3onedata
Make network communication more reliable



# IRT5300-AW-5T2D
# Industrial 4G Router
# User Manual

Version: 01

Issue Date: 2019-03-20

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

## Copyright © 2019 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 

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

## Notes

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
Make network communication more reliable




## 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: | +86-400-880-4496 |
| E-mail: | sales@3onedata.com |
| Fax: | +86-0755-26703485 |
| Website: | http://www.3onedata.com |

# Preface

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

- Product feature
- Network management method
- Network management relative principle overview

## Readers

This manual mainly suits for engineers as follows:

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

## Text Format Convention

| Format | Description |
|---|---|
| “” | Words with "" represent the interface words. e.g.: "The port number". |
| > | Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection". |
| Light Blue Font | Represent the words click to achieve hyperlink. Font color as: "Light blue". |
| About This Chapter | The "About This Chapter" section provides links to each section and corresponding principles / operating chapters in this chapter. |

## Icon Convention



Copyright © 3onedata Co., Ltd.

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

# Revision Record

| Version NO. | Revision Date | Revision Description |
|---|---|---|
| 01 | 2019-03-20 | Product Release |



Copyright © 3onedata Co., Ltd.

# Content

PREFACE ..... 1
CONTENT ..... I
1 LOG IN THE WEB INTERFACE ..... 1
1.1 WEB BROWSING SYSTEM REQUIREMENTS ..... 1
1.2 SETTING IP ADDRESS OF PC ..... 1
1.3 LOG IN THE WEB CONFIGURATION INTERFACE ..... 3
2 SYSTEM STATUS ..... 4
3 BASIC NETWORK ..... 8
3.1 WAN NETWORK ..... 8
3.2 MOBILE DETECTION ..... 13
3.3 LOCAL AREA NETWORK ..... 15
3.4 DYNAMIC DOMAIN NAME ..... 17
3.5 ROUTING TABLE ..... 19
4 WLAN SETTINGS ..... 22
4.1 BASIC PARAMETER SETTINGS ..... 22
4.2 WIRELESS CLIENT FILTERING ..... 28
4.3 WIRELESS SEARCH ..... 30
5 ADVANCED NETWORK ..... 32
5.1 PORT FORWARD ..... 32
5.2 PORT REDIRECTION ..... 33
5.3 DMZ SETTINGS ..... 34
5.4 SERIAL PORT APPLICATION ..... 35
5.4.1 RealCom Mode ..... 39
5.4.2 TCP Server Mode ..... 42
5.4.3 TCP Client Mode ..... 45
5.4.4 UDP Server Mode ..... 49
5.4.5 UDP Client Mode ..... 53
5.5 UPNP SETTINGS ..... 56
5.6 VRRP ..... 58
5.7 RIP ..... 63
5.8 OSPF ..... 64
5.9 STATIC DHCP ..... 66



Copyright © 3onedata Co., Ltd.

6 FIREWALL ..... 69
6.1 IP FILTER ..... 69
6.2 MAC FILTER ..... 71
6.3 URL FILTER ..... 72
6.4 KEYWORD FILTER ..... 74
7 VPN TUNNEL ..... 76
7.1 GRE SETTINGS ..... 76
7.2 PPTP CLIENT SETTINGS ..... 77
7.3 PPTP SERVER SETTINGS ..... 79
7.4 L2TP CLIENT SETTINGS ..... 81
7.5 L2TP SERVER SETTINGS ..... 83
7.6 IPSEC ..... 85
8 SYSTEM MANAGE ..... 89
8.1 TIME SETTING ..... 89
8.2 ACCESS SETTINGS ..... 90
8.3 TIMED RESTART ..... 92
8.4 BACKUP RECOVERY ..... 93
8.5 LOG MANAGE ..... 94
8.6 FIRMWARE UPGRADE ..... 95
8.7 FIRMWARE RESTART ..... 96
9 DIAGNOSTIC TOOLS ..... 97
9.1 SYSTEM LOG ..... 97
9.2 PING TEST ..... 98
9.3 ROUTE TRACKING ..... 99
10 MAINTENANCE AND SERVICE ..... 101
10.1 INTERNET SERVICE ..... 101
10.2 SERVICE HOTLINE ..... 101
10.3 PRODUCT REPAIR OR REPLACEMENT ..... 102



Copyright © 3onedata Co., Ltd.

# 1 Log in the Web Interface

## 1.1 WEB Browsing System Requirements

While using the managed Industrial router, the system should meet the following conditions.

| Hardware and Software | System Requirements |
|---|---|
| CPU | Above Pentium 586 |
| Memory | Above 128MB |
| Resolution | Above 1024x768 |
| Color | Above 256 color |
| Browser | Above Internet Explorer 6.0 |
| Operating System | Windows XP<br>Windows 7 |

## 1.2 Setting IP Address of PC

The router default management as follows:

| IP Setting | Default Value |
|---|---|
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |

While configuring the router via Web:



Copyright © 3onedata Co., Ltd.

- Before remote configuration, please make sure the route between computer and switch is reachable.
- Before local configuration, please make sure the computer IP address is on the same subnet as the one of switch.

Notes:
While first configuring the router, if it is a local configuration mode, please make sure that the network segment of current PC is 1.

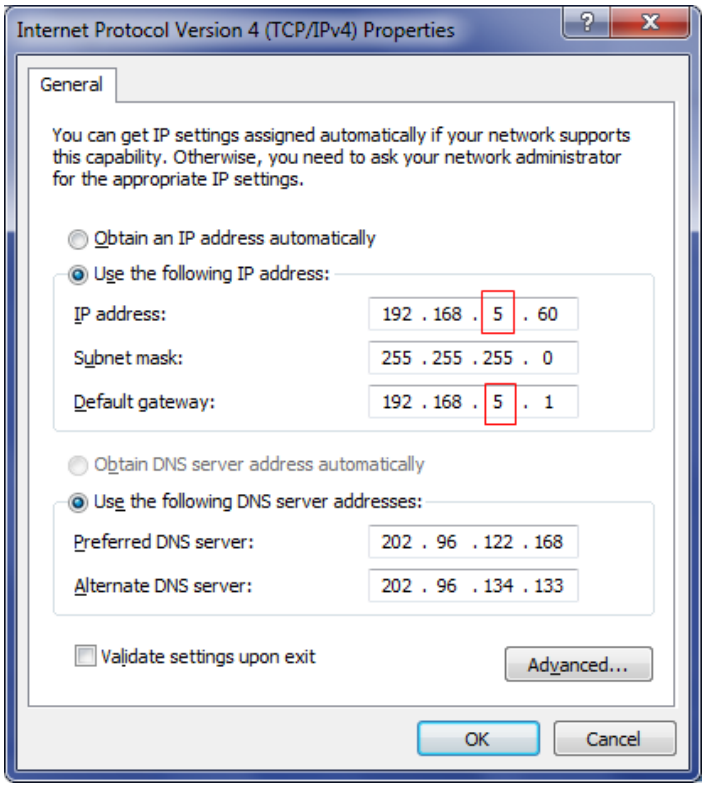
E.g.: Assume that the IP address of current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

## Operation Steps

Amendment steps as follows:

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

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




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

**Step 4** End.



Copyright © 3onedata Co., Ltd.

# 1.3 Log in the Web Configuration Interface

### Operation Steps

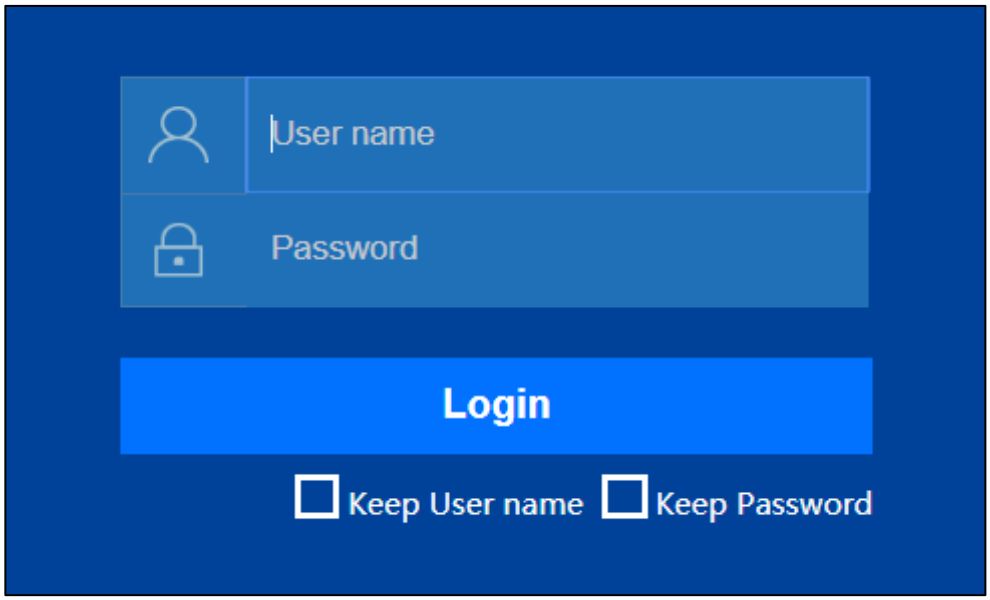
Login in the web configuration interface as follows:

**Step 1** Run the computer browser.

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

**Step 3** Click the “Enter” key.

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




Notes:

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

**Step 5** Click "OK".

**Step 6** End.

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

Notes:

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



Copyright © 3onedata Co., Ltd.

# 2 System Status

## Function Description

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

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

## Operation Path

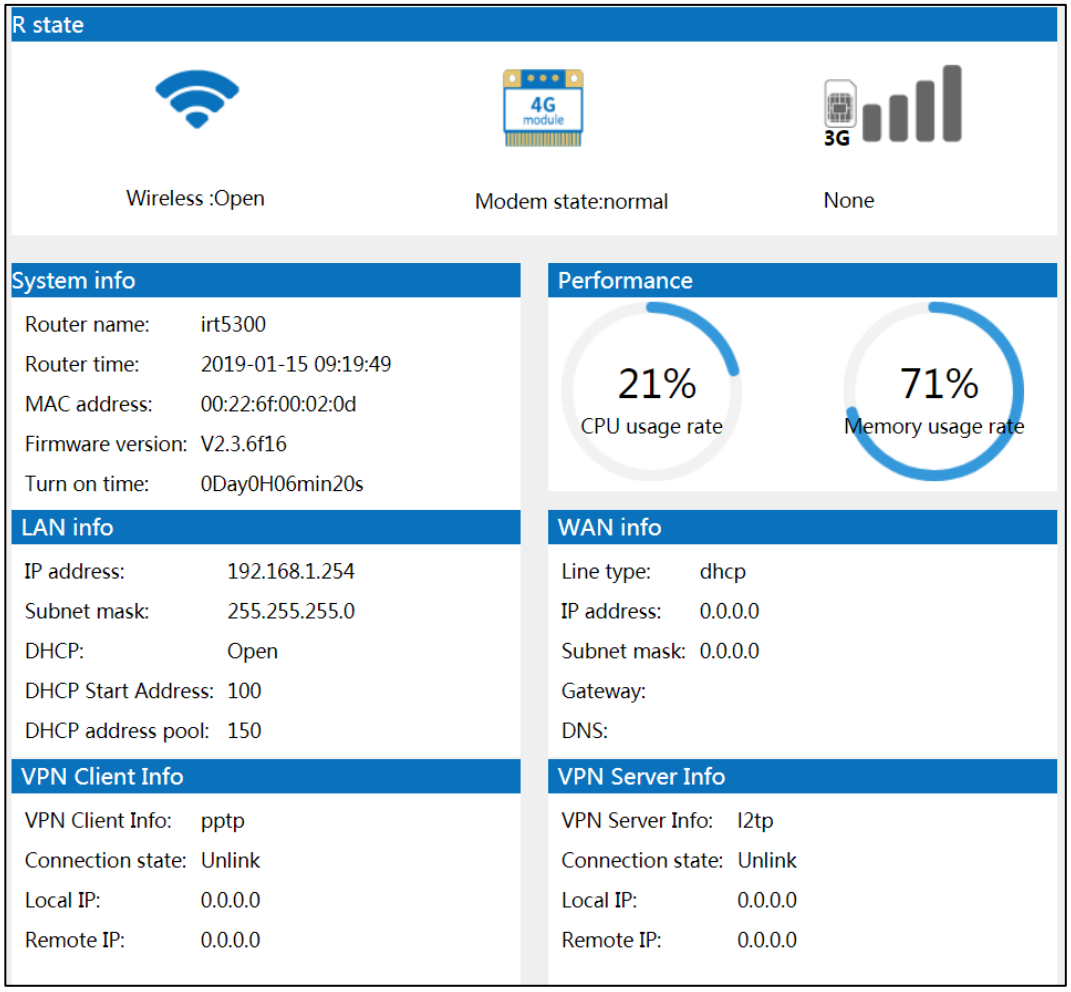
Choose “System Status” in the navigation bar.

## Interface Description

System status interface as follows:



Copyright © 3onedata Co., Ltd.




The main element configuration description of system status interface:

| Interface Element | Description |
|---|---|
| **R state** | **The running state bar** |
| Wireless | The status of device wireless function is displayed as follows:<br>• Open: the wireless WiFi function has been enabled;<br>• Close: the wireless WiFi function hasn't been enabled. |
| Modem state | The states of device 4G module Modem are displayed as follows:<br>• Normal;<br>• Close. |
| 4G | Information including the existence state of SIM card used by current device, operator's network, network operating mode and signal strength etc. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| **System info** | **The system information bar** |
| Router name | Device name |
| Firmware version | The firmware version of the device |
| Router time | The current time displayed by router. Its format is Year-Month-Day Hour: Minute: Second |
| Turn on time | The run time after turning on the device |
| **Performance** | **The performance bar** |
| CPU usage rate (%) | The usage rate of device CPU. |
| Memory usage rate (%) | The usage rate of device memory.<br>Note:<br>The performance of the device would be affected if the application consumes too much memory. |
| **LAN info** | **The LAN information bar** |
| IP address | The IP address information of LAN |
| Subnet mask | The subnet mask information of LAN |
| DHCP | Whether the DHCP function is enabled:<br>• Open<br>• Close |
| 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 line type of WAN, which is 3G/4G by default |
| 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** |
| VPN client info | Related information about VPN client. It displays related information when VPN client is enabled, otherwise it displays pptp by default |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Connection state | The connection state of VPN client:<br>• Unlink<br>• Link |
| Local IP | The IP address of local client |
| Remote IP | The IP address of remote server |
| **VPN Server Info** | **The VPN server information bar** |
| VPN server info | Related information about VPN server. It displays related information when VPN server is enabled, otherwise it displays pptp by default |
| Connection state | The connection state of VPN server:<br>• Unlink<br>• Link |
| 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

### Function Description

On the “WAN Network” page, user can set the line type and parameter of WAN. The line types are as follows:

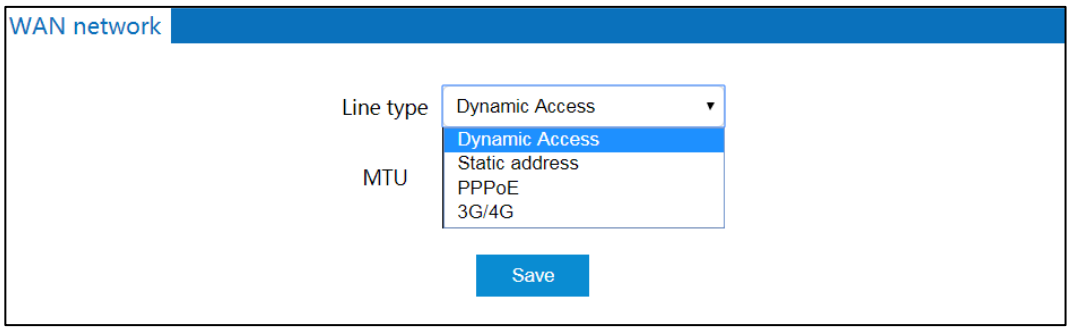
- Dynamic access: the WAN port of the device accesses network address information allocated by network provider or outer network automatically;
- Static address: configuring the network information of the device WAN port manually;
- PPPoE: implement PPPoE point-to-point protocol dial-up via wired network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

### Operation Path

Click: “Basic Network > WAN Network”.

### Interface Description 1: Dynamic Access

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





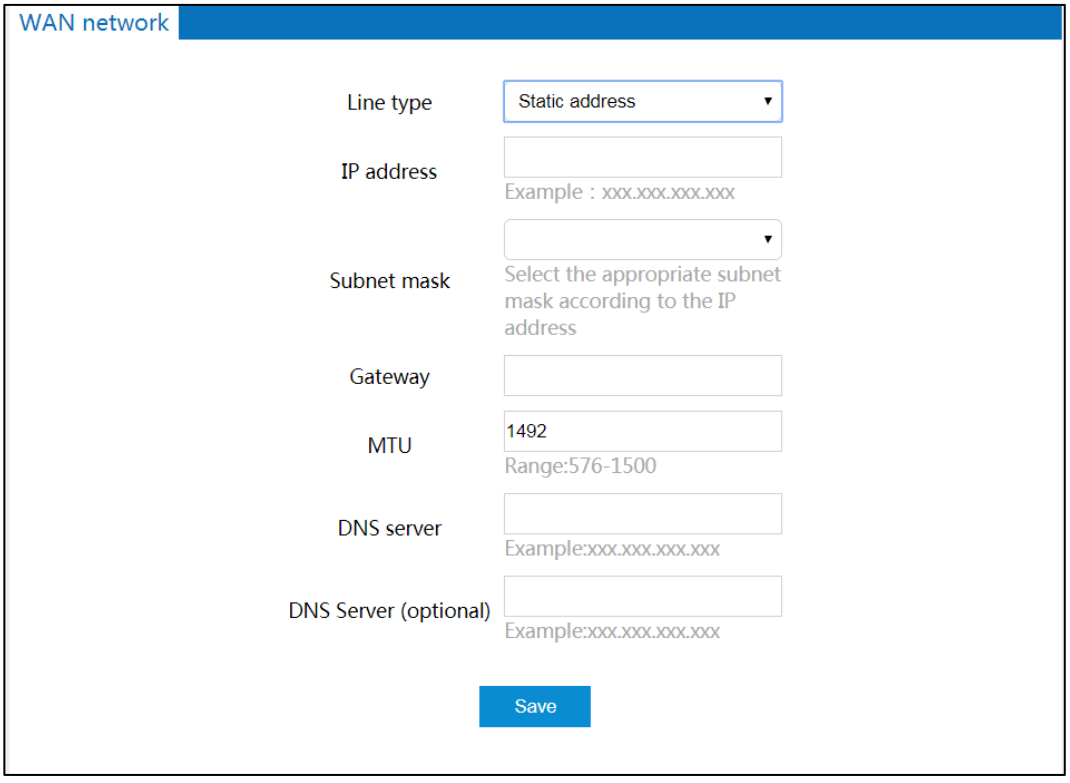

Copyright © 3onedata Co., Ltd.

The main element configuration description of dynamic access interface:

| Interface Element | Description |
|---|---|
| Line type | Dynamic Access: the WAN port of the device accesses network address information allocated by network provider or outer network automatically. |
| MTU | The maximal length of single message that can get through in WAN network communication, the value range is 576-1500 bytes.<br>Notes:<br>• 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;<br>• MTU value is recommended to be same to the one of superior router. |

### Interface Description 2: Static Address

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






Copyright © 3onedata Co., Ltd.

The main element configuration description of static address interface:

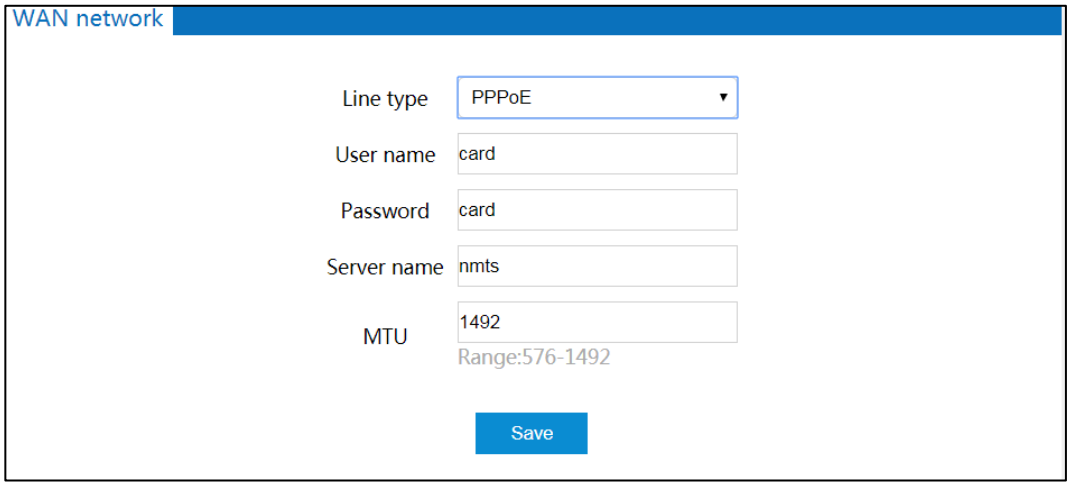
| Interface Element | Description |
|---|---|
| Line type | Static address: the network information configuration of device WAN port. |
| IP address | The fixed IP address distributed by network provider or outer network. |
| Subnet mask | Drop-down list of subnet mask. |
| Gateway | The default gateway address automatically distributed by network provider or outer network. |
| MTU | The maximal length of single message that can get through in WAN network communication, the value range is 576-1500 bytes.<br>Notes:<br>• MTU (Maximum Transmission Unit), the device will divide the data packet into multiple small packets if the maximum length of single message exceeds given MTU value; so reasonable setting can optimize network speed;<br>• MTU value is recommended to be same to the one of superior router. |
| DNS server | The DNS server address provided by network provider or outer network. |
| DNS Server (optional) | The backup DNS server address provided by network provider or outer network. This item can be skipped. |

### Interface Description 3: PPPoE

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



Copyright © 3onedata Co., Ltd.




