3onedata



IRT2000-A1-1T1D-12-LV
Industrial-Grade 4G Router
User Manual

Document Version: 01

Issue Date: 06/41/2024

Copyright © 2024 3onedata Co., Ltd. All rights reserved.

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

Trademark statement

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

Note

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

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

3onedata



3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86 0755-2670-3485
Website:	http://www.3onedata.com

Preface

Industrial grade 4G router user manual, describes this router:

- Product characteristics
- Product installation and deployment
- Guidance on device configuration and maintenance through the Web network management client
- Web network client provides basic configuration, application configuration, VPN configuration, forwarding configuration, security configuration and system management configuration

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Port Convention

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

Text Format Convention

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

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

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

Symbols

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

Button Operation Convention

Format	Description
	There is a logout button in the upper right corner of the webpage. After clicking it, the webpage returns to the login page.
	There is a port button in the upper right corner of the webpage. Click or press F2 to view the port status, and press F2 or Esc to close the port status page.
	There is a restart button in the upper right corner of the webpage. After clicking, a restart confirmation box pops up. After confirmation, the device will restart.
	There is a Save button in the upper right corner of the webpage. Click it to save the current device configuration. After setting the device, the save icon will flash to remind the user to save the configuration, so as to avoid losing unsaved configuration information due to restart and other operations.
	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.

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

Format	Description
Delete	Check the line to be deleted, and then click the Delete button to delete the configuration.
Config	Check the line to be configured, and then click the configure button to enter the configuration page.
	Click the function status button to switch the function status,  means on and  means off.
Apply	Click the Set button to submit the current configuration.
Clear	Click the “Clear” button to clear the information of current page.
Refresh	Click the Refresh button to refresh the information of current page.

Revision Record

Version No.	Date	Revision note
01	06/17/2024	Product release

Copyright © 3onedata Co., Ltd.

Contents

PREFACE 1
CONTENTS I
1 BASIC CONFIGURATION 1
1.1 LOCAL CONNECTION CONFIGURATION 1
1.1.1 configure PC 1
1.1.2 Configuration check 4
1.2 BASIC CONFIGURATION 6
1.3 LOG ON TO THE WEB CONFIGURATION PAGE 6
1.4 LAN CONFIGURE 8
1.5 MOBILE NETWORK 9
1.6 WLAN CONFIGURE 16
1.7 DHCP, THE SERVICE CONFIGURATION 20
2 APPLICATION CONFIGURATION 23
2.1 KEEP ONLINE 23
2.2 SERIAL PORT APPLICATION 25
2.3 DDNS CONFIGURE 29
2.4 TRAFFIC STATISTICS 31
2.5 QOS 33
2.6 TIMED TASK 34
2.7 LOCATION SERVICE 36
3 VPN CONFIGURE 43
3.1 VPDN CONFIGURATION (L 2 TP / PPTP) 43
3.2 L 2 TP SERVER FUNCTION CONFIGURATION 48
3.3 THE N2N_V2 CONFIGURATION 51
3.4 OPENVPN 52
3.5 IPSEC 55
3.6 GRE 59
3.7 EOIP 61
3.8 VXLAN 63
4 FORWARD CONFIGURATION 65
4.1 NAT 65
4.2 ROUTING CONFIGURATION 67
4.3 DMZ 69
4.4 OSPF CONFIGURE 70
5 SECURITY CONFIGURATION 73
5.1 FIREWALL 73
5.2 IP FILTER 74

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

5.3 MAC FILTER 76
5.4 DOMAIN NAME FILTERING....79
6 SYSTEM CONFIGURATION 81
6.1 USER MANAGEMENT 81
6.2 CONFIGURATION MANAGEMENT 82
6.3 FIRMWARE UPGRADE....83
6.4 APP INSTALL 84
6.5 SYSTEM TIME 85
6.6 LOG MANAGEMENT....86
6.7 DIAGNOSE....87
6.8 DEVICE CLOUD NETWORK PIPE 90
6.9 SERVICE CONFIGURATION 91
6.10 MODULE UPGRADE 93
7 SYSTEM MODE 96
7.1 SYSTEM 96
7.2 MOBILE NETWORK 97
7.3 98
7.4 DHCP CLIENT 98
7.5 WLAN STATE....99
7.6 THE WLAN HAS BEEN CONNECTED TO THE DEVICE 99
7.7 DDNS STATE....100
8 FAQ 101
8.1 HARDWARE PROBLEMS....101
8.1.1 All indicator lights are inactive.... 101
8.1.2 The SIM card holder connection issue 101
8.1.3 Network port connection problem.... 102
8.1.4 Antenna connection problem.... 102
8.2 DIAL CLASS PROBLEM 103
8.2.1 Dial interrupt 103
8.3 THE WEB CONFIGURATION ACTION CLASS PROBLEM 103
8.3.1 Unable to log on to the configuration page 103
8.3.2 Failed to upgrade firmware 104
8.3.3 The router is restarted repeatedly.... 104
9 APPENDIX.... 105
9.1 PARAMETER SPECIFICATION TABLE 105
9.2 TERM 106
10 MAINTENANCE AND SERVICE 108
10.1 INTERNET SERVICE 108
10.2 SERVICE HOTLINE....108
10.3 PRODUCT REPAIR OR REPLACEMENT....108

Copyright © 3onedata Co., Ltd.

