3onedata



ICPE3300-C61 Series
Industrial 5G CPE
User Manual

Document Version: 01

Issue Date: 10/13/2026

Industrial Ethernet Communication Solution Expert **3onedata Co., Ltd.**

Copyright © 2026 3onedata Co., Ltd. All rights reserved.

No company or individual is allowed to duplicate or transmit this manual in any forms without written permission issued by 3onedata Co., Ltd.

Trademark Statement

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

Notice

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

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

3onedata



3onedata Co., Ltd.

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

Preface

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

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

Audience

This manual applies to the following engineers:

- Network administrators responsible for network configuration and maintenance
- On-site technical support and maintenance personnel
- Network engineer

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.

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’ provides links to various sections of this chapter, as well as links to the Principles/Operations Section of this chapter.

Copyright © 3onedata Co., Ltd.

Icon Convention

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 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.

Revision Record

Version No.	Revision Date	Revision Note
01	10/13/2026	Product release

Copyright © 3onedata Co., Ltd.

Contents

PREFACE 1
CONTENTS I
1 LOGIN TO THE WEB INTERFACE 1
1.1 SYSTEM REQUIREMENTS FOR WEB BROWSING 1
1.2 SET THE IP ADDRESS OF PC 1
1.3 LOGIN TO THE WEB CONFIGURATION INTERFACE 2
2 SYSTEM INFORMATION 4
3 MOBILE NETWORK INFORMATION 8
4 BASIC NETWORK 10
4.1 WAN MODE 10
4.2 WIFI& CELLULAR WIRELESS ROAMING 11
4.2.1 Policy Status 11
4.2.2 Roaming Policy 12
4.3 WAN NETWORK SETTINGS 19
4.4 FREQUENCY LOCKING SETTING 25
4.5 MOBILE DETECTION 28
4.6 LINK BACKUP 30
4.7 LOCAL AREA NETWORK 31
4.8 DYNAMIC DOMAIN NAME 33
4.9 ROUTING TABLE 34
5 WLAN SETTINGS 37
5.1 BASIC PARAMETER SETTINGS 37
5.2 WIRELESS CLIENT FILTERING 48
6 ADVANCED NETWORK 51
6.1 PORT FORWARD 51
6.2 PORT REDIRECTION 52
6.3 DMZ SETTINGS 53
6.4 SERIAL PORT SETUP 54
6.4.1 Serial Port Setup 54
6.4.2 Serial Port Server setting 56
6.4.3 Serial Log 73
6.5 UPNP SETTINGS 74
6.6 MULTICAST NAT 76
6.7 VRRP 77

Copyright © 3onedata Co., Ltd.

6.8 RIP 81
6.9 OSPF 82
6.10 STATIC DHCP 84
6.11 DHCP CLIENT 85
6.12 QOS 86
6.13 SNMP 88
6.14 SLA 89
6.15 TRACK 90
7 FIREWALL 92
7.1 IP FILTER 92
7.2 MAC FILTERING 94
7.3 URL FILTERING 95
7.4 KEYWORD FILTER 96
7.5 IP ADDRESS BLACK/WHITE LIST 97
8 VPN TUNNEL 100
8.1 GRE SETTINGS 100
8.2 PPTP CLIENT SETTINGS 101
8.3 PPTP SERVER SETTINGS 103
8.4 L2TP CLIENT SETTINGS 104
8.5 L2TP SERVER SETTINGS 106
8.6 IPSEC 108
8.7 OPENVPN CLIENT SETTINGS 111
8.8 CERTIFICATE SETTINGS 114
9 SYSTEM MANAGEMENT 116
9.1 DEVICE ALIAS 116
9.2 TIME SETTINGS 117
9.3 ACCESS SETTINGS 118
9.4 TIMED RESTART 119
9.5 BACKUP RECOVERY 120
9.6 LOG MANAGE 121
9.7 FIRMWARE UPGRADE 122
9.8 SYSTEM SETTINGS 123
9.9 SYSTEM LOG 124
10 DIAGNOSTIC TOOLS 126
10.1 PING TEST 126
10.2 ROUTE TRACKING 127
11 FAQ 128
12 MAINTENANCE AND SERVICE 131
12.1 INTERNET SERVICE 131
12.2 SERVICE HOTLINE 131
12.3 PRODUCT REPAIR OR REPLACEMENT 132

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

1 Login to the WEB Interface

1.1 System Requirements for WEB Browsing

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

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

1.2 Set the IP Address of PC

The default management network address of the device is as follows:

IP Settings	Default Value
IP address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Please confirm the computer has installed and enabled Ethernet network card.
- Before conducting remote configuration, please confirm the route between computer and device is reachable.
- Before making a local configuration, make sure that the IP address of the computer and the device are on the same subnet.

Copyright © 3onedata Co., Ltd.

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.

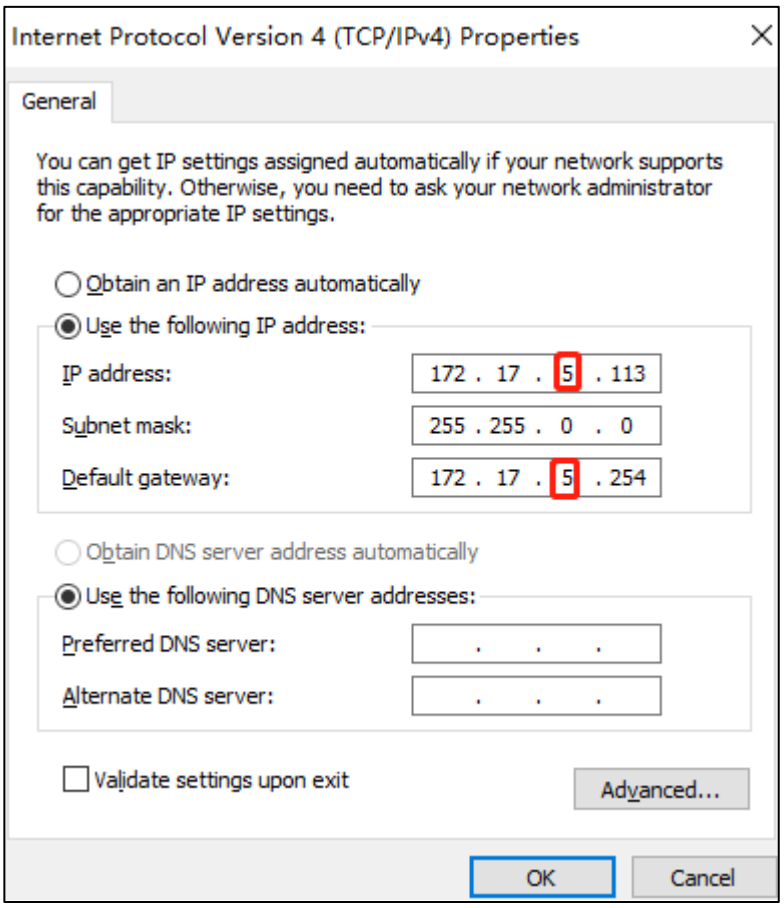
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps are as follows:

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

Step 2 Change the "5" selected by the red frame in the figure to "1".



Step 3 Click "OK", modification is successful.

Step 4 End.

1.3 Login to the WEB Configuration Interface

Operation Steps

Log in to the WEB configuration interface as follows:

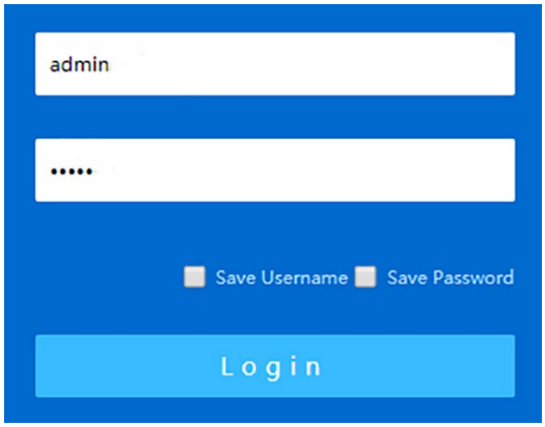
Copyright © 3onedata Co., Ltd.

Step 1 Run the computer browser.

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

Step 3 Click the “Enter” key.

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



Note:

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

Step 5 Click "Login".

Step 6 End.

After login successfully, user can configure relative parameters and information of WEB interface according to demands.

Note:

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

Copyright © 3onedata Co., Ltd.

2 System Information

Function Description

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

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

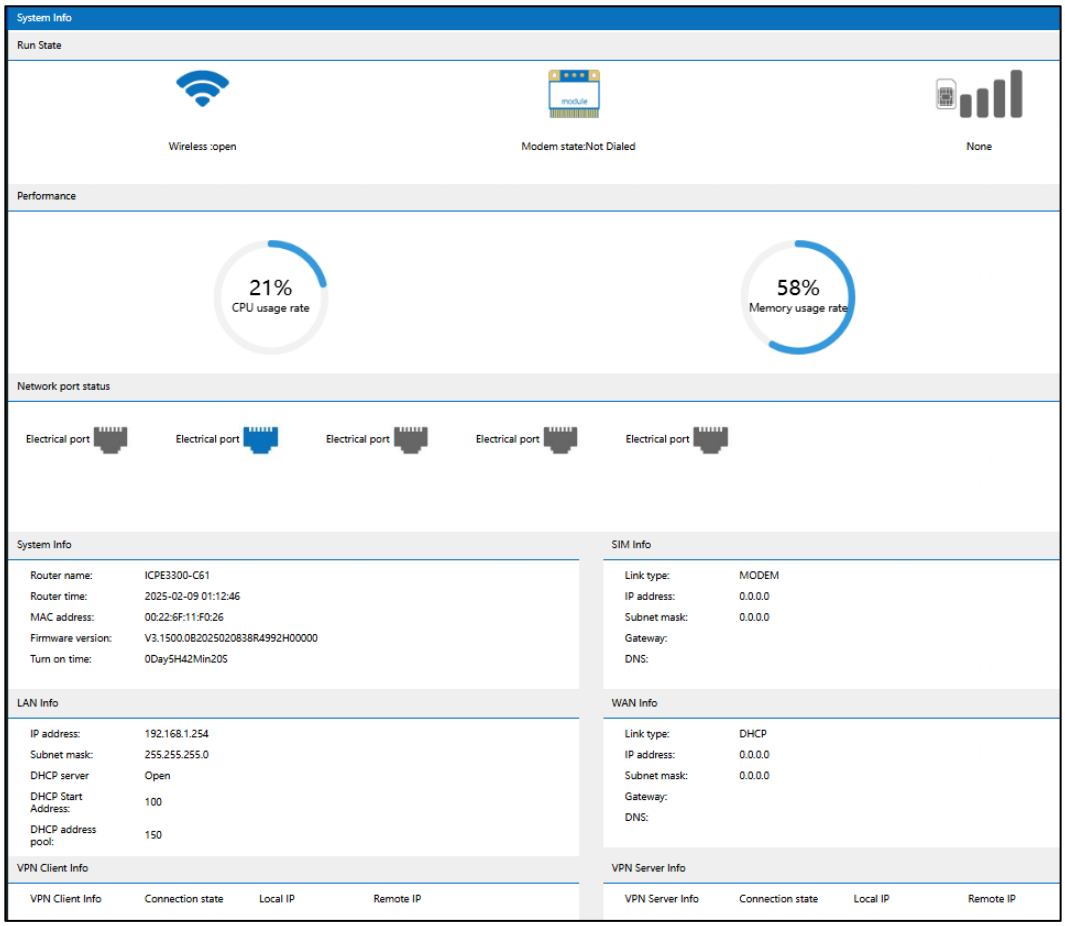
Operation Path

On the navigation bar, select "System information".

Interface Description

System information interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of System Info 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 state of device 5G module Modem.
SIM card	Information including the existence state of SIM card used by current device, operator's network, network operating mode and signal strength etc.
Performance	**The performance bar**
CPU usage rate	Device CPU utilization rate (%).
Memory usage rate	Device memory utilization rate (%). Note: It will influence the device performance if the program takes up too much memory.
Network port status	**Network port status bar**

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Electrical port	Display copper port state: •  : Gray indicates that the copper port is disconnected; •  : Blue indicates that copper port is connected.
System Info	**System information bar**
Router name	Display the device name.
Router time	The current time displayed by router. Its format is Year-Month-Day Hour: Minute: Second.
MAC address	The MAC address of this device.
Firmware version	Device firmware version.
Turn on time	The run time after turning on the device
SIM Info	**SIM information bar**
Link type	SIM connection Type
IP address	IP address obtained by SIM card from network operator.
Subnet mask	Subnet mask address of SIM.
Gateway	The gateway address of SIM.
DNS	DNS server address of SIM.
LAN Info	**The LAN information bar**
IP address	The IP address information of LAN.
Subnet mask	The subnet mask information of LAN.
DHCP Server	The state of the DHCP server function. • Disable; • Enable.
DHCP Start Address	The minimum host number of IP address assigned by DHCP address pool, which is 100 by default.
DHCP address pool	The maximum IP address number assigned by DHCP address pool, which is 150 by default
WAN Info	**The WAN information bar**
Link type	The connection type of WAN.
IP address	The IP address information of WAN.
Subnet mask	The subnet mask information of WAN.
Gateway	The gateway information of WAN
DNS	The DNS information of WAN
VPN Client Info	**The VPN client information bar**

Copyright © 3onedata Co., Ltd.

Interface Element	Description
VPN Client Info	Related information about VPN client. It displays related information when VPN client is enabled.
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.
Connection state	The connection state of VPN server: • Not connected; • Connected.
Local IP	The IP address of local server.
Remote IP	The IP address of remote client.

Copyright © 3onedata Co., Ltd.

3 Mobile Network Information

Function Description

On the "Mobile Network Info" page, user can check the following information:

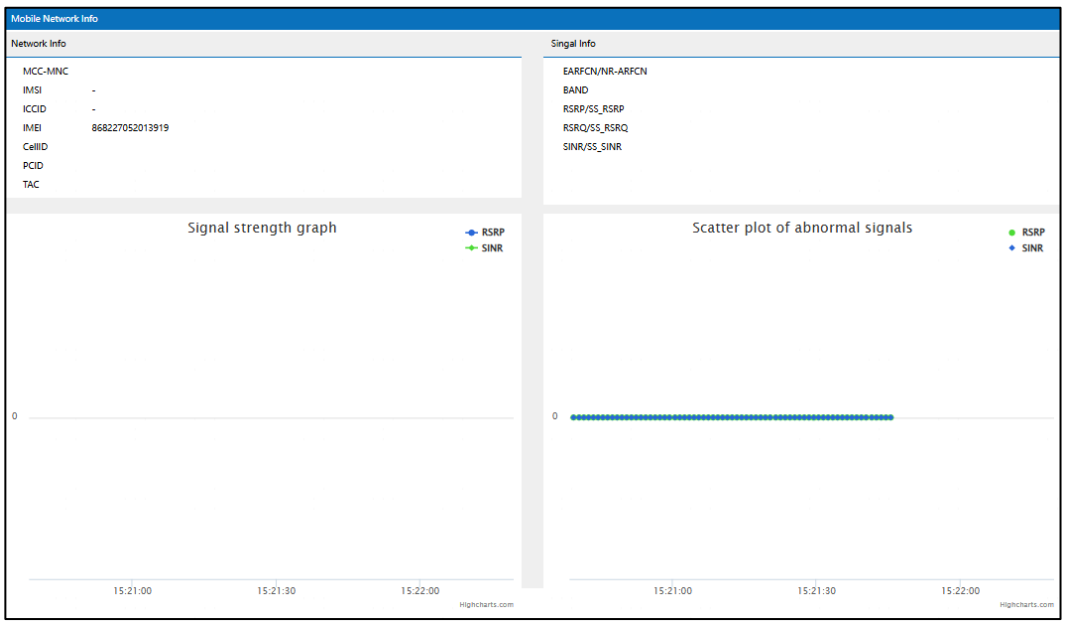
- Network information
- Signal information
- Curve graph of current signal strength
- Scatter diagram of abnormal signal

Operation Path

On the navigation bar, select "Mobile Network Info".

Interface Description

The Mobile Network Information interface is as follows:



The main element configuration description of Mobile Network Information interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Network Info	**Network information bar**
MCC-MNC	The mobile identification code of the currently registered network, which is used to identify the country/region and operator of the network.
IMSI	The mobile subscriber identification code of the current SIM card is used to identify and verify the identity of the mobile subscriber in the mobile network.
ICCID	ICCID stands for Integrated Circuit Card Identification Code, which is the unique identifier for SIM cards.
IMEI	International Mobile Device Identification Code.
Cell ID	The currently registered cell number, used to locate the device.
PCID	The current physical cell number, used to locate the device.
TAC	The current tracking area code, used to identify different location areas.
EARFCN/NR-ARFCN	The current absolute frequency point, used to identify the working RF channel number of the 5G module.
BAND	The current radio frequency band, used to identify the working RF band number of the 5G module.
RSRP/SS_RSRP	The reception power of current reference signal. (Only applicable to 4G/5G networks)
RSRQ/SS_RSRQ	The reception quality of current reference signal. (Only applicable to 4G/5G networks)
SINR/SS_SINR	The current signal to interference noise ratio. (Only applicable to 4G/5G networks)
Signal strength graph	It shows the graph of wireless signal receiving power RSRP and signal-to-noise ratio SINR changing with time.
Scatter plot of abnormal signals	It shows the scatter diagram of the abnormal points of wireless signal reception power RSRP and signal-to-noise ratio SINR in time.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

4 Basic Network

4.1 WAN Mode

Function Description

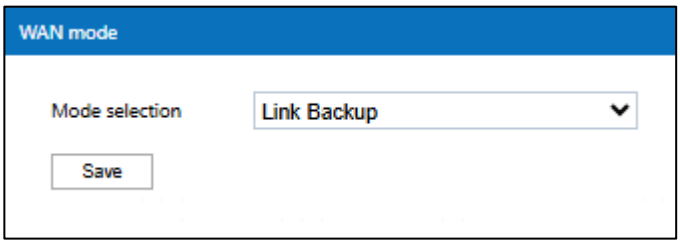
On “WAN mode” page, users can set network mode. The device can be connected to the network via wired (WAN port), wireless roaming (WiFi), or 5G mobile network (SIM card).

Operation Path

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

Interface Description

The WAN mode interface is as follows:



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

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	mobile network.

4.2 WIFI& Cellular Wireless Roaming

Noe
When “WAN mode” is set to “WiFi & Cellular Wireless Roaming”, the “Basic Network” menu will have “WiFi & Cellular Wireless Roaming”.

4.2.1 Policy Status

Function Description

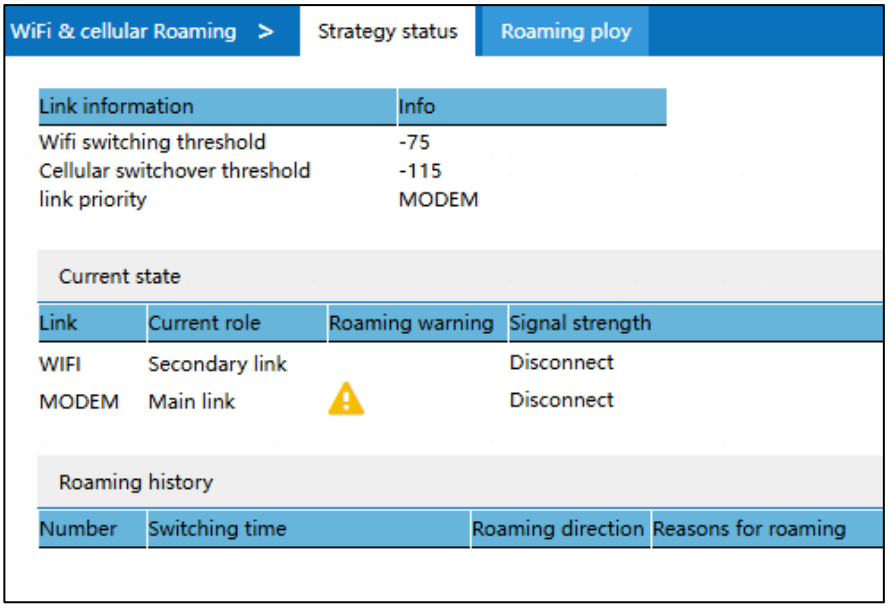
On the "Policy Status" page, users can view link status of current wireless roaming and record of roaming history.

Operation Path

Choose “Basic Network > WIFI & Cellular Roaming > Strategy Status” in the navigation bar.

Interface Description

Strategy status interface is as follows:



The main elements configuration description of strategy status interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Link information	The threshold and link name corresponding to the link information.
Info	Display the threshold for switching signals between Wi Fi and cellular wireless networks, as well as priority link information.
Current state	**Current status display bar**
Link	Display link name information, which can be taken as: • WIFI • MODEM
Current role	Display the current role of the link, which can be taken as: • Main link • Deputy link
Roaming warning	Prompt whether the current roaming conditions have been met and whether the roaming is about to take place, values are: •  : At present, the roaming conditions have been satisfied, and the roaming will happen soon. •  : At present, the roaming conditions are not satisfied, so there is no need for roaming
Signal strength	Displays the strength of the current link signal in dBm.
Roaming history	**Roaming history display bar** Note: Displays only the last 20 roaming records.
Number	Displays the serial number of roaming history record.
Switching time	Show the time of switching link.
Roaming direction	Display the main link after roaming, for example: when the value of roaming direction is WiFi, it means roaming from ZigBee to WiFi.
Reasons for roaming	Shows the specific reason for roaming.

4.2.2 Roaming Policy

Function Description

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

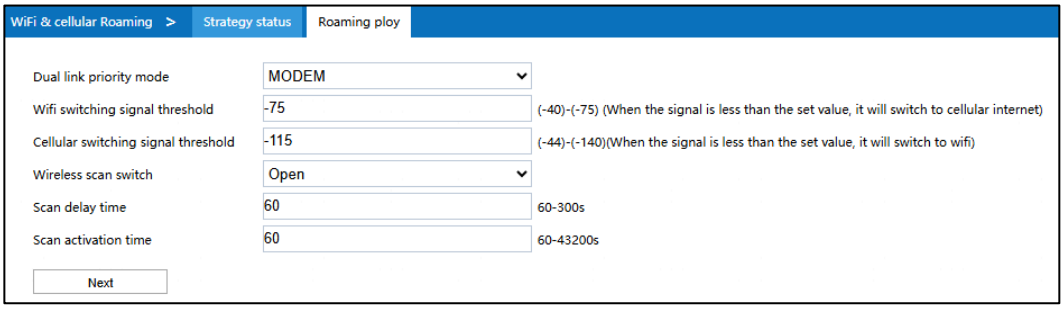
Copyright © 3onedata Co., Ltd.

Operation Path

Choose “Basic Network > WIFI & Cellular Roaming > Roaming Ploy” on the navigation bar.

