

Interface Element	Discription
	– Char: Automatically connects to the target host when receiving data from the serial port. – None: Never shut down the network connection automatically. • Char/Idel – Char: Automatically connects to the target host when receiving data from the serial port. – Idle: If the idle timeout time is greater than 0, the system will automatically shut down TCP connections that do not have any data send and receive activity for a specified period of time. • DSR On/ DSR Off – DSR On: Automatically connects to the target host when the DSR signal is detected. – DCD Off: Automatically shuts down the network connection when the DCD signal is detected invalid. • DSR On/ None – DSR On: Automatically connects to the target host when the DSR signal is detected. – None: Never shut down the network connection automatically. • DCD On / DCD Off – DCD On: Automatically connects to the target host when the DCD signal is detected. – DCD Off: Automatically shuts down the network connection when the DCD signal is detected invalid. • DCD On / None – DCD On: Automatically connects to the target host when the DCD signal is detected. – None: Never shut down the network connection automatically.
TCP Alive check Time	If there isn't any TCP activity within schedule time, the system will automatically send connection detection message and check whether the TCP connection is valid. If the reply packet of opposite side hasn't been received after sending probe packet for 3 times, system will regard the opposite side as

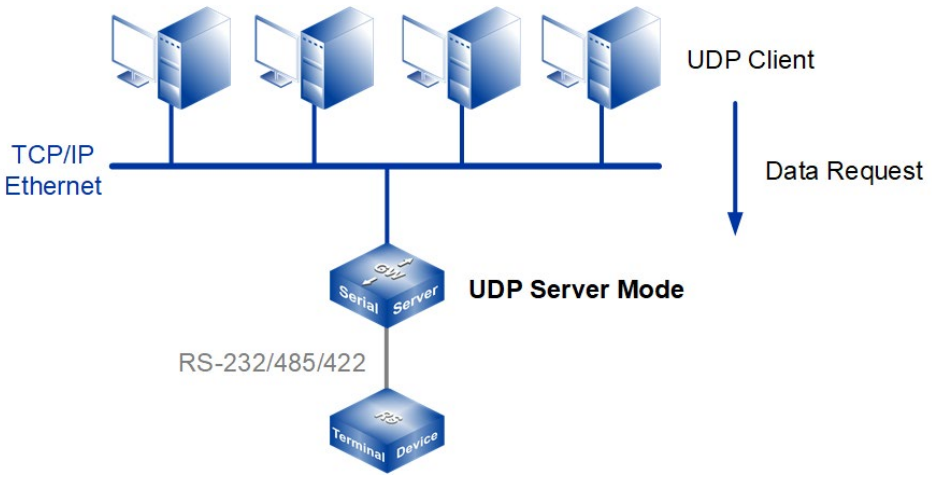
Interface Element	Discription
	down and forwardly close the communication connection.
Inactivity time	Set the idle time of current data communication link of the device. If the idle time-out during communication is larger than 0, the system would close the TCP connection without any data transmission activity occurring in the specified time automatically. 0 means the free TCP connection would not be closed automatically.
Advanced Settings	**Advanced Settings Configuration Bar**
Packing mode	Serial port data packaging Ethernet data time, the options are as follows: • Interval: after sending the last Ethernet packet for some time, the system packages the received serial port data into Ethernet packets and sends them out; • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them.
Packing length	The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1024. It means no limit on data transmission length when it' set to 0. Note: There are some slight deviations between the actual package length value and the set value.
Delimiter	Select the number of delimited characters, the options are as follows: • Disable: disable delimiter function; • 1: enable delimiter 1; • 2: enable Delimiter 2. Note: If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network.
Delimiter 1	The Delimiter 1 is expressed in hexadecimal, value range is 00-FF.
Delimiter 2	The Delimiter 2 is expressed in hexadecimal, value range is 00-FF.

Interface Element	Discription
Delimiter process	Select the delimiter processing method. Options: • Retain: the system would send out the received delimiter and other data via network. • Delimiter+1: the system transfers data after receiving a delimiter and an extra byte. • Delimiter+2: the system transfers data after receiving a delimiter and 2 extra byte. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.
Force transmit	If the transmission time is greater than 0, the system sends the serial data received within the specified time through a packet, in the range of 0 to 65535 ms. When the transfer time is 0, it means that the data transmission interval is not restricted.
Apply to All Ports	Check the “Apply to all port” check box to apply the current settings to all serial ports.

Notice

The inactivity time takes effect only when "Control Connection" is set to "Char/Idle".

10.4 UDP Server Mode



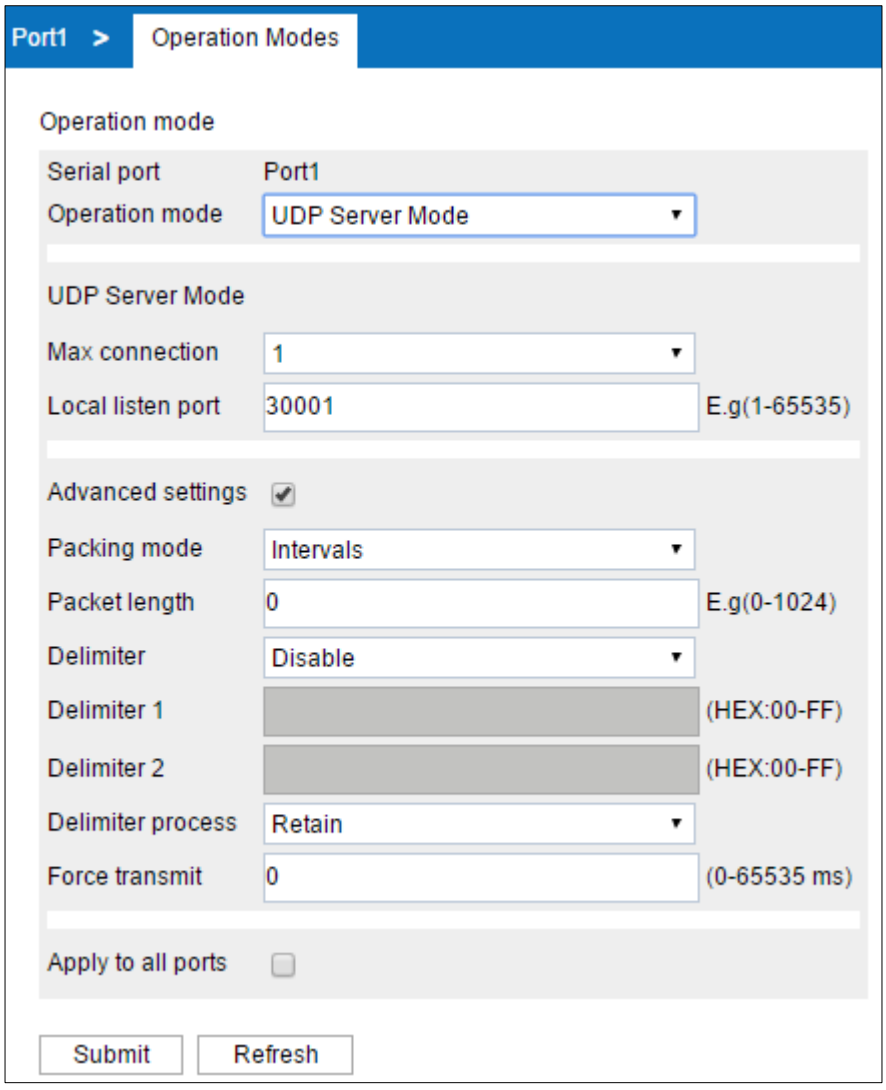
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or serial port type is subject to the device obtained.

In UDP Server mode, the device, as a server, is assigned a UDP port number, passively waits for the host session, and transmits serial data with the host through UDP protocol. Devices in UDP mode can transmit data from serial devices to one or more hosts, and serial devices can also receive data from one or more hosts. Compared with TCP mode, UDP protocol is faster and more efficient.

Interface Description

TCP Server Mode interface is as follows:

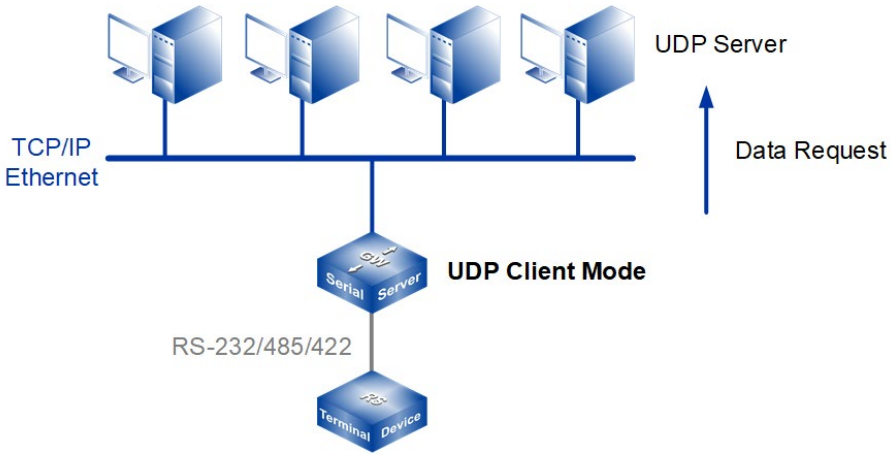


UDP Server Mode interface main element configuration instructions

Interface Element	Discription
Operation mode	**Working Mode Configuration Bar**
Serial port	Displays the serial number of the device currently configured.
Operation mode	The working modes of serial port of the device are as follows: • RealCom Mode • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • Disable Mode
UDP Server Mode	**TCP Server Mode Configuration Bar**
Max connection	The number of host that one serial port has session with. • Each host communicates with serial port in the order of first-in first-out; • The system supports up to 4 sessions.
Local Listen port	The network receives the listening port of UDP data. The user must assign a unique listening port to each serial port so that the system can normally receive UDP data.
Advanced Settings	**Advanced Settings Configuration Bar**
Packing mode	Serial port data packaging Ethernet data time, the options are as follows: • Interval: after sending the last Ethernet packet for some time, the system packages the received serial port data into Ethernet packets and sends them out; • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them.
Packing length	The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1024. It means no limit on data transmission length when it' set to 0. Note: There are some slight deviations between the actual package length value and the set value.
Delimiter	Select the number of delimited characters, the options are as

Interface Element	Discription
	follows: • Disable: disable delimiter function; • 1: enable delimiter 1; • 2: enable Delimiter 2. Note: If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network.
Delimiter 1	The Delimiter 1 is expressed in hexadecimal, value range is 00-FF.
Delimiter 2	The Delimiter 2 is expressed in hexadecimal, value range is 00-FF.
Delimiter process	Select the delimiter processing method. Options: • Retain: the system would send out the received delimiter and other data via network. • Delimiter+1: the system transfers data after receiving a delimiter and an extra byte. • Delimiter+2: the system transfers data after receiving a delimiter and 2 extra byte. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.
Force transmit	If the transmission time is greater than 0, the system sends the serial data received within the specified time through a packet, in the range of 0 to 65535 ms. When the transfer time is 0, it means that the data transmission interval is not restricted.
Apply to All Ports	Check the “Apply to all port” check box to apply the current settings to all serial ports.

