3onedata



IAP2600
Industrial-grade 5G Router
User Manual

Document Version: 01

Issue Date: 02/24/2025

Copyright © 2025 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 3ondedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

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

3onedata



3onedata Co., Ltd.

Headquarter	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen,
Technology	tech-support@3onedata.com
Service	+86-400-880-4496
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:

- Network management method

Readers

This manual mainly suits for engineers as follows:

- Network administrator responsible for network configuration and maintenance
- On-site technical support and maintenance staff
- Network Engineer

Text Format Convention

Format	Description
“”	Words with “” represent the interface words. e.g.: "The port number".
>	Multi-level paths are 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.

Symbols

Format	Description
Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
Note	Make a necessary supplementary instruction for operation description.

Copyright © 3onedata Co., Ltd.

Format	Description
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Revision Date	Revision Description
01	2025-02-24	Product release

Copyright © 3onedata Co., Ltd.

Contents

PREFACE 1
CONTENTS I
1 LOG IN THE WEB INTERFACE 1
1.1 WEB BROWSING SYSTEM REQUIREMENTS 1
1.2 SET THE IP ADDRESS OF THE COMPUTER 1
1.2.1 Wired Access Mode 1
1.2.2 Wireless Access Mode 2
1.3 LOG IN THE WEB CONFIGURATION INTERFACE 3
2 SYSTEM INFORMATION 1
3 BASIC NETWORK 1
3.1 WAN NETWORK SETTINGS 1
3.2 MOBILE DETECTION 6
3.3 LINK BACKUP 7
3.4 LOCAL AREA NETWORK 9
3.5 DYNAMIC DOMAIN NAME 10
3.6 ROUTING TABLE 11
4 WLAN SETTINGS 1
4.1 BASIC PARAMETER SETTINGS 1
4.2 WIRELESS CLIENT FILTERING 12
5 ADVANCED NETWORK 1
5.1 PORT FORWARD 1
5.2 PORT REDIRECTION 2
5.3 DMZ SETTINGS 3
5.4 UPNP SETTINGS 4
5.5 VRRP 6
5.6 RIP 10
5.7 OSPF 11
5.8 STATIC DHCP 13
5.9 QOS 14
6 FIREWALL 1
6.1 IP FILTER 1
6.2 MAC FILTER 3
6.3 URL FILTER 4

Copyright © 3onedata Co., Ltd.

6.4 KEYWORD FILTER 5
7 VPN TUNNEL 1
7.1 GRE SETTINGS 1
7.2 PPTP CLIENT SETTINGS 2
7.3 PPTP SERVER SETTINGS 4
7.4 L2TP CLIENT SETTINGS 5
7.5 L2TP SERVER SETTINGS 7
7.6 IPSEC 8
8 SYSTEM MANAGEMENT 1
8.1 TIME SETTING 1
8.2 ACCESS SETTINGS 2
8.3 TIMED RESTART 3
8.4 BACKUP RECOVERY 4
8.5 LOG MANAGE 5
8.6 FIRMWARE UPGRADE 6
8.7 SYSTEM SETTINGS 7
9 DIAGNOSTIC TOOLS 1
9.1 SYSTEM LOG 1
9.2 PING TEST 3
9.3 ROUTE TRACKING 3
10 FAQ 5
11 MAINTENANCE AND SERVICE 7
11.1 INTERNET SERVICE 7
11.2 SERVICE HOTLINE 7
11.3 PRODUCT REPAIR OR REPLACEMENT 7

Copyright © 3onedata Co., Ltd.

1 Log in the Web Interface

1.1 WEB Browsing System Requirements

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

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

1.2 Set the IP Address of the Computer

1.2.1 Wired Access Mode

The default management network address of the device 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

Copyright © 3onedata Co., Ltd.

computer and device is reachable.

- Before making a local configuration, make sure that the IP address of the computer and the serial server are on the same subnet.

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

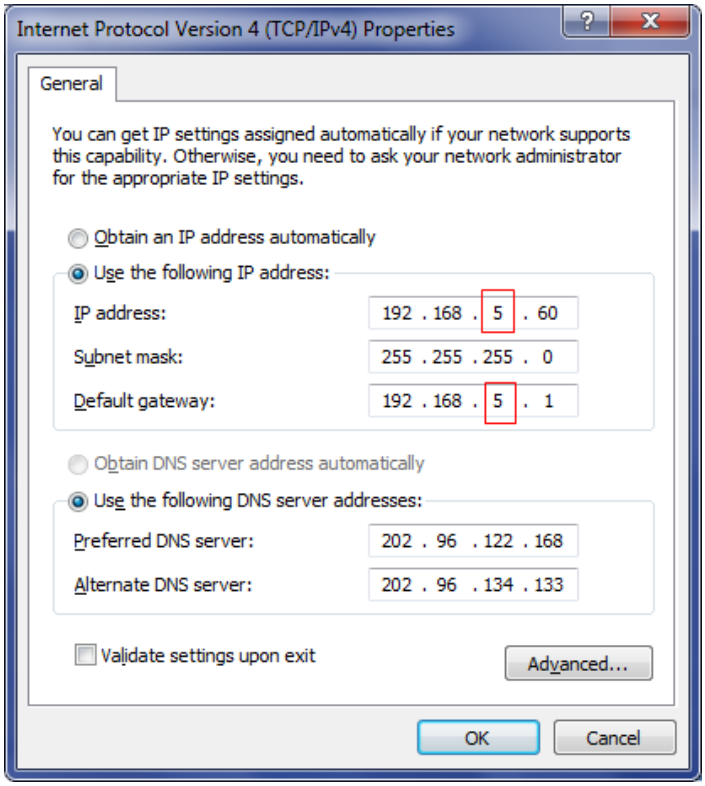
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follows:

Step 1 Open “Control panel > Network connection > Local area connection > Properties > Internet protocol version (TCP/IPv4) > Properties”.

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



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

Step 4 End.

1.2.2 Wireless Access Mode

The default management network address of the device as follows:

IP Settings	Default Value
IP address	192.168.1.254

Copyright © 3onedata Co., Ltd.

IP Settings	Default Value
Subnet mask	255.255.255.0

When configuring a device through the Web:

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

Notice:

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

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

Operation Steps

Operation steps of wireless connection as follows.

Notes:

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

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

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

Note:

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

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

1.3 Log in the Web Configuration Interface

Operation Steps

Login in the web configuration interface as follow:

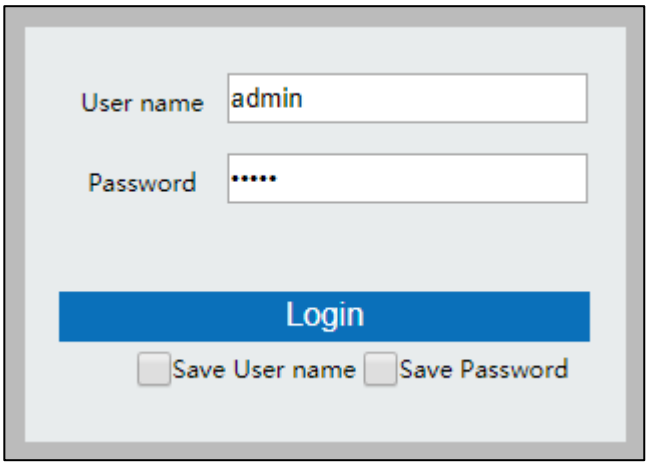
步骤 **1** Run the computer browser.

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

步骤 **3** Click the "Enter" key.

步骤 **4** Pop up a window as the figure below, enter the user name and password on the login window.

Copyright © 3onedata Co., Ltd.



Note:

The default user name and password for the serial server are "admin", which is strictly case-sensitive when typing.

步骤 **5** Click "Login".

步骤 **6** End.

After login in successfully, user can configure relative parameters and information 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;
- System Information
- SIM card information;
- LAN information;
- WAN information;
- VPN client information;
- VPN server information.

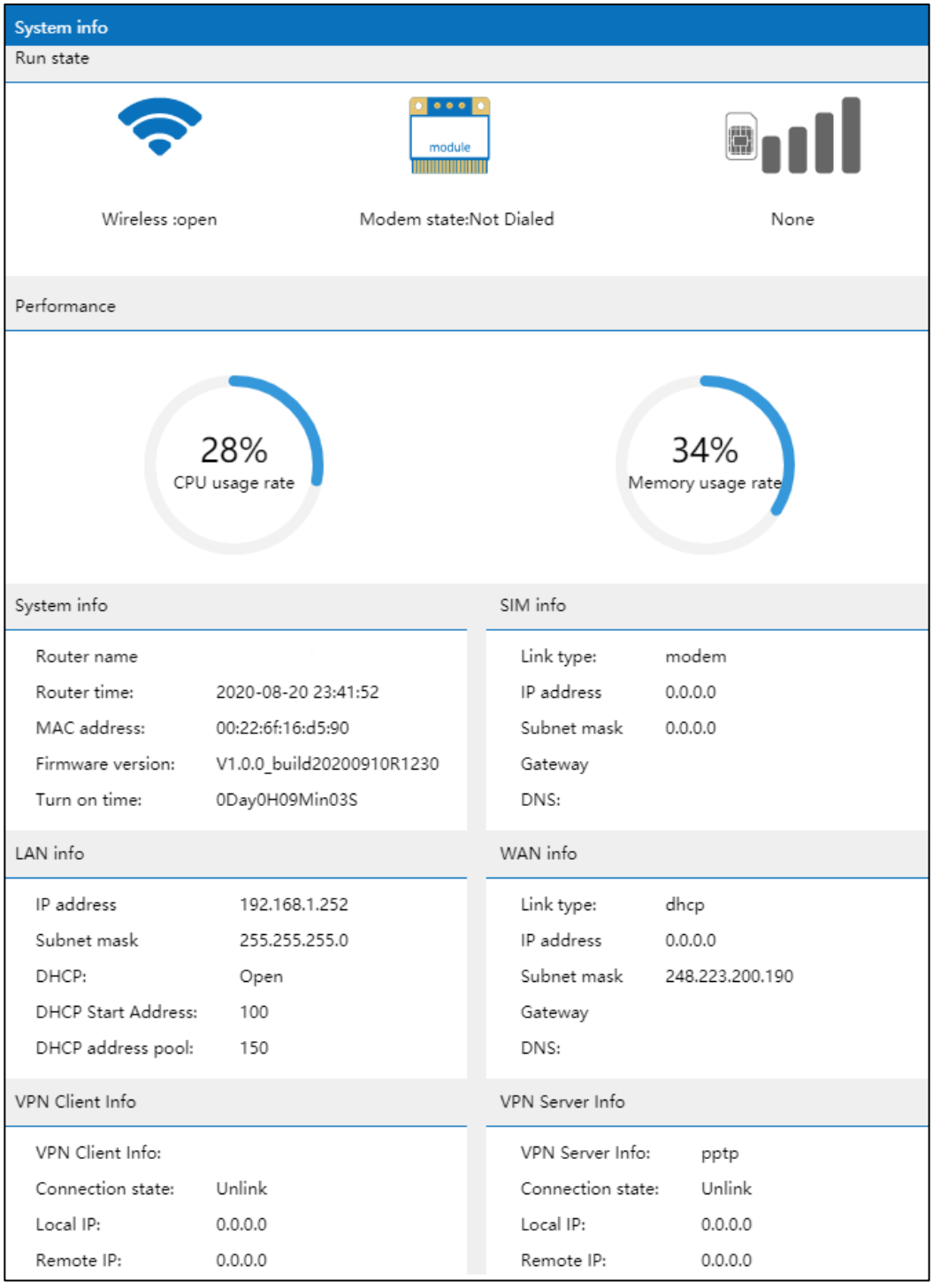
Operation Path

On the navigation bar, select "System information".

Interface Description

System status interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of system status interface:

Interface Element	Description
Running state	**The running state bar**
Wireless	The status of device wireless function is displayed as follows: • Open: the wireless WiFi function has been enabled; • Close: the wireless WiFi function hasn't been enabled.
Modem state	The states of 5G module Modem.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
SIM card	Information including the existence state of SIM card used by current device, operator's network, network operating mode and signal strength etc.
Performance	**The performance bar**
CPU (%)	Device CPU utilization rate(%).
Memory (%)	Device memory utilization rate(%). Note: It will influence the device performance if the program takes up too much memory.
System Info	**System information bar**
Router name	Display the device name.
Router time	The current time displayed by router. Its format is Year-Month-Day Hour: Minute: Second.
Firmware version	Device firmware version.
Turn on time	The run time after turning on the device
SIM info	**SIM information bar**
Line Type	SIM connection Type
IP Address	IP address obtained by SIM card from network operator.
Subnet mask.	Subnet mask address of SIM.
Gateway	The gateway address of SIM.
DNS	DNS server address of SIM.
LAN info	**The LAN information bar**
IP Address	The IP address information of LAN.
Subnet mask.	The subnet mask information of LAN.
DHCP	The state of the DHCP server function.
DHCP start address	The minimum host number of IP address assigned by DHCP address pool, which is 100 by default.
DHCP address pool	The maximum IP address number assigned by DHCP address pool, which is 150 by default
WAN info	**The WAN information bar**
Line 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.
Link status	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.
Link status	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 Basic Network

3.1 WAN network settings

Function Description

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

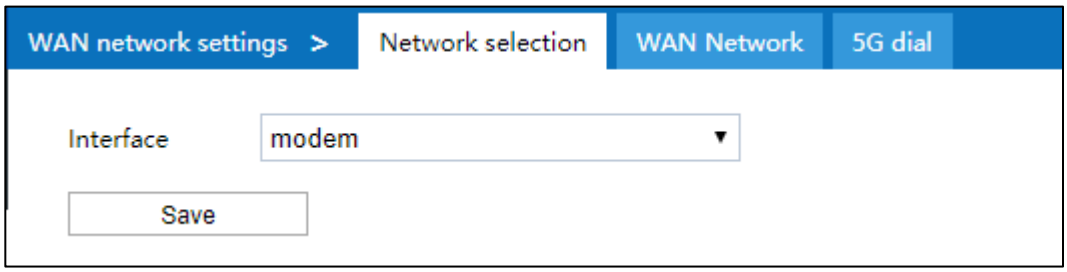
- WAN: connecting WAN through WAN port of the device.
  - Dynamic: the WAN port of the device accesses network address information allocated by network provider or outer network automatically;
  - Static address: configuring the network information of the device WAN port manually;
  - PPPoE: implement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

Operation Path

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

Interface Description 1: Network selection

Network selection interface as follows:



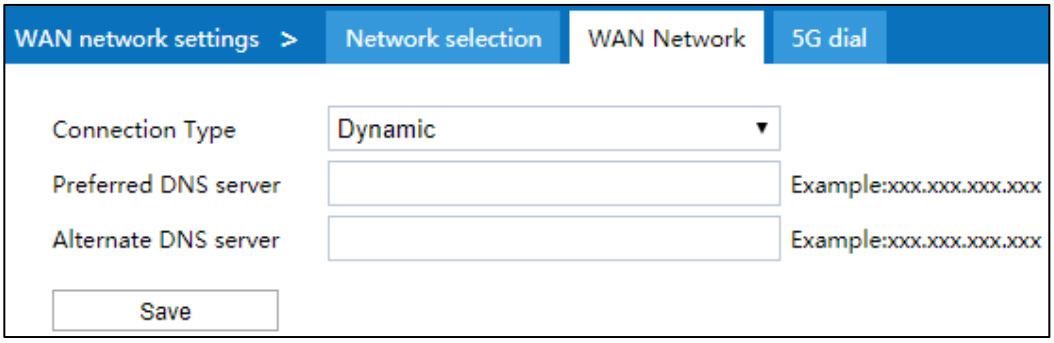
Copyright © 3onedata Co., Ltd.

The main elements configuration description of network selection interface:

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.