Interface Description 1: Dual Link Priority Method

The ‘Roaming Ploy’ interface is as follows:



The main element configuration description of “Roaming Ploy - Dual link priority mode” interface:

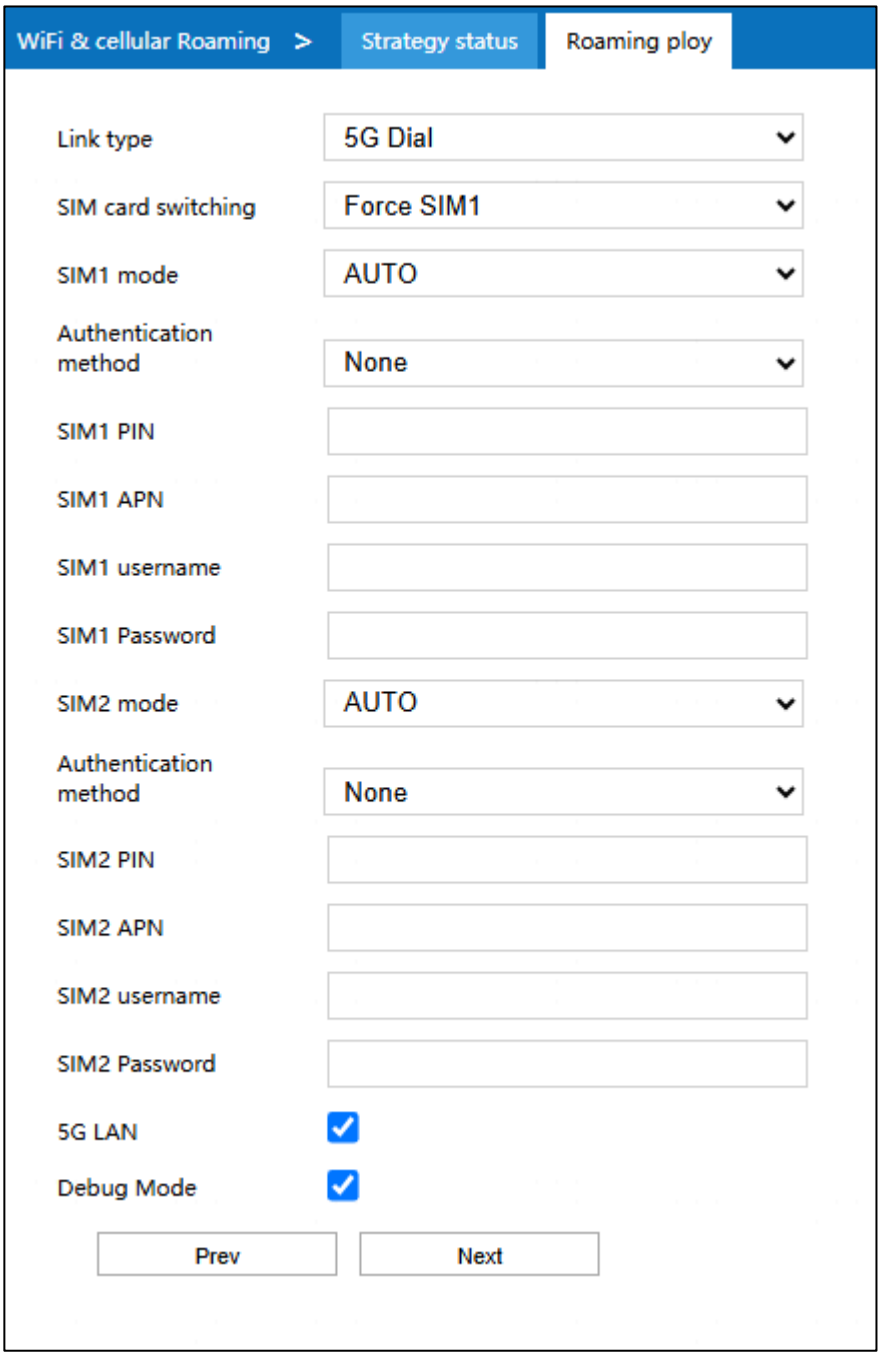
Interface Element	Description
Dual link priority mode	The drop-down list of wireless roaming Link Priority Method, the options are as follows: • MODEM: adopts cellular wireless mobile signal to access network in priority. • WiFi: adopts WiFi wireless signal to access network in priority.
WiFi switching signal threshold	Switch to the cellular wireless accessing network when the peer WiFi signal strength is less than specified threshold, with a value range of -40~-75.
Cellular switching signal threshold	Switch to Wi-Fi accessing network when the peer cellular wireless signal strength is less than specified threshold, with a value range of -44~-140.
Wireless scan switch	For wireless scanning enable switch, options are as follows: • On: When there is no signal from the peer Wi Fi, the wireless scanning time parameter can be customized. • Off: When there is no signal from the peer Wi Fi, the device automatically connects to the peer Wi-Fi service in default mode.
Scan delay time	The wireless scanning delay time is the scanning time interval, with a value range of 60-300s.
Scan activation time	The wireless scanning activation time is the scanning working time, with a value range of 60-43200s.

Copyright © 3onedata Co., Ltd.

Click the "Next" button on the "Roaming ploy" interface to configure 5G network parameters.

Interface Description 2: 5G Dial

Roaming Policy-5G dialing interface is as follows:



The main element configuration description of Roaming Policy-5G dial interface:

Interface Element	Description
Link type	5G Dial

Copyright © 3onedata Co., Ltd.

Interface Element	Description
SIM card switching	In the drop-down list of Switch SIM card, user can choose specified SIM card. The options are: • SIM1; • SIM2.
SIM1 mode	The drop-down list of SIM1 mode. The options are: • Auto: self-adaptation; • 3G: WCDMA/TD-SCDMA; • 4G: LTE; • 5G: NR.
Authentication method	The user authentication method is as follows: • None: Not validate • 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.
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. Note: 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 three times.
SIM1 APN	The SIM1 access point name.
SIM1 username	SIM1 username
SIM1 Password	SIM1 password
SIM2 mode	The drop-down list of SIM2 network mode. The options are: • Auto: self-adaptation; • 3G: WCDMA/TD-SCDMA; • 4G: LTE; • 5G: NR.
Authentication method	The user authentication method is as follows: • None: Not validate • PAP: Password authentication protocol, unencrypted authentication. • CHAP: Challenge handshake authentication protocol,

Copyright © 3onedata Co., Ltd.

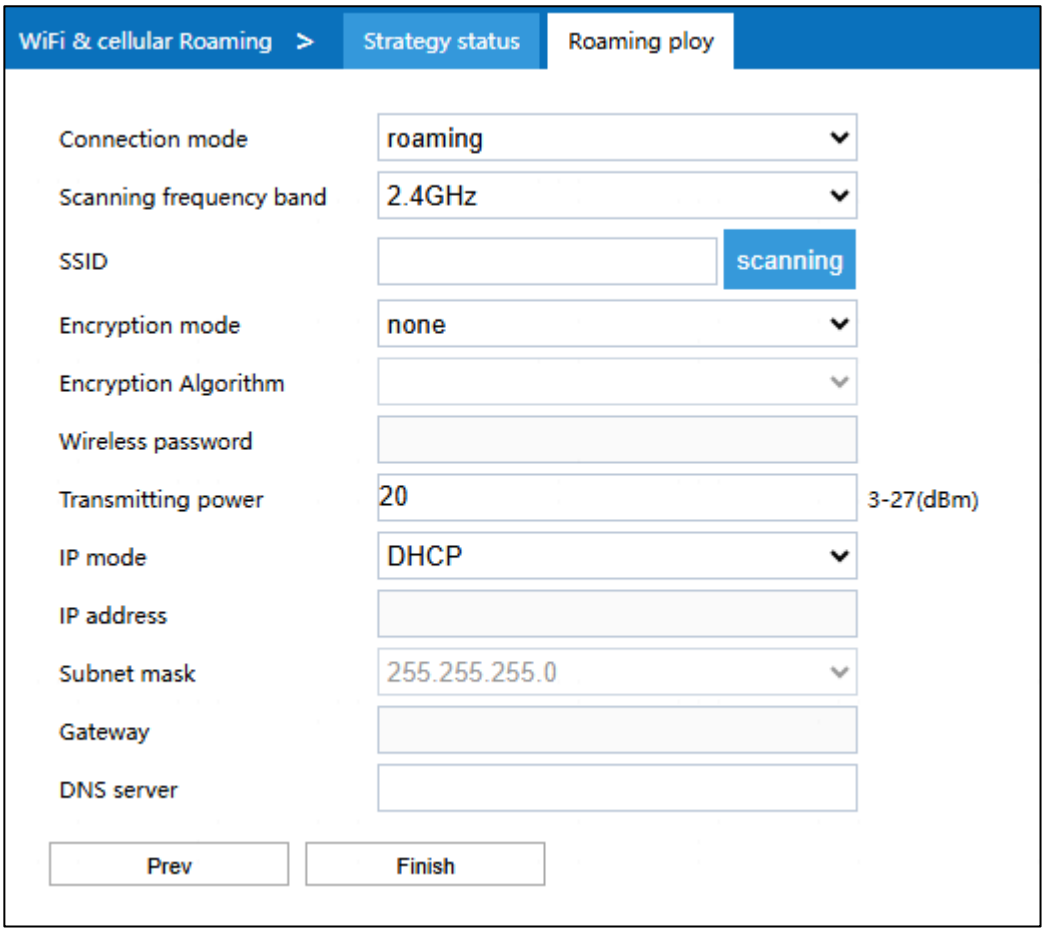
Interface Element	Description
	encrypted authentication. • PAP or CHAP: Select Password Authentication Protocol or Challenge Handshake Authentication Protocol.
SIM2 PIN	The Personal Identification Number (PIN) of SIM2. Please enter 4 to 8 digits PIN code if the boot PIN code is enabled; It is null by default if not enabled. Note: 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 three times.
SIM2 APN	The SIM2 access point name.
SIM2 username	SIM2 username
SIM2 password	SIM2 password
5G LAN	Enable checkbox, check to enable 5G LAN function. Note: • Only the CN version supports 5G LAN function. • 5G LAN is a new feature defined by the 3GPP specification in R16 stage. It is based on the private mobile LAN service of 5G network and the access capability of 5G terminals. It refers to providing flexible communication services such as terminal interconnection or terminal separation for group member terminals by building a "group" for enterprises' terminals and bypassing load balancing device. The communication mode of point-to-point and multipoint transmission based on IP or Ethernet can be applied in LAN. In essence, through 5G technology, terminals are grouped to form a LAN network, that is, LAN over 5G.
Debug mode	Enable the check box, and check it to turn on the Debug function, output the log information related to the dial-up program, and display it in the "System Log".

Click the "Next" button on the "5g Dial" interface to configure WiFi network parameters.

Interface Description 3: WiFi

Roaming Policy-WIFI interface is as follows:

Copyright © 3onedata Co., Ltd.



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

Interface Element	Description
Connection mode	The connection mode between the device and the wireless device on the opposite end is roaming by default: seamless switching between different APS.
Scanning frequency band	Scanning frequency band. Options are as follows: • 2.4GHz • 5GHz
SSID	SSID name of the opposite device wireless network. Note: User can add the wireless signal needed to connect via scan button.
Encryption mode	Encryption mode of opposite device wireless network, options as follows: • No encryption. • WPA2: WiFi Protected Access II is suitable for the individual or average family network. It adopts pre-shared key and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm.
Encryption Algorithm	Wireless network encryption algorithm of the opposite device, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES(CCMP) encryption algorithm is supported.
Wireless password	Password of opposite device wireless network.
Transmitting power	Transmitted power of the device wireless signal, defaults to 20dBm, the value range is 3~27dBm. Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is; • Different device has different transmitting power range.
IP mode	The acquisition mode of wireless roaming segment IP, options following: • DHCP: acquires IP address by DHCP protocol. • Static IP: manually configure IP address.
IP address	The fixed IP address provided by network provider or WAN.
Subnet mask	Drop-down list of netmask.
Gateway	The default gateway address automatically distributed by network provider or outer network.
DNS server	IP address of DNS server. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

Click the 'Finish' button on the 'WiFi Policy' to submit wireless roaming configuration information.

Copyright © 3onedata Co., Ltd.

4.3 WAN network settings

Note
When the "Wan mode" is "link backup", there is "WAN network settings" in the "basic network" menu.

Function Description

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

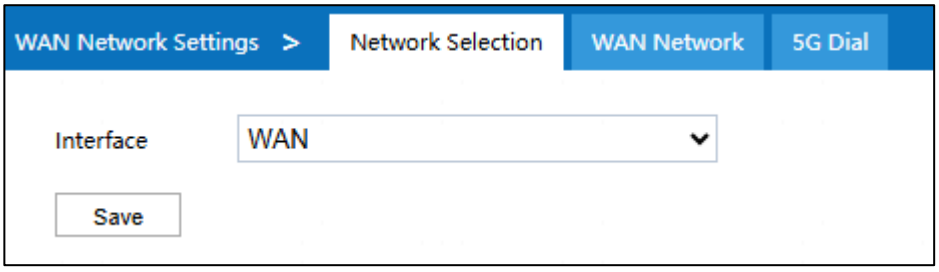
- WAN: connecting WAN through WAN port of the device.
  - Dynamic: the WAN port of the device accesses network address information allocated by network provider or outer network automatically;
  - Static address: configuring the network information of the device WAN port manually;
  - PPPoE: implement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

Operation Path

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

Interface Description 1: Network selection

Network selection interface is as follows:



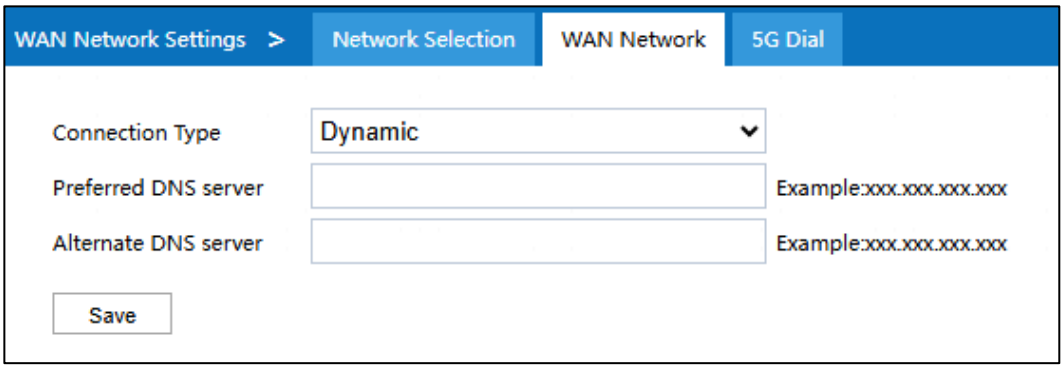
The main elements configuration description of network selection interface:

Copyright © 3onedata Co., Ltd.

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

Interface Description 2-1: WAN Network-Dynamic access

WAN Network-Dynamic interface is as follows:

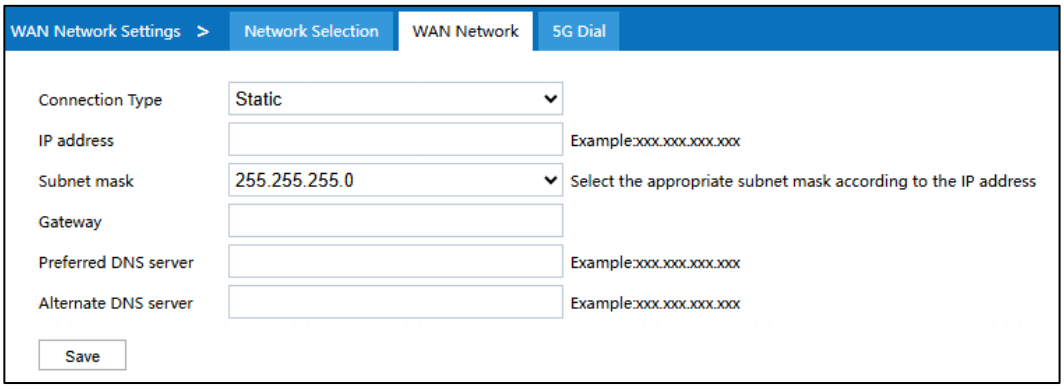


The main elements configuration description of WAN Network-Dynamic interface:

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

Interface Description 2-2: WAN Network-Static Address

WAN Network-Static Address interface is as follows:



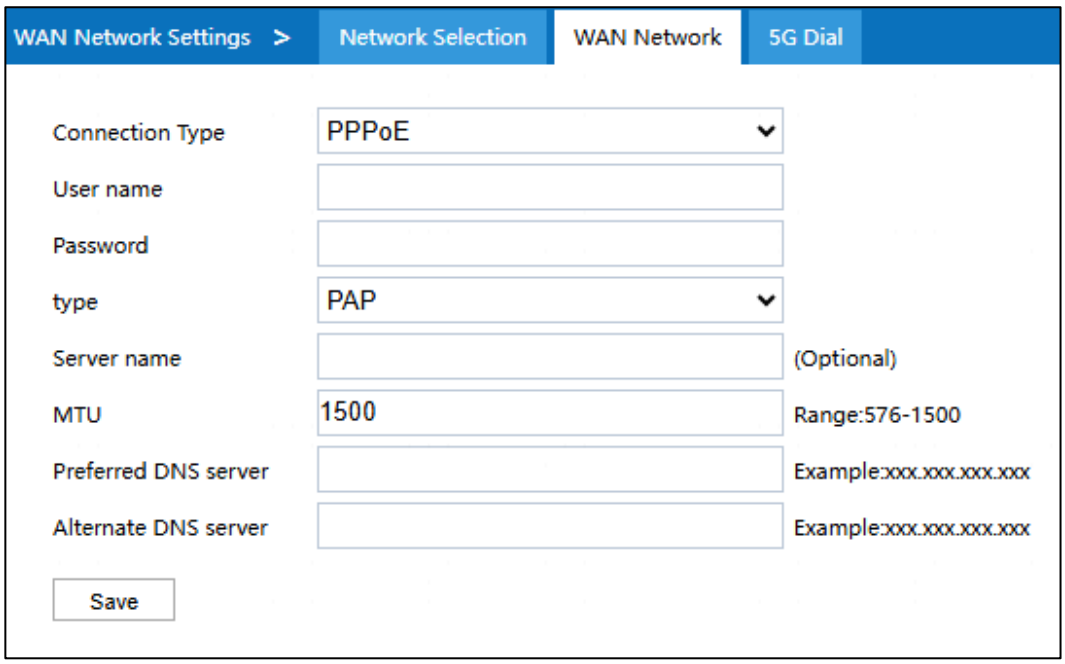
Copyright © 3onedata Co., Ltd.

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

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

Interface Description 2-3: WAN Network-PPPoE Dialing

WAN Network-PPPoE Dialing interface is as follows:



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

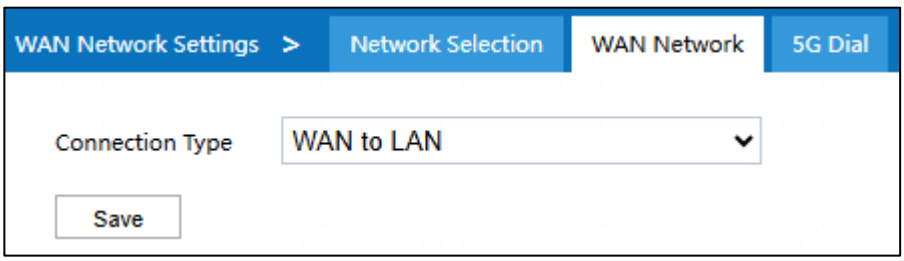
Interface Element	Description
Connection Type	PPPoE dial: realize Internet access via PPPoE point-to-point protocol dialing.
User name	User name of PPPoE connection. Note: User name, password and service name are provided by network provider.

Copyright © 3onedata Co., Ltd.

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

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

WAN Network- WAN to LAN interface is as follows:



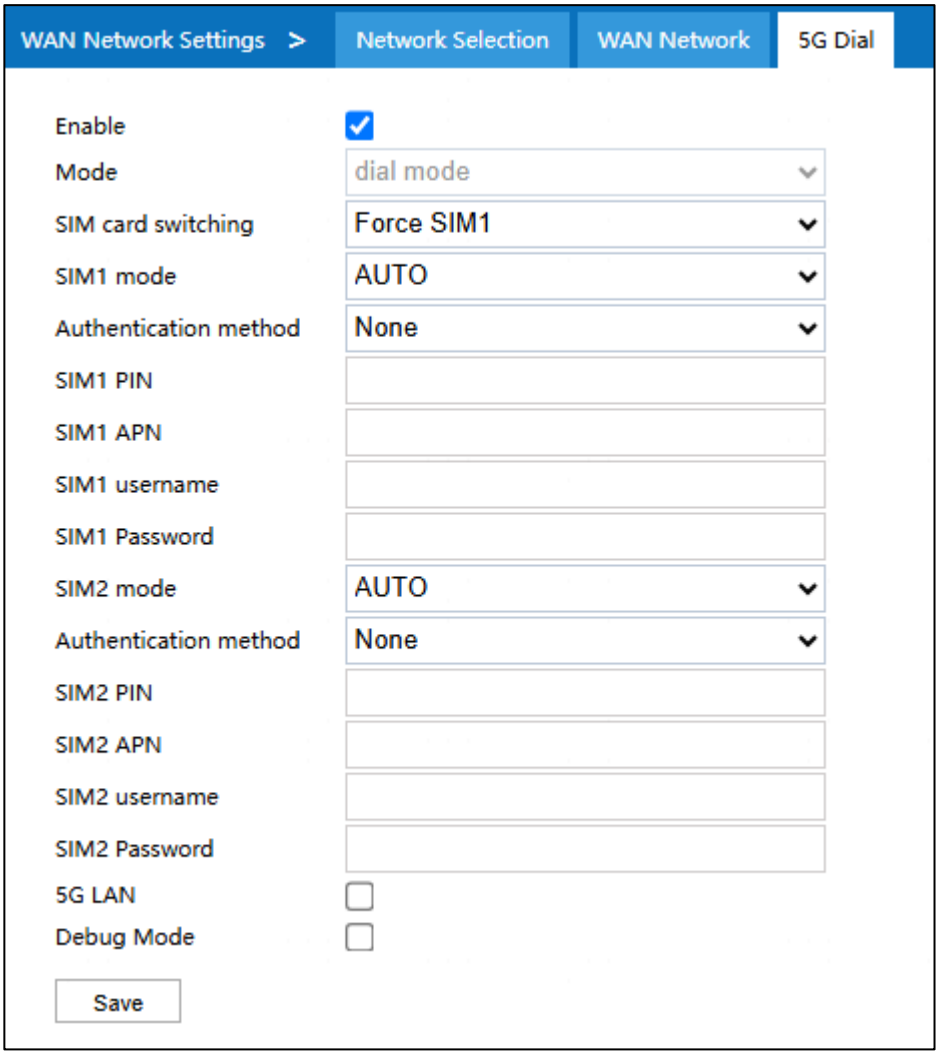
Copyright © 3onedata Co., Ltd.

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

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

Interface Description 3: 5G dial

The 5G dial interface is as follows:



The main elements configuration description of 5G dial interface:

Interface Element	Description
Enable	Enable checkbox, check to enable 5G dialing function.
Mode	The default selection is dial mode. Note: The current system 5G module does not support passthrough mode.
SIM card switching	In the drop-down list of Switch SIM card, user can choose

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	specified SIM card. The options are: • SIM1; • SIM2.
SIM1 mode	The drop-down list of SIM1 mode. The options are: • Auto: self-adaptation; • 3G: WCDMA/TD-SCDMA; • 4G: LTE; • 5G: NR.
Authentication method	The user authentication method is as follows: • None: Not validate • 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.
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. Note: 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 three times.
SIM1 APN	The SIM1 access point name. It defaults to 3GNET.
SIM1 username	The username of SIM1. It defaults to card.
SIM1 Password	The password of SIM1. It defaults to card.
SIM2 mode	The drop-down list of SIM2 network mode. The options are: • Auto: self-adaptation; • 3G: WCDMA/TD-SCDMA; • 4G: LTE; • 5G: NR.
Authentication method	The user authentication method is as follows: • None: Not validate • PAP: Password authentication protocol, unencrypted authentication.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• CHAP: Challenge handshake authentication protocol, encrypted authentication. • PAP or CHAP: Select Password Authentication Protocol or Challenge Handshake Authentication Protocol.
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. Note: 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 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.
5G LAN	Enable checkbox, check to enable 5G LAN function. Note: • Only the CN version supports 5G LAN function. • 5G LAN is a new feature defined by the 3GPP specification in R16 stage. It is based on the private mobile LAN service of 5G network and the access capability of 5G terminals. It refers to providing flexible communication services such as terminal interconnection or terminal separation for group member terminals by building a "group" for enterprises' terminals and bypassing load balancing device. The communication mode of point-to-point and multipoint transmission based on IP or Ethernet can be applied in LAN. In essence, through 5G technology, terminals are grouped to form a LAN network, that is, LAN over 5G.
Debug Mode	Enable the check box, and check it to turn on the Debug function, output the log information related to the dial-up program, and display it in the "System Log".

4.4 Frequency Locking Setting

Function Description

On the "Frequency Lock Settings" page, you can set the frequency band locking and cell locking for the 5G of the SIM card.

Copyright © 3onedata Co., Ltd.

Note:

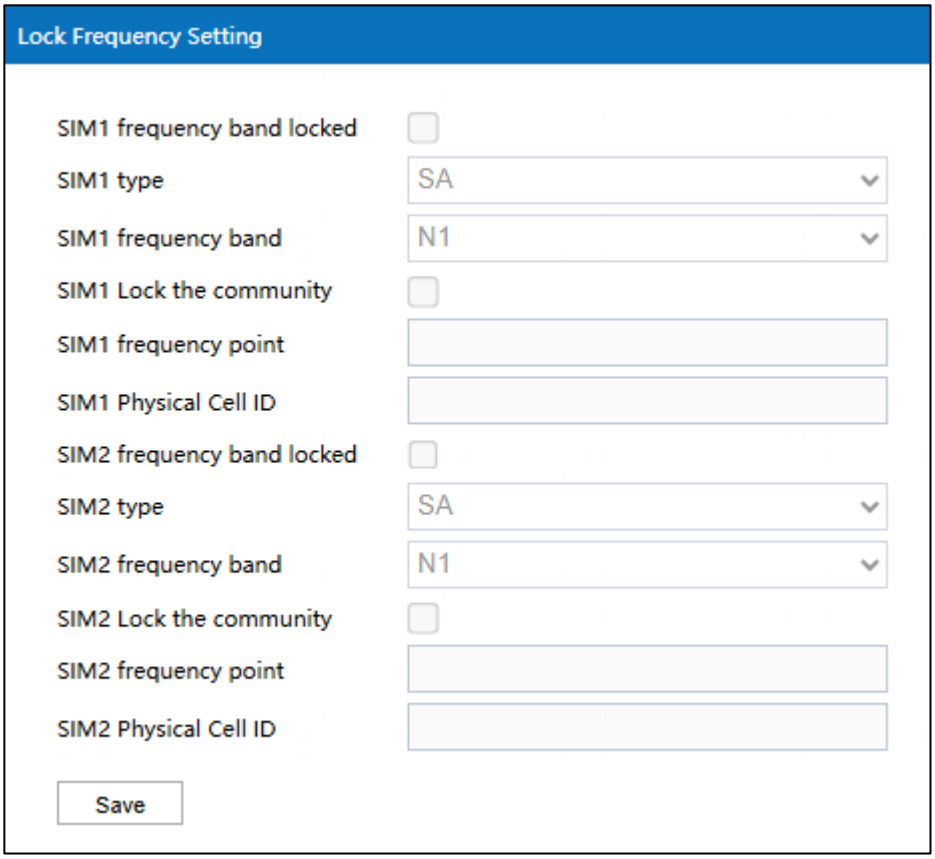
At present, the frequency locking setting only supports the "5G" network mode of SIM card, and the "5G" network mode is enabled. The specific path is "WAN Network Settings > 5G Dialing > SIM1 Mode or SIM2 Mode", and select "5G".