10.5 UDP Client Mode



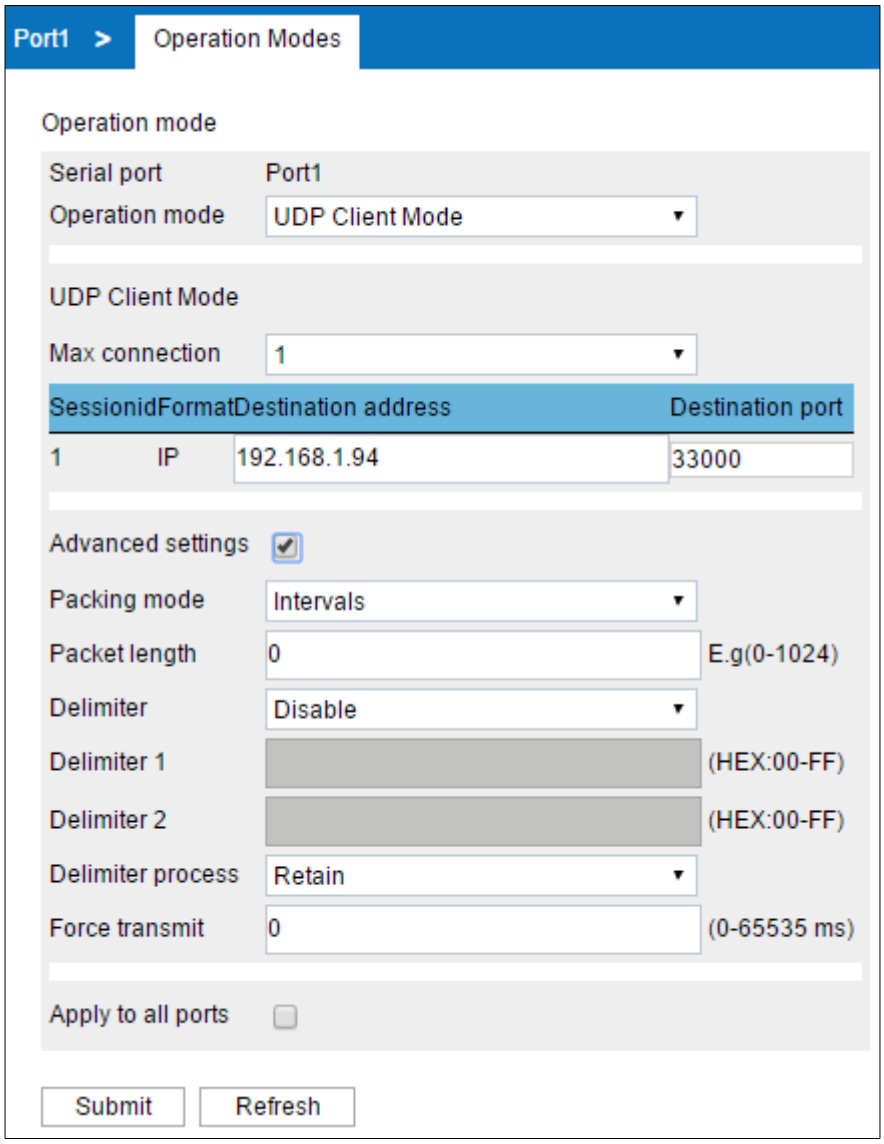
Note:

The device picture mentioned in above figure is only an example , and the actual appearance of the device or serial port type is subject to the device obtained.

Under CAN Client Mode, the device can be a client, and it can actively transmit serial data with the host user appointed under the UDP protocol. Devices in UDP mode can transmit data from serial devices to one or more hosts, and serial devices can also receive data from one or more hosts. Compared with TCP mode, UDP protocol is faster and more efficient.

Interface Description

UDP Client Mode interface is as follows:



UDP Client Mode interface main element configuration instructions:

Interface Element	Discription
operation mode	**Working Mode Configuration Bar**
Serial port	Displays the serial number of the device currently configured.
operation mode	The working modes of serial port of the device are as follows: • RealCom Mode • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • Disable Mode
UDP Client Mode	**UDP Client Mode Configuration Bar**

Interface Element	Discription
Max connection	The number of host that one serial port has session with. • Each host communicates with serial port in the order of first-in first-out; • The system supports up to 4 sessions.
Session	The number of UDP sessions corresponds to the maximum number of connections.
Format	Destination address format.
Destination address	Enter the IP address of the server that the device needs to have session with.
Destination port	Enter the UDP port number of the server that the device needs to have session with.
Advanced Settings	**Advanced Settings Configuration Bar**
Packing mode	Serial port data packaging Ethernet data time, the options are as follows: • Interval: after sending the last Ethernet packet for some time, the system packages the received serial port data into Ethernet packets and sends them out; • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them.
Packing length	The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1024. It means no limit on data transmission length when it' set to 0. Note: There are some slight deviations between the actual package length value and the set value.
Delimiter	Select the number of delimited characters, the options are as follows: • Disable: disable delimiter function; • 1: enable delimiter 1; • 2: enable Delimiter 2. Note: If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network.

Interface Element	Discription
Delimiter 1	The Delimiter 1 is expressed in hexadecimal, value range is 00-FF.
Delimiter 2	The Delimiter 2 is expressed in hexadecimal, value range is 00-FF.
Delimiter process	Select the delimiter processing method. Options: • Retain: the system would send out the received delimiter and other data via network. • Delimiter+1: the system transfers data after receiving a delimiter and an extra byte. • Delimiter+2: the system transfers data after receiving a delimiter and 2 extra byte. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.
Force Transmit	If the transmission time is greater than 0, the system sends the serial data received within the specified time through a packet, in the range of 0 to 65535 ms. When the transfer time is 0, it means that the data transmission interval is not restricted.
Apply to all port	Check the “Apply to all port” check box to apply the current settings to all serial ports.

11 Serial Status

11.1 Serial Port Count

Function Description

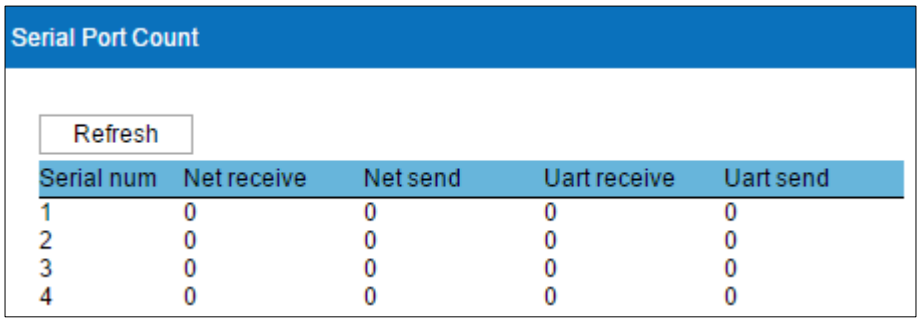
On the "Serial Port Count" page, you can view the statistics of the number of bytes received and sent during the conversion between each serial port and the network.

Operation Path

Open in order: “Serial Status> Seiral Port Count" .

Interface Description

The interface of COM Communication Statistics is as follows:



The main element configuration description of Serial Port Count interface:

Interface Element	Discription
Serial num	Display corresponding device serial port.
Network receive	Number of bytes received by the device network interface.
Net send	Number of bytes sent by the device network interface.
Uart receive	Number of bytes received by the serial port of the device.

Interface Element	Discription
Uart send	Number of bytes sent by serial port of device.

11.2 Serial Port Status

Function Description

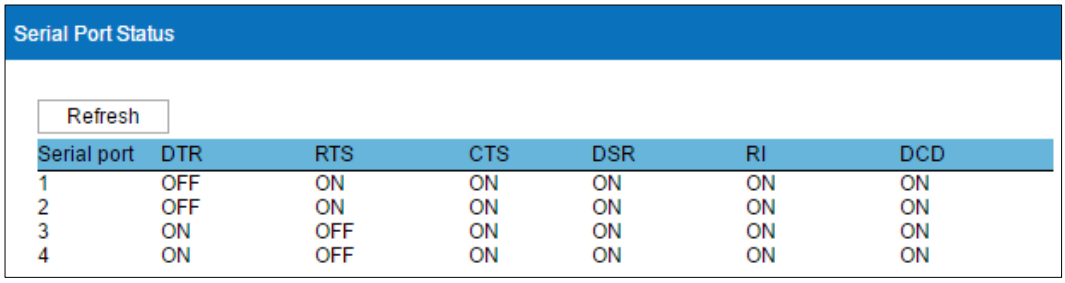
On the "Serial Port Status" page, you can view the pin status of each serial port of the device.

Operation Path

Open in order: "Serial Status > Serial Port Status".

Interface Description

Serial Port Status interface is as follows:



Main element configuration instructions in Serial Port Status interface:

Interface Element	Discription
Serial port	Display corresponding device serial port.
DTR	the status of DTR(Data Terminal Ready) pin of serial port can be displayed as follows: • ON Status • OFF
RTS	At present, the status of RTS(Request To Send) pin of serial port can be displayed as follows: • ON Status • OFF
CTS	At present, the status of CTS(Clear To Send) pin of serial port can be displayed as follows:

Interface Element	Discription
	• ON Status • OFF
DSR	The current status of DSR(Data Set Ready) pin of serial port can be displayed as follows: • ON Status • OFF
RI	The current status of RI(Ring Indicator) pin of serial port can be displayed as follows: • ON Status • OFF
DCD	The current status of DCD(Data Carrier Detect) pin of serial port can be displayed as follows: • ON Status • OFF

11.3 Network Connection state

Function Description

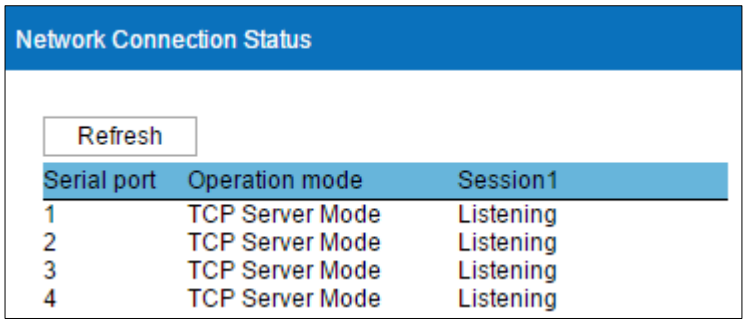
On the "Network Connection Status" page, you can view the working mode and network session connection status of each serial port of the device.

Operation Path

Open in order: "Seial Status > Network Connection Status".

Interface Description

The network connection status interface is as follows:



The main elements configuration descriptions of the network connection status interface:

Interface Element	Discription
Serial port	Display corresponding device serial port.
Operation mode	The operation mode of current serial port are as follows: • RealCom Mode • Reverse RealCom Mode • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode • Pair Slave Mode • Pair Master Mode • Telnet Mode • Reverse Telnet Mode • RFC2217 Mode • Redundant COM Mode • DRDAS RealCom Mode • DRDAS TCP Server Mode • Disable Mode
Session1	The current connection state of network session 1 of the serial port can be displayed as follows: • Connected • Connecting • Listening • (None): the session is not enabled or UDP is not connected
Session2	The current connection state of network session 2 of the serial port can be displayed as follows: • Connected • Connecting • Listening • (None): the session is not enabled or UDP is not connected

Interface Element	Discription
Session3	The current connection state of network session 3 of the serial port can be displayed as follows: • Connected • Connecting • Listening • (None): the session is not enabled or UDP is not connected
Session4	The current connection state of network session 4 of the serial port can be displayed as follows: • Connected • Connecting • Listening • (None): the session is not enabled or UDP is not connected

11.4 Serial Port Error Count

Function Description

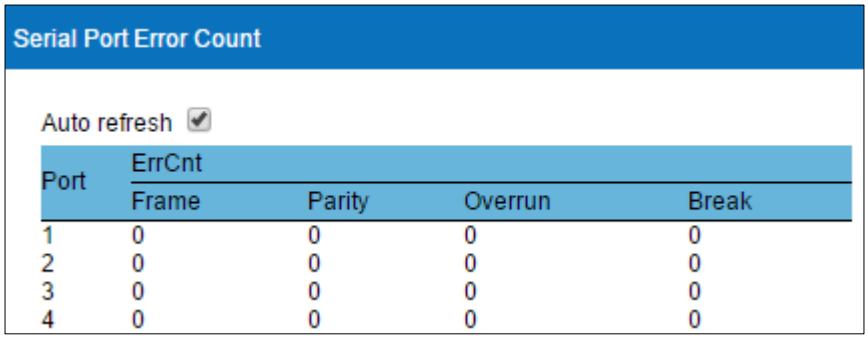
On the "Serial Port Error Count" page, user can check the error data count of each serial port of the device.