Interface Description 2-1: WAN Network-Dynamic access

WAN Network-Dynamic interface is as follows:

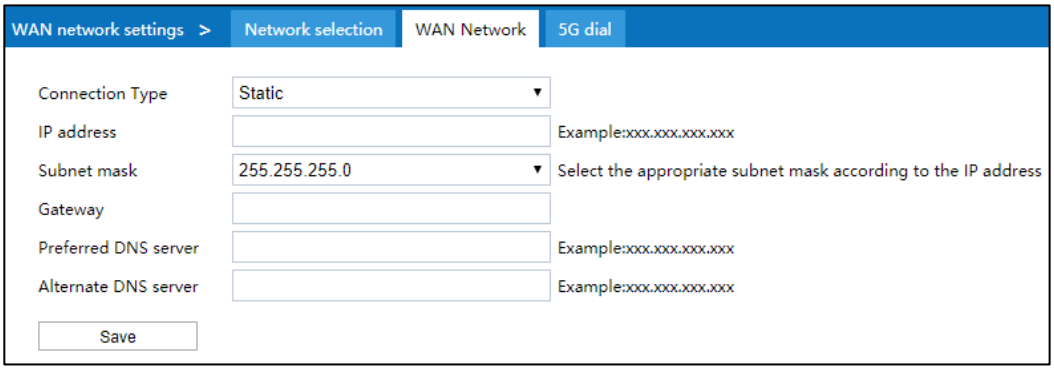


The main elements configuration description of WAN Network-Dynamic interface:

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 outer network.
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:



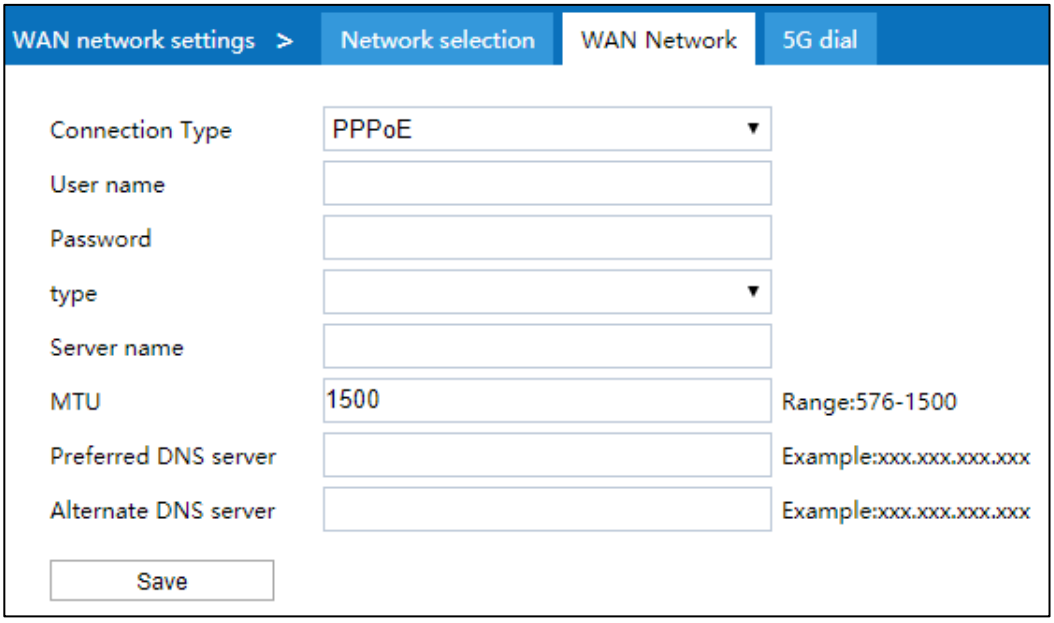
Copyright © 3onedata Co., Ltd.

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

Interface Element	Description
Connectin Type	Static address: the network information configuration of device WAN port.
IP Address	The fixed IP address distributed by network provider or outer network.
Subnet mask	Drop-down list of subnet mask.
Gateway	Gateway address offered by network provider or WAN.
Preferred DNS server	The DNS server address provided by network provider or outer network.
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: realize Internet access via PPPoE point-to-point protocol dialing.
User name	User name of PPPoE connection. Note:

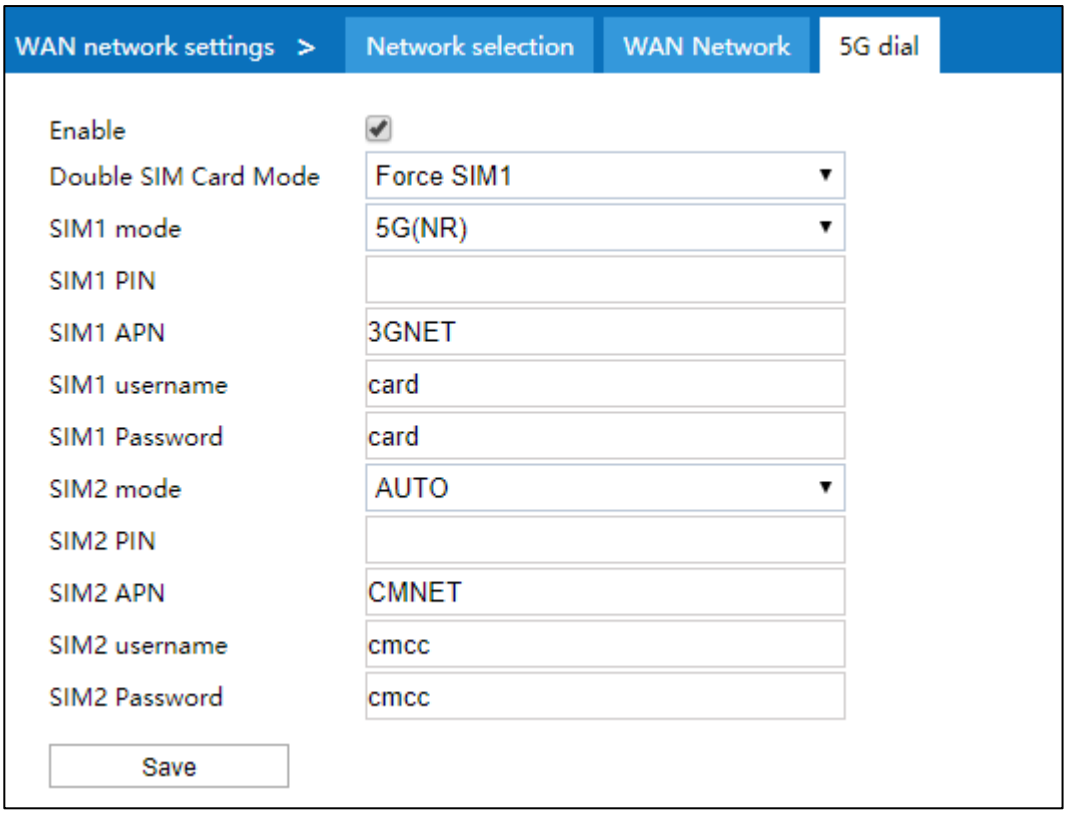
Copyright © 3onedata Co., Ltd.

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

Interface Description 3: 5G dial

5G dial interface as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of 5G dial interface:

Interface Element	Description
Enabled	Enable checkbox, check to enable 5G dialing function.
Double SIM card mode	In the drop-down list of double SIM card mode, user can choose specified SIM card. The options are: • Force SIM1; • Force SIM2;
SIM1 mode	The drop-down list of SIM1 mode. The options are: • Auto: self-adaptation; • 5G(NR) • LTE(4G) • (WCDMS/TD-SCDMA) • 3G(CDMA/EVDO)
SIM1 PIN	The Personal Identification Number (PIN) of SIM1. Please enter 4 to 8-digit PIN code if the boot PIN code is enabled; It is null by default if not enabled. Notice: When PIN code is enabled, user needs to enter it every time turning on the device. Please be cautious, it would be locked automatically if you enter wrong codes in three times.
SIM1 APN	The SIM1 access point name. It defaults to 3GNET.

Copyright © 3onedata Co., Ltd.

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

3.2 Mobile Detection

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

Function Description

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

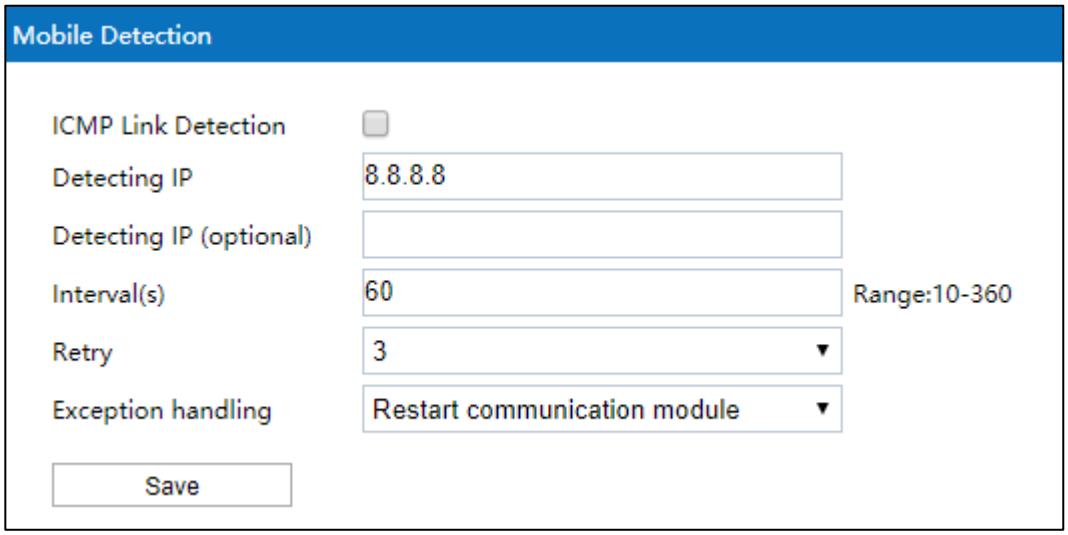
Operation Path

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

Interface Description

The mobile detection interface as follows:

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.
Detecting IP	To detect whether the specified IP address could be connected. It defaults to 8.8.8.8.
Detecting IP (optional)	To detect whether the backup IP address could be connected.
Interval (s)	The time interval of detection, the unit is second and defaults to 60. The value range is 10-360.
Retry	To detect the times of retry, the drop-down list of retry. Options are: 2-5.
Exception handling	The corresponding way of handling detected exception. The drop-down list of exception handling, options are: • Restart communication module; • Switch SIM card; • Reboot the system.

3.3 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

Copyright © 3onedata Co., Ltd.

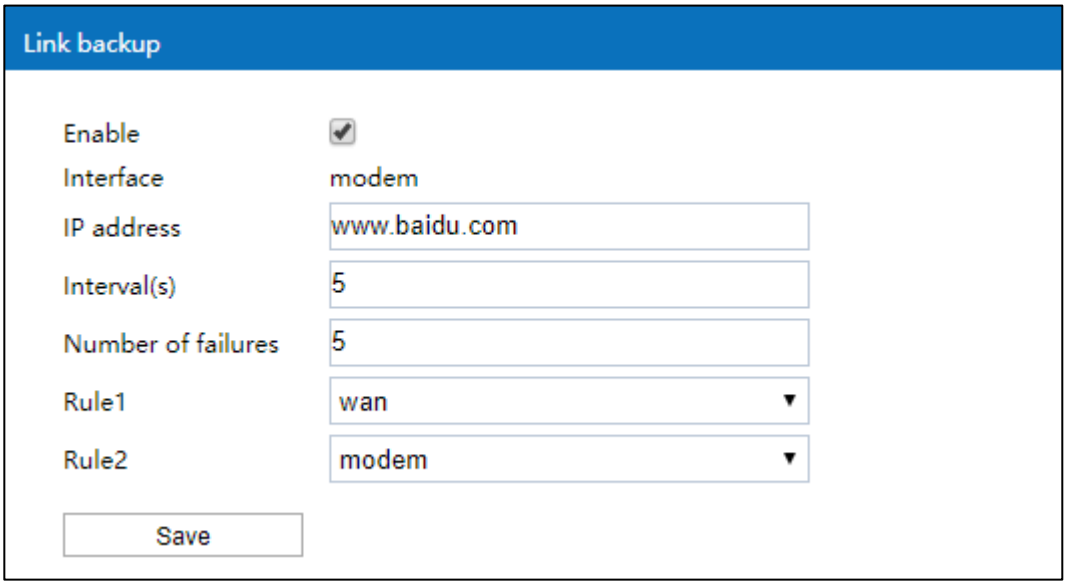
main network is abnormal, network connections can be switched to the backup network; When the main network returns to normal, network connections will automatically switch to the main network.

Operation Path

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

Interface Description

The Link Backup interface as follows:



The main elements configuration description of Link backup interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• modem
Rule2	When the network interface specified by Rule 1 is still abnormal, the device will switch to the network interface specified by Rule 2. Rule2 drop-down list, options as follows: • wan • modem

3.4 Local Area Network

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

Function Description

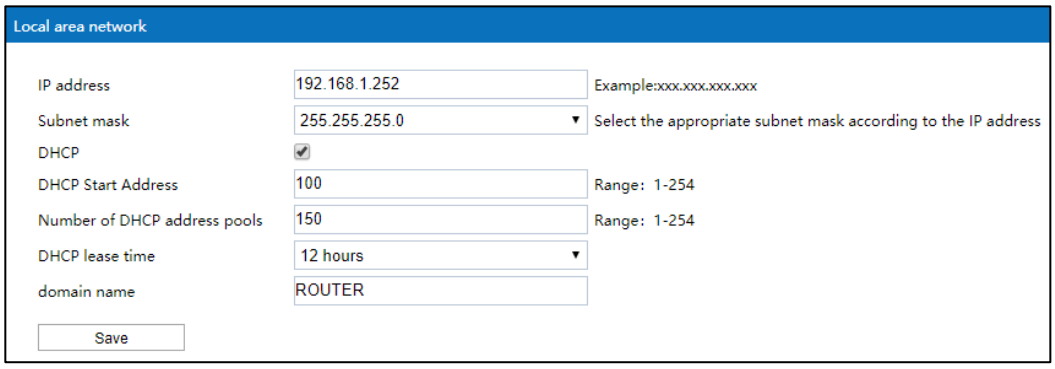
On the “Local Area Network” page, user can turn on DHCP server function and set relevant parameters of gateway.

Operation Path

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

Interface Description

The local area network interface as follows:



The main element configuration description of local area network interface:

Interface Element	Description
IP address	IP address of the device LAN port.
Subnet mask	Drop-down list of subnet mask.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
DHCP	DHCP function enable checkbox, check to enable DHCP server function.
DHCP start address	The minimum IP address host number allocated by DHCP address pool. Value range is 1-254.
Number of DHCP addresses pools	The maximum IP address number allocated by DHCP address pool. Value range is 1-254.
DHCP lease time	Valid time of IP address distributed by DHCP address pool, it defaults to 12 hours. Drop-down list of time unit, options as follows: • 30 minutes; • 1 hour; • 6 hours; • 12 hours; • 1 day; • 3 days; • 7 days.
Domain name	DHCP domain name is composed of letter, number and underline; it supports 0-32 valid characters.

3.5 Dynamic Domain Name

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

Function Description

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

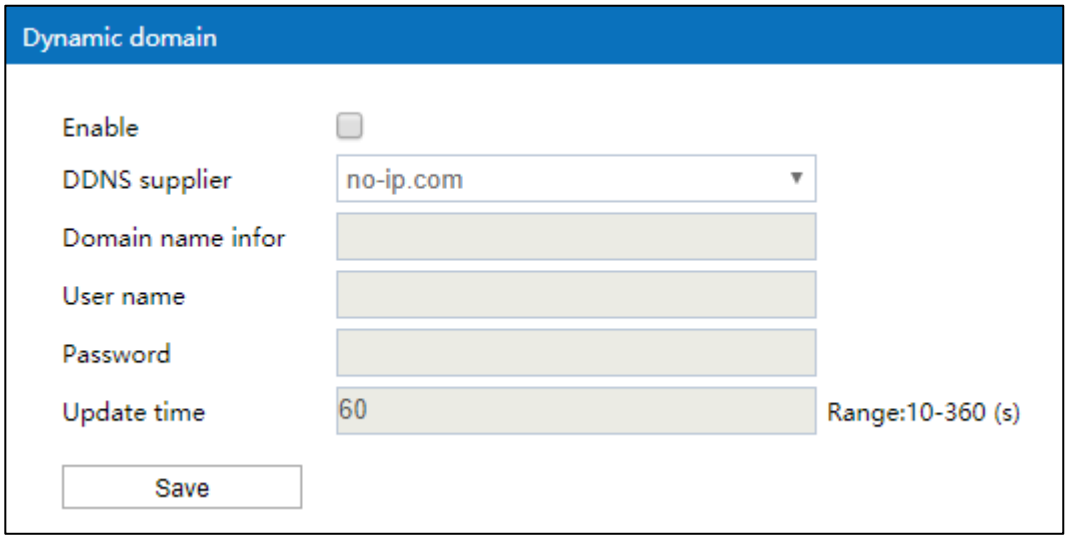
Operation Path

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

Interface Description

The dynamic domain interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of dynamic domain interface:

Interface Element	Description
Enabled	Dynamic Domain Name function checkbox, check to enable dynamic domain function.
DDNS supplier	The router supports multiple DDNS suppliers. The options in the DDNS supplier drop-down list are: • no-ip.com • 3322.org • dyndns.org • oray.com • Custom: When user chooses this item, the corresponding DDNS supplier name could be entered in the input box of DDNS supplier.
Domain name info	The relevant information of domain name applied from DDNS supplier.
Username	The user name applied from DDNS supplier.
Password	The password applied from DDNS supplier.
update time	Update the time interval of dynamic DNS to server, the unit is second, it defaults to 60, the value range is 10-360.