Operation Path

Choose “Basic Network > Lock Frequency Setting” in the navigation bar.

Interface Description

The Frequency Locking Setting interface is as follows:



Configuration description of main elements of the Lock Frequency Setting interface:

Interface Element	Description
SIM1 frequency band locked	The check box of SIM1 frequency band locking, and check it to enable the 5G frequency band locking.
SIM1 type	In the drop-down list of SIM1 type, user can choose specified SIM type. The options are: • SA: independent networking mode.
SIM1 frequency band	The drop-down list of SIM1 frequency band. The options are: • N1;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• N28; • N41; • N77; • N78; • N79. Note: When the locked frequency band is selected, the system will automatically register the frequency band, and you can view the currently registered frequency band in "Mobile Network Information > Signal Information".
SIM1 Lock the community	The check box of SIM1 cell locking, and check it to enable the 5G cell locking.
SIM1 frequency point	Frequency point used by SIM1 card. Note: SIM1“Absolute Frequency points” registered by the system can be viewed in "Mobile Network Information > Signal Information".
SIM1 Physical Cell ID	Physical cell ID is used to uniquely identify each physical cell in a 5G network, that is, the SIM1 frequency band range. Note: SIM1 “Physical cell ID” registered by the system can be viewed in "Mobile Network Information > Network Information".
SIM2 frequency band locked	The check box of SIM2 frequency band locking, and check it to enable the 5G frequency band locking.
SIM2 type	In the drop-down list of SIM2 type, user can choose specified SIM type. The options are: SA: independent networking mode.
SIM2 frequency band	The drop-down list of SIM2 frequency band. The options are: • N1; • N28; • N41; • N77; • N78; • N79. Note: When the locked frequency band is selected, the system will automatically register the frequency band, and you can view the currently registered frequency band in "Mobile Network Information > Signal Information".
SIM2 Lock the community	The check box of SIM2 cell locking, and check it to enable the 5G cell locking.
SIM2 frequency point	Frequency point used by SIM2 card. Note: SIM2 “Absolute Frequency points” registered by the system can be viewed in "Mobile Network Information > Signal Information".

Copyright © 3onedata Co., Ltd.

Interface Element	Description
SIM2 Physical Cell ID	Physical cell ID is used to uniquely identify each physical cell in a 5G network, that is, the SIM2 frequency band range. Note: “Physical cell ID” registered by the system can be viewed in "Mobile Network Information > Network Information".

4.5 Mobile Detection

Note

When "Network Selection" is "modem", this page is displayed.

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.

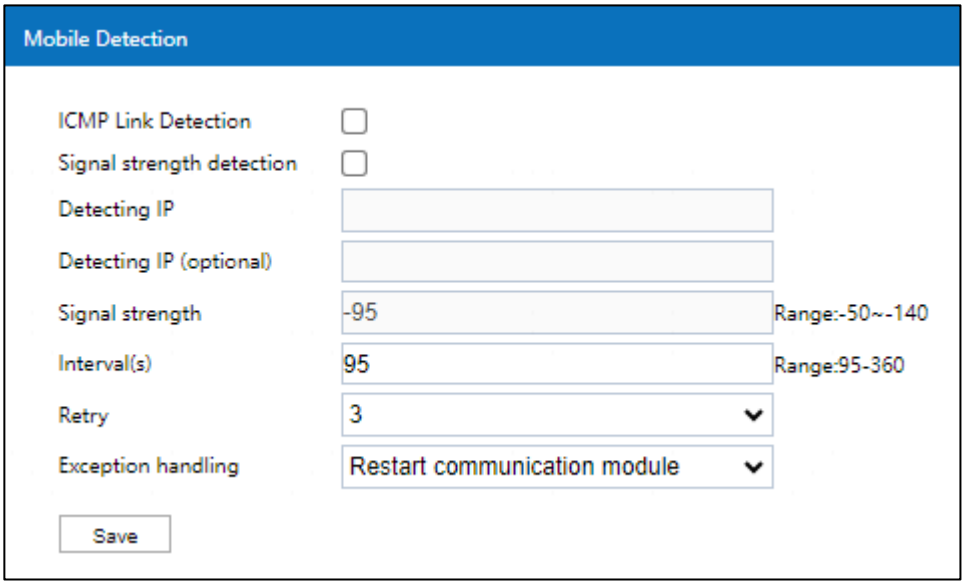
Operation Path

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

Interface Description

The mobile detection interface is as follows:

Copyright © 3onedata Co., Ltd.



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.
Signal strength detection	Check the signal strength detection function checkbox to enable the signal strength detection function, which can detect the link signal strength.
Detecting IP	To detect whether the specified IP address could be connected.
Detecting IP (optional)	To detect whether the backup IP address could be connected.
Signal strength	Set the size of the link signal strength, default to -95, unit in dBm, range: -140~-50. Note: If the system detects that the current 'signal strength' of the device is lower than the default value, it will automatically perform 'exception handling'.
Interval (s)	The time interval of detection, the unit is second. The value range is 95-360.
Retry	To detect the times of retry, the drop-down list of retry. Options are: 2-5.
Exception handling	The corresponding way of handling detected exception. The drop-down list of exception handling, options are: • Restart communication module; • Switch SIM card;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Reboot the system.

4.6 Link Backup

Function Description

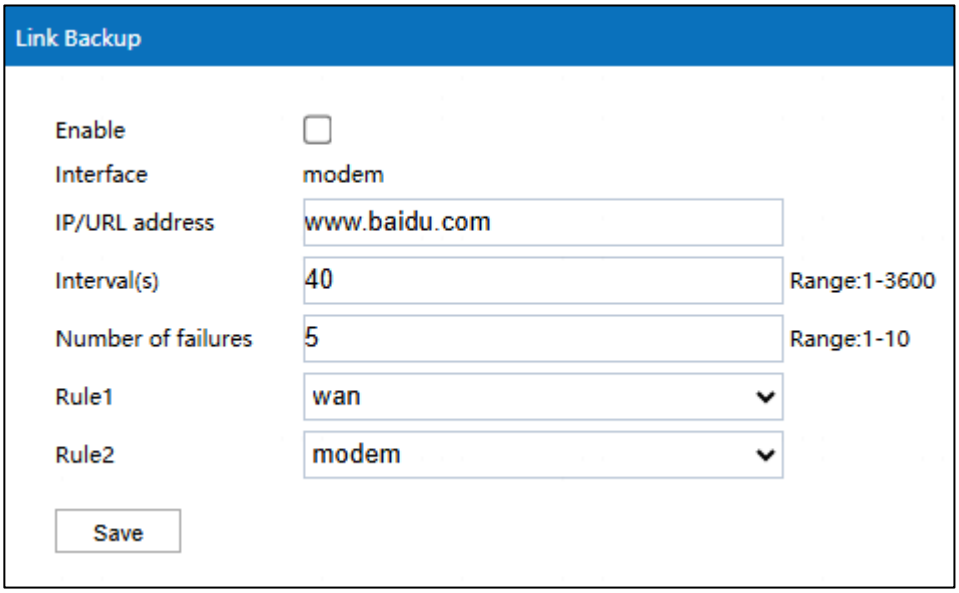
On the "Link Backup" page, user can configure the wired network and the wireless cellular network as link backup network. After Link Backup is enabled, if the current main network is abnormal, network connections can be switched to the backup network; When the main network returns to normal, network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

Operation Path

Choose “Basic Network > Link Backup” in the navigation bar.

Interface Description

The Link Backup interface is as follows:



The main elements configuration description of Link backup interface:

Interface Element	Description
Enable	Link Backup function enable checkbox, check to enable Link Backup function.
Interface	Show the current working network interface of the device.
IP/URL address	To detect whether the specified IP address or network

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	address can be accessed.
Interval (s)	The time interval of detection, the unit is second and defaults to 5.
Number of failures.	Number of detection failures, when number of detection failures exceed specified value, the corresponding network interface will be started in turn according to the rules.
Rule1	When number of failures exceed the threshold value due to interface network anomalies, the device will preferentially switch to the network interface specified by Rule 1. Rlue1 drop-down list, options as follows: • When "Network Selection" is "modem", this page is displayed. • modem
Rule2	When the network interface specified by Rule 1 is still abnormal, the device will switch to the network interface specified by Rule 2. Rule2 drop-down list, options as follows: • When "Network Selection" is "modem", this page is displayed. • modem

4.7 Local Area Network

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

Function Description

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

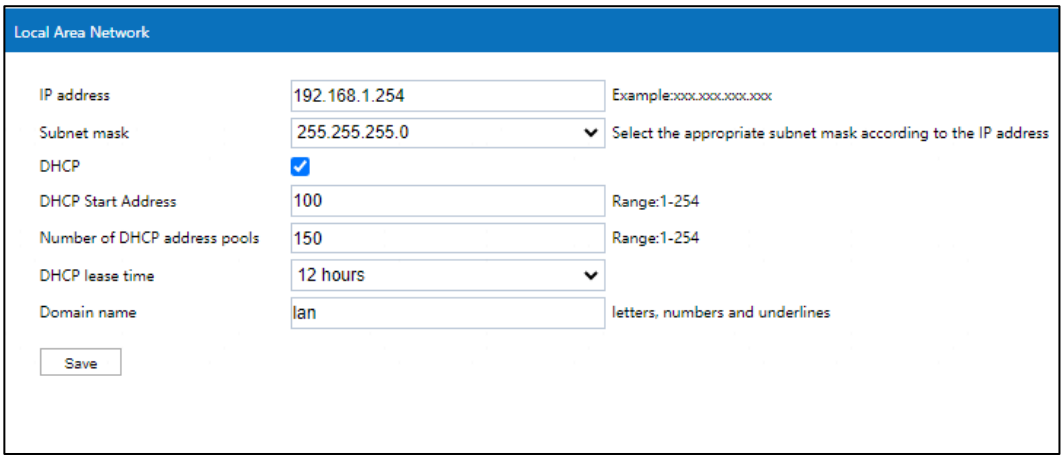
Operation Path

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

Interface Description

The local area network interface is as follows:

Copyright © 3onedata Co., Ltd.



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 Address	The minimum IP address host number allocated by DHCP 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.

Copyright © 3onedata Co., Ltd.

4.8 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

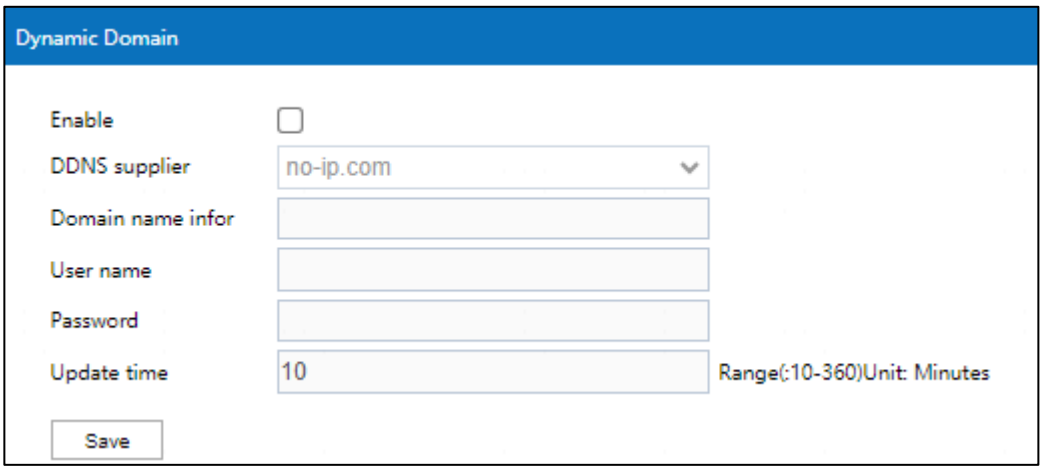
On the “Dynamic Domain” page, user can set relevant information of dynamic domain name.

Operation Path

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

Interface Description

The dynamic domain interface is 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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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.
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.

4.9 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

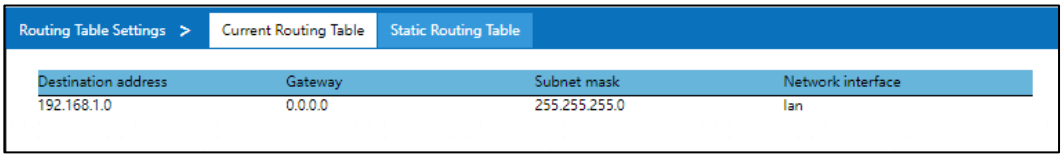
On the “Routing Table” page, user can set relevant information of routing table.

Operation Path

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

Interface Description 1: Current Routing Table

The current routing table interface is as follows:



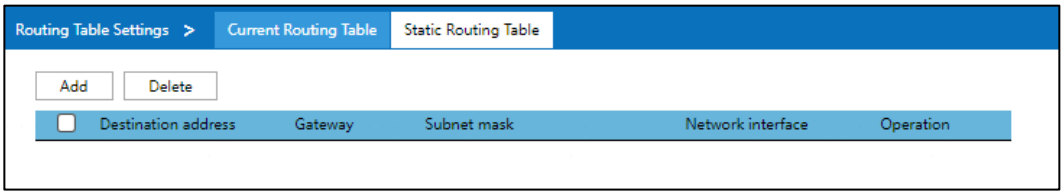
The main element configuration description of current routing table interface:

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.

Copyright © 3onedata Co., Ltd.

Interface Description 2: Static Routing Table

The static routing table interface is as follows:



The main element configuration description of static routing table interface:

Interface Element	Description
☐	The check box of static routing entry. Click to check all static routing entries.
Destination address	The destination IP address information of static routing.
Gateway	The destination gateway information of static routing.
Subnet mask	The subnet mask information of static routing: • 255.255.255.0 • 255.255.255.255 • 255.255.255.254 • 255.255.255.252 • 255.255.255.248 • 255.255.255.224 • 255.255.255.192 • 255.255.255.128 • 255.255.254.0 • 255.255.252.0 • 255.255.248.0 • 255.255.240.0 • 255.255.224.0 • 255.255.192.0 • 255.255.128.0 • 255.255.0.0 • 255.254.0.0 • 255.252.0.0 • 255.248.0.0 • 255.224.0.0 • 255.192.0.0

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 255.128.0.0 • 255.0.0.0 • 254.0.0.0 • 252.0.0.0 • 248.0.0.0 • 240.0.0.0 • 224.0.0.0 • 192.0.0.0 • 128.0.0.0
Network interface	The network interface of static routing: • WAN • LAN • MODEM • vif_sta0 • Manual Input Note: Under the "WIFI & Cellular Roaming" mode, the network interface option "vif_sta0" becomes selectable.
Interface Name	This item is displayed when the network interface is "manually entered", and the interface name is entered manually.
Operation	Edit: modify static routing table information.
Add	Click the “add” button at the top right corner to add static routing in the pop-up window of “static routing.
Delete	Check the static routing information to be deleted, and then click the “delete select’ button at the top right corner to delete them.

Copyright © 3onedata Co., Ltd.

5 WLAN Settings

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

5.1 Basic Parameter Settings

Function Description

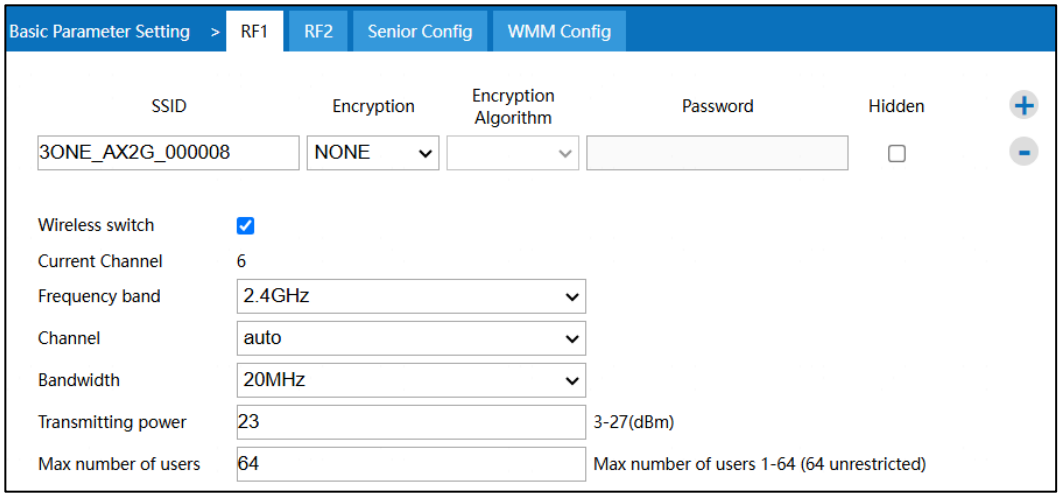
On the "Basic Parameter Settings" page of WLAN settings, you can complete RF 1 configuration, RF 2 configuration, advanced configuration, and WMM configuration.

Operation Path

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

Interface Description 1: RF1 Configuration

The RF1 configuration interface is as follows:



The main element configuration description of RF1 configuration interface:

Copyright © 3onedata Co., Ltd.

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/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm.
Encryption Algorithm	Wireless network supports different encryption algorithms when it using WPS, WPA2 or WPA-MIXED encryption method, options as follows: • AES(CCMP): CCMP (Counter Mode with CBC-MAC Protocol) uses AES (Advanced Encryption Standard) encryption algorithm. • TKIP: Temporal Key Integrity Protocol, provides more secure protection mechanism than WEP encryption. • TKIP/AES: compatible with both TKIP and AES encryption algorithm.
Password	Password of wireless network, it supports 8-63 valid characters.
Hidden	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.
Wireless switch	Wireless Network function enable checkbox, check to enable wireless network function.
Current Channel	The working channel of current 2.4G wireless network.

Copyright © 3onedata Co., Ltd.

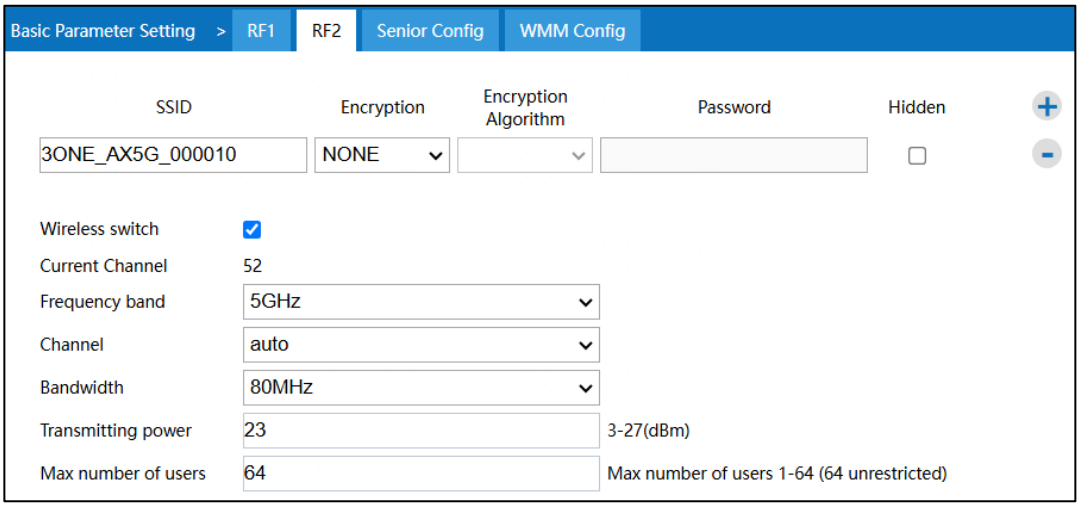
Interface Element	Description
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: • 2.4GHz
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 1: main frequency band 2412Hz, frequency range 2401~2423Hz; • 2: main frequency band 2417Hz, frequency range 2406~2428Hz; • 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 are as follows: • 20MHz;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 40MHz. Note: 40MHz bandwidth binds two 20MHz bandwidth channels together to gain the throughput capacity more than twice of the 20MHz bandwidth.
Transmitting power	Transmitted power of the device wireless signal, defaults to 27dBm, value range 3~27dBm. 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: RF2 Configuration

The RF 2 configuration interface is as follows:



The main element configuration description of RF1 configuration 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; • WPA2: WiFi Protected Access II is suitable for the individual or average family network. It adopts pre-shared key and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard)

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption Algorithm	Encryption algorithm of wireless network, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES(CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 valid characters.
Hidden	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.
Wireless switch	Wireless Network function enable checkbox, check to enable wireless network function.
Current Channel	The working channel of current 5G wireless network.
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: • 5GHz
Channel	Working channel of 5G wireless network, options are as follows: • Auto: channel self-adaptation; • 36: main frequency band 5180Hz, frequency range 5170~5190Hz; • 40: main frequency band 5200Hz，frequency range 5190~5210Hz; • 44: main frequency band 5220Hz, frequency range

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	5210~5230Hz; • 48: main frequency band 5230Hz, frequency range 5210~5250Hz; • 52: main frequency band 5260Hz, frequency range 5250~5270Hz; • 56: main frequency band 5280Hz, frequency range 5270~5290Hz; • 60: main frequency band 5300Hz, frequency range 5290~5310Hz; • 64: main frequency band 5320Hz, frequency range 5310~5330Hz; • 100: main frequency band 5500Hz, frequency range 5490~5510Hz, this frequency band is not open in China, so it's temporarily unavailable; • 104: main frequency band 5520Hz, frequency range 5510~5530Hz, this frequency band is not open in China, so it's temporarily unavailable; • 108: main frequency band 5540Hz, frequency range 5530~5550Hz, this frequency band is not open in China, so it's temporarily unavailable; • 112: main frequency band 5560Hz, frequency range 5550~5570Hz, this frequency band is not open in China, so it's temporarily unavailable; • 116: main frequency band 5580Hz, frequency range 5570~5590Hz, this frequency band is not open in China, so it's temporarily unavailable; • 120: main frequency band 5600Hz, frequency range 5590~5610Hz, this frequency band is not open in China, so it's temporarily unavailable; • 124: main frequency band 5620Hz, frequency range 5610~5630Hz, this frequency band is not open in China, so it's temporarily unavailable; • 128: main frequency band 5640Hz, frequency range 5630~5650Hz, this frequency band is not open in China, so it's temporarily unavailable; • 132: main frequency band 5660Hz, frequency range 5650~5670Hz, this frequency band is not open in China, so it's temporarily unavailable; • 136: main frequency band 5680Hz, frequency range 5670~5690Hz, this frequency band is not open in China, so it's temporarily unavailable;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 140: main frequency band 5700Hz, frequency range 5690~5710Hz, this frequency band is not open in China, so it's temporarily unavailable; • 144: main frequency band 5720Hz, frequency range 5710~5730Hz, this frequency band is not open in China, so it's temporarily unavailable; • 149: main frequency band 5745Hz, frequency range 5735~5755Hz; • 153: main frequency band 5765Hz, frequency range 5755~5775Hz; • 157: main frequency band 5785Hz, frequency range 5775~5795Hz; • 161: main frequency band 5805Hz, frequency range 5795~5815Hz; • 165: main frequency band 5825Hz, frequency range 5815~5835Hz. Note: • In order to improve the network performance, please choose unused channel in the device working environment. • Different frequency bands and countries support different channel options.
Bandwidth	Channel bandwidth of wireless network, it defaults to 80MHz, options are as follows: • 20MHz; • 40MHz; • 80MHz; • 160MHz. Note: 5G frequency band, channel 36 and 165 only support 20MHz bandwidth configuration • When the country code is China: 40-64 support a maximum bandwidth configuration of 160MHz, while 149-161 only supports a maximum bandwidth configuration of 80MHz; • When the country code is the United States: channel 36 only supports 20MHz bandwidth configuration, channel 40-128 support a maximum bandwidth configuration of 160MHz, and channel 132-161 support a maximum bandwidth configuration of 80MHz.
Transmitting power	Transmitted power of the device wireless signal, defaults to 27dBm, value range 3~27dBm. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may have different transmitted power range.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
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 client number.

Interface Description 3: 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. Note: Please enable WDS function while bridging the device and other wireless devices.
Wireless Isolate	Wireless user isolation, it's used for isolating the wireless clients connected to the device wireless network with same SSID, defaults to disabled. Note: After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
RTS	Data packet RTS (Request to Send) threshold, value range 0-2347, defaults to 2347. • RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will send RTS signal; • 0 < RTS threshold < 2347: when the length of data packet surpasses RTS threshold, the device wireless terminal will send RTS signal to avoid signal conflict; • RTS threshold = 2347: the device wireless terminal won't send RTS signal. Note: • As for the wireless nodes in different wireless detection range of AP range, collision will occur when the nodes send out signals; RTS function can avoid the collision. • The device will send RTS to destination station for negotiation when the length of data packet surpasses RTS threshold. After receiving RTS frame, the wireless station will send a CTS (Clear to Send) frame to response the device, which represents the two stations can conduct wireless communication.
Country	Applied countries and regions of wireless network. Options are as follows: • China; • USA. Note: Different country opens different channels.
Verification Method	Authentication mode of wireless network, options are 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 a text input box when the wireless network authentication method is “enterprise edition”.