Operation Path

Open in order: "Seiral Status > Serial Port Error Count".

Interface Description

Serial Port Error Count interface as follows:



The main element configuration description of serial port error count:

Interface Element	Discription
Serial port	Display corresponding device serial port.
Frame	The number of data frames with wrong stop bits, the received data characters have no valid stop bits.
Parity	The number of data frames with wrong check mode, and the received data characters do not match the configured check bits.
Overrun	The number of overrun data frames, and the received data characters exceeded the processing speed of the device and caused the buffer overflow.
Break	The number of interrupted data frames, and the time that the received data characters remain low level exceeds the transmission time of one complete data frame (the total time of transmission start bit, data bit, check bit and stop bit).

12 Modbus Upgrade

12.1 Upgrade

Function Description

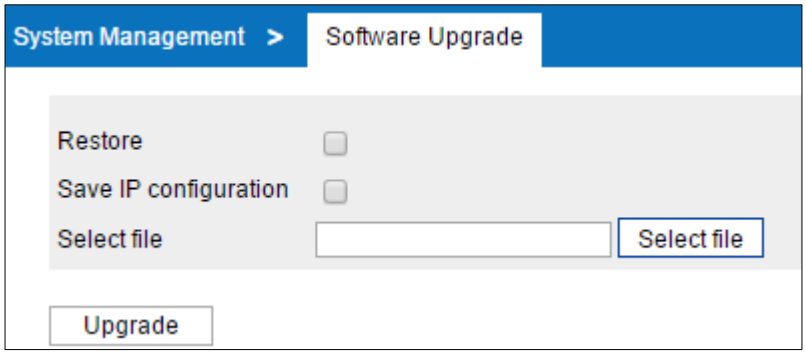
On the "Software Upgrade" page, you can update and upgrade some device programs of CAN port and serial port.

Operation Path

Open in order: "System management > Software Upgrade".

Interface Description

The software update interface as follows:



The main elements configuration description of software update interface:

Interface Element	Discription
Restore	When checked, the device will be restored to the factory settings after upgrading. After unchecking, the configuration parameters will be kept after the device software is upgraded.

Interface Element	Discription
Save IP configuration	After the software upgrade is checked to restore the factory configuration, the IP configuration can be checked to keep the current IP address and other parameters will be restored to the factory configuration.
Select file	Select the path of the local upgrade file, and click “Select file” to select the required configuration file.
Upgrade	Click “upgrade” button to start the program upgrade.

Note

- Do not click on or configure other WEB pages of the device or restart the device or power off the device when upgrading software. Otherwise, the software update will fail, or the device system will crash.
- Keep a reliable wired connection when upgrading.
- When the online upgrade is complete, the device will restart automatically.

13 Firewall

Firewall is a network security system between internal network and external network. It's an information security protection system that allows or restricts the transmission of data in accordance with specific rules.

13.1 IP Filter

Function Description

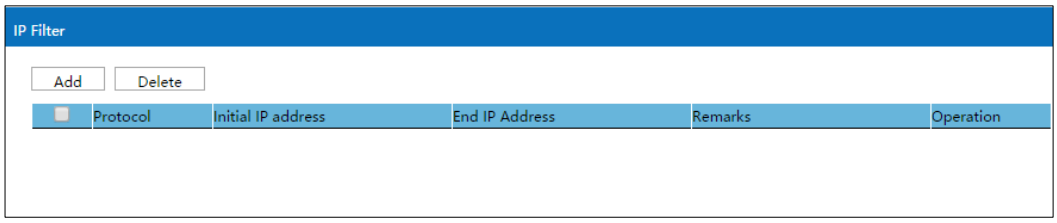
On the "IP filter" page of firewall, user can check or add IP filter to forbid the communication between the clients in LAN and WAN.

Operation Path

Please open in order: "Firewall > IP filter".

Interface Description

IP filter interface as follows:



The main element configuration description of IP filter interface:

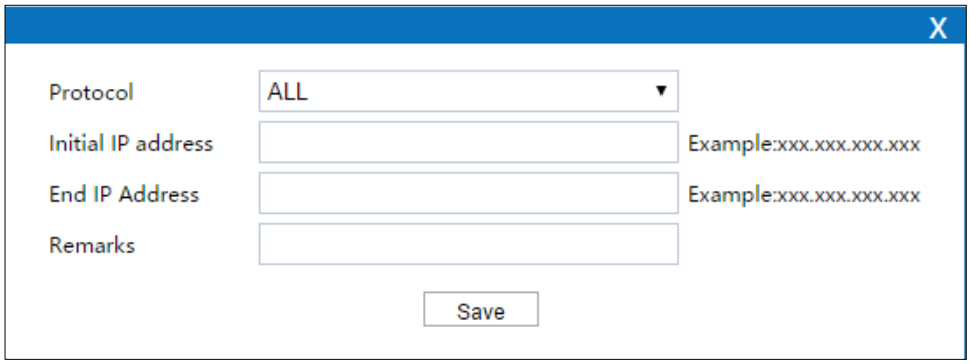
Interface Element	Discription
☐	Check box of IP address filtering entries, click to check all IP filter entries.
Protocol	Protocols used by data packets.
Initial IP address	Start IP address of LAN IP address range filtered by the device.

Interface Element	Discription
End IP address	End IP address of LAN IP address range filtered by the device.
Remarks	Remarks of IP filter entries.
Operation	Edit: Modify the filtering entries information.

Interface Description: Add IP Filter Entry

Click "Add" to increase IP filter entry.

The Add interface as follows:



The main elements configuration description of Add interface:

Interface Element	Discription
Protocol	Drop-down list of data packet protocol, options as follows: • ALL; • TCP; • UDP.
Initial IP address	Start IP address of LAN IP address range filtered by the device, such as: 192.168.1.123.
End IP address	End IP address of LAN IP address range filtered by the device, such as: 192.168.1.123.
Remarks	Remarks of IP address filter list support 32 valid characters, optional.

13.2 MAC Filter

Function Description

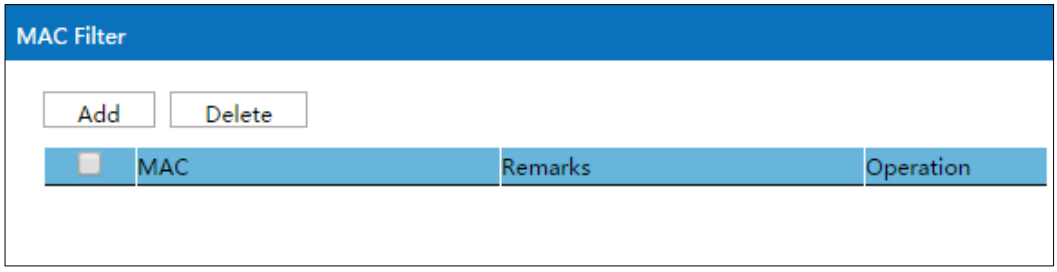
On the "MAC filter" page of firewall, user can check or add MAC filter to forbid the communication between the clients in LAN and WAN; it can effectively control the WAN access rights of user in LAN.

Operation Path

Please open in order: "Firewall > MAC filter".

Interface Description

MAC filter interface as follows:



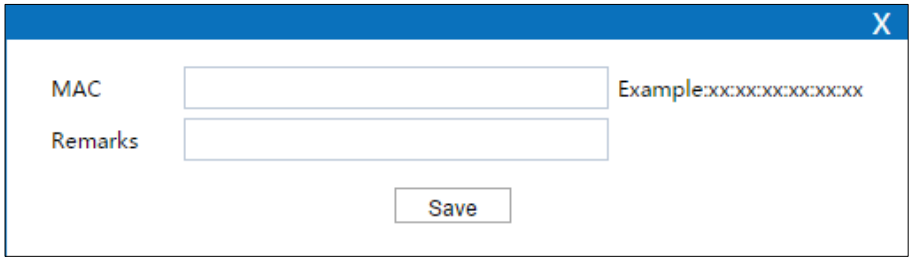
The main element configuration description of MAC filter interface:

Interface Element	Discription
☐	Check box of MAC address filtering entries, click to check all MAC filter entries.
MAC	MAC address of LAN client filtered by the device.
Remarks	Remarks of MAC filter entries.
Operation	Edit: Modify the filtering entries information.

Interface Description: Add MAC Filter Entry

Click "Add" to increase MAC filter entry.

The Add interface as follows:



The main elements configuration description of Add interface:

Interface Element	Discription
MAC	MAC address of LAN client filtered by the device.
Remark	Remarks of the URL filtering entry, it supports 32 valid characters, optional.

13.3 URL Filter

URL (Uniform Resource Locator) is the brief expression of access method and location of resources gained from Internet; it's the address of standard Internet resources. Each Internet file has a unique URL, which refers to the network address.

Function Description

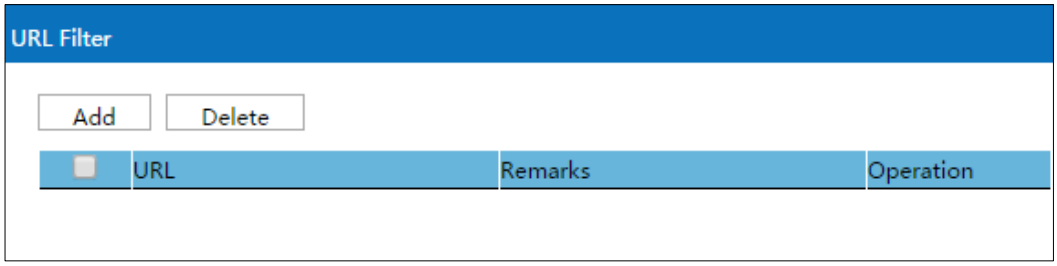
On the "URL filter" page of firewall, user can check or add URL filter to prohibit the client in LAN from accessing URL address in WAN and prevent user from accessing some of the websites.

Operation Path

Please open in order: "Firewall > URL filter".

Interface Description

URL filter interface as follows:



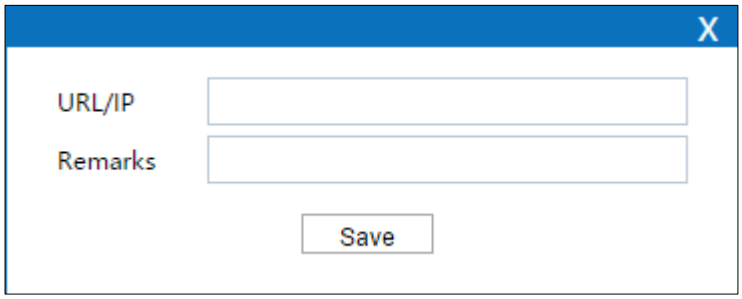
The main element configuration description of URL filter interface:

Interface Element	Discription
☐	URL filter check box, click to check all URL filter entries.
URL	URL address in LAN filtered by the device.
Remarks	Remarks for URL filter entries.
Operation	Edit: modify the filter list.

