3onedata

IRT5300L Series
Industrial 4G Router
User Manual

Document Version: 01

Release Date: 2021-11-12

Trademark statement

3onedata , 3onedata and 

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

Note

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 Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

The Industrial 4G Router User Manual has introduced this series of routers:

- Product features
- Product network management configuration
- Overview of related principles of network management

Note
The screenshot reference model for this manual is 1 RS-232/485/422 serial port + 4 100M LAN ports + 1 100M WAN port. In addition to the supported number of ports, the interface functions and interface operations are the same.

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’.
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	Conduct a necessary supplements and explanations for the description of operation content.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

Revision Record

Version No.	Date	Revision note
01	11/12/2021	Product release

Content

1 Log in the Web Interface

1.1 WEB Browsing System Requirement

While using the industrial router, the system should meet the following conditions.

Hardware and software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 6.0 or above
Operating system	Windows XP/7/8/10

1.2 Setting IP Address of PC

The router default management is as follows:

IP Settings	Default Value
IP Address (LAN port)	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- 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.

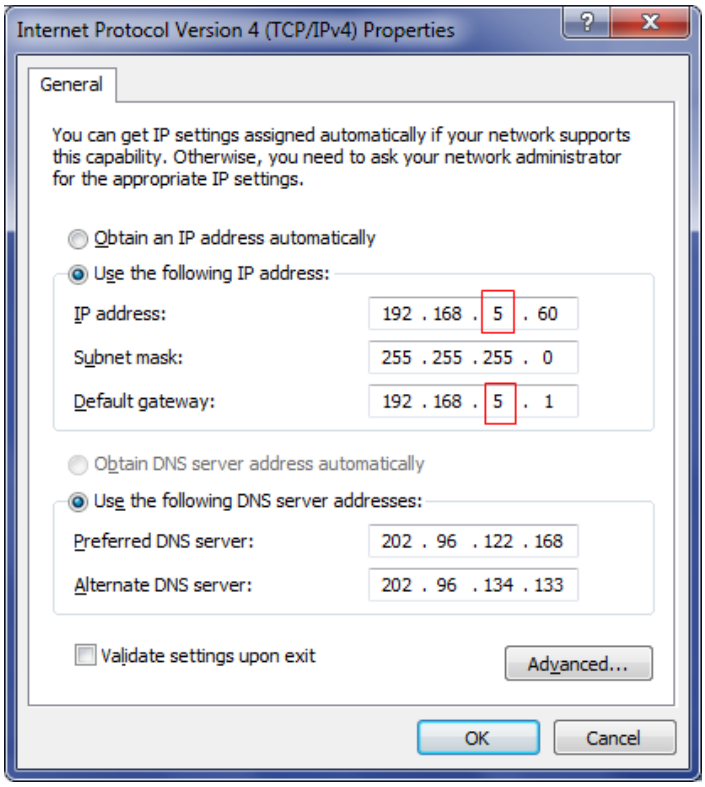
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

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.

1.3 Log in the Web Configuration Interface

Operation Steps

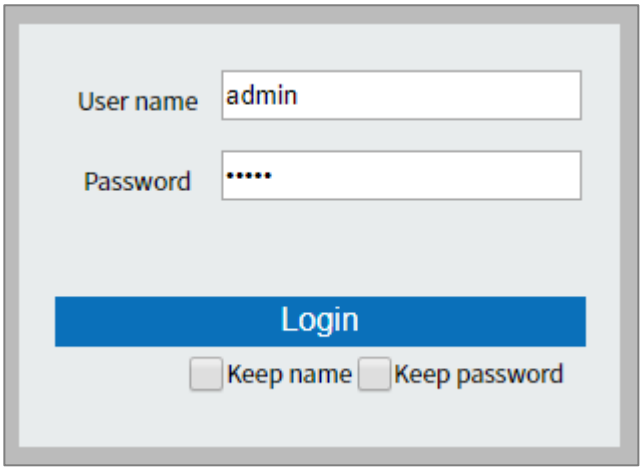
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 On the browser's address bar, type in the switch addresses "http://192.168.1.254 ".

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.
- Default user account has the administrator privileges.

Step 5 Click "Login".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.

Note
After login in the device, modify the switch IP address for usage convenience.

2 System Info

Function Description

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

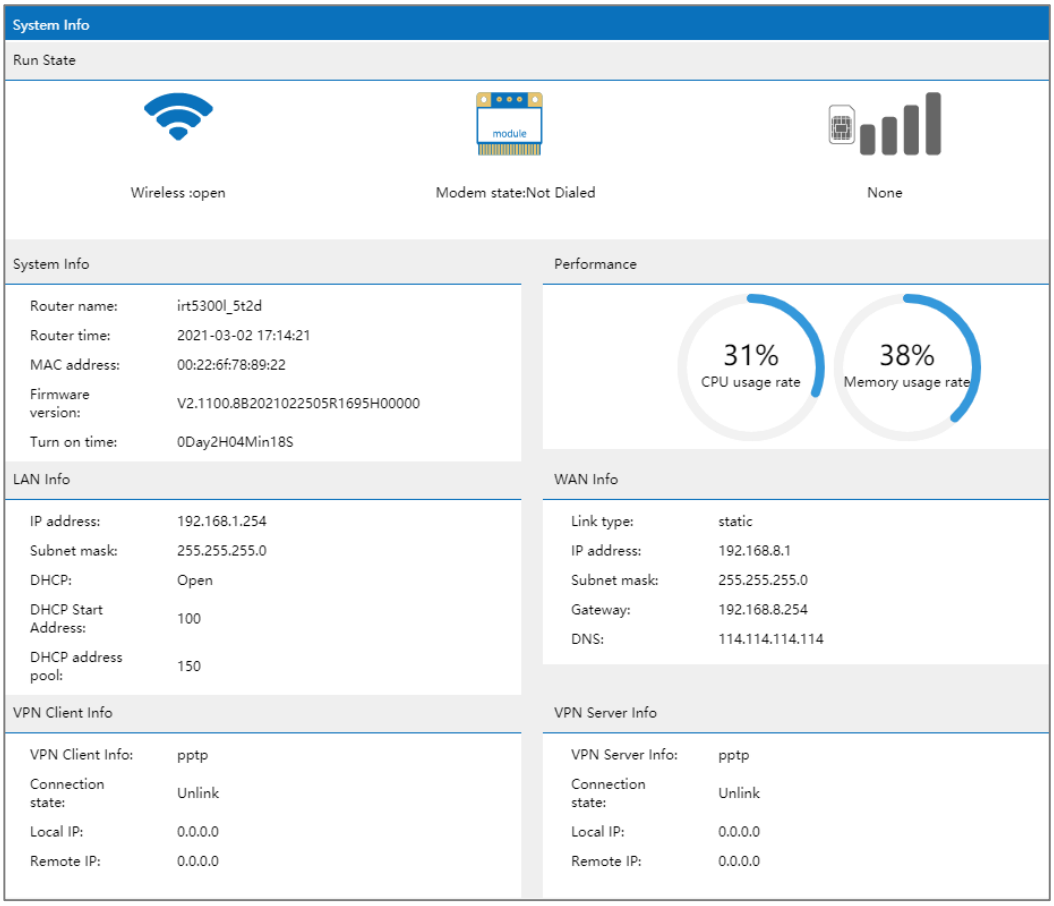
- System Information;
- Performance;
- LAN information;
- WAN information;
- VPN client information;
- VPN server information.

Operation Path

On the navigation bar, select "System information".

Interface Description

System information interface as follows:



The main element configuration description of state information interface:

Interface Element	Description
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 4G 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.
System Info	**System information bar**
Router Name	Device name.
Router Time	The current time displayed by router. Its format is Year-Month-Day Hour: Minute: Second.
Mac Address	The MAC address information of this device.
Firmware Version	Device firmware version.
Turn on Time	The run time after turning on the device
Performance	**The performance bar**

Interface Element	Description
CPU usage rate(%)	The usage rate of device CPU.
Memory usage rate (%)	The usage rate of device memory. Note: The performance of the device would be affected if the application consumes too much memory.
LAN info	**The LAN information bar**
IP Address	The IP address information of LAN.
Subnert Mask	The subnet mask information of LAN.
DHCP	DHCP Server Status: • Open • Disable
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 line type of WAN, which is 3G/4G by default
IP Address	The IP address information of WAN.
Subnert Mask	The subnet mask information of WAN.
Gateway	The gateway information of WAN
DNS	The DNS information of WAN
VPN Client Info	**The VPN client information bar**
VPN Client Info	Related information about VPN client. It displays related information when VPN client is enabled, otherwise it displays pptp by default.
Connection State	The connection state of VPN client: • Not connected • Connected
Local IP	The IP address of local client.
Remote IP	The IP address of remote server.
VPN Server Info	**The VPN server information bar**
VPN Server Info	Related information about VPN server. It displays related information when VPN server is enabled, otherwise it displays pptp by default.
Connection State	The connection state of VPN server: • Not connected

Interface Element	Description
	• Connected
Local IP	The IP address of local server.
Remote IP	The IP address of remote client.

3 Basic Network

3.1 WAN Network Settings

Function Description

On the “WAN Settings” page, user can set the connection type and parameter of WAN.

The connection types are as follows:

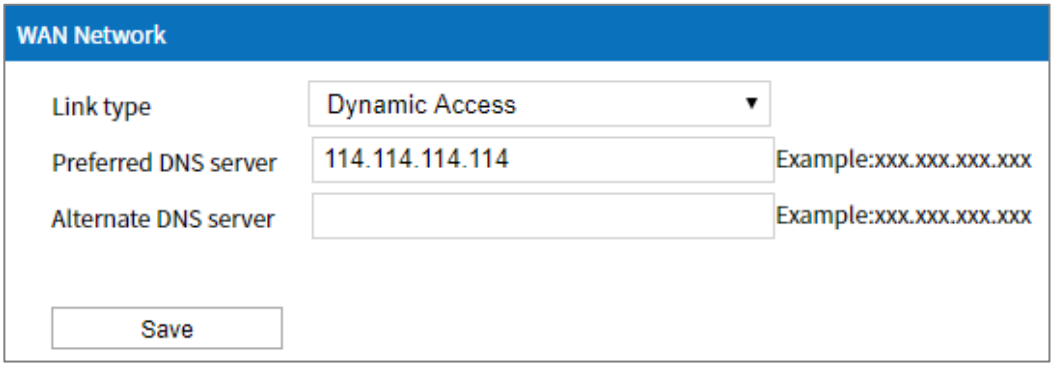
- Dynamic access: the WAN port of the device accesses network address information allocated by network provider or outer network automatically;
- Static address: configuring the network information of the device WAN port manually;
- PPPoE: implement PPPoE point-to-point protocol dial-up via wired network WAN port to access network;
- 3G/4G: connect to 3G/4G signal via SIM card to access Internet.

Operation Path

Click: “Basic Network > WAN Settings”.

Interface Description 1: Dynamic Access

Choose “Dynamic Access” in “Line Type”. The dynamic access interface as follows:

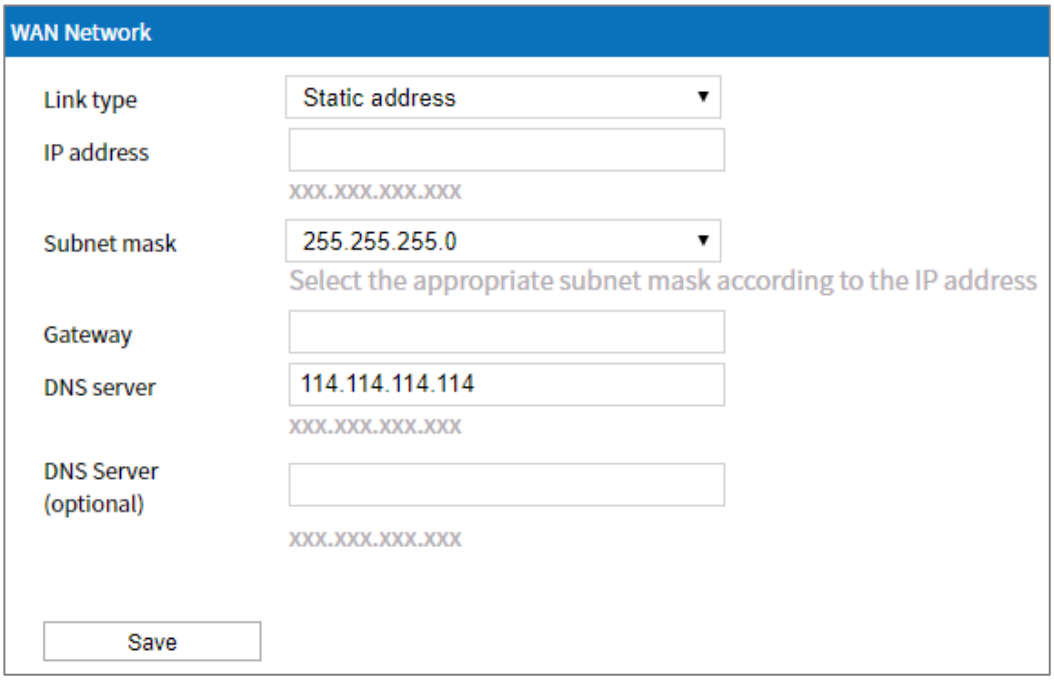


The main element configuration description of dynamic access interface:

Interface Element	Description
Link Type	Dynamic Access: 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: Static Address

Choose “Static address” in “Line type”. The static address interface as follows:



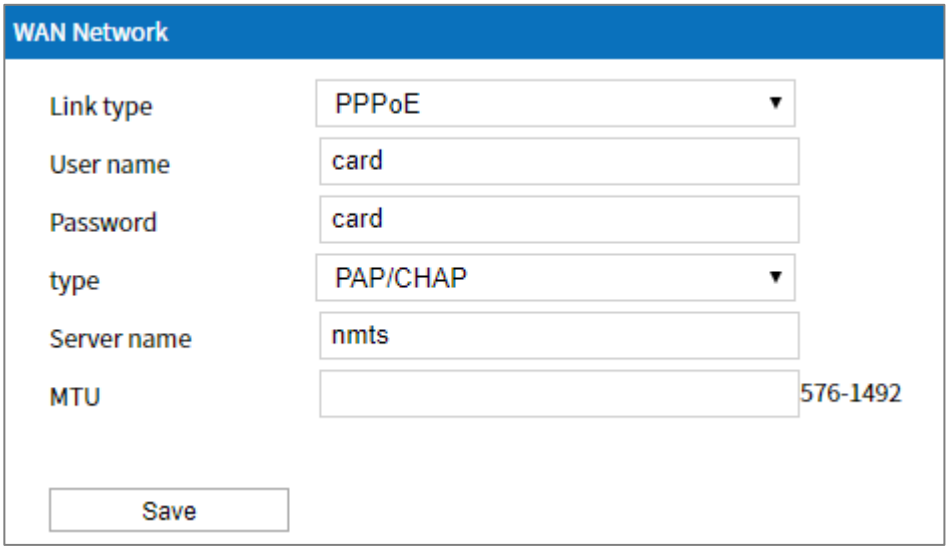
The main element configuration description of static address interface:

Interface Element	Description
Link Type	Static address: the network information configuration of device WAN port.
IP Address	The fixed IP address provided by network provider or extranet.
Subnet Mask	Drop-down list of netmask.
Gateway	The default gateway address provided by network provider or extranet.
DNS Server	The DNS server address provided by network provider or

Interface Element	Description
	extranet.
DNS Server (optional)	The backup DNS server address provided by network provider or outer network. This item can be skipped.

Interface description 3：PPPoE

Choose “PPPoE” in “Line type”. The PPPoE interface as follows:



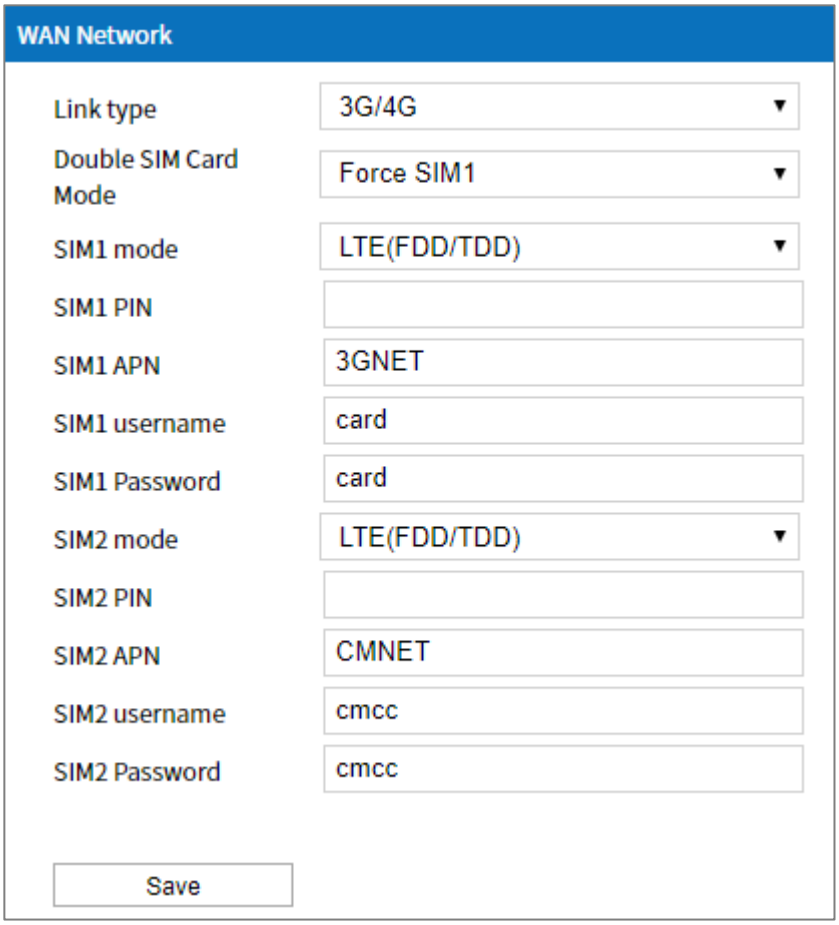
The main element configuration description of PPPoE interface:

Interface Element	Description
Link Type	PPPoE: realize Internet access via PPPoE 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.