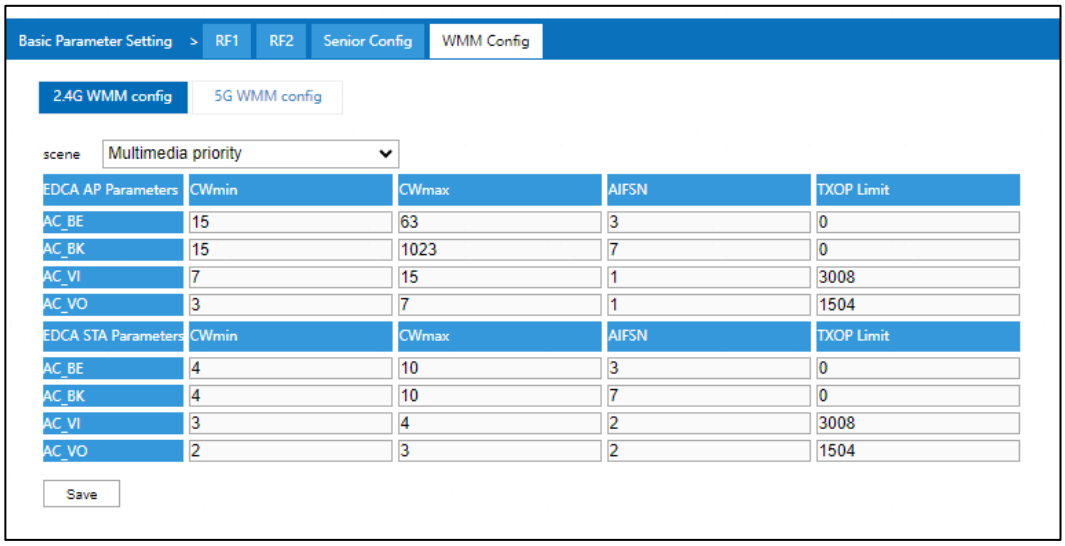
Copyright © 3onedata Co., Ltd.

Interface Element	Description
Radius Server port	The authentication port number of the RADIUS server, value range is 0-65535. Note: The item will display as a 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 a text input box when the wireless network authentication method is “enterprise edition”.

Interface Description 4: WMM Configuration

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

The WMM configuration interface is as follows:



Main element configuration description of WMM configuration interface:

Copyright © 3onedata Co., Ltd.

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	time. Note: 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.

5.2 Wireless Client Filtering

Function Description

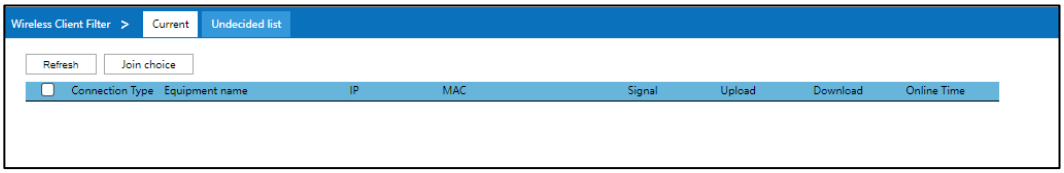
On the “Wireless Client Filtering” page, user can check current connecting devices and manage wireless user connection.

Operation Path

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

Interface Description 1: Currently Connected Device

The interface of the current connected device is as follows:



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

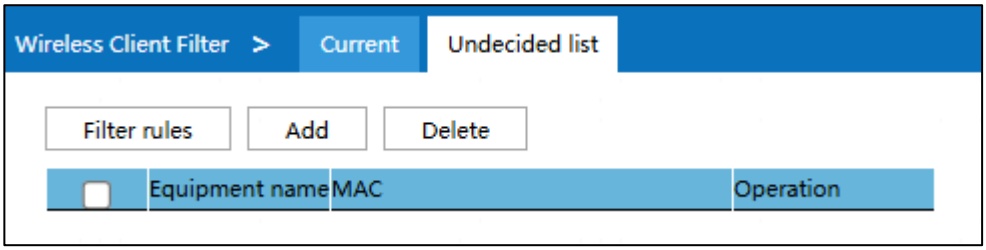
Interface Element	Description
Connection Type	The connection mode of wireless client connected to this device currently.
Equipment name	The equipment name of wireless client connected to this device currently.
IP	The IP address of wireless client connected to this device currently.
MAC	The MAC address 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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	the signal.
Upload	The upload flow of wireless client connected to this device currently.
Download	The download flow of wireless client connected to this device currently.
Online Time	The online time of wireless client connected to this device currently.

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

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



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

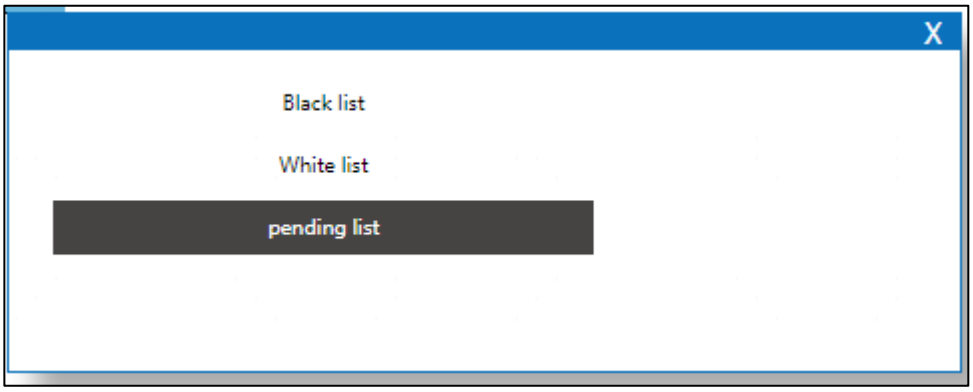
Interface Element	Description
Equipment name	The device name of wireless client in the list. Note: • Click “add” to add device to list manually. • Click “Filter rules” button, you can switch current list between black List, white List and undecided list, to filter wireless client.
MAC	MAC address of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

Copyright © 3onedata Co., Ltd.



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.
pending List	The pending list of wireless client visiting wireless device.

Note

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

Copyright © 3onedata Co., Ltd.

6 Advanced Network

6.1 Port Forward

The Port Forwarding 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 these types of requests to your network via internet, the router would forward them to the corresponding client via port forwarding function.

Function Description

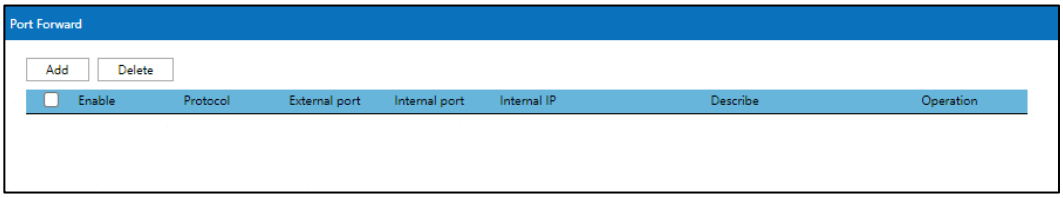
On the “Port Forward” page, user can check or add port forward entry. It allows outer network client to visit specified device via specified port.

Operation Path

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

Interface Description

The port forward interface is as follows:



The main element configuration description of port forward interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Protocol	The protocol type used by port forward data package: • TCP • UDP • TCP/UDP
External port	The external port number used by external network.
Internal port	The internal port number used by internal network.
Internal IP	The IP address of device specified by internal network
Description	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.

6.2 Port Redirection

Function Description

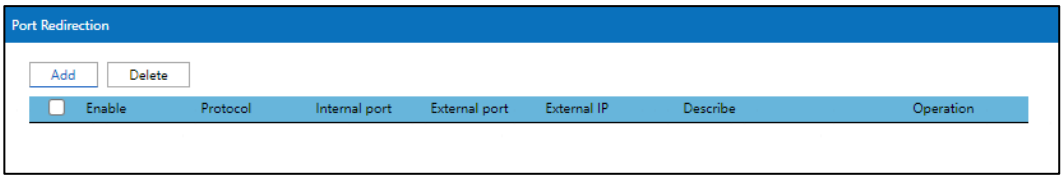
On the “Port Redirection” page, user can check or add port redirection entry, which allows client in LAN to visit the specified port of device with IP address specified by external network via specified port.

Operation Path

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

Interface Description

The port redirection interface is as follows:



The main element configuration description of port redirection interface:

Interface Element	Description
☐	The checkbox of port redirection entry. Click to check all port redirection entries
Enable	Enable port redirection or not:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• ON • OFF
Protocol	The protocol type used by port redirection data package: • TCP • UDP • TCP/UDP
Internal port	The internal port number used by internal network
External port	The external port number used by external network
External IP	The device IP address specified by external network
Description	The remark information of port redirection entry
Operation	Edit: modify port redirection entry information
Add	Click the “add” button at the top right corner to add new port redirection in the pop-up window of “Port Redirection”
Delete	Check the port redirection information that needs to be deleted, then click “delete” button at the top right corner to delete it

6.3 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.

Function Description

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

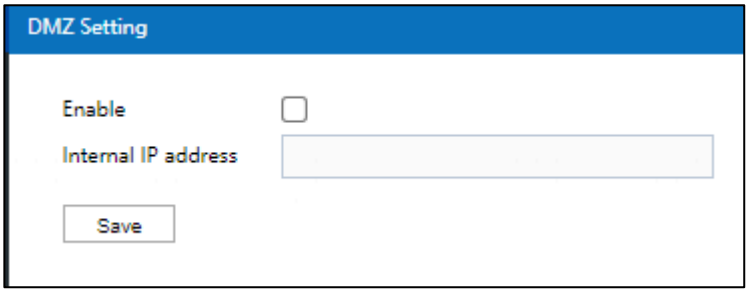
Operation Path

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

Interface Description

The DMZ setting interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of DMZ setting interface:

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

6.4 Serial Port Setup

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

6.4.1 Serial Port Setup

Function Description

On the “Serial Port Setup” page, users can configure serial server mode and specify basic parameter information such as baud rate, data bit, stop bit and check bit for the corresponding serial port number.

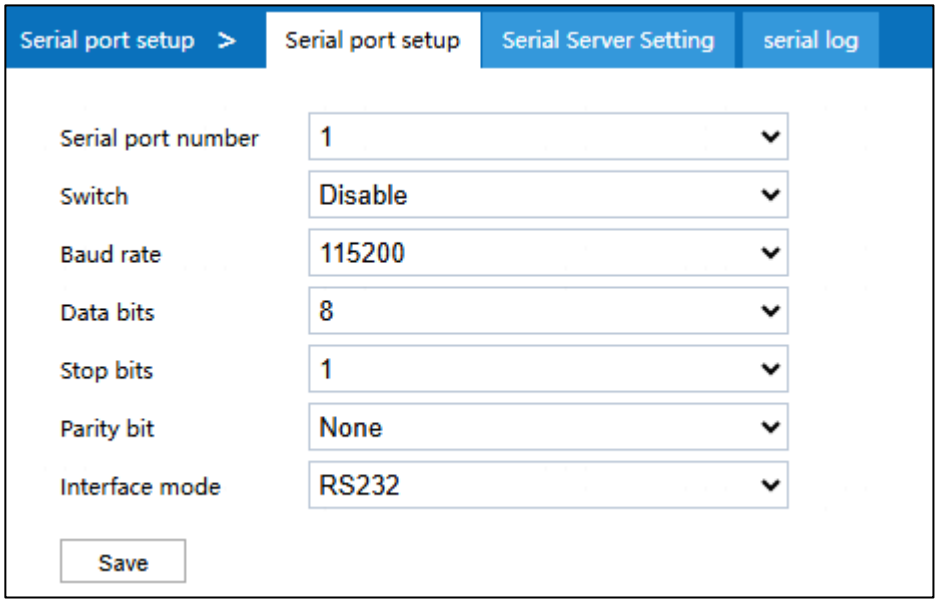
Operation Path

Open in order: "Advanced Network > Serial port setup > Serial port setup".

Interface Description

Serial port setup interface is as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of serial port setup interface:

Interface Element	Description
Serial port number	The corresponding serial port number of device's serial port.
Switch	The drop-down list of serial server enable switch, options are as follows. • Disable; • Serial server activation: support serial port working mode;
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. • 8
Stop bits	Choose stop bit of corresponding serial port. Options: • 1 • 2
Parity bit	Select parity bits of corresponding serial number. Options: • None • Odd • Even
Interface mode	Display the interface mode of the device's serial port: • RS485 • RS232

Copyright © 3onedata Co., Ltd.

6.4.2 Serial Port Server setting

Function Description

On the "Serial Settings" page, users can configure the work mode and related parameters of the serial port.

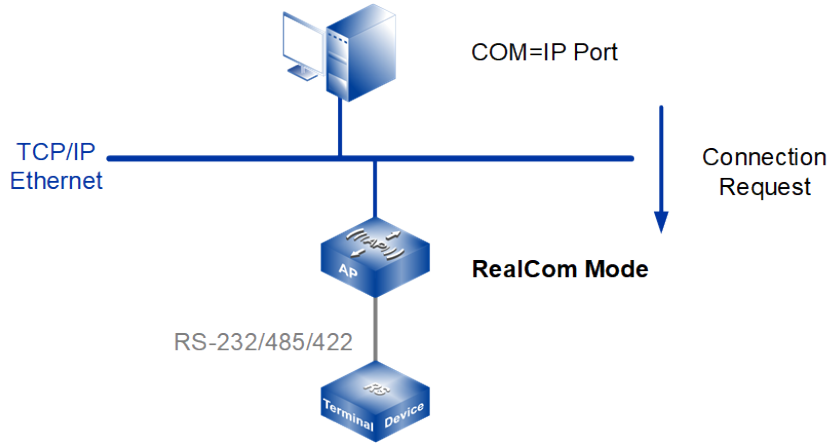
The working modes supported by the device are:

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

Operation Path

Open in order: "Advanced Network > Serial port setup > Serial Server Settings".

6.4.2.1 RealCom Mode



Note:

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

In RealCom mode, the device 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 device to the local COM/TTY device of the host according to the user configured device IP address and serial port number and other

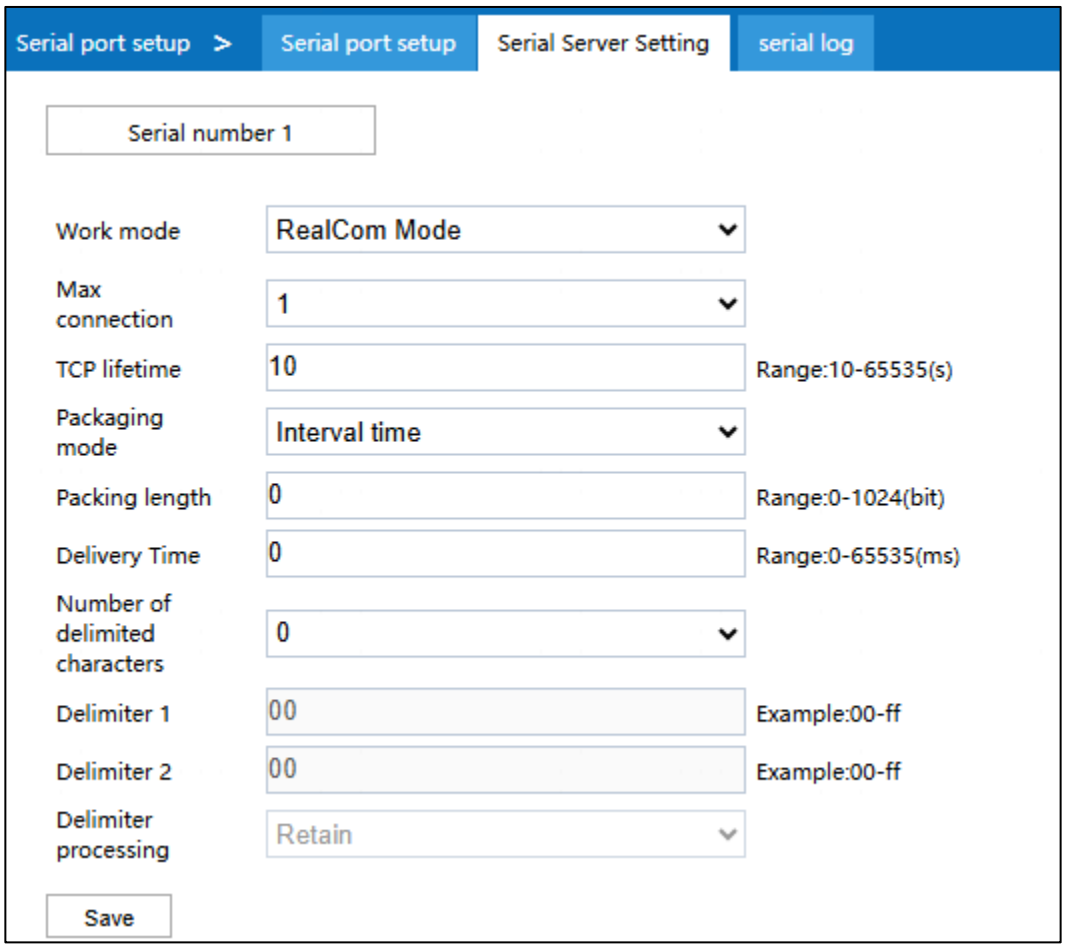
Copyright © 3onedata Co., Ltd.

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 transparent transmission, the device receives the TCP/IP data packet, and after unpacking, sends the original data to the serial port 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 COM Settings interface:

Interface Element	Description
Serial number 1	Serial port number corresponding to the device
Work mode	The work modes of serial port are as follows: • RealCom Mode: Real serial port mode; • TCP Server Mode • TCP Client Mode • UDP Server Mode

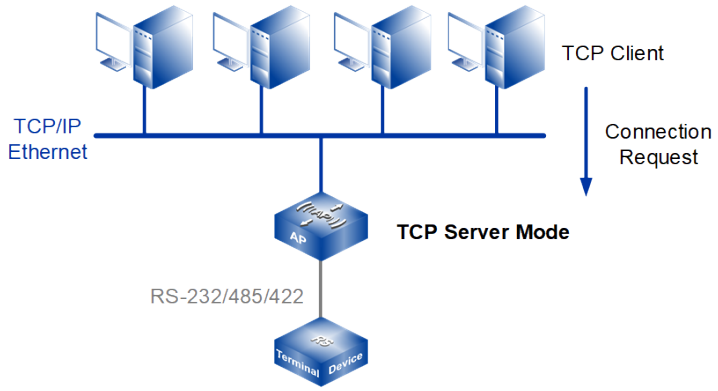
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• UDP Client Mode
Max connection	The number of hosts connected to a serial port simultaneously. • Each host communicates with the 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 it 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: • Mandatory 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	For the frame length of the serial data to Ethernet data, the data frame is forwarded within the set time range when it is greater than or equal to the set frame length, and the value ranges from 0 to 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: • 0: disable the delimited character function; • 1: enable delimiter 1; • 2: enable Delimiter 2. Note:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	If the packaging length or the forced transfer time is 0 and the number of delimited characters 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	Delimiter 1 is represented in hexadecimal format, for example: 00-ff.
Delimiter 2	Delimiter 2 is represented in hexadecimal format, for example: 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.

6.4.2.2 TCP Server Mode



Note:

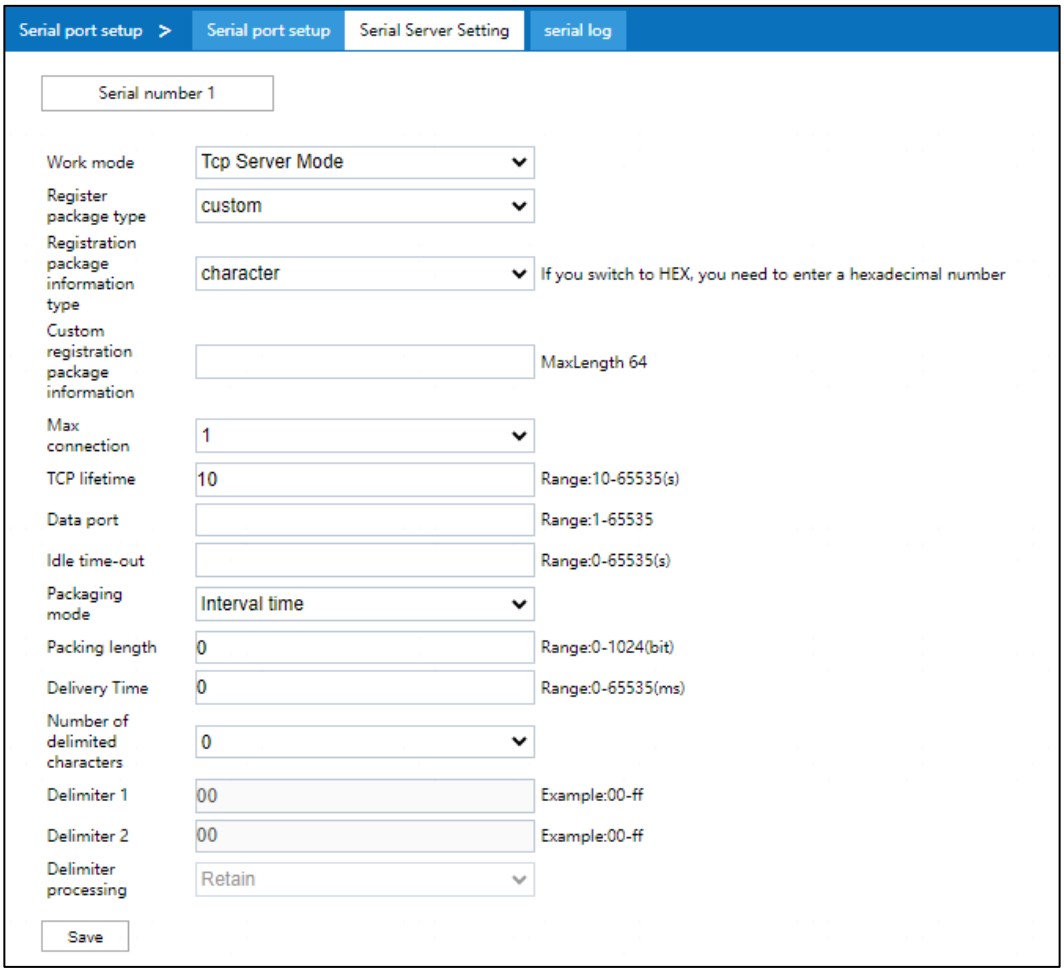
The device picture mentioned in above figure is only an example, and the actual appearance of the device or serial port type is subject to the device obtained.

In TCP server mode, the device is assigned an IP port number and passively waits for the host to connect. When the host initiates a connection request and establishes a connection with the device, the host can realize bidirectional transparent data transmission through network connection and serial port. The TCP server mode supports up to four session connections simultaneously, allowing multiple hosts to simultaneously read or send Ethernet data to a serial device.

Copyright © 3onedata Co., Ltd.

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
Serial number 1	Serial port number corresponding to the device
Work mode	The work modes of serial port are as follows: • RealCom Mode: Real serial port mode; • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode
Register package type	The information sent after the device is connected to the peer client. Options: • Disable: After the connection is successful, no information is sent to the peer client. • IP address: After the connection is successful, send

Copyright © 3onedata Co., Ltd.

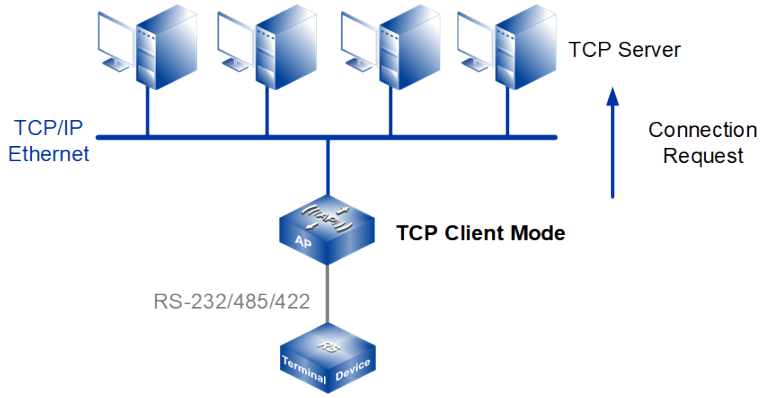
Interface Element	Description
	the IP address of the device to the peer client. • Device name: After the connection successful, send the device name of the device to the peer client. • Custom: Send custom message to the opposite client after successful connection.
Registration package information type	When the register package type is "Custom", the options for customizing the register package information are as follows: • Character 1 • HEX: Hexadecimal.
Custom registration package information	This item is displayed when the Register Package Type is “Custom”.
Max connection	The number of hosts connected to a serial port simultaneously. • 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 it to "0", the function will be disabled. Effective time range 0~65535s.
Data port	The destination connection port of TCP client.
Idle time-out	Set the idle time-out of current serial data communication link. • 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: • Mandatory time: the system packages serial port data received within a specified time into Ethernet packets

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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	For the frame length of the serial data to Ethernet data, the data frame is forwarded within the set time range when it is greater than or equal to the set frame length, and the value ranges from 0 to 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: • 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	Delimiter 1, represent in hexadecimal, the value range is 0x00-0xFF.
Delimiter 2	Delimiter 2, represent in hexadecimal, the value range is 0x00-0xFF.
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.