Interface Description: Add URL Filter List

Click "Add" to increase URL filter list.

URL filter interface as follows:



The main element configuration description of URL filter interface:

Interface Element	Discription
URL/IP	URL/IP address in LAN filtered by the device.
Remarks	Remarks of the URL filtering entry, it supports 32 valid characters, optional.

13.4 Keyword Filter

Keyword filtering refers to the pre-programming filtering of transmitted information in the network application, detecting the specified keywords and intelligently identifying whether there exists any violation of the specified policy in the network.

Function Description

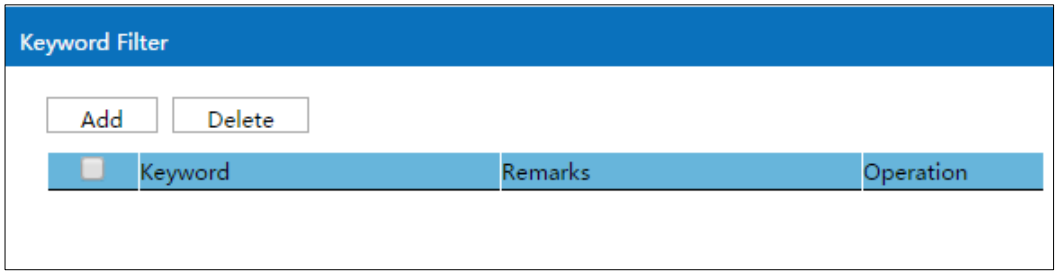
On the page of "Keyword filter" of the firewall, user can view or add keyword filtering entries to prevent clients on the LAN from accessing to the network address corresponding to the keywords in the WAN.

Operation Path

Open in order: "Firewall > Keyword Filter".

Interface Description

Keyword filter interface as follows:



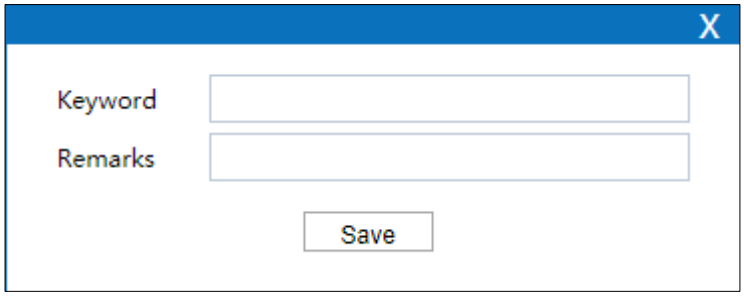
The main elements configuration description of keyword filter interface:

Interface Element	Discription
☐	Keyword filter entry check box and click to select all keyword filtering entries.
Keyword	Keywords in the WAN filtered by this device.
Remarks	Remarks for keyword filtering entries.
Operation	Edit: Modify the filtering entries information.

Interface Description: Add keyword filtering entry

Click the "Add" button to add the keyword filtering entry.

The Add interface as follows:



The main elements configuration description of Add interface:

Interface Element	Discription
Keyword	Keywords in the WAN filtered by this device.
Remark	Remarks of the keyword filtering list; it supports 32 valid characters, and can be left blank.

13.5 IP Address Black/White List

Function Description

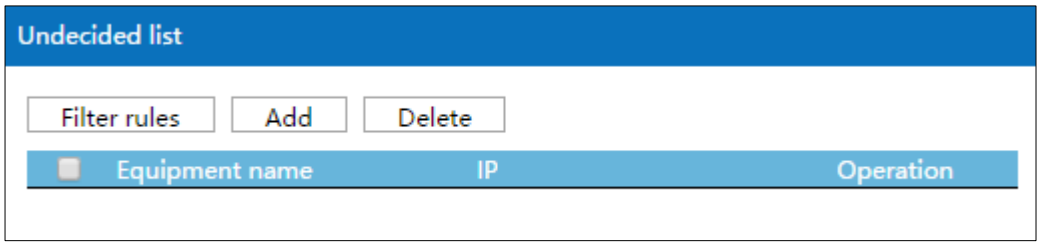
On the "Black and White List of IP Addresses" page of the firewall, you can control the communication between the client with the specified IP address in the LAN and the WAN according to the filter list.

Operation Path

Open in order "Firewall > IP Address Black and White List".

Interface Description

IP Address Black/White List interface is as follows:



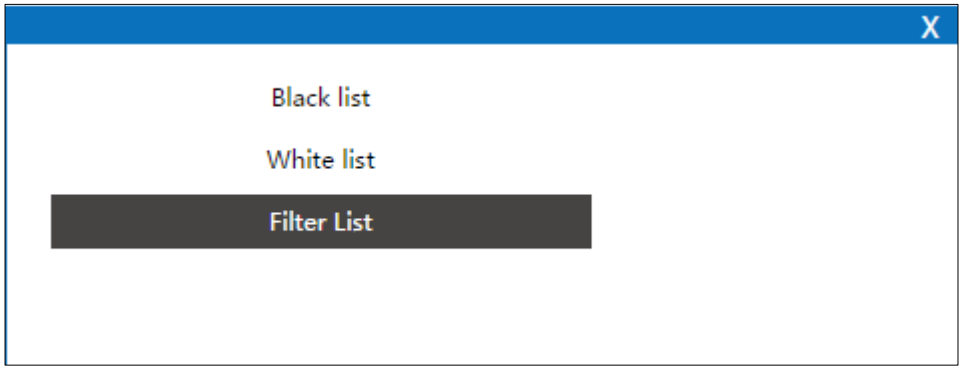
The main element configuration description of black/white list of IP address interface:

Interface Element	Discription
Equipment name	The device name of client in the list. Note: • Click “add” to add device to list manually. • Click “Filters rule” button, you can switch current list between black List, white List and undecided list, to filter the Client device.
IP	IP address of client in the list.
Operation	Edit device information.

Interface Description 3: Filter Rule

Click "Filter rules" button for list switching.

The filter rules interface as follows:



The main element configuration description of filter rules:

Interface Element	Discription
Black List	The client is prohibited from accessing the WAN list.
White List	The client is allowed to access the WAN list.
Filtered List	The pending list of client visiting WAN.

Note

Only the current list takes effect after switching the list via filter rules.

14 VPN Tunnel

VPN (Virtual Private Network) is a temporary, secure connection established through a public network (usually the Internet). It is a secure and stable tunnel passing through a chaotic public network. Adopting this tunnel to encrypt data can ensure the secure use of Internet.

14.1 GRE Settings

Generic Routing Encapsulation (GRE) protocol encapsulates data packets of certain network layer protocols (such as IP and IPX), so that these encapsulated data packets can be transmitted in another network layer protocol (such as IP). GRE adopts tunnel technology, which is the layer 3 tunnel protocol of VPN (Virtual Private Network).

Function Description

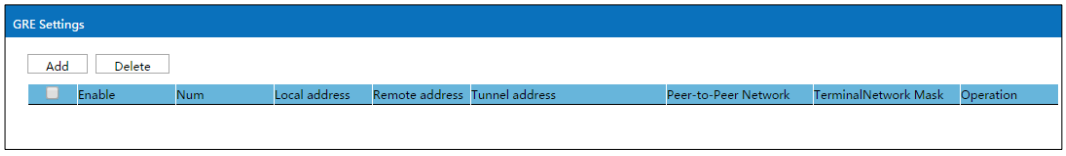
On the page of "GRE Settings", user can configure the relevant parameters of GRE.

Operation Path

Open in order: "VPN tunnel > GRE Settings".

Interface Description

GRE settings interface as follows:



The main elements configuration description of GRE settings interface:

Interface Element	Discription
☐	Check box of GRE settings entries, click to select all GRE settings entries.

Interface Element	Discription
Enable	GRE settings is enabled or not: • ON Status • OFF
Num	The serial number of GRE settings.
Local address	Local IP address.
Remote address	End IP address.
Tunnel address	IP address of local GRE tunnel.
Peer-to-Peer Network	Subnet IP of the end GRE, for example: 192.168.1.0.
Terminal Network Mask	Subnet mask of end GRE.
Operation	Edit: Modify the information of GRE settings entries.
Add	Click the "Add" button to add GRE settings in the pop-up window of "GRE Settings".
Delete	User can select the GRE settings information that needs to be deleted, and then click the “Delete Select” button in the upper right corner to delete the GRE settings.

14.2 PPTP Client Settings

Point to Point Tunneling Protocol (PPTP) is an enhanced security protocol. It supports multi-protocol virtual private network (VPN), which can enhance security through password authentication protocol (PAP), extensible authentication protocol (EAP) and other methods, and provide encrypted communication between PPTP client and server.

Function Description

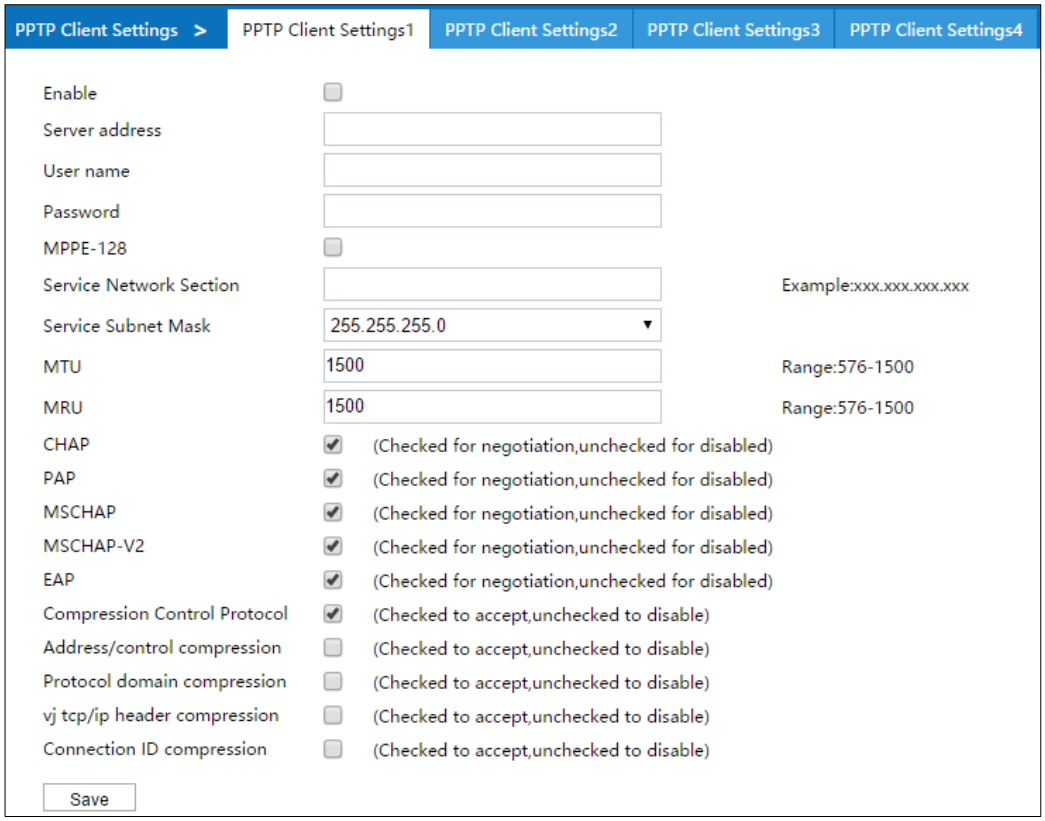
On the page of "PPTP Client Settings", user can configure the parameters related to PPTP client.