The main element configuration description of PPPoE interface:

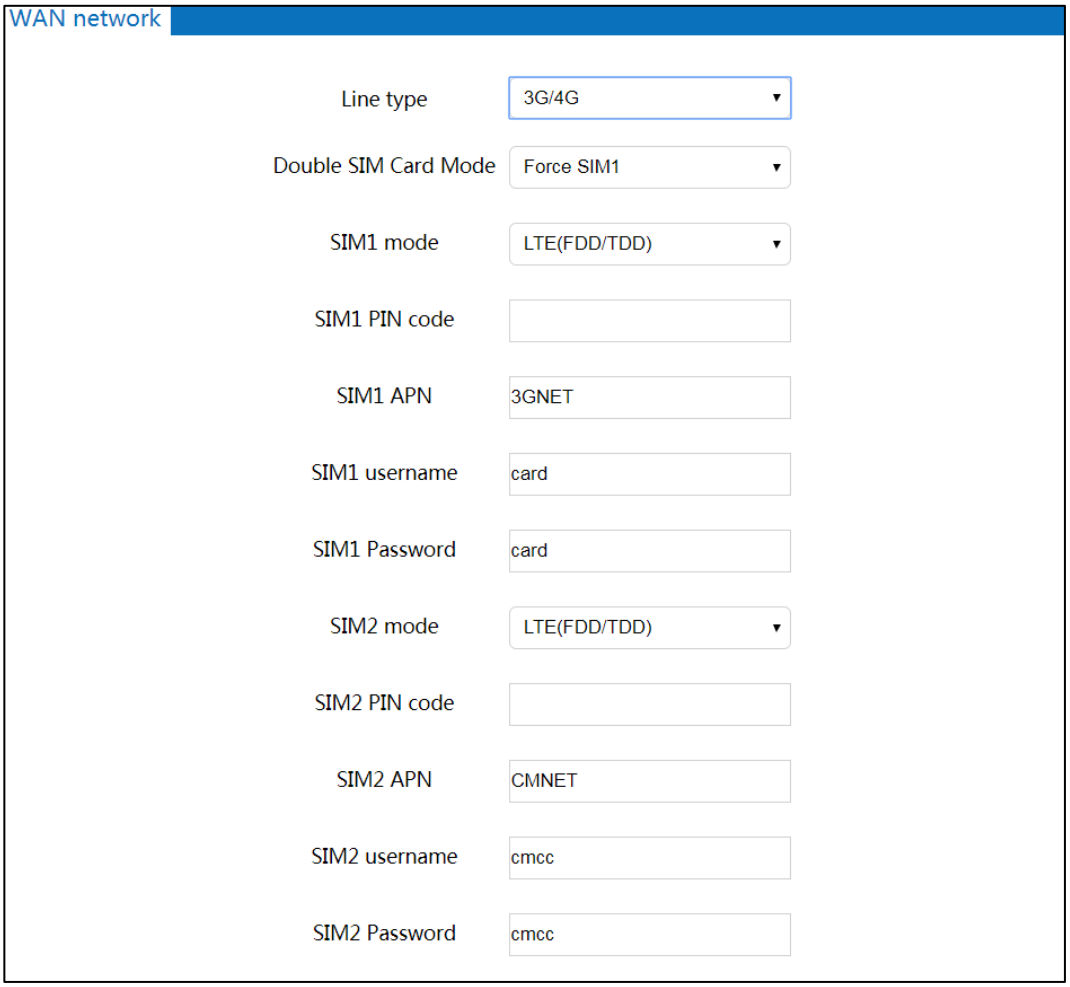
| Interface Element | Description |
|---|---|
| Line type | PPPoE: achieve internet access via PPPoE point-to-point protocol dial-up. |
| User name | User name of PPPoE connection.<br>Notes:<br>User name, password and server name are provided by network provider. |
| Password | Password of PPPoE connection.<br>Notes:<br>User name, password and server name are provided by network provider. |
| Server name | Server name, not fill if network provider doesn't supply.<br>Notes:<br>User name, password and server name are provided by network provider |
| MTU | The maximal length of single message that can get through in WAN network communication, the value range is 576-1492 bytes.<br>Notes:<br>• MTU (Maximum Transmission Unit), the device will divide the data packet into multiple small packets if the maximum length of single message exceeds given MTU value; so reasonable setting can optimize network speed;<br>• MTU value is recommended to be same to the one of superior router. |



Copyright © 3onedata Co., Ltd.

### Interface Description 4: 3G/4G

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




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

| Interface Element | Description |
|---|---|
| Line type | 3G/4G: achieve 3G/4G network access via SIM card dial-up. |
| Double SIM card mode | In the drop-down list of double SIM card mode, user can choose specified SIM card. The options are:<br>• Force SIM1<br>• Force SIM2<br>• Switch failure: when SIM1 or SIM2 fails to connect, it will switch to SIM2 or SIM1 automatically |
| SIM1 mode | The drop-down list of SIM1 mode. The options are:<br>• LTE(FDD/TDD) |



Copyright © 3onedata Co., Ltd.

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



Copyright © 3onedata Co., Ltd.

## Function Description

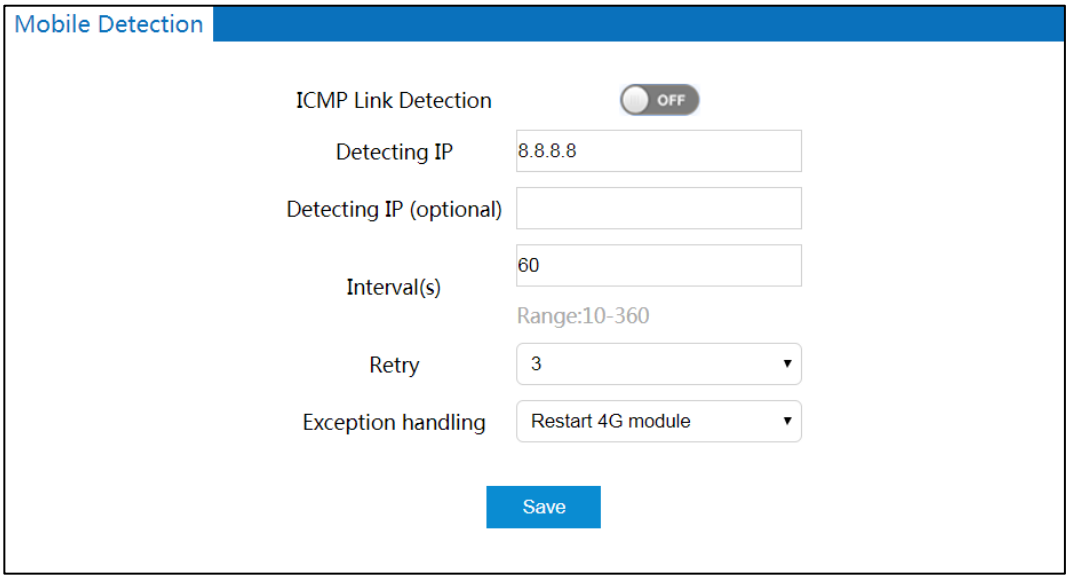
On the “Mobile Detection” page, user can detect the connection status of network and make corresponding operation.

## Operation Path

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

## Interface Description

The mobile detection interface as follows:




The main element configuration description of mobile detection interface:

| Interface Element | Description |
|---|---|
| ICMP Link Detection | The enable switch of ICMP link detection. Click the right button to switch between ON and OFF.<br>• ON: turn on ICMP link detection function to detect network connection.<br>• OFF: turn off ICMP link detection function. |
| 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 60-360 |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Retry | To detect the times of retry, the drop-down list of retry. Options are: 1-5 |
| Exception handling | The corresponding way of handling detected exception. The drop-down list of exception handling, options are:<br>• Restart 4G module<br>• Switch SIM card<br>• Reboot the system |

## 3.3 Local Area Network

DHCP (Dynamic Host Configuration Protocol) is a network protocol of LAN; it adopts UDP protocol to automatically distribute IP address to LAN, improving the IP address utilization. The client in network environment can gain the dynamic IP address, Gateway address, DNS server address and other information from DHCP server.

### Function Description

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

### Operation Path

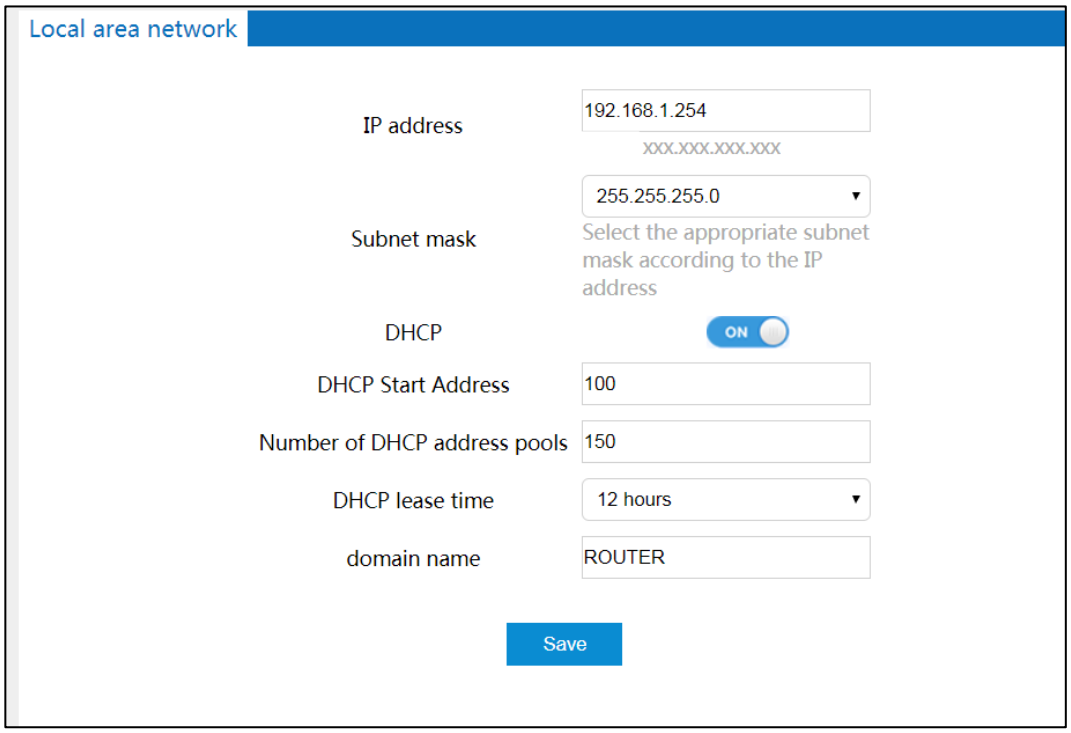
Please open in order: “Basic Network > Local Area Network”.

### Interface Description

The local area network interface as follows:



Copyright © 3onedata Co., Ltd.




The main element configuration description of local area network interface:

| Interface Element | Description |
|---|---|
| IP address | IP address of the device LAN port. |
| Subnet mask | Drop-down list of subnet mask. |
| DHCP | The enable switch of DHCP function. Click the right button to switch between ON and OFF.<br>• ON: turn on DHCP server function.<br>• OFF: turn off DHCP server function. |
| DHCP start address | Minimum IP address host number distributed by DHCP address pool, value range is 1-254. |
| IP address pool size | Maximum IP address number distributed by IP 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:<br>• 30 minutes;<br>• 1 hour;<br>• 6 hours;<br>• 12 hours; |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • 1 day;<br>• 3 days;<br>• 7 days. |
| Domain name | DHCP domain name is composed of letter, number and underline; it supports 0-32 valid characters. |

## 3.4 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

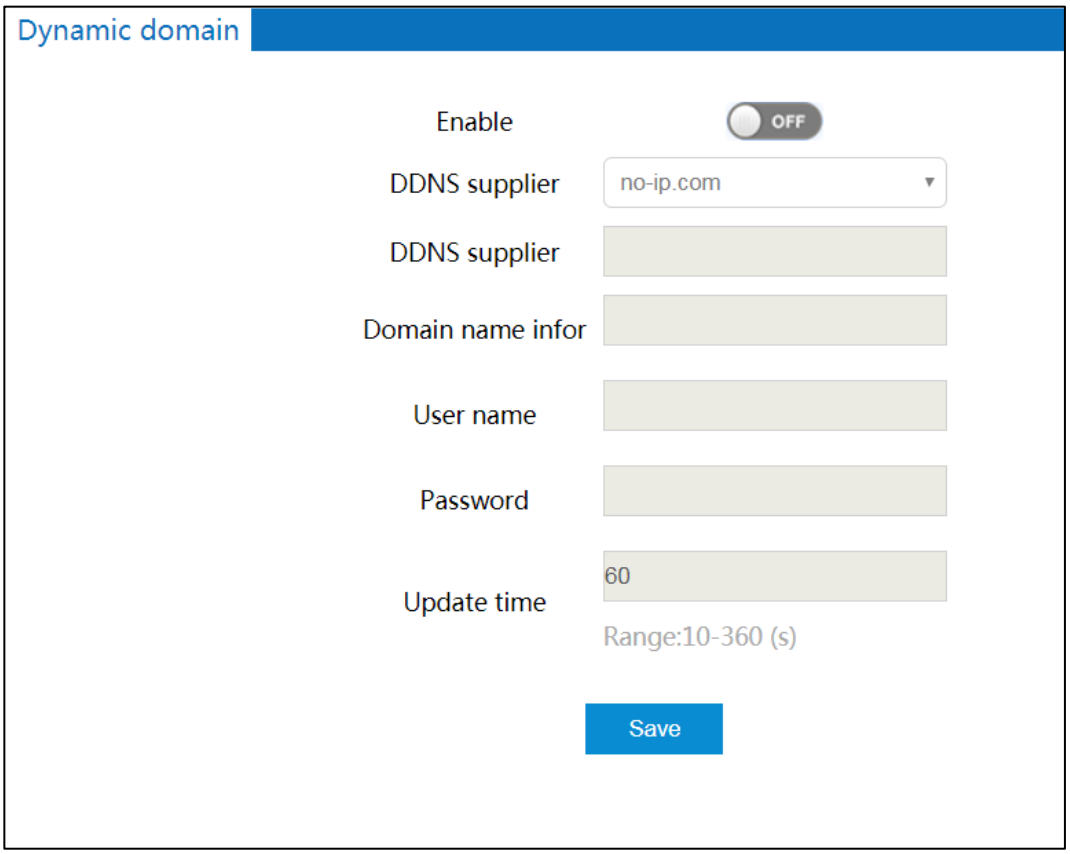
Choose “Basic Network > Dynamic Domain” in the navigation bar.

### Interface Description

The dynamic domain interface as follows:



Copyright © 3onedata Co., Ltd.




The main element configuration description of dynamic domain interface:

| Interface Element | Description |
|---|---|
| Enable | The enable switch of dynamic domain name function. Click the right button to switch between ON and OFF<br>• ON: turn on dynamic domain name function;<br>• OFF: turn off dynamic domain name function. |
| DDNS supplier | The router supports multiple DDNS suppliers. The options in the DDNS supplier drop-down list are:<br>• no-ip.com<br>• 3322.org<br>• dyndns.org<br>• oray.com<br>• 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 it applied for from DDNS supplier |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| User name | The user name it applied for from DDNS supplier |
| Password | The password it applied for from DDNS supplier |
| Update time (s) | Update the time interval of dynamic DNS to server, the unit is second, it defaults to 60, the value range is 10-360 |

# 3.5 Routing Table

Routing table is a spreadsheet or database stored in router, which has saved the paths to specified network address. The routing table includes topological information of perimeter network, which mainly aims to implement selection between routing protocol and static routing.

### Function Description

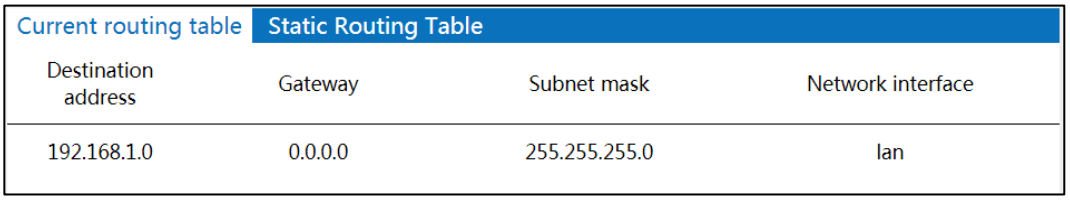
On the “Routing Table” page, user can set relevant information of routing table.

### Operation Path

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

### Interface Description 1: Current Routing Table

The current routing table interface as follows:




The main element configuration description of current routing table interface:

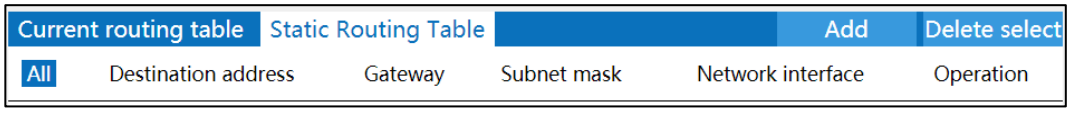
| Interface Element | Description |
|---|---|
| Destination address | The destination IP address information of current routing |
| Gateway | The destination gateway information of current routing |
| Subnet mask | The subnet mask information of current routing |
| Network interface | The network interface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

### Interface Description 2: Static Routing Table

The static routing table interface as follows:



Copyright © 3onedata Co., Ltd.




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 gateway information of static routing |
| Subnet mask | The subnet mask information of static routing:<br>• 255.255.255.255<br>• 255.255.255.254<br>• 255.255.255.252<br>• 255.255.255.248<br>• 255.255.255.224<br>• 255.255.255.192<br>• 255.255.255.128<br>• 255.255.255.0<br>• 255.255.254.0<br>• 255.255.252.0<br>• 255.255.248.0<br>• 255.255.240.0<br>• 255.255.224.0<br>• 255.255.192.0<br>• 255.255.128.0<br>• 255.255.0.0<br>• 255.254.0.0<br>• 255.252.0.0<br>• 255.248.0.0<br>• 255.224.0.0<br>• 255.192.0.0<br>• 255.128.0.0<br>• 255.0.0.0<br>• 254.0.0.0<br>• 252.0.0.0<br>• 248.0.0.0<br>• 240.0.0.0 |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • 224.0.0.0<br>• 192.0.0.0<br>• 128.0.0.0 |
| Network interface | The network interface of static routing:<br>• WAN<br>• LAN |
| 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

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

## 4.1 Basic Parameter Settings

### Function Description

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

### Operation Path

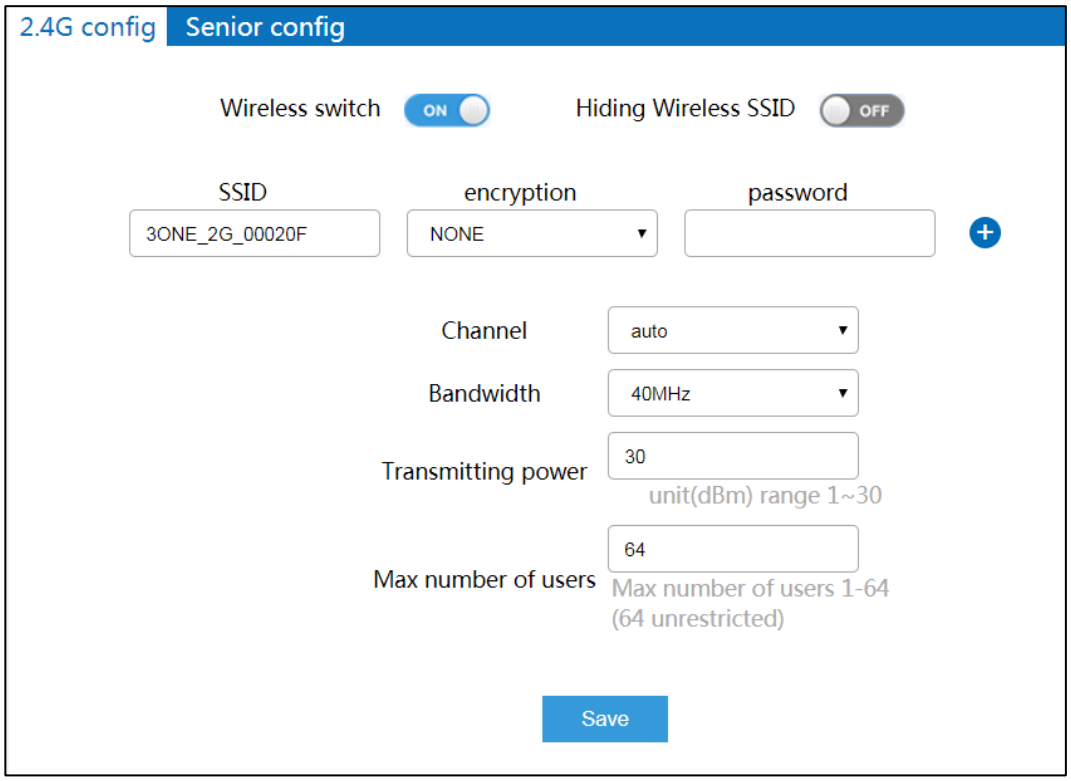
Please open in order: “WLAN Settings > Basic Parameter Settings”.

### Interface Description 1: 2.4G Configuration

The 2.4G configuration interface as follows:



Copyright © 3onedata Co., Ltd.