Copyright © 3onedata Co., Ltd.

6.4.2.3 TCP Client Mode



Note:

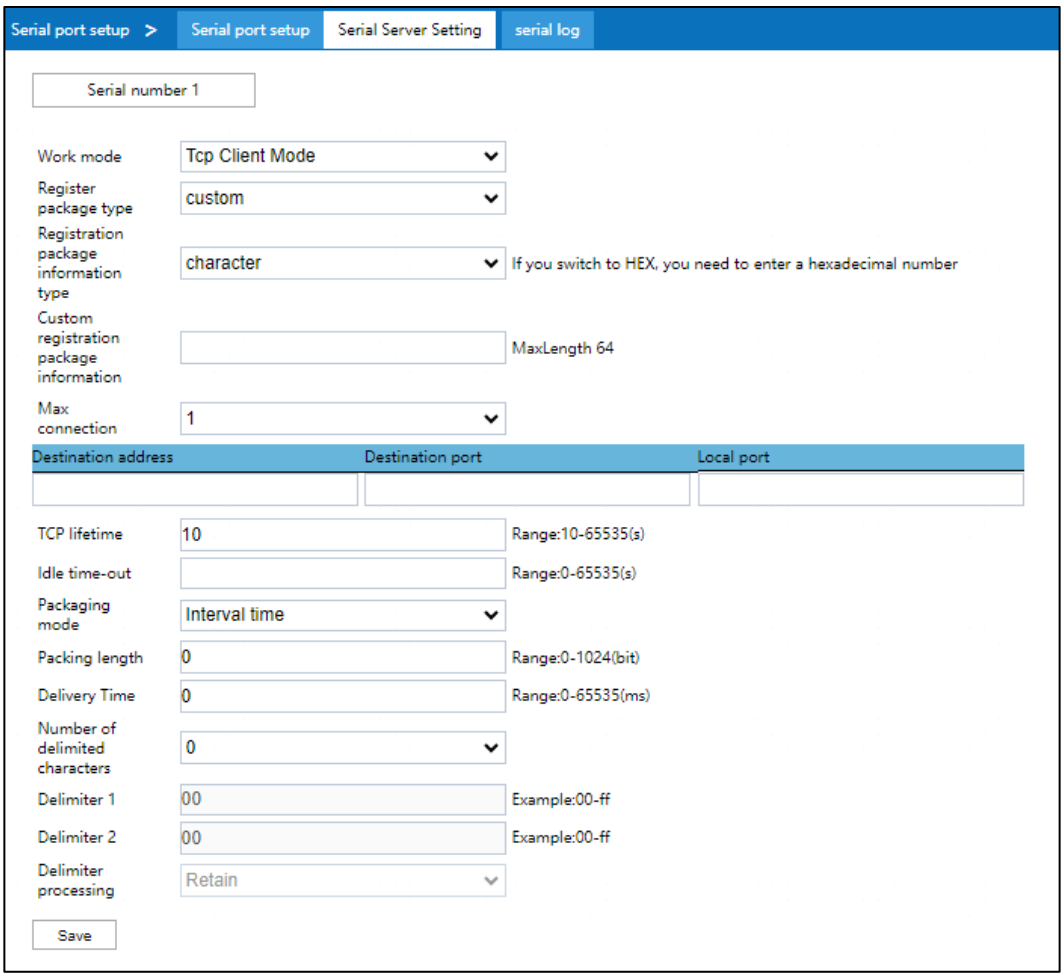
The device picture mentioned in above figure is only an example, and the actual appearance of the device or serial port type is subject to the device obtained.

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

Interface Description

The serial port setup interface in TCP Client Mode:

Copyright © 3onedata Co., Ltd.



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

Interface Element	Description
Serial number 1	Serial port number corresponding to the device
Work mode	The work modes of serial port are as follows: • RealCom Mode: Real serial port mode; • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode
Register package type	The information sent after the device is connected to the peer client. Options: • Disable: After the connection is successful, no information is sent to the peer client. • IP address: After the connection is successful, send the IP address of the device to the peer client. • Device name: After the connection successful, send the device name of the device to the peer client.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Custom: Send custom message to the opposite client after successful connection.
Registration package information type	When the register package type is "Custom", the options for customizing the register package information are as follows: • Character 1 • HEX: Hexadecimal.
Custom registration package information	This item is displayed when the Register Package Type is “Custom”.
Max connection	The number of hosts connected to a serial port simultaneously. • Each host communicates with the 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 it to "0", the function will be disabled. Effective time range 0~65535s.
Idle time-out	Set the idle time-out of current serial data communication link. • 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

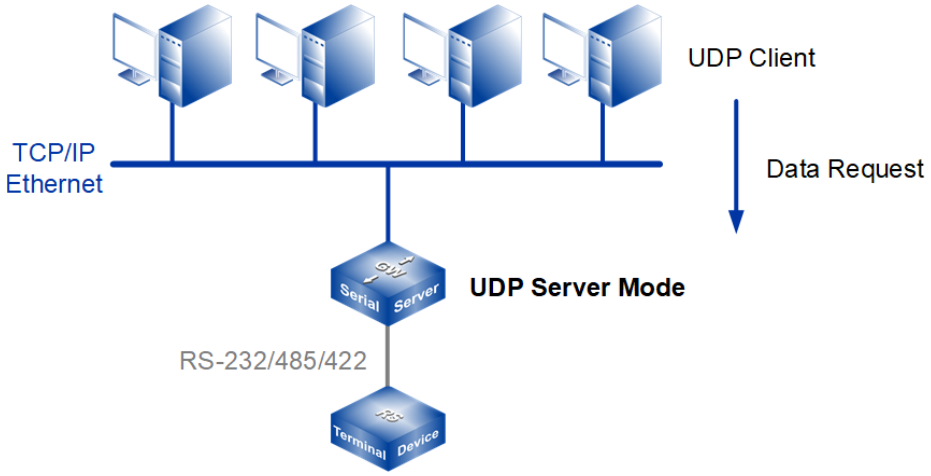
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	connection would not be closed automatically.
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Mandatory 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	For the frame length of the serial data to Ethernet data, the data frame is forwarded within the set time range when it is greater than or equal to the set frame length, and the value ranges from 0 to 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: • 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	Delimiter 1, represent in hexadecimal, the value range is 0x00-0xFF.
Delimiter 2	Delimiter 2, represent in hexadecimal, the value range is 0x00-0xFF.
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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	delimiter) would be deleted. The system only transmits data except delimiter.

6.4.2.4 UDP Server Mode



Note:

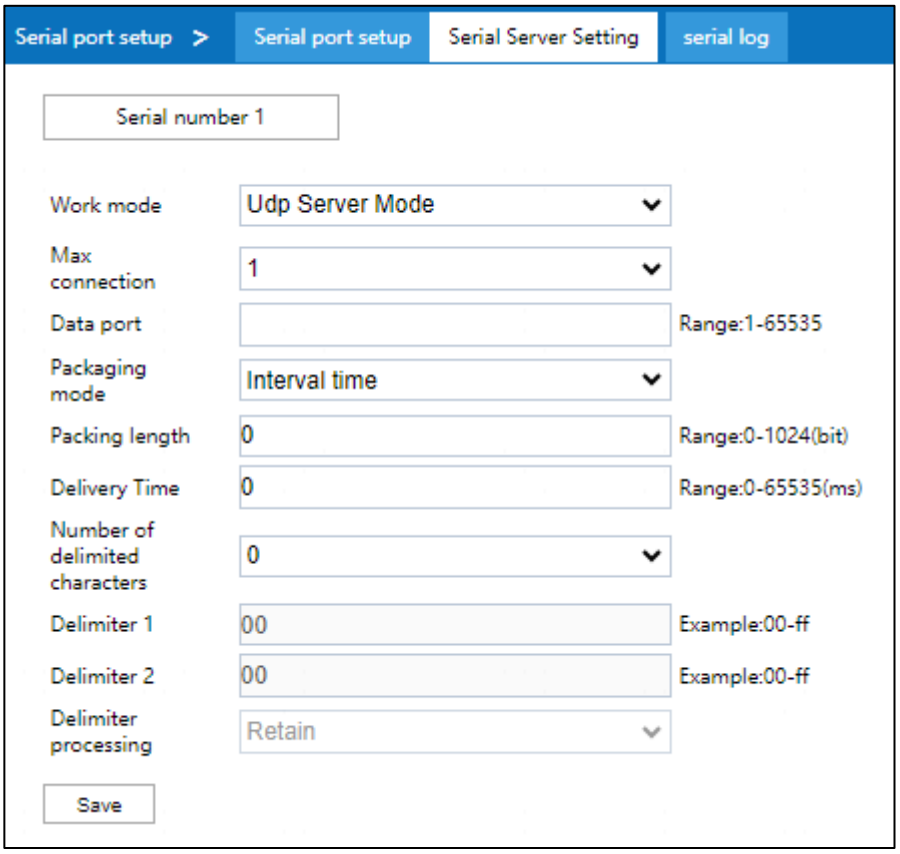
The device picture mentioned in above figure is only an example, and the actual appearance of the device or serial port type is subject to the device obtained.

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

Interface Description

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

Copyright © 3onedata Co., Ltd.



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

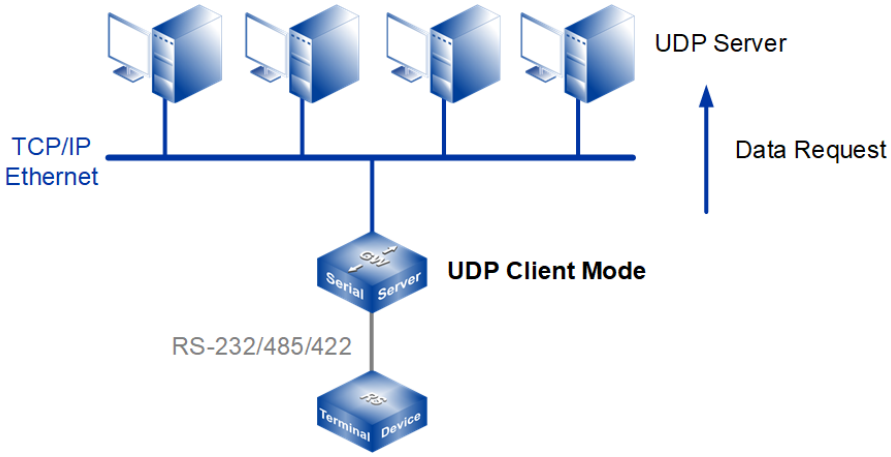
Interface Element	Description
Serial number 1	Serial port number corresponding to the device
Work mode	The work modes of serial port are as follows: • RealCom Mode: Real serial port mode; • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode
Max connection	The number of host that one serial port has session with. • Each host communicates with serial port in the order of first-in first-out; • The system supports up to 4 sessions.
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: • Mandatory time: the system packages serial port

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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	For the frame length of the serial data to Ethernet data, the data frame is forwarded within the set time range when it is greater than or equal to the set frame length, and the value ranges from 0 to 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.
Delivert 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	Delimiter 1, represent in hexadecimal, the value range is 00-ff.
Delimiter 2	Delimiter 2, represent in hexadecimal, the 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.

Copyright © 3onedata Co., Ltd.

6.4.2.5 UDP Client Mode



Note:

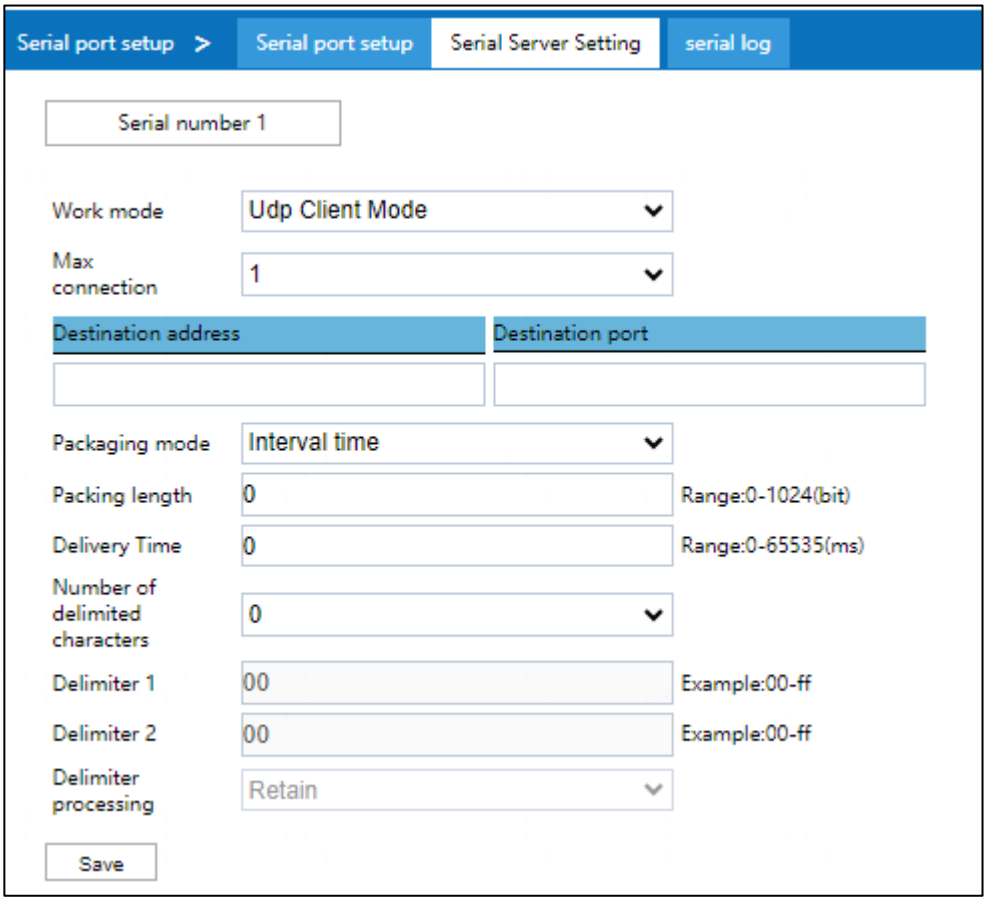
The device picture mentioned in above figure is only an example, and the actual appearance of the device or serial port type is subject to the device obtained.

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

Interface Description

Screenshot of the serial settings interface in UDP Client Mode:

Copyright © 3onedata Co., Ltd.



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

Interface Element	Description
Serial number 1	Serial port number corresponding to the device
Work mode	The work modes of serial port are as follows: • RealCom Mode: Real serial port mode; • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode
Max connection	The number of hosts connected to a serial port simultaneously. • Each host communicates with the 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.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Packaging mode	The serial data is packaged into Ethernet data frame. The options are as follows: • Mandatory 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	For the frame length of the serial data to Ethernet data, the data frame is forwarded within the set time range when it is greater than or equal to the set frame length, and the value ranges from 0 to 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: • 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	Delimiter 1, represent in hexadecimal, the value range is 00-ff.
Delimiter 2	Delimiter 2, represent in hexadecimal, the 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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	transmits data except delimiter.

6.4.3 Serial Log

Function Description

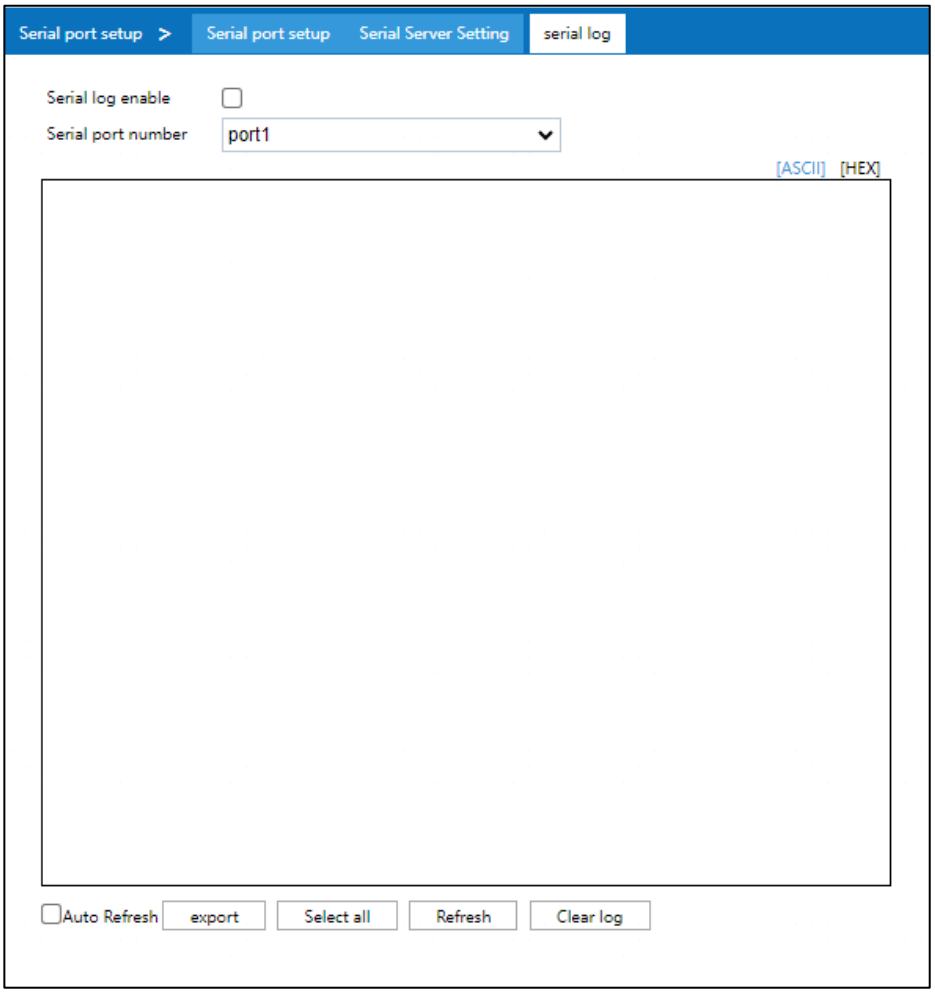
On the "Serial Port Log" page, you can monitor the serial port communication parameters.

Operation Path

Click "Advanced Network > Serial port setup > serial log".

Interface Description

The serial log interface is as follows:



Main elements configuration description of serial log interface:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Serial log enbale	Serial log switch check box, check it to enable serial log function to record serial data communication.
Serial port number	The drop-down list of serial number, you can choose the corresponding serial number.
[ASCII] [HEX]	Click to display the communication data in the serial port log in ASCII characters or HEX.
Auto Refresh	The check box of automatic refresh, and check it to automatically refresh the serial log information of the page every 30 seconds.
export	Click the "Export" button to export the ".txt" format serial log.
Select all	Click "Select all" button to select all serial log information.
Refresh	Click “Refresh” to manually refresh the serial log information of the page.
Clear log	Click the “Clear log” button to clear the current serial log.

6.5 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.

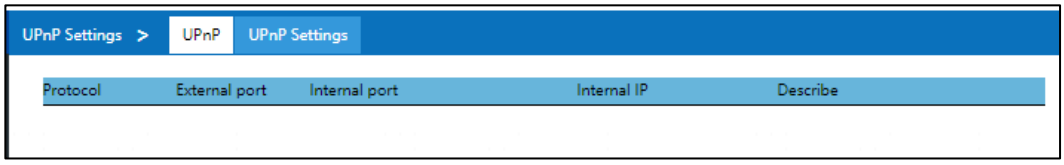
Copyright © 3onedata Co., Ltd.

Operation Path

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

Interface Description 1: UPnP

UPnP settings interface is as follows:

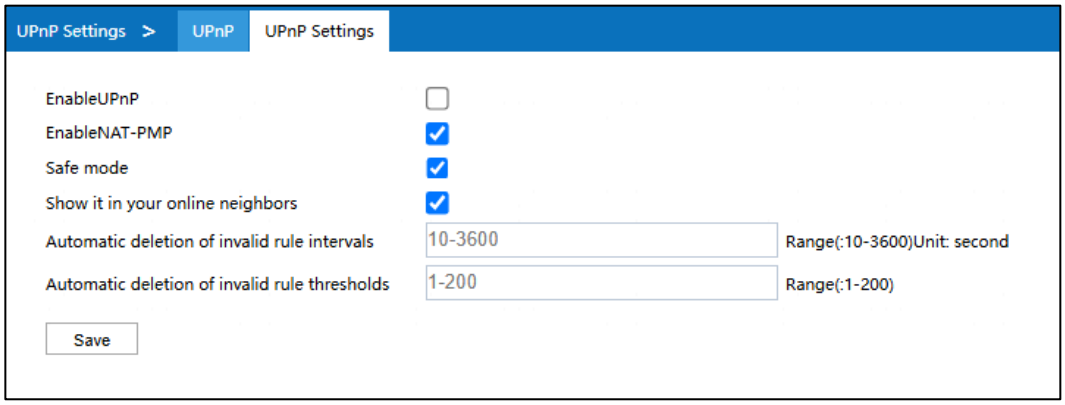


The main elements configuration description of UPnP settings interface:

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 is as follows:



The main element configuration description of UPnP settings interface:

Interface Element	Description
Enable UPnP	UPnP enable checkbox, check to enable UPnP function.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Enable NAT-PMP	The NAT-PMP function enable checkbox, check to enable NAT-PMP function, and the router will allow the LAN host to communicate with external devices to automate port conversion.
Safe mode	Safe mode enable checkbox, after the safe mode is enabled, the client can only forward an input port to itself.
Show it in your online neighbors	Show the enable check box in Online neighbors, after checked, the device can be found in the PC Online neighbors or network devices.
Automatic deletion of invalid rule intervals	The system automatically deletes the invalid UPnP rules list after the specified interval, unit: second.
Automatic deletion of invalid rule thresholds	The system automatically deletes the invalid UPnP rules list after the quantity of invalid UPnP rules reaches the threshold.

6.6 Multicast NAT

Function Description

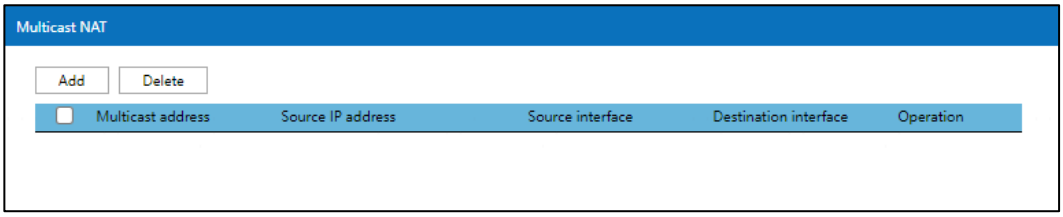
On the "Multicast NAT" page, you can configure specified multicast transparent transmitting between various network.

Operation Path

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

Interface Description

Multicast NAT interface is as follows:



The main element configuration description of multicast NAT interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	The multicast address range is 224.0.0.0~239.255.255.255, addresses in different ranges have different functions.
Source IP address	Source IPv4 address of multicast
Source interface	The device interface to receive multicast data, such as lan, wan, vif_sta0 or modem. Note: Under the "WIFI & Cellular Roaming" mode, the network interface option "vif_sta0" becomes selectable.
Destination interface	The device interface to send multicast data, such as lan, wan, vif_sta0 or modem. Note: Under the "WIFI & Cellular Roaming" mode, the network interface option "vif_sta0" becomes selectable.
Operation	Click “Edit” button to modify the information of current entry.

6.7 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

Copyright © 3onedata Co., Ltd.

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: VID, 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.

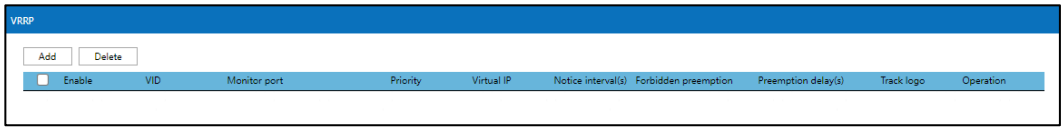
Operation Path

Open in order: "Advanced Network > VRRP".

Interface Description

VRRP interface is as below:

Copyright © 3onedata Co., Ltd.