Operation Path

Open in order: "VPN tunnel > PPTP Client Settings".

Interface description: PPTP client1-4

The PPTP client1-4 settings interface is as follows:



The main elements configuration description of PPTP client1-4 settings interface:

Interface Element	Discription
Enable	PPTP Client Settings enable checkbox, check to enable the PPTP client settings function.
Server Address	IP address of PPTP server
User name	User name allowed by PPTP server
Password	Password corresponding to the user name allowed by PPTP server.
MPPE	Functional enablement checkbox of MPPE (Microsoft Point-to-Point Encryption) protocol, click to enable MPPE encryption function.
Service Network Section	Subnet segment of the PPTP server.
Service Subnet Mask	Drop-down box of subnet mask of the PPTP server.
Advanced Parameters	Click advanced parameters checkbox, the advanced parameters configuration will be displayed.
MTU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.

Interface Element	Discription
MRU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.
CHAP	Authentication allows the use of Challenge Handshake Authentication Protocol (CHAP).
PAP	Authentication allows the use of unencrypted keyword (PAP).
MSCHAP	Authentication allows the use of Microsoft CHAP Protocol.
MSCHAP-V2	Authentication allows the use of Microsoft CHAP V2 Protocol.
EAP	Authentication uses the Extensible Authentication Protocol (EAP).
Compression Control Protocol	Compression Control Protocol (CCP) is responsible for configuring and negotiating which compression algorithm to use on both ends of a PPP link.
Address/Control Compression	PPTP compresses address/control field of PPP frame.
Protocol domain Compression	PPTP compresses the upper-layer protocol fields carried by PPP frame.
Vj tcp/ip header compression	PPTP adopts Van Jacobson TCP/IP header compression algorithm, compresses the message header of upper-layer protocol TCP/IP fields carried by PPP frame.
Connection ID compression	PPTP compresses PPP frame ID.

14.3 PPTP Server Settings

Function Description

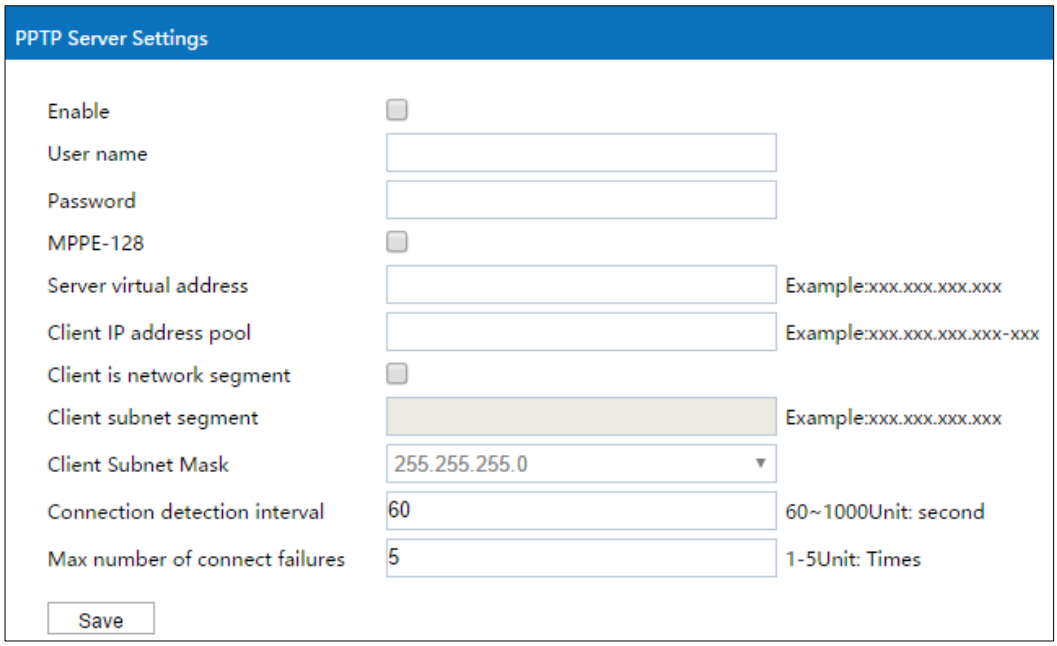
On the page of "PPTP Server Settings", user can configure the parameters related to PPTP server.

Operation Path

Open in order: "VPN tunnel > PPTP Server Settings".

Interface Description

The PPTP server settings interface is as follows:



The main elements configuration description of PPTP server settings interface:

Interface Element	Discription
Enable	PPTP Server Settings enable checkbox, check to enable the PPTP server settings function;
User name	User name provided by PPTP to the client for connection.
Password	Password corresponding to the user name provided by PPTP to the client for connection
MPPE	Functional enable checkbox of MPPE (Microsoft Point-to-Point Encryption) , click to enable MPPE encryption function.
Server virtual address	Virtual IP address of PPTP server.
Client IP address pool	IP address pool range assigned to the client, the format is: xxx.xxx.xxx.xxx-xxx.
Client is network segment	“Client is network segment “enablement checkbox, it allows the router whose subnet is the network segment to connect as a client and access the PPTP VPN server. Click the right button for ON and OFF switching. • ON: Enable the function of the client as network segment, and input the subnet segment and mask of the client; • OFF: Disable the function of client as network segment.
Client subnet segment	Set the network segment that allows the client to access,

Interface Element	Discription
	and use it with the client as the network segment. Note: This input box can only be entered after enabling the function of client as the network segment.
Client Subnet Mask	Drop-down box of subnet mask of the PPTP client. Note: This input box can only be entered after enabling the function of client as the network segment.
Connection detection interval	Detect the interval of connection, the default value is 60, unit: second.
Max number of connect failures	Detect the maximum number of failed connections. The default value is 5.

14.4 L2TP Client Settings

Layer 2 Tunneling Protocol (L2TP) is an industry-standard Internet tunneling protocol. Its functions are roughly similar to those of PPTP protocol. It can also encrypt the network data flow. There are some differences between the two protocols: For example, PPTP requires the network to be an IP network, L2TP requires a point-to-point connection for data packets; PPTP uses a single tunnel, L2TP uses multiple tunnels; L2TP provides header compression and tunnel authentication, but PPTP does not support.

Function Description

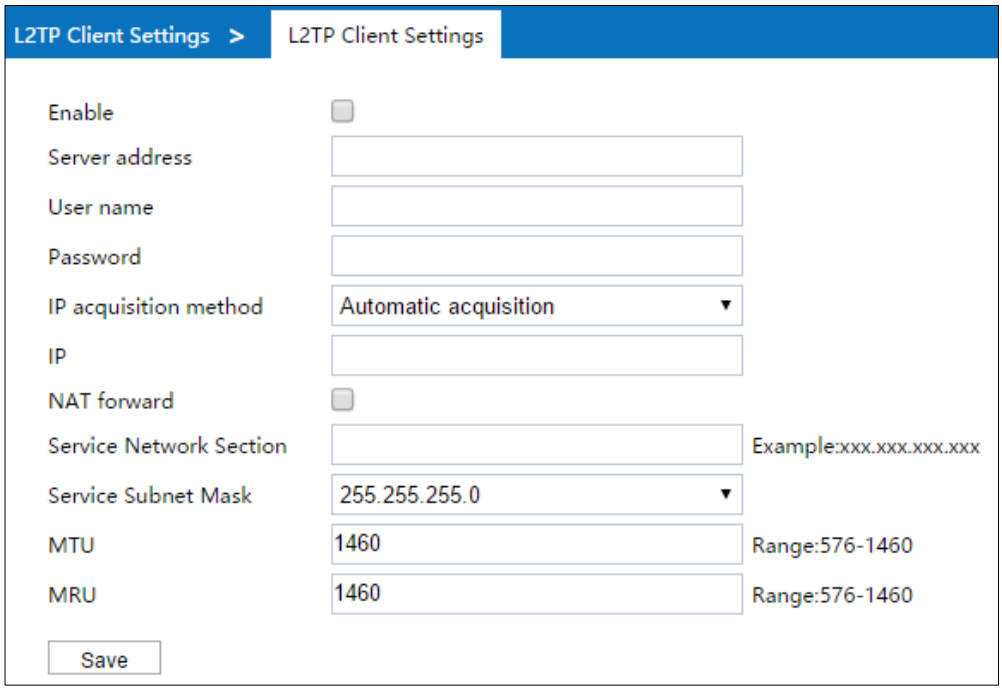
On the page of "L2TP Client Settings", user can configure the parameters related to L2TP client.

Operation Path

Open in order: "VPN tunnel > L2TP Client Settings".

Interface Description

The L2TP client settings interface is as follows:



The main elements configuration description of L2TP client settings interface:

Interface Element	Discription
Enable	L2TP Client Settings enable checkbox, check to enable the L2TP client settings function.
Server Address	IP address of L2TP server
User name	User name allowed by L2TP server.
Password	Password corresponding to the user name allowed by L2TP server.
IP Acquisition Method	Acquisition mode of L2TP clients IP address, options are as follows: • Automatic acquisition • Local IP
ip	When “IP acquisition mode” is “Local IP”, the local IP address of the item will be displayed, and the IP address format is xxx.xxx.xxx.xxx.
NAT forward	Enablement checkbox of NAT(Network Address Translation), check to enable NAT forwarding. All data flows of client are forwarded through the VPN server.
Service Network Section	User name provided by L2TP to the client for connection
Service Subnet Mask	Password corresponding to the user name provided by L2TP to the client for connection

Interface Element	Discription
MTU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.
MRU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.

14.5 L2TP Server Settings

Function Description

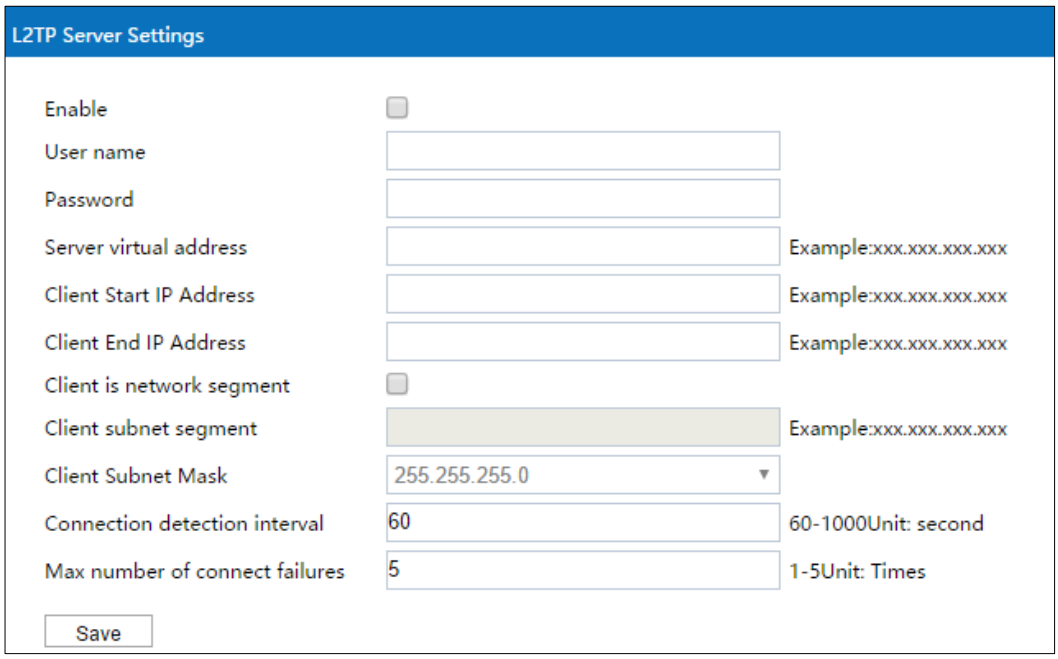
On the page of "L2TP Server Settings", user can configure the parameters related to L2TP server.