1 Basic configuration

1.1 Local Connection Configuration

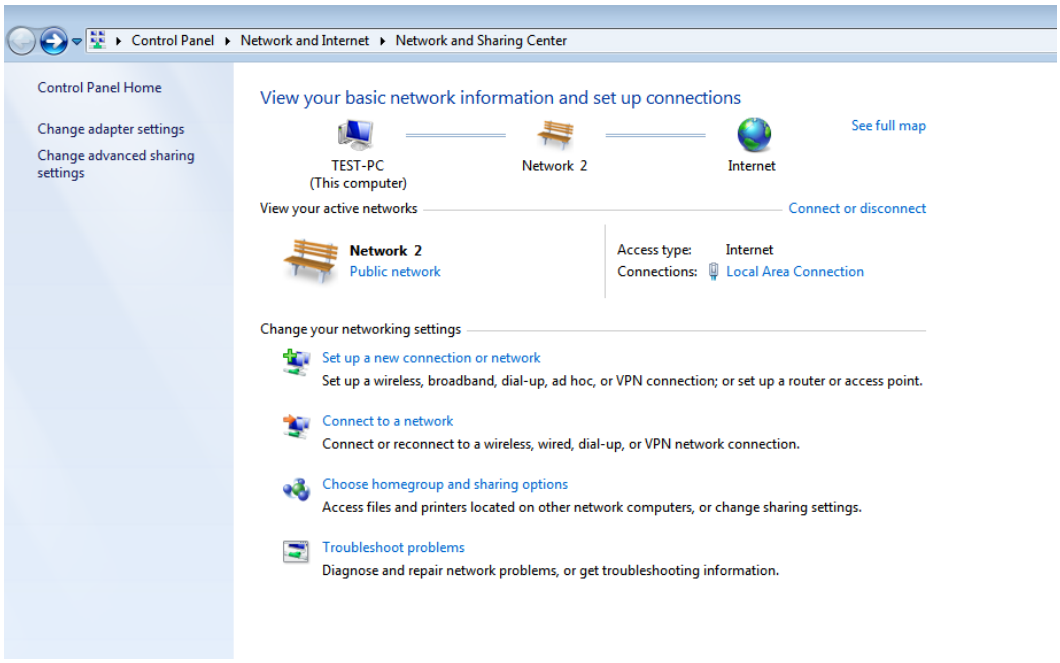
prerequisite

- Has already supplied the power to the router.
- The LAN port connecting the router and the PC terminal via the Ethernet cable.

1.1.1 configure PC

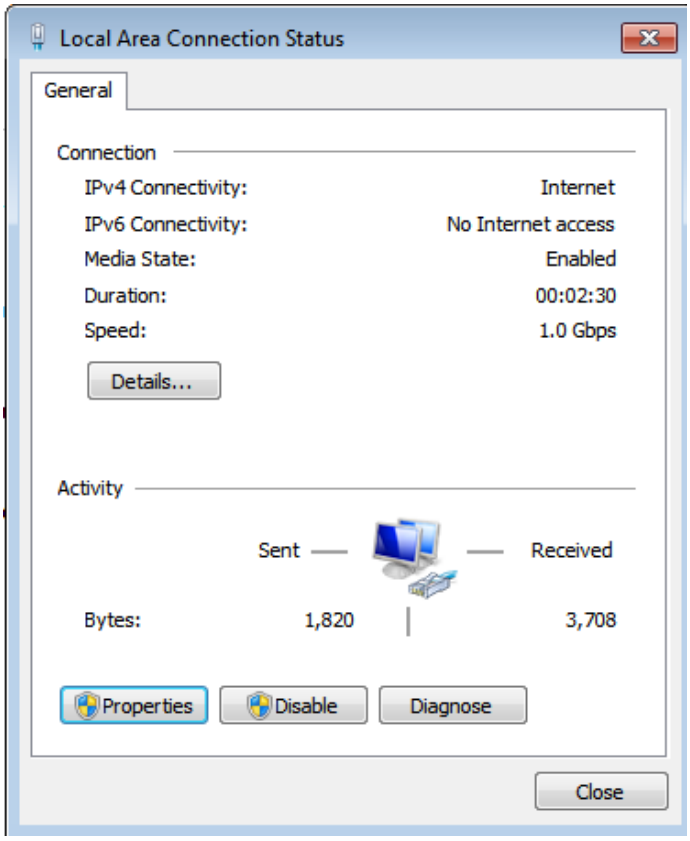
operating steps

Click Start> Control Panel> Network and Shared Center, and double-click Local Connection in the open window.

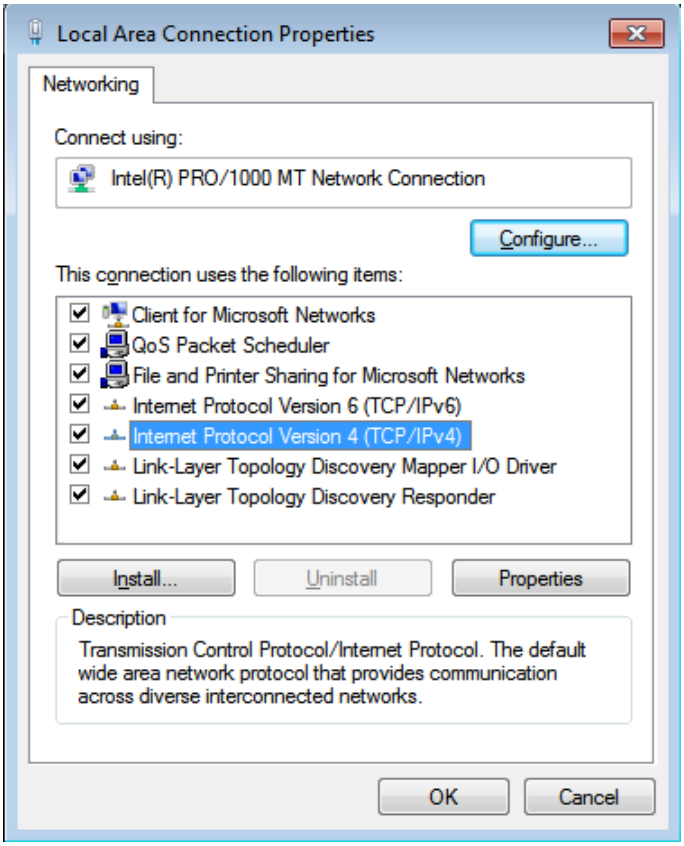


Copyright © 3onedata Co., Ltd.

In the Local Connection Status window, click Properties.