The main element configuration descriptions of VRRP interface:

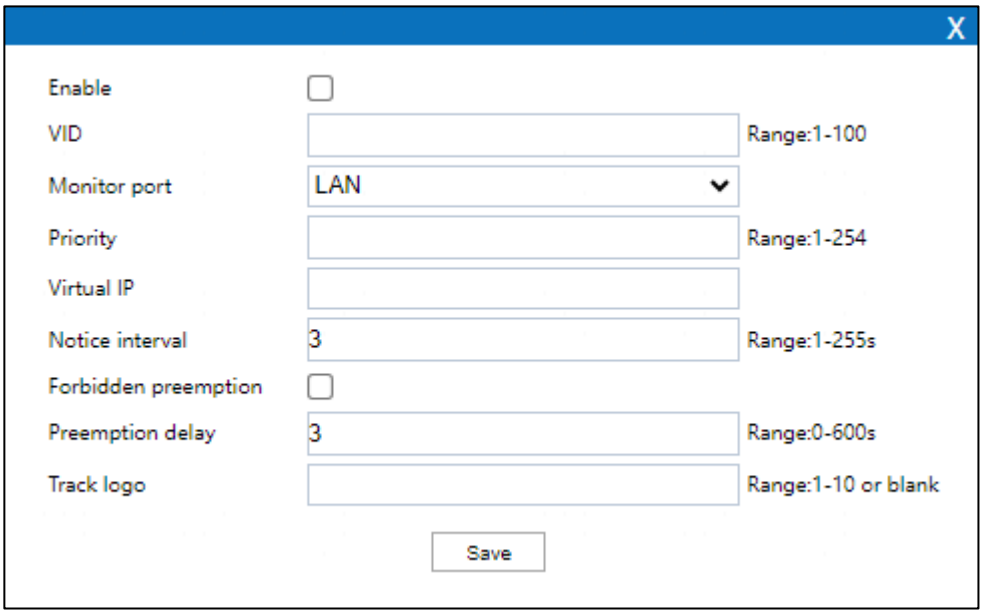
Interface Element	Description
Enable	VRRP function status is displayed, options include: • ON • OFF
VID	Identity of the virtual router is displayed.
Monitor port	Monitor ports of the device is displayed, options include: • LAN • WAN
Priority	Priority of the device. The priority is used for the election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

Interface Description: VRRP-Add

Click the "Add" button to add virtual route.

The VRRP-Add interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of VRRP-Add interface:

Interface Element	Description
Enable	VRRP enable check box, check it to enable the VRRP function.
VID	Identity of the virtual router, the valid range is 1-1100. 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;
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 1-255 seconds. Master device periodically sends VRRP notice messages to announce its operating status.
Forbidden preemption	Disable preemption check box of VRRP, check it to disable preemption. • Non-preemptive mode. When the priority of Backup device is higher than the one of Master device, Backup device won't become the Master device; • Preemptive mode. When the priority of Backup device is higher than the one of Master device, Backup device will actively switch to Master device.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Preemption delay	The delay time of switching from Backup device to Master device, the valid range is 0-600 seconds. Note: If the preemption delay time is too short, the device status will be frequently switched; so increasing the preemption delay time can effectively solve this problem.
Track ID	Trace and probe Track ID, the ID range is 1-10, optional.

6.8 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

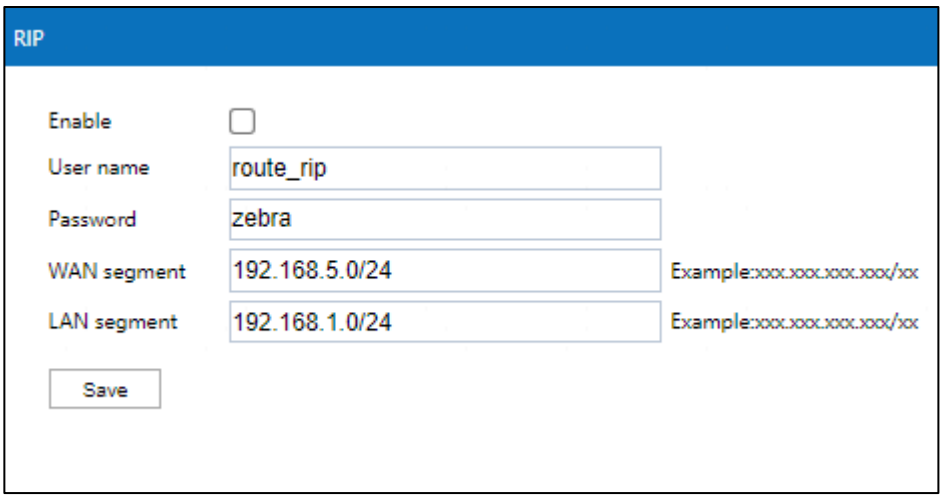
On the page of "RIP", user can configure the RIP-related parameters.

Operation Path

Open in order: "Advanced Network > RIP".

Interface Description

RIP interface is as below:



The main element configuration descriptions of RIP interface:

Copyright © 3onedata Co., Ltd.

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.

6.9 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.

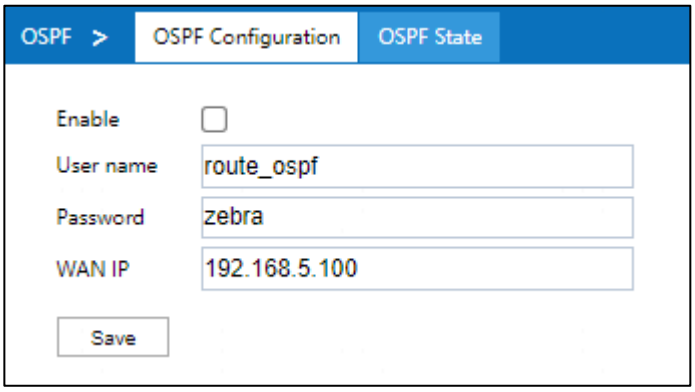
Operation Path

Open in order: "Advanced Network > OSPF".

Interface Description 1: OSPF Configuration

The OSPF configuration interface is as follows:

Copyright © 3onedata Co., Ltd.

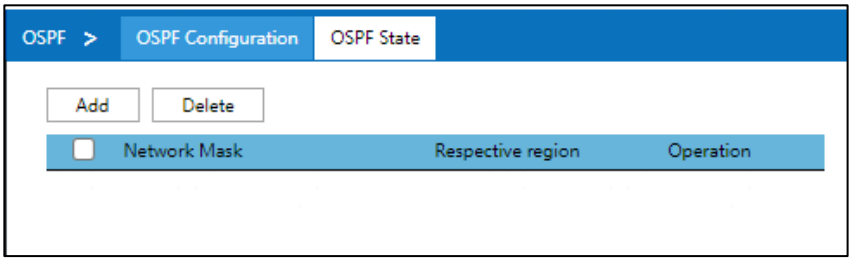


Main element configuration description of OSPF configuration interface:

Interface Element	Description
Enable	OSPF enable checkbox, check to enable OSPF protocol.
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.
WAN IP	The router ID number, like the IP address format, is the unique identification of router in the autonomous system.

Interface Description 2: OSPF State

OSPF State interface is as follows:



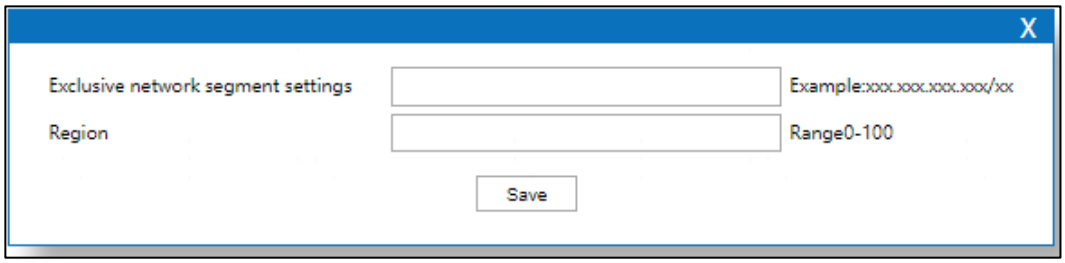
The main element configuration description of OSPF State interface:

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

Copyright © 3onedata Co., Ltd.

Interface Description 21: OSPF State-Add

The OSPF State-Add interface is as follows:



The main elements configuration description of OSPF State-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.

6.10 Static DHCP

Function Description

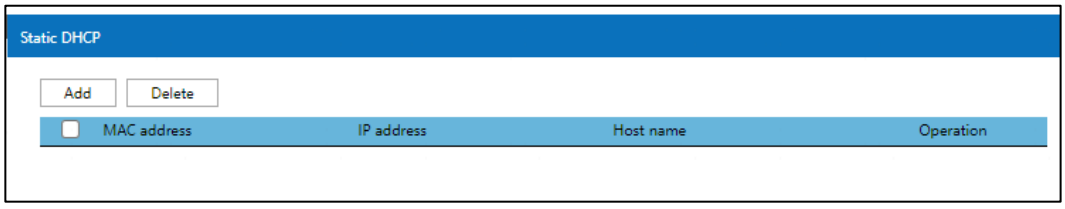
On the page of "Static DHCP", user can add, delete, and view the configuration information of static clients. Bind the client's MAC address to the specified IP address to ensure that the address that the client obtains from the server each time is the binding IP address.

Operation Path

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

Interface Description

Static DHCP interface is as follows:



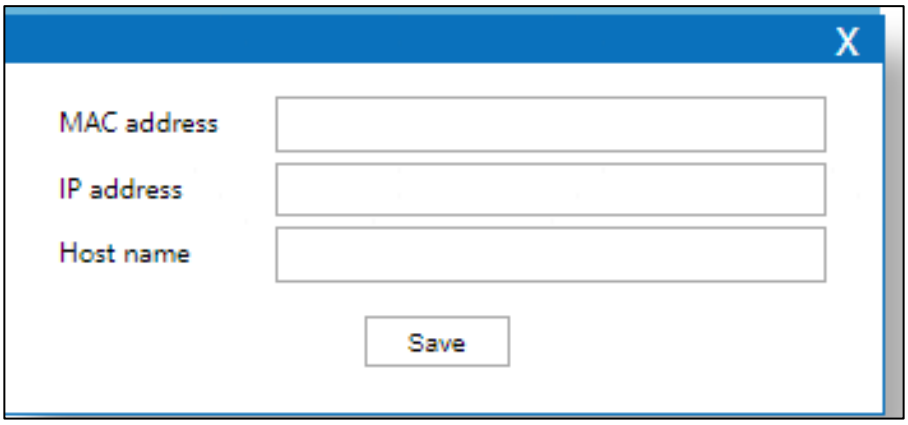
The main element configuration description of static DHCP interface:

Copyright © 3onedata Co., Ltd.

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 is 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.

6.11 DHCP Client

Function Description

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

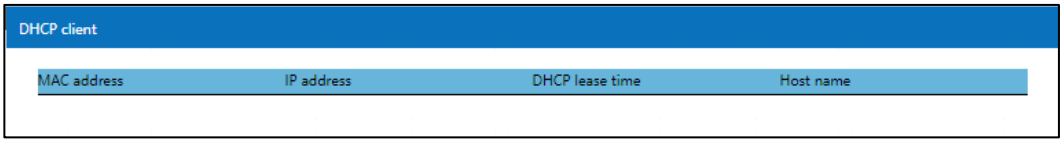
Operation Path

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

Copyright © 3onedata Co., Ltd.

Interface Description

The DHCP client settings interface is as follows:



Interface Element	Description
MAC address	MAC address of DHCP client.
IP address	IP address of DHCP client.
DHCP lease time	Valid lease of DHCP client.
Host name	Name or remarks of the DHCP client.

6.12 QoS

Function Description

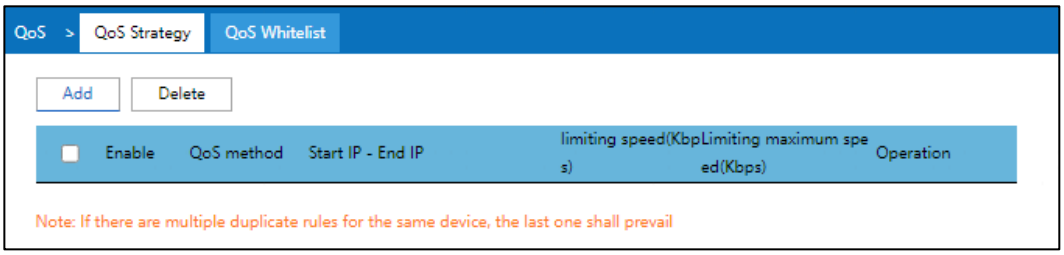
On the "QoS" page, the QoS strategy can be set to limit the rate of specified IP or MAC, and to make device list which is not affected by QoS strategy.

Operation Path

Open in order: "Advanced Network> QoS".

Interface Description 1: QoS strategy

The QoS Strategy interface is as follows:



The main element configuration description of QoS classification interface:

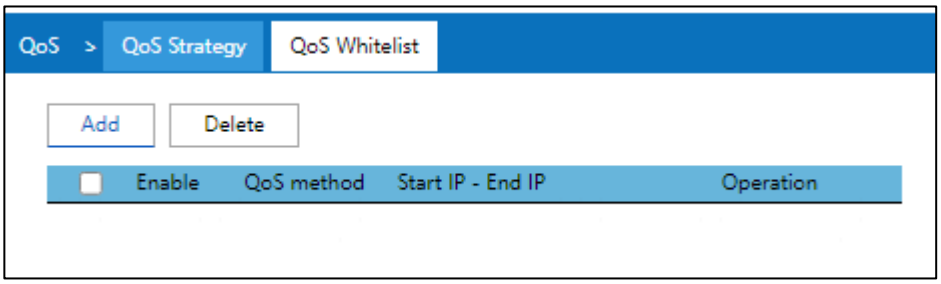
Interface Element	Description
Enable	Enable QoS strategy or not.
QoS method	The method of enabling QoS strategy, available values: • IP-based speed limit
Start IP-End IP	The range of the speed limit from the start IP address to the

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	end IP address.
limiting speed (Kbps)	Limit average rate value, the value range of the threshold is 64-1000000Kbps.
Limiting maximum speed (Kbps)	The maximum Limit rate value, the value range is 64-1000000Kbps.
Operation	Click "Edit" button to modify this QoS strategy.
Add	Click "Add" button to add QoS strategy. Note: If there are multiple repeated rules for the same device, the last rule shall prevail.
Delete	Check the QoS strategy to be deleted, and click the "Delete" button to delete QoS strategy.

Interface Description 2: QoS Whitelist

QoS Whitelist interface is as follows:



The main element configuration description of QoS white list interface:

Interface Element	Description
Enable	Enable QoS whitelist or not.
QoS method	The method of enabling QoS strategy, available values: • IP white list
Start IP-End IP	The range of starting IP addresses to ending IP addresses that are not affected by QoS strategy.
Operation	Click "Edit" button to modify this QoS whitelist.
Add	Click "Add" button to add QoS whitelist. Note: If there are multiple repeated rules for the same device, the last rule shall prevail.
Delete	Check the QoS whitelist entry to be deleted, and click "Delete" button to delete QoS whitelist.

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

6.13 SNMP

Now, the broadest network management protocol in network is SNMP (Simple Network Management Protocol). SNMP is the industrial standard that is widely accepted and comes into use, it's used for guaranteeing the management information transmission between two points in network, and is convenient for network manager search information, modify information, locate faults, complete fault diagnosis, conduct capacity plan and generate a report. SNMP adopts polling mechanism and only provides the most basic function library, especially suit for using in minitype, rapid and low price environment. SNMP implementation is based on connectionless transmission layer protocol UDP, therefore, it can achieve barrier - free connection to many other products.

Function Description

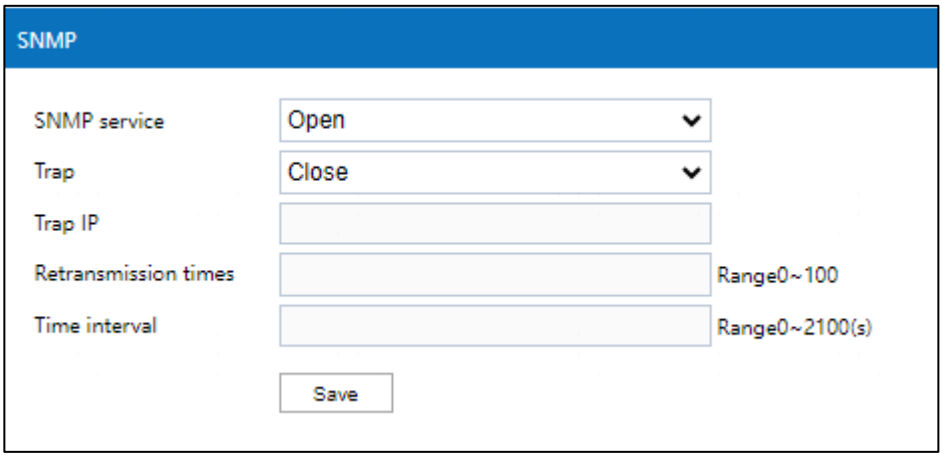
On the SNMP page, you can enable or disable the SNMP service and Trap message.

Operation Path

Open in order: "Advanced Network > SNMP".

Interface Description

SNMP interface is as below:



The main element configuration descriptions of SNMP interface:

Interface Element	Description
SNMP service	Whether to enable SNMP service, options: • Enable; • Close.
Trap	Whether to enable Trap message, options: • Enable;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• Close. Note: Trap messages can be enabled only after the SNMP service is enabled.
Trap IP	The IP address used to send Trap messages.
Retransmission times	Retransmission times indicates that the device retransmits data based on the specified retransmission times. The value ranges from 0 to 100. For example, a Trap message is usually sent once plus the number of retransmission times. If the number of retransmission times is 2, a Trap message is sent three times.
Time interval	The time interval is the interval between sending Trap messages three times in the above example, with a value range of 1-2100 seconds.

6.14 SLA

Function Description

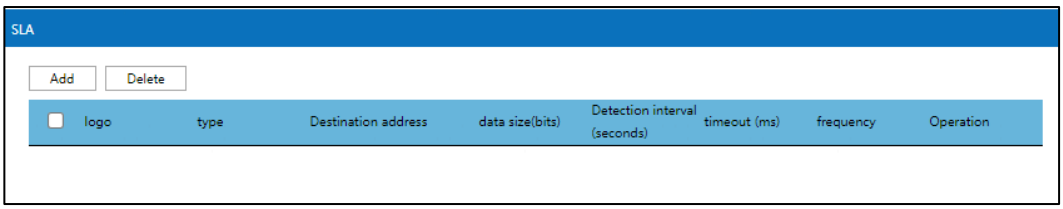
On the "SLA" page, Track objects can be defined by tracking and probing one or more targets through SLA.

Operation Path

Open in order: "Advanced Network > SLA".

Interface Description

SLA Settings interface is as follows:



The main element configuration description of SLA settings interface:

Interface Element	Description
logo	SLA ID number, value range is 1-10.
type	Display SLA probe type, the default is icmp-echo.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	The device sends an ICMP request to the specified target, and if the ICMP response from the target is received, the target is online.
Destination address	Destination IP address of ICMP probe packet.
data size (bits)	The data size of the probe packet, it value range is 56-1000 bytes.
Detection interval (seconds)	Time interval to send probe packets, ranging from 3 to 259200s.
timeout (ms)	Response timeout time, the value range is 50-3000 milliseconds. If the response is received within the specified time, the probing fails and the next probing is performed.
Frequency	Time-out number of SLA probe failures, ranging from 1 to 5. When the timeout times reach the specified value, the link failure is considered as SLA probe failure.
Operation	Click “Edit” button to modify the SLA entry parameters.

6.15 Track

Function Description

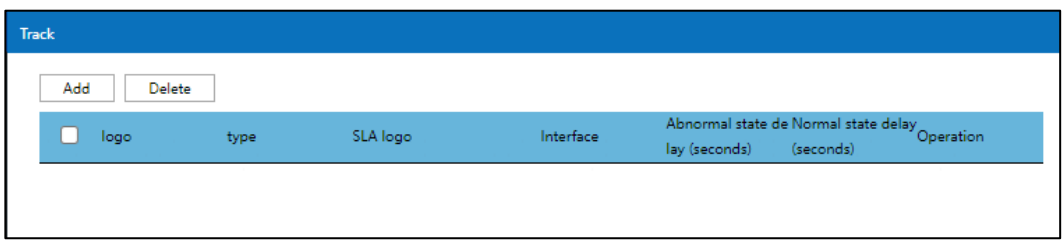
On the "Track" page, it can be configured to probe interface and link status (SLA) and realize linkage with other applications, such as VRRP.

Operation Path

Open in order: "Advanced Network > Track".

Interface Description

Track Settings interface is as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of Track Settings interface:

Interface Element	Description
logo	Track ID number, value range is 1-10.
type	Display track probe type, it can be displayed as follows: • sla: Tracking and probing according to SLA settings. • interface: Tracking and probing according to interface status.
SLA logo	SLA ID number, value range is 1-10.
Interface	Device network interface, such as LAN or WAN.
Abnormal state delay (seconds)	When the interface or SLA is in abnormal state (interface DOWN or SLA probe fails), the delay time of Track becoming abnormal, the value range is 0-180 seconds.
Normal state delay (seconds)	When the interface or SLA is in normal state (interface UP or SLA probe normal), the delay time of Track becoming normal is 0-180 seconds.
Operation	Click “Edit” button to modify the Track entry parameters.

Copyright © 3onedata Co., Ltd.

7 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.

7.1 IP Filter

Function Description

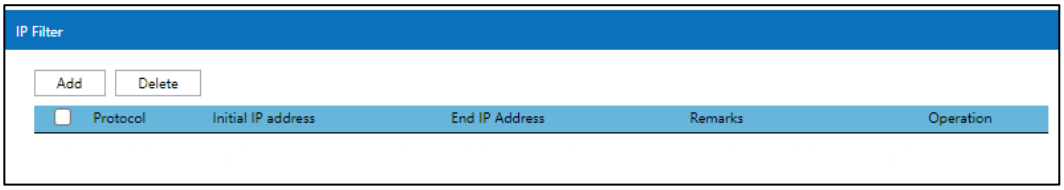
On the "IP filter" page of firewall, user can check or add IP filter to forbid the communication between the clients in LAN and WAN.

Operation Path

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

Interface Description

IP filter interface is as follows:



The main element configuration description of IP filter interface:

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

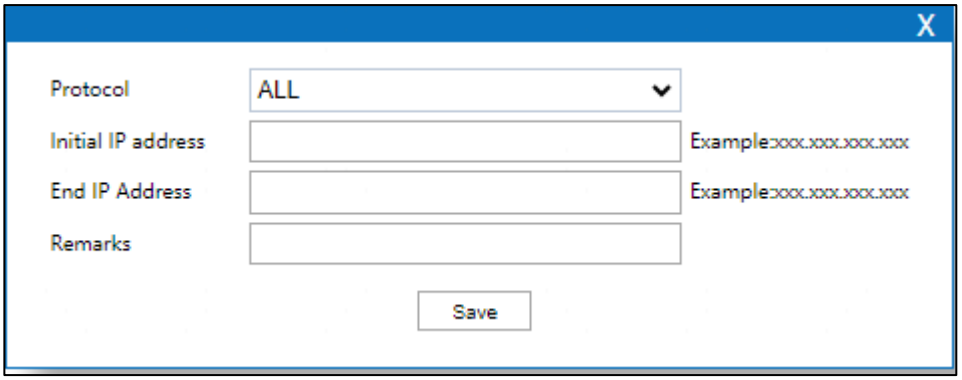
Copyright © 3onedata Co., Ltd.

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

Interface Description: Add IP Filter Entry

Click "Add" to increase IP filter entry.

The Add interface is as follows:



The main elements configuration description of “Add” interface:

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

Copyright © 3onedata Co., Ltd.

7.2 MAC Filtering

Function Description

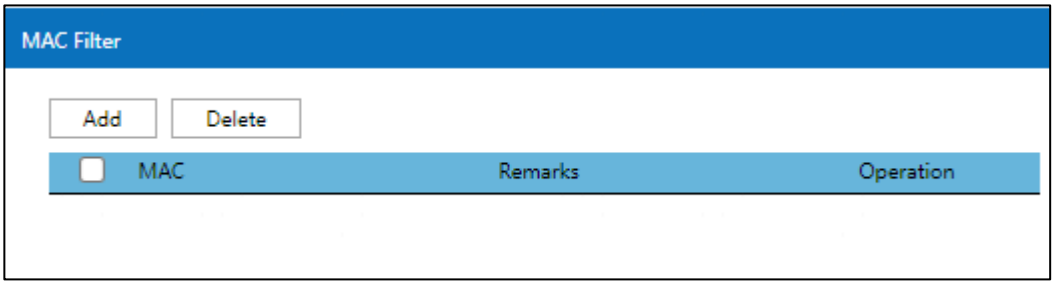
On the "MAC filter" page of firewall, user can check or add MAC filter to forbid the communication between the clients in LAN and WAN; it can effectively control the WAN access rights of user in LAN.

Operation Path

Open in order: "Firewall > MAC filter".

Interface Description

MAC filter interface is as follows:



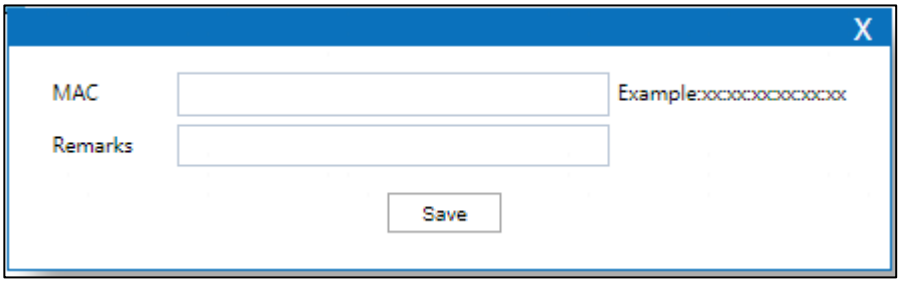
The main element configuration description of MAC filter interface:

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

Interface Description: Add MAC Filter Entry

Click "Add" to increase MAC filter entry.