3.6 Routing Table

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

Copyright © 3onedata Co., Ltd.

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

Function Description

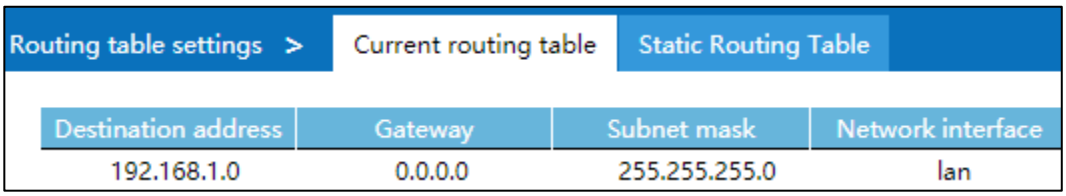
On the “Routing Table” page, user can set relevant information of routing table.

Operation Path

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

Interface Description 1: Current Routing Table

The current routing table interface as follows:

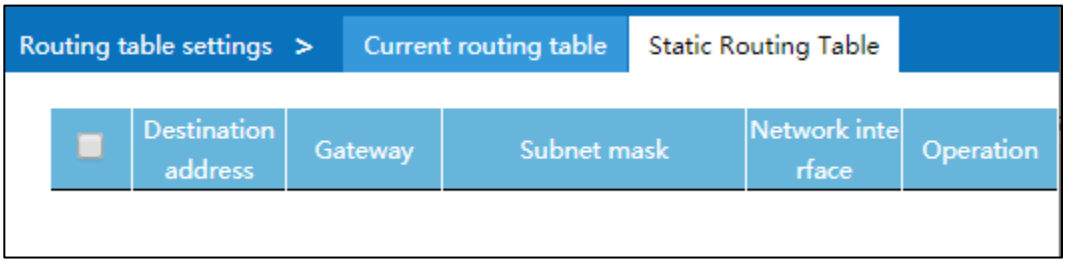


The main element configuration description of current routing table interface:

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

Interface Description 2: Static Routing Table

The static routing table interface as follows:



The main element configuration description of static routing table interface:

Interface Element	Description
All	The check box of static routing entry. Click “All” 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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• 255.255.255.255 • 255.255.255.254 • 255.255.255.252 • 255.255.255.248 • 255.255.255.224 • 255.255.255.192 • 255.255.255.128 • 255.255.254.0 • 255.255.252.0 • 255.255.248.0 • 255.255.240.0 • 255.255.224.0 • 255.255.192.0 • 255.255.128.0 • 255.255.0.0 • 255.254.0.0 • 255.252.0.0 • 255.248.0.0 • 255.224.0.0 • 255.192.0.0 • 255.128.0.0 • 255.0.0.0 • 254.0.0.0 • 252.0.0.0 • 248.0.0.0 • 240.0.0.0 • 224.0.0.0 • 192.0.0.0 • 128.0.0.0
Network interface.	The network interface of static routing: • WAN • LAN • MODEM
Operation	Edit: modify static routing table information.
Add	Click the “add” button at the top right corner to add static routing in the pop-up window of “static routing.
Delete select	Check the static routing information to be deleted, and then click the “delete select’ button at the top right corner to delete them.

Copyright © 3onedata Co., Ltd.

4 WLAN Settings

4.1 Basic Parameter Settings

Function Description

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

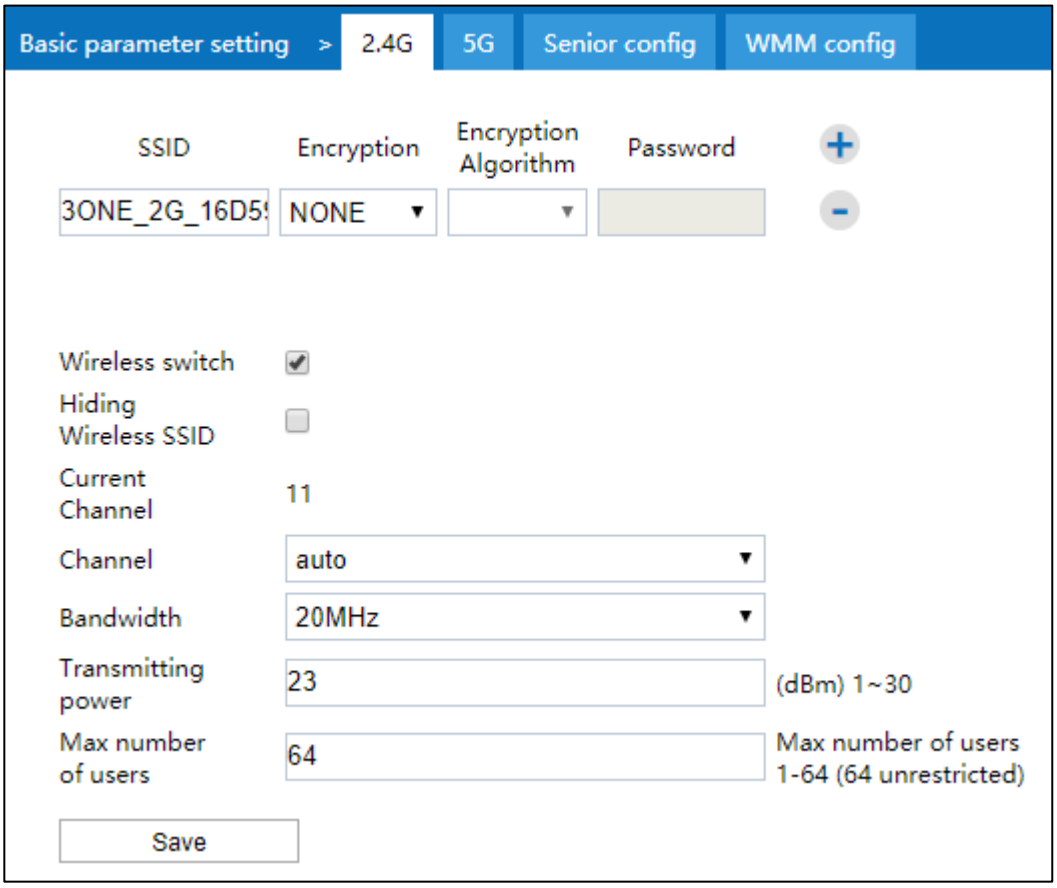
Operation Path

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

Interface Description 1: 2.4G

The 2.4G interface is as follows:

Copyright © 3onedata Co., Ltd.



Main elements configuration descriptions of 2.4G interface:

Interface Element	Description
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE: No encryption; • WPA: Wi-Fi Protected Access. When the wireless authentication method is personal edition, encryption method is PSK (pre-shared key); when the wireless authentication method is enterprise edition, encryption method is 802.1X authentication which use RADIUS server and EAP to authenticate. • WPA2: upgrade version of WPA, supports AES (Advanced Encryption Standard), and provides higher security for WLAN. • WPA-MIXED: the mixed-mode of WPA, is compatible with both WPA and WPA2 encryptions. • WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode.
Encryption	Wireless network supports different encryption algorithms when it

Copyright © 3onedata Co., Ltd.

Interface Element	Description
algorithm	using WPS、WPA2 or WPA-MIXED encryption method, options as follows: • AES(CCMP): CCMP(Counter Mode with CBC-MAC Protocol) uses AES(Advanced Encryption Standard) encryption algorithm. • TKIP: Temporal Key Integrity Protocol, provides more secure protection mechanism than WEP encryption. • TKIP/AES: compatible with both TKIP and AES encryption algorithm.
Password	Password of wireless network, it supports 5 or 8-32 characters.
Wireless switch	Wireless Network function enable checkbox, check to enable 2.4G wireless Wi-Fi network.
Hiding wireless SSID	Hidden wireless SSID enable checkbox, check to enable hidden wireless SSID function. After enabled, name of SSID from the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal first while connecting hidden wireless signal.
Current channel	The working channel of current 2.4G wireless network.
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 1: main frequency band 2412MHz, frequency range 2401~2423MHz; • 2: main frequency band 2417MHz，frequency range 2406~2428MHz. • 3: main frequency band 2422MHz，frequency range 2411~2433MHz. • 4: main frequency band 2427MHz，frequency range 2416~2438MHz. • 5: main frequency band 2432MHz，frequency range 2421~2443MHz. • 6: main frequency band 2437MHz，frequency range 2426~2448MHz. • 7: main frequency band 2442MHz，frequency range 2431~2453MHz. • 8: main frequency band 2447MHz，frequency range 2436~2458MHz. • 9: main frequency band 2452MHz，frequency range

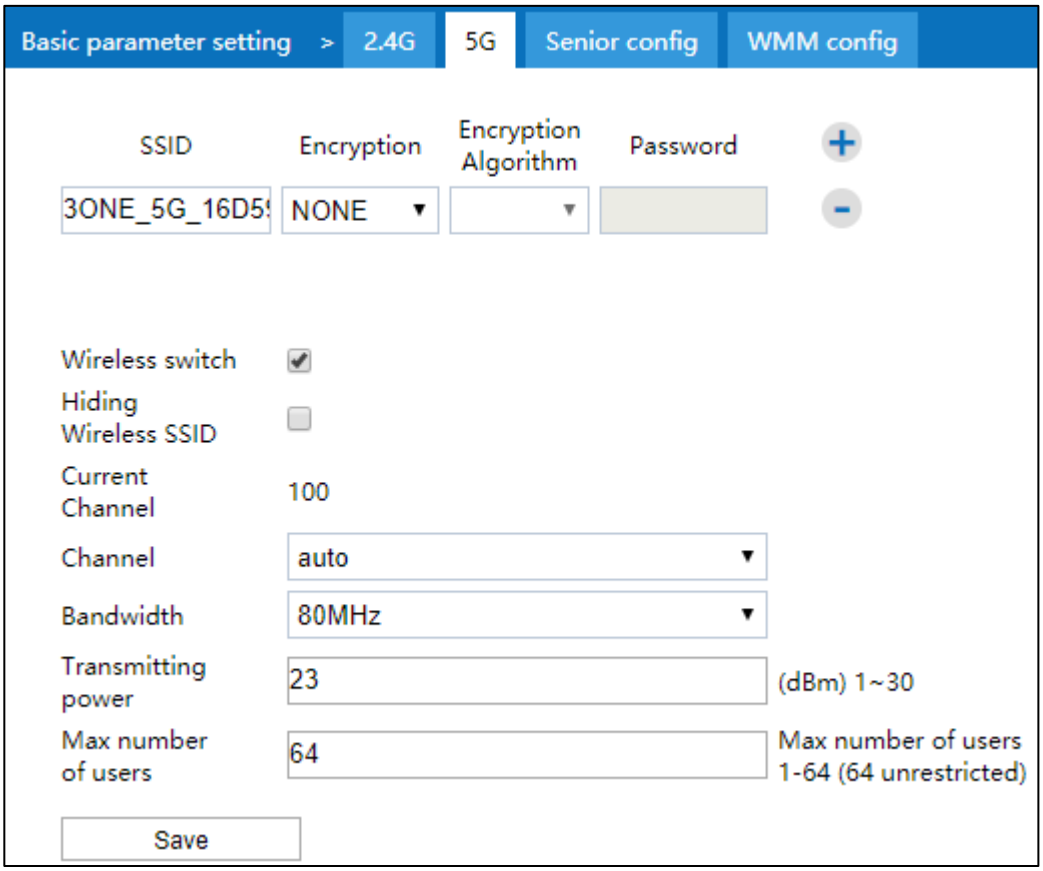
Copyright © 3onedata Co., Ltd.

Interface Element	Description
	2441~2463MHz. • 10: main frequency band 2457MHz，frequency range 2446~2468MHz. • 11: main frequency band 2462MHz，frequency range 2451~2473MHz. • 12: main frequency band 2467MHz, frequency range 2456~2478MHz, this frequency band is not open in USA, so it's temporarily unavailable; • 13: main frequency band 2472MHz, frequency range 2461~2483MHz, this frequency band is not open in USA, so it's temporarily unavailable; Note: In order to improve the network performance, please choose unused channel in the device working environment. Different country opens different channels.
Bandwidth	Channel bandwidth of wireless network, it defaults to 20MHz, options as follows: • 20MHz； • 40MHz。 Note: 40MHz bandwidth binds two 20MHz bandwidth channels together to gain the handling capacity more than twice of the 20MHz bandwidth.
Transmitting power	Transmitted power of the device wireless signal, defaults to 23dBm, value range 1~30dBm. Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is. • Different device has different transmitting power range.
Max number of users	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.

Interface Description 2: 5G

The 5G interface is as follows:

Copyright © 3onedata Co., Ltd.



Main elements configuration descriptions of 5G interface:

Interface Element	Description
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE: No encryption; • WPA: Wi-Fi Protected Access. When the wireless authentication method is personal edition, encryption method is PSK (pre-shared key); when the wireless authentication method is enterprise edition, encryption method is 802.1X authentication which use RADIUS server and EAP to authenticate. • WPA2: upgrade version of WPA, supports AES (Advanced Encryption Standard), provides higher security for WLAN. • WPA-MIXED: the mixed-mode of WPA, is compatible with both WPA and WPA2 encryptions. • WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode.
Encryption algorithm	Wireless network supports different encryption algorithms when it using WPS、WPA2 or WPA-MIXED encryption method, options as follows:

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• AES(CCMP): CCMP(Counter Mode with CBC-MAC Protocol) uses AES(Advanced Encryption Standard) encryption algorithm. • TKIP: Temporal Key Integrity Protocol, provides more secure protection mechanism than WEP encryption. • TKIP/AES: compatible with both TKIP and AES encryption algorithm.
Password	Password of wireless network, it supports 5 or 8-32 characters.
Wireless switch	Wireless Network function enable checkbox, check to enable 5.8G wireless Wi-Fi network.
Hiding wireless SSID	Hidden wireless SSID enable checkbox, check to enable hidden wireless SSID function. After enabled, name of SSID from the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal first while connecting hidden wireless signal.
Current channel	The working channel of current 5.8G wireless network.
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: • Auto: channel self-adaptation; • 36: main frequency band 5180MHz, frequency range 5170~5190MHz; • 40: main frequency band 5200MHz，frequency range 5190~5210MHz. • 44: main frequency band 5220MHz，frequency range 5210~5230MHz. • 48: main frequency band 5230MHz，frequency range 5210~5250MHz. • 52: main frequency band 5260MHz，frequency range 5250~5270MHz. • 56: main frequency band 5280MHz，frequency range 5270~5290MHz. • 60: main frequency band 5300MHz，frequency range 5290~5310MHz. • 64: main frequency band 5320MHz，frequency range 5310~5330MHz. • 100: main frequency band 5500MHz, frequency range 5490~5510MHz, this frequency band is not open in China, so it's temporarily unavailable;

Copyright © 3onedata Co., Ltd.