The main element configuration description of 2.4G configuration interface:

| Interface Element | Description |
|---|---|
| Wireless switch | Function enabling switch of wireless network; click the right button for ON and OFF switching.<br>• ON: enable wireless network function.<br>• OFF: disable wireless network function. When the wireless switch is in OFF state, wireless network will be unavailable, and the wireless connection will be disconnected. |
| Hiding Wireless SSID | Function enabling switch of hidden SSID; click the right button for ON and OFF switching.<br>• ON: enable hidden SSID function, SSID name of the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal while connecting hidden wireless signal.<br>• OFF: disable hidden SSID function. |
| SSID | SSID name of wireless network, it supports 1-32 characters. |
| Encryption | Encryption mode of wireless network, options as follows:<br>• NONE: No encryption; |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • WPA2-PSK(Recommended): Wi-Fi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes.<br>• WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode.<br>Notes:<br>WPA2-PSK is recommended, because it's stronger and safer than WEP-SHARED. |
| Password | Password of wireless network, different encryption mode has different password requirements as follows:<br>• Under WPA2-PSK encryption mode, wireless password supports 8-32 valid characters;<br>• Under WEP-SHARED, wireless password supports 5, 13 ASSIC characters or 10, 26 hexadecimal characters. |
| Channel | Working channel of wireless network, default "auto" self-adaptation, options as follows:<br>• Auto: channel self-adaptation;<br>• 1: main frequency band 2412Hz, frequency range 2401~2423Hz;<br>• 2: main frequency band 2417Hz, frequency range 2406~2428Hz;<br>• 3: main frequency band 2422Hz, frequency range 2411~2433Hz;<br>• 4: main frequency band 2427Hz, frequency range 2416~2438Hz;<br>• 5: main frequency band 2432Hz, frequency range 2421~2443Hz;<br>• 6: main frequency band 2437Hz, frequency range 2426~2448Hz;<br>• 7: main frequency band 2442Hz, frequency range 2431~2453Hz;<br>• 8: main frequency band 2447Hz, frequency range 2436~2458Hz;<br>• 9: main frequency band 2452Hz, frequency range 2441~2463Hz; |



Copyright © 3onedata Co., Ltd.

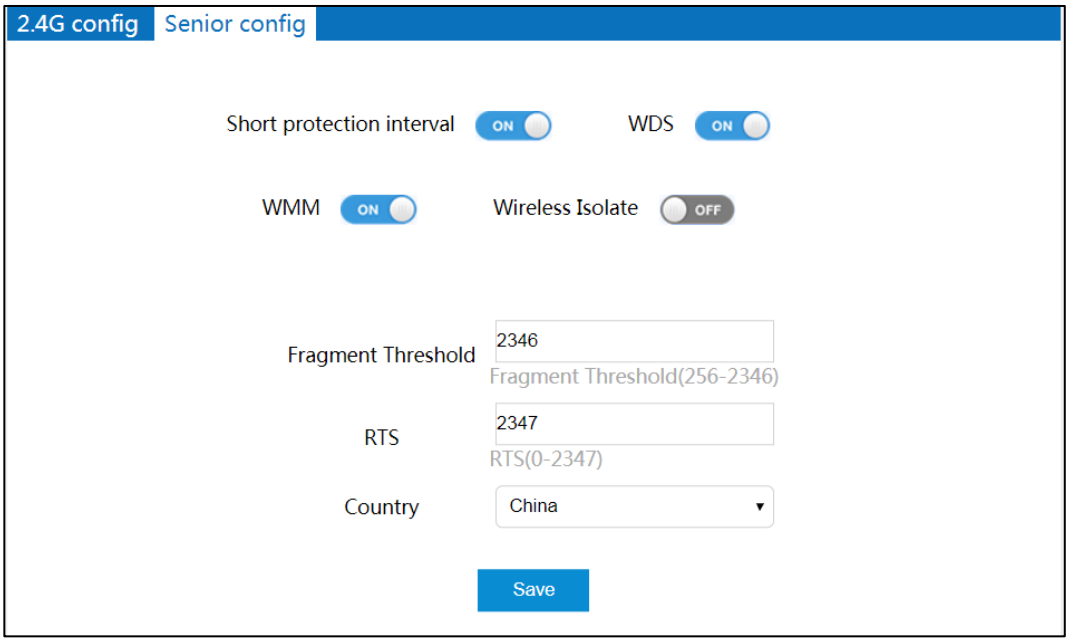
| Interface Element | Description |
|---|---|
| | • 10: main frequency band 2457Hz, frequency range 2446~2468Hz;<br>• 11: main frequency band 2462Hz, frequency range 2451~2473Hz;<br>• 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in USA, so it's temporarily unavailable;<br>• 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in USA, so it's temporarily unavailable;<br>Notes:<br>In order to improve the network performance, please choose unused channel in the device working environment. |
| Bandwidth | Channel bandwidth of wireless network, it defaults to 40MHz, options as follows:<br>• 20MHz;<br>• 40MHz.<br>Notes:<br>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 20dBm, value range 1~20dBm.<br>Notes:<br>• Greater the transmitted power, better the transmutability, longer the transmission range;<br>• Different device has different transmitted 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. |



Copyright © 3onedata Co., Ltd.

### Interface Description 2: Senior Configuration

The senior configuration interface as follows:




The main element configuration description of senior configuration interface:

| Interface Element | Description |
|---|---|
| Short protection interval | Short protection interval enabling switch, click the right button for ON and OFF switching.<br>• ON: enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed.<br>• OFF: after disabling the function, the transmission interval of data packet defaults to 800ns.<br>Notes:<br>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.<br>Notes:<br>Please enable WDS function while bridging the device and other wireless devices. |
| WMM | WMM (WiFi Multimedia) function, defaults to enabled.<br>Notes:<br>After enabling 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. |
| 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.<br>Notes:<br>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.<br>Notes:<br>• The data frame will be segmented when its length surpasses fragment threshold.<br>• 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.<br>• 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.<br>• RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will send RTS signal;<br>• 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;<br>• RTS threshold = 2347: the device wireless terminal won't send RTS signal.<br>Notes:<br>• 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.<br>• 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. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Country | Applied national region of wireless network, options as follows:<br>• China<br>• USA<br>Notes:<br>Open channels are different in different countries. |

# 4.2 Wireless Client Filtering

### Function Description

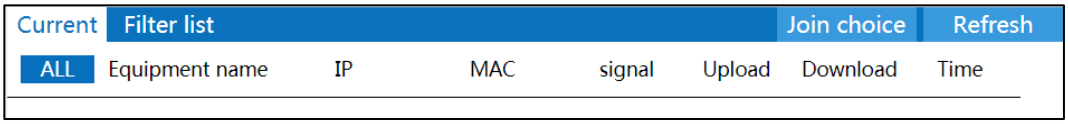
On the “Wireless Client Filtering” page, user can check current connecting devices and manage wireless user connection.

### Operation Path

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

### Interface Description 1: Current

The current interface as follows:




The main element configuration description of current interface:

| Interface Element | Description |
|---|---|
| Equipment name | The equipment name of wireless client connected to this device currently. |
| IP | The IP address of wireless client connected to this device currently. |
| MAC | The MAC address of wireless client connected to this device currently. |
| Signal | The signal strength of wireless client connected to this device currently. The unit is dBm, the larger the value, the stronger the signal. |
| Upload | The upload flow of wireless client connected to this device |

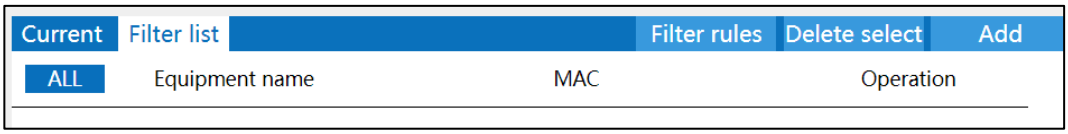


Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | 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: Filter List

The filter list interface as follows:




The main element configuration description of filter list interface:

| Interface Element | Description |
|---|---|
| Equipment name | The equipment name of wireless client banned from connecting this device. |
| MAC | The MAC address of wireless client banned from connecting this device. |
| Operation | Edit wireless client information. |

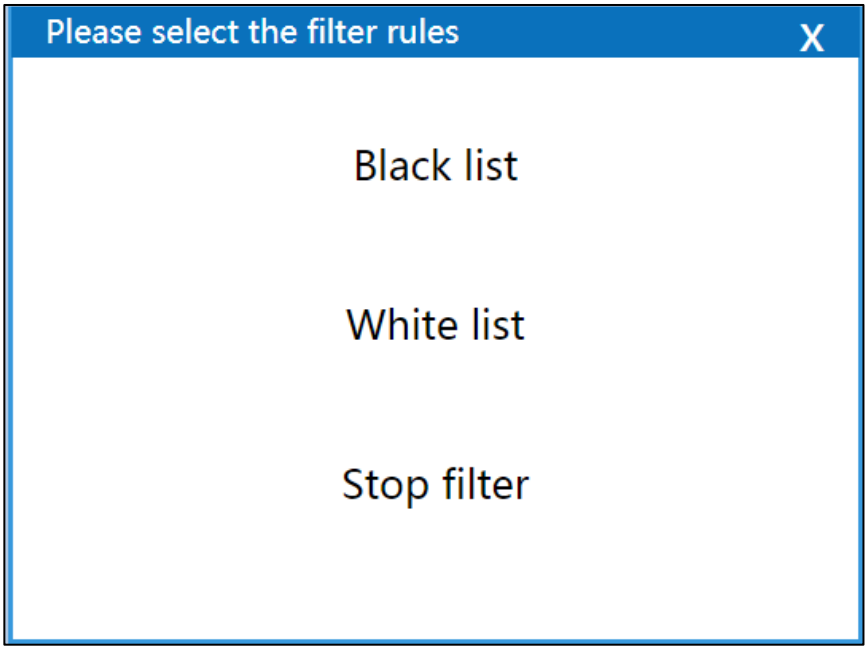
### Interface Description 3: Filter Rule

Click the “Filter Rule” button to switch lists.

The filter rule interface as follows:



Copyright © 3onedata Co., Ltd.




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.

## 4.3 Wireless Search

### Function Description

On the “Wireless Search” page, user can check the wireless WiFi information of device’s environment.

### Operation Path

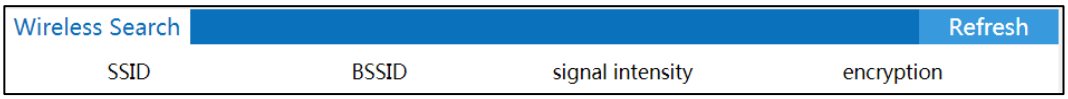
Please open in order: “WLAN Settings > Wireless Search”.



Copyright © 3onedata Co., Ltd.

## Interface Description

The wireless search interface as follows:




The main element configuration description of wireless search interface:

| Interface Element | Description |
|---|---|
| SSID | The SSID name of wireless network in device's surroundings. |
| BSSID | The BSSID (Basic Service Set Identifier) name of wireless network in device's surroundings, which is the MAC address of wireless network device. |
| Signal intensity | The signal intensity of wireless network in device's surroundings. The unit is dbm, the greater the value, the stronger the signal. |
| Encryption | The encryption method of wireless network in device's surroundings. |



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

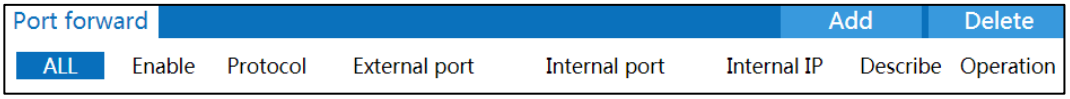
On the “Port Forward” page, user can check or add port forward entry. It allows outer network client to visit specified device via specified port.

### Operation Path

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

### Interface Description

The port forward interface as follows:




The main element configuration description of port forward interface:

| Interface Element | Description |
|---|---|
| All | The checkbox port forward entry. Click “All” to check all port forward entry. |
| Enable | Enable port forward or not: |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • ON<br>• OFF |
| Protocol | The protocol type used by port forward data package:<br>• TCP<br>• UDP<br>• 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 | The remark information of port forward entry |
| Operation | Edit: modify port forward entry information |
| Add | Click the “Add” button at the top right corner to add new port forward in the pop-up window of “Port Forward” |
| Delete | Check the port forward information that needs to be deleted, then click “delete” button at the top right corner to delete it |

# 5.2 Port Redirection

### Function Description

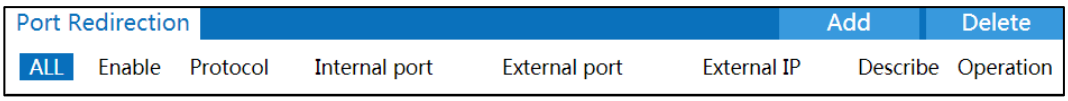
On the “Port Redirection” page, user can check or add port redirection entry, which allows client in LAN to visit the specified port of device with IP address specified by external network via specified port.

### 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:



Copyright © 3onedata Co., Ltd.

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

## 5.3 DMZ Settings

DMZ(Demilitarized Zone）is a 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

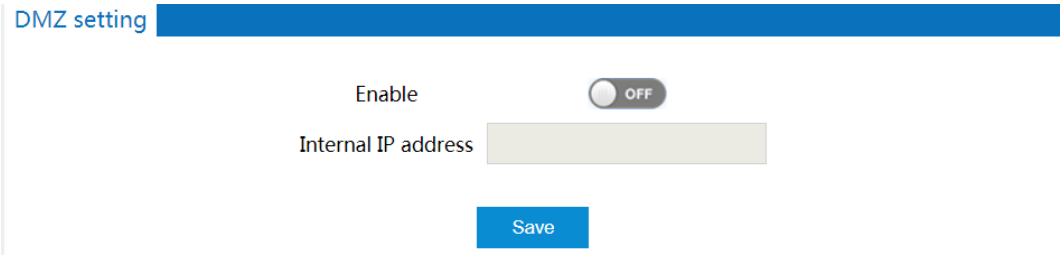
Please open in order: “Advanced Network > DMZ Setting”.



Copyright © 3onedata Co., Ltd.

### Interface Description

The DMZ setting interface as follows:




The main element configuration description of DMZ setting interface:

| Interface Element | Description |
|---|---|
| Enable | The enable switch of DMZ setting. Click the right button to switch between ON and OFF.<br>• ON: enable DMZ setting function.<br>• OFF: disable DMZ setting function. |
| Internal IP address | The IP address of LAN client, for example: 192.168.1.123. |

## 5.4 Serial Port Application

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

### Function Description

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

### Operation Path

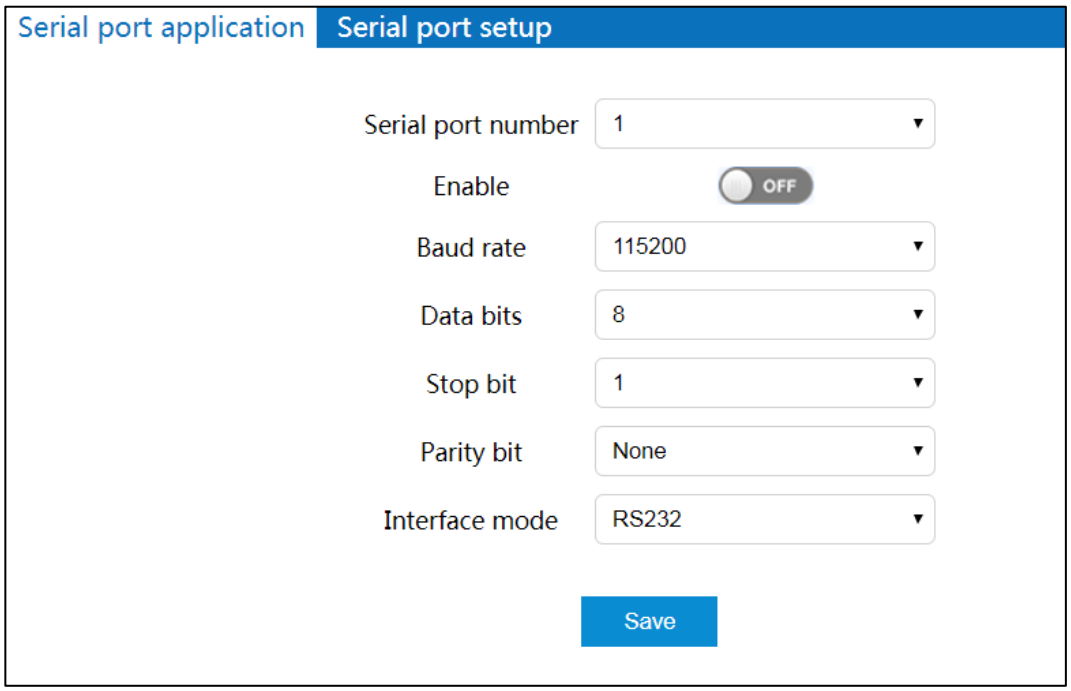
Please open in order: "Advanced Network > Serial Port Application".

### Interface Description 1: Serial Port Application

The serial port application interface as follows:



Copyright © 3onedata Co., Ltd.




The main element configuration description of serial port application interface:

| Interface Element | Description |
|---|---|
| Serial port number | The corresponding serial port number of device's serial port. |
| Enable | The enable switch of serial server. Click the right button to switch between ON and OFF.<br>• ON: enable serial server function of corresponding serial port;<br>• OFF. |
| Baud rate | Choose baud rate of corresponding serial port. Unit: bps. Options are:<br>300/600/1200/2400/4800/9600/19200/38400/57600/115200. |
| Data bit | Choose data bit of corresponding serial port. Unit: bit. Options are:<br>• 7;<br>• 8. |
| Stop bit | Choose stop bit of corresponding serial port. Options are:<br>• 0;<br>• 1; |
| Parity bit | Choose parity bit of corresponding serial port. Options are:<br>• None |

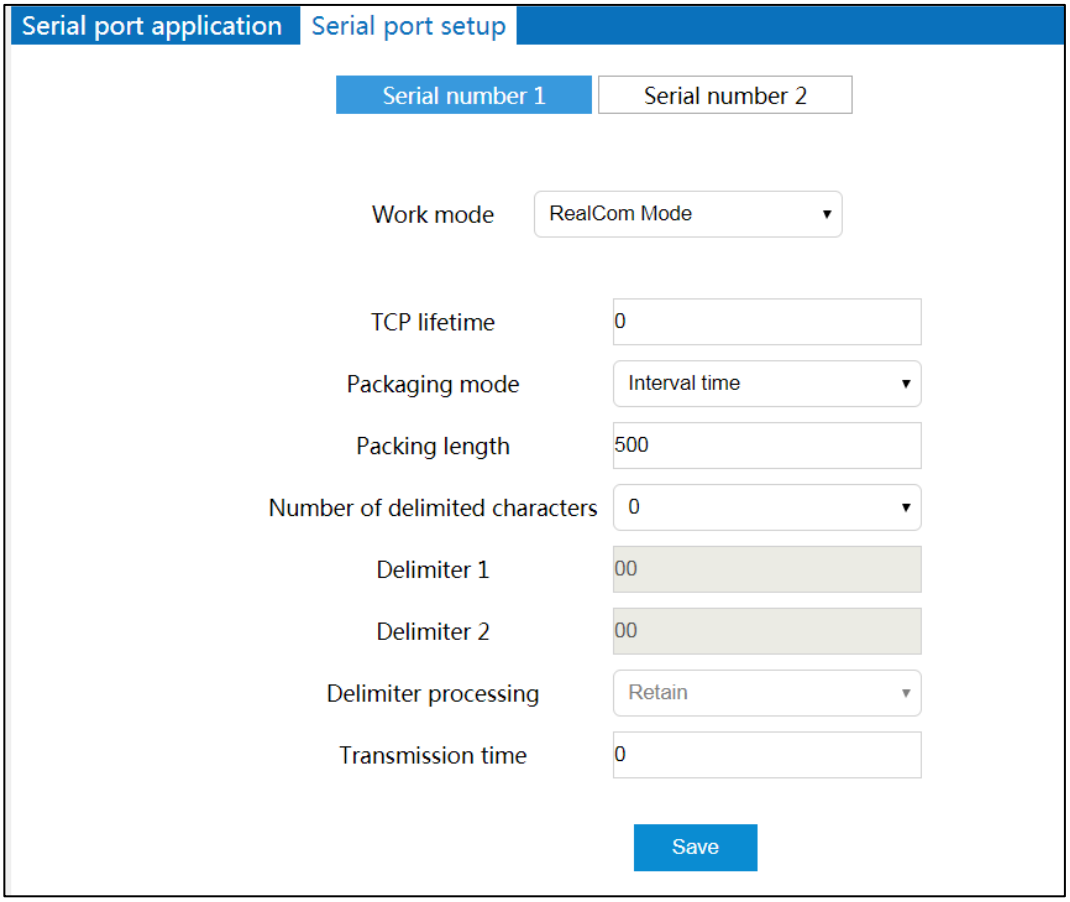


Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • Odd<br>• Even |
| Interface mode | Serial port mode. Options are:<br>• RS232;<br>• RS485. |

### Interface Description 2: Serial Port Setup

The serial port setup interface:




The main element configuration description of serial port setup interface:

| Interface Element | Description |
|---|---|
| Work mode | The work modes of serial port are as follows:<br>• RealCom Mode: Real serial port mode;<br>• TCP Server: TCP server mode;<br>• TCP Client: TCP client mode;<br>• UDP Server: UDP server mode; |



Copyright © 3onedata Co., Ltd.