Interface Element	Description
	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 576-1492 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.

Interface Description 4: 3G/4G

Choose “3G/4G” in “Line type”. The 3G/4G interface as follows:



The main element configuration description of 3G/4G interface:

Interface Element	Description

Interface Element	Description
Link Type	3G/4G: achieve 3G/4G network access via SIM card dial-up.
Double SIM card mode	In the drop-down list of double SIM card mode, user can choose specified SIM card. The options are: • Force SIM1 • Specified SIM2
SIM1 mode	The drop-down list of SIM1 mode. The options are: • LTE(FDD/TDD) • 3G(WCDMS/TD-SCDMA/HSPA) • 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. Notes: 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 mode. The options are: • LTE(FDD/TDD) • 3G(WCDMS/TD-SCDMA/HSPA) • 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. Notes: 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.

3.2 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

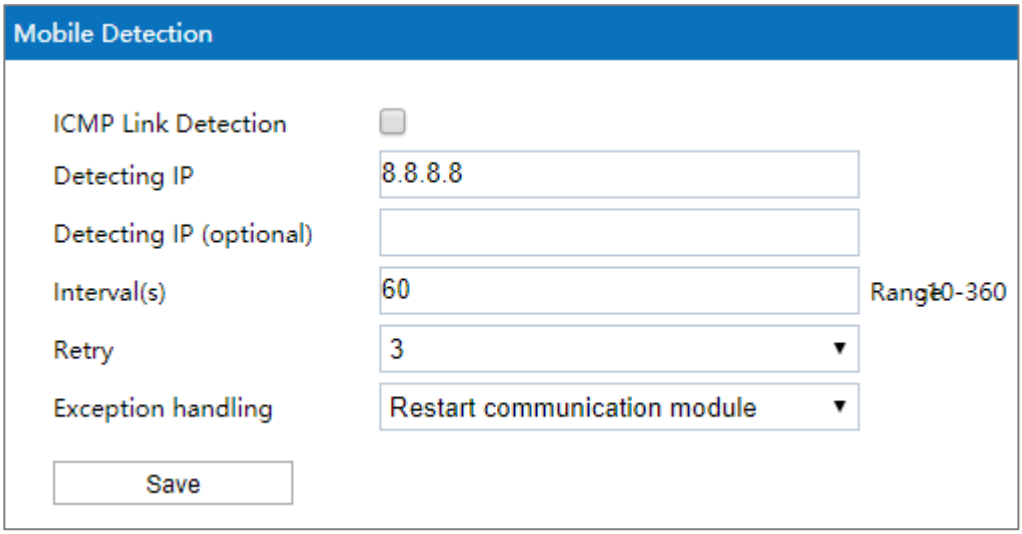
On the “Mobile Detection” page, user can detect the connection status of network and make corresponding operation.

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	Description
ICMP Link Detection	ICMP Link Detection checkbox, checking to turn on ICMP link detection function, which can detect network connection.
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 and defaults to 60. The value range is 10-360.
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.

Interface Element	Description
	The drop-down list of exception handling, options are: • Restart communication module; • Switch SIM card; • Reboot the system.

3.3 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

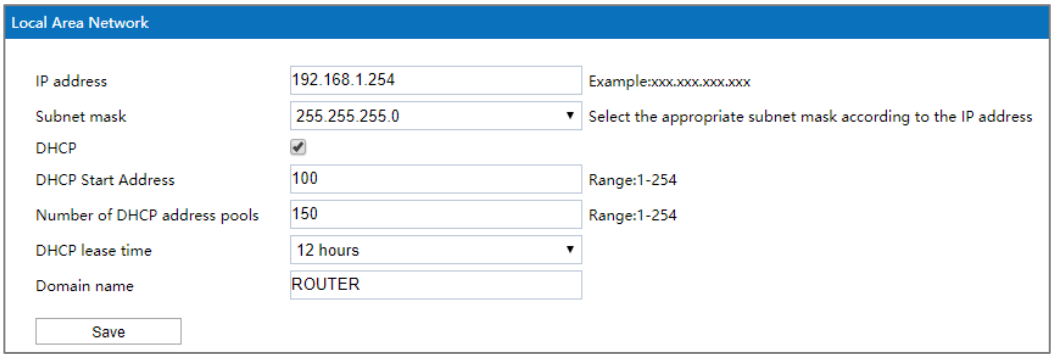
On the “Local Area Network” page, user can turn on DHCP server function and set relevant parameters of gateway.

Operation Path

Please open in order: “Basic Network > Local Area Network”.

Interface Description

The local area network interface as follows:



The main element configuration description of local area network interface:

Interface Element	Description
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	The minimum IP address host number allocated by DHCP

Interface Element	Description
Address	address pool. Value range is 1-254.
Number of DHCP Address Pools	The maximum IP address number allocated by DHCP address pool. Value range is 1-254.
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.

3.4 VLAN Settings

VLAN is Virtual Local Area Network. VLAN is the data switching technology that logically (note: not physically) divides the LAN device into each network segment (or smaller LAN) to achieve the virtual working group (unit).

VLAN advantages mainly include:

- Port isolation. Ports in different VLAN, even in the same switch, can't intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLAN can't directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. Changing the network user belongs to, don’t need to change ports or connection; only needs to change the software configuration.

That is, ports within the same VLAN can intercommunicate; otherwise, ports can't communicate with each other. A VLAN is identified with VLAN ID, and ports with the same VLAN ID belong to a same VLAN.

3.4.1 Port PVID Settings

Function Description

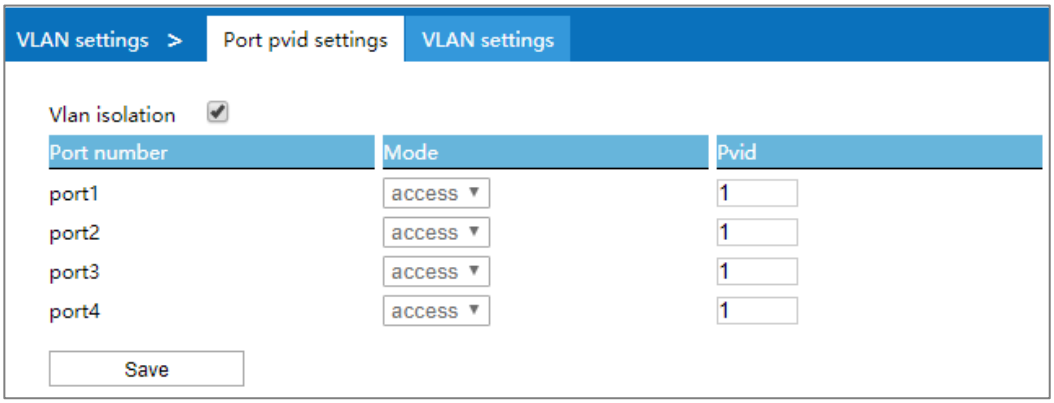
On the “Port PVID Settings” page, the port VLAN mode is access by default. You can configure the port VLAN ID: PVID.

Operation Path

Open in order: "Basic Network > VLAN Settings > Port pvid Settings".

Interface Description

Port PVID setting interface is as follows:



Main elements configuration description of port PVID settings interface:

Interface Element	Description
VLAN Isolation	VLAN isolation function check box, check it to enable VLAN port isolation.
Port Number	The corresponding port number of this device’s Ethernet port.
Mode	The port link type supported by the device is access: Port can only belong to 1 VLAN, which is generally used to connect user device. All default ports belong to access port.
Pvid	Port-base VLAN ID is the port-based virtual LAN ID number. For access mode, a physical port has one and only one PVID.

3.4.2 VLAN Settings

Function Description

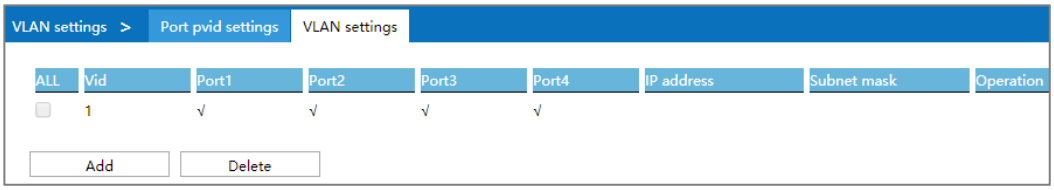
On the page of "VLAN Settings", user can configure the relevant parameters of VLAN.

Operation Path

Open in order “Main Menu> Basic Network > VLAN Configuration > VLAN Settings”.

Interface Description

VLAN settings interface is as follows:



The main element configuration description of VLAN configuration interface:

Interface Element	Description
All	VLAN entry radio box, you can check one or more VLAN entries for configuration.
Vid	Displays the PVID value set for the port.
Port1-4	Displays the ports included in this VLAN, and "√" is displayed below the included ports.
IP Address	Displays the IP address corresponding to this VLAN. Note: IP addresses of different VLANs cannot be in the same network segment.
Subnet mask	Displays the subnet mask corresponding to this VLAN.
Operation	Click "Edit" to modify the IP address and subnet mask of this VLAN. Note: When VID is 1, the corresponding IP address and subnet mask cannot be modified.
Add	Click "Add" button to add VID, IP address and subnet mask corresponding to VID. Note: To add the port corresponding to VID, you can modify it on the port PVID setting page.
Delete	You can check one or more VLAN configurations and click the "Delete selected" button to delete them.

3.5 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	Description
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.
User name	The user name applied from DDNS supplier.

Interface Element	Description
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.

3.6 Routing Table

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

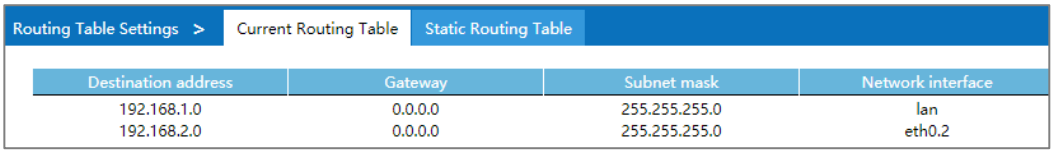
On the “Routing Table” page, user can set relevant information of routing table.

Operation Path

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

Interface Description 1: Current Routing Table

The current routing table interface as follows:

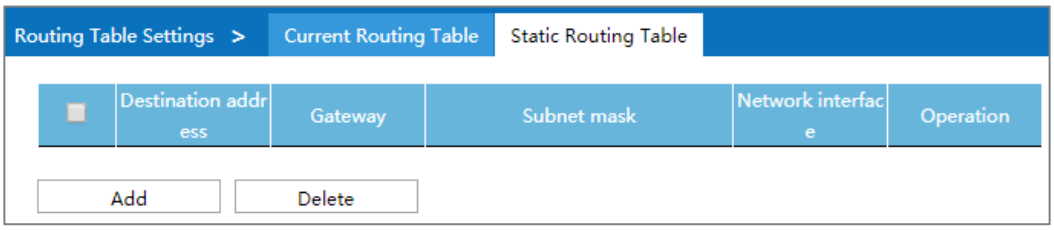


The main element configuration description of current routing table interface:

Interface Element	Description
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	Description
Destination Address	The destination IP address information of static routing
Gateway	The gateway information of static routing
Subnet mask	The subnet mask information of static routing: • 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 • 255.255.255.0 • 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

Interface Element	Description
Network interface	The network interface of static routing: • WAN • LAN
Operation	Edit: modify static routing table information.
Add	Click the “Add” button to add static routing in the pop-up window of “static routing.
Delete	Check the static routing information to be deleted, and then click the “Delete” button to delete them.

4 WLAN Settings

On the “WLAN Settings” page, user can create WiFi hotspot and manage WiFi user connection.

4.1 Basic Parameter Settings

Function Description

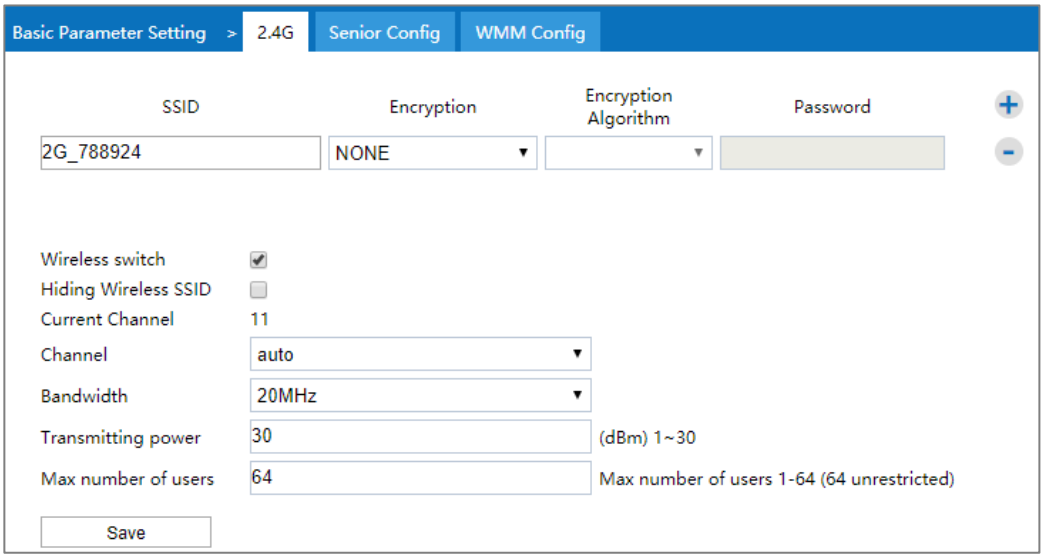
On the “Basic Parameter Settings” page of WLAN settings, user can implement 2.4G basic configuration, advanced configuration and WMM Configuration.

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:

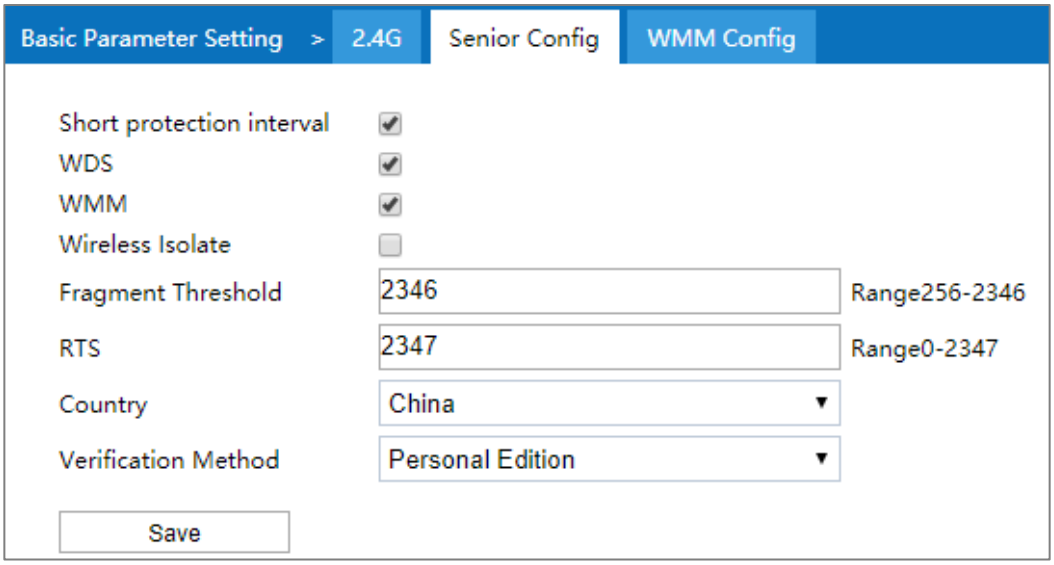
Interface Element	Description
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE: No encryption; • WPA: Wi-Fi Protected Access. When the wireless authentication method is personal edition, encryption method is PSK (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), and provides higher security for WLAN. • WPA-MIXED: the mixed-mode of WPA, is compatible with both WPA and WPA2 encryptions. • WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode.
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 5 or 8-32 characters.
Wireless switch	Wireless Network function enable checkbox, check to enable 2.4G wireless Wi-Fi network.
Hidden 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:

Interface Element	Description
	• Auto: channel self-adaptation; • 1: main frequency band 2412Hz, frequency range 2401~2423Hz; • 2: main frequency band 2417Hz, frequency range 2406~2428Hz; • 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 America, 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 40MHz, options as follows: • 20MHz; • 40MHz. Note: 40MHz bandwidth binds two 20MHz bandwidth channels together to gain the throughput capacity more than twice of the 20MHz bandwidth.
Transmitting	Transmitted power of the device wireless signal, defaults to

Interface Element	Description
power	30dBm, value range 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 2: Senior Configuration

The advanced interface is as follows:



The main element configuration description of advanced interface:

Interface Element	Description
Short protection interval	Check box for Short GI(Short Guard Interval) protection interval: • 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.