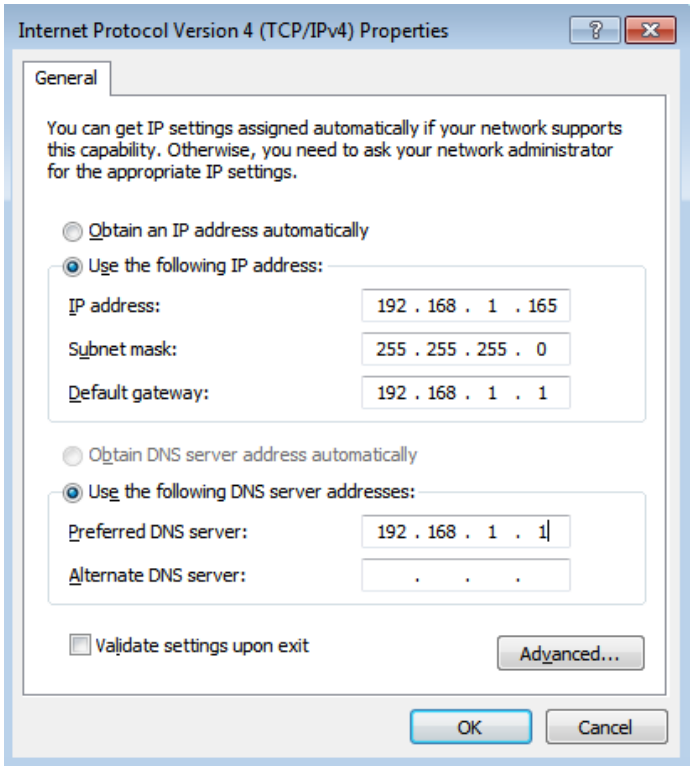
Select Internet Protocol Version 4 (TCP / IPv4), and click Properties.



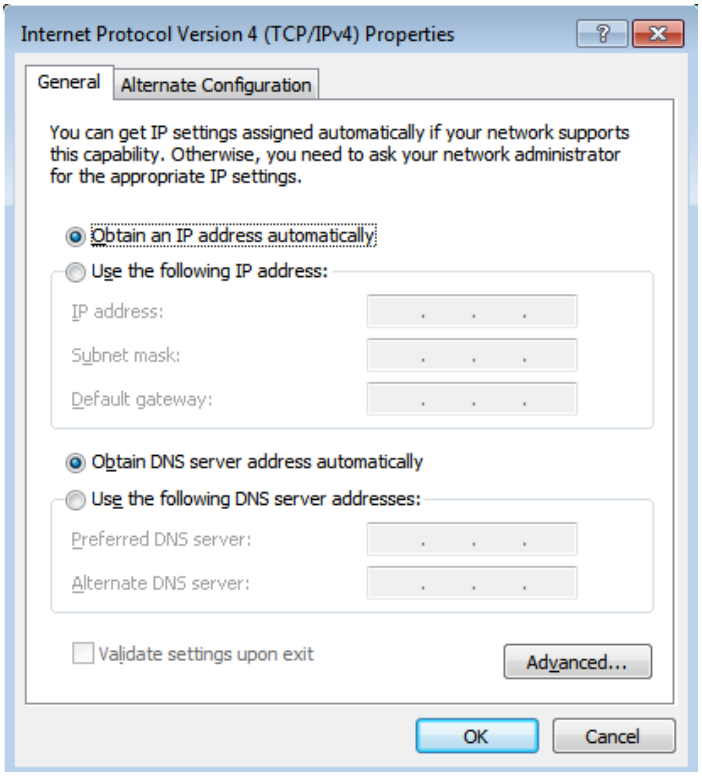
Copyright © 3onedata Co., Ltd.

Configure the IP address of the PC in both ways

Manually configure the PC with a static IP address in the same subnet as the router address, click and configure Use the IP address below.



Automatically obtain the IP address from the DHCP server and click Automatic Get IP Address.

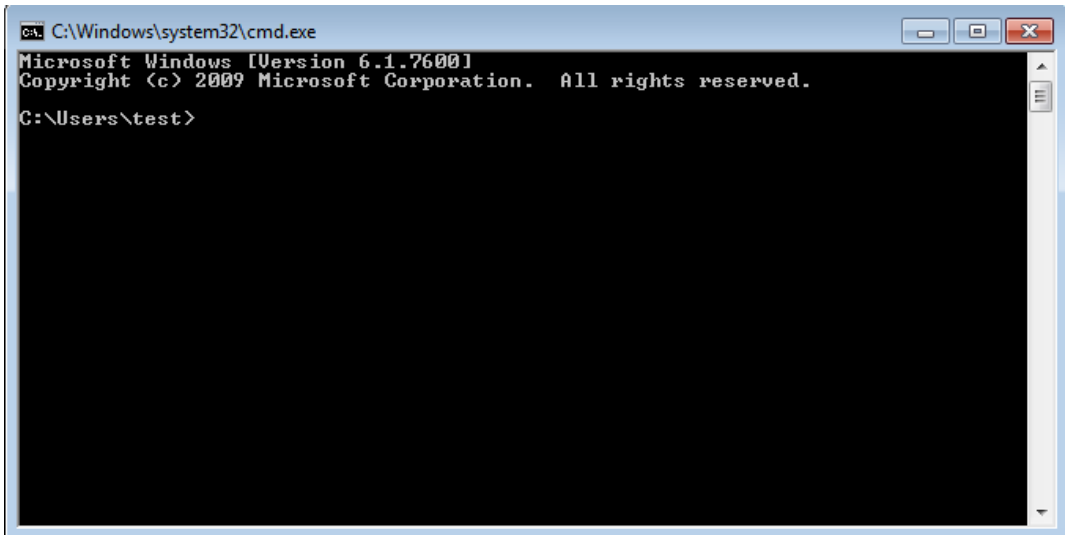


Copyright © 3onedata Co., Ltd.