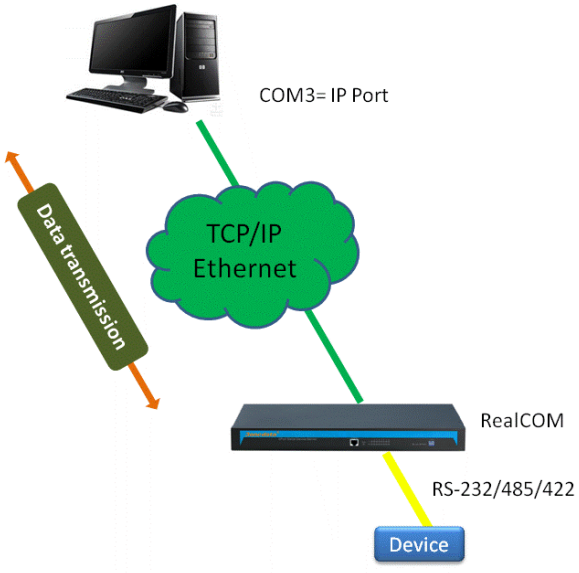
| Interface Element | Description |
|---|---|
| | • UDP Client: UDP client mode. |
| TCP lifetime | If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If not receiving any reply packet from the other after sending probing packet three times in succession, it would consider the other as offline and take the initiative to close communication connection. If it's set to "0", it means this function is disabled. The valid time range 0~65535s. |
| Packaging mode | The serial data is packaged into Ethernet data frame. The options are as follows:<br>• Mandatory time: system packages the serial data received within the specified time into Ethernet data packet to send;<br>• Interval time: after sending the last Ethernet data packet for a while, the system packages the received serial data into Ethernet data packet and sends it. |
| Packing length | The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1460. It means no limit on data transmission length when it' set to 0.<br>Notes:<br>There are some slight deviations between the actual package length value and the set value. |
| Number of delimited characters | To select the number of delimited characters. Options are as follows:<br>• 0: disable the delimited character function;<br>• 1: enable delimiter 1;<br>• 2: enable delimiter 2.<br>Notes:<br>If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network. |
| Delimiter 1 | Delimiter 1, represent in hexadecimal, the value range is 00-FF. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Delimiter 2 | Delimiter 2, represent in hexadecimal, the value range is 00-FF. |
| Delimiter processing | Select the method of delimiter processing. Options are:<br>• Retain: the system would send out the received delimiter and other data via network.<br>• Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter. |
| Transmission time | The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms.<br>Notes:<br>Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time. |

### 5.4.1 RealCom Mode




In RealCom mode, the serial port server and Windows / Linux operating system with the RealCOM drive work cooperatively. RealCom COM / TTY driver establishes a transparent network transmission connection between the host and the serial device

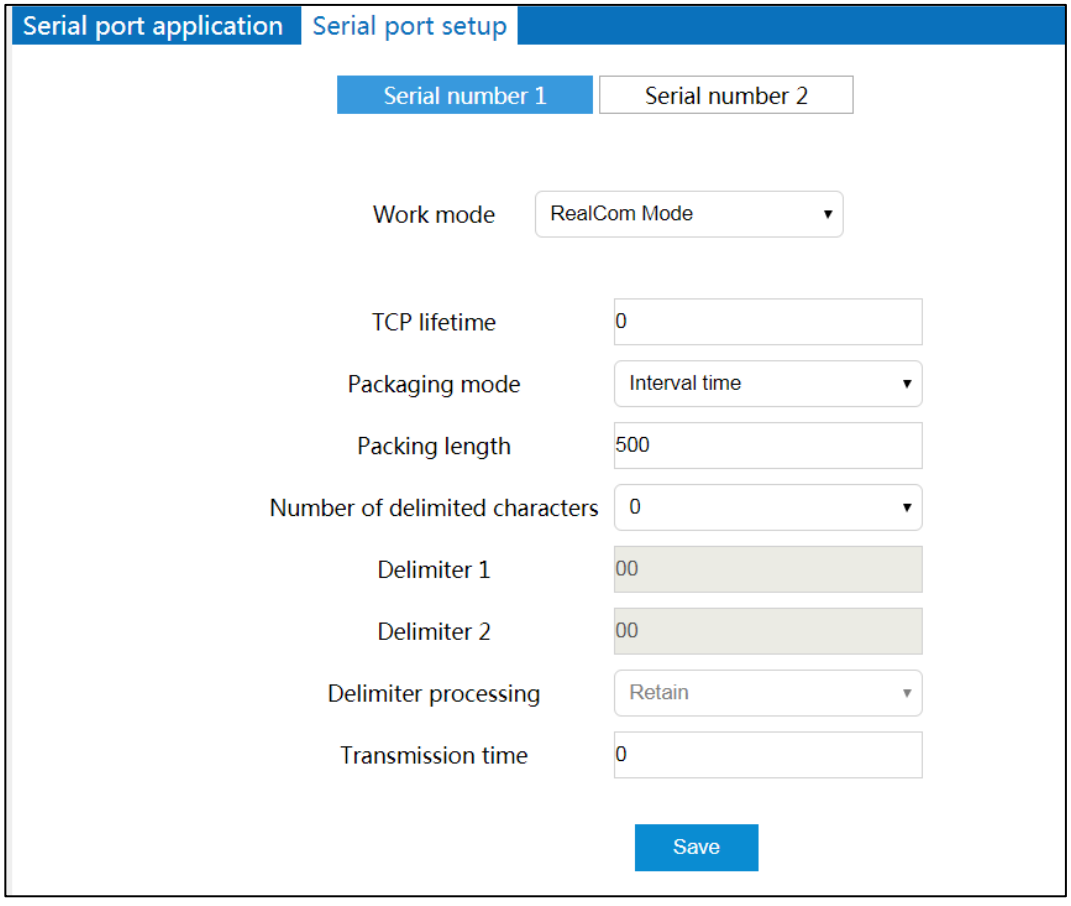


Copyright © 3onedata Co., Ltd.

in the operating system. Map the serial port of the serial port server to the local COM/TTY device of the host according to the user configured serial server IP address and serial port number and other parameters. The original serial device software or communication module without modification can be used directly without modification. The RealCom driver gets the data be sent to the local COM / TTY device of the host, then sends it over Ethernet in the form of TCP / IP packet. At the other end of the transparent transmission, the serial server will receive the TCP / IP packet and analyse the packet, and after unpacking send the original data to the serial device through the corresponding serial port, and vice versa.

## Interface Description

The serial port setup interface in RealCom Mode:






Copyright © 3onedata Co., Ltd.

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

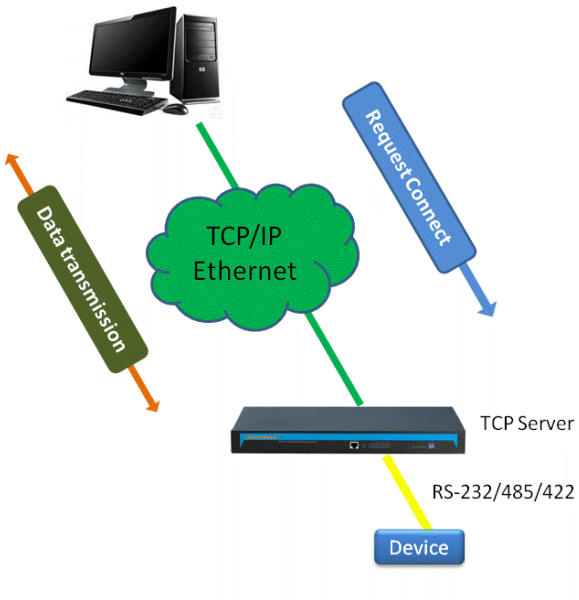
| Interface Element | Description |
|---|---|
| TCP lifetime | If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If not receiving any reply packet from the other after sending probing packet three times in succession, it would consider the other as offline and take the initiative to close communication connection. If it's set to "0", it means this function is disabled. The valid time range 0~65535s. |
| Packaging mode | The serial data is packaged into Ethernet data frame. The options are as follows:<br>• Mandatory time: system packages the serial data received within the specified time into Ethernet data packet to send;<br>• Interval time: after sending the last Ethernet data packet for a while, the system packages the received serial data into Ethernet data packet and sends it. |
| Packing length | The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1460. It means no limit on data transmission length when it' set to 0.<br>Notes:<br>There are some slight deviations between the actual package length value and the set value. |
| Number of delimited characters | To select the number of delimited characters. Options are as follows:<br>• 0: disable the delimited character function;<br>• 1: enable delimiter 1;<br>• 2: enable delimiter 2.<br>Notes:<br>If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network. |
| Delimiter 1 | Delimiter 1, represent in hexadecimal, the value range is |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | 00-FF. |
| Delimiter 2 | Delimiter 2, represent in hexadecimal, the value range is 00-FF. |
| Delimiter processing | Select the method of delimiter processing. Options are:<br>• Retain: the system would send out the received delimiter and other data via network.<br>• Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter. |
| Transmission time | The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms.<br>Notes:<br>Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time. |

## 5.4.2 TCP Server Mode




In the TCP server mode, the serial device server is assigned an IP port number, passive waiting for the host connection. When the host initiates a connection request

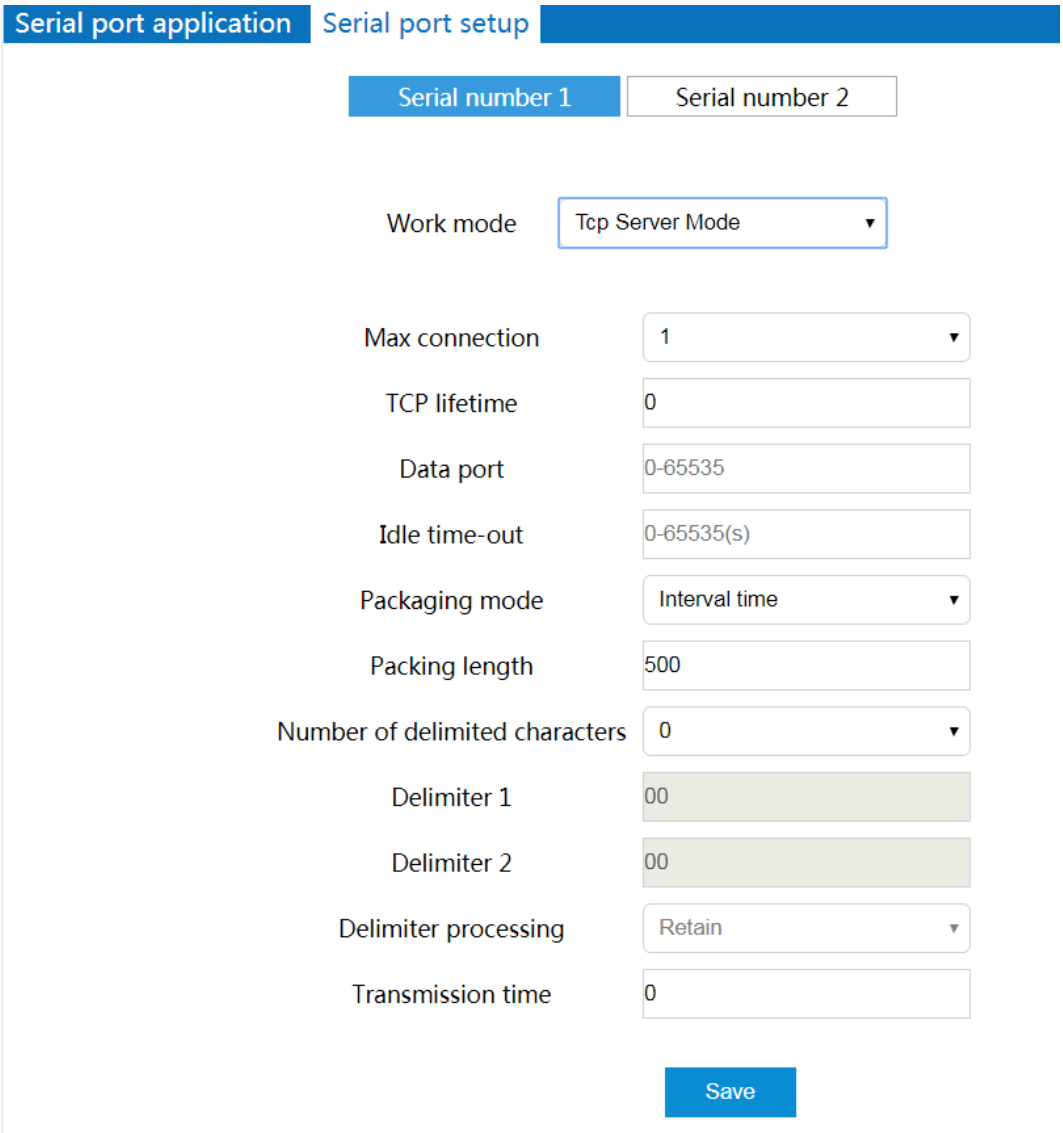


Copyright © 3onedata Co., Ltd.

and establishes a connection with the serial device server, the host can realize bidirectional transparent data transmission through the network connection and the serial port. The TCP server mode supports up to four session connections simultaneously, allowing multiple hosts to simultaneously read or send Ethernet data to a serial device.

### Interface Description

The serial port setup interface in TCP Server Mode:




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



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Max connection | The number of host that one serial port connects to.<br>• Each host communicates with serial port in the order of first-in first-out;<br>• The system supports up to 4 connections. |
| TCP lifetime | If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If not receiving any reply packet from the other after sending probing packet three times in succession, it would consider the other as offline and take the initiative to close communication connection. If it's set to "0", it means this function is disabled. The valid time range 0~65535s. |
| Data port | The destination connection port of TCP client. |
| Idle time-out | Set the idle time-out of current serial data communication link.<br>• If the idle time-out during communication is larger than 0, the system would close the TCP connection without any data transmission activity occurring in the specified time automatically;<br>• If the idle time-out is equal to 0, it means the free TCP connection would not be closed automatically. |
| Packaging mode | The serial data is packaged into Ethernet data frame. The options are as follows:<br>• Mandatory time: system packages the serial data received within the specified time into Ethernet data packet to send;<br>• Interval time: after sending the last Ethernet data packet for a while, the system packages the received serial data into Ethernet data packet and sends it. |
| Packing length | The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1460. It means no limit on data transmission length when it' set to 0.<br>Notes:<br>There are some slight deviations between the actual package length value and the set value. |
| Number of | To select the number of delimited characters. Options are as |



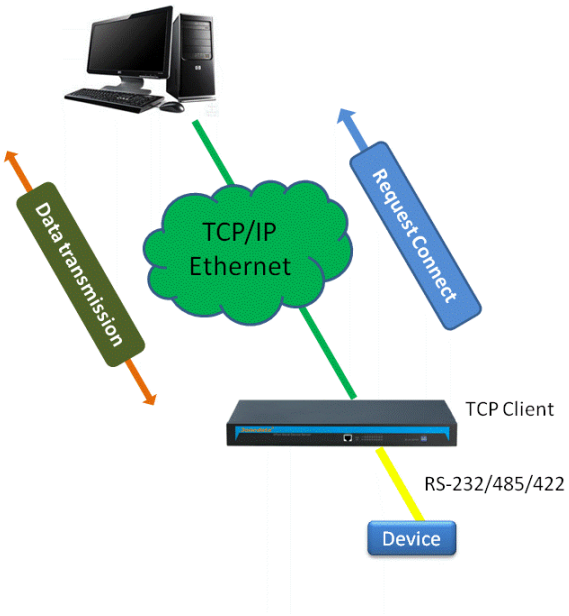
Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| delimited characters | follows:<br>• 0: disable the delimited character function;<br>• 1: enable delimiter 1;<br>• 2: enable delimiter 2.<br>Notes:<br>If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network. |
| Delimiter 1 | Delimiter 1, represent in hexadecimal, the value range is 00-FF. |
| Delimiter 2 | Delimiter 2, represent in hexadecimal, the value range is 00-FF. |
| Delimiter processing | Select the method of delimiter processing. Options are:<br>• Retain: the system would send out the received delimiter and other data via network.<br>• Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter. |
| Transmission time | The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms.<br>Notes:<br>Setting the transmission time to 0 means no limit on data transmission interval time or not to enable forced time. |

## 5.4.3 TCP Client Mode



Copyright © 3onedata Co., Ltd.



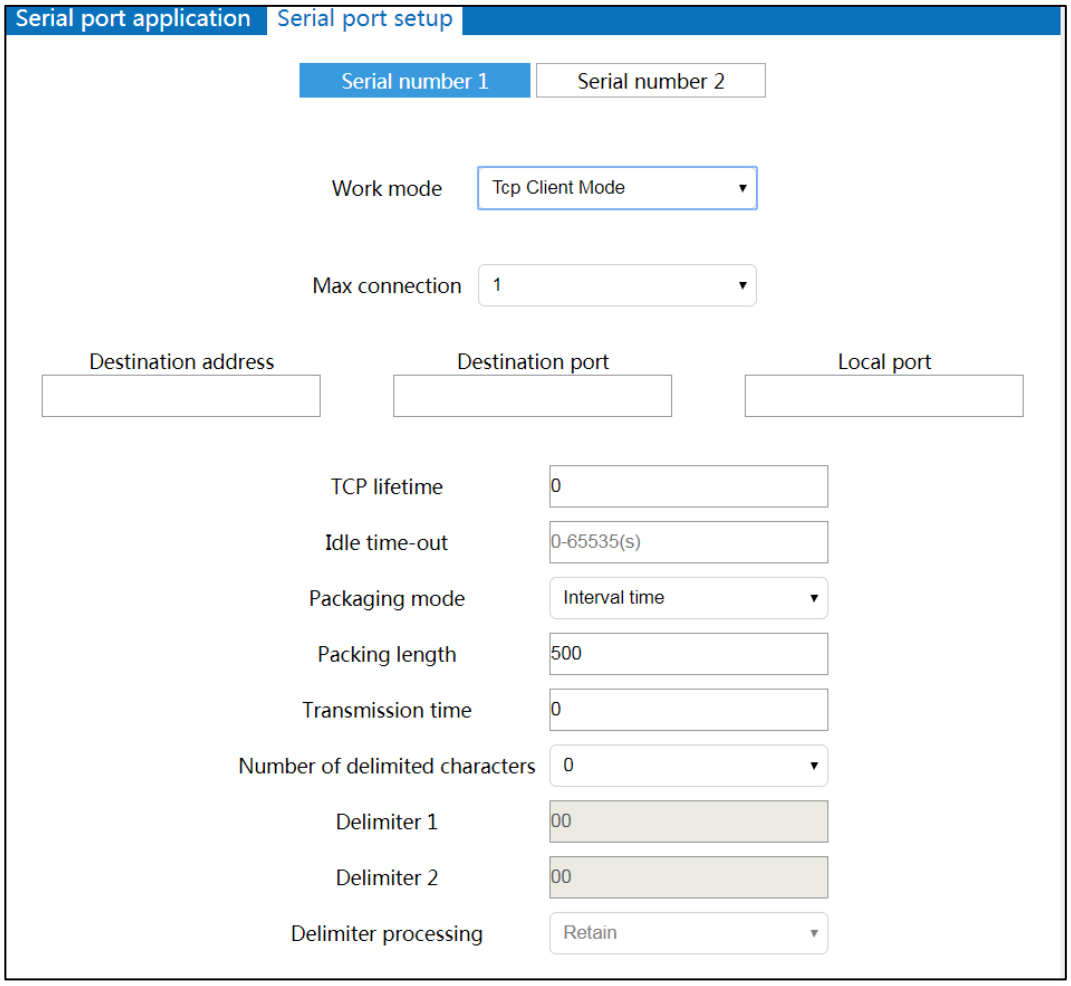

In the TCP client mode, the serial device server can automatically establish a network connection with the host specified by the user when the serial data arrives. When the data transmission is completed, the serial server will automatically shut down the network connection according to the parameters such as TCP alive time and TCP idle timeout time. Similarly, TCP client mode can support up to four session connections at the same time, so that multiple hosts can simultaneously read or send Ethernet data to a serial device.

### Interface Description

The serial port setup interface in TCP Client Mode:



Copyright © 3onedata Co., Ltd.