Interface Element	Description
	Note: Please enable WDS function while bridging the device and other wireless devices.
WMM	WMM (WiFi Multimedia) function, defaults to enabled. Note: After enabling 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.
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 is 256-2346, defaults to 2346. Note: • The data frame will be segmented when its length surpasses 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

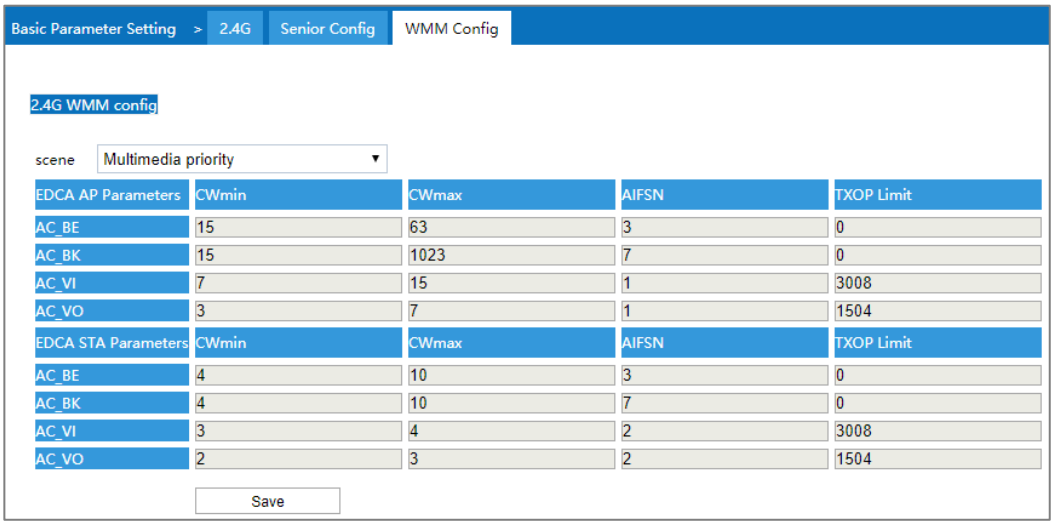
Interface Element	Description
	the two stations can conduct wireless communication.
Country	Applied countries and regions. Options are as follows: • China; • USA. Note: Different country opens different channels.
Verification method	Authentication mode of wireless network, options as follows: • Personal 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 suitable for enterprise users with high security requirements.
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 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 3: 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:



The main element configuration description of WMM configuration interface:

Interface Element	Description
2.4G WMM Configuration	**2.4G WMM Configuration Bar**
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.

Interface Element	Description
CWmax	Maximum competition window, available values: 1, 3, 7, 15, 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 is 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

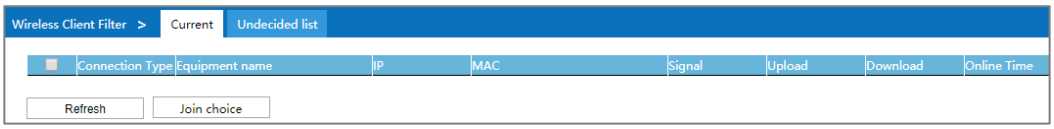
On the “Wireless Client Filtering” page, user can check current connecting devices and manage wireless user connection.

Operation Path

Open in order: “WLAN Settings > Wireless Client Filtering".

Interface Description 1: Current Connected

The interface of the current connected device is as follows:

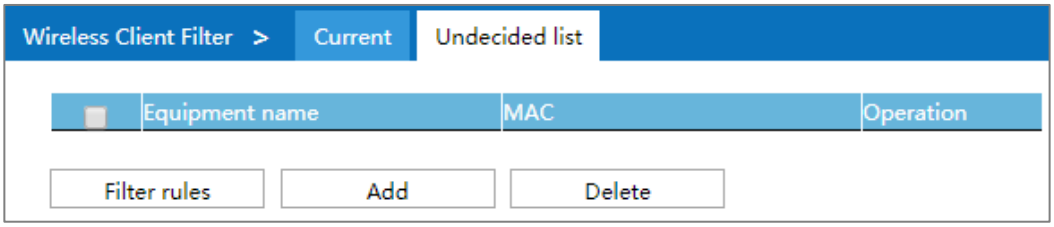


Configuration of the main elements of the current connected device interface:

Interface Element	Description
Connection Type	The connection mode 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.
OnlineTime	The online time of wireless client connected to this device currently.

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

Undecided List/Black List/White List interface is as follows:



The main element configuration description of Undecided List/Black List/White List interface:

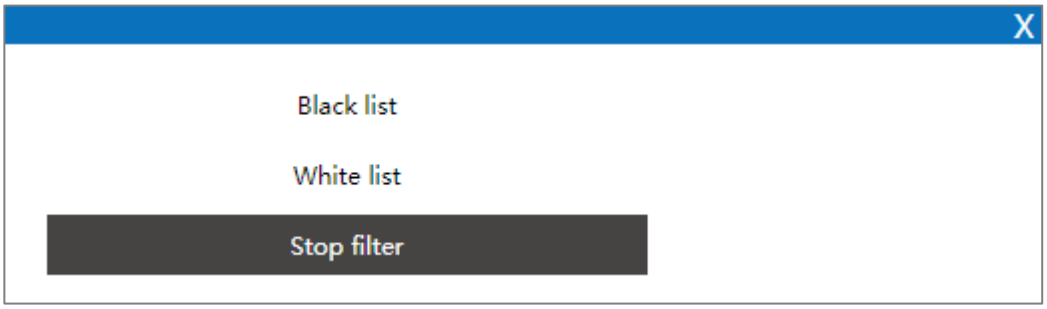
Interface Element	Description
Equipment name	The device name of wireless client in the list. Note: • Click “add” to add device to list manually. • Click “Filter rules” button, you can switch current list between black List, white List and undecided list, to filter wireless client.

Interface Element	Description
MAC	MAC address of wireless client in the list.
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	Description
Black List	The list of wireless client banned from visiting wireless device.
White List	The list of wireless client allowed to visit wireless device.
Stop filter	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

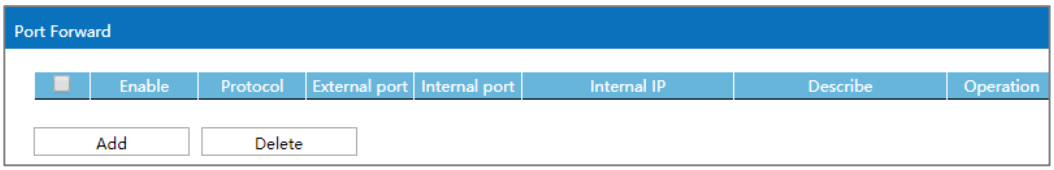
On the “Port Forward” page, user can check or add port forward entry. It allows outer network client to visit specified device via specified port.

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	Description
Enable	Enable port forward or not: • ON Status • OFF
Protocol	The protocol type used by port forward data package: • TCP • UDP

Interface Element	Description
	• 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

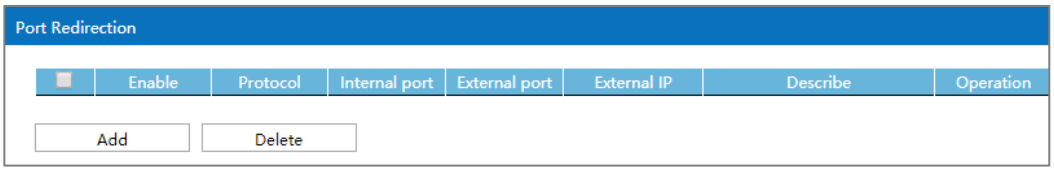
On the “Port Redirection” page, user can check or add port redirection entry, which allows client in LAN to visit the specified port of device with IP address specified by external network via specified port.

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	Description
Enable	Enable port redirection or not: • ON Status • OFF
Protocol	The protocol type used by port redirection data package: • TCP • UDP • TCP/UDP

Interface Element	Description
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 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 to delete the port redirection.

5.3 DMZ Settings

DMZ(Demilitarized Zone) is a buffer zone built between non-safety system and safety system for solving the problem that visitor from external network cannot visit internal network server after the firewall is installed.

Function Description

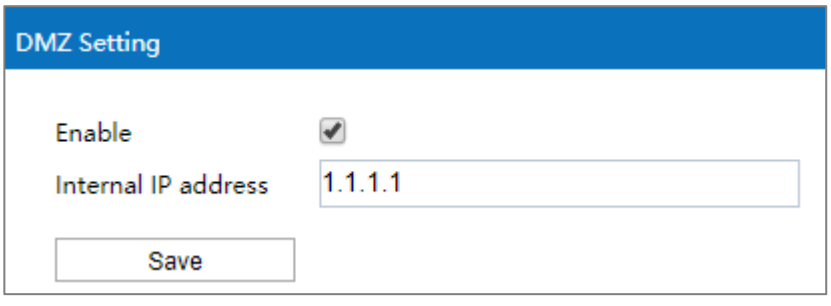
On the page “DMZ Settings”, user can enable or disable DMZ function. The client can visit the specified LAN client via WAN.

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	Description
Enable	DMZ Settings enable checkbox, check to enable DMZ settings function.

Interface Element	Description
Internal IP address	The IP address of LAN client, for example: 192.168.1.123.

5.4 Serial Port Application

The device has integrated instant networking function for serial device, which can convert serial signal into Ethernet wired or wireless signal to achieve signal transmission of serial port on Ethernet.

Function Description

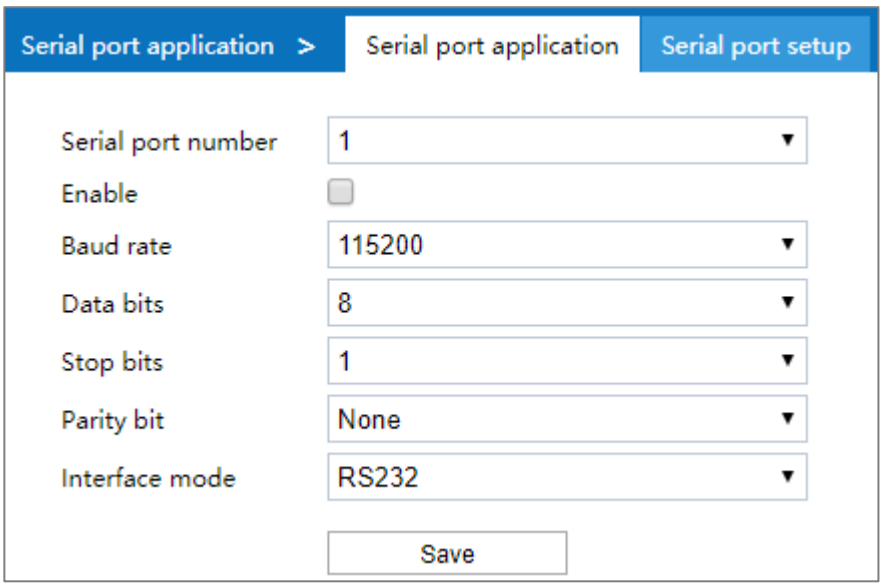
On the “Serial Port Application” page, user can configure basic parameter information of the corresponding serial port, including baud rate, data bit, stop bit and parity bit, as well as work mode.

Operation Path

Please open in order: "Advanced Network > Serial Port Application".

Interface Description 1: Serial Port Application

The serial port application interface as follows:



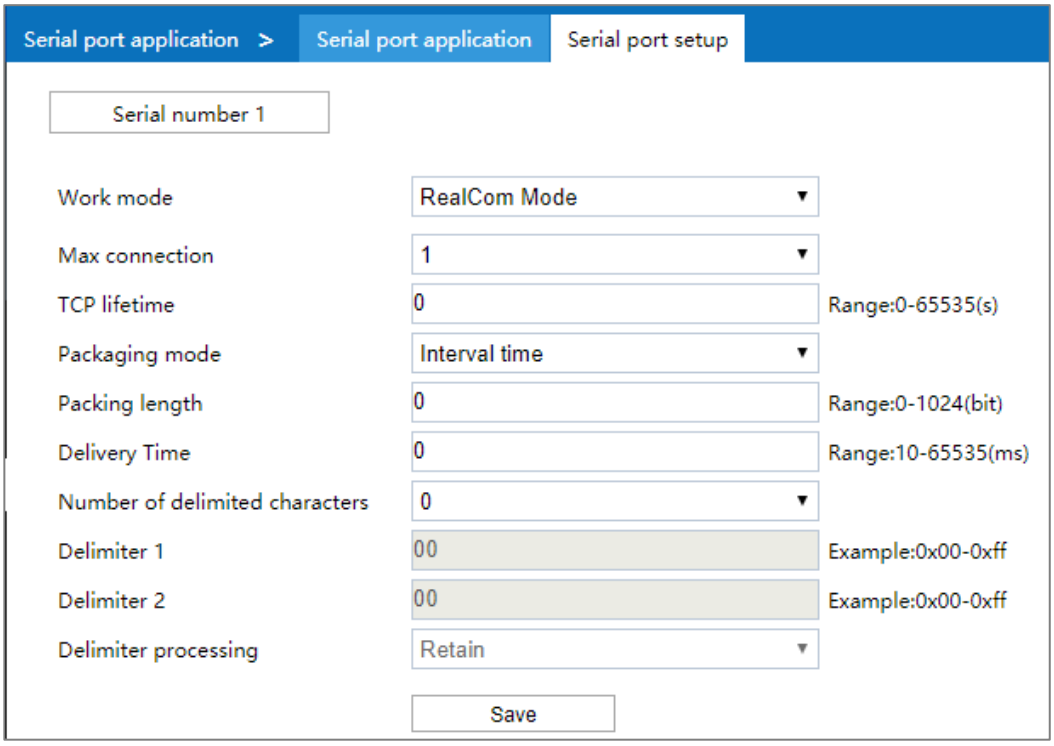
The main element configuration description of serial port application interface:

Interface Element	Description
Serial port number.	The corresponding serial port number of device’s serial port.
Enable	Serial server enable check box, check it to enable the serial server function.

Interface Element	Description
Baud Rate	Choose baud rate of corresponding serial port. Unit: bps. Options: 300/600/1200/2400/4800/9600/19200/38400/57600/115200.
Data Bits	Choose data bit of corresponding serial port. Unit: bit. Options: • 7; • 8.
Stop Bits	Choose stop bit of corresponding serial port. Options: • 0; • 1;
Parity Bit	Select parity bits of corresponding serial number. Options: • None • Odd • Even
Interface mode	Serial port mode. Options are: • RS232; • RS485/RS422.

Interface Description 2: Serial Port Setup

The serial port setup interface:

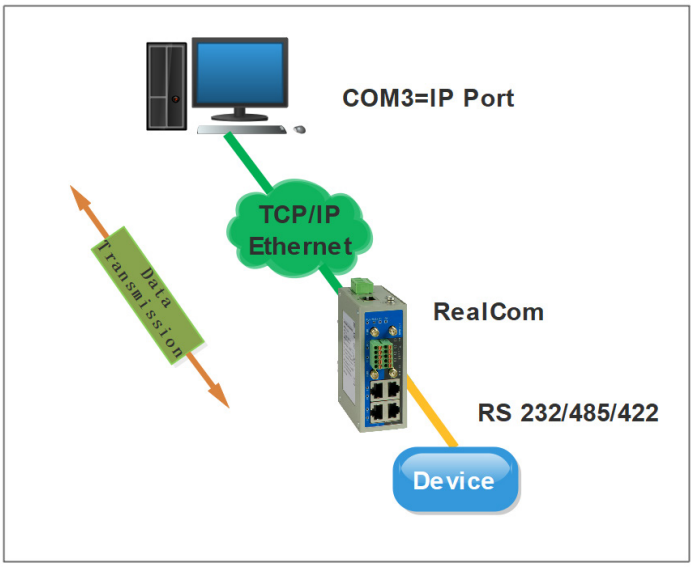


The main element configuration description of serial port setup interface:

Interface Element	Description
Work mode	The work modes of serial port are as follows: • RealCom Mode: Real serial port mode; • TCP Server: TCP server mode; • TCP Client: TCP client mode; • UDP Server: UDP server mode; • UDP Client: UDP client mode.
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 lifetime	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.
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them. • 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;
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.
Delivery time	The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms. Note: Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time.
Number of delimited characters	Select the number of delimited characters, the options are as follows:

Interface Element	Description
	• 0: disable the delimited character 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 character processing method. Options: • Retain: the system would send out the received delimiter and other data via network. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.