Operation Path

Open in order: "VPN tunnel > L2TP Server Settings".

Interface Description

The L2TP server settings interface is as follows:



The main elements configuration description of L2TP server settings interface:

Interface Element	Discription
Enable	L2TP Server Settings enable checkbox, check to enable the L2TP server settings function;

Interface Element	Discription
User name	User name provided by L2TP to the client for connection
Password	Password corresponding to the user name provided by L2TP to the client for connection
Server virtual address	Virtual IP address of L2TP server
Client Start IP address	Minimum start IP address of L2TP client
Client End IP Address	Maximum end IP address of L2TP client
Client is network segment	"Client subnet segment" enable checkbox. It allows the router whose subnet is the network segment to connect as a client and access the L2TP VPN server.Click to enable the function of the client as network segment.After enabled, the subnet segment and mask of the client can be input.
Client subnet segment	Set the network segment that allows the client to access, and use it with the client as the network segment. Note: This input box can only be entered after enabling the function of client as the network segment.
Client Subnet Mask	Drop-down box of subnet mask of the L2TP client. Note: This input box can only be entered after enabling the function of client as the network segment.
Connection detection interval	Detect the interval of connection, the default value is 60, unit: second.
Max number of connect failures	Detect the maximum number of failed connections. The default value is 5.

14.6 IPsec

The Internet Protocol Security (IPsec) protocol suite is a series of protocols developed by the Internet Engineering Task Force (IETF) that provides high-quality, interoperable, cryptographic-based security for IP packets. The specific communication parties can ensure the privacy, integrity, authenticity and anti-replay of the datagram during transmission on the network through encryption and data source authentication at the IP layer.

- Confidentiality refers to the encryption and protection of user data and is transmitted in the form of cipher text.

- Data integrity refers to the authentication of received data, which can determine whether a message has been tampered with.
- Anti-replay refers to preventing an attack that malicious user repeatedly transmits captured packet, that is, the receiver rejects old or duplicate packets.

Function Description

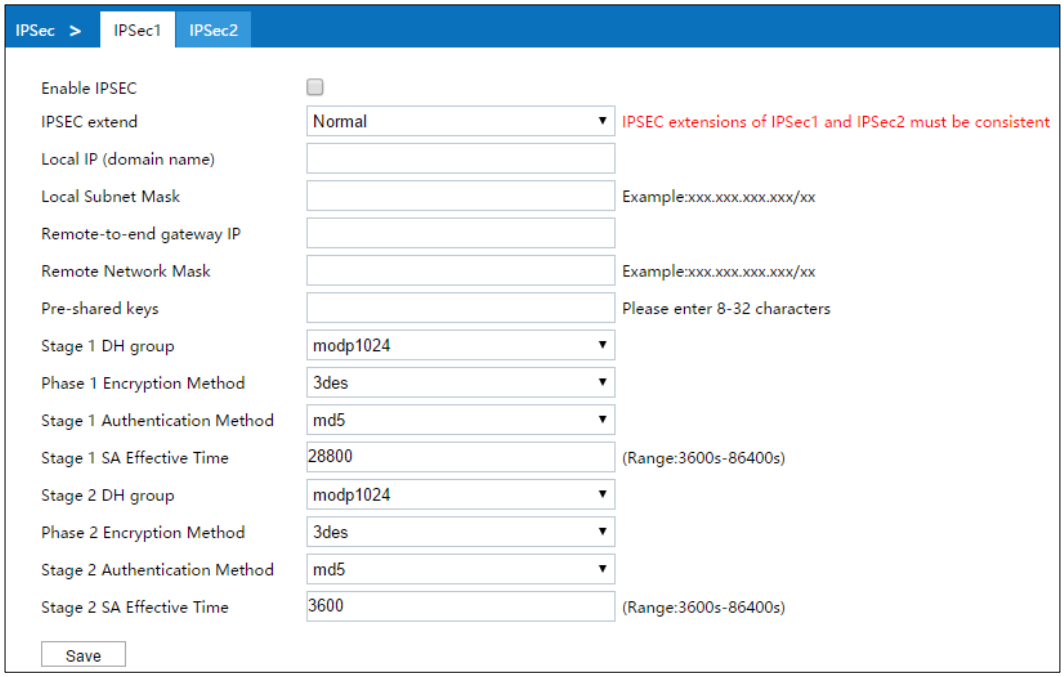
On the page of "IPsec", user can configure the relevant parameters of IPsec.

Operation Path

Open in order: "VPN tunnel > IPsec".

Interface Description

IPsec settings interface as follows:



The main elements configuration description of IPsec settings interface:

Interface Element	Discription
Enable IPSEC	IPSec Settings enable checkbox, check to enable IPSec settings function.
IPSEC extend	Drop-down box of IPSEC extension, options as follows: • Normal: Regular IPSEC; • GRE: GRE over IPSEC, GRE encapsulation based on IPSEC encryption; • L2TP: GRE over L2TP, L2TP encapsulation based on IPSEC encryption.
Local IP (domain name)	IP address or domain name of the local external network

Interface Element	Discription
	port
Local Subnet Mask	The local subnet and mask of the router, for example: 192.168.4.0/24.
Remote-to-end gateway IP	External network port IP of the opposite end
Remote Network Mask	Protected subnet and subnet mask of the opposite IPsec end , for example: 192.168.4.0/24.
Pre-shared keys	• Unicode string that verifies the IPsec connection.
Stage 1 DH group	• Stage 1 DH exchange algorithm, options as follows: • modp768 • modp1024 • modp1536
Phase 1 Encryption Method	Phase 1 encryption algorithm, options as follows: • 3des • aes128 • aes192
Phase 1 Authentication Method	Stage 1 Authentication Method, options as follows: • md5 • sha • sha256 • sha384 • sha512
Stage 1 SA Effective Time	Stage 1 SA survival time, unit is second and default is 28800.
Stage 2 DH group	• Stage 2 DH exchange algorithm, options as follows: • modp768 • modp1024 • modp1536
Stage 2 Encryption Method	Phase 2 encryption algorithm, options as follows: • 3des • aes128 • aes192
Stage 2 Authentication Method	Stage 2 Authentication Method, options as follows: • md5 • sha

Interface Element	Discription
	• sha256 • sha384 • sha512
Stage 2 SA Effective Time	Stage 2 SA survival time, unit is second and default is 3600.

15 System Management

15.1 Device Alias

Function Description

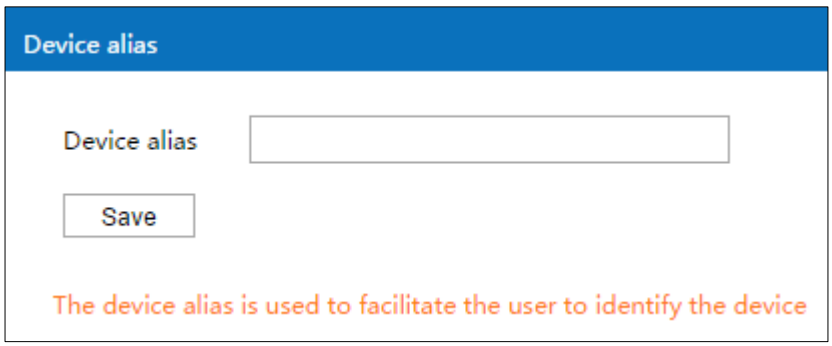
On the “Device Alias” page of system tool, user can set the device alias.

Operation Path

Please open in order: "System Management > Device Alias".

Interface Description

The Device Alias interface is as follows:



Configuration of the main elements of the device alias interface:

Interface Element	Discription
Device Alias	Set the name of the device. The device alias is used to facilitate user identification of the device.
Save	Click “Save” button to save device alias.

15.2 Time Settings

Function Description

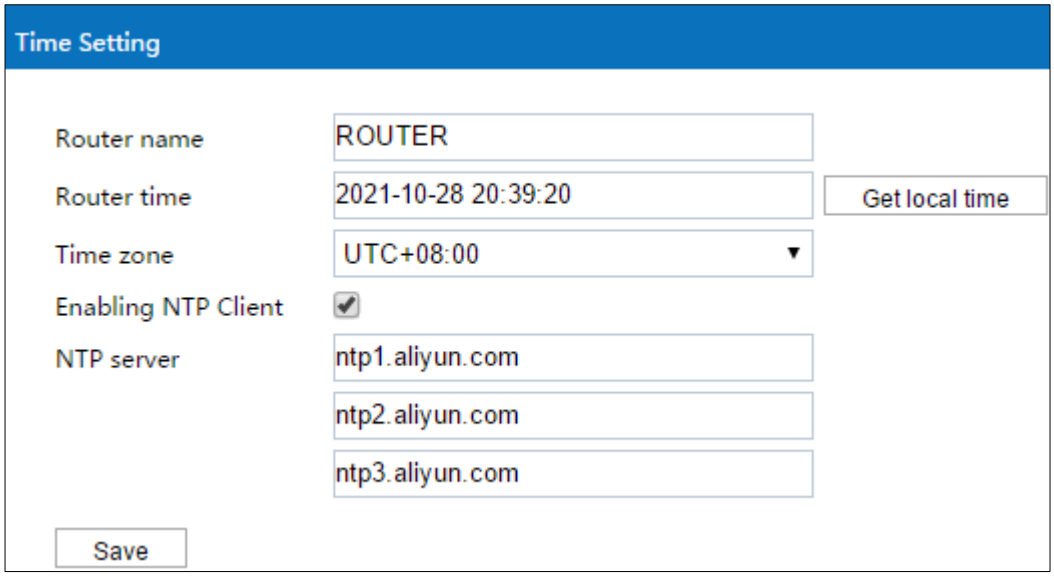
On the page of "Time Setting", user can configure time-related parameters information.

Operation Path

Open in order: "System manage > Time setting".

Interface Description

Time setting interface as follows:



The main elements configuration description of time settings interface:

Interface Element	Discription
Router name	The name of the router.
Router time	The time of the router, the format is: year-month-day hour: minute: second.
Get local time	Click the button of Get local time to synchronize the local time with the router.
Time Zone	Drop-down box of time zone, user can choose according to their demands.
Enabling NTP Client	NTP Client Settings enable checkbox, check to enable the NTP client function to synchronize the time of the server with the client.

Interface Element	Discription
NTP server	The address of the server that needs to be synchronized. Note: When there are multiple candidate NTP clients, the default is the first one. The higher the order, the higher the priority.