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

| Interface Element | Description |
|---|---|
| Max connection | The number of host that one serial port connects to.<br>• Each host communicates with serial port in the order of first-in first-out;<br>• The system supports up to 4 connections. |
| Destination address | Enter the IP address of the server that would be connected to serial port. |
| Destination port | Enter the TCP port number of the server that would be connected to serial port. |
| Local port | The local port allocated for TCP connection by the system, which could offer service or connection for the outside world, |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | used for connecting and communicating with server. |
| TCP lifetime | If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If not receiving any reply packet from the other after sending probing packet three times in succession, it would consider the other as offline and take the initiative to close communication connection. If it's set to "0", it means this function is disabled. The valid time range 0~65535s. |
| Idle time-out | Set the idle time-out of current serial data communication link.<br>• If the idle time-out during communication is larger than 0, the system would close the TCP connection without any data transmission activity occurring in the specified time automatically;<br>• If the idle time-out is equal to 0, it means the free TCP connection would not be closed automatically. |
| Packaging mode | The serial data is packaged into Ethernet data frame. The options are as follows:<br>• Mandatory time: system packages the serial data received within the specified time into Ethernet data packet to send;<br>• Interval time: after sending the last Ethernet data packet for a while, the system packages the received serial data into Ethernet data packet and sends it. |
| Packing length | The frame length of serial data to Ethernet data. In the set time range, the data forwards when it is greater than or equals to the set frame length. The value range is 0~1460. It means no limit on data transmission length when it' set to 0.<br>Notes:<br>There are some slight deviations between the actual package length value and the set value. |
| Transmission time | The time parameters in the packaging mode of forced time or interval time. The value range is 0-65535ms.<br>Notes:<br>Setting the transmission time to 0 means no limit on data |



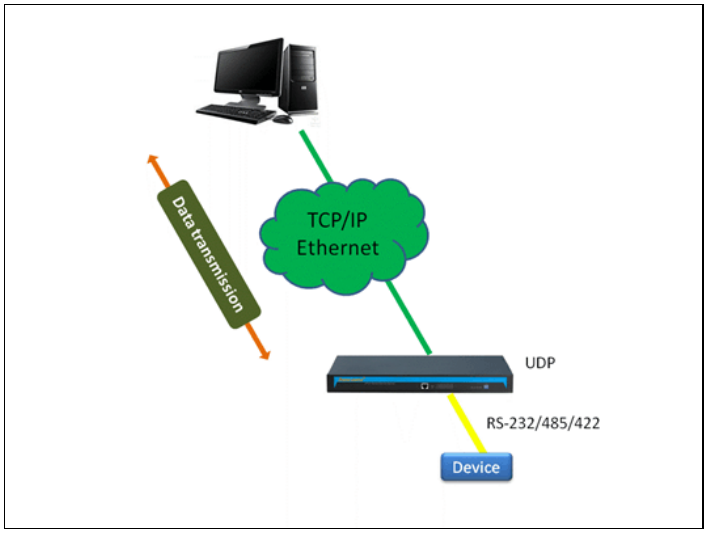
Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | transmission interval time or not to enable forced time. |
| Number of delimited characters | To select the number of delimited characters. Options are as follows:<br>• 0: disable the delimited character function;<br>• 1: enable delimiter 1;<br>• 2: enable delimiter 2.<br>Notes:<br>If the packaging length or the forced transfer time is 0 and the number of delimited character is greater than 0, the system would detect and process the delimiter after receiving serial data. Every time it receives matched delimiter (or combination of characters), the system would send out all cached serial data via network. |
| Delimiter 1 | Delimiter 1, represent in hexadecimal, the value range is 00-FF. |
| Delimiter 2 | Delimiter 2, represent in hexadecimal, the value range is 00-FF. |
| Delimiter processing | Select the method of delimiter processing. Options are:<br>• Retain: the system would send out the received delimiter and other data via network.<br>• Delete: the matched delimiter (or combination of delimiter) would be deleted. The system only transmits data except delimiter. |

### 5.4.4 UDP Server Mode



Copyright © 3onedata Co., Ltd.



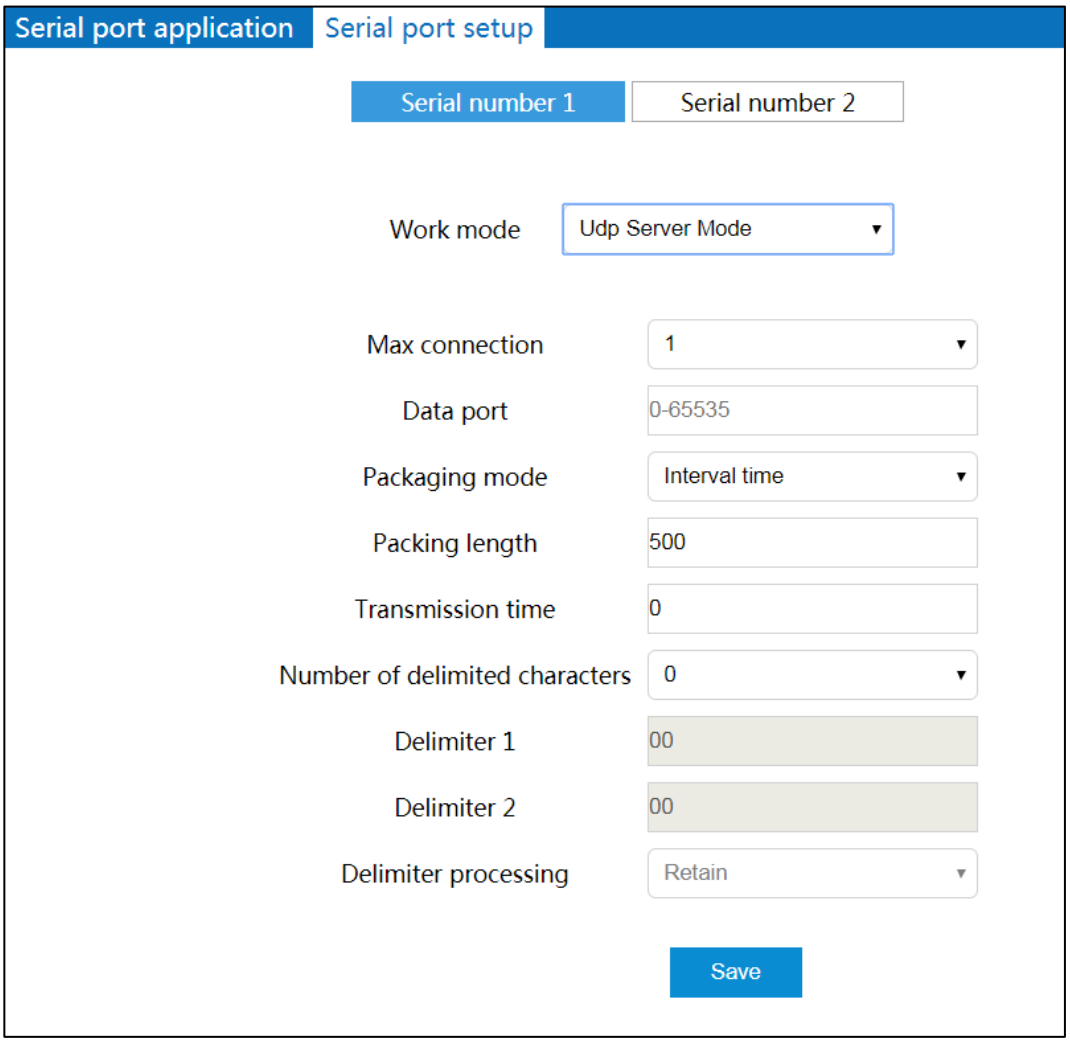

In UDP server mode, the serial server through the UDP protocol and user-specified host for serial data transmission. UDP mode serial device server can transfer data from the serial device to one or more hosts, and the serial device server can also receive data from one or more hosts. Compared with TCP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

### Interface Description

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



Copyright © 3onedata Co., Ltd.




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

| Interface Element | Description |
|---|---|
| Max connection | The number of hosts connected to a serial port at the same time.<br>• Each host communicates with the serial port in the order of “first-in, first-out”.<br>• The system supports up to 4 connections. |
| Data port | The data port on which the network receives UDP data. The user must assign a unique data port to each serial port for the system to receive UDP data normally. |
| Packaging mode | The serial port data is packaged as an Ethernet data frame. |



Copyright © 3onedata Co., Ltd.

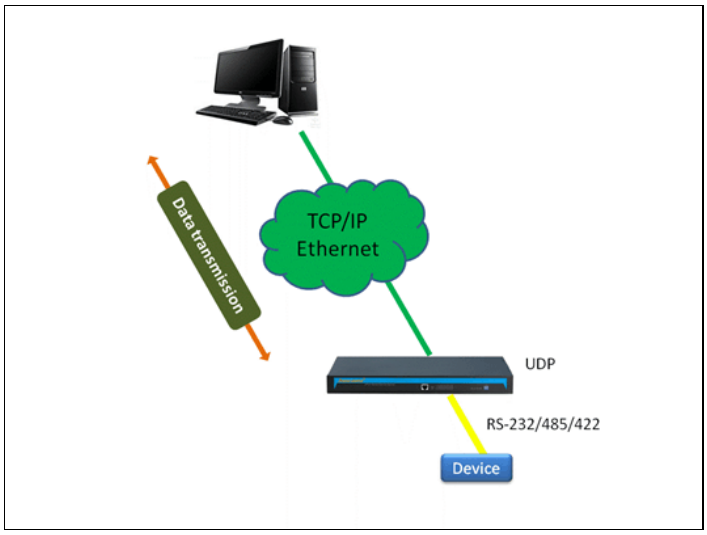
| Interface Element | Description |
|---|---|
| | The options are as follows:<br>• Mandatory time: The system packs the serial port data received within the specified time into Ethernet packets and sends them out.<br>• Interval time: After sending an Ethernet packet for a period of time, the system will package the received serial data into Ethernet packets for transmission. |
| Packing length | The frame length of the serial data to Ethernet data, the data frame is forwarded within the set time range when it is greater than or equal to the set frame length. The value ranges from 0 to 1460. Set to 0 indicates that the data transfer length is not limited.<br>Notes:<br>The actual package length value has a small deviation from the set value. |
| Transmission time | The time parameter in the packaging mode of mandatory time or interval time, ranging from 0 to 65535ms.<br>Notes:<br>The transmission time is set to 0, which means that the data transmission interval is not limited or the mandatory time is disabled. |
| Number of delimited characters | Select the number of delimited characters. The options are as follows:<br>• 0: Disable the delimiter;<br>• 1: Enable delimiter 1;<br>• 2: Enable delimiter 2.<br>Notes:<br>If the package length or mandatory transfer time is 0 and the number of delimited characters is greater than 0, the system will detect the delimiter after receiving the serial data. Whenever a matching delimiter character (or combination of characters) is received, the system will immediately transfer all cached serial data over the network. |
| Delimiter 1 | The delimiter 1 is expressed in hexadecimal, value range is 00-FF. |
| Delimiter 2 | The delimiter 2 is expressed in hexadecimal, value range is 00-FF. |
| Delimiter | Select the character processing method. The options are:<br>• Retain: The system transmits the received delimiter |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| processing | characters along with other data over the network.<br>• Delete: The matching delimiter character (or combination of characters) will be deleted, and the system will only transmit data other than the delimiter. |

## 5.4.5 UDP Client Mode



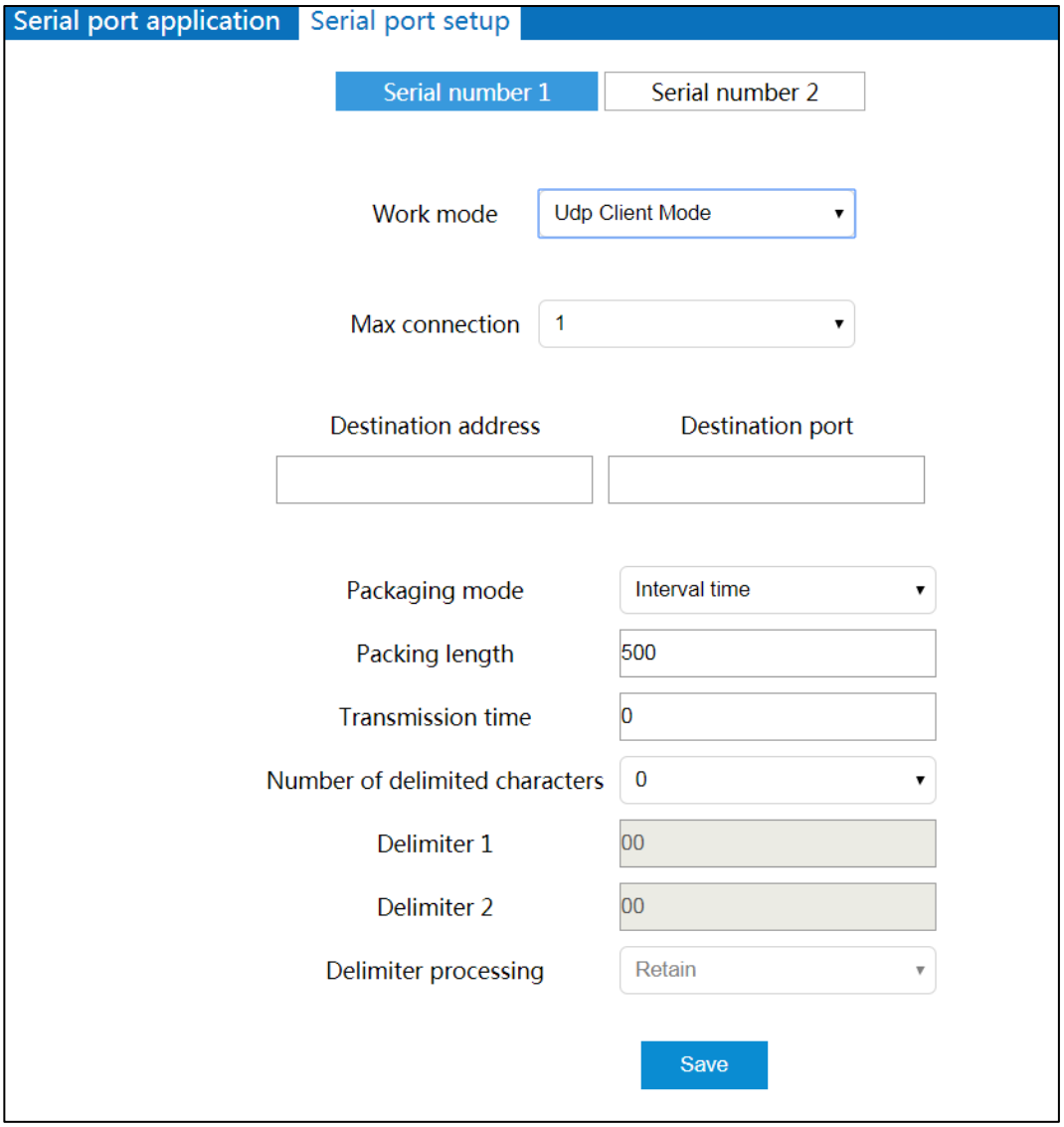

In UDP Client mode, the serial server through the UDP protocol and user-specified host for serial data transmission. UDP mode serial device server can transfer data from the serial device to one or more hosts, and the serial device server can also receive data from one or more hosts. Compared with TCP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

### Interface Description

Screenshot of the serial settings interface in UDP Client Mode:



Copyright © 3onedata Co., Ltd.




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

| Interface Element | Description |
|---|---|
| Max connection | The number of hosts connected to a serial port at the same time.<br>• Each host communicates with the serial port in the order of “first-in, first-out”.<br>• The system supports up to 4 connections. |
| Destination address | Enter the IP address of the opposite host that serial port needs to be connected to. |
| Destination port | Enter the port number of the opposite host that serial port |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | needs to be connected to. |
| Packaging mode | The serial port data is packaged as an Ethernet data frame. The options are as follows:<br>• Mandatory time: The system packs the serial port data received within the specified time into Ethernet packets and sends them out.<br>• Interval time: After sending an Ethernet packet for a period of time, the system will package the received serial data into Ethernet packets for transmission. |
| Packing length | The frame length of the serial data to Ethernet data, the data frame is forwarded within the set time range when it is greater than or equal to the set frame length. The value ranges from 0 to 1460. Set to 0 indicates that the data transfer length is not limited.<br>Notes:<br>The actual package length value has a small deviation from the set value. |
| Number of delimited characters | Select the number of delimited characters. The options are as follows:<br>• 0: Disable the delimiter;<br>• 1: Enable delimiter 1;<br>• 2: Enable delimiter 2.<br>Notes:<br>If the package length or mandatory transfer time is 0 and the number of delimited characters is greater than 0, the system will detect the delimiter after receiving the serial data. Whenever a matching delimiter character (or combination of characters) is received, the system will immediately transfer all cached serial data over the network. |
| Transmission time | The time parameter in the packaging mode of mandatory time or interval time, ranging from 0 to 65535ms.<br>Notes:<br>The transmission time is set to 0, which means that the data transmission interval is not limited or the mandatory time is disabled. |
| Delimiter 1 | The delimiter 1 is expressed in hexadecimal, value range is 00-FF. |
| Delimiter 2 | The delimiter 2 is expressed in hexadecimal, value range is |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | 00-FF. |
| Delimiter processing | Select the character processing method. The options are:<br>• Retain: The system transmits the received delimiter characters along with other data over the network.<br>• Delete: The matching delimiter character (or combination of characters) will be deleted, and the system will only transmit data other than the delimiter. |

## 5.5 UPnP Settings

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

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

### Function Description

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

### Operation Path

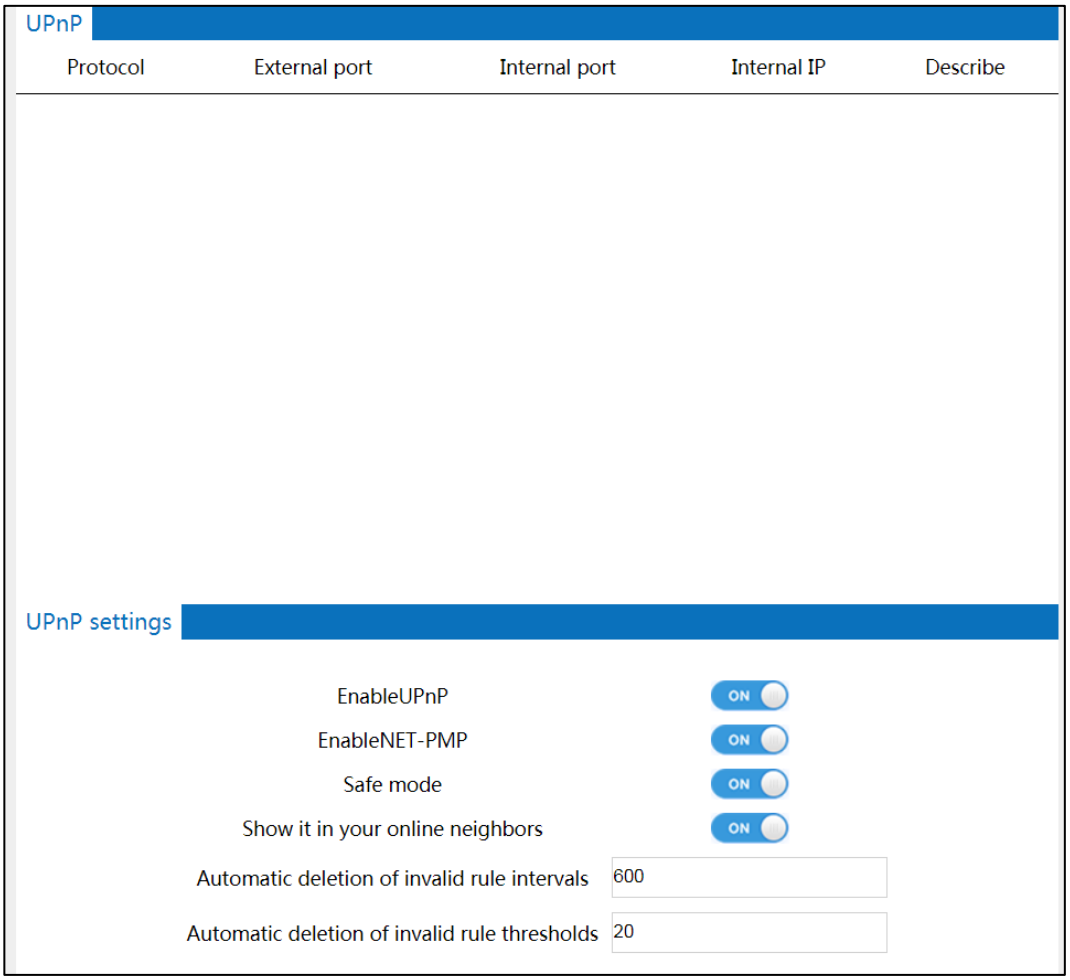
Open in order: "Advanced Network > UPnP Settings".

### Interface Description

UPnP settings interface as follows:



Copyright © 3onedata Co., Ltd.




The main element configuration description of UPnP settings interface:

| Interface Element | Description |
|---|---|
| **UPnP** | **UPnP list column** |
| 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. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| **UPnP Settings** | **UPnP Settings Column** |
| Enable UPnP | UPnP enablement switch, click the right button for ON and OFF switching.<br>• ON;<br>• OFF. |
| Enable NAT-PMP | NAT-PMP enablement switch, click the right button for ON and OFF switching.<br>• ON: After the NAT-PMP function is enabled, the router allows the NAT LAN host to communicate with external devices to automate port conversion;<br>• OFF. |
| Safe mode | Enablement switch of safe mode, click the right button for ON and OFF switching.<br>• ON: After the safe mode is enabled, the client can only forward an input port to itself;<br>• OFF. |
| Show it in your online neighbors | Show enablement switch in the online neighbor; click the right button for ON and OFF switching.<br>• ON: The device can be found in the PC online neighbor or network device;<br>• OFF. |
| Automatic deletion of invalid rule intervals | The system automatically deletes the invalid UPnP rules list after the specified interval, unit: second. |
| Automatic deletion of invalid rule thresholds | The system automatically deletes the invalid UPnP rules list after the quantity of invalid UPnP rules reaches the threshold. |

## 5.6 VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. In general, all hosts in a network will set a default route, when the destination address of the message sent by host isn't in the network segment; the message will be sent to the Router A via default router, achieving the communication between the host and



Copyright © 3onedata Co., Ltd.

external network. When the Router A breaks down, all hosts that takes Router A as default router in the network segment will disconnect communication to the outside, generating single point of failure.VRRP is proposed to solve the problem above, and it's designed for the local area network (such as: Ethernet) with multicast or broadcast capability.

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

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 repeated 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 receive announce with 0 priority.



**Copyright © 3onedata Co., Ltd.**

In the VRRP router group, master router is elected according to the priority, and 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.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

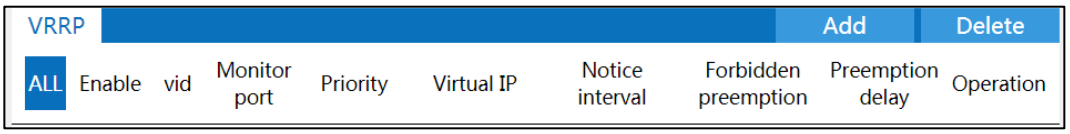
On the page of VRRP, user can configure VRRP parameters.

## Operation Path

Open in order: "Advanced Network > VRRP".