5.4.1 RealCom Mode



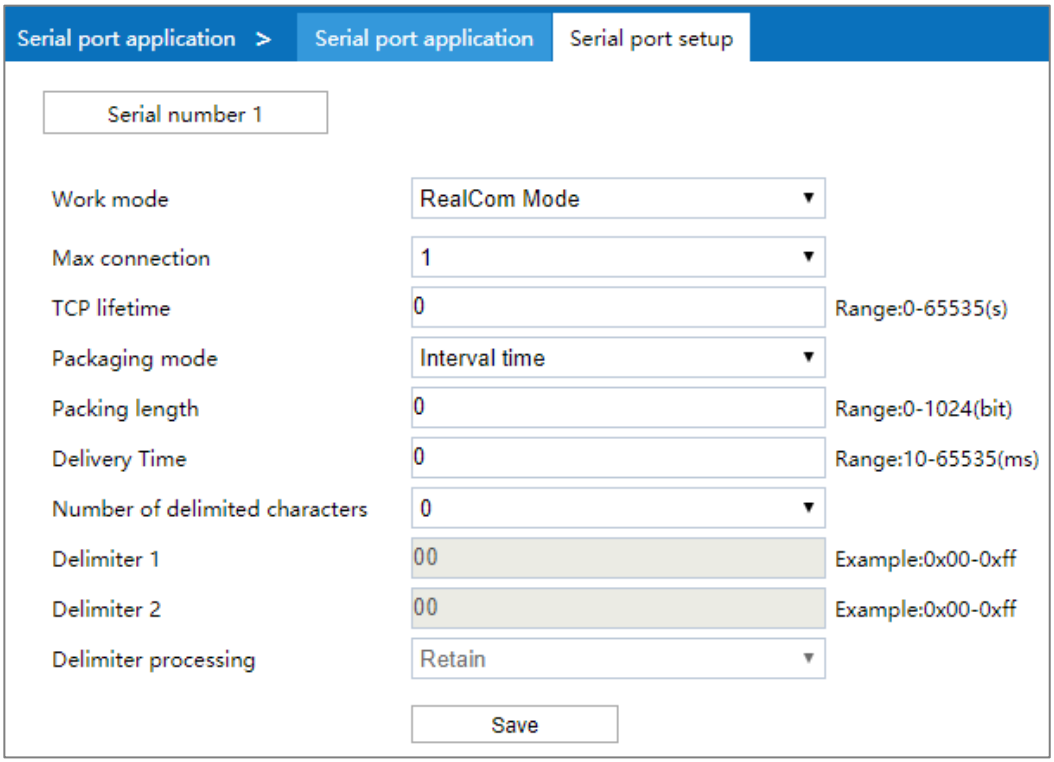
Note:

The device picture mentioned in above figure is only an example, and the actual appearance of the device 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 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 transparent 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 serial port setup interface in RealCom Mode:



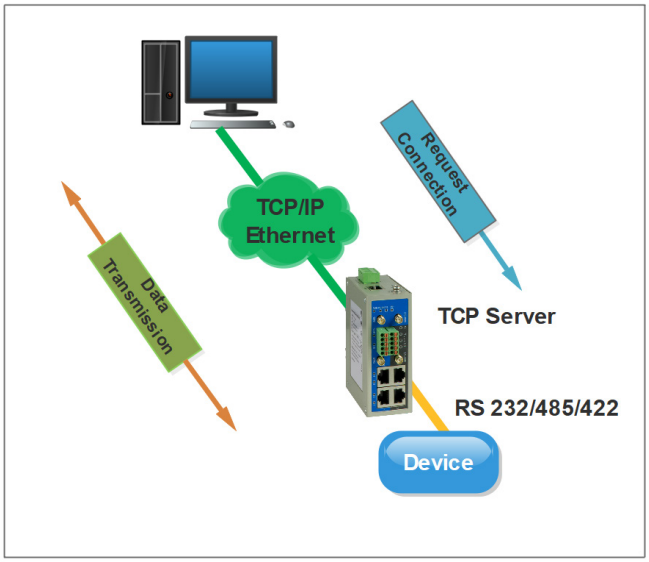
The main element configuration description of serial port setup interface in RealCom Mode:

Interface Element	Description
Max connection	The number of host that one serial port connects to. • Each host communicates with serial port in the order of

Interface Element	Description
	first-in first-out; • The system supports up to 4 connections.
TCP lifetime	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.
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them. • 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;
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 0~1460. 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.
Delivery time	The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms. Note: Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time.
Number of delimited characters	Select the number of delimited characters, the options are as follows: • 0: disable the delimited character 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

Interface Element	Description
	00-FF.
Delimiter 2	The Delimiter 2 is expressed in hexadecimal, value range is 00-FF.
Delimiter processing	Select the method of delimiter processing. Options: • Retain: the system would send out the received delimiter and other data via network. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.

5.4.2 TCP Server Mode



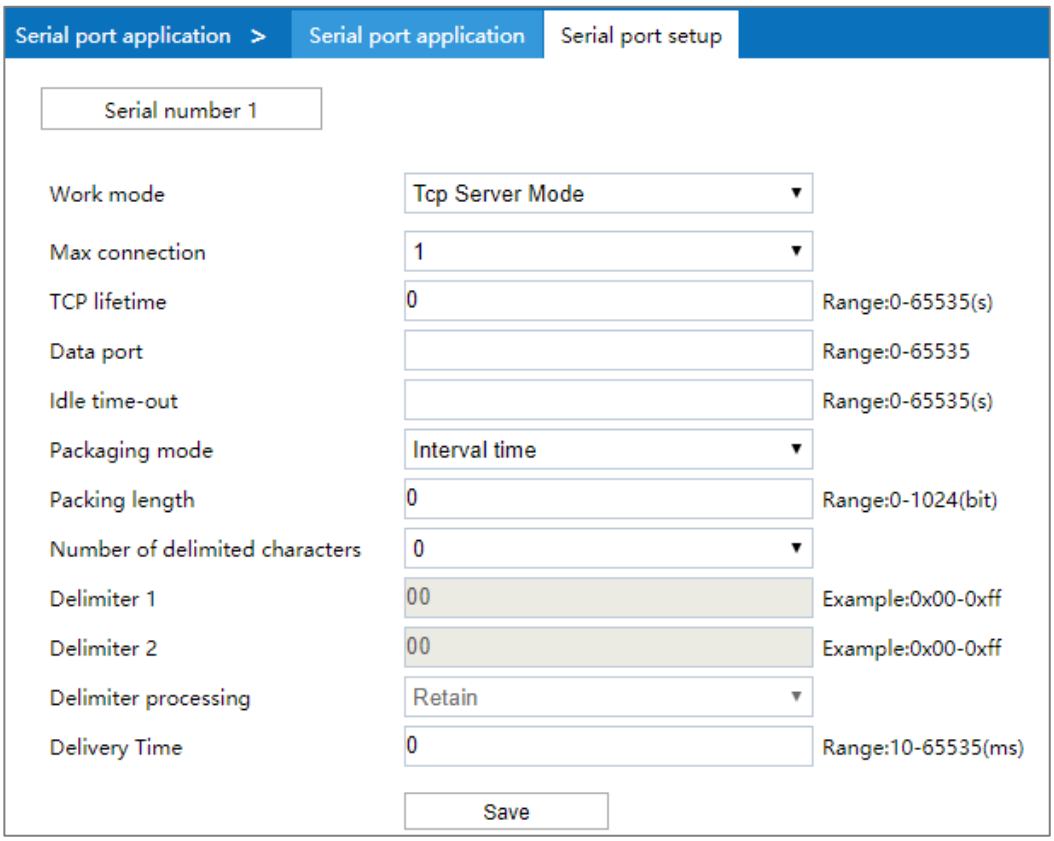
Note:

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

In the TCP server mode, the serial device server is assigned an IP port number, passive waiting for the host connection. When the host initiates a connection request and establishes a connection with the serial device server, the host can realize bidirectional transparent data transmission through the network connection and the 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

The serial port setup interface in TCP Server Mode:



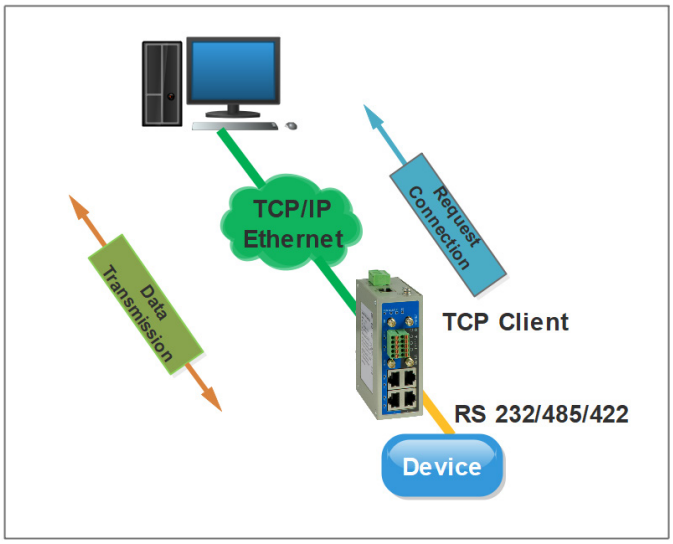
The main element configuration description of serial port setup interface in TCP Server Mode:

Interface Element	Description
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 lifetime	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.
Data port	The destination connection port of TCP client.
Idle timeout	Set the idle time-out of current serial data communication link. • If the idle time-out during communication is larger than 0,

Interface Element	Description
	the system would close the TCP connection without any data transmission activity occurring in the specified time automatically; • If the idle time-out is equal to 0, it means the free TCP connection would not be closed automatically.
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them. • 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;
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 0~1460. 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.
Number of delimited characters	Select the number of delimited characters, the options are as follows: • 0: disable the delimited character 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 method of delimiter processing. Options: • Retain: the system would send out the received delimiter and other data via network. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.

Interface Element	Description
Delivery time	The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms. Note: Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time.

5.4.3 TCP Client Mode



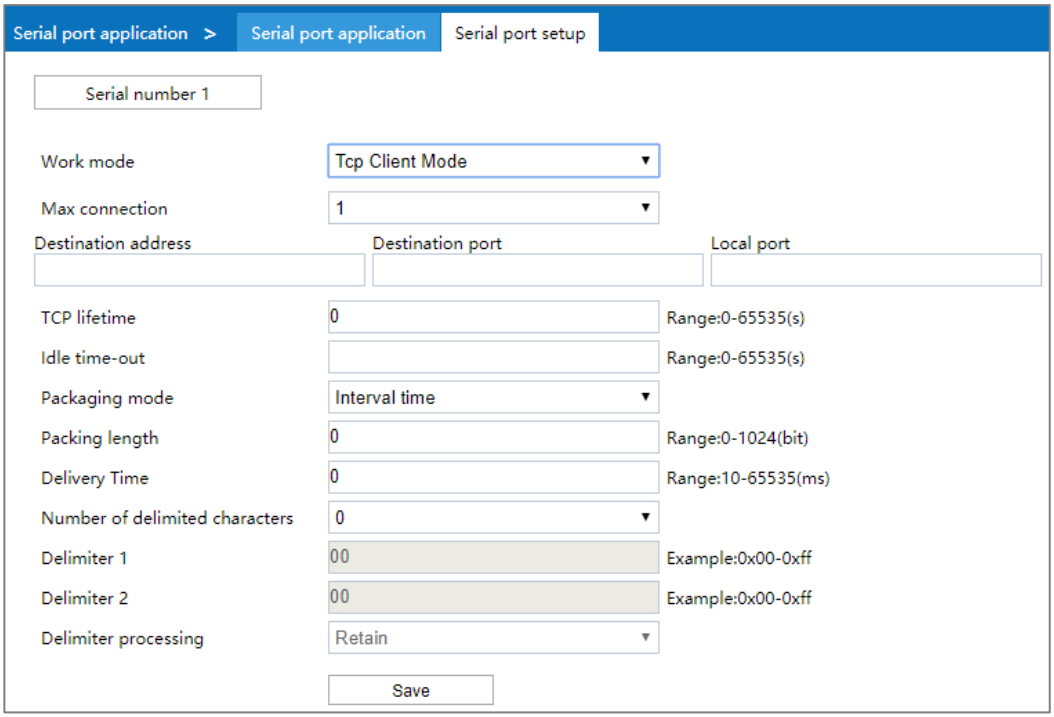
Note:

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

In the TCP client mode, the serial device server can automatically establish a network connection with the host specified by the user when the serial data arrives. When the data transmission is completed, the serial server will automatically shut down the network connection according to the parameters such as TCP alive time and TCP idle timeout time. 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

The serial port setup interface in TCP Client Mode:



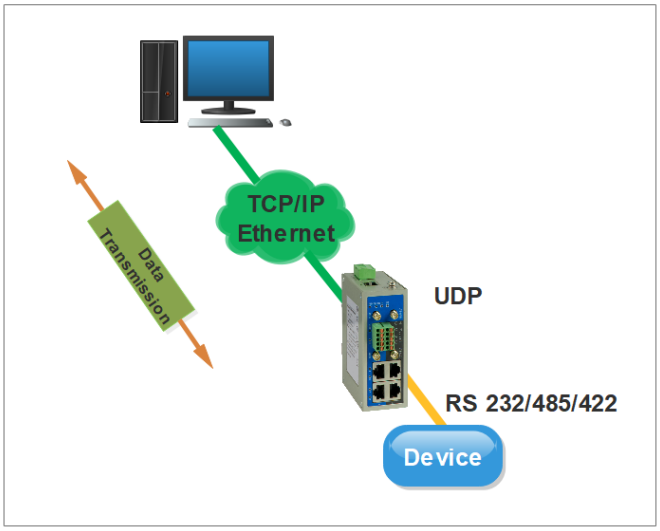
The main element configuration description of serial port setup interface in TCP Client Mode:

Interface Element	Description
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.
Destination Address	Enter the IP address of the server that would be connected to serial port.
Destination Port	Enter the TCP port number of the server that would be connected to serial port.
Local port	The local port allocated for TCP connection by the system, which could offer service or connection for the outside world, used for connecting and communicating with server.
TCP lifetime	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.
Idle timeout	Set the idle time-out of current serial data communication link.

Interface Element	Description
	• 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; • If the idle time-out is equal to 0, it means the free TCP connection would not be closed automatically.
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them. • 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;
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 0~1460. 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.
Delivery time	The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms. Note: Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time.
Number of delimited characters	Select the number of delimited characters, the options are as follows: • 0: disable the delimited character 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	Select the method of delimiter processing. Options:

Interface Element	Description
processing	• Retain: the system would send out the received delimiter and other data via network. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.

5.4.4 UDP Server Mode



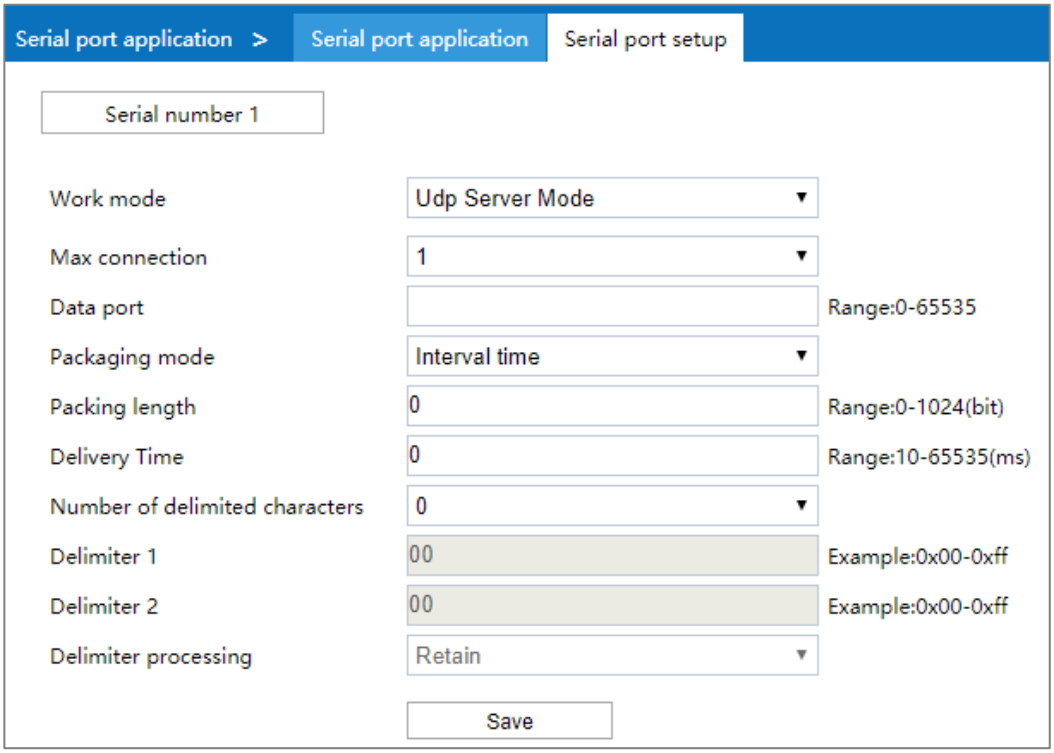
Note:

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

In UDP mode, serial server can be a server or a client. It use the UDP protocol and user-specified host for serial data transmission. UDP mode serial device server can transfer data from the serial device to one or more hosts, and the serial device server can also receive data from one or more hosts. Compared with TCP mode, UDP protocol is faster and more efficient.

Interface Description

Screenshot of the serial port settings interface in UDP Server Mode:

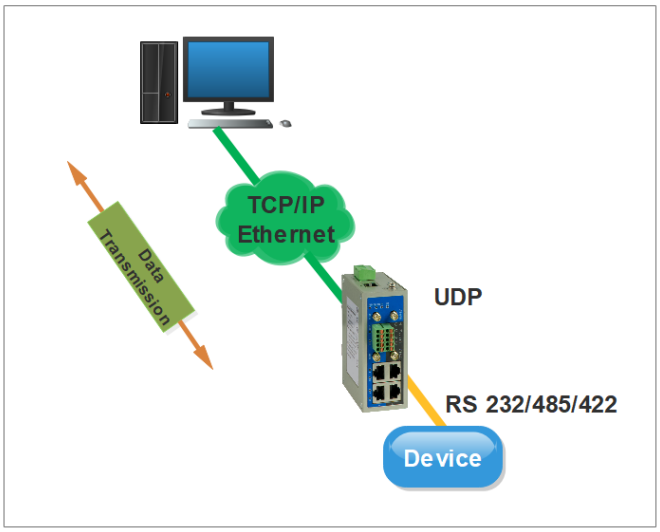


The main elements configuration description of serial port settings interface under UDP Server Mode:

Interface Element	Description
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.
Data port	The data port on which the network receives UDP data. The user must assign a unique data port to each serial port for the system to receive UDP data normally.
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them. • 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;
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 0~1460. It means no limit on data transmission length when it' set to 0.

Interface Element	Description
	Note: There are some slight deviations between the actual package length value and the set value.
Delivery time	The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms. Note: Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time.
Number of delimited characters	Select the number of delimited characters, the options are as follows: • 0: disable the delimited character 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 method of delimiter processing. Options: • Retain: the system would send out the received delimiter and other data via network. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.