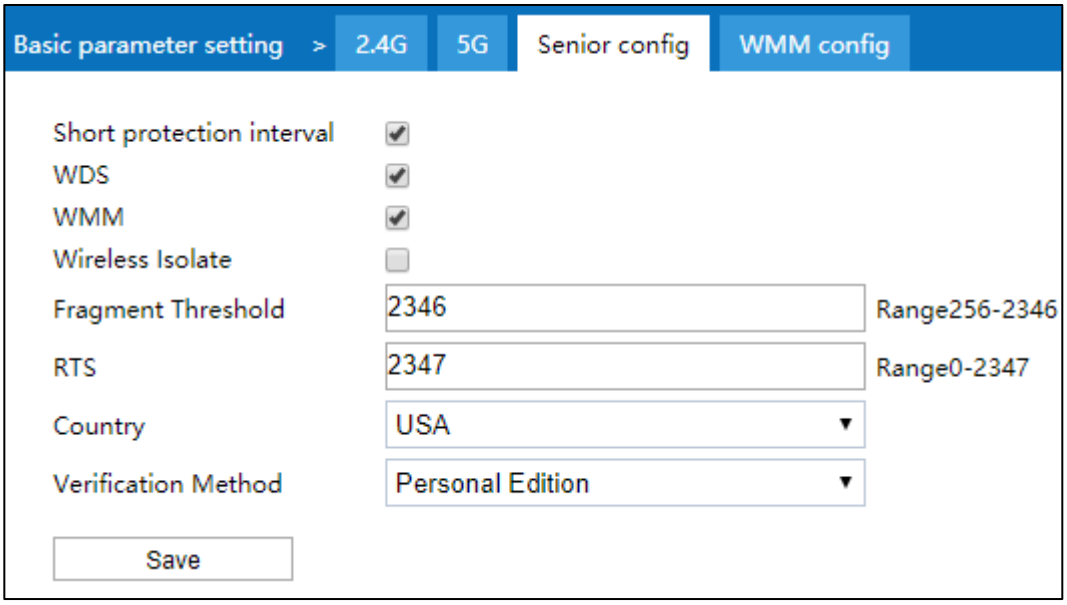
Interface Element	Description
	• 104: main frequency band 5520MHz, frequency range 5510~5530MHz, this frequency band is not open in China, so it's temporarily unavailable; • 108: main frequency band 5540MHz, frequency range 5530~5550MHz, this frequency band is not open in China, so it's temporarily unavailable; • 112: main frequency band 5560MHz, frequency range 5550~5570MHz, this frequency band is not open in China, so it's temporarily unavailable; • 116: main frequency band 5580MHz, frequency range 5570~5590MHz, this frequency band is not open in China, so it's temporarily unavailable; • 120: main frequency band 5600MHz, frequency range 5590~5610MHz, this frequency band is not open in China, so it's temporarily unavailable; • 124: main frequency band 5620MHz, frequency range 5610~5630MHz, this frequency band is not open in China, so it's temporarily unavailable; • 128: main frequency band 5640MHz, frequency range 5630~5650MHz, this frequency band is not open in China, so it's temporarily unavailable; • 132: main frequency band 5660MHz, frequency range 5650~5670MHz, this frequency band is not open in China, so it's temporarily unavailable; • 136: main frequency band 5680MHz, frequency range 5670~5690MHz, this frequency band is not open in China, so it's temporarily unavailable; • 140: main frequency band 5700MHz, frequency range 5690~5710MHz, this frequency band is not open in China, so it's temporarily unavailable; • 144: main frequency band 5720MHz, frequency range 5710~5730MHz, this frequency band is not open in China, so it's temporarily unavailable; • 149: main frequency band 5745MHz, frequency range 5735~5755MHz; • 153: main frequency band 5765MHz，frequency range 5755~5775MHz. • 157: main frequency band 5785MHz，frequency range 5775~5795MHz. • 161: main frequency band 5805MHz，frequency range

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	5795~5815MHz. • 165: main frequency band 5825MHz，frequency range 5815~5835MHz. Note: • In order to improve the network performance, please choose unused channel in the device working environment. • Different country opens different channels.
Bandwidth	Channel bandwidth of wireless network, it defaults to 80MHz, options as follows: • 20MHz； • 40MHz； • 80MHz。
Transmitting power	Transmitted power of the device wireless signal, defaults to 23dBm, value range 1~30dBm. Note: • The larger the transmitting power is, the stronger the transmitting ability is and the farther the transmission distance is. • Different device has different transmitting power range.
Max number of users	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.

Interface Description 3: Senior Configuration

The advanced configuration interface as follows:



Copyright © 3onedata Co., Ltd.

The main element configuration description of advanced interface:

Interface Element	Description
Short protection interval	Short GI (Short Guard Interval) checkbox: • Check: enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed. • Uncheck: after disabling the function, the transmission interval of data packet defaults to 800ns. Note: Under high signal strength and low latency, this function can be enabled to improve nearly 10% handling capacity.
WDS	WDS (Wireless Distribution System), this function is used for bridging multiple WLAN. Note: Please enable WDS function while bridging the device and other wireless devices.
WMM	WMM (WiFi Multimedia) function, defaults to enabled. Note: After enabling WMM function, the device can process the data packet with priority level, improving the data transmission performance of WMM and ensuring the service quality of voice, video and other services with high real-time requirements.
Wireless isolate	Wireless user isolation, it's used for isolating the wireless clients connected to the device wireless network with same SSID, defaults to disabled. Note: After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.
Fragment threshold	Fragment threshold of data packet, value range 256-2346, defaults to 2346. Note: • The data frame will be segmented when its length surpasses fragment threshold. • With large interference or high utilization ratio of wireless network, user can adopt smaller fragmentation threshold to increase the transmission reliability; but it is low efficiency. • The wireless network is easy to be interfered while adopting large fragment threshold; but it is high efficiency.
RTS	Data packet RTS (Request to Send) threshold, value range 0-2347, defaults to 2347. • RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will send RTS signal;

Copyright © 3onedata Co., Ltd.

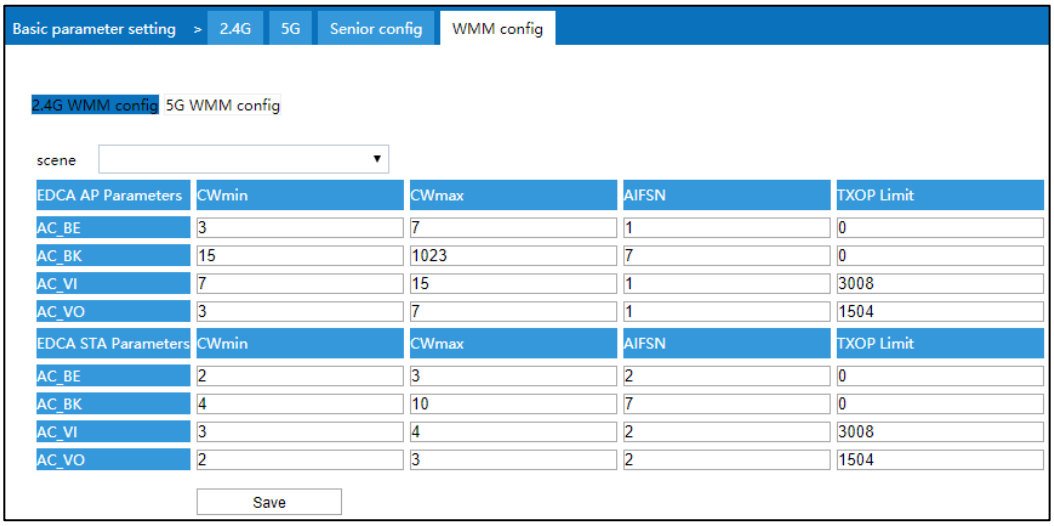
Interface Element	Description
	• 0 < RTS threshold < 2347: when the length of data packet surpasses RTS threshold, the device wireless terminal will send RTS signal to avoid signal conflict; • RTS threshold = 2347: the device wireless terminal won't send RTS signal. Note: • As for the wireless nodes 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. Options are as follows: • China • USA Note: Different country opens different channels.
Authentication method	Authentication mode of wireless network, options as follows: • Personal edition: wireless network WPA/WPA2 uses WPA-PSK / WPA2-PSK encryption method and pre-shared key. Personal edition is suitable for personal and home users. • Enterprise edition: wireless network WPA/WPA2 uses WPA-802.1X/WPA2-802.1X encryption method. It is necessary to install Radius server to authenticate, and suitable for enterprise users with high security requirements.
Radius Server IP	IP address of RADIUS(Remote Authentication Dial In User Service) sever. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.
Radius Server port	The authentication port number of the RADIUS server,value range is 0-65535. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.
RADIUS Shared key	Shared key of RADIUS server. Note: The item will display as an text input box when the wireless network authentication method is enterprise edition.

Copyright © 3onedata Co., Ltd.

Interface Description 4: WMM Configuration

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

WMM configuration interface is as follows:



Main elements configuration description of WMM configuration interface:

Interface Element	Description
WMM Configuration Tab	• 2.4G WMM Configuration • 5G WMM Configuration
Scene	WMM scene settings, options: • No priority; • Multimedia First; • User-defined. Note: • The default scenario is no priority. At this time, data stream and video voice stream have the same priority, and no one has the priority. • After selecting WMM function, the device can process the data packet with priority level, improving the data transmission

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	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: 1-255.
TXOP Limit	Transmission Opportunity Limit The maximum length of time the user can occupy the channel after a successful competition The larger this value is, the longer the user can occupy the channel at a time. If it is 0, only one message can be sent after occupying the channel at a time. The value of this parameter must be positive and modification is not recommended.
EDCA STA Parameters	The EDCA(Enhanced Distributed Channel Access) parameters of terminal device(namely workstation STA) supporting 802.11 standard, such as CWmin, CWmax, AIFSN, TXOP Limit.

4.2 Wireless Client Filtering

Function Description

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

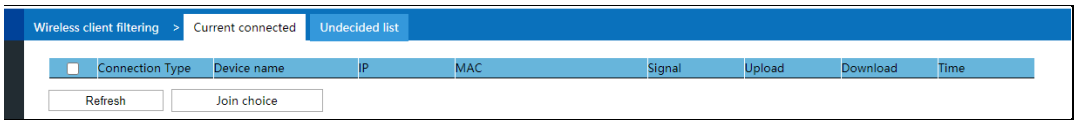
Copyright © 3onedata Co., Ltd.

Operation Path

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

Interface Description 1: Current

The interface of the current connected device is as follows:

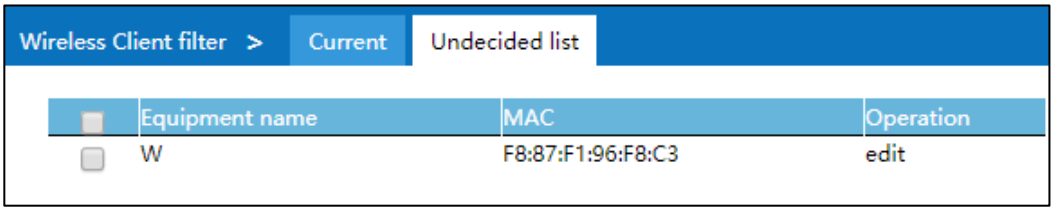


Configuration of the main elements of the current connected device interface:

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

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

Undecided list interface as follows:



Copyright © 3onedata Co., Ltd.

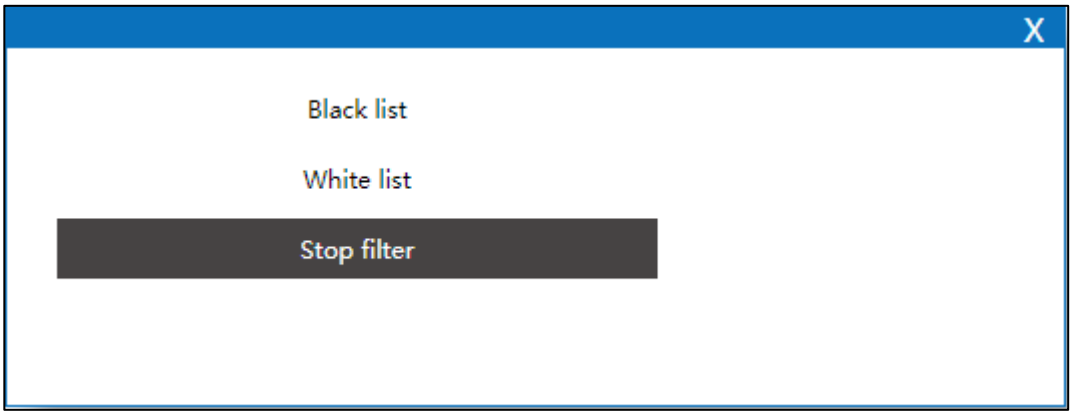
The main element configuration description of undecided list interface:

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

Interface Description 3: Filter Rule

Click the “Filter Rule” button to switch lists.

The filter rule interface as follows:



The main element configuration description of filter rules interface:

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

Note

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

Copyright © 3onedata Co., Ltd.

5 Advanced Network

5.1 Port Forward

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

Function Description

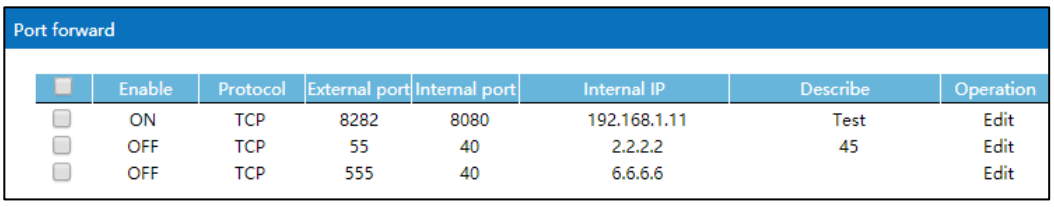
On the “Port Forward” page, user can check or add port forward entry. It allows outer network client to visit specified device via specified port.

Operation Path

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

Interface Description

The port forwarding interface as follows:



The main element configuration description of port forward interface:

Interface Element	Description
All	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
Describe	Remarks of port forward entries.
Operation	Edit: modify port forwarding entry information
Add	Click the “Add” button to add new port forwarding entry in the pop-up window of “Port Forwarding”.
Delete select	Check the port forwarding information that needs to be deleted, then click “delete” button to delete it.

5.2 Port Redirection

Function Description

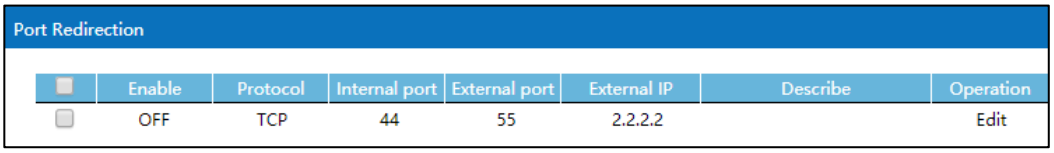
On the “Port Redirection” page, user can check or add port redirection entry, which allows client in LAN to visit the specified port of device with IP address specified by external network via specified port.

Operation Path

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

Interface Description

The port redirection interface as follows:



The main element configuration description of port redirection interface:

Interface Element	Description
All	The checkbox of port redirection entry. Click “All” to check all port redirection entries

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Enabled	Enable port redirection or not: • 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
Describe	The remark information of port redirection entry
Operation	Edit: modify port redirection entry information
Add	Click the “add” button at the top right corner to add new port redirection in the pop-up window of “Port Redirection”
Delete select	Check the port redirection information that needs to be deleted, then click “delete” button at the top right corner to delete it

5.3 DMZ Settings

DMZ(Demilitarized Zone） is a 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.

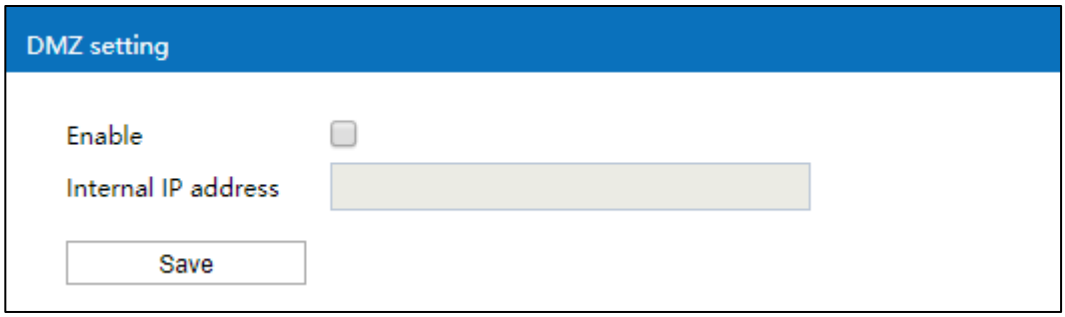
Operation Path

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

Interface Description

DMZ setting interface as follows:

Copyright © 3onedata Co., Ltd.



The main element configuration description of DMZ setting interface:

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

5.4 UPnP Settings

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

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

Function Description

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

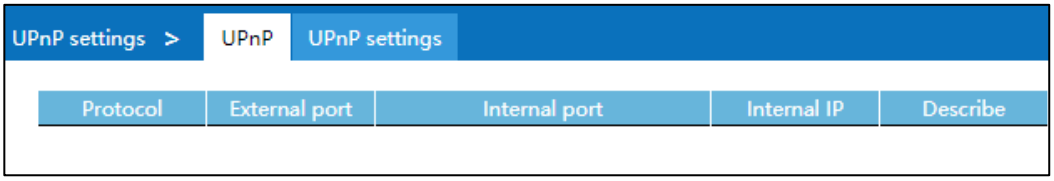
Operation Path

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

Copyright © 3onedata Co., Ltd.