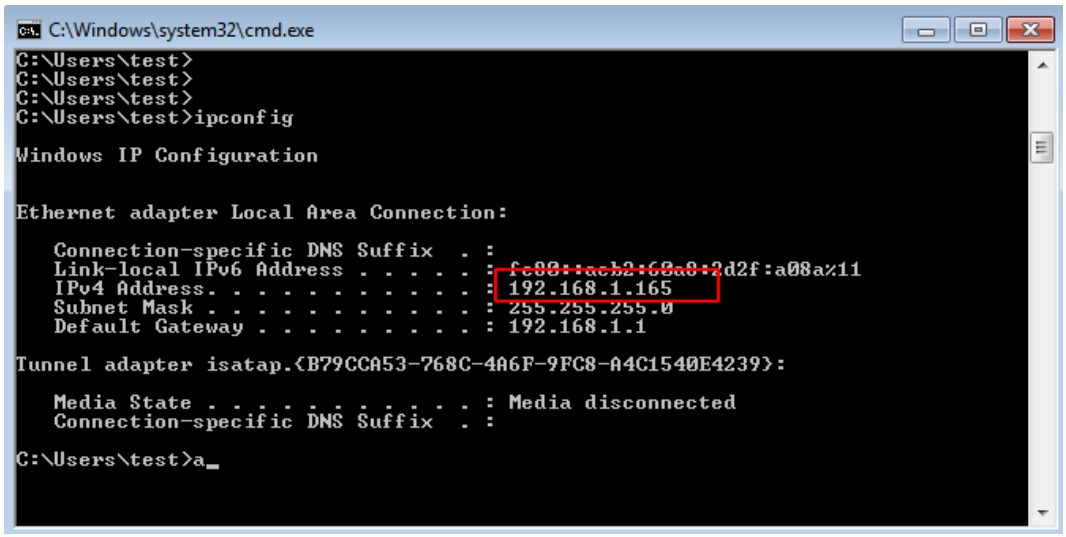
1.1.2 Configuration check

operating steps

Step 1 Click Start> Run, and press Enter after entering the cmd command in the Run input box. Opes the Run window.

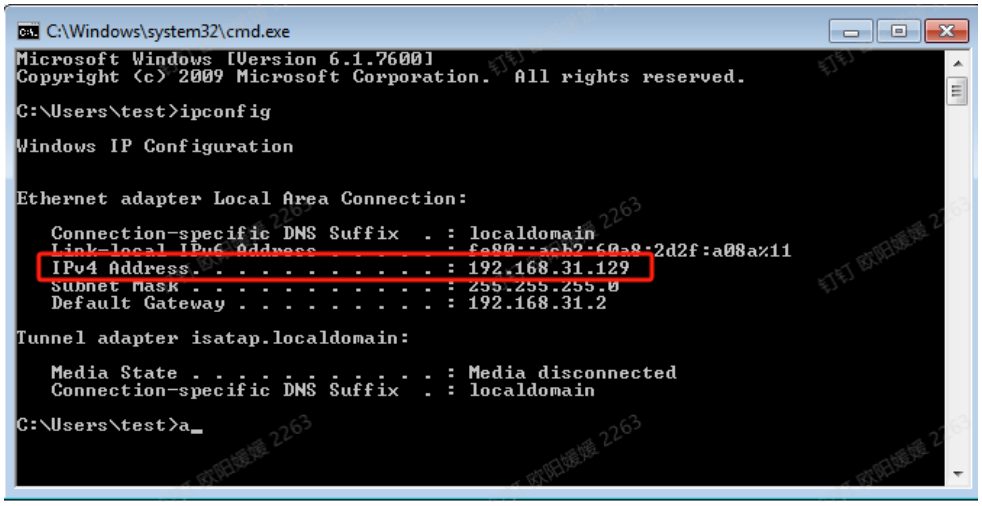


Step 2 Enter the command "ipconfig" in the Run window, and the IP Address in the configuration method of IP Address in the specified IP mode; automatically get the random number of "2~254" in the configuration method of IP in the router DHCP.

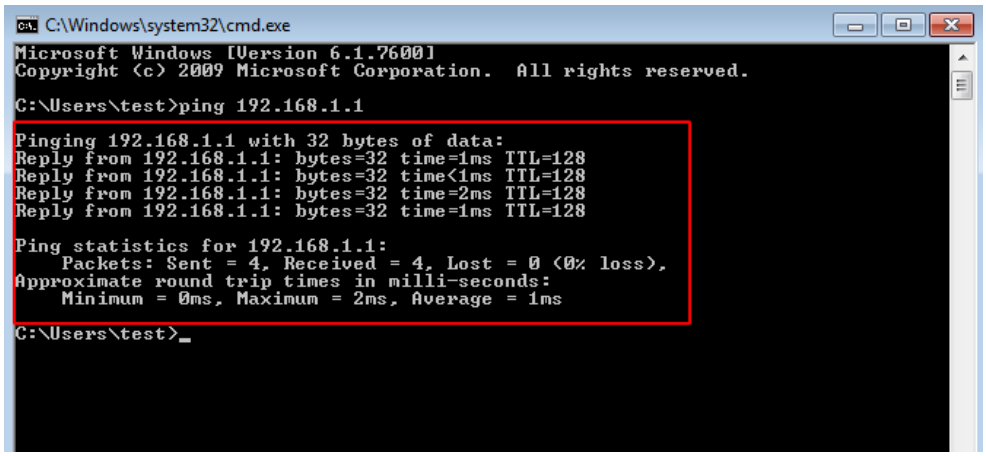


DHCP, automatically get the IP mode "ipconfig" execution results

Copyright © 3onedata Co., Ltd.



Step 3 In the command line window, enter: ping 192.168.1.1. If the interface shown below appears, the connectivity between the local computer and the router is normal.



—— **finish**

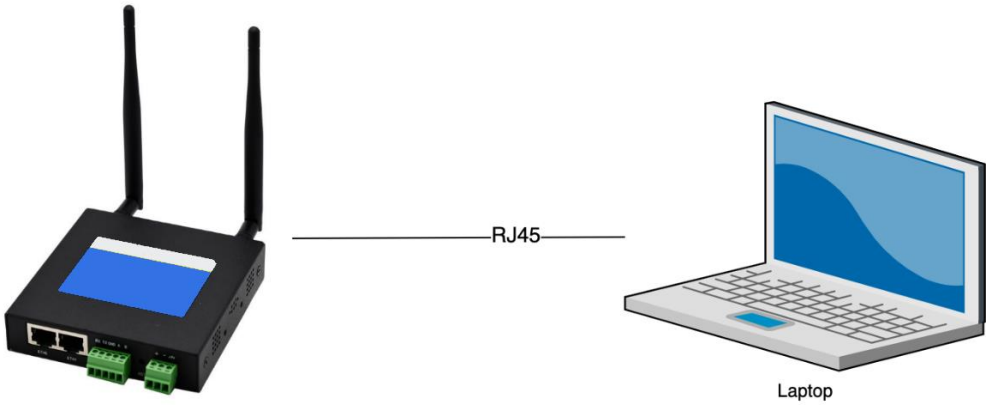
1.2 basic configuration

1.3 Log on to the WEB Configuration page

background information

Users can use the factory configuration of the device to directly log in to WEB network management to manage and maintain the device, or configure the IP address, WEB network management parameters, WEB, and users on the command line, and then log in to WEB network management.