## Interface Description

The VRRP interface as follows:




The main elements configuration description of VRRP interface:

| Interface Element | Description |
|---|---|
| Enable | VRRP function status is displayed, options include:<br>• ON<br>• OFF |
| Vid | Identity of the virtual router is displayed. |
| Monitor port | Monitor ports of the device is displayed, options include:<br>• Br-lan<br>• Eth1 |
| Virtual IP | The IP address of the virtual router is displayed. |
| Notice interval | Interval at which Master device sends VRRP notice |



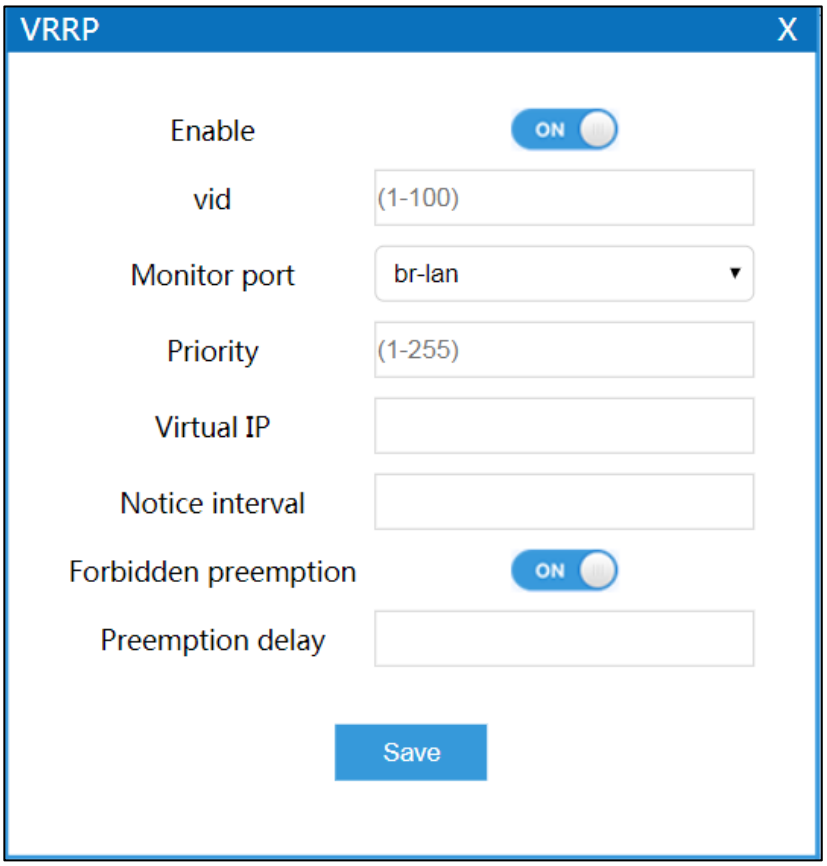
Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | 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:<br>• ON<br>• 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:




The main elements configuration description of VRRP-Add interface:



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Enable | 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:<br>• Br-lan: LAN port as the monitor port;<br>• Eth1: 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 | Notice interval, the 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.<br>• 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;<br>• 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. |
| Preemption delay | The delay time of switching from Backup device to Master device, the valid range is 1-1000 seconds.<br>Notes:<br>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. |



Copyright © 3onedata Co., Ltd.

# 5.7 RIP

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

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

## Function Description

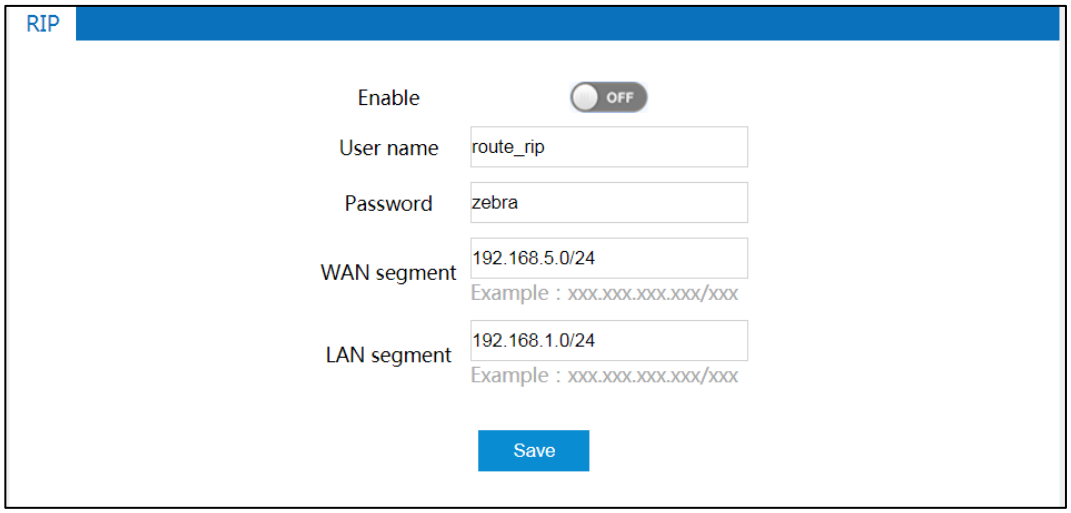
On the page of "RIP", user can configure the RI related parameters.

## Operation Path

Open in order: "Advanced Network > RIP".

## Interface Description

The RIP interface as follows:




The main elements configuration description of RIP interface:

| Interface Element | Description |
|---|---|
| Enable | RIP enablement switch; click the right button for ON and OFF switching.<br>• ON: Enable RIP default configuration;<br>• OFF. |
| User name | User name used to log in to the RIP command line configuration. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Password | Password used to log in to the RIP command line configuration. |
| WAN segment | WAN segment information. |
| LAN segment | LAN segment information. |

# 5.8 OSPF

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

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

### Function Description

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

### Operation Path

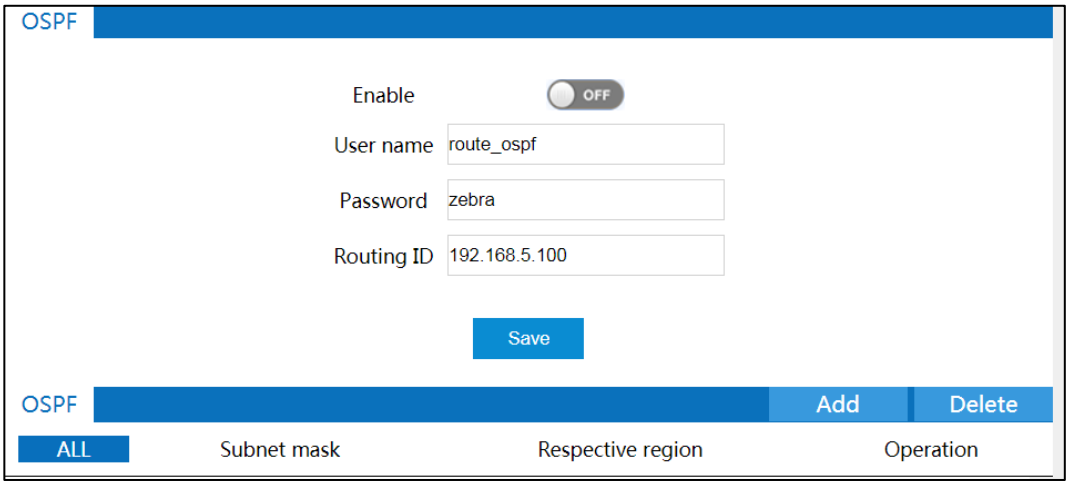
Open in order: "Advanced Network > OSPF".

### Interface Description

The OSPF interface as follows:



Copyright © 3onedata Co., Ltd.




The main elements configuration description of OSPF interface:

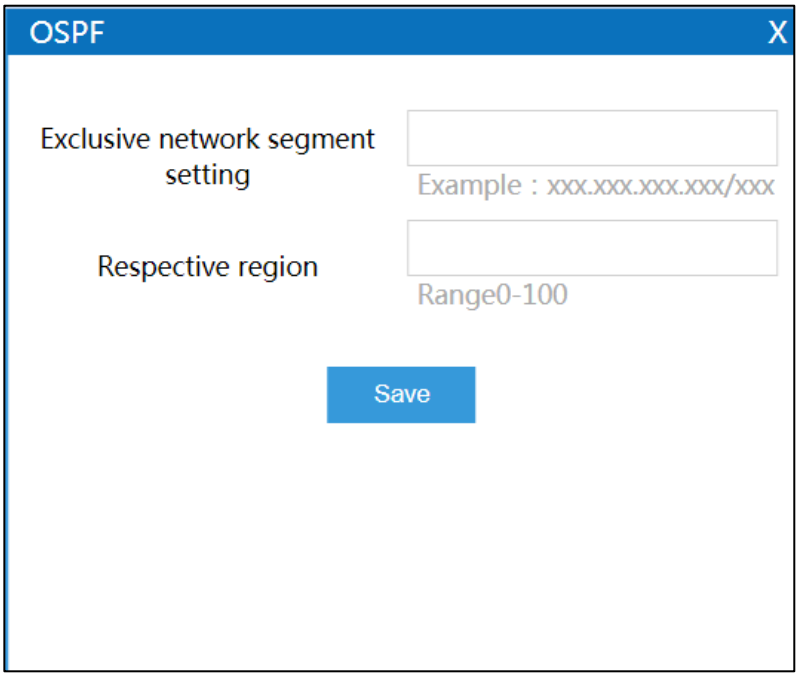
| Interface Element | Description |
|---|---|
| **OSPF** | **OSPF Configuration Column** |
| Enable | OSPF enablement switch, click the right button for ON and OFF switching.<br>• ON: Enable OSPF default configuration;<br>• OFF. |
| User name | User name used to log in to the OSPF command line configuration. |
| 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. |
| **OSPF** | **OSPF Configuration Column** |
| 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: OSPF-Add

The OSPF-Add interface as follows:



Copyright © 3onedata Co., Ltd.




The main elements configuration description of OSPF-Add interface:

| Interface Element | Description |
|---|---|
| Dedicated 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. |
| Respective region | The area number of the device. OSPF protocol divides the autonomous system into different areas, the valid range is 0-4294967295. |

# 5.9 Static DHCP

### Function Description

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



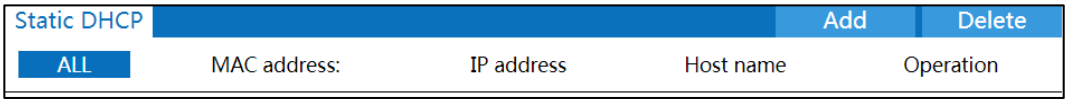
Copyright © 3onedata Co., Ltd.

## Operation Path

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

## Interface Description

Static DHCP interface as follows:

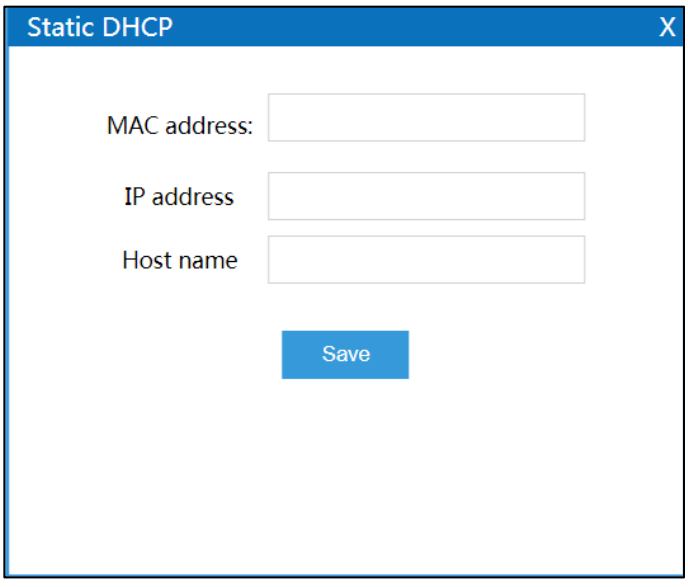



The main elements configuration description of static DHCP interface:

| Interface Element | Description |
|---|---|
| MAC address | MAC address of the DHCP client. |
| IP address | IP address bound to the MAC address of DHCP client. |
| Host name | The name of DHCP client. |
| Operation | Edit the static DHCP list. |

## Interface Description: Static DHCP - Add

Static DHCP-Add interface as follows:




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

| Interface Element | Description |
|---|---|
| MAC address | MAC address of the DHCP client, the format is |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | 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. |



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

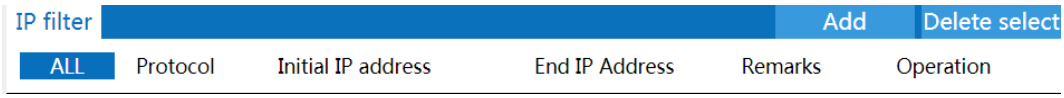
On the "IP filter" page of firewall, user can check or add IP filter to forbid the communication between the clients in LAN and WAN.

### 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 | IP filter check box, click "ALL" to check all IP filter entries. |
| Protocol | Protocols used by data packets. |
| IP start | Start IP address of LAN IP address range filtered by the |



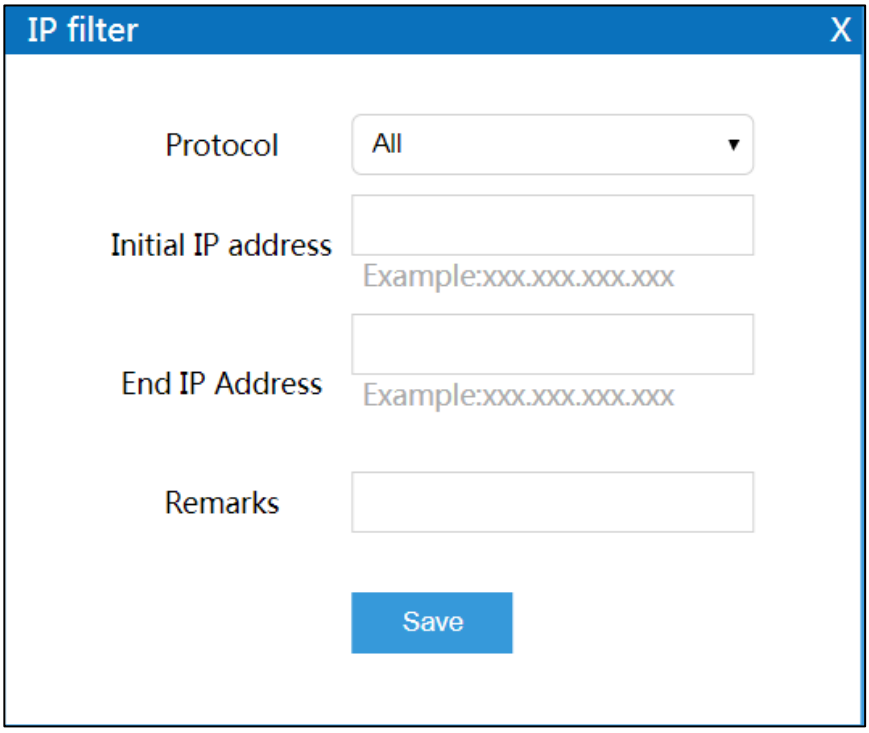
Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | device. |
| IP end | End IP address of LAN IP address range filtered by the device. |
| Remarks | Remarks of IP filter entries. |
| Operation | Edit: modify the filter entries information. |

### Interface Description: Add IP Filter Entry

Click "Add" to increase IP filter entry.

IP filter interface as follows:




The main element configuration description of IP filter interface:

| Interface Element | Description |
|---|---|
| Protocol | Drop-down list of data packet protocol, options as follows:<br>• ALL;<br>• TCP;<br>• UDP. |
| Start IP address | Start IP address of LAN IP address range filtered by the device, such as: 192.168.1.123. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| End IP address | End IP address of LAN IP address range filtered by the device, such as: 192.168.1.123. |
| Remarks | Remarks of IP filter list support 10 Chinese characters or 32 valid characters, optional. |

# 6.2 MAC Filter

### Function Description

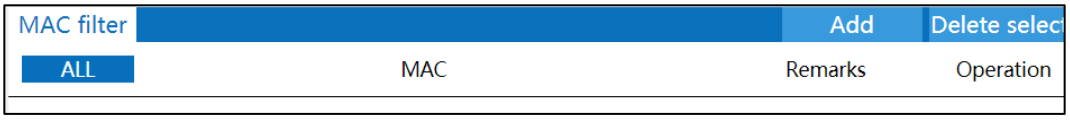
On the "MAC filter" page of firewall, user can check or add MAC filter to forbid the communication between the clients in LAN and WAN; it can effectively control the WAN access rights of user in LAN.

### Operation Path

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 | MAC filter check box, click "ALL" 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 filter entries information. |

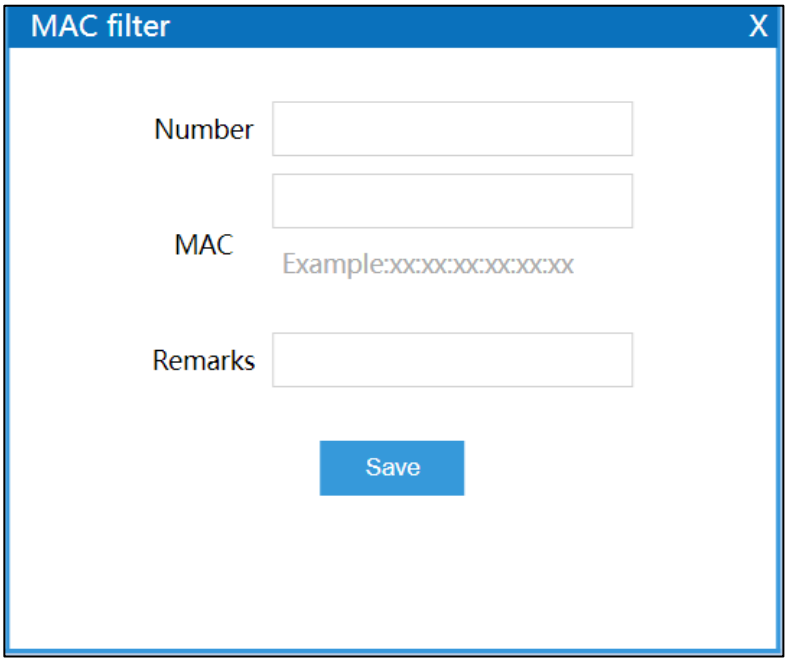
### Interface Description: Add MAC Filter Entry

Click "Add" to increase MAC filter entry.

MAC filter interface as follows:



Copyright © 3onedata Co., Ltd.




The main element configuration description of MAC filter interface:

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

## 6.3 URL Filter

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

### Function Description

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



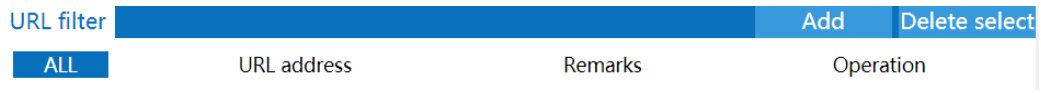
Copyright © 3onedata Co., Ltd.

## Operation Path

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

## Interface Description

URL filter interface as follows:



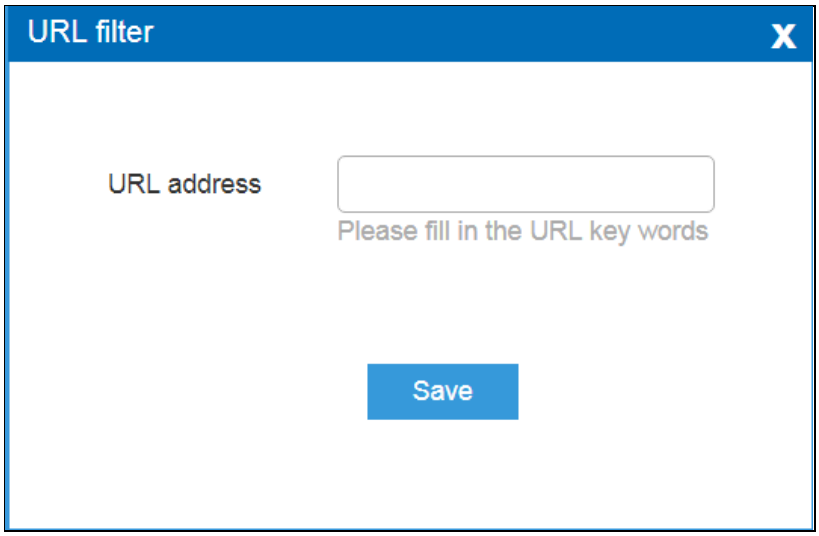

The main element configuration description of URL filter interface:

| Interface Element | Description |
|---|---|
| ALL | URL filter check box, click "ALL" to check all URL filter entries. |
| URL | URL address in LAN filtered by the device. |
| Operation | Edit: modify the filter list. |

## Interface Description: Add URL Filter List

Click "Add" to increase URL filter list.

URL filter interface as follows:




The main element configuration description of URL filter interface:

| Interface Element | Description |
|---|---|
| URL address | URL address in WAN filtered by the device, ending with ".com", ".cn" and so on. Such as: sina. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Remarks | Remarks of the URL filtering entry, it supports 32 valid characters or 10 Chinese characters, and can be left blank. |

# 6.4 Keyword Filter

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

### Function Description

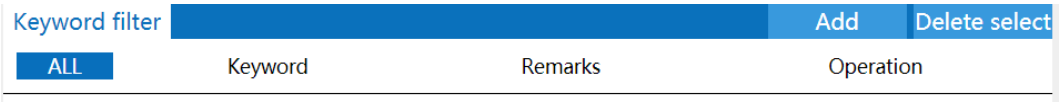
On the page of "Keyword filter" of the firewall, user can view or add keyword filtering entries to prevent clients on the LAN from accessing to the network address corresponding to the keywords in the WAN.