5.4.5 UDP Client Mode



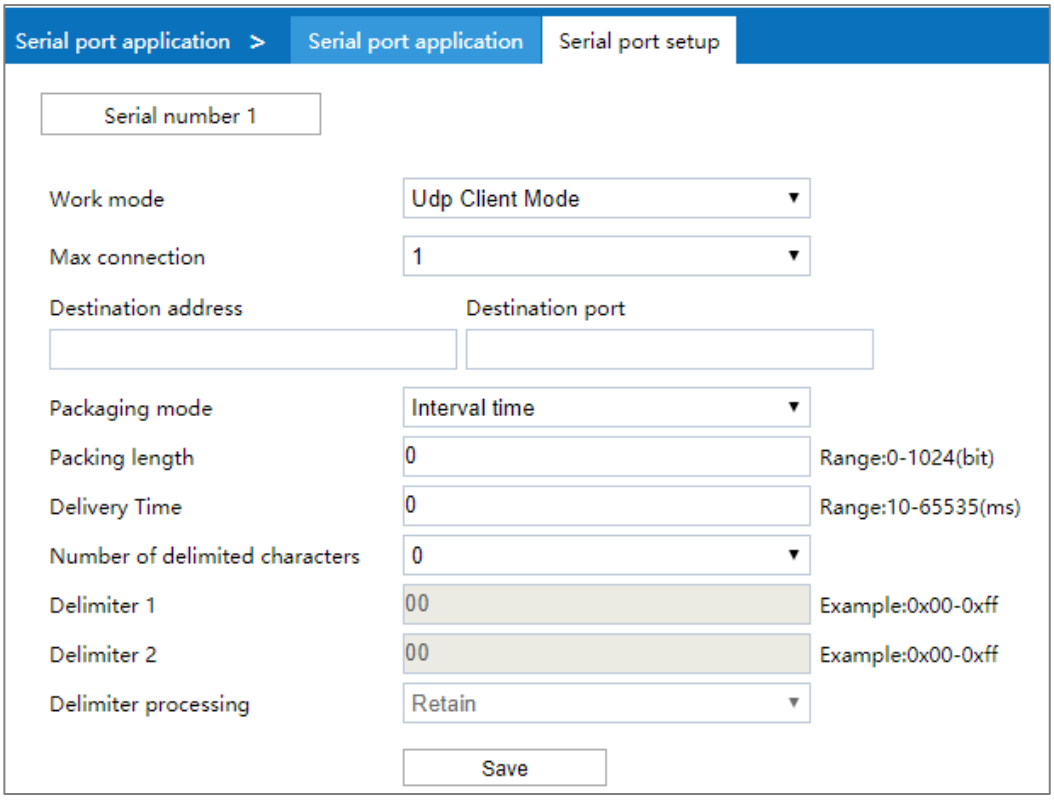
Note:

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

In UDP mode, serial server can be a server or a client. It use the UDP protocol and user-specified host for serial data transmission. UDP mode serial device server can transfer data from the serial device to one or more hosts, and the serial device server can also receive data from one or more hosts. Compared with TCP mode, UDP protocol is faster and more efficient.

Interface Description

Screenshot of the serial settings interface in UDP Client Mode:



The main elements configuration description of serial settings interface under UDP Client Mode:

Interface Element	Description
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.
Destination Address	Enter the IP address of the opposite host that serial port needs to be connected to.
Destination Port	Enter the port number of the opposite host that serial port needs to be connected to.
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Forced time: the system packages serial port data received within a specified time into Ethernet packets and transmit them. • 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;
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

Interface Element	Description
	to the set frame length. The value range is 0~1460. 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.
Delivery time	The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms. Note: Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time.
Number of delimited characters	Select the number of delimited characters, the options are as follows: • 0: disable the delimited character 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 method of delimiter processing. Options: • Retain: the system would send out the received delimiter and other data via network. • Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter.

5.5 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

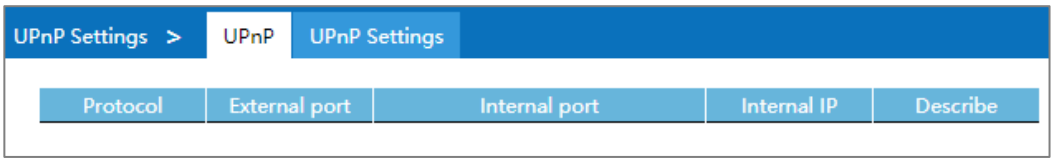
On the page of "UPnP Settings", user can view internal ports translation information and configure UPnP parameters.

Operation Path

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

Interface Description 1: UPnP

UPnP settings interface as follows:

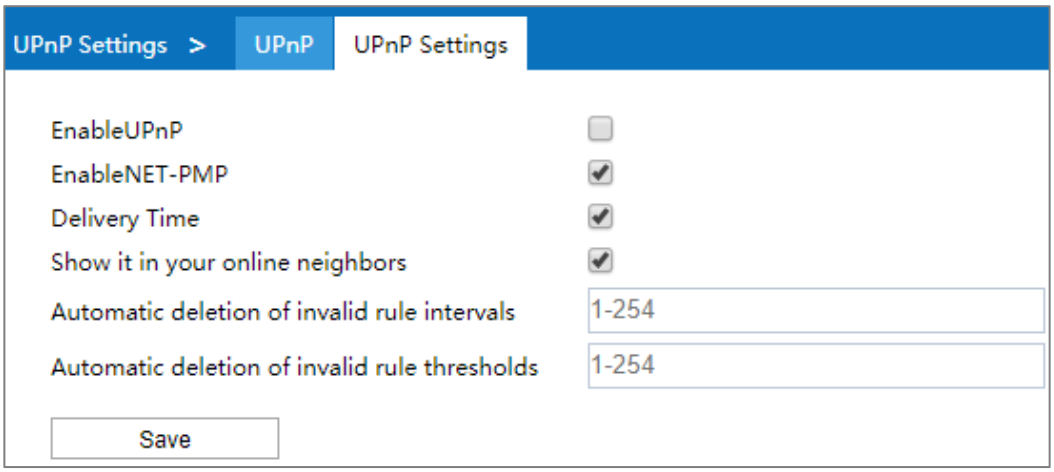


The main elements configuration description of UPnP settings interface:

Interface Element	Description
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	Description
Enable UPnP	UPnP enable checkbox, check to enable UPnP function.
EnableNET-PMP	The NAT-PMP function enable checkbox, check to enable NAT-PMP function, and the router will allow the NAT LAN host to communicate with external devices to automate port conversion.
Security Model	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.

5.6 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

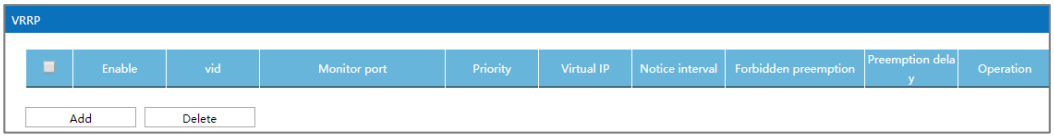
On the "VRRP Configuration" page, user can configure VRRP parameters.

Operation Path

Open in order: "Advanced Network > VRRP".

Interface Description

VRRP interface as below:



The main elements configuration description of VRRP interface:

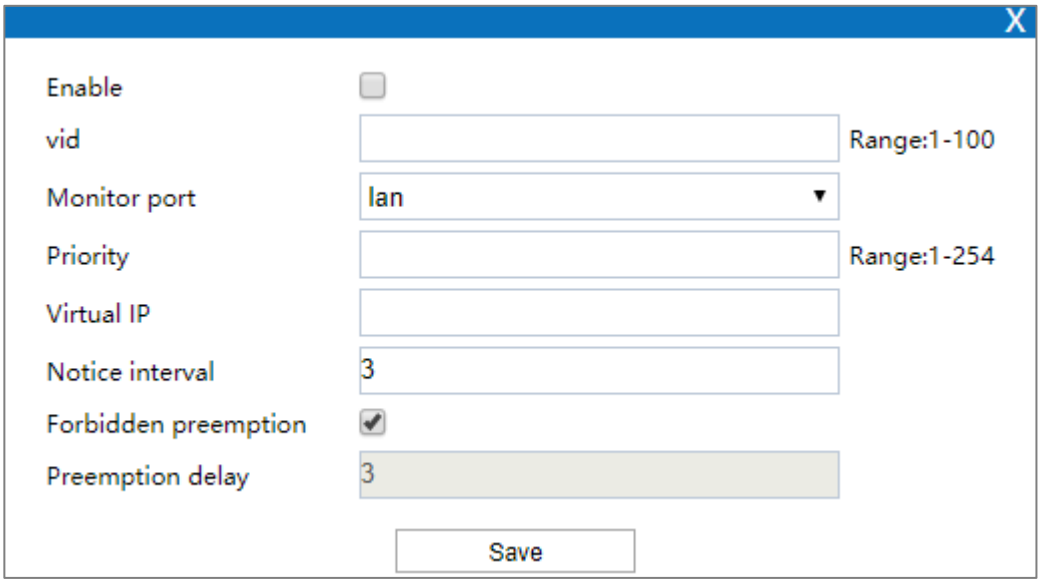
Interface Element	Description
Enable	VRRP function status is displayed, options include: • ON Status • OFF
Vid	Identity of the virtual router is displayed.
Monitor port	Monitor ports of the device is displayed, options include: • Br-lan • Eth1
Virtual IP	The IP address of the virtual router is displayed.
Notice interval	Interval at which Master device sends VRRP notice messages, unit: second.
Priority	Priority of the device. The priority is used for the election of Master device. The greater the value, the higher the priority.
Forbidden preemption	Status display of forbidden preemption, options include: • ON Status • OFF

Interface Element	Description
Preemption delay	The delay time of switching from Backup device to Master device.
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	Description
Enable	VRRP enable check box, check it to enable VRRP.
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 monitor port; • wan: WAN port as the monitor 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	Notice interval, valid range is 1-10 seconds. Master device

Interface Element	Description
	periodically sends VRRP notice messages to announce its operating status.
Forbidden preemption	Disable preemption check box, check it to disable preemption. • Check: 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; • Uncheck: 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 1-1000 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.

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

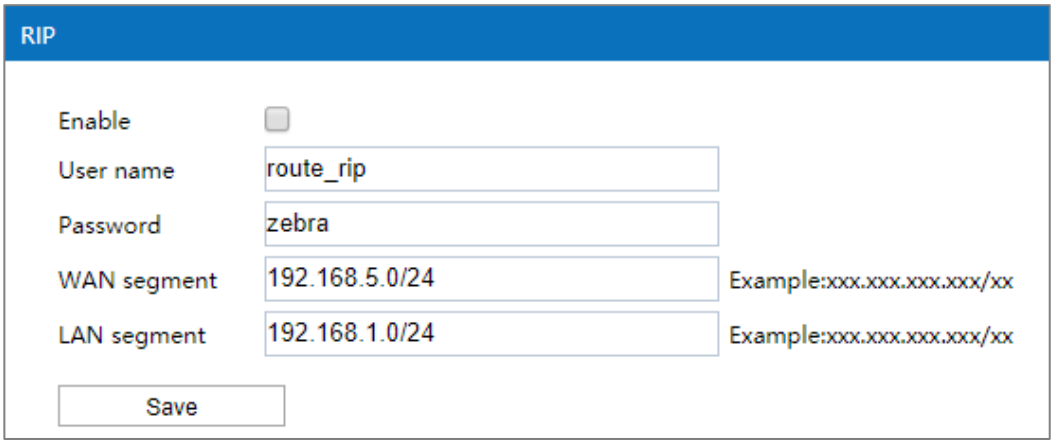
On the page of "RIP", user can configure the RI related parameters.

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	Description
Enable	RIP Enable checkbox, check to enable the RIP default configuration.
User name	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

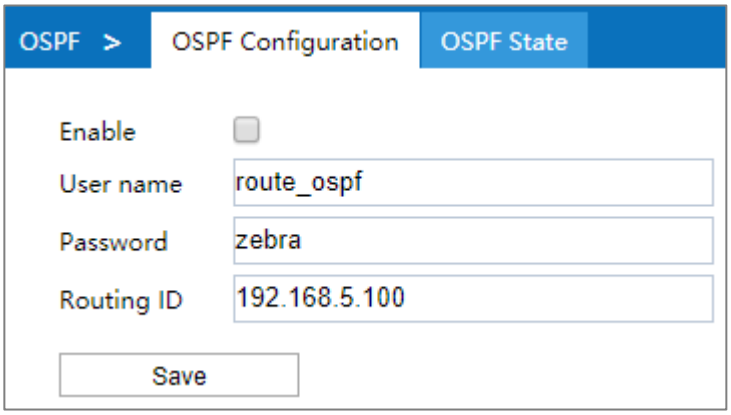
On the page of "OSPF", user can configure the OSPF parameters.

Operation Path

Open in order: "Advanced Network > OSPF".

Interface Description 1: OSPF Configuration

OSPF configuration interface is as follows:

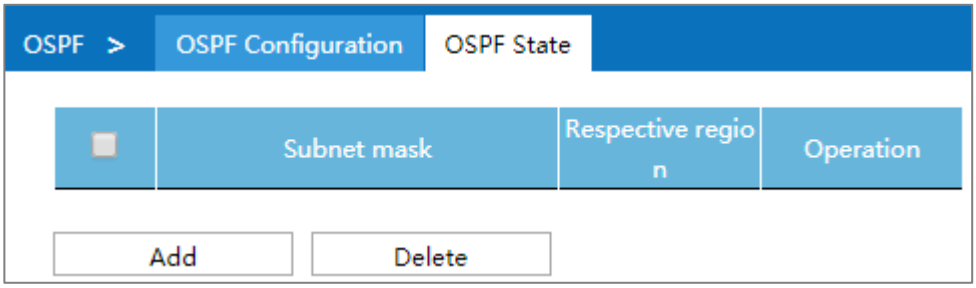


The main element configuration description of OSPF configuration interface:

Interface Element	Description
Enable	OSPF enable check box, check it to enable the OSPF function.
User name	User name used to log in to the OSPF command line configuration.
Password	Password used to log in to the OSPF command line configuration.
Routing ID	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:



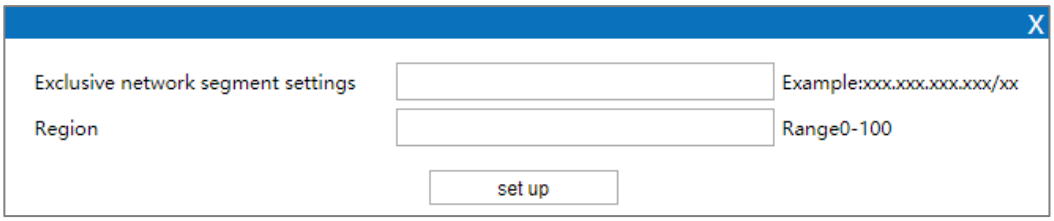
The main elements configuration description of OSPF State interface:

Interface Element	Description
Subnet mask	The network segment where the IP address of interface running OSPF protocol is located. A network segment can only belong to one area.

Interface Element	Description
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: OSPF-Add

The OSPF-Add interface as follows:



The main elements configuration description of OSPF-Add interface:

Interface Element	Description
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	Description
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	Description
MAC address;	MAC address of the DHCP client, the format is 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.

6 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.

6.1 IP Filter

Function Description

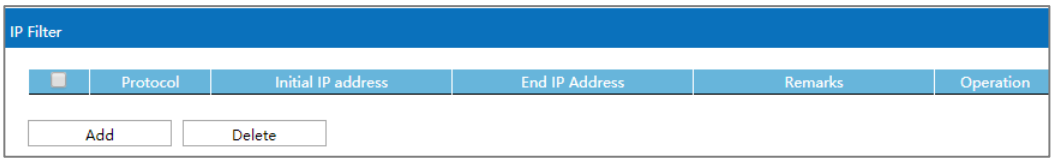
On the "IP filter" page of firewall, user can check or add IP filter to forbid the communication between the clients in LAN and WAN.

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:

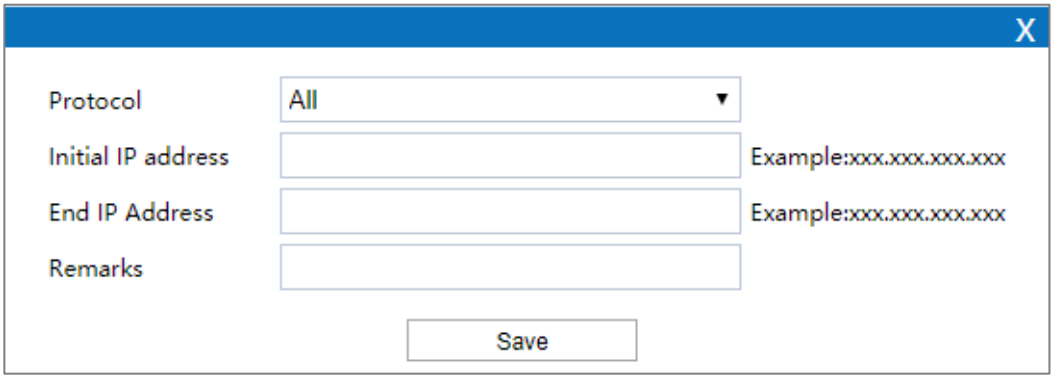
Interface Element	Description
Protocol	Protocols used by data packets.
Initial IP address	Start IP address of LAN IP address range filtered by the device.
End IP address	End IP address of LAN IP address range filtered by the device.
Remarks	Remarks of IP filter entries.

Interface Element	Description
Operation	Edit: Modify the filtering entries information.

Interface Description: Add IP Filter Entry

Click "Add" to increase IP filter entry.

IP filter interface as follows:



The main element configuration description of IP filter interface:

Interface Element	Description
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 filter list support 10 Chinese characters or 32 valid characters, optional.

6.2 MAC Filter

Function Description

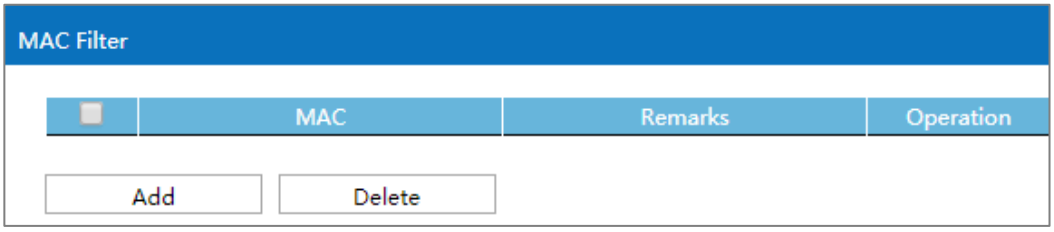
On the "MAC filter" page of firewall, user can check or add MAC filter to forbid the communication between the clients in LAN and WAN; it can effectively control the WAN access rights of user in LAN.