Users can use the PC to manage and configure the device through the WEB network management system. Table 21 Description of interface wiring for each model1-1



model	interface specification	The wiring instructions
IRT2000-A1-1T1D-12-LV	ETH: The LAN interface.	The computer connects to the ETH interface through the network cable.

Pre-task

Before logging in with the WEB mode, complete the following tasks:

- The access port of the device has a configured IP address.

explain

The device contains a factory configuration with an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0.

- The PC terminal is already connected to the device via the network cable.

Copyright © 3onedata Co., Ltd.

explain

If the PC automatically obtains the IP address mode and cannot log in to WEB, it is recommended that the PC set the static IP with the same network segment as the device, and then log in to WEB.

- The equipment operates normally.
- The PC terminal has installed the browser software.

operating steps

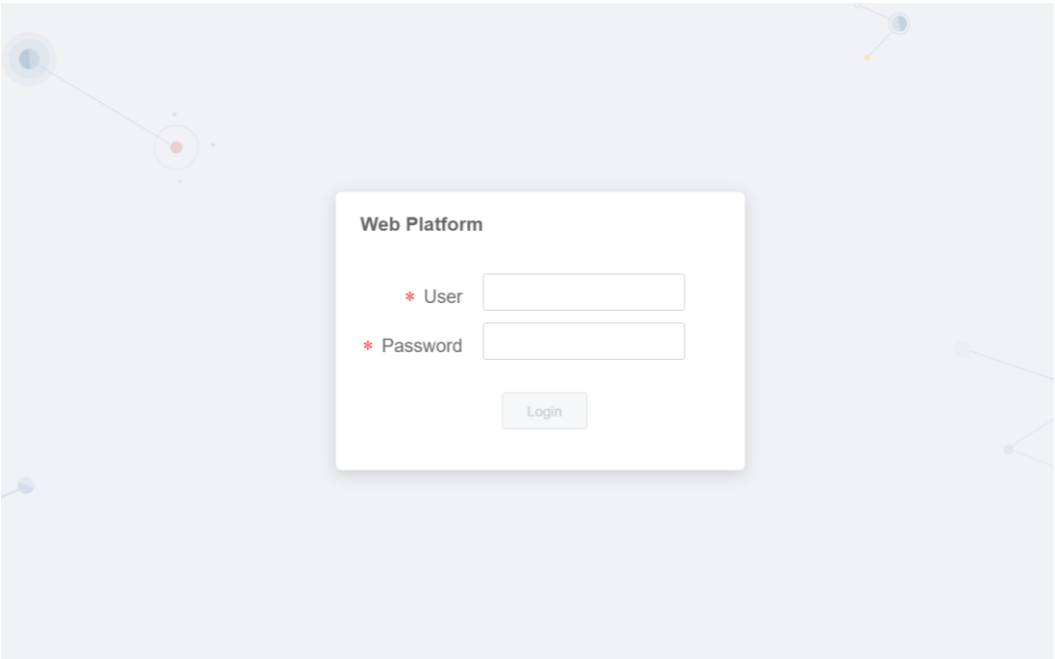
Step 1 The PC terminal opens the chrome browser and enters the IP address of the router in the address barhttp://192.168.1.1To enter the user login identity authentication page.

Enter the User Name and Password on the login page, and click OK to enter the operation page.

explain

The user first logs into the system and must use the default user name and password. The default user name is "admin" and the password is "admin". To change the password, see the"7.1 User Management”

After a successful login, the home page is shown in the figure below. On the home page, the user can change the language, restart the router, and log off the login.



Copyright © 3onedata Co., Ltd.

You need to exit the current login and click the "Exit" button in the upper right corner of the page to return to the user login page.

—— **finish**

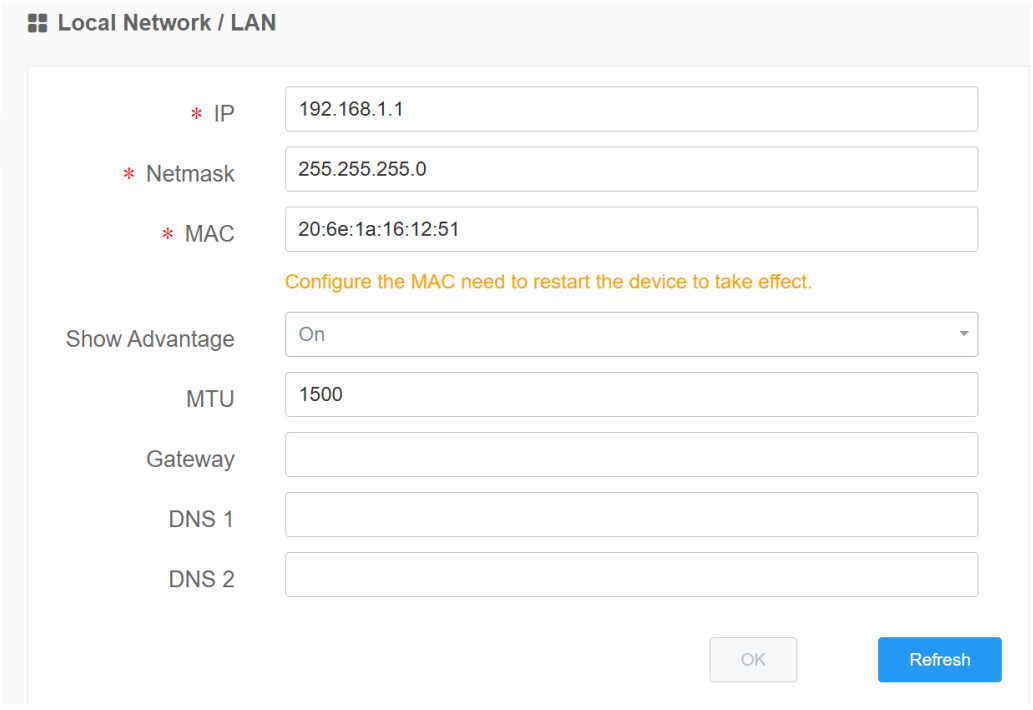
1.4 LAN configure

background information

The configuration of LAN port is mainly used for the connection between the router and the lower machine, so that the lower machine can access the external network through the router, and also ensure the normal communication between the network segments connected under the router.

operating steps

Step 1 After logging on to the WEB configuration page, click Network Configuration> LAN Configuration to open the LAN tab.