Interface Description 1: UPnP

UPnP settings interface as follows:

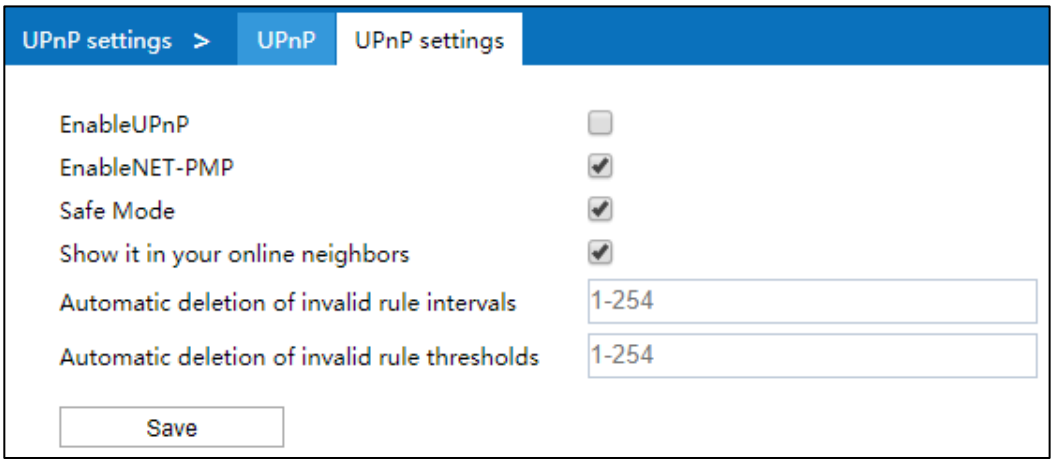


The main elements configuration description of UPnP settings interface:

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

Interface description 2: UPnP settings

UPnP settings interface as follows:



The main element configuration description of UPnP settings interface:

Interface Element	Description
Enable UPnP	UPnP enable checkbox, check to enable UPnP function.
Enable NAT-PMP	The NAT-PMP function enable checkbox, check to enable

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	NAT-PMP function, and the router will allow the NAT 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.

5.5 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

Copyright © 3onedata Co., Ltd.

communicate with other networks via the virtual router. If the Master router in backup team breaks down, Backup router will elect a new Master router via election strategy and provide router service for hosts in the network. Therefore, hosts in the network can uninterruptedly communicate with outside network.

Principle of realization

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

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

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

Function Description

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

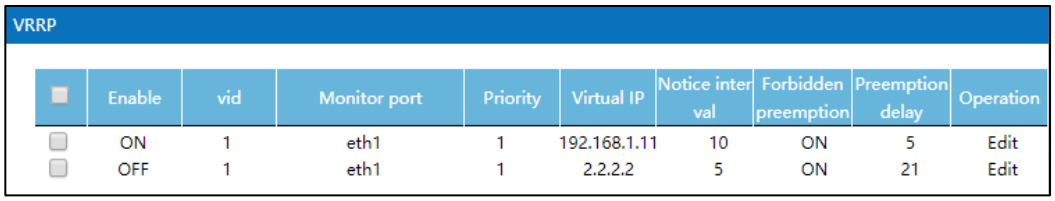
Copyright © 3onedata Co., Ltd.

Operation Path

Open in order: "Advanced Network > VRRP".

Interface Description

VRRP interface as below:



The main elements configuration description of VRRP interface:

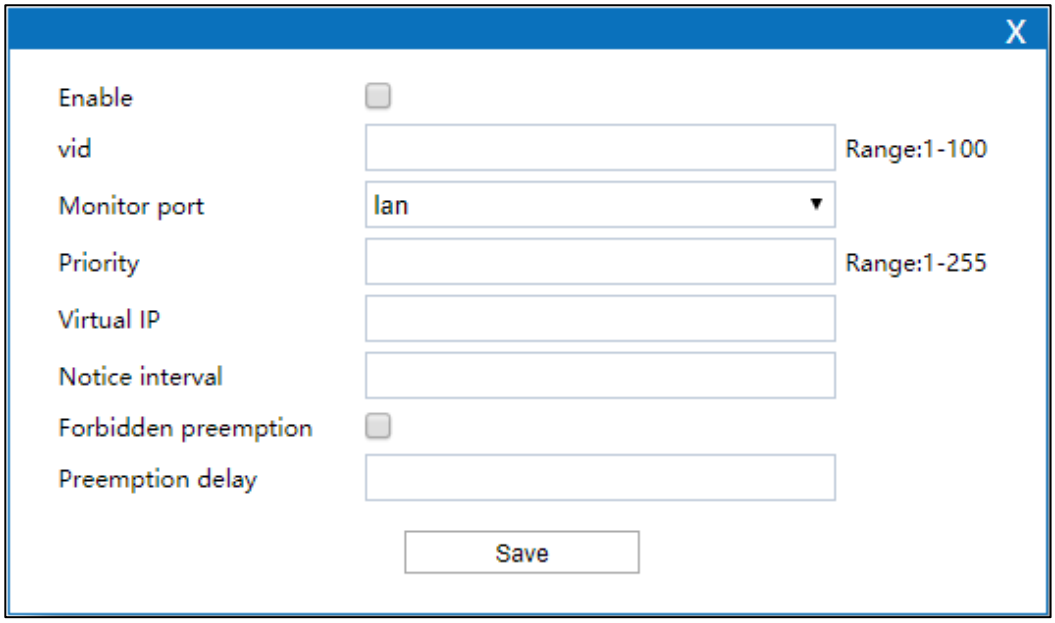
Interface Element	Description
Enabled	VRRP function status is displayed, options include: • ON • OFF
Vid	Identity of the virtual router is displayed.
Monitor port	Monitor ports of the device is displayed, options include: • Br-lan • Eth1
Virtual IP	The IP address of the virtual router is displayed.
Notice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

Interface Description: VRRP-Add

Click the "Add" button to add virtual route.

The VRRP-Add interface as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of VRRP-Add interface:

Interface Element	Description
Enabled	VRRP enablement switch, click the right button for ON and OFF switching.
Vid	Identity of the virtual router, the valid range is 1-100. Virtual routers consisting of one master device and multiple backup devices have the same identity.
Monitor port	Drop-down list of VRRP monitor port, options as follows: • lan: LAN port as the monitor port; • wan: WAN port as the monitor port.
Priority	Priority of the device. The priority is used for the election of Master device. The greater the value, the higher the priority. The more likely it is to become Master device; the valid range is 1-255.
Virtual IP	IP address of the virtual router, such as 192.168.1.1. A virtual router can have one or more IP addresses.
Notice interval	Annunciate time interval, valid range is 1-10 seconds. Master device periodically sends VRRP notice messages to announce its operating status.
Forbidden preemption	VRRP enablement switch, click the right button for ON and OFF switching. • ON: 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;

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	• OFF: Preemptive mode. When the priority of Backup device is higher than the one of Master device, Backup device will actively switch to Master device.
Delay of Preemption delay	The delay time of switching from Backup device to Master device, the valid range is 1-1000 seconds. Note: If the preemption delay time is too short, the device status will be frequently switched; so increasing the preemption delay time can effectively solve this problem.

5.6 RIP

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

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

Function Description

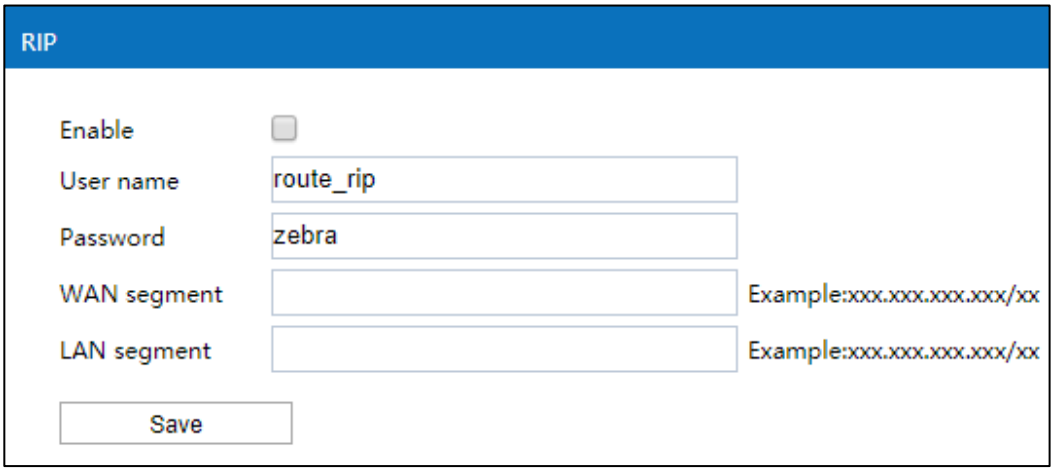
On the page of "RIP", user can configure the RI related parameters.

Operation Path

Open in order: "Advanced Network > RIP".

Interface Description

The RIP interface as follows:



The main elements configuration description of RIP interface:

Copyright © 3onedata Co., Ltd.

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

5.7 OSPF

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

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

Function Description

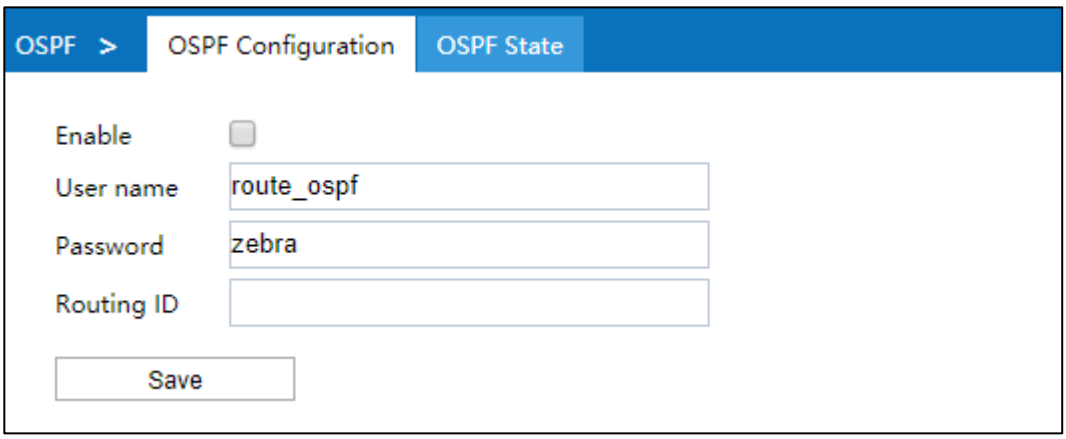
On the page of "OSPF", user can configure the OSPF parameters.

Operation Path

Open in order: "Advanced Network > OSPF".

Interface Description 1: OSPF Configuration

OSPF configuration interface is as follows:



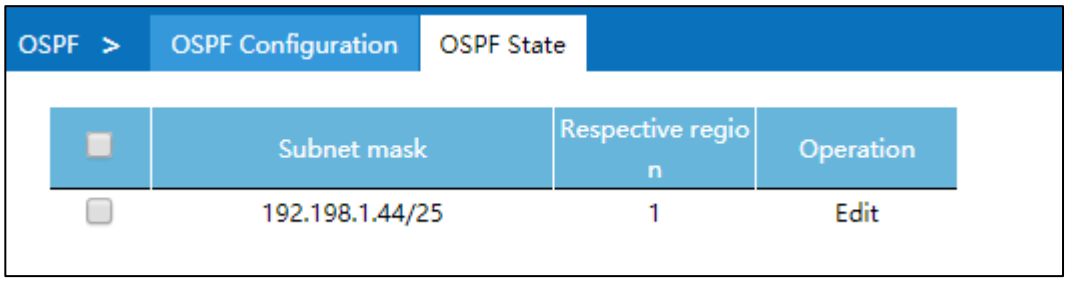
Copyright © 3onedata Co., Ltd.

Main elements configuration description of OSPF configuration interface:

Interface Element	Description
Enabled	OSPF enablement switch, click the right button for ON and OFF switching. • ON: Enable OSPF default configuration; • OFF.
User name	User name used to log in to the OSPF command line configuration.
Password	Password used to log in to the OSPF command line configuration.
Routing ID	The router ID number, similar to the IP address format, is the unique identification of router in the autonomous system.

Interface Description 2: OSPF State

OSPF State interface as follow:



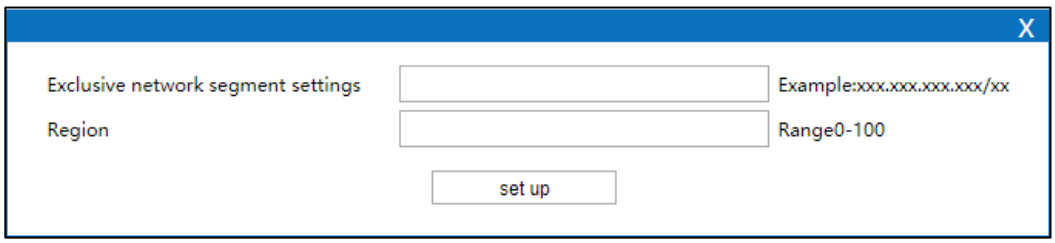
The main elements configuration description of OSPF State interface:

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

Interface Description 3: OSPF State-Add

The OSPF State-Add interface as follows:

Copyright © 3onedata Co., Ltd.



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.

5.8 Static DHCP

Function Description

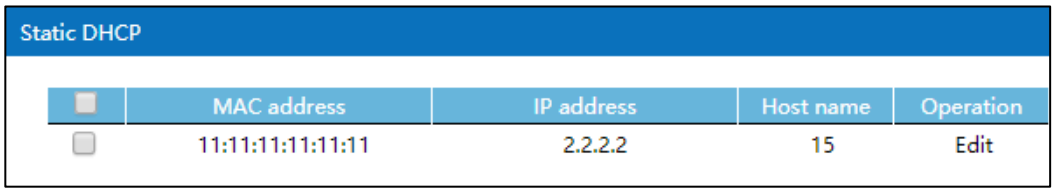
On the page of "Static DHCP", user can add, delete, and view the configuration information of static clients. Bind the client's MAC address to the specified IP address to ensure that the address that the client obtains from the server each time is the binding IP address.

Operation Path

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

Interface Description

Static DHCP interface as follows:



The main elements configuration description of static DHCP interface:

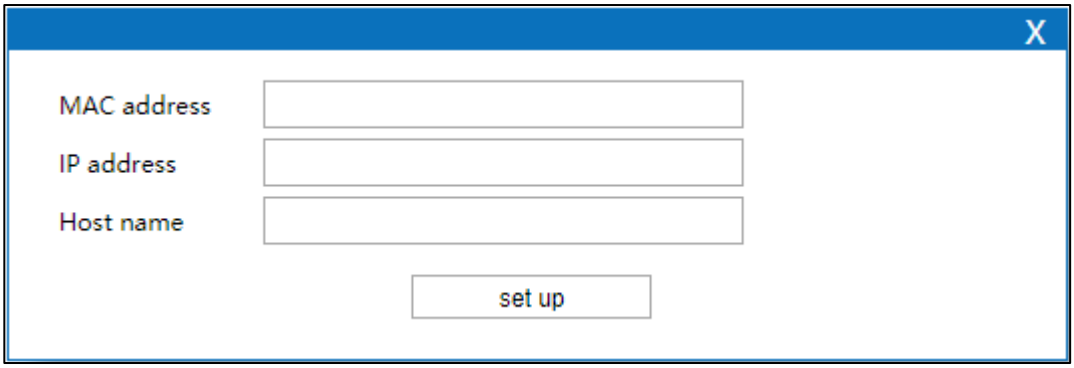
Interface Element	Description
MAC Address	MAC address of DHCP client.
IP Address	IP address bound to the MAC address of DHCP client.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Host name	The name of DHCP client.
Operation	Edit the static DHCP list.

Interface Description: Static DHCP - Add

Static DHCP-Add interface as follows:



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

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

5.9 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.

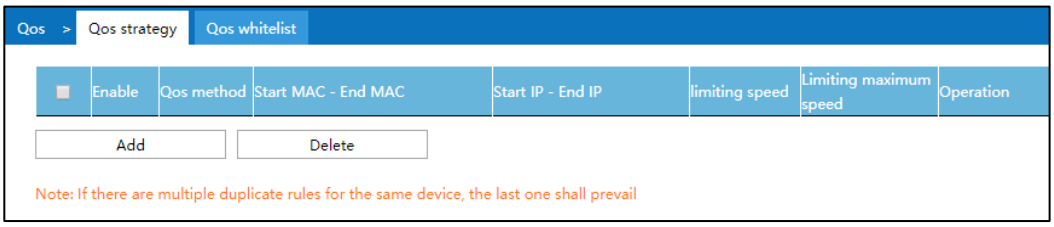
Operation Path

Open in order: "Network Settings > QoS".

Interface Description 1:QoS strategy

The QoS Strategy interface as follows:

Copyright © 3onedata Co., Ltd.