Operation Path

Open in order: "Firewall > MAC filter".

Interface Description

MAC filter interface as follows:



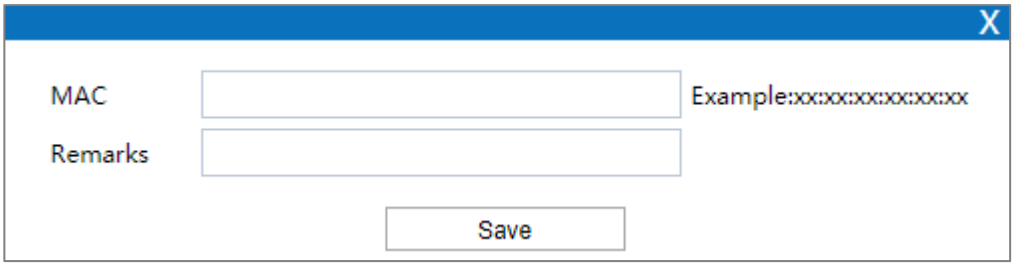
The main element configuration description of MAC filter interface:

Interface Element	Description
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.

MAC filter interface as follows:



The main element configuration description of MAC filter interface:

Interface Element	Description
MAC	MAC address of LAN client filtered by the device, such as: 00:22:6F:00:00:01.
Remarks	Remarks of MAC filter entries, support 32 valid characters or 10 Chinese characters, optional.

6.3 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

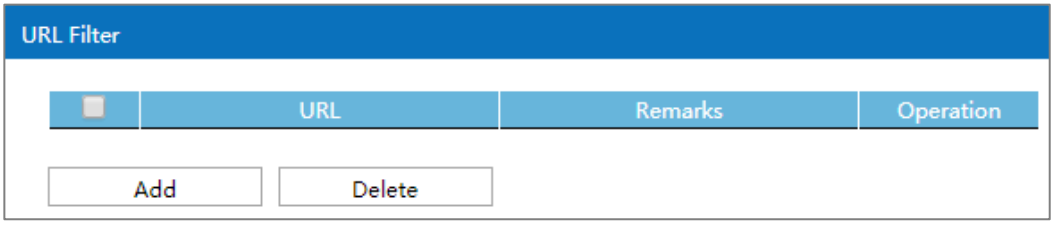
On the "URL filter" page of firewall, user can check or add URL filter to prohibit the client in LAN from accessing URL address in WAN and prevent user from accessing some of the websites.

Operation Path

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

Interface Description

URL filter interface as follows:



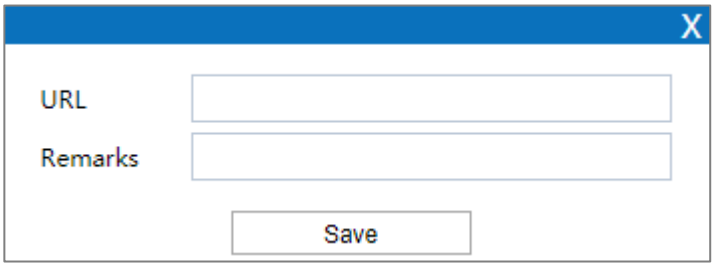
The main element configuration description of URL filter interface:

Interface Element	Description
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	Description

Interface Element	Description
URL	URL address in WAN filtered by the device, ending with ".com", ".cn" and so on. Such as: sina.
Remarks	Remarks of the URL filtering entry, it supports 32 valid characters or 10 Chinese characters, and can be left blank.

6.4 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

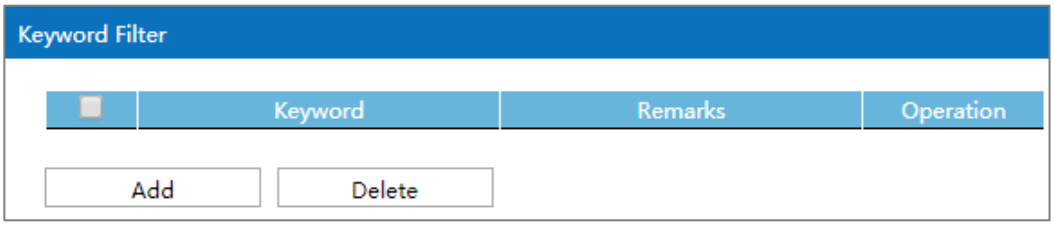
On the page of "Keyword filter" of the firewall, user can view or add keyword filtering entries to prevent clients on the LAN from accessing to the network address corresponding to the keywords in the WAN.

Operation Path

Open in order: "Firewall > Keyword Filter".

Interface Description

Keyword filter interface as follows:



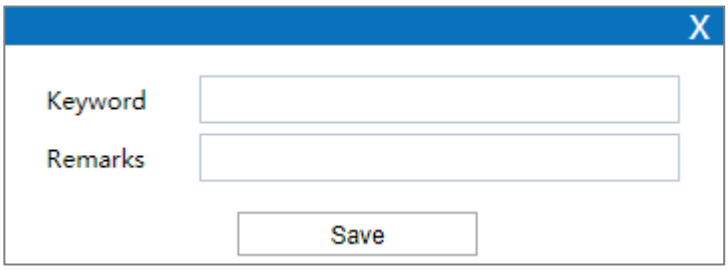
The main elements configuration description of keyword filter interface:

Interface Element	Description
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.

Keyword filter interface as follows:



The main elements configuration description of keyword filter interface:

Interface Element	Description
Keyword	Keywords in the WAN filtered by this device.
Remarks	Remarks of the keyword filtering list; it supports 10 Chinese characters or 32 valid characters, and can be left blank.

6.5 IP Address Black/White List

Function Description

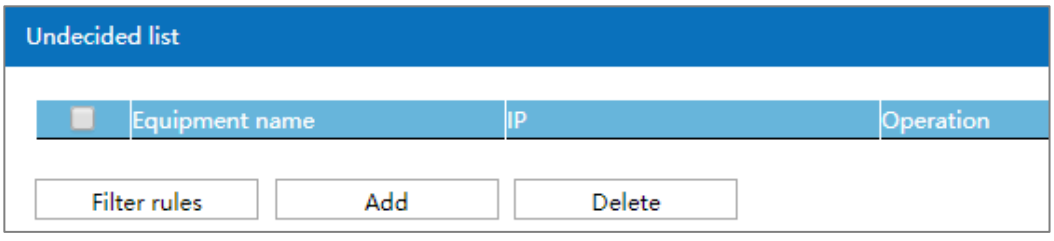
On the "Black and White List of IP Addresses" page of the firewall, you can control the communication between the client with the specified IP address in the LAN and the WAN according to the filter list.

Operation Path

Open in order "Firewall > IP Address Black/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:

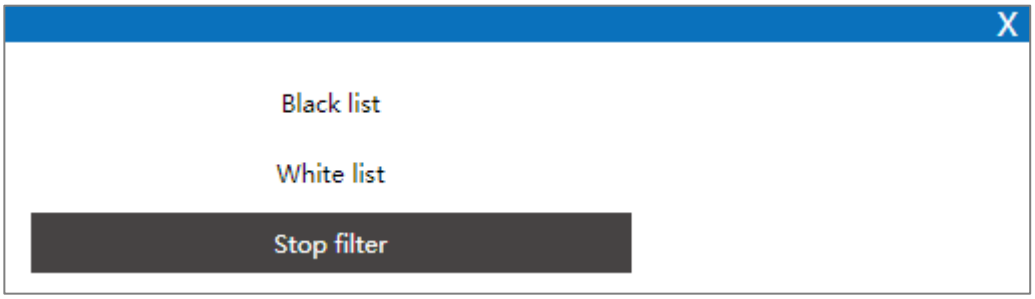
Interface Element	Description
Equipment name	The device name of client in the list. Note: • Click “add” to add device to list manually. • Click “Filters rule” button, you can switch current list between black List, white List and undecided list, to filter the Client device.

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

Note

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

7 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.

7.1 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

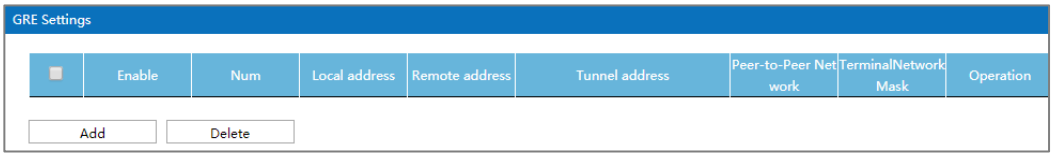
On the page of "GRE Settings", user can configure the relevant parameters of GRE.

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	Description
Enable	GRE settings is enabled or not:

Interface Element	Description
	• 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.

7.2 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

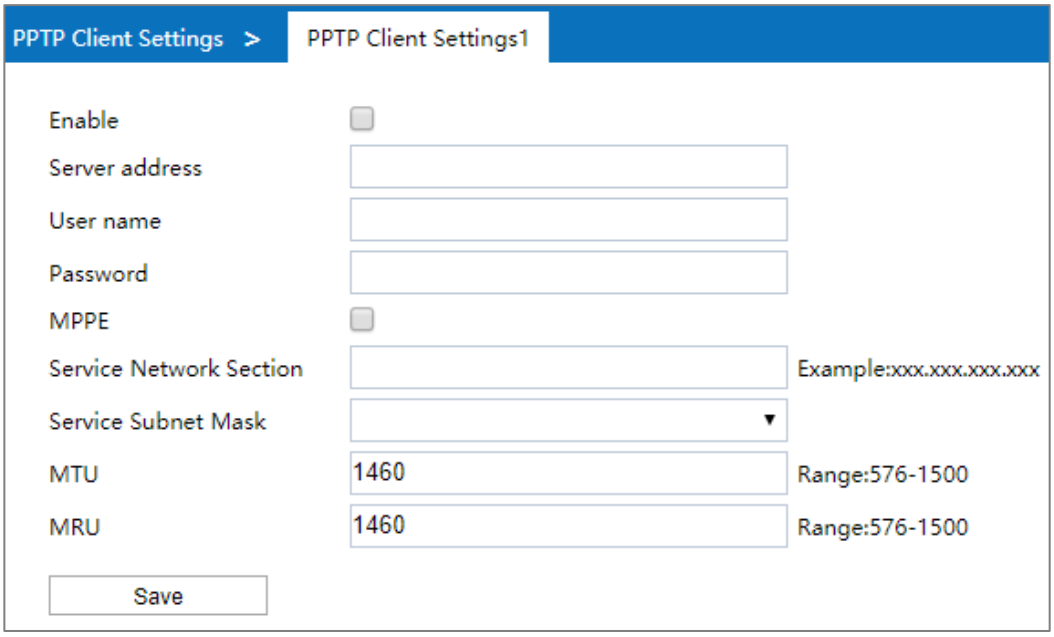
On the page of "PPTP Client Settings", user can configure the parameters related to PPTP client.

Operation Path

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

Interface Description

The PPTP client settings interface is as follows:



The main elements configuration description of PPTP client settings interface:

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

7.3 PPTP Server Settings

Function Description

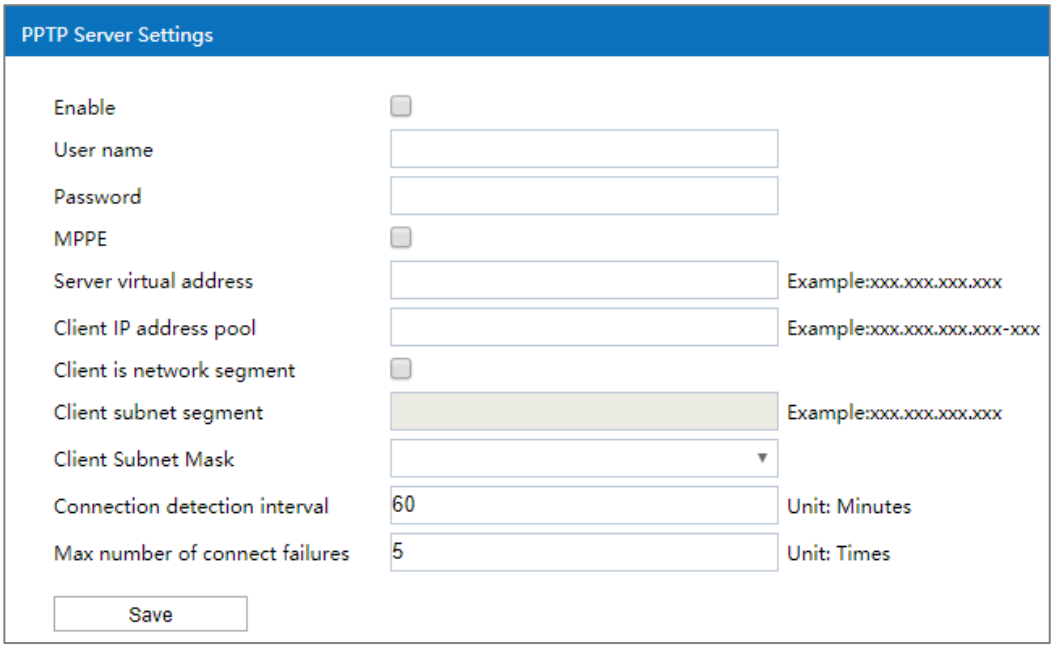
On the page of "PPTP Server Settings", user can configure the parameters related to PPTP server.

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	Description
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 enablement 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.

Interface Element	Description
Client is network segment	The client is network segment enable check box allows routers with subnets as network segments to connect and access PPTP VPN servers as clients. Check this box to enable the client is network segment function.
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 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.

7.4 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

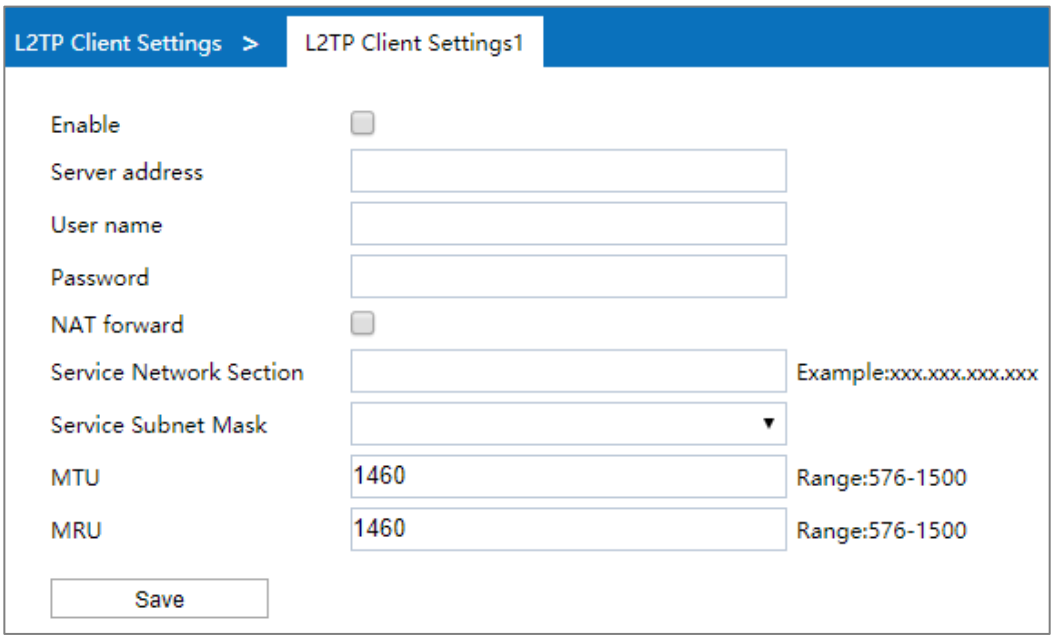
On the page of "L2TP Client Settings", user can configure the parameters related to L2TP client.

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

7.5 L2TP Server Settings

Function Description

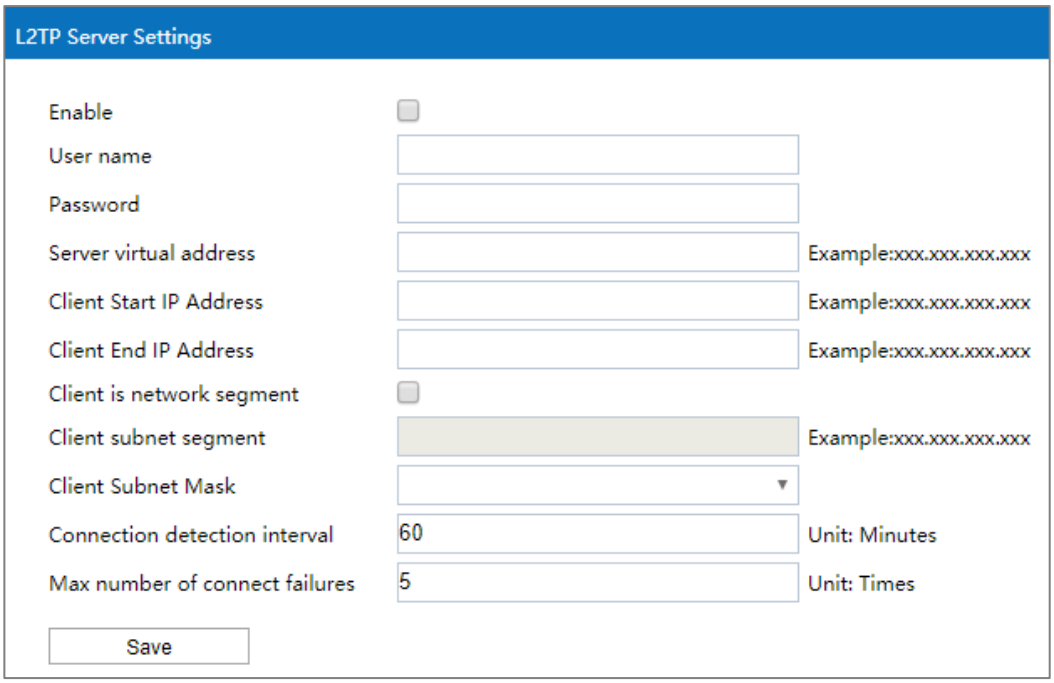
On the page of "L2TP Server Settings", user can configure the parameters related to L2TP server.