Configure the LAN port connection parameters as described in Table 2-2.

1-Table 22 Description of LAN port connection type parameters

The parameter name	explain	collocation
IP address	Set up the IP address of the LAN port.	Enter manually in the input box form:X.X.X.X Default value: 192.168.1.1

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
subnet mask	Set the subnet mask for the LAN port.	Enter manually in the input box form:X.X.X.X Default value: 255.255.255.0
MAC address	Set the MAC address of the LAN port.	Format is not modified under normal circumstances XX: XX: XX: XX: XX: XX:
gateway	Sets the gateway for the LAN port IP.	Enter manually in the input box form:X.X.X.X
DNS1	Set up the preferred DNS server.	Enter manually in the input box form:X.X.X.X
DNS2	Set up the alternate DNS server.	Enter manually in the input box form:X.X.X.X

Click OK to complete the configuration of the LAN port connection type.

—— **finish**

explain

When the user changes the LAN port address, if the page does not jump automatically jump, make sure that the user has the address in the same network segment, or set the computer to automatically obtain IP, and then enter a new LAN address in the browser.

1.5 mobile network

background information

One of the core functions of Sanwang industrial wireless router, the router can access the Internet through modem dialing, providing users with high-speed wireless broadband Internet access function.3G network can usually reach the Internet rate of 1~5Mbps, 3.5G network up to 20Mbps Internet rate, 4G can be up to nearly 100Mbps Internet rate, 5G network can reach 1000Mbps Internet rate.

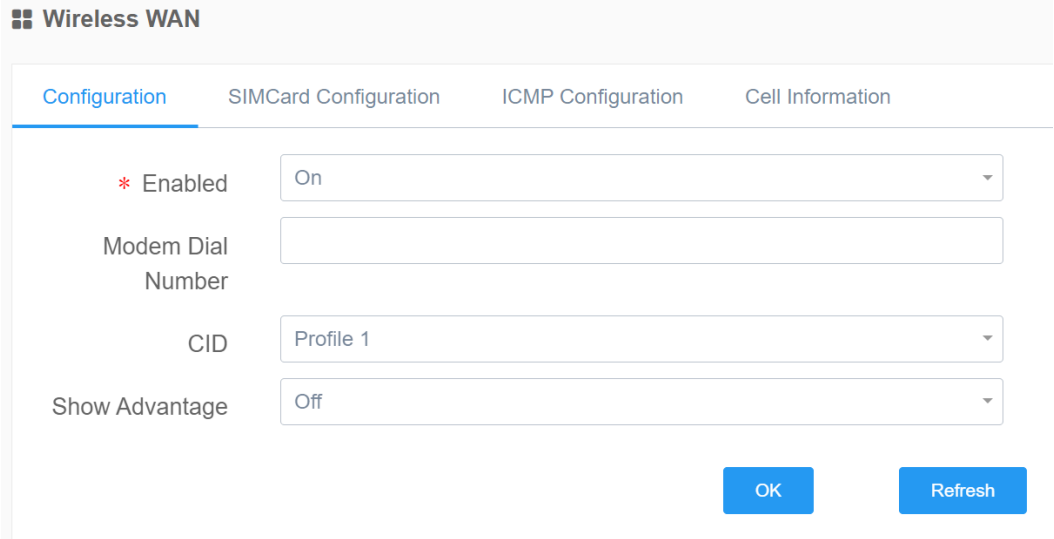
explain

IRT2000-A1-1T1D-12-LV does not support 5G related configuration function, does not support dual SIM, card function

Copyright © 3onedata Co., Ltd.

operating steps

Step 1 After logging on to the WEB Configuration page, click Network Configuration> Mobile Networks to open the Mobile Networks tab.



The Edit, Enable, and Disable operations for the Mobile Network Parameters. The parameters of "Mobile Network" are described in Table 2-4.