15.3 Access Settings

Function Description

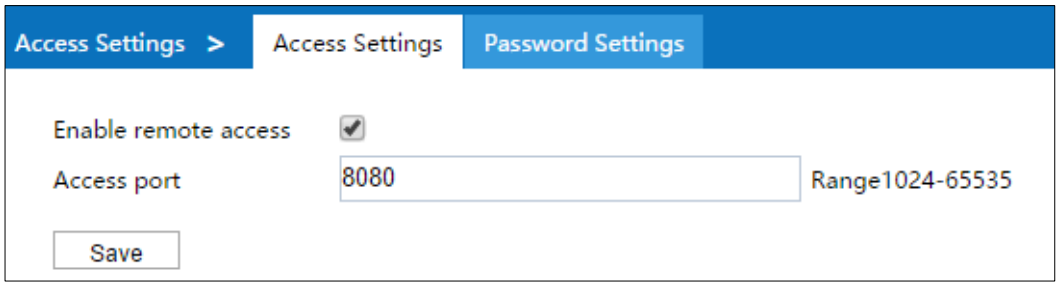
On the page of "Access settings", user can enable remote access and modify the username and password for accessing the device.

Operation Path

Open in order: "System manage > Access settings".

Interface Description 1: Access Settings

Access settings interface as follows:

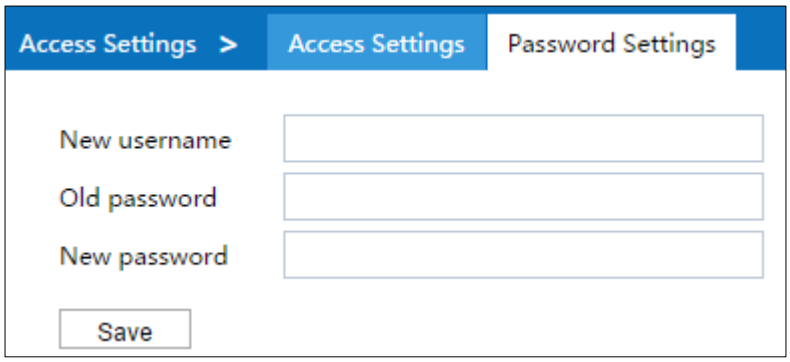


The main elements configuration description of access settings interface:

Interface Element	Discription
Enable remote access	Remote access enable checkbox, check to enable remote access, the user can access the device through the HTTP/HTTPS protocol on the external network.
Access port	Port number of remote access, the port number defaults to 8080. Note: Ensure the consistency of access port when accessing the device through a browser.

Interface Description 2: Password Settings

Password settings interface as follows:



The main elements configuration description of password settings interface:

Interface Element	Discription
New username	New username settings of the device. Note: Username and password are composed of capital and lower-case letters and numbers.
Old password	The login password used by the current device. Note: The username and password of the device are both admin by default.
New password	New password settings of the device. Note: Username and password are composed of capital and lower-case letters and numbers.

15.4 Timed Restart

Function Description

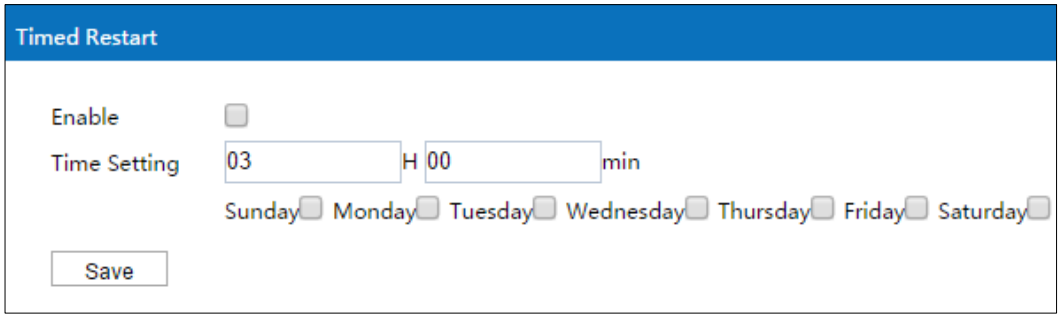
On the page of "Timed restart", user can configure the time for the device to automatically restart.

Operation Path

Open in order: "System manage > Timed restart".

Interface Description

The timed restart interface as follows:



The main elements configuration description of timed restart interface:

Interface Element	Discription
Enable	Timed Restart enable checkbox, check to enable Timed Restart function.
Time setting	Device restart time and date settings. When the set time is the same as the router time, the device will automatically restart.

15.5 Backup Recovery

Function Description

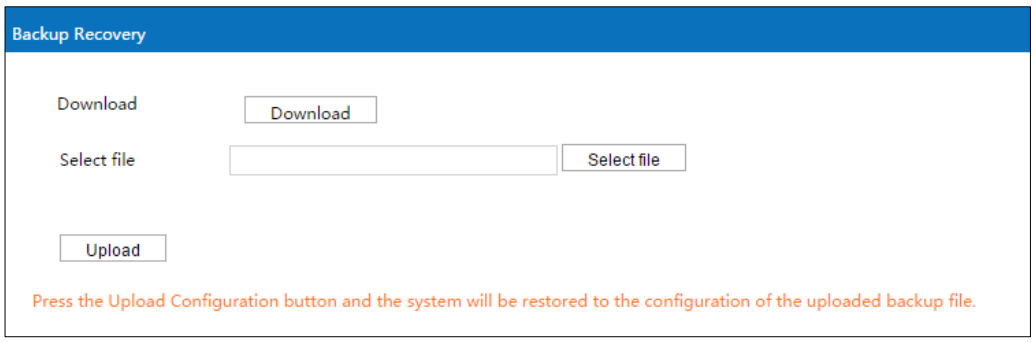
On the page of "Backup Recovery", user can select files for uploading configuration.

Operation Path

Open in order: "System manage > Backup Recovery".

Interface Description

The backup recovery settings interface as follows:



The main elements configuration description of backup recovery settings interface:

Interface Element	Discription
Download	Click “download” button, you can download the current configuration “backup.file”.
Select file	The "Select file" button allows user to select the configuration file for the host backup.
Upload	Click “ Upload configuration”, users can upload the selected file to device.

15.6 Log Manage

Function Description

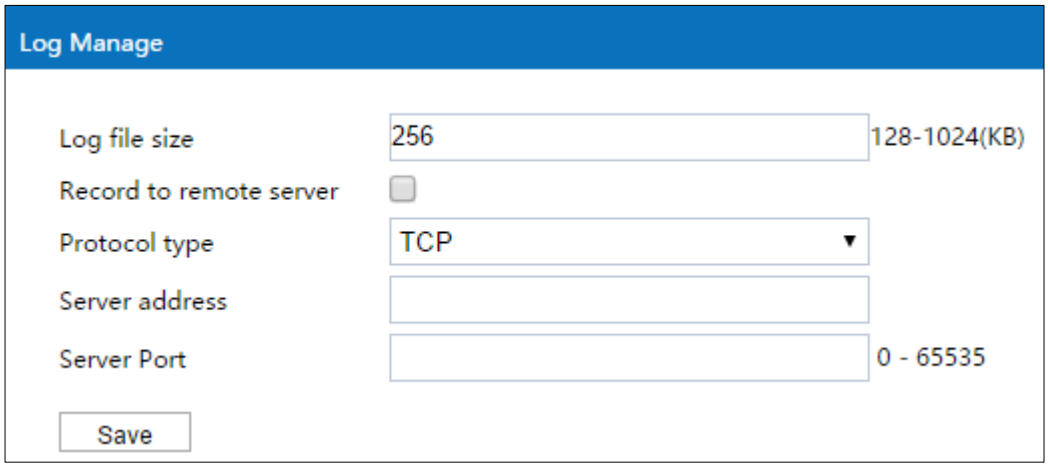
On the page of "Log manage", user can record the log files to the remote server.

Operation Path

Open in order: "System manage > Log manage".

Interface Description

The log management interface as follows:



The main elements configuration description of log management interface:

Interface Element	Discription
Log file size	Set the size of the log file, the default is 256
Record to remote server	Record to remote server enable checkbox, check to enable the function of recording to remote server to record log files to the remote server.
Protocol type	Drop-down box of the protocol type used by the record to

Interface Element	Discription
	remote server, options as follows: • TCP; • UDP.
Server Address	IP address information of the remote server
Server Port	Port number of the remote server.

15.7 Firmware Upgrade

Function Description

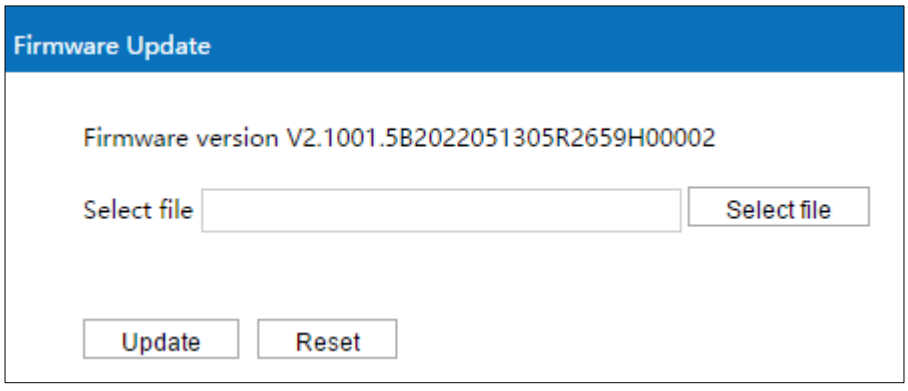
On the "Firmware Upgrade" page, user can update the device system program via firmware upgrade.

Operation Path

Open in order: "System manage > Firmware update".

Interface Description

System upgrade interface as follows:



The main element configuration description of Firmware Upgrade interface:

Interface Element	Discription
Firmware version	Software version used by current device.
Select file	Click "Select file" to select local upgrade file of the host. Note: Please select the program version that is compatible with the current hardware during upgrading.
Update	The button of "Update" to upgrade the device program. Notice: • It takes a while during the upgrade process. Do not power off

Interface Element	Discription
	the device. • After a successful upgrade, the configuration of the device will remain unchanged and the firmware version information will be changed.

15.8 System Settings

Function Description

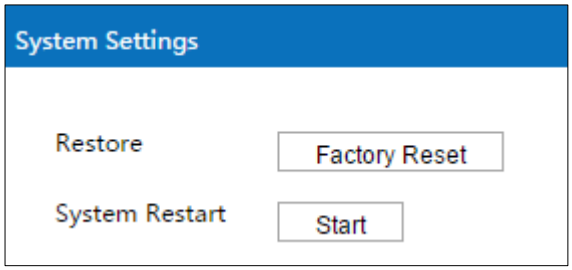
On the “System Settings” page, you can download the current configuration files, restore factory settings or reboot the device.

Operation Path

Open in order: “System Management > System Settings”.

Interface Description

System settings interface is as follows:



The main elements configuration description of system settings interface:

Interface Element	Discription
Restore	Click “Factory Reset” button, then click "OK” button to confirm restoring factory defaults.
System Restart	Click "Start” button, the click "OK” button to confirm rebooting system, and the device starts to reboot automatically.