### Operation Path

Open in order: "Firewall > Keyword Filter".

### Interface Description

Keyword filter interface as follows:




The main elements configuration description of keyword filter interface:

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

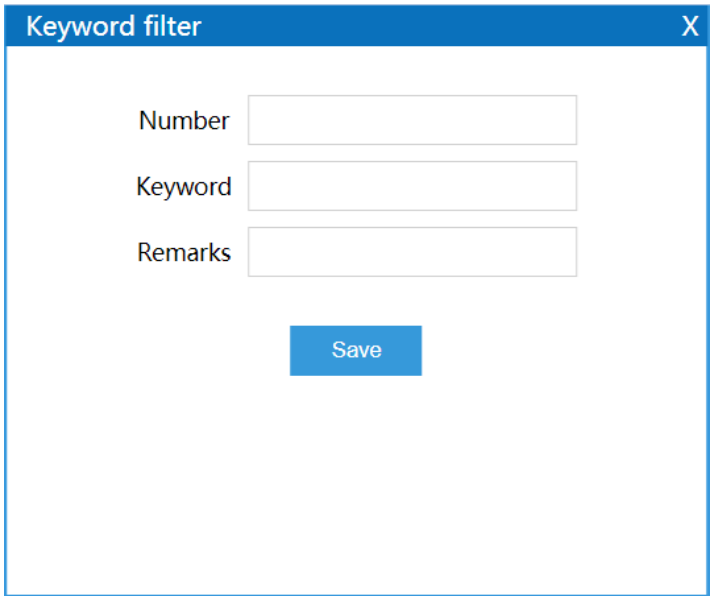
### Interface Description: Add keyword filtering entry

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

Keyword filter interface as follows:



Copyright © 3onedata Co., Ltd.




The main elements configuration description of keyword filter interface:

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



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 adopts Tunnel technology and is the third layer tunneling protocol of Virtual Private Network (VPN).

### Function Description

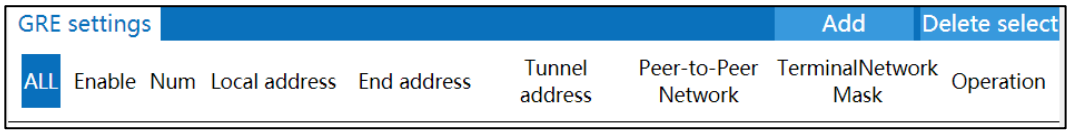
On the page of "GRE Settings", user can configure the relevant parameters of GRE.

### 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:



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| ALL | Check box of GRE settings entries, click "ALL" to select all GRE settings entries. |
| Enable | GRE settings is enabled or not:<br>• ON<br>• 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 in the upper right corner 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.



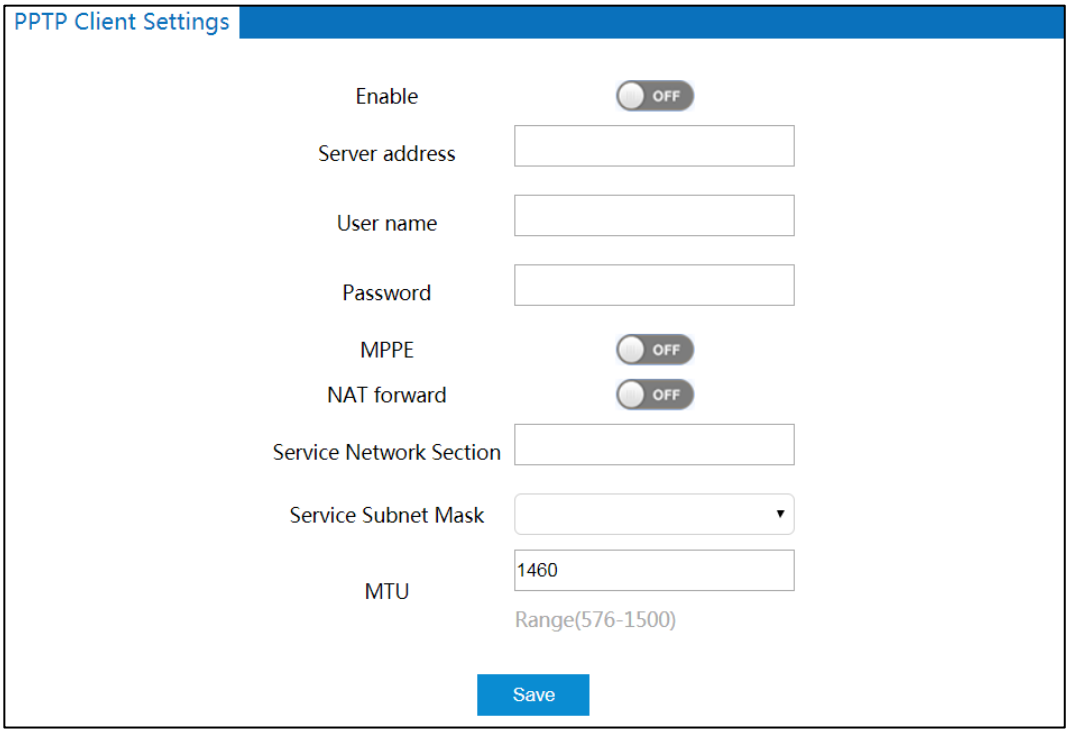
Copyright © 3onedata Co., Ltd.

## Operation Path

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

## Interface Description

The PPTP client settings interface is as follows:




The main elements configuration description of PPTP client settings interface:

| Interface Element | Description |
|---|---|
| Enable | Functional enablement switch of PPTP client settings, click the right button for ON and OFF switching.<br>• ON: Enable the PPTP client settings function;<br>• OFF: Disable 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 switch of MPPE (Microsoft Point-to-Point Encryption) protocol, click the right button for ON and OFF switching. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • ON: Enable MPPE encryption;<br>• OFF: Disable MPPE encryption. |
| NAT forward | Functional enablement switch of Network Address Translation (NAT) forwarding, click the right button for ON and OFF switching.<br>• ON: Enable NAT forwarding. All data flows of the client are forwarded through the VPN server;<br>• OFF: Disable NAT forwarding. |
| Service Network Section | Subnet segment of the PPTP server |
| Service Subnet Mask | Drop-down box of subnet mask of the PPTP server |
| MTU | Maximum Transmission Unit (MTU) input box, unit is byte, the default value is 1460, and the recommended value range is 1400-1500. |

# 7.3 PPTP Server Settings

### Function Description

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

### Operation Path

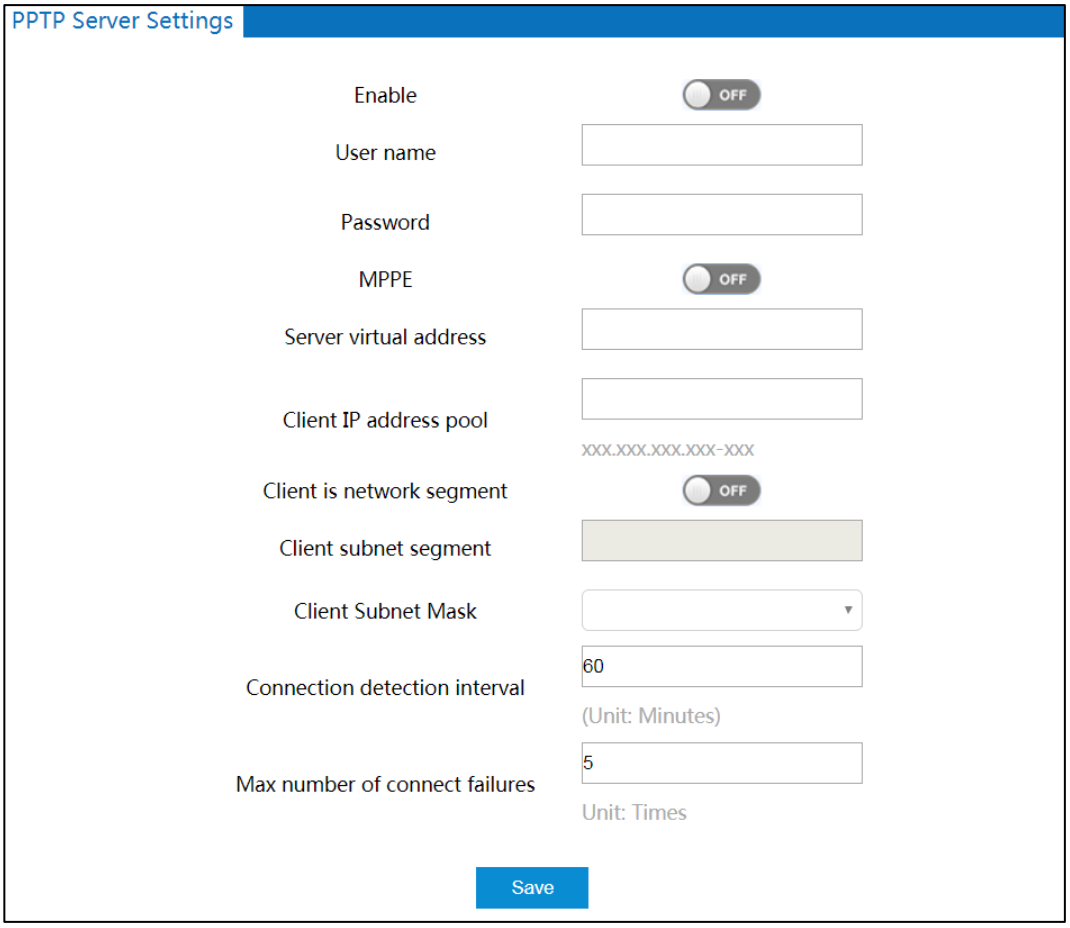
Open in order: "VPN tunnel > PPTP Server Settings".

### Interface Description

The PPTP server settings interface is as follows:



Copyright © 3onedata Co., Ltd.




The main elements configuration description of PPTP server settings interface:

| Interface Element | Description |
|---|---|
| Enable | Functional enablement switch of PPTP server settings, click the right button for ON and OFF switching.<br>• ON: Enable the PPTP server settings function;<br>• OFF: Disable 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 switch of Microsoft Point-to-Point Encryption (MPPE) protocol, click the right button for ON and OFF switching.<br>• ON: Enable MPPE encryption;<br>• OFF: Disable MPPE encryption. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Server virtual address | Virtual IP address of PPTP server |
| Client IP address pool | IP address pool range assigned to the client, the format is: xxx.xxx.xxx.xxx-xxx |
| Client is network segment | The client is network segment enablement switch, 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.<br>• ON: Enable the function of the client as network segment, and input the subnet segment and mask of the client;<br>• 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.<br>Notes:<br>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<br>Notes:<br>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



Copyright © 3onedata Co., Ltd.

multiple tunnels; L2TP provides header compression and tunnel authentication, but PPTP does not support.

## Function Description

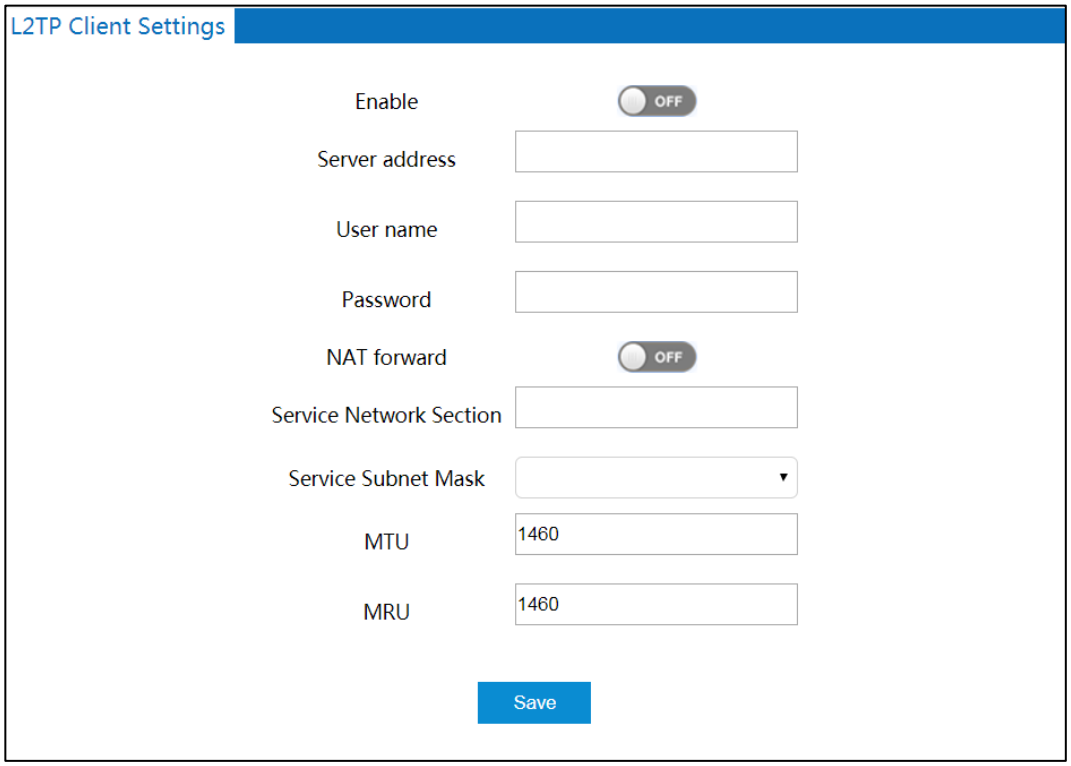
On the page of "L2TP Client Settings", user can configure the parameters related to L2TP client.

## Operation Path

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

## Interface Description

The L2TP client settings interface is as follows:




The main elements configuration description of L2TP client settings interface:

| Interface Element | Description |
|---|---|
| Enable | Functional enablement switch of L2TP client settings, click the right button for ON and OFF switching.<br>• ON: Enable the L2TP client settings function;<br>• OFF: Disable the L2TP client settings function. |
| Server address | IP address of L2TP server |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| User name | User name allowed by L2TP server |
| Password | Password corresponding to the user name allowed by L2TP server |
| NAT forward | Functional enablement switch of Network Address Translation (NAT) forwarding, click the right button for ON and OFF switching.<br>• ON: Enable NAT forwarding. All data flows of the client are forwarded through the VPN server;<br>• OFF: Disable NAT forwarding. |
| 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 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

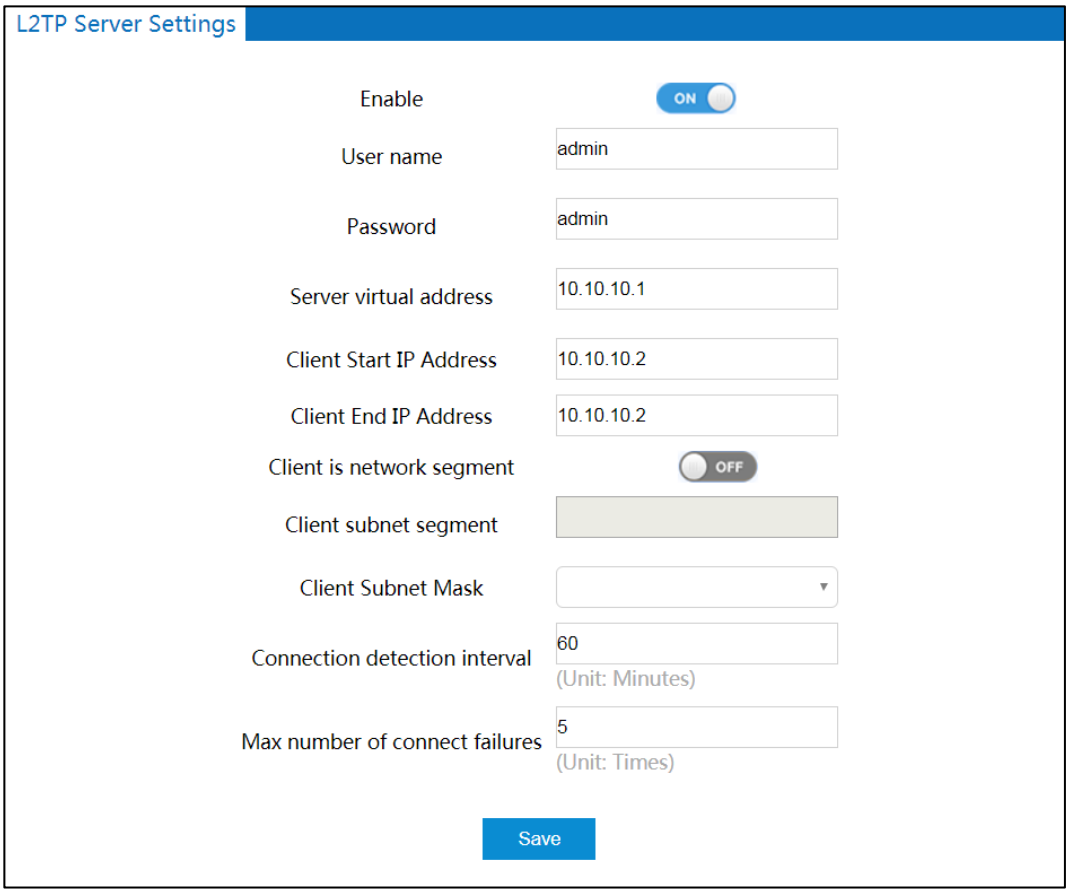
Open in order: "VPN tunnel > L2TP Server Settings".

### Interface Description

The L2TP server settings interface is as follows:



Copyright © 3onedata Co., Ltd.




The main elements configuration description of L2TP server settings interface:

| Interface Element | Description |
|---|---|
| Enable | Functional enablement switch of L2TP server settings, click the right button for ON and OFF switching.<br>• ON: Enable the L2TP server settings function;<br>• OFF: Disable the L2TP server settings function. |
| User name | User name provided by L2TP to the client for connection |
| Password | Password corresponding to the user name provided by L2TP to the client for connection |
| Server virtual address | Virtual IP address of L2TP server |
| Client Start IP address | Minimum start IP address of L2TP client |
| Client End IP Address | Maximum end IP address of L2TP client |
| Client is network segment | Enablement switch of the client as network segment, it allows the router whose subnet is the network segment to connect as a client and access the L2TP VPN server. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | Click the right button for ON and OFF switching.<br>• ON: Enable the function of the client as network segment, and input the subnet segment and mask of the client;<br>• 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.<br>Notes:<br>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<br>Notes:<br>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



Copyright © 3onedata Co., Ltd.

captured packet, that is, the receiver rejects old or duplicate packets.

## Function Description

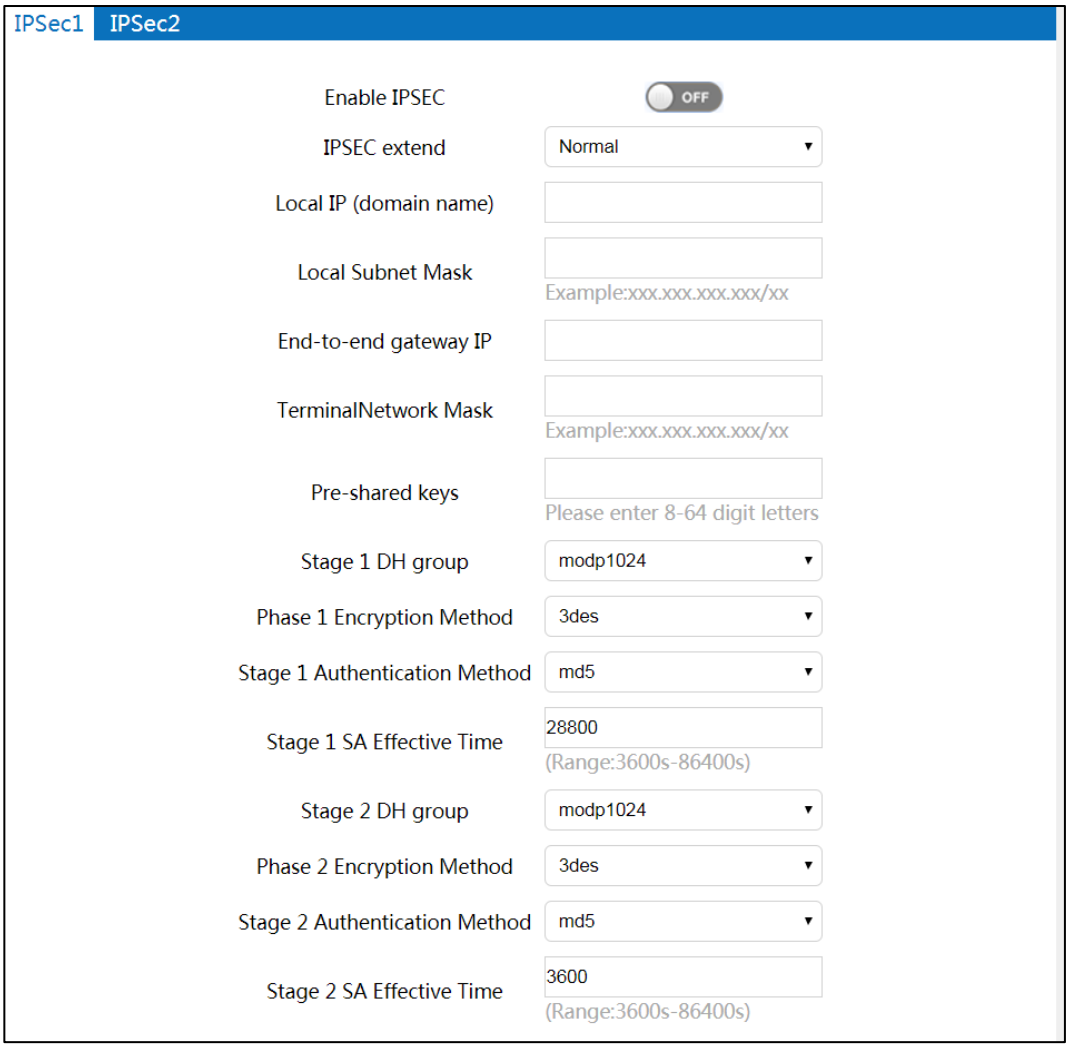
On the page of "IPsec", user can configure the relevant parameters of IPsec.