1-Table 24 Description of the mobile network parameters

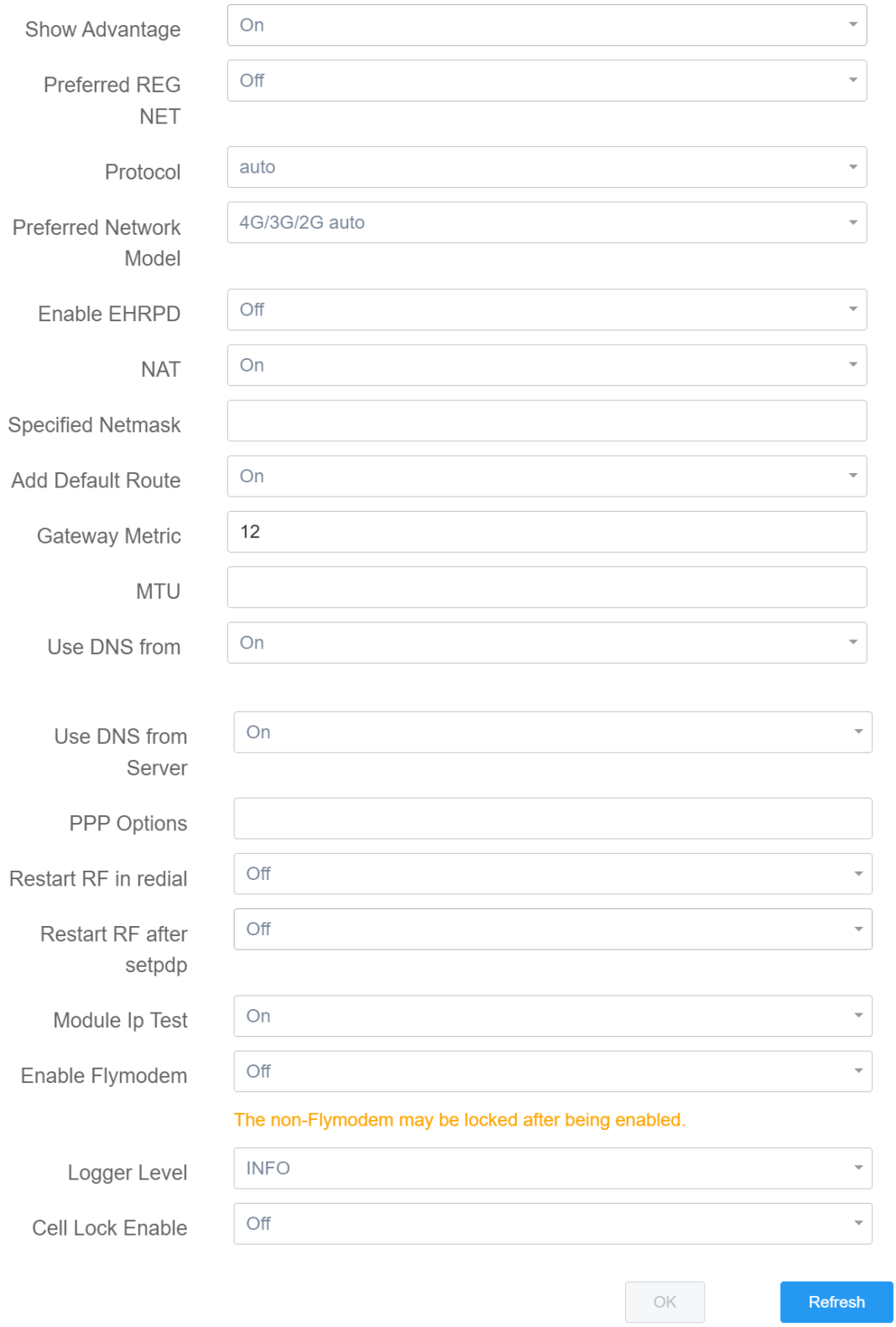
The parameter name	explain	collocation
start using	Whether to use the mobile network function.	Drop-down list selection ● yes ● deny
MODEM Dial the number	A code identification of a network, usually a standard network has a fixed service code, such as G network: * 99 * * * 1 #, C network: # 777.	CODE type, max. 64 bytes, input specification see"Parameter specification table"
CID		Drop-down list selection ● P rofile 0~16
APN	Enter the access point for a cellular network dial-up connection provided by the local Internet service provider.	manual input

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Certification type	Router authentication type, selected according to the local ISP.	Drop-down list selection ● close ● PAP ● CHAP ● voluntarily
User name / password	Enter the user name / password for the cellular dial-up connection provided by the local Internet service provider.	WORD type / CODE type, maximum length of 64 bytes, both existing or empty
PIN a sign or object indicating number	Lock card PIN code for the carrier-provided SIM card.	It's usually 4 digits
Enable the dual SIM cards	IRT2000-A1-1T1D-12-LV does not support dual SIM cards, and if this function is not enabled, it only supports the SIM card 1 network.	Drop-down list selection ● yes ● deny The master card selects either SIM1 or SIM2

Copyright © 3onedata Co., Ltd.

In the Show Advanced Configuration drop-down box, select Yes for mobile networks.



Configure the advanced configuration parameters, which are described in Table 2-5.

1-Table 25 Description of the advanced configuration parameters of the mobile network

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
The 5G access mode	The optional 5G networking mode is not supported by IRT2000-A1-1T1D-12-LV.	Drop-down list selection ● NSA+SA ● NSA ● SA
White card mode	Test card mode, belongs to the three major operators SIM card without configuration	Drop-down list selection ● yes ● deny
Priority registration network	Priority on whether to register the network.	Drop-down list selection ● yes ● deny
protocol	The dial-up protocol usually uses auto. The router will automatically select the dial-up protocol according to the situation, and force the pppd when necessary.	Drop-down list selection ● auto ● pppd
The preferred network mode	Sets the routing of the preferred network mode.	Drop-down list selection 5G / 4G / 3G / 2G automatic selection ● only NR ● only LTE+NR ● only LTE ● Only Unicom 3G ● Move only 3G ● Telecom 3G only ● only GPRS ● Only the CDMA 1x
open EHRPD	This feature is effective only for partial EVDO networks.	Drop-down list selection ● yes ● deny
NAT	When the private network PC is connected to the Internet, the NAT function needs to be turned on.	Drop-down list selection ● yes ● deny

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

The parameter name	explain	collocation
MTU	Maximum transmission unit of the interface. If the MTU configuration is too small and the message size is large, it may cause excessive fragmentation, and the message will be discarded by the QoS queue. If the MTU value is configured too large, the transmission speed of the message will be slow, and even the message will be lost.	Enter the numerical MTU manually, with the default to 1500
Specifies the subnet mask	Modify the mobile network interface mask address	Enter manually in the input box form:X.X.X.X
Specify the gateway	Mobile network interface gateway address can be modified	Enter manually in the input box form:X.X.X.X
Add default routing	When the private network PC is connected to the Internet, it needs to be turned on.	Drop-down list selection ● yes ● deny
Gateway jump point	The lower the setting of the interface priority value, the higher the priority	Normal without modification, multi-link can be set the priority through the jump point
DNS 1	Set up the preferred DNS server.	Enter manually in the input box form:X.X.X.X
DNS 2	Set up the alternate DNS server.	Enter manually in the input box form:X.X.X.X
PPP option	dial mode	
Log level	Filter the detailed log	DEBUG-shakedown test INFO-message NOTICE-Notice WARNING-Alert ERROR-wrong CRITICAL-Critical ALERT-report to the police EMERG-urgent

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

The parameter name	explain	collocation
Whether to lock the base station	IRT2000-A1-1T1D-12-LV does not support locking the specified base station	Configure the relevant base station frequency point, ID, carrier, BAND

Online detection configuration, and the parameter configuration is as follows

The parameter name	explain	collocation
The main server	The master server address must be routed and accessible. The default address is empty, and the primary / standby servers are empty, meaning closing the probe	form:X.X.X.X Default is empty
Standby server	The alternate service address must be routed accessible, with the default address and the primary / standby server empty, indicating that detection is not enabled	form:X.X.X.X Default is empty
interval	Automatically perform probe time intervals in seconds	Default 3 seconds
Timeout time	Set ICMP probe timeout time (probe timeout auto restart)	Default 5 seconds
Maximum number of retries	Set the maximum number of retries when the ICMP probe failed)	Default 5 times
Strict detection	Open detection or off, strict detection open can not detect the network within the specified time, the equipment will self-check the network re-dial	Drop-down list selection ● yes ● deny
Offline forced restart	Forced restart beyond the maximum number of retries	Drop-down list selection ● yes ● deny

Copyright © 3onedata Co., Ltd.