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	Description
Enable	L2TP Server Settings enable checkbox, check to enable the L2TP server settings function;
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	"Client subnet segment" enblement checkbox. It allows

Interface Element	Description
segment	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.

7.6 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

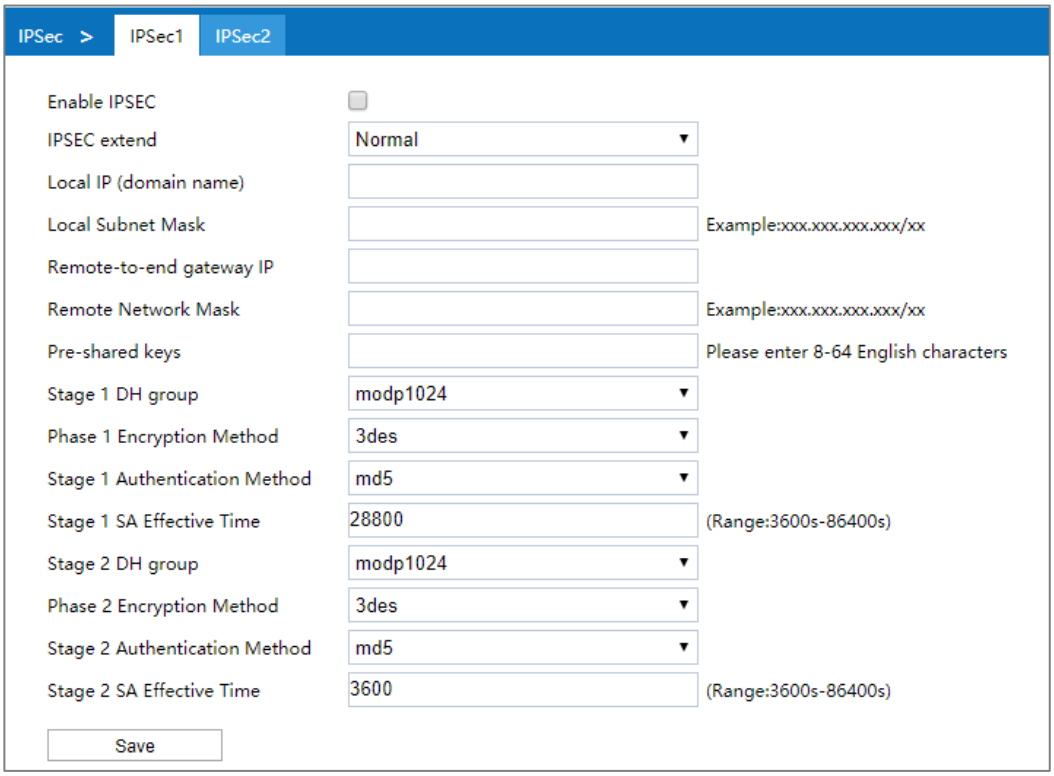
On the page of "IPsec", user can configure the relevant parameters of IPsec.

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	Description
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/domain name of the local external network port.
Local Subnet Mask	The local subnet and mask of the router, for example: 192.168.4.0/24.
Remote-to-end gateway IP	IP or domain name of the end-to-end external network port.

Interface Element	Description
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: • modp 768 • modp1024 • modp1536
Phase 1 Encryption Method	Phase 1 encryption algorithm, options as follows: • 3des • aes128 • aes192 • aes512
Stage 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: • modp 768 • modp1024 • modp1536
Phase 2 Encryption Method	Phase 2 encryption algorithm, options as follows: • 3des • aes128 • aes192 • aes512
Stage 2 Authentication Method	Stage 2 Authentication Method, options as follows: • md5 • sha • sha256 • sha384 • sha512
Stage 2 SA Effective Time	Stage 2 SA Effective time, unit is second and default is 3600.

7.7 OpenVpn Client Settings

OpenVPN is an open source encrypted tunnel construction tool. Based on the SSL/TLS protocol of OpenSSL, it can realize point-to-point SSL VPN secure connection in the Internet. OpenVPN provides two types of virtual network interfaces: TUN and TAP, which are used to establish IP tunnel and Ethernet bridge respectively. OpenVPN provides a variety of authentication methods to confirm the identities of both parties involved in the connection, including pre-shared private key, third-party certificate and user name/password combination.

By using OpenVPN, you can:

- Use specific UDP or TCP ports to realize VPN connection between two hosts.
- Realize the C/S structure and realize the interconnection of multiple Clients through server.
- Ensure the security of data transmission through TLS/SSL encryption.
- Through data compression, improve the speed of data transmission.

Function Description

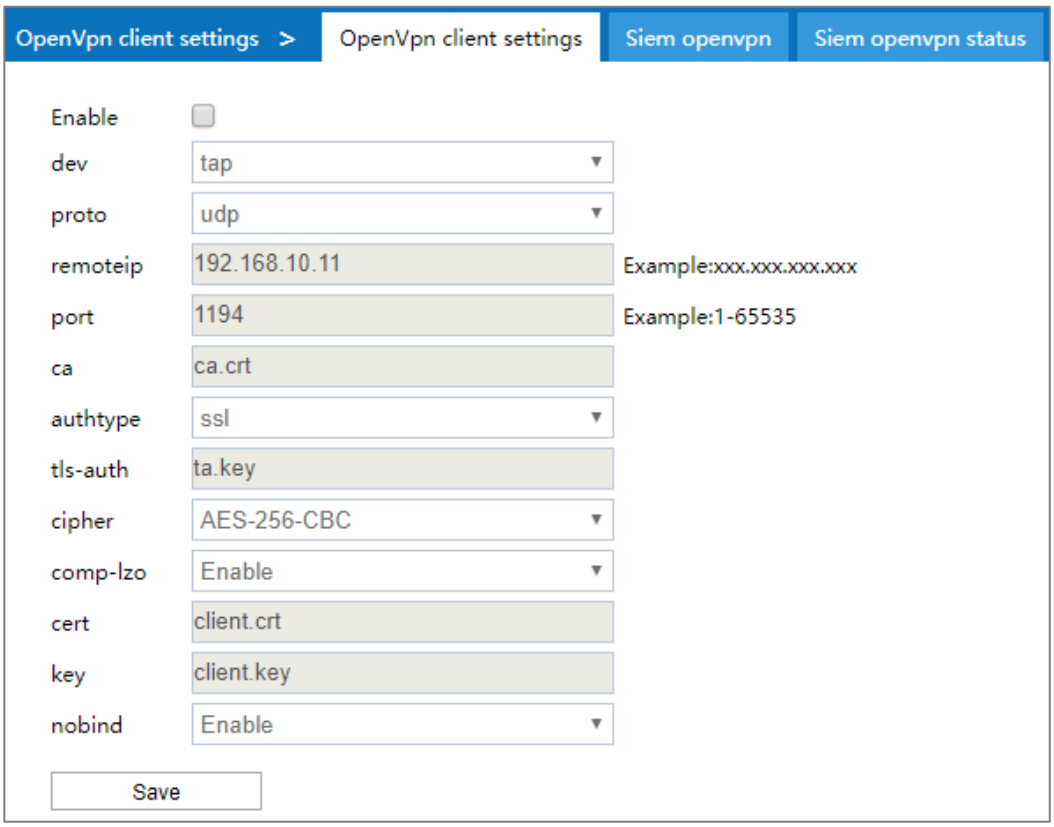
On the page of "OpenVpn Client Settings", user can configure the parameters related to OpenVpn client.

Operation Path

Open in order: "VPN Tunnel > OpenVpn Client Settings".

Interface Description 1: OpenVpn Client Settings

The OpenVpn client settings interface is as follows:



The main elements configuration description of OpenVpn client settings interface:

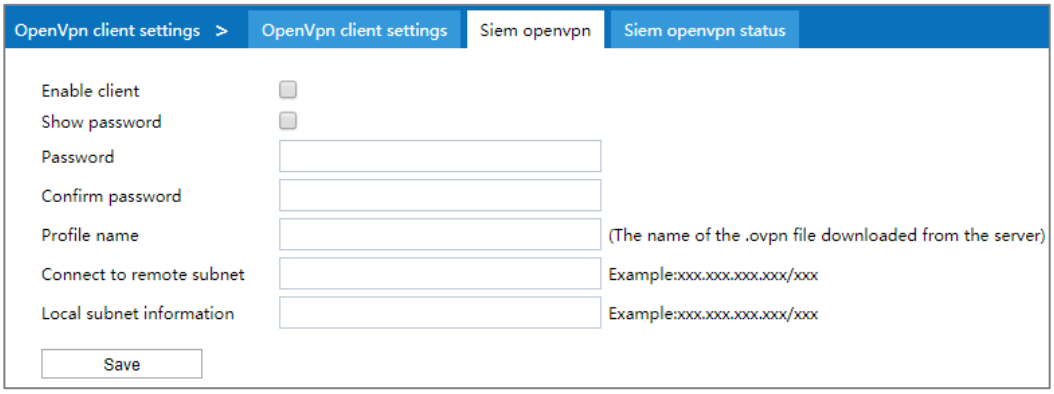
Interface Element	Description
Enable	Check the enable check box to enable the OpenVPN client.
dev	The drop-down list of OpenVpn work mode, the options are as follows: • tun: Tun mode is the routing mode, which creates an IP routing tunnel through OpenVPN. • tap: tap mode is the bridging mode, which creates a bridging network tunnel through OpenVPN.
proto	The drop-down list of OpenVPN data transmission protocol type. The options are: • tcp: Transmission Control Protocol; • udp: User Datagram Protocol.
remoteip	IPv4 address information of OpenVPN server, such as 192.168.10.11.
port	The port number monitored by the OpenVPN server. The default value is 1194. The value range is 1-65535.
ca	CA (Certificate Authority) certificate file name, which is the CA certificate used by OpenVPN client and server. It is mainly used to verify the legitimacy of server or client certificate.

Interface Element	Description
authtype	The drop-down list of OpenVPN certificate type. The options are: • txt: use user name and password for authentication. • ssl: use SSL (Secure Sockets Layer) certificate for authentication.
tls-auth	TLS (Transport Layer Security) authentication key file name, enhanced authentication encryption, and synchronization with the server.
cipher	The drop-down list of OpenVPN encryption algorithm. The client and server are synchronized. The options are as follows: • NONE • BF-CBC • DES-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • RC2-64-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC
comp-lzo	LZO drop-down list, options are: • Enable: enable LZO algorithm to compress data, which is consistent with the server settings. • Disable.
cert	In SSL authentication mode, the certificate file name of OpenVPN client.
key	In SSL authentication mode, the key file name of OpenVPN.
txtuser	In Txt authentication mode, the user name of OpenVPN client.
txtpassword	In Txt authentication mode, the user password of OpenVPN client.
nobind	Nobind drop-down list, options are: • Enable: the device does not bind any port to listen for incoming data. • Disable.

Note
CA, TLS-Auth, Cert, Key and other authentication files can be imported on the "VPN Tunnel > Certificate Settings" page.

Interface Description 2: Siemens OpenVPN

Siemens OpenVPN interface is as follows:

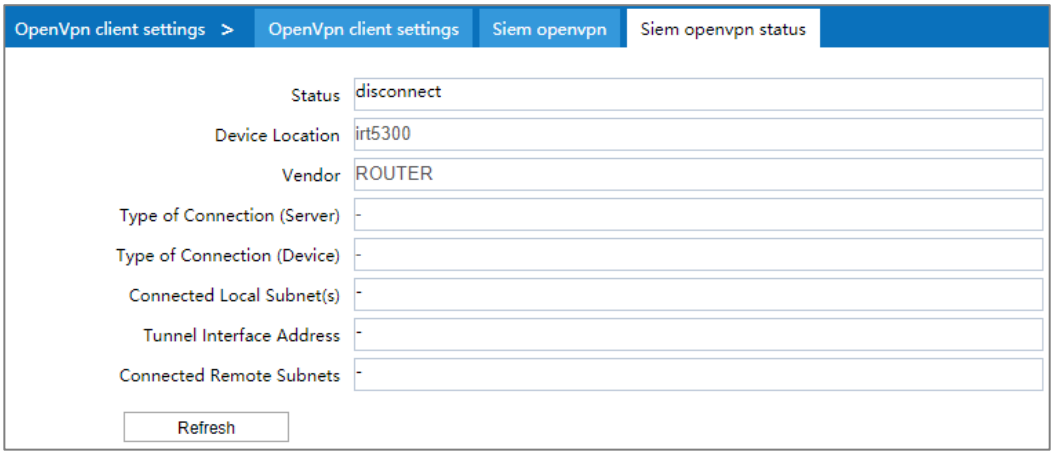


Main elements configuration descriptions of Siemens openvpn interface:

Interface Element	Description
Enable client	Enable check box to enable Siemens OpenVPN client.
Show password	Show password check box. Check it to view password information.
Password	Device password of the OpenVPN server.
Confirm password	Enter the device password of the OpenVPN server again.
Profile Name	The profile of OpenVPN server contains the configuration and authentication information of VPN server. Note The profile can be imported on the “VPN Tunnel > Certificate Settings” page.
Connect to remote subnet	IP address and subnet mask information of the remote OpenVPN server network.
Local subnet information	IP address and subnet mask information of the local subnet.

Interface Description 3: Siemens openvpn State

Siemens openvpn state interface is as follow:



The main elements configuration description of Siemens openvpn state interface:

Interface Element	Description
Status	Display OpenVPN connection status.
Device Location	Display the geographic location or name of the device.
Vendor	Display the supplier name.
Type of Connection (Server)	Displays the connection type of the server.
Type of Connection (Device)	Display the connection type of the device.
Connected Local Subnet(s)	Display the information of the connected local subnet.
Tunnel Interface Address	Displays the tunnel interface address.
Connected Remote subnet	Display the information of the connected remote subnets.

7.8 Certificate Settings

Function Description

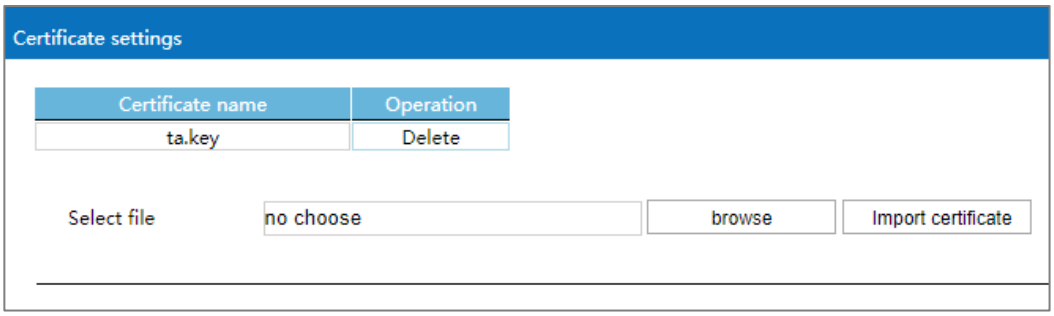
On the “Certificate Settings” page, you can add OpenVPN client authentication certificates and related configuration files.

Operation Path

Open in order: "VPN Tunnel > Certificate Settings".

Interface Description

Certificate Settings interface is as follows:



The main element configuration description of Certificate Settings interface:

Interface Element	Description
Certificate name	Certificate name.
Operation	Click “Delete” to delete the corresponding certificate file.
Select file	Click “Browse” to select a local certificate file, and then click “Import Certificate” to upload the certificate file to the device. Note: Only files in ". crt", ".key" or ". ovpn" format can be uploaded.

8 System Management

8.1 Time Settings

Function Description

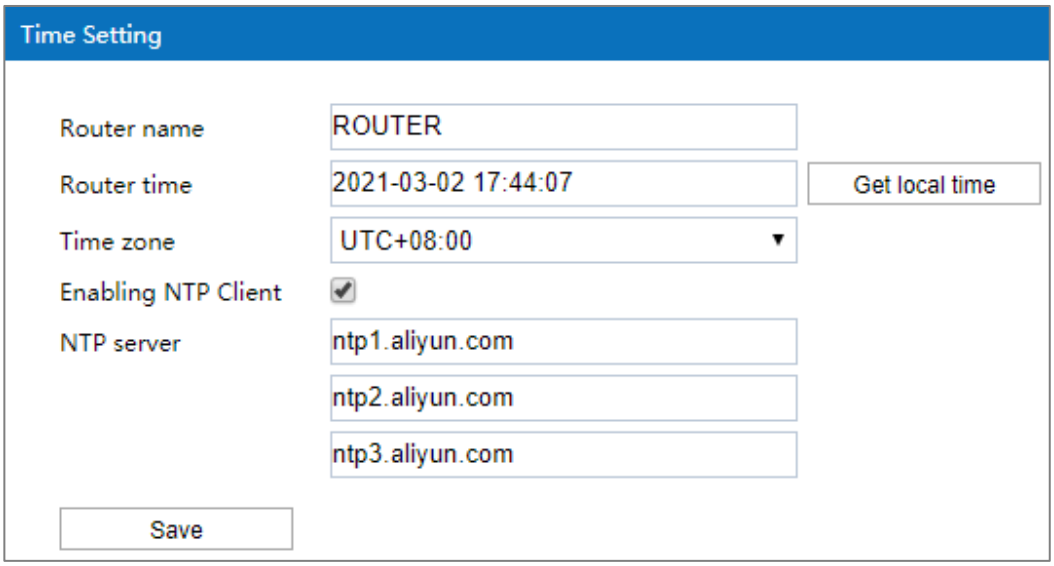
On the page of "Time Setting", user can configure time-related parameters information.