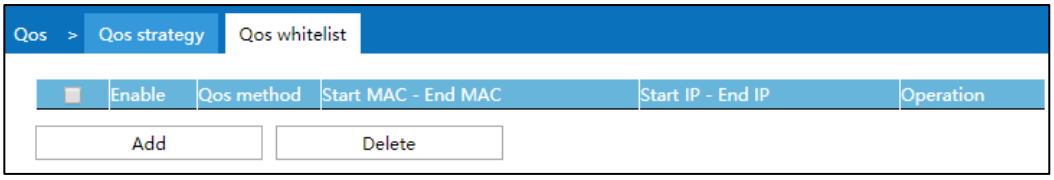


The main element configuration description of QoS strategy interface:

Interface Element	Description
Enable	Enable QoS strategy or not.
QoS method	The method of enabling QoS strategy, available values: • IP-based speed limit; • MAC-based speed limit.
Start MAC-End MAC	The range of the speed limit from the start MAC address to the end MAC address.
Start IP-End IP	The range of the speed limit from the start IP address to the end IP address.
Limiting Speed	The limited average rate value.
Limiting maximum speed	The maximum limited rate value,
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 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; • MAC whitelist.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Start MAC-End MAC	The range of starting and ending MAC addresses that are not affected by QoS strategy.
Start IP-End IP	The range of starting IP addresses to ending IP ddresses 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.

Copyright © 3onedata Co., Ltd.

6 Firewall

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

6.1 IP Filter

Function Description

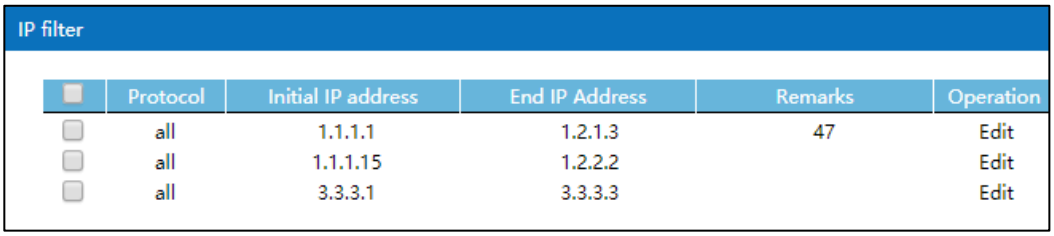
On the "IP filter" page of firewall, user can check or add IP filter to forbid the communication between the clients in LAN and WAN.

Operation Path

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

Interface Description

IP filter interface as follows:



The main element configuration description of IP filter interface:

Interface Element	Description
All	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

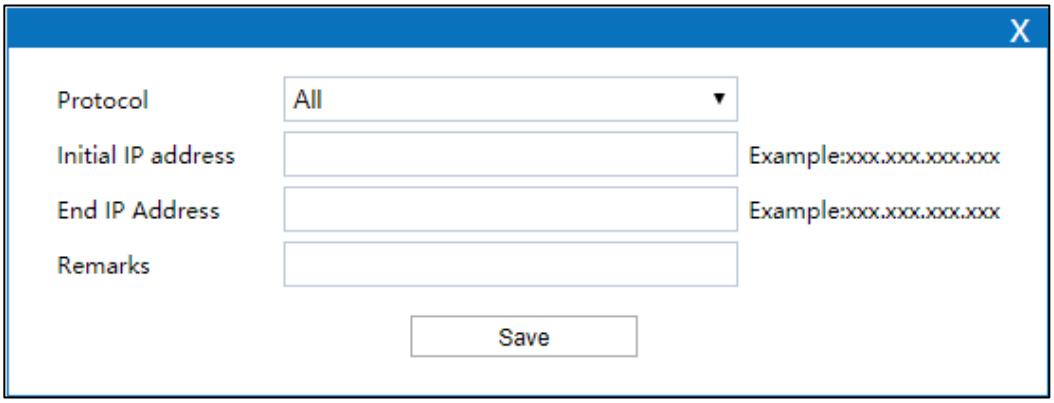
Copyright © 3onedata Co., Ltd.

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

Interface Description: Add IP Filter Entry

Click "Add" to increase IP filter entry.

The Add interface as follows:



The main elements configuration description of Add interface:

Interface Element	Description
Protocol	Drop-down list of data packet protocol, options as follows: • ALL； • TCP； • UDP。
Initial IP Address	Start IP address of LAN IP address range filtered by the device, such as: 192.168.1.123.
End IP Address	End IP address of LAN IP address range filtered by the device, such as: 192.168.1.123.
Remarks	Remarks of IP filter list support 10 Chinese characters or 32 valid characters, optional.

Copyright © 3onedata Co., Ltd.

6.2 MAC Filter

Function Description

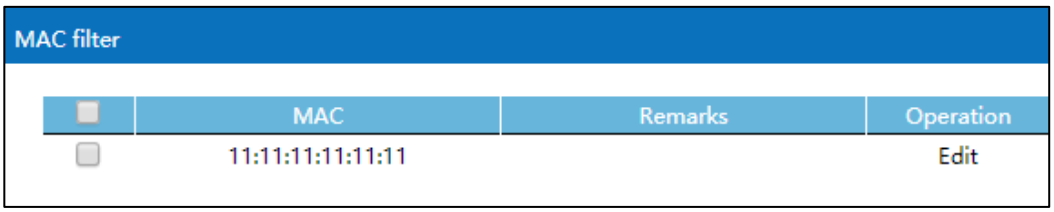
On the "MAC filter" page of firewall, user can check or add MAC filter to forbid the communication between the clients in LAN and WAN; it can effectively control the WAN access rights of user in LAN.

Operation Path

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

Interface Description

MAC filter interface as follows:



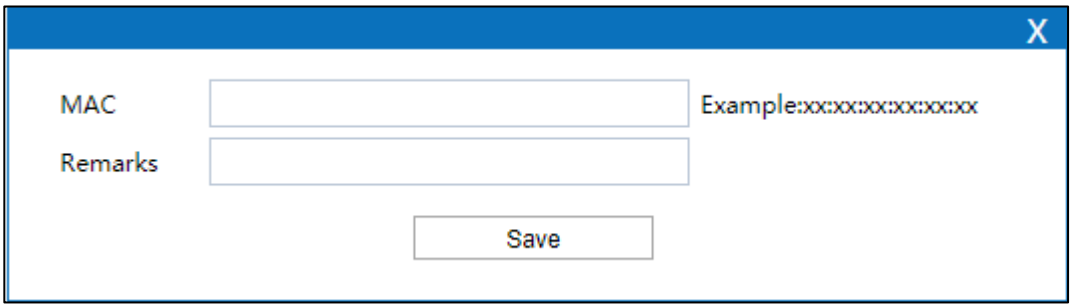
The main element configuration description of MAC filter interface:

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

Interface Description: Add MAC Filter Entry

Click "Add" to increase MAC filter entry.

The Add interface as follows:



The main elements configuration description of Add interface:

Copyright © 3onedata Co., Ltd.

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

6.3 URL Filter

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

Function Description

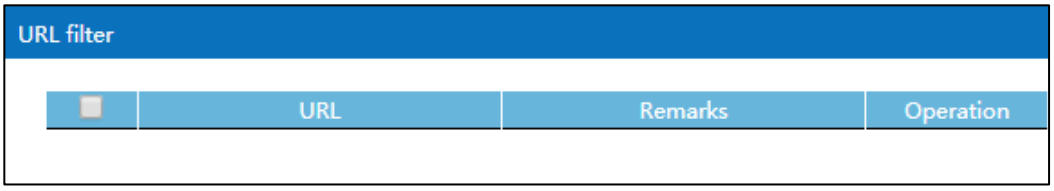
On the "URL filter" page of firewall, user can check or add URL filter to prohibit the client in LAN from accessing URL address in WAN and prevent user from accessing some of the websites.

Operation Path

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

Interface Description

URL filter interface as follows:



The main element configuration description of URL filter interface:

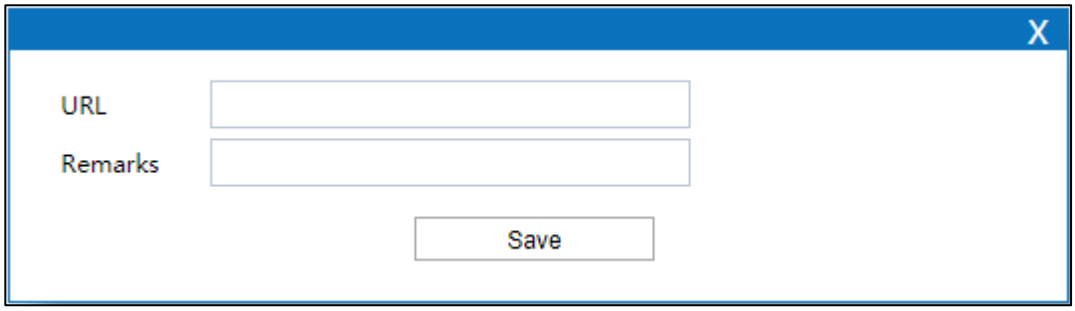
Interface Element	Description
All	URL filter check box, click to check all URL filter entries.
URL	URL address in LAN filtered by the device.
Remarks	Remarks for URL filter entries.
Operation	Edit: modify the filter list.

Copyright © 3onedata Co., Ltd.

Interface Description: Add URL Filter List

Click "Add" to increase URL filter list.

URL filter interface as follows:



The main element configuration description of URL filter interface:

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

6.4 Keyword Filter

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

Function Description

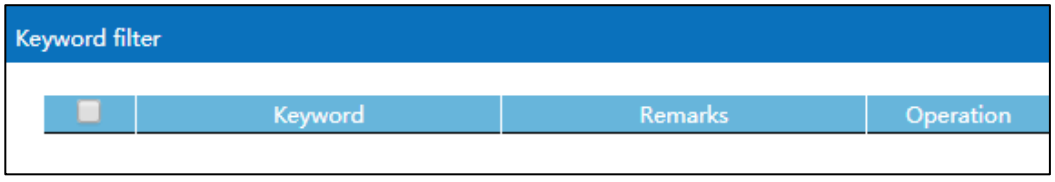
On the page of "Keyword filter" of the firewall, user can view or add keyword filtering entries to prevent clients on the LAN from accessing to the network address corresponding to the keywords in the WAN.

Operation Path

Open in order: "Firewall > Keyword Filter".

Interface Description

Keyword filter interface as follows:



Copyright © 3onedata Co., Ltd.

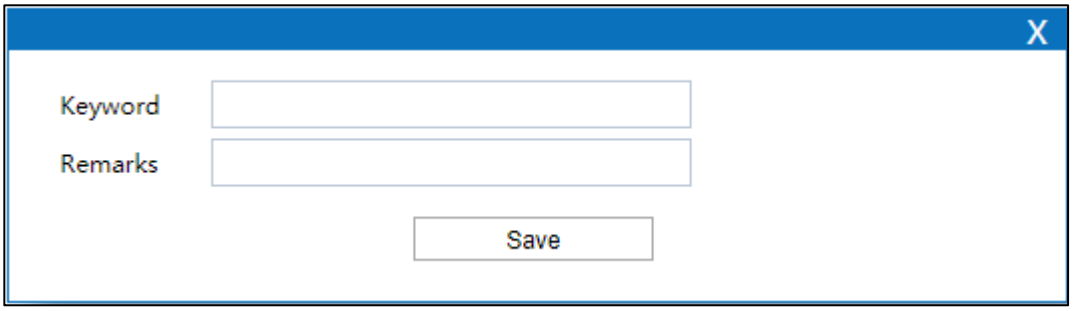
The main elements configuration description of keyword filter interface:

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 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 10 Chinese characters or 32 valid characters, and can be left blank.

Copyright © 3onedata Co., Ltd.

7 VPN Tunnel

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

7.1 GRE Settings

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

Function Description

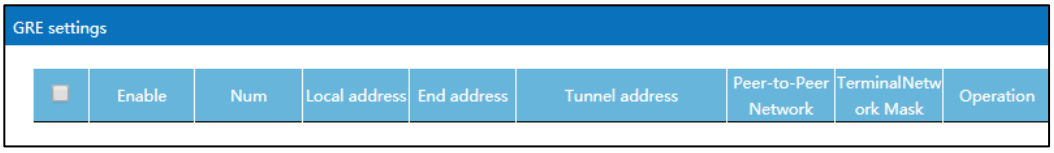
On the page of "GRE Settings", user can configure the relevant parameters of GRE.

Operation Path

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

Interface Description

GRE settings interface as follows:



The main elements configuration description of GRE settings interface:

Interface Element	Description
All	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.
End 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 select	User can select the GRE settings information that needs to be deleted, and then click the “Delete Select” button in the upper right corner to delete the GRE settings.

7.2 PPTP Client Settings

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

Function Description

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

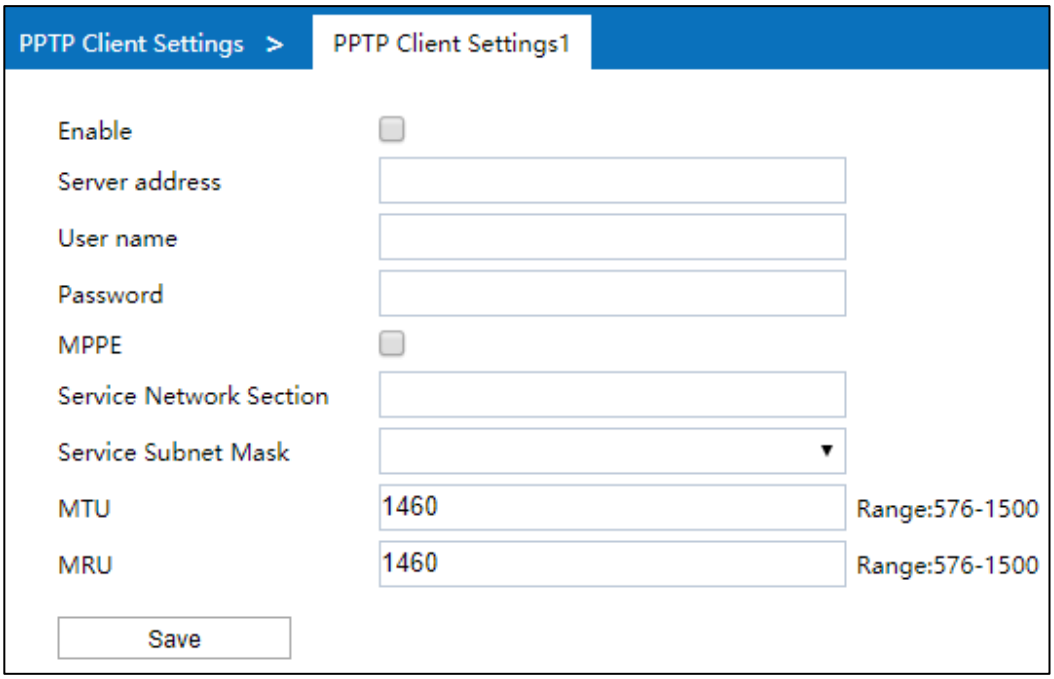
Operation Path

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

Interface Description

The PPTP client settings interface is as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of PPTP client settings interface:

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

Copyright © 3onedata Co., Ltd.

7.3 PPTP Server Settings

Function Description

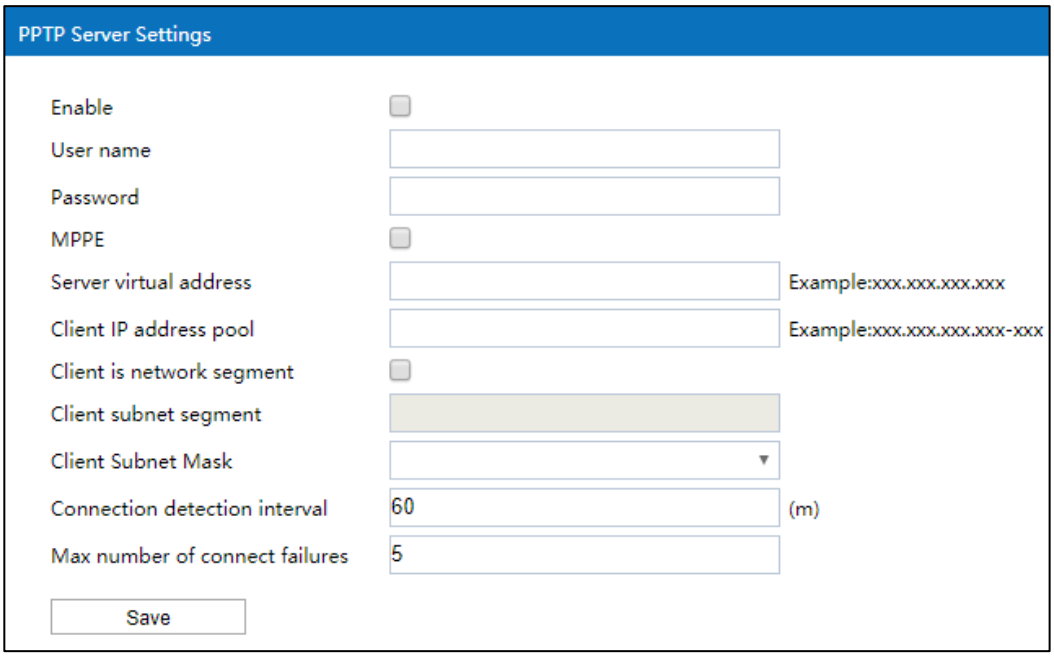
On the page of "PPTP Server Settings", user can configure the parameters related to PPTP server.