Click OK to complete the mobile network parameter configuration.—— **finish**

1.6 WLAN configure

background information

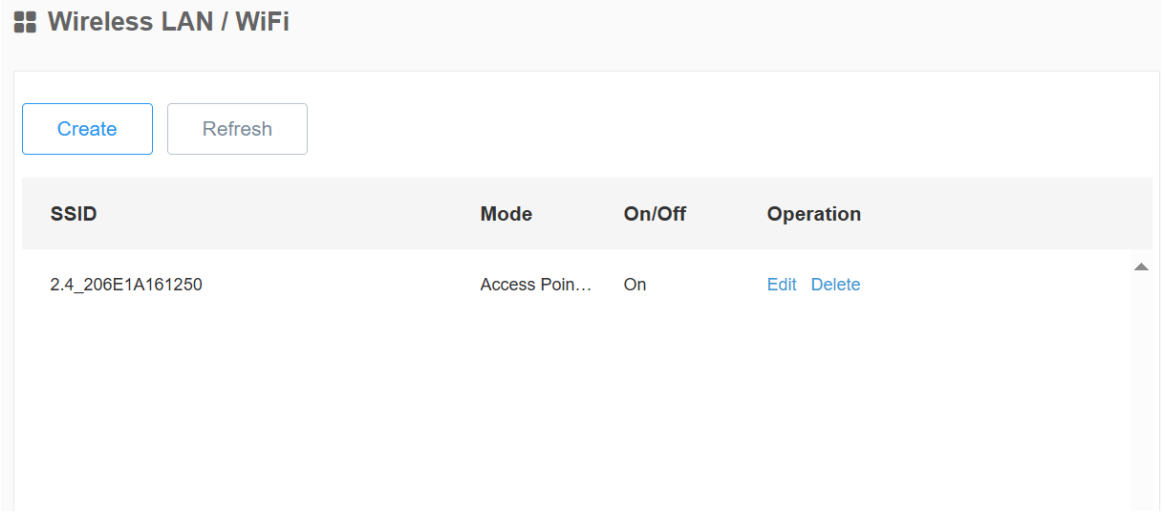
Sanwang industrial grade wireless router provides two functions: AP mode and client mode. Through the function of AP mode, it can provide you with wireless LAN hot spots, facilitate access to the network and save wiring trouble. Through the function of client mode, you can let the router access other AP devices, so that the lower machine of the router can access the external network through the connected AP devices.

explain

When selecting the client mode, the router will automatically match the corresponding encryption mode and algorithm according to the selected AP (to keep the same encryption mode with the AP); the shared key needs to fill in the key to connect the AP, IRT2000-A1-1T1D-12-LV model does not support WIFI function.

operating steps

Step 1 After logging on to the WEB Configuration page, click Network Configuration> WLAN to open the WLAN Configuration tab. Display parameters are shown in Table 2-6.



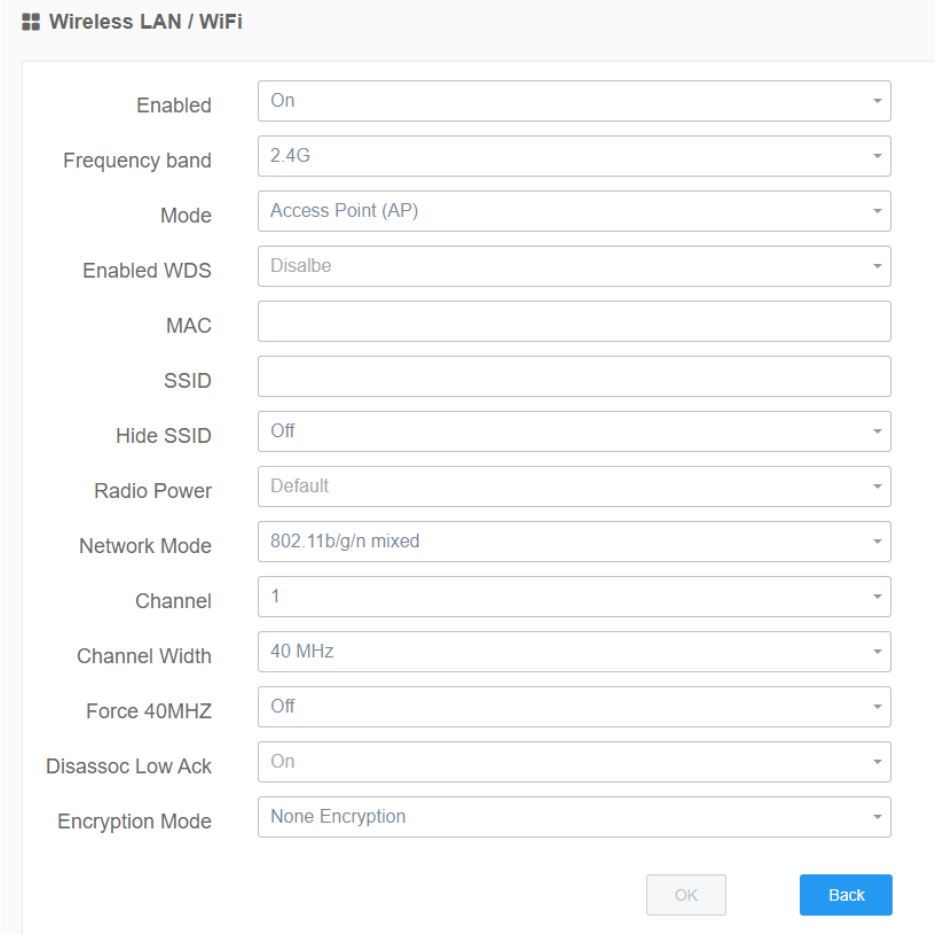
1-Table 26 WLAN, description of the parameters

The parameter name	explain
SSID	Set the custom WiFi name.