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	Description
Router name	The name of the router.
Router time	The time of the router, the format is: year-month-day hour:

Interface Element	Description
	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.
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.
Save	Synchronize client and server time by clicking the button of "Save"

8.2 Access Settings

Function Description

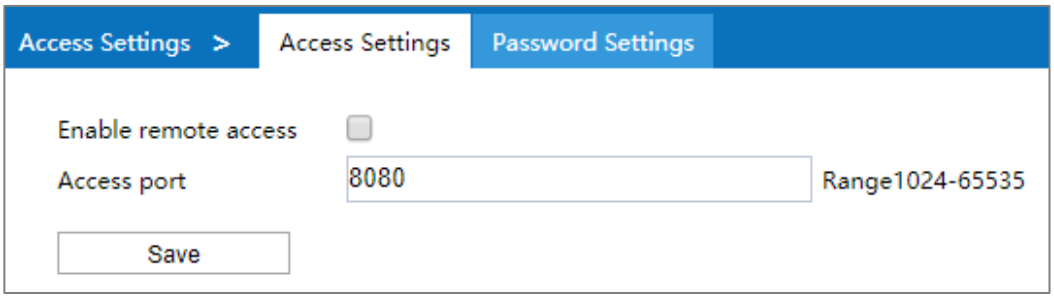
On the page of "Access settings", user can enable remote access and modify the username and password for accessing the device.

Operation Path

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

Interface Description 1: Access Settings

Access settings interface as follows:



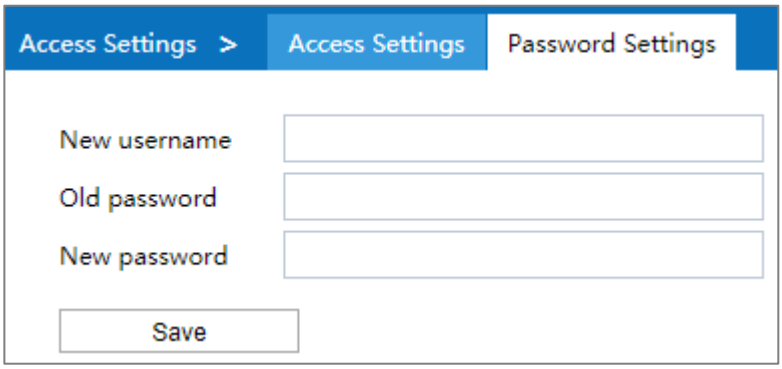
The main elements configuration description of access settings interface:

Interface Element	Description
Enable remote access	Remote access enable checkbox, check to enable remote access, the user can access the device through the

Interface Element	Description
	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	Description
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.

8.3 Timed Restart

Function Description

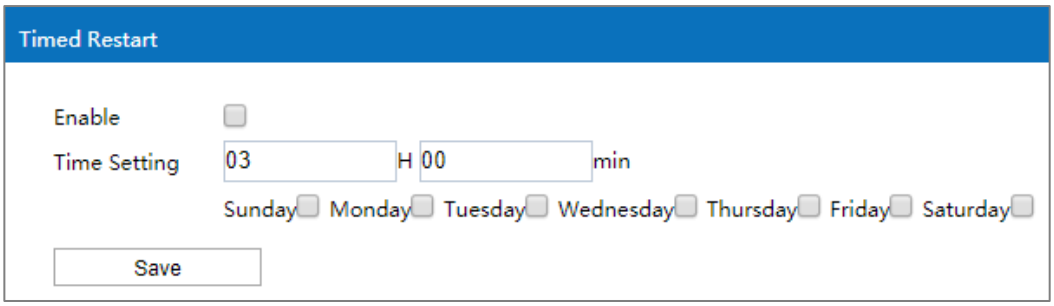
On the page of "Timed restart", user can configure the time for the device to automatically restart.

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

8.4 Backup Recovery

Function Description

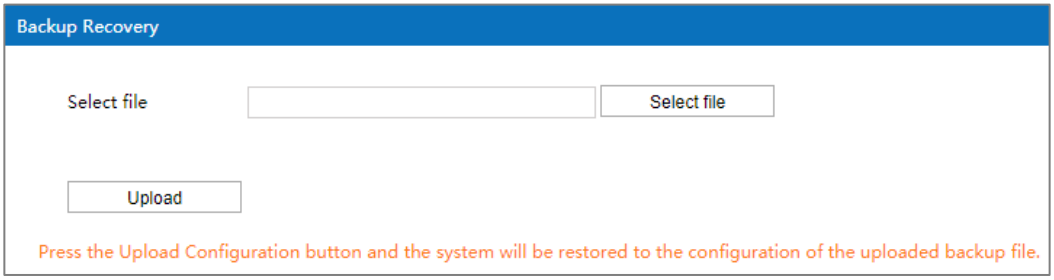
On the page of "Backup Recovery", user can select files for uploading configuration.

Operation Path

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

Interface Description

The backup recovery settings interface as follows:



The main elements configuration description of backup recovery settings interface:

Interface Element	Description
Select file	The "Select file" button allows user to select the backup configuration file for the host.
Upload	Click the "Upload" button to upload the backup configuration file to the current device, so that the device can restore the configuration in the backup file.

8.5 Log Manage

Function Description

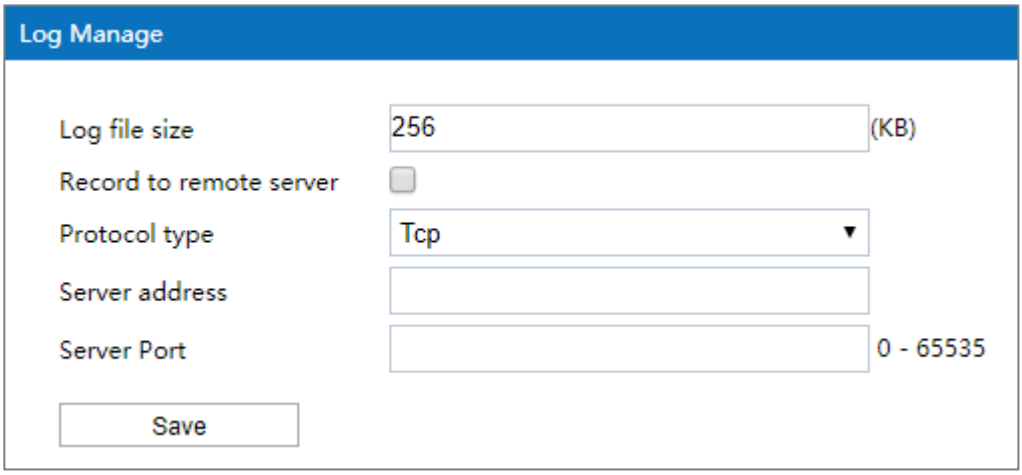
On the page of "Log Manage", user can record the log files to the remote server.

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	Description
Log file size	Set the size of the log file, the default is 256KB.
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 remote server, options as follows: • TCP

Interface Element	Description
	• UDP
Server Address	IP address information of the remote server
Server Port	Port number of the remote server.

8.6 Firmware Upgrade

Function Description

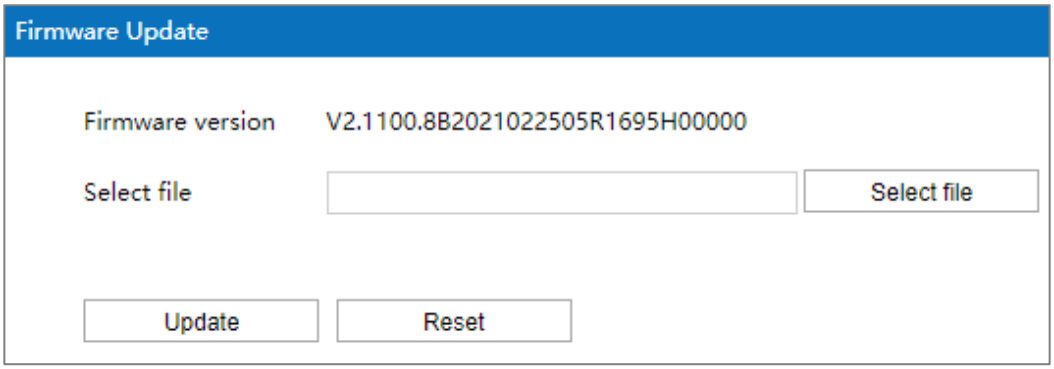
On the "Firmware Upgrade" page, user can update the device system program via firmware upgrade.

Operation Path

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

Interface Description

System upgrade interface is as follows:



The main element configuration description of Firmware Upgrade interface:

Interface Element	Description
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	Click the button of "Update" to upgrade the device program. Notes: • It takes a while during the upgrade process. Do not power off the device. • After a successful upgrade, the configuration of the device will remain unchanged and the firmware version information will be changed.

8.7 System Settings

Function Description

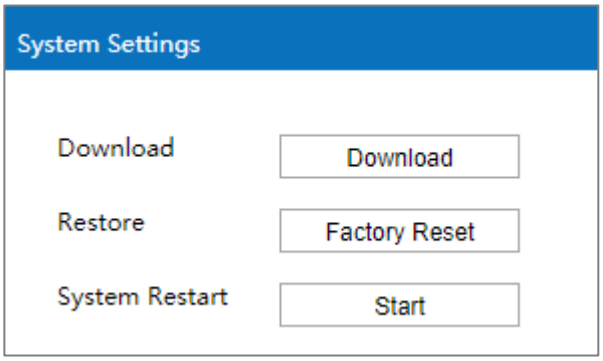
On the “System Settings” page, you can download the current configuration files, restore factory settings or reboot the device.

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	Description
Download	Click “download” button, you can download the current configuration “bakup.file” to local PC to backup the device configuration.
Restore	Click “Factory Reset” button, then click "OK” button to confirm restoring factory defaults.
System Restart	Click “Start” to reboot the device system. After the system restarts, it will jump back to the login interface.

9 Diagnostic Tools

9.1 System Log

Function Description

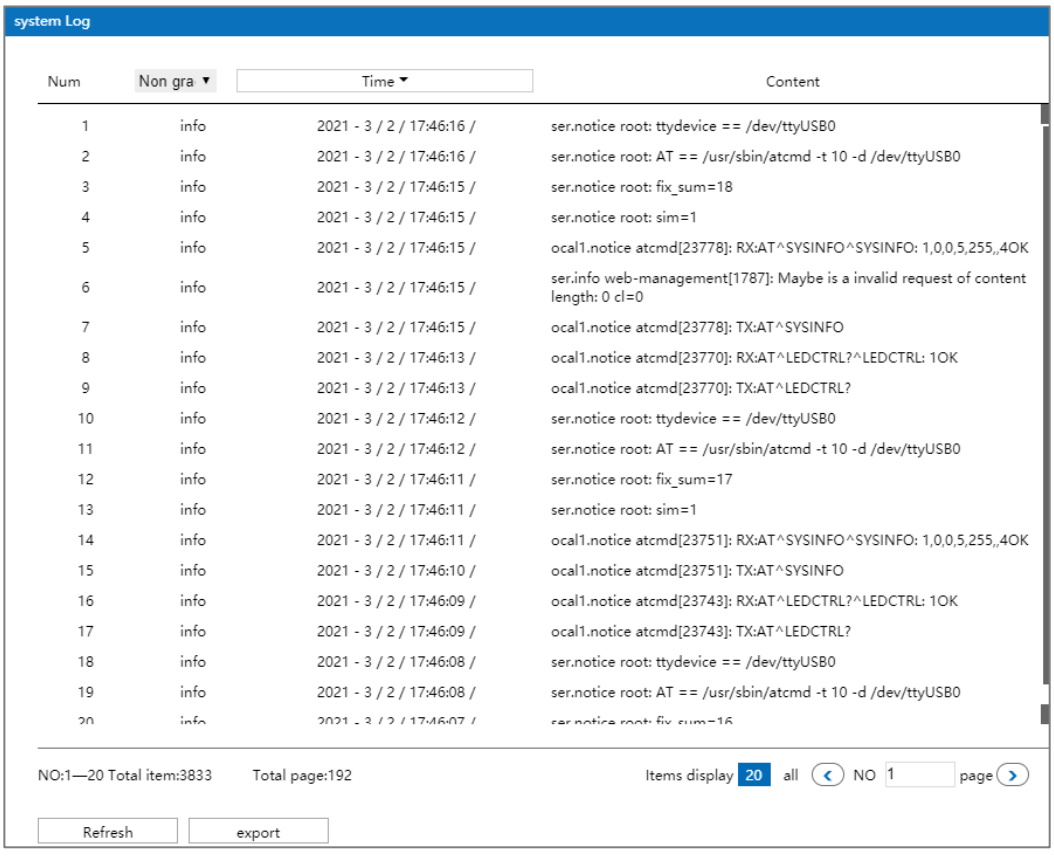
On the page of "System log", user can view the device system logs.

Operation Path

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

Interface Description

System log interface as follows:



The main elements configuration description of system log interface:

Interface Element	Description
Num	Log messages display sequence.
None	User can select the category of log to display specific log information. Optional values: • NONE: 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".

9.2 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

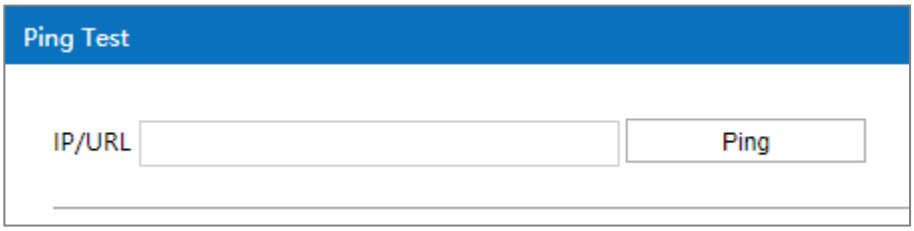
On the page of "Ping test", user can detect whether the target host can be connected.

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	Description
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.

9.3 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

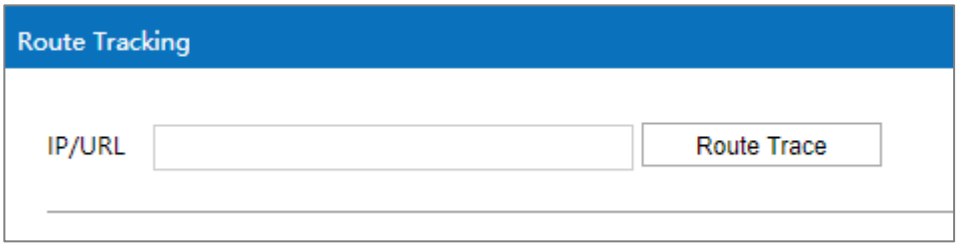
On the page of "Route Tracking", user can perform route tracking for the target host.

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	Description
IP/URL	Destination IP/URL address that requires route tracking.
Route Trace	Click the "Route Trace" button to start tracking, and the test results are displayed below.

10 Maintenance and Service

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 product, consumers can get help and solutions in the following ways:

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

10.1 Internet Service

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

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

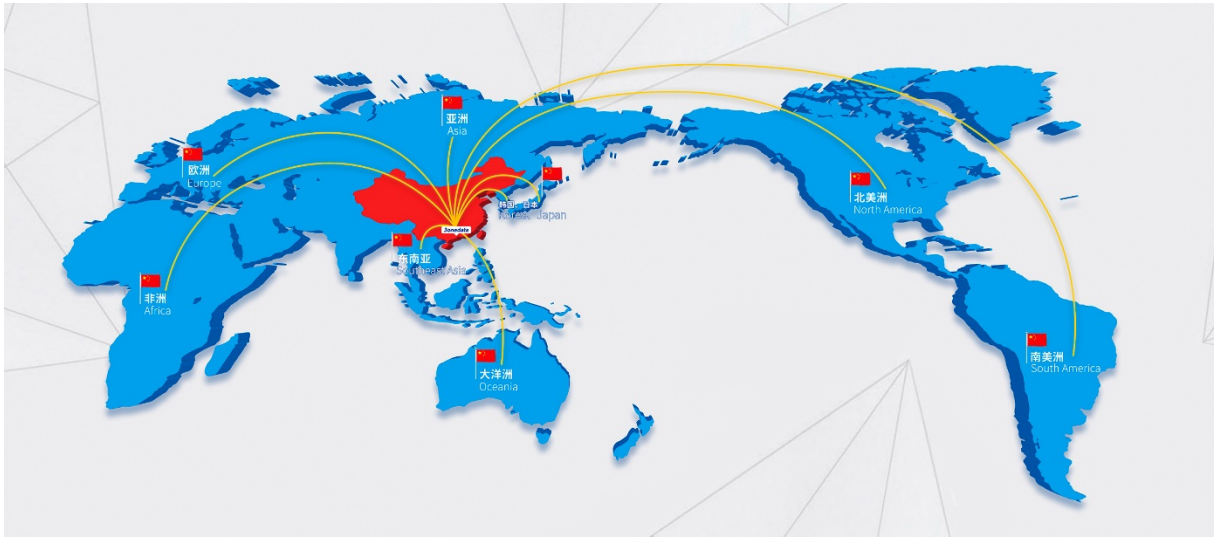
10.2 Service Hotline

Users using our company products can call technical support office. Our company has professional technical engineers to answer the questions and help solve the products or usage problems ASAP. Free service hotline: +86-4008804496

10.3 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, 518108, China
Technology Support:	tech-support@3onedata.com
Service Hotline:	4008804496
Official Website:	http://www.3onedata.com