16 Diagnostic Tools

16.1 System Log

Function Description

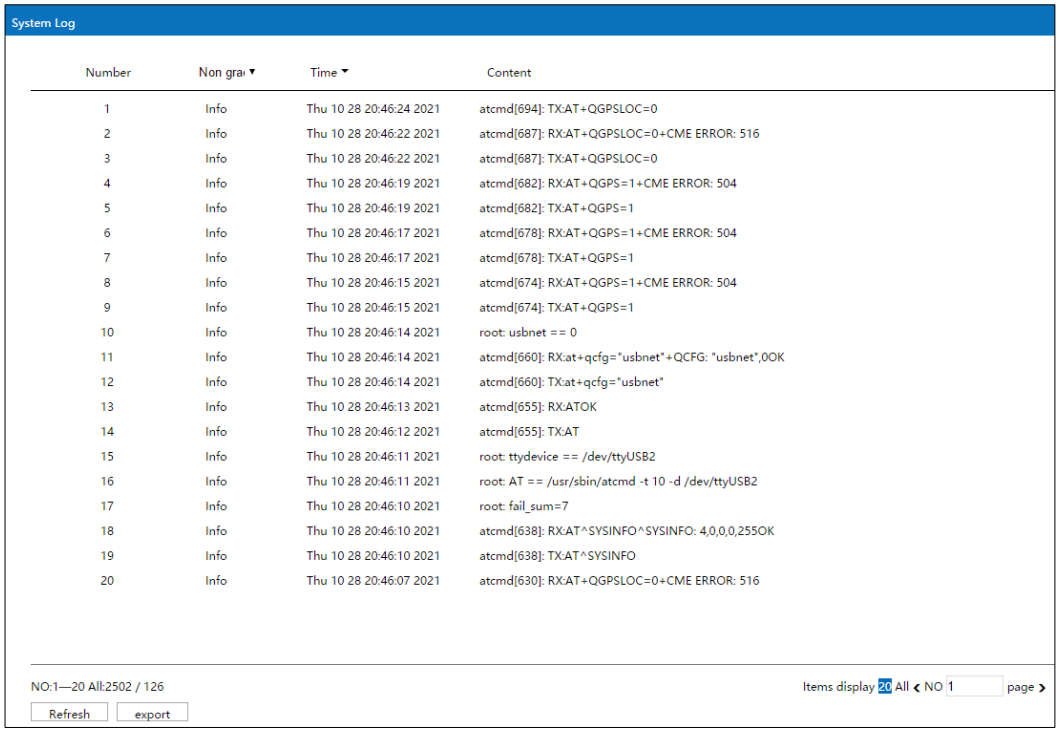
On the page of "System log", user can view the device system logs.

Operation Path

Open in order: "Diagnostic tools > System log".

Interface Description

The system log interface is as follows:



The main elements configuration description of system log interface:

Interface Element	Discription
Serial number	Log messages display sequence.
None grading	User can select the category of log to display specific log information. Optional values: • None grading: all information; • Error: error messages; • Warning: warning messages.
Time	The date and time filter button for log information. Note: Click the "Time" button to filter the start date and end date.
Content	A detailed description of the log contents.
Items display	"Items display" button, log information display mode, options as follows: • 20: Display 20 log messages per page; • All: Single page displays all log information.
Refresh	Click the "Refresh" button to regain the latest log information of the device.
Export	Click the "Export" button to export the log information in the format of ".txt".

16.2 Ping Test

Ping belongs to a communication protocol and is part of the TCP/IP protocol. User can adopt the ping command to check whether the network is connected, which can help us analyze and determine network faults.

Function Description

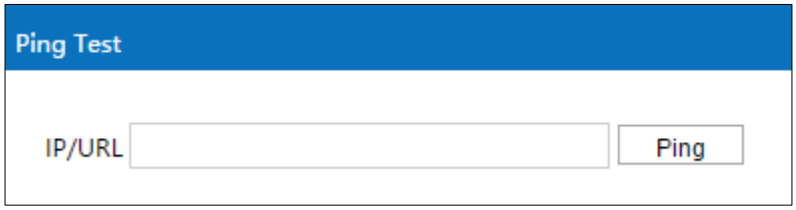
On the page of "Ping test", user can detect whether the target host can be connected.

Operation Path

Open in order: "Diagnostic tools > Ping test".

Interface Description

The Ping test interface as follows:



The main elements configuration description of Ping test interface:

Interface Element	Discription
IP/URL	Target IP/URL address information to be detected.
Ping	Click the “Ping” button to start the test, and the test result is displayed below.

16.3 Route Tracking

Route Tracking is a route-tracking utility that determines the path taken by an IP datagram to access a destination. The Route Tracking command uses the IP Time to Live (TTL) field and ICMP error messages to determine the route from one host to other hosts on the network.

Function Description

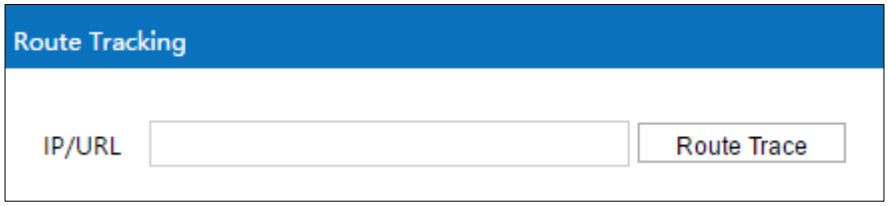
On the page of "Route Tracking", user can perform route tracking for the target host.

Operation Path

Open in order: "Diagnostic tools > Route tracking".

Interface Description

The route tracking interface is as follows:



The main elements configuration description of route tracking interface:

Interface Element	Discription
IP/URL	Destination IP/URL address that requires route tracking.

Interface Element	Discription
Route Tracking	Click the "Route Trace" button to start tracking, and the test results are displayed below.

17 FAQ

1. **Why is the signal strength very good, but the throughput is very low?**

   Sometimes, during the throughput test, it is found that the signal strength of connection is very strong (> -30dbm), but the tested throughput is very low, and even disconnection occurs. A common misconception is that the stronger the signal, the better the quality. This is not true. Signal quality and signal strength are not positively correlated. The signal strength has a saturation RSSI. When the signal strength is above this threshold, the received signal is excessively saturated and the receiver is unable to demodulate, leading to a significant decrease of throughput and even disconnection. This problem can be solved by reducing the AP power or increasing the attenuation between the AP and the client.

2. **Why do some 5G client devices fail to scan the 5G SSID of AP?**

   5G has three frequency bands: high, medium and low. Different countries support different frequency bands. Some support two of them and some only support one of them. Therefore, when AP works in the frequency band that the client does not support, the client cannot scan the SSID of AP, and another client that supports this frequency band can scan it. Another possible reason is the problem mentioned in 4.1, that is, the signal is too strong, which will also lead to the failure to scan the SSID. This situation usually occurs when the feeder directly connects the AP to the client without adding an appropriate attenuator.

3. **Why is the near throughput of an outdoor AP worse than an indoor AP?**

   This is determined by the nature of the outdoor AP antenna. The antenna of outdoor AP is different from that of indoor AP. Its advantage lies in long-distance transmission. It is a normal phenomenon that the throughput of an outdoor AP is

slightly worse than an indoor AP in the short distance transmission (within 50 meters).

4. What is a universal bridging?

Universal bridging is a way to bridge an AP and a client by creating a proxy forwarding mechanism. Instead of putting the wired network port and the wireless network port in the same bridge, it modifies the policy routing table to make all the host devices connected establish forwarding relationship with the wireless network port, and let the wireless port agent forward data packets, ARP and DHCP packets. In other words, it realizes the soft bridging between wireless port and wired port.

5. When should universal bridging and WDS be used?

General bridge and client mode use WDS to bridge with AP, but WDS does not have a standard protocol, different wireless chip manufacturers implement WDS in different ways, resulting in the WDS bridge of different manufacturers have serious compatibility problems, the phenomenon is unable to bridge or bridge can not communicate. Universal bridging has no compatibility issues, but due to its nature, is not suitable for networks involving routing learning (such as OSPF networks) and is only suitable for simple application scenarios. Therefore, WDS is preferred if WDS is compatible and universal bridging is preferred if WDS is not compatible. At present, the company's self-developed wireless products are all Qualcomm solutions. They have no compatibility problems. Therefore, if both the AP end and the client are our self-developed products, WDS can be used.

6. Why does throughput not improve after 2.4G is changed from 20M to 40M?

In an environment with severe interference, if 2.4G is changed from 20M to 40M, the throughput may not improve, or even get worse. Because there are only 13 channels in 2.4G, each channel is 5M, and all the channels add up to 65M, while a signal of 40M occupies 40M. Therefore, if there are 2.4G signals of similar channels nearby, serious interference problems will inevitably occur due to channel overlap, leading to the throughput failure. Therefore, in the environment with severe interference, 20M is recommended for 2.4G.

7. **How do I access a device when an Intranet IP is acquired dynamically but not connected to a DHCP server?**

   When the self-developed product fails to obtain the address allocated by the DHCP server within 1 minute, a default IP address will be set automatically. The IP address is 192.168.1.254, and you can use this address to access the device. When the device obtains the address allocated by the DHCP server, the default IP would be automatically overwritten.

18 Maintenance and Service

Since the date of product delivery, our company provides five-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's wireless AP, consumers can get help and solutions in the following ways:

- Internet Service;
- Service Hotline;
- Product repair or replacement;

18.1 Internet Service

More useful information and tips are available via our company website.

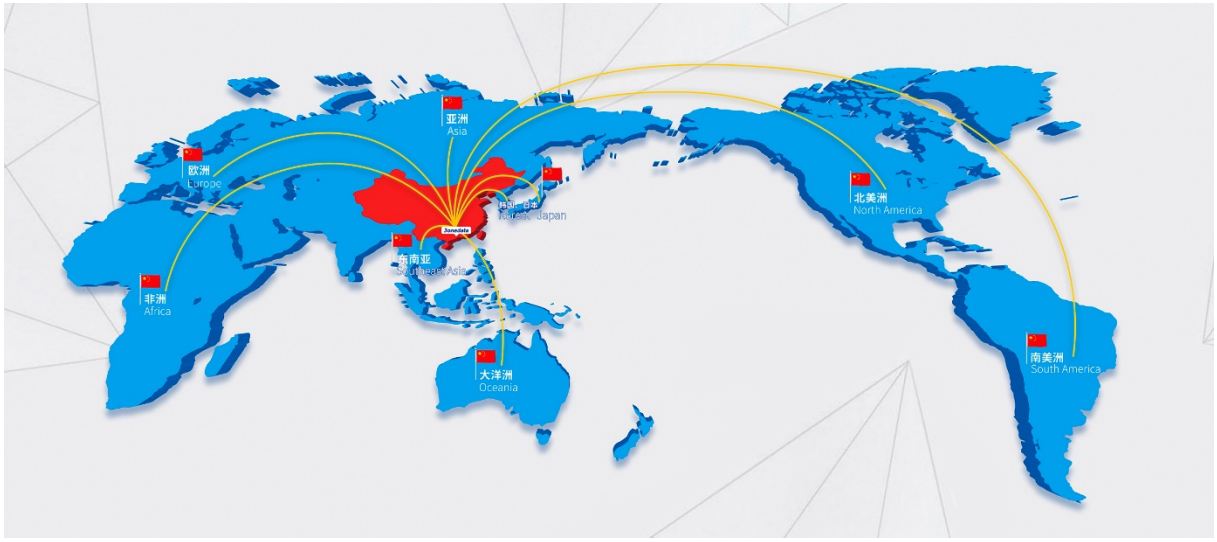
Website: http://www.3onedata.com

18.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you solve the product or usage problems ASAP. Free service hotline: +86-400-880-4496

18.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem. According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.



3onedata Co., Ltd.

Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen

Technology support: tech-support@3onedata.com

Service hotline: +86-400-880-4496

Official Website: http://www.3onedata.com