The Add interface is as follows:



The main elements configuration description of “Add” interface:

Copyright © 3onedata Co., Ltd.

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

7.3 URL Filtering

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

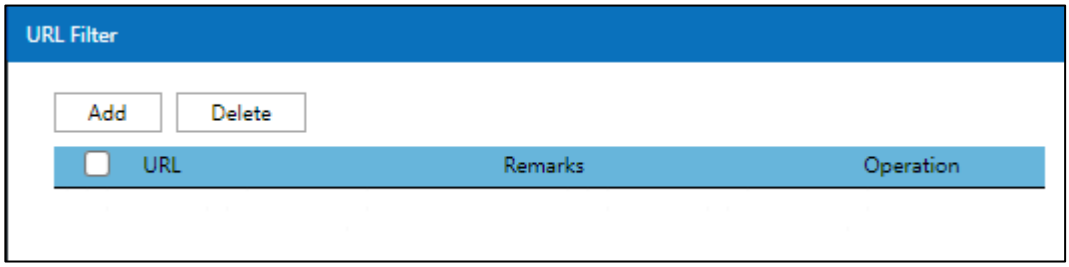
On the "URL filter" page of firewall, user can check or add URL filter to prohibit the client in LAN from accessing URL address in WAN and prevent user from accessing some of the websites.

Operation Path

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

Interface Description

URL filter interface is as follows:



The main element configuration description of URL filter interface:

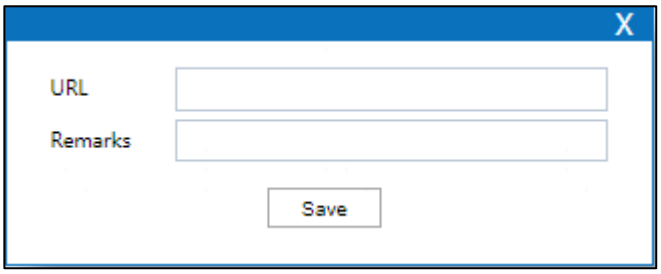
Interface Element	Description
☐	URL filter check box, click to check all URL filter entries.
URL	URL address in LAN filtered by the device.
Remarks	Remarks for URL filter entries.
Operation	Edit: modify the filter list.

Interface Description: Add URL Filter List

Click "Add" to increase URL filter list.

URL filter interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of URL filter interface:

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

7.4 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

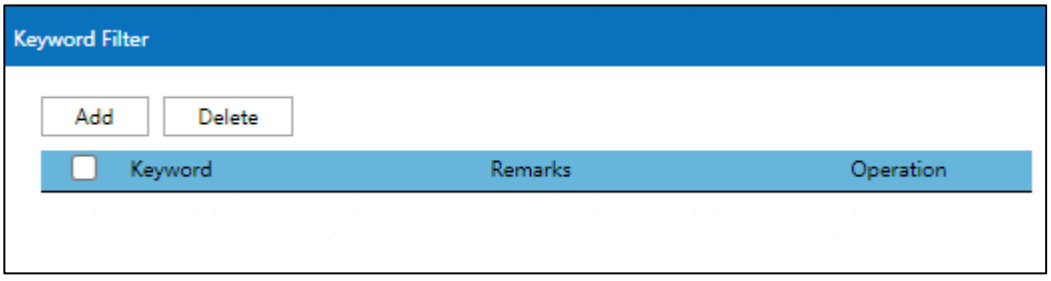
On the page of "Keyword filter" of the firewall, user can view or add keyword filtering entries to prevent clients on the LAN from accessing to the network address corresponding to the keywords in the WAN.

Operation Path

Open in order: "Firewall > Keyword Filter".

Interface Description

Keyword filter interface is as follows:



The main elements configuration description of keyword filter interface:

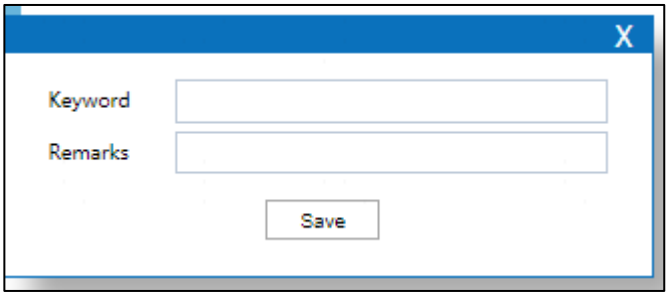
Copyright © 3onedata Co., Ltd.

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

Interface Description: Add keyword filtering entry

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

The Add interface is as follows:



The main elements configuration description of “Add” interface:

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

7.5 IP Address Black/White List

Function Description

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

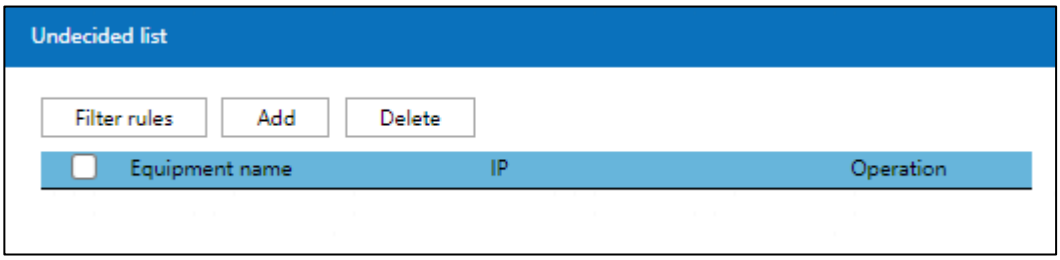
Operation Path

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

Interface Description

IP Address Black/White List interface is as follows:

Copyright © 3onedata Co., Ltd.



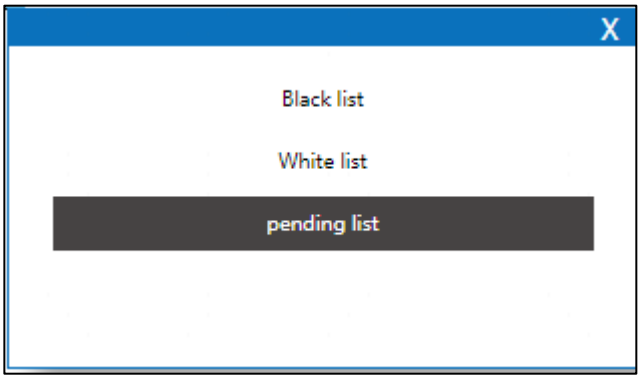
The main element configuration description of black/white list of IP address interface:

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.
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 is 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.
pending list	The pending list of client visiting WAN.

Note

Copyright © 3onedata Co., Ltd.

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

Copyright © 3onedata Co., Ltd.

8 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.

8.1 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

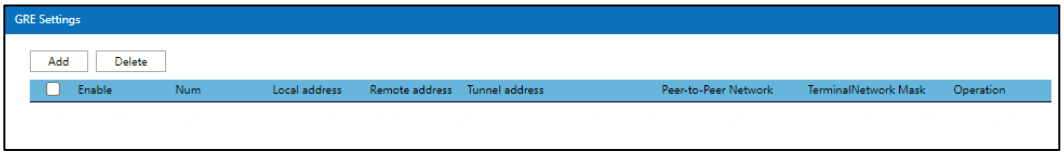
On the page of "GRE Settings", user can configure the relevant parameters of GRE.

Operation Path

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

Interface Description

The GRE settings interface is as follows:



The main element configuration description of GRE settings interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Enable	GRE settings is enabled or not: • ON • 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.

8.2 PPTP Client Settings

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

Function Description

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

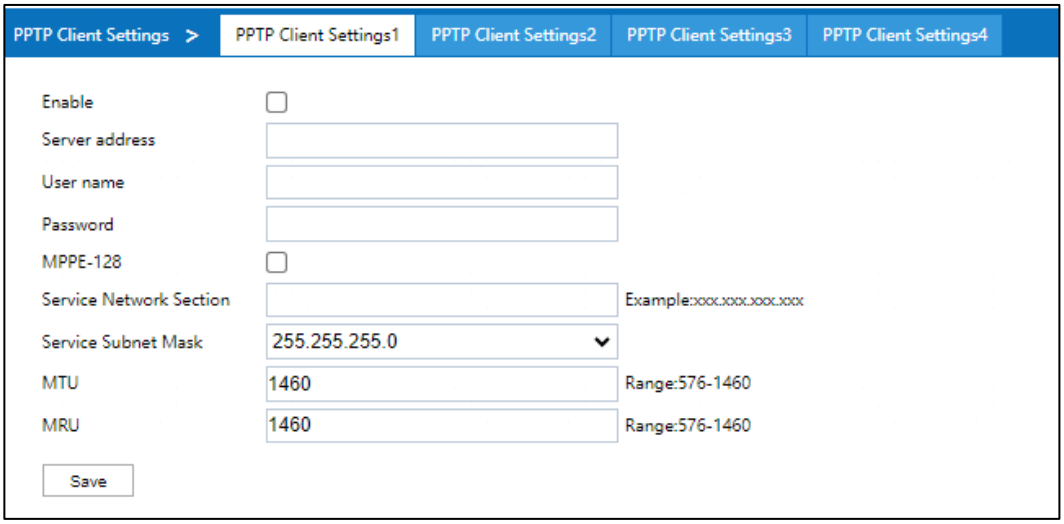
Operation Path

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

Interface Description: PPTP Client 1-4

The PPTP client 1-4 settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of PPTP client 1-4 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-128	Functional enablement checkbox of MPPE (Microsoft Point-to-Point Encryption) protocol, click to enable MPPE encryption function.
Service Network Section	Subnet segment of the PPTP server.
Service Subnet Mask	Drop-down box of subnet mask of the PPTP server.
Advanced Parameters	Click advanced parameters checkbox, the advanced parameters configuration will be displayed.
MTU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.
MRU	Maximum Receive Unit (MRU) input box, unit is byte, the default value is 1460, and the value range is 576-1500.

Copyright © 3onedata Co., Ltd.

8.3 PPTP Server Settings

Function Description

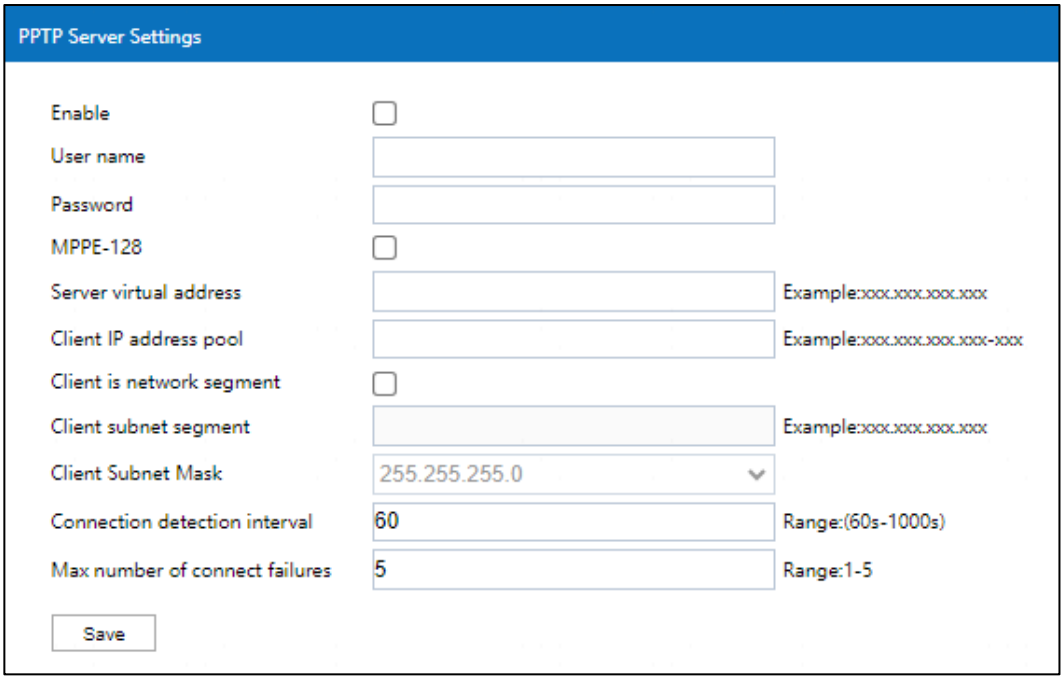
On the page of "PPTP Server Settings", user can configure the parameters related to PPTP server.

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-128	Functional enable checkbox of MPPE (Microsoft Point-to-Point Encryption), click to enable MPPE encryption function.
Server virtual address	• Virtual IP address of PPTP server.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Client IP address pool	• IP address pool range assigned to the client, the format is: xxx.xxx.xxx.xxx-xxx.
Client is network segment	"Client is network segment "enablement checkbox, it allows the router whose subnet is the network segment to connect as a client and access the PPTP VPN server. Click the right button for ON and OFF switching. • ON: Enable the function of the client as network segment, and input the subnet segment and mask of the client; • OFF: Disable the function of client as network segment.
Client subnet segment	Set the network segment that allows the client to access, 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.

8.4 L2TP Client Settings

Layer 2 Tunneling Protocol (L2TP) is an industry-standard Internet tunneling protocol. Its functions are roughly like 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.

Copyright © 3onedata Co., Ltd.

Function Description

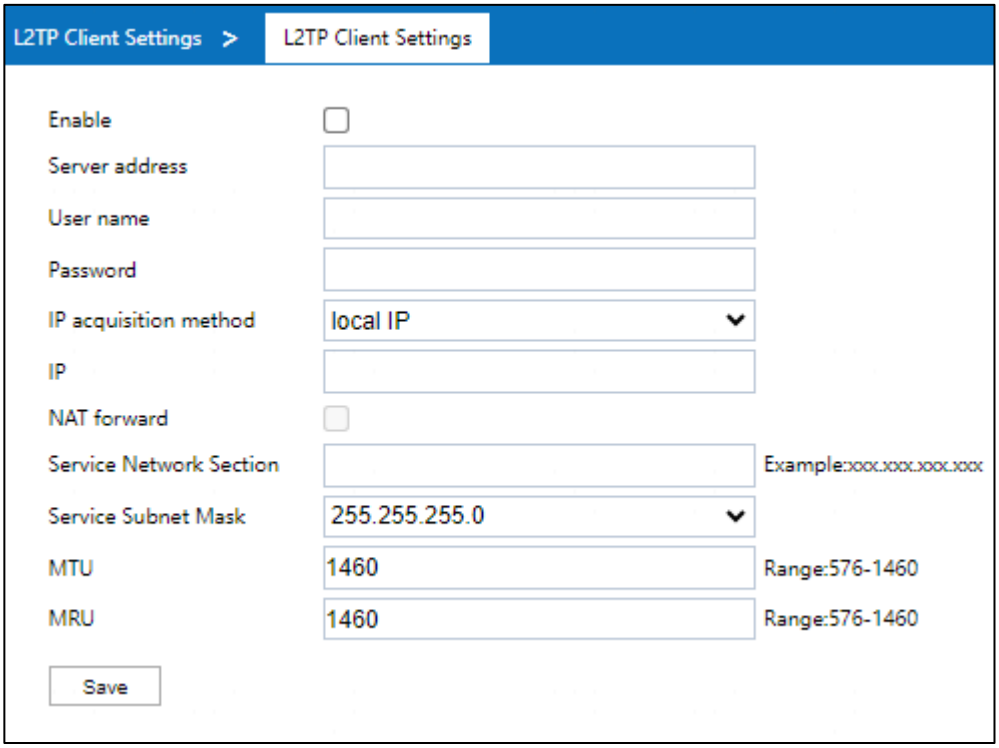
On the page of "L2TP Client Settings", user can configure the parameters related to L2TP client.

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.
IP acquisition method	Acquisition mode of L2TP clients IP address, options are as follows: • Automatic acquisition • Local IP
IP	When “IP acquisition mode” is “Local IP”, the local IP

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	address of the item will be displayed, and the IP address format is xxx.xxx.xxx.xxx.
NAT forward	Enablement checkbox of NAT (Network Address Translation), check to enable NAT forwarding. All data flows of client are forwarded through the VPN server.
Service Network Section	User name provided by L2TP to the client for connection
Service Subnet Mask	Password corresponding to the user name provided by L2TP to the client for connection
MTU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the value range is 576-1460.
MRU	Maximum Receive Unit (MRU) input box, unit is byte, the default value is 1460, and the value range is 576-1460.

8.5 L2TP Server Settings

Function Description

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

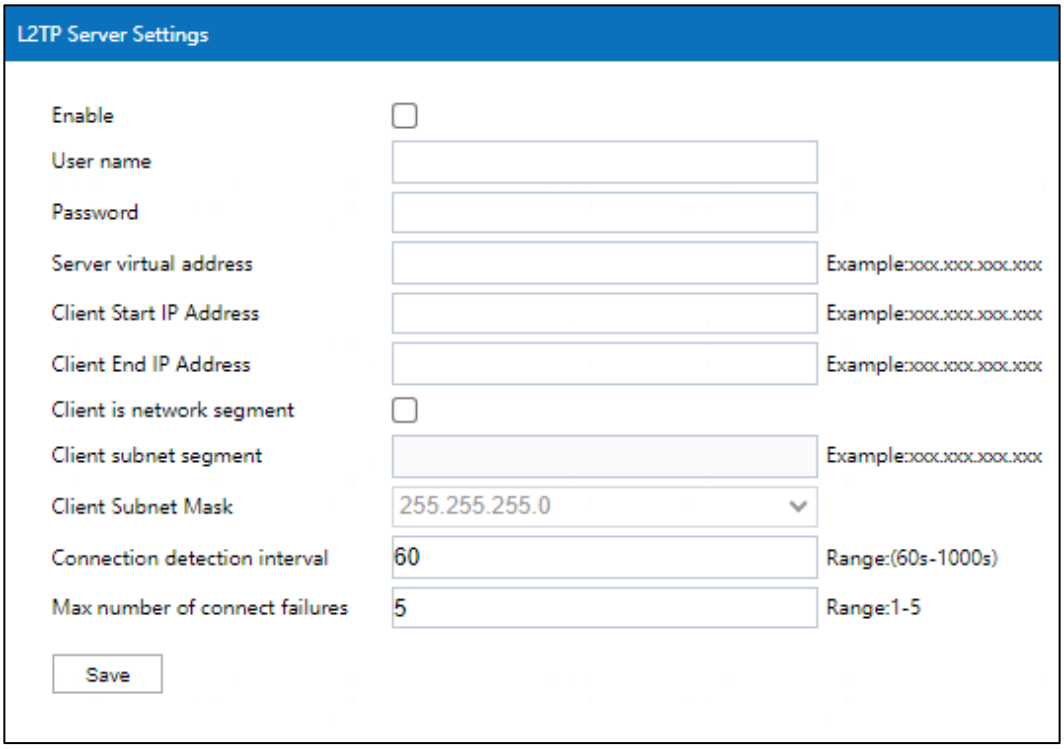
Operation Path

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

Interface Description

The L2TP server settings interface is as follows:

Copyright © 3onedata Co., Ltd.



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 segment	"Client subnet segment" enable checkbox. It allows the router whose subnet is the network segment to connect as a client and access the L2TP VPN server. Click to enable the function of the client as network segment. After enabled, the subnet segment and mask of the client can be input.
Client Subnet segment	Set the network segment that allows the client to access, and use it with the client as the network

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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.

8.6 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.

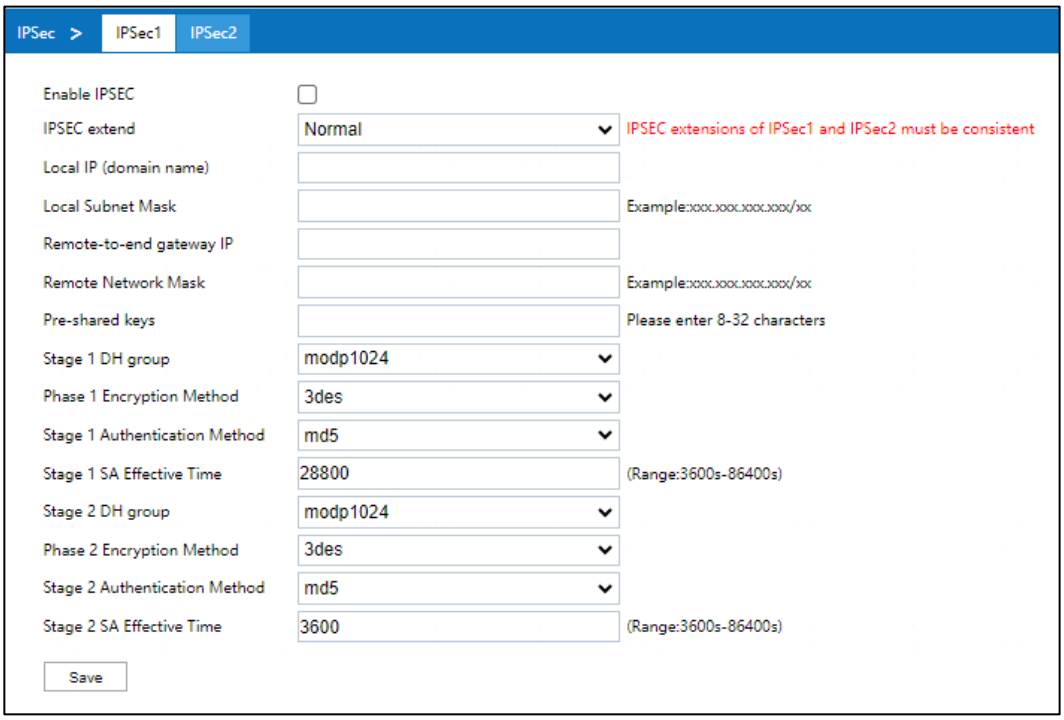
Operation Path

Open in order: "VPN tunnel > IPsec".

Interface Description

IPsec settings interface is as follows:

Copyright © 3onedata Co., Ltd.



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 are as follows: • Normal: Regular IPSEC; • GRE: GRE over IPSEC, GRE encapsulation based on IPSEC encryption; • L2TP: GRE over L2TP, L2TP encapsulation based on IPSEC encryption.
Local IP (domain name)	IP address or domain name of the local external network port
Local Subnet Mask	The local subnet and mask of the router, for example: 192.168.4.0/24.
Remote-to-end gateway IP	External network port IP of the opposite end
Remote Network Mask	Protected subnet and subnet mask of the opposite IPsec end, for example: 192.168.4.0/24.
Pre-shared keys	Unicode string that verifies the IPsec connection.
Stage 1 DH group	Stage 1 DH exchange algorithm, options are as follows: • modp768

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• modp1024 • modp1536 • modp2048
Phase 1 Encryption Method	Phase 1 encryption algorithm, options: • 3des • aes128 • aes192
Stage 1 Authentication Method	Stage 1 Authentication Method, options are 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 are as follows: • modp768 • modp1024 • modp1536 • modp2048
Stage 2 Encryption Method	Phase 2 encryption algorithm, options are as follows: • 3des • aes128 • aes192
Stage 2 Authentication Method	Stage 2 Authentication Method, options are as follows: • md5 • sha • sha256 • sha384 • sha512

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Stage 2 SA Effective Time	Stage 2 SA Effective time, unit is second and default is 3600.

8.7 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.

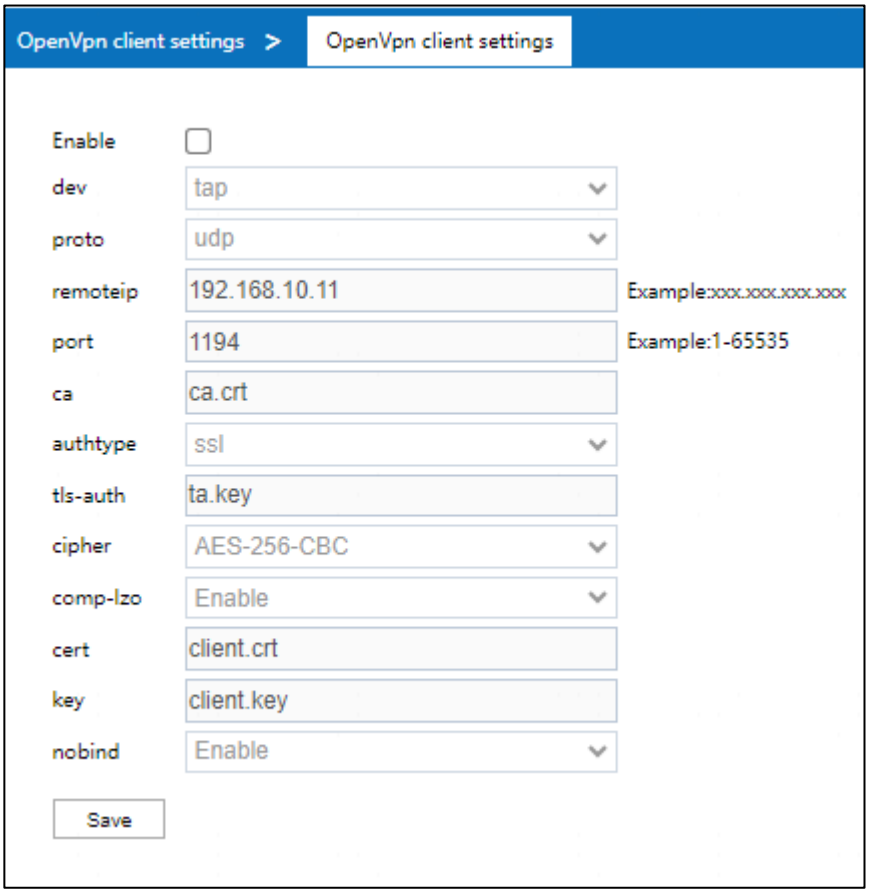
Operation Path

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

Interface Description: OpenVpn Client Settings

The OpenVpn client settings interface is as follows:

Copyright © 3onedata Co., Ltd.



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.
remote ip	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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	mainly used to verify the legitimacy of server or client certificate.
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:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 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.

8.8 Certificate Settings

Function Description

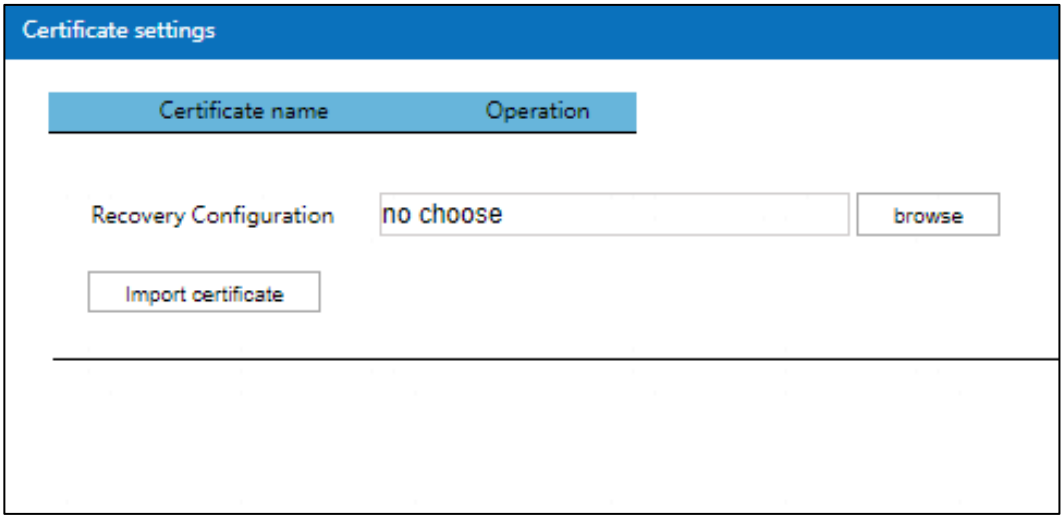
On the “Certificate Settings” page, you can add OpenVPN client authentication certificates and related configuration files.

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.
Import certificate	Click “browse” to select a local certificate file, and then

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	click “Import Certificate” to upload the certificate file to the device. Note: Only files in ". crt", ".key" or ". ovpn" format can be uploaded.

Copyright © 3onedata Co., Ltd.

9 System Management

9.1 Device Alias

Function Description

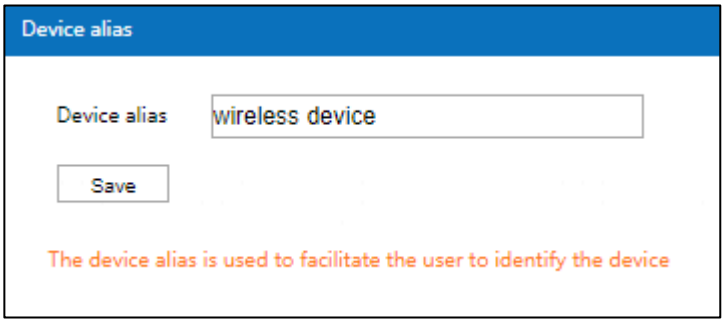
On the “Device Alias” page of system tool, user can set the device alias.

Operation Path

Please open in order: "System Manage > Device alias".

Interface Description

The Device alias interface is as follows:



Configuration of the main elements of the device alias interface:

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

Copyright © 3onedata Co., Ltd.

9.2 Time Settings

Function Description

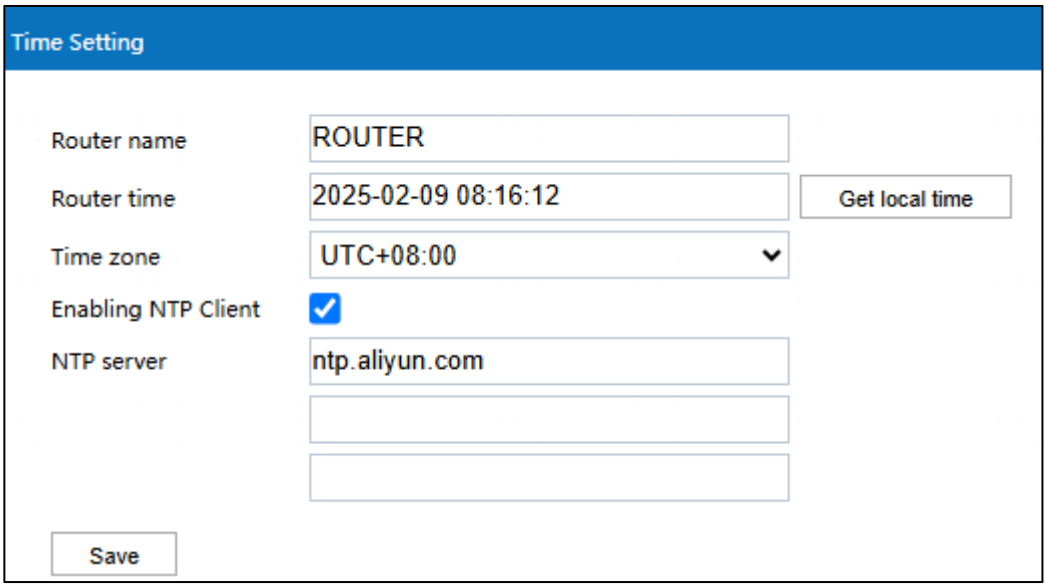
On the page of "Time Setting", user can configure time-related parameters information.

Operation Path

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

Interface Description

Time setting interface is as follows:



The main elements configuration description of time setting 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: minute: second.
Time zone	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:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	When there are multiple candidate NTP clients, the default is the first one. The higher the order, the higher the priority.

9.3 Access Settings

Function Description

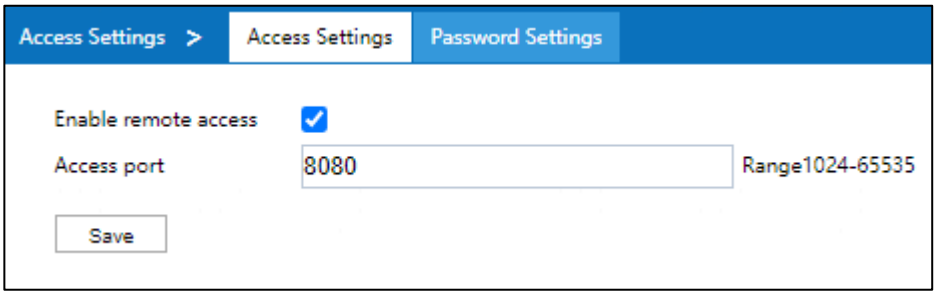
On the page of "Access settings", user can enable remote access and modify the username and password for accessing the device.

Operation Path

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

Interface Description 1: Access Settings

Access settings interface is as follows:



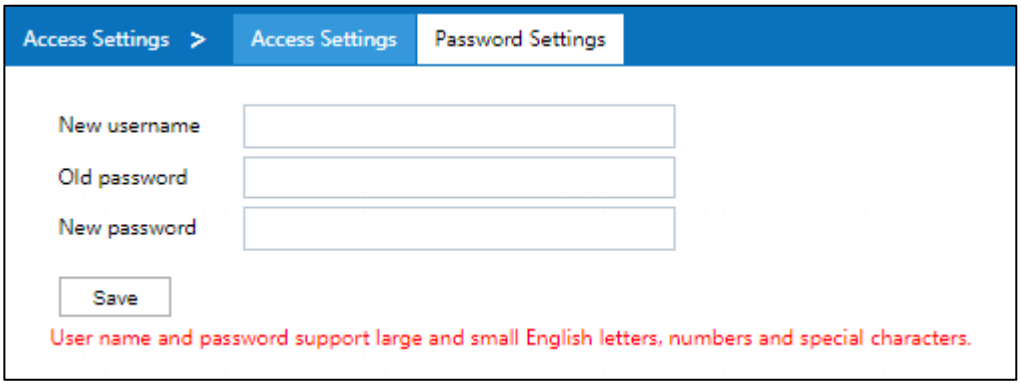
The main elements configuration description of access settings interface:

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

Copyright © 3onedata Co., Ltd.



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.

9.4 Timed Restart

Function Description

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

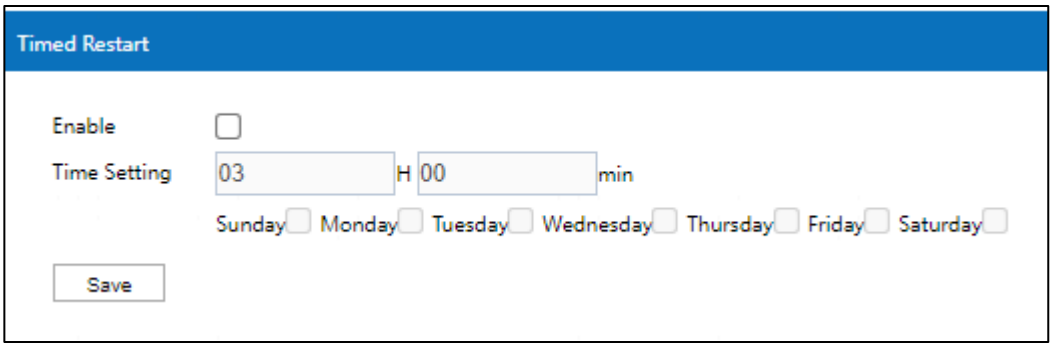
Operation Path

Open in order: "System Manage > Timed Restart".

Interface Description

The timed restart interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of timed restart interface:

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

9.5 Backup Recovery

Function Description

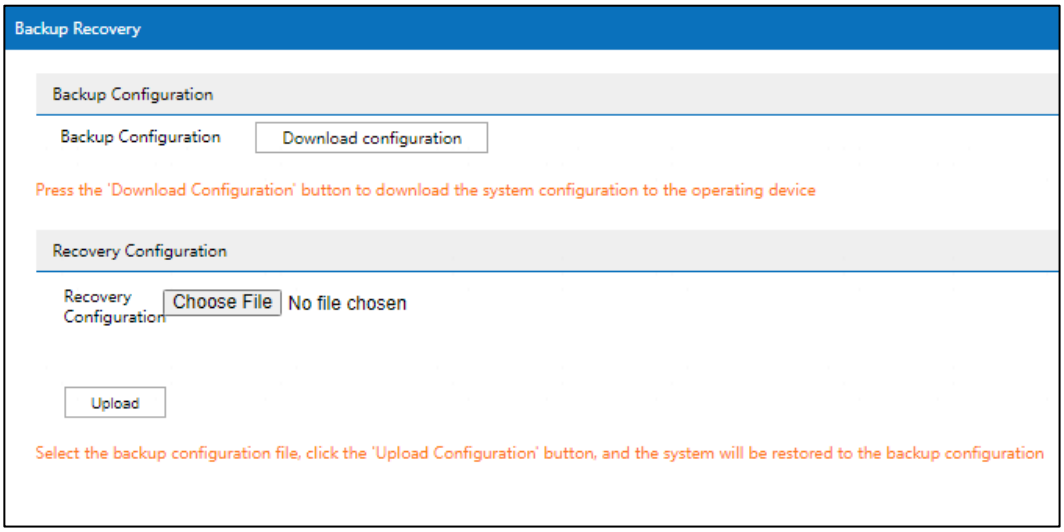
On the page of "Backup Recovery", user can select files for uploading configuration.

Operation Path

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

Interface Description

The backup recovery settings interface is as follows:



Copyright © 3onedata Co., Ltd.

The main elements configuration description of backup recovery settings interface:

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

9.6 Log Manage

Function Description

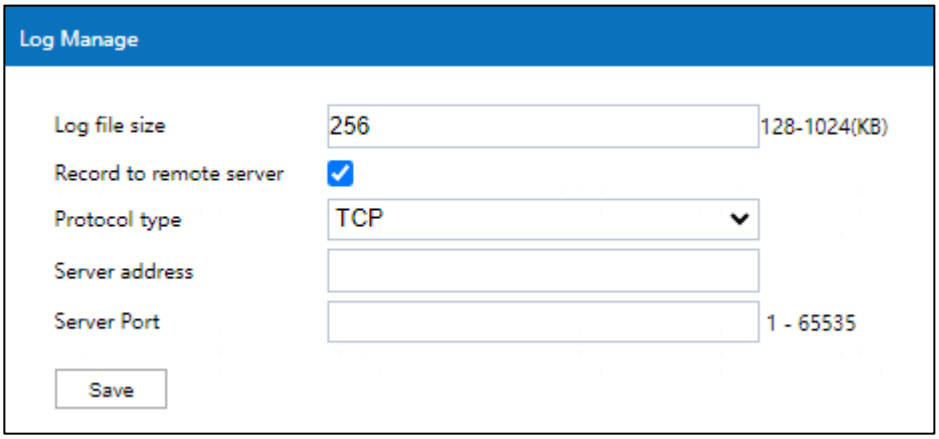
On the page of "Log manage", user can record the log files to the remote server.

Operation Path

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

Interface Description

The log management interface is 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 256
Record to remote server	Record to remote server enable checkbox, check to enable the function of recording to remote server to record log files to the remote server.
Protocol type	• Drop-down box of the protocol type used by the record to remote server, options as follows:

Copyright © 3onedata Co., Ltd.

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

9.7 Firmware Upgrade

Function Description

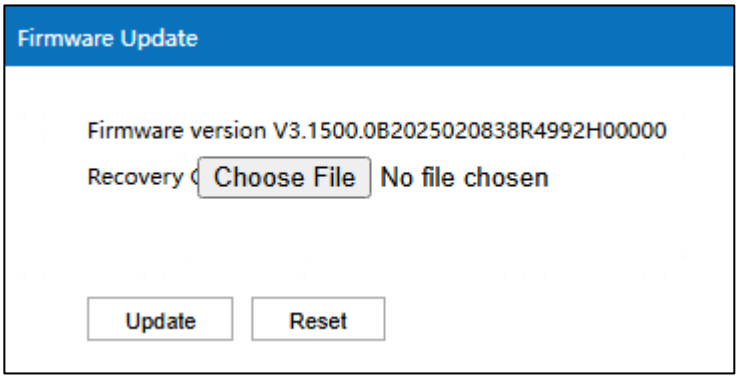
On the "Firmware Upgrade" page, user can update the device system program via firmware upgrade.

Operation Path

Open in order: "System Manage > Firmware Update".

Interface Description

System upgrade interface is as follows:



The main element configuration description of Firmware Upgrade interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	remain unchanged and the firmware version information will be changed.

9.8 System Settings

Function Description

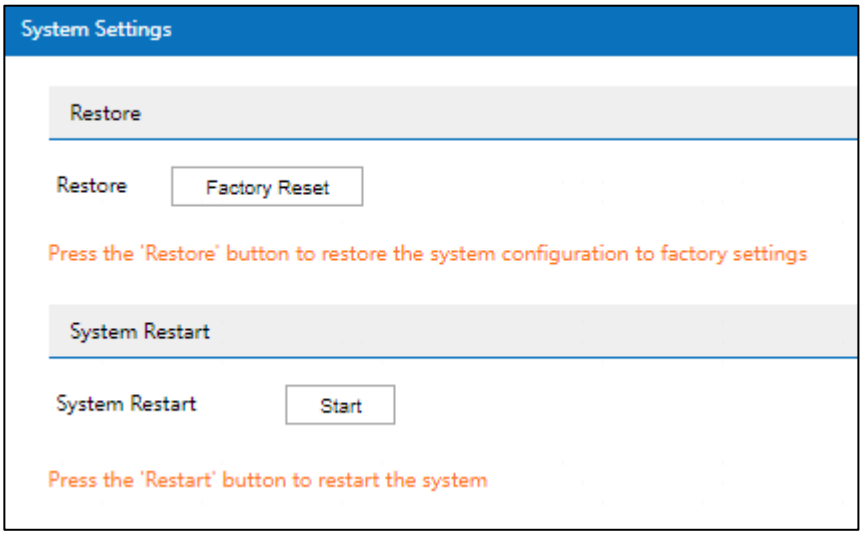
On the “System Settings” page, you can download the current configuration files, restore factory settings, or reboot the device.

Operation Path

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

Interface Description

System settings interface is as follows:



The main elements configuration description of system settings interface:

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

Copyright © 3onedata Co., Ltd.

9.9 System Log

Function Description

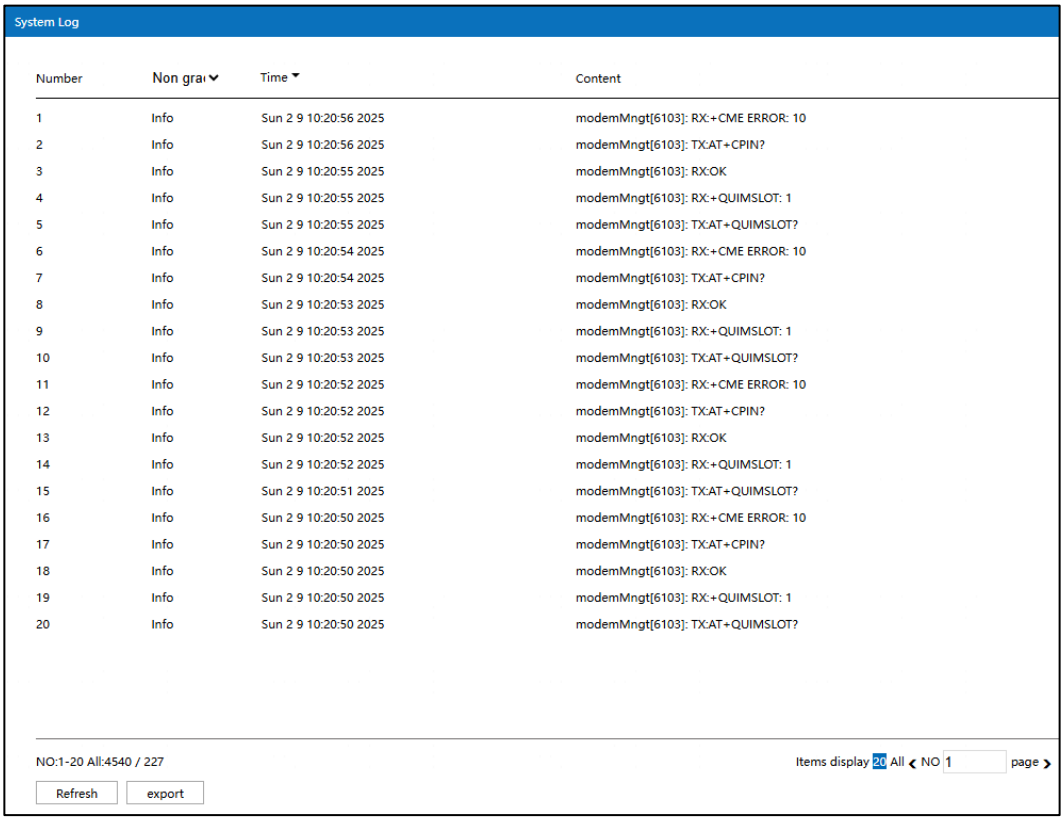
On the page of "System log", user can view the device system logs.

Operation Path

Open in order: “System Manage > System Log”.

Interface Description

The system log interface is as follows:



The main elements configuration description of system log interface:

Interface Element	Description
Number	Log messages display sequence.
Category dropdown box	User can select the category of log to display specific log information. Optional values: • Non grading: all information; • Error: error messages; • Warning: warning messages.
Time	The date and time filter button for log information. Note:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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 are as follows: • 20: Display 20 log messages per page; • All: a 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".

Copyright © 3onedata Co., Ltd.

10 Diagnostic Tools

10.1 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

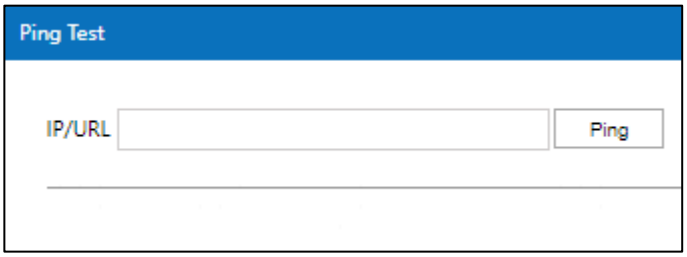
On the page of "Ping test", user can detect whether the target host can be connected.

Operation Path

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

Interface Description

The Ping test interface is 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.

Copyright © 3onedata Co., Ltd.

10.2 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

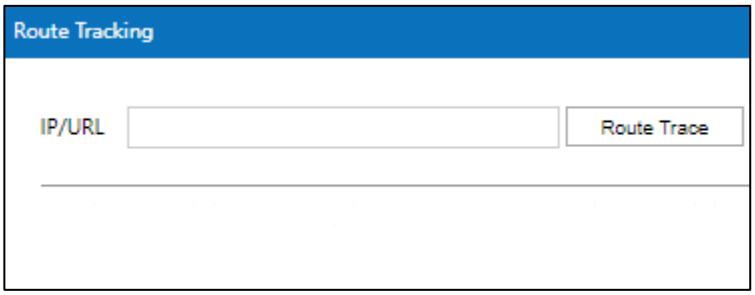
On the page of "Route Tracking", user can perform route tracking for the target host.

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.

Copyright © 3onedata Co., Ltd.

11 FAQ

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

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

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

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

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

   This is determined by the nature of the outdoor AP antenna. The antenna of outdoor AP is different from that of indoor AP. Its advantage lies in long-distance transmission. It is a normal phenomenon that the throughput of an outdoor AP is slightly worse than an indoor AP in the short distance transmission (within 50 meters).

3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

4. **What is a universal bridging?**

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

5. **When should universal bridging and WDS be used?**

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

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

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

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

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

Copyright © 3onedata Co., Ltd.

IP would be automatically overwritten.

Copyright © 3onedata Co., Ltd.

12 Maintenance and Service

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

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

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

12.1 Internet Service

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

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

12.2 Service Hotline

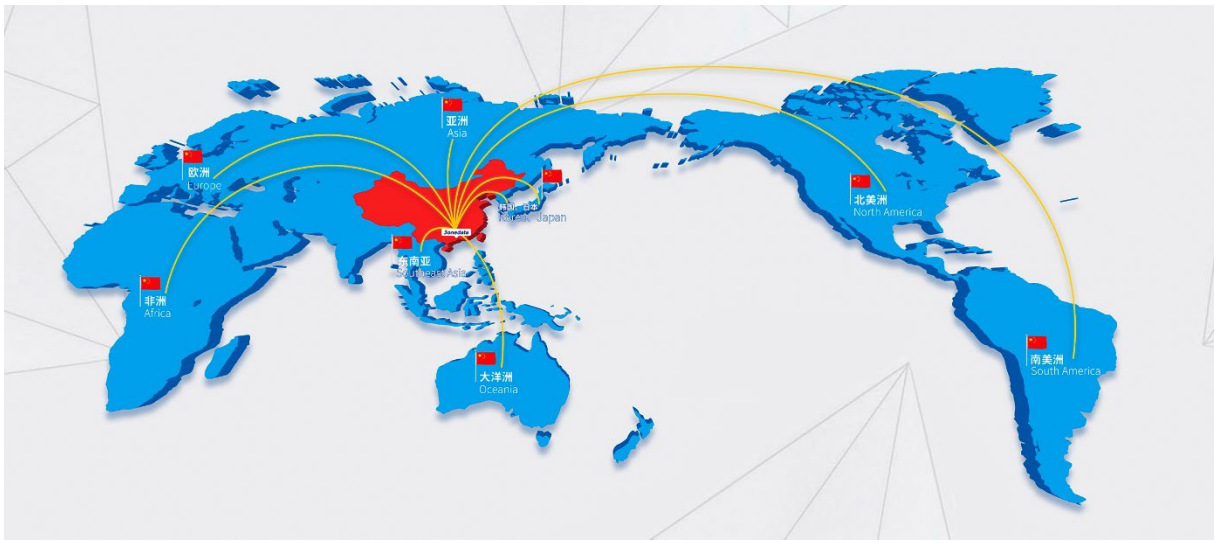
Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you solve the product or usage problems ASAP. Free service hotline: +86-4008804496.

Copyright © 3onedata Co., Ltd.

12.3 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 proprietary and confidential
Copyright © 3onedata Co., Ltd.



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