Operation Path

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

Interface Description

The PPTP server settings interface is as follows:



The main elements configuration description of PPTP server settings interface:

Interface Element	Description
Enable	PPTP Server Settings enable checkbox, check to enable the PPTP server settings function;
User name	User name provided by PPTP to the client for connection.
Password	Password corresponding to the user name provided by PPTP to the client for connection
MPPE	Functional enablement checkbox of MPPE (Microsoft Point-to-Point Encryption) , click to enable MPPE encryption function.
Server virtual address	Virtual IP address of PPTP server.
Client IP address pool	IP address pool range assigned to the client, the format is: xxx.xxx.xxx.xxx-xxx.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
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.

7.4 L2TP Client Settings

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

Function Description

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

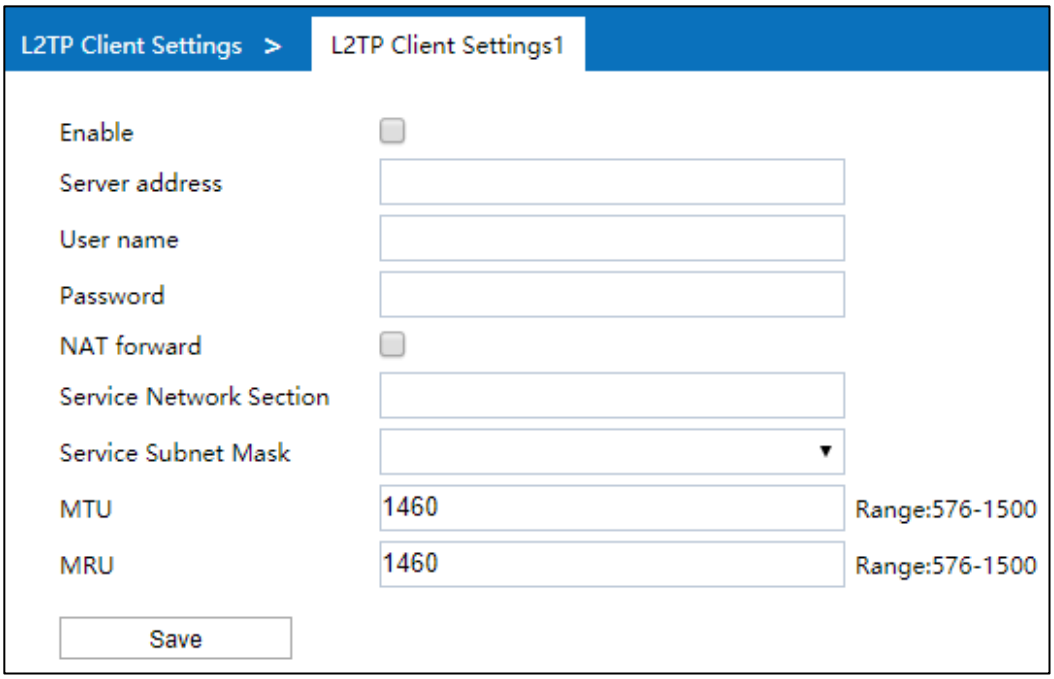
Operation Path

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

Copyright © 3onedata Co., Ltd.

Interface Description

The L2TP client settings interface is as follows:



The main elements configuration description of L2TP client settings interface:

Interface Element	Description
Enable	L2TP Client Settings enable checkbox, check to enable the L2TP client settings function.
Server Address	IP address of L2TP server
User name	User name allowed by L2TP server.
Password	Password corresponding to the user name allowed by L2TP server.
NAT forward	Enablement checkbox of NAT(Network Address Translation), check to enable NAT forwarding. All data flows of client are forwarded through the VPN server.
Service Network Section	User name provided by L2TP to the client for connection
Service Subnet Mask	Password corresponding to the user name provided by L2TP to the client for connection
MTU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the recommended value range is 1400-1500.
MRU	Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the recommended

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	value range is 1400-1500.

7.5 L2TP Server Settings

Function Description

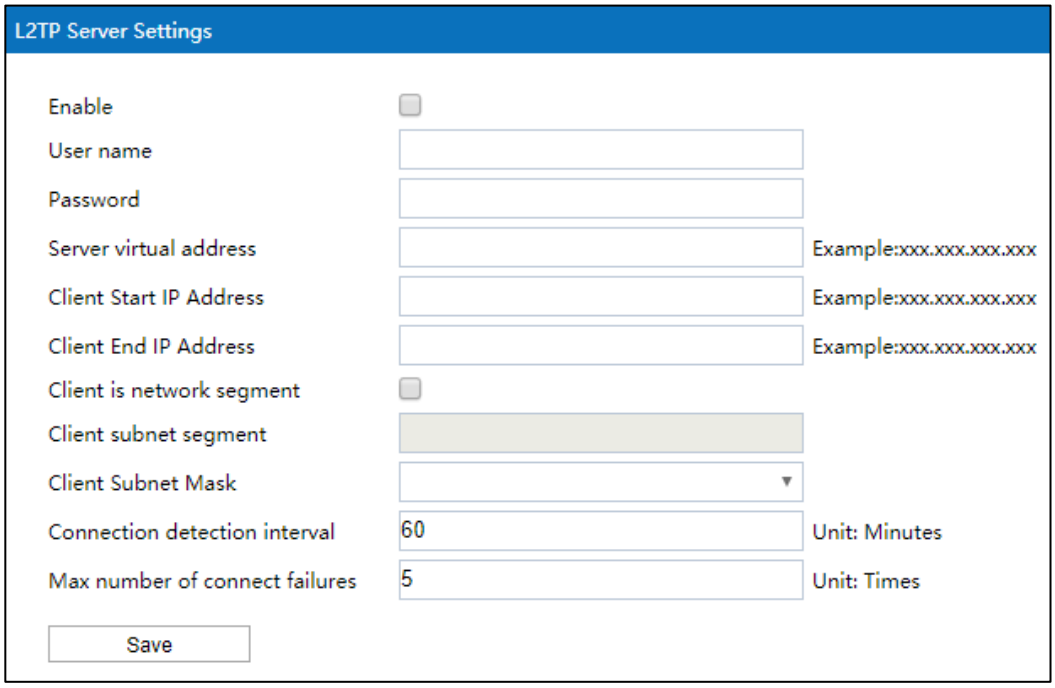
On the page of "L2TP Server Settings", user can configure the parameters related to L2TP server.

Operation Path

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

Interface Description

The L2TP server settings interface is as follows:



The main elements configuration description of L2TP server settings interface:

Interface Element	Description
Enable	L2TP Server Settings enable checkbox, check to enable the L2TP server settings function;
User name	User name provided by L2TP to the client for connection
Password	Password corresponding to the user name provided by L2TP to the client for connection
Server virtual address	Virtual IP address of L2TP server

Copyright © 3onedata Co., Ltd.

Interface Element	Description
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" enblement checkbox. It allows the router whose subnet is the network segment to connect as a client and access the L2TP VPN server.Click to enable the function of the client as network segment.After enabled, the subnet segment and mask of the client can be input.
Client subnet segment	Set the network segment that allows the client to access, and use it with the client as the network segment. Note: This input box can only be entered after enabling the function of client as the network segment.
Client Subnet Mask	Drop-down box of subnet mask of the L2TP client. Note: This input box can only be entered after enabling the function of client as the network segment.
Connection detection interval	Detect the interval of connection, the default value is 60, unit: second.
Max number of connect failures	Detect the maximum number of failed connections. The default value is 5.

7.6 IPsec

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

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

Copyright © 3onedata Co., Ltd.

Function Description

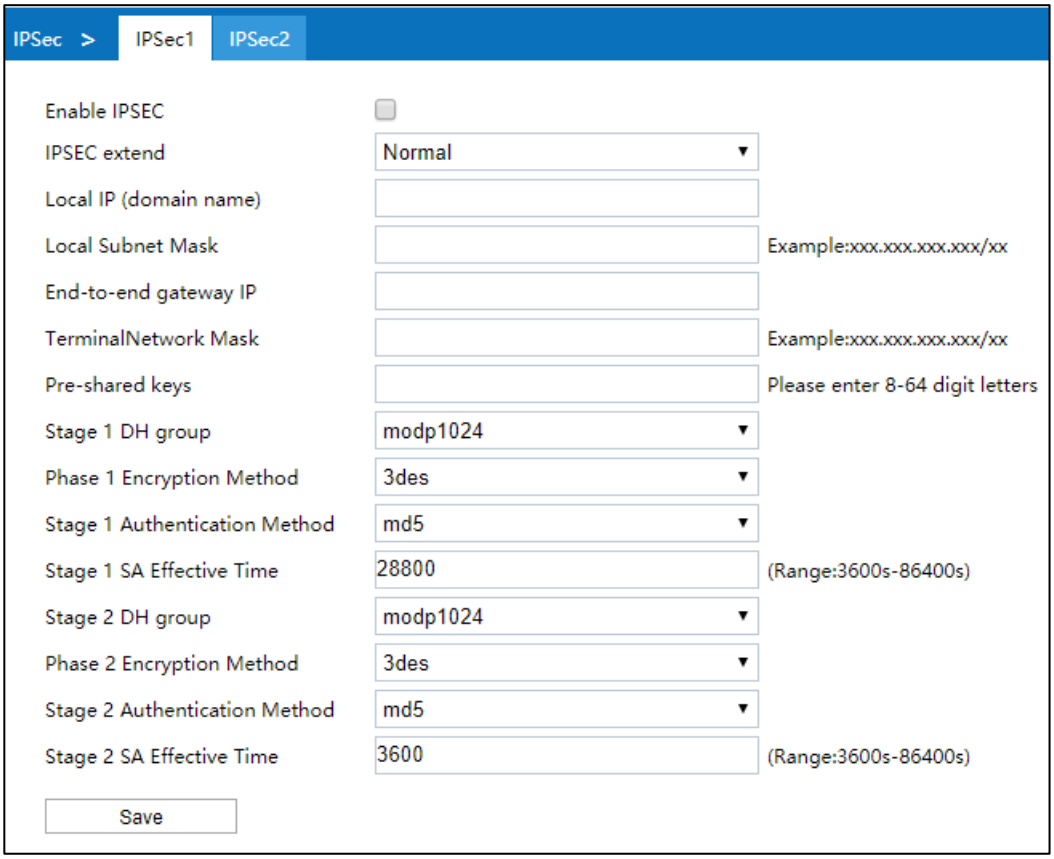
On the page of "IPsec", user can configure the relevant parameters of IPsec.

Operation Path

Open in order: "VPN tunnel > IPsec".

Interface Description

IPsec settings interface as follows:



The main elements configuration description of IPsec settings interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Local Subnet Mask	The local subnet and mask of the router, for example: 192.168.4.0/24.
End-to-End gateway IP	External network port IP of the opposite end
Terminal Network Mask	Protected subnet and subnet mask of the opposite IPsec end , for example: 192.168.4.0/24.
Pre-shared keys	Unicode string that verifies the IPsec connection.
Stage 1 DH group	Stage 1 DH exchange algorithm, options as follows: • modp768 • modp1024 • modp1536
Phase 1 Encryption Method	Phase 1 encryption algorithm, options as follows: • 3des • aes128 • aes192 • aes512
Stage 1 Authentication Method	Stage 1 Authentication Method, options as follows: • md5 • sha • sha256 • sha384 • sha512
Stage 1 SA Effective Time	Stage 1 SA survival time, unit is second and default is 28800.
Stage 2 DH group	Stage 2 DH exchange algorithm, options as follows: • modp768 • modp1024 • modp1536
Phase 2 Encryption Method	Phase 2 encryption algorithm, options as follows: • 3des • aes128 • aes192 • aes512
Stage 2 Authentication Method	Stage 2 Authentication Method, options as follows: • md5 • sha • sha256 • sha384 • sha512
Stage 2 SA Effective	Stage 2 SA survival time, unit is second and default is

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Time	3600.

Copyright © 3onedata Co., Ltd.

8 System Management

8.1 Time Setting

Function Description

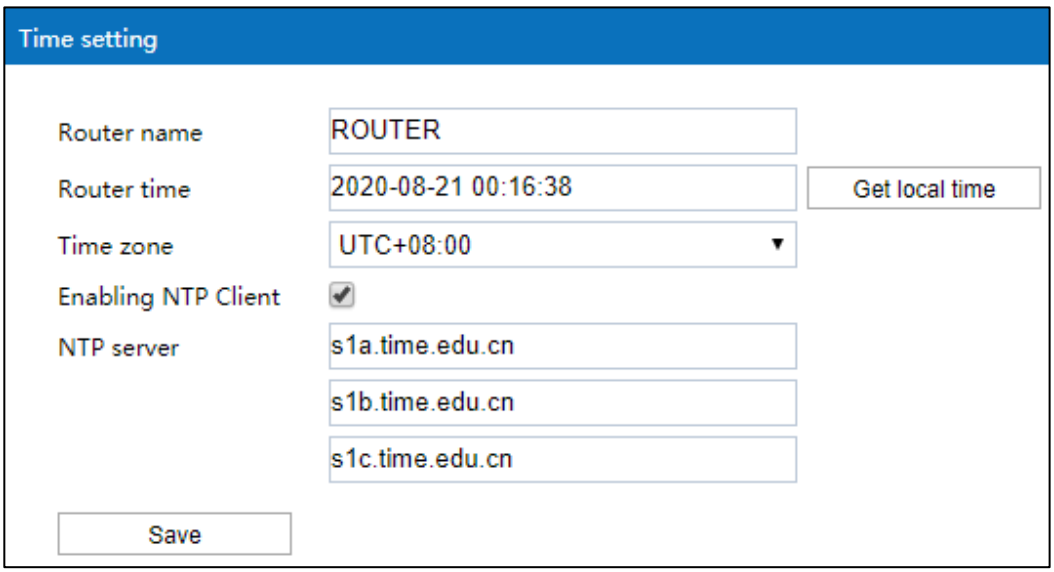
On the page of "Time Setting", user can configure time-related parameters information.

Operation Path

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

Interface Description

Time setting interface as follows:



The main elements configuration description of time settings interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Get local time	Click the button of Get local time to synchronize the local time with the router.
Time Zone	Drop-down box of time zone, user can choose according to their demands.
Enabling NTP Client	NTP Client Settings enable checkbox, check to enable the NTP client function to synchronize the time of the server with the client.
NTP Server	The address of the server that needs to be synchronized. Note: When there are multiple candidate NTP clients, the default is the first one. The higher the order, the higher the priority.

8.2 Access Settings

Function Description

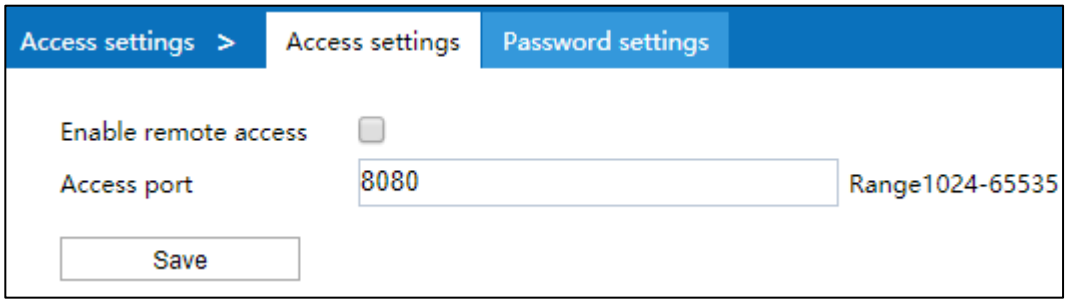
On the page of "Access settings", user can enable remote access and modify the username and password for accessing the device.