## Operation Path

Open in order: "VPN tunnel > IPsec".

## Interface Description

IPsec settings interface as follows:




The main elements configuration description of IPsec settings interface:

| Interface Element | Description |
|---|---|
| Enable IPSEC | Functional enablement switch of IPsec settings, click the right button for ON and OFF switching. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • ON: Enable the IPsec settings function;<br>• OFF: Disable the IPsec settings function. |
| IPSEC extend | Drop-down box of IPSEC extension, options as follows:<br>• Normal: Regular IPSEC<br>• GRE: GRE over IPSEC, GRE encapsulation based on IPSEC encryption<br>• L2TP: GRE over L2TP, L2TP encapsulation based on IPSEC encryption |
| Local IP (domain name) | IP address/domain name of the local external network port |
| Local Subnet Mask | The local subnet and mask of the router, for example: 192.168.4.0/24 |
| End-to-end gateway IP | IP or domain name of the end-to-end external network port |
| Terminal Network Mask | IPsec end-to-end subnet and subnet mask, 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:<br>• mop 768<br>• modp1024<br>• modp1536 |
| Phase 1 Encryption Method | Phase 1 encryption algorithm, options as follows:<br>• 3des<br>• aes128<br>• aes192<br>• aes512 |
| Stage 1 Authentication Method | Stage 1 Authentication Method, options as follows:<br>• md5<br>• she<br>• sha256<br>• sha384<br>• sha512 |
| Stage 1 SA Effective Time | Stage 1 SA Effective time, unit is second. The default is 28800 |
| Stage 2 DH group | Stage 2 DH exchange algorithm, options as follows:<br>• mop 768 |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | • modp1024<br>• modp1536 |
| Phase 2 Encryption Method | Phase 2 encryption algorithm, options as follows:<br>• 3des<br>• aes128<br>• aes192<br>• aes512 |
| Stage 2 Authentication Method | Stage 2 Authentication Method, options as follows:<br>• md5<br>• sha<br>• sha256<br>• sha384<br>• sha512 |
| Stage 2 SA Effective Time | Stage 2 SA Effective time, unit is second. The default is 3600 |



Copyright © 3onedata Co., Ltd.

# 8 System Manage

## 8.1 Time Setting

### Function Description

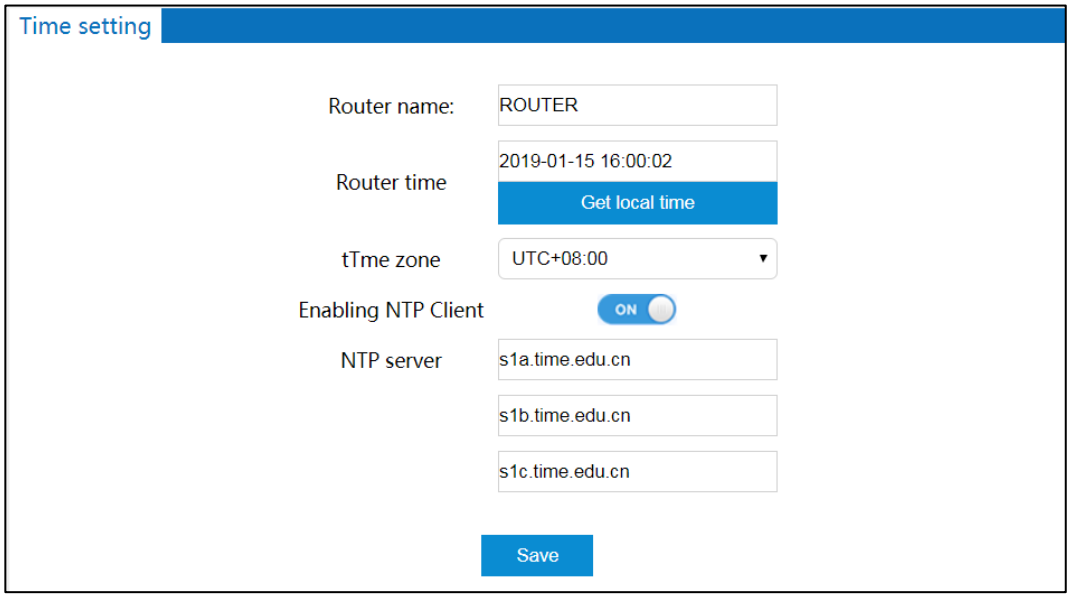
On the page of "Time Setting", user can configure time-related parameters information.

### Operation Path

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

### Interface Description:

Time setting interface as follows:






Copyright © 3onedata Co., Ltd.

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 |
| 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 | Functional enablement switch of NTP client settings, click the right button for ON and OFF switching.<br>• ON: Enable the NTP client function to synchronize the time of the server with the client.<br>• OFF: Disable the NTP client function. |
| NTP server | The address of the server that needs to be synchronized<br>Notes:<br>When there are multiple candidate NTP clients, the default is the first one. The higher the order, the higher the priority. |
| Save | Synchronize client and server time by clicking the button of "Save" |

# 8.2 Access Settings

### Function Description

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

### Operation Path

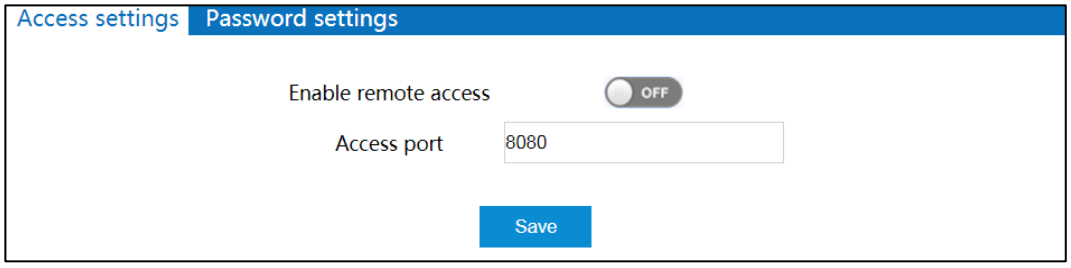
Open in order: "System manage > Access settings".

### Interface Description 1: Access Settings

Access settings interface as follows:



Copyright © 3onedata Co., Ltd.

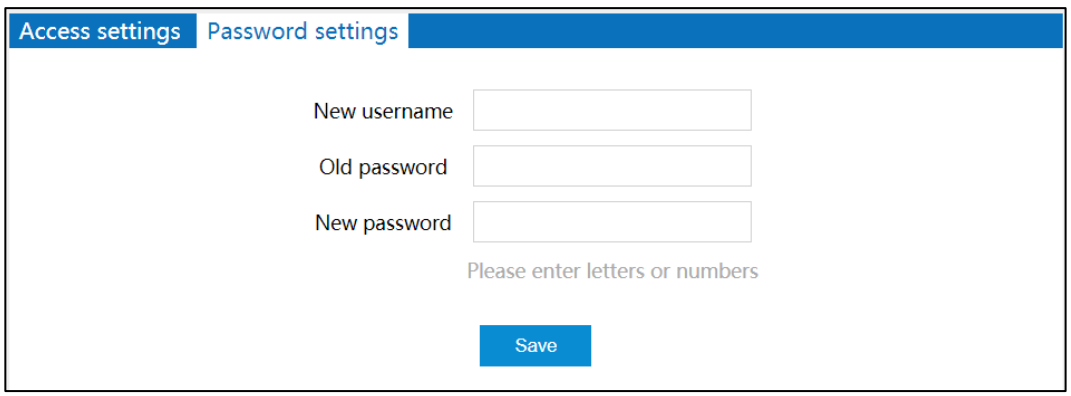



The main elements configuration description of access settings interface:

| Interface Element | Description |
|---|---|
| Enable remote access | Enablement switch of remote access, click the right button for ON and OFF switching.<br>• ON: Enable remote access, the user can access the device through the HTTP/HTTPS protocol on the external network;<br>• OFF: Disable remote access. |
| Access port | Port number of remote access, the port number defaults to 8080.<br>Notes:<br>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.<br>Notes:<br>Username and password are composed of capital and lower-case |



Copyright © 3onedata Co., Ltd.

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

# 8.3 Timed Restart

## Function Description

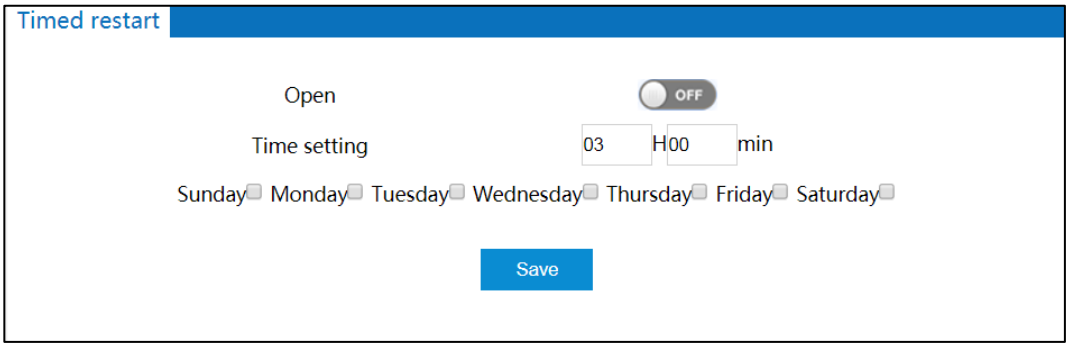
On the page of "Timed restart", user can configure the time for the device to automatically restart.

## Operation Path

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

## Interface Description:

The timed restart interface as follows:




The main elements configuration description of timed restart interface:

| Interface Element | Description |
|---|---|
| Open | Enablement switch of timed restart, click the right button for ON and OFF switching.<br>• ON: Enable the timed restart function;<br>• OFF: The default is off. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| 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

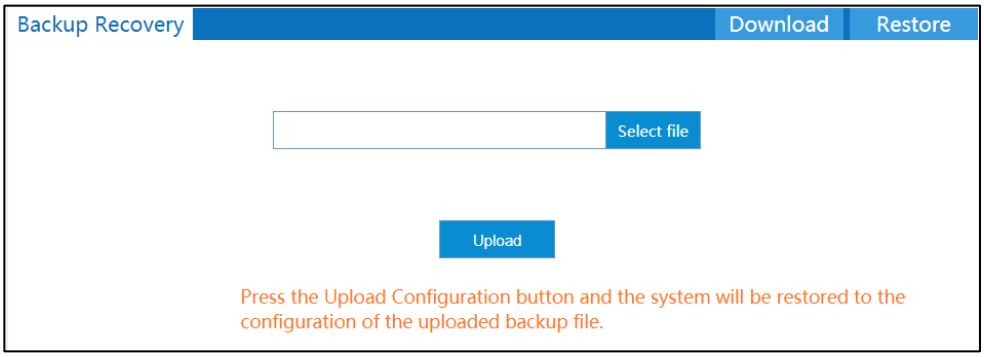
On the page of "Backup Recovery", user can select files for upload configuration, downloadable configuration, and restore factory defaults.

### Operation Path

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

### Interface Description:

The backup recovery settings interface as follows:




The main elements configuration description of backup recovery settings interface:

| Interface Element | 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. |
| Download | Click the "Download" button to download the configuration file of the current device and save it in the format of ".file". |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Restore | Click the button of "Restore" to restore factory defaults of the device. |

# 8.5 Log Manage

### Function Description

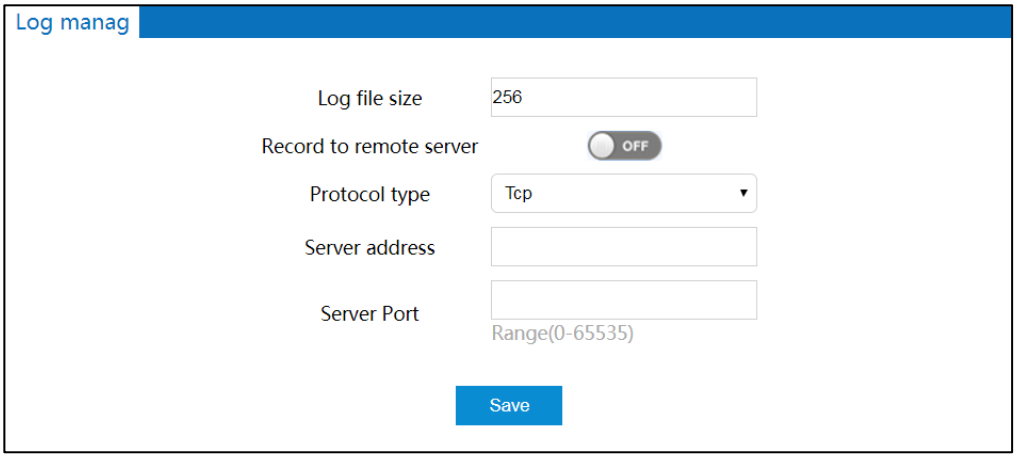
On the page of "Log manage", user can record the log files to the remote server.

### 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 | Enablement switch of record to remote server, click the right button for ON and OFF switching.<br>• ON: Enable the function of record to remote server to record log files to the remote server;<br>• OFF: Disable the function of record to remote server. |
| Protocol type | Drop-down box of the protocol type used by the record to |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | remote server, options as follows:<br>• TCP<br>• UDP |
| Server address | IP address information of the remote server |
| Server Port | Port number of the remote server. |

# 8.6 Firmware Upgrade

### Function Description

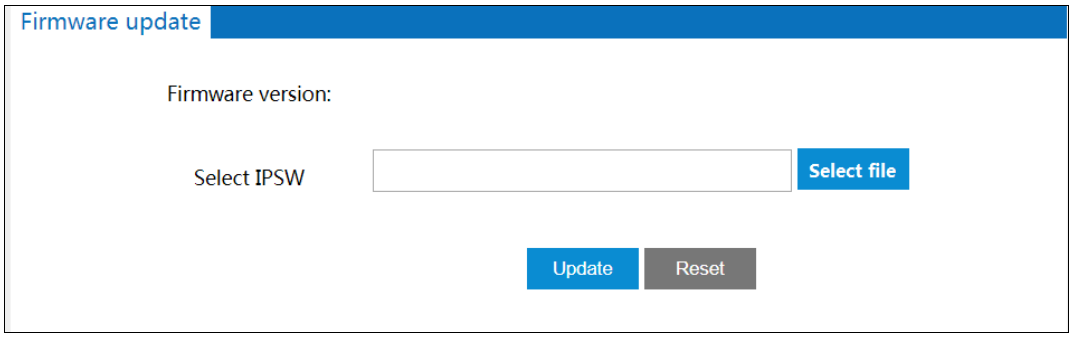
On the page of "Firmware upgrade", user can update the system program of the device via the upgrade file.

### Operation Path

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

### Interface Description

The firmware update interface as follows:




The main elements configuration description of firmware update interface:

| Interface Element | Description |
|---|---|
| Firmware version | The software version used by the current device. |
| Select IPSW | Click the button of "Select IPSW" to select the local upgrade file of the host.<br>Notes:<br>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. |



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| | Notes:<br>• It takes a while during the upgrade process. Do not power off the device.<br>• After successful upgrade, the configuration of the device will remain unchanged and the firmware version information will change. |

# 8.7 Firmware Restart

### Function Description

On the page of "Firmware restart", user can restart the device.

### Operation Path

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

### Interface Description

The firmware restart interface as follows:




The main elements configuration description of firmware restart interface:

| Interface Element | Description |
|---|---|
| Reboot icon | Click this icon to reboot the device system. After the system restarts, it will jump back to the login interface. |



Copyright © 3onedata Co., Ltd.

# 9 Diagnostic Tools

## 9.1 System log

### Function Description

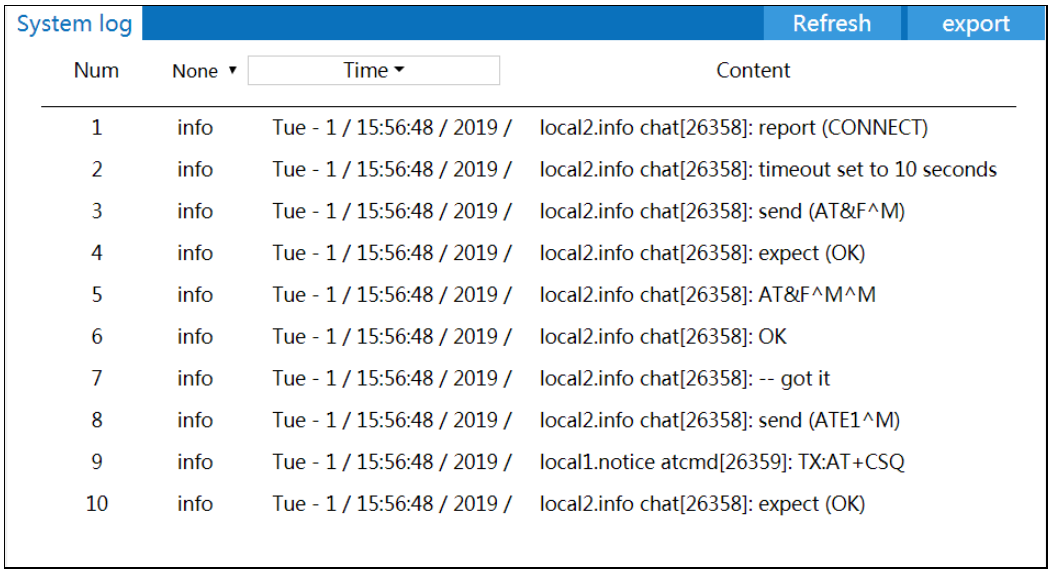
On the page of "System log", user can view the device system logs.

### Operation Path

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

### Interface Description

The system log interface as follows:




The main elements configuration description of system log interface:

| Interface Element | Description |
|---|---|



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
|---|---|
| Refresh | Click the "Refresh" button to regain the latest log information of the device. |
| Export | Click the "Export" button to export the log information in the format of ".txt". |
| Num | Log information shows sequence entries |
| None | User can select the category of log to display specific log information. Optional values:<br>• NONE: all messages;<br>• Info: general messages;<br>• Error: error messages;<br>• Warning: warning messages. |
| Time | The date and time filter button for log information.<br>Notes:<br>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:<br>• 10: Display 10 log messages per page;<br>• All: Single page displays all log information. |

## 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

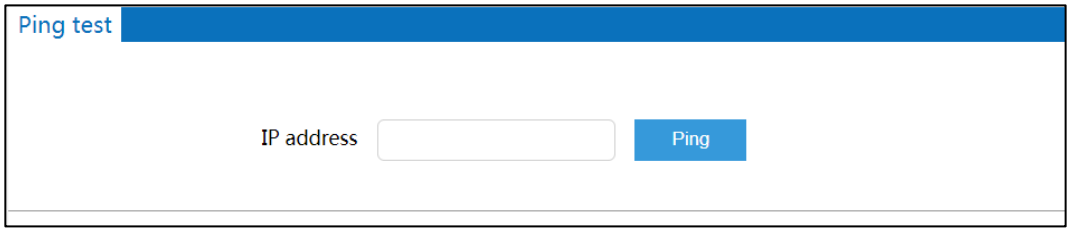
Open in order: "Diagnostic tools > Ping test".

### Interface Description

The Ping test interface as follows:



Copyright © 3onedata Co., Ltd.




The main elements configuration description of Ping test interface:

| Interface Element | Description |
|---|---|
| IP address | Target IP 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.

### Function Description

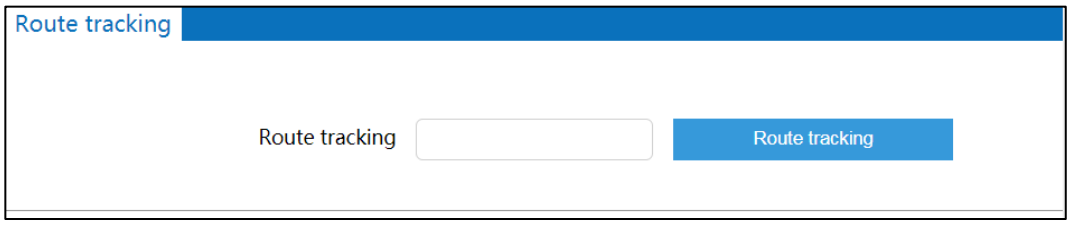
On the page of "Route Tracking", user can perform route tracking for the target host.

### 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:



Copyright © 3onedata Co., Ltd.

| Interface Element | Description |
| --- | --- |
| IP address | Destination IP address or domain name that requires route tracking |
| Route Tracking | Click the "Route Tracking" button to start tracking, and the test results are displayed below. |



Copyright © 3onedata Co., Ltd.

# 10 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 managed switch products, consumers can get help and solutions in the following ways:

- Internet service;
- Call technical support office;
- Product repair or replacement;

## 10.1 Internet Service

More useful information and tips are available via our company website. Website: http://www.3onedata.com

## 10.2 Service Hotline

Users using our company products can call technical support office. Our company has professional technical engineers to answer the questions and help solve the products or usage problems ASAP. Free service hotline: 86-400-880-4496



Copyright © 3onedata Co., Ltd.

## 10.3 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 salesmen 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
Make network communication more reliable



3onedata Co., Ltd.

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

Technology support: tech-support@3onedata.com

Service hotline: +86-400-880-4496

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



**Copyright © 3onedata Co., Ltd.**