Operation Path

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

Interface Description 1: Access Settings

Access settings interface as follows:



The main elements configuration description of access settings interface:

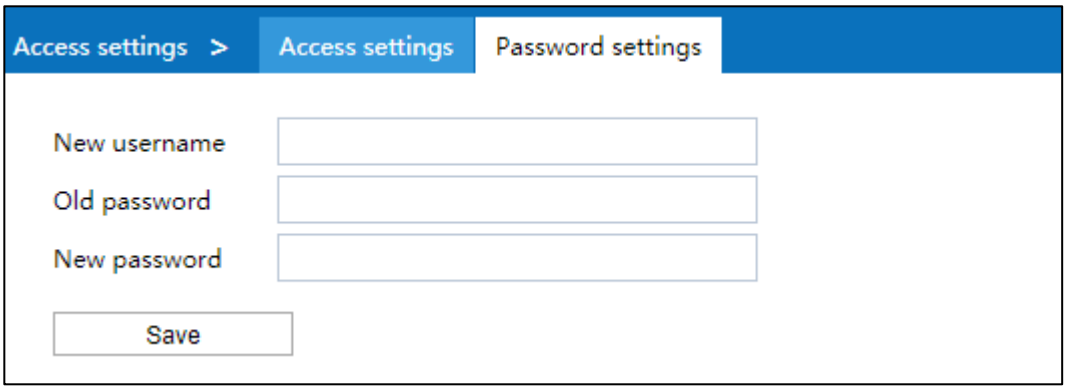
Interface Element	Description
Enable remote access	Remote access enable checkbox, check to enable remote access, the user can access the device through the HTTP/HTTPS protocol on the external network.
Access port	Port number of remote access, the port number defaults to 8080.

Copyright © 3onedata Co., Ltd.

Interface Element	Description
	Note: Ensure the consistency of access port when accessing the device through a browser.

Interface Description 2: Password Settings

Password settings interface as follows:



The main elements configuration description of password settings interface:

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

8.3 Timed Restart

Function Description

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

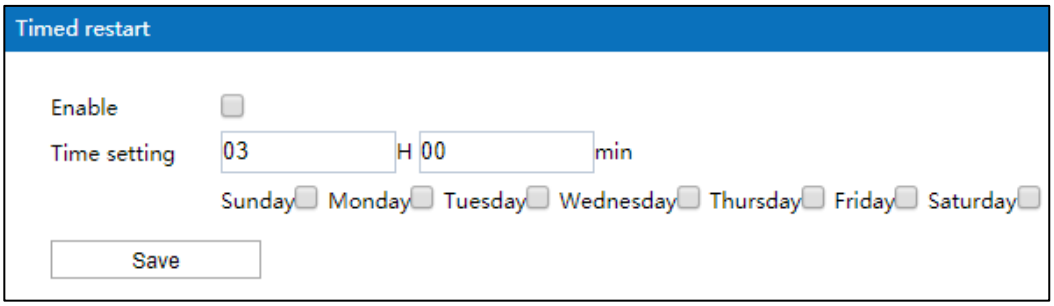
Operation Path

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

Copyright © 3onedata Co., Ltd.

Interface Description

The timed restart interface as follows:



The main elements configuration description of timed restart interface:

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

8.4 Backup Recovery

Function Description

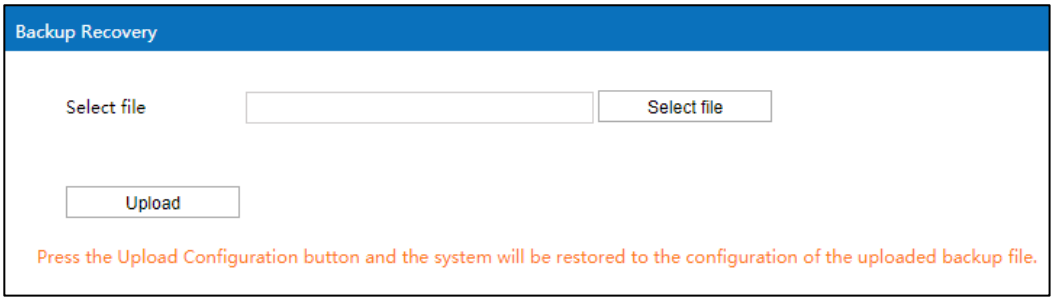
On the page of "Backup Recovery", user can select files for uploading configuration.

Operation Path

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

Interface Description

The backup recovery settings interface as follows:



The main elements configuration description of backup recovery settings interface:

Copyright © 3onedata Co., Ltd.

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

8.5 Log Manage

Function Description

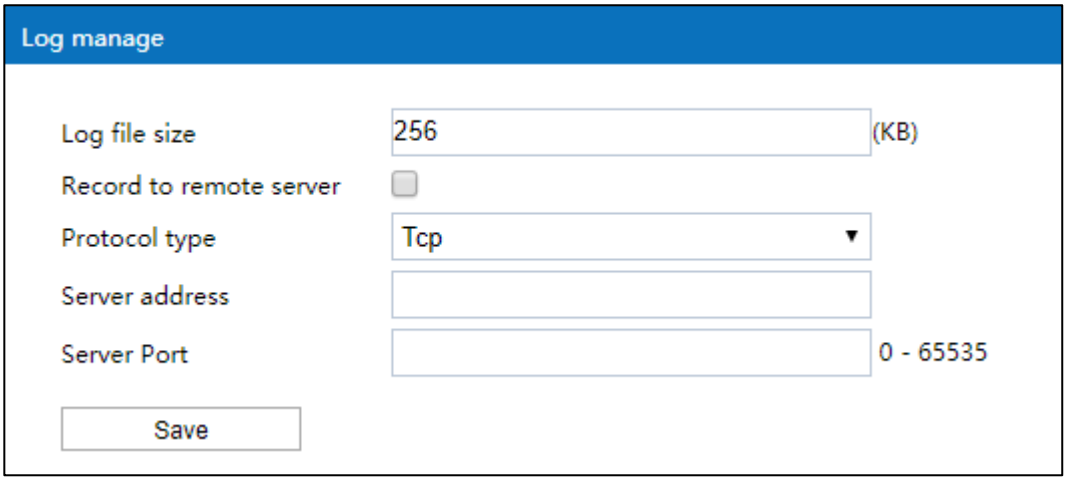
On the page of "Log manage", user can record the log files to the remote server.

Operation Path

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

Interface Description

The log management interface as follows:



The main elements configuration description of log management interface:

Interface Element	Description
Log file size	Set the size of the log file, the default is 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: • TCP;

Copyright © 3onedata Co., Ltd.

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

8.6 Firmware Upgrade

Function Description

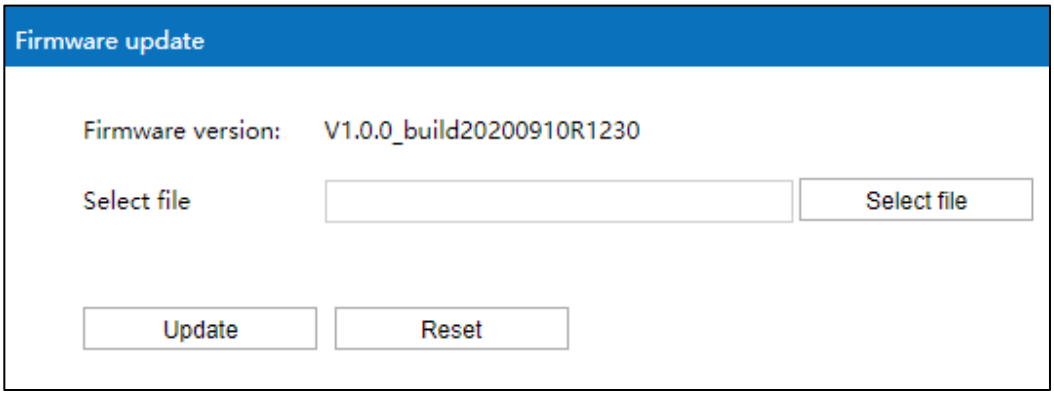
On the "System upgrade" page of system tools, user can update the device system program via firmware upgrade.

Operation Path

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

Interface Description

System upgrade interface as follows:



The main elements configuration description of system upgrade interface:

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

Copyright © 3onedata Co., Ltd.

8.7 System Settings

Function Description

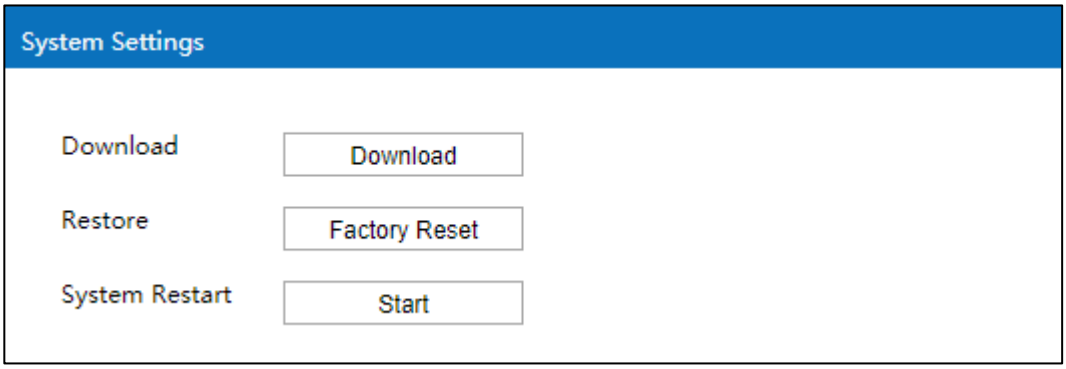
On the “System Settings” page, you can download the current configuration files, restore factory settings or reboot the device.

Operation Path

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

Interface Description

System settings interface is as follows:



The main elements configuration description of system settings interface:

Interface Element	Description
Download	Click “download” button, you can download the current configuration “bakup.file” to local PC to backup the device configuration.
Restore	Click “Factory Reset” button, then click "OK” button to confirm restoring factory defaults.
System Restart	Click "Start” button, the click "OK” button to confirm rebooting system, and the device starts to reboot automatically.

Copyright © 3onedata Co., Ltd.

9 Diagnostic Tools

9.1 System log

Function Description

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

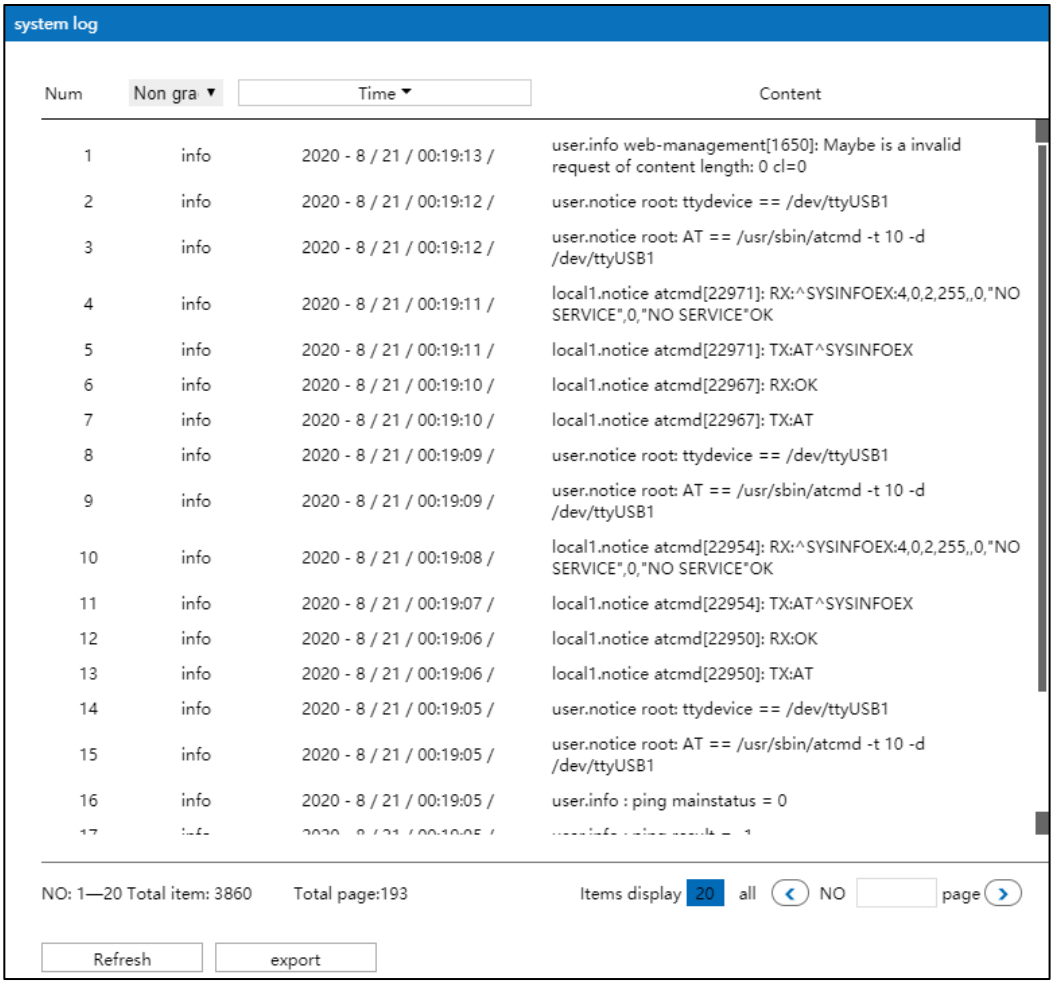
Operation Path

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

Interface Description

The system log interface as follows:

Copyright © 3onedata Co., Ltd.



The main elements configuration description of system log interface:

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

Copyright © 3onedata Co., Ltd.

Interface Element	Description
Export	Click the "Export" button to export the log information in the format of ".txt".

9.2 Ping Test

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

Function Description

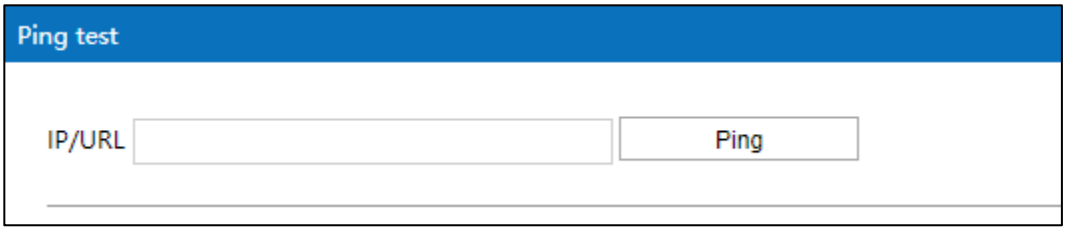
On the page of "Ping test", user can detect whether the target host can be connected.

Operation Path

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

Interface Description

The Ping test interface as follows:



The main elements configuration description of Ping test interface:

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

9.3 Route Tracking

Tracert is a route-tracking utility that determines the path taken by an IP datagram to access a destination. The Tracert 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.

Copyright © 3onedata Co., Ltd.

Function Description

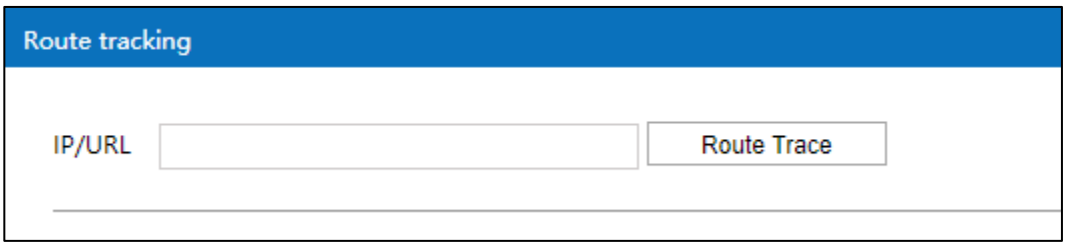
On the page of "Route Tracking", user can perform route tracking for the target host.

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 Tracking" button to start tracking, and the test results are displayed below.

Copyright © 3onedata Co., Ltd.

10 FAQ

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

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

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

4. **What is a universal bridging?**
   Universal bridging is a way to bridge an AP and a client by creating a proxy

Copyright © 3onedata Co., Ltd.

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

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

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

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

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

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

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

Copyright © 3onedata Co., Ltd.

11 Maintenance and Service

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

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

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

11.1 Internet Service

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

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

11.2 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 to solve the product or usage problems ASAP. Free service hotline: +86-400-880-4496

11.3 Product repair or replacement

As for the product repair, replacement or return, customers should firstly confirm with the company technical staff, and then contact the company salesman and 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.

Copyright © 3onedata Co., Ltd.

3onedata



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: 400-880-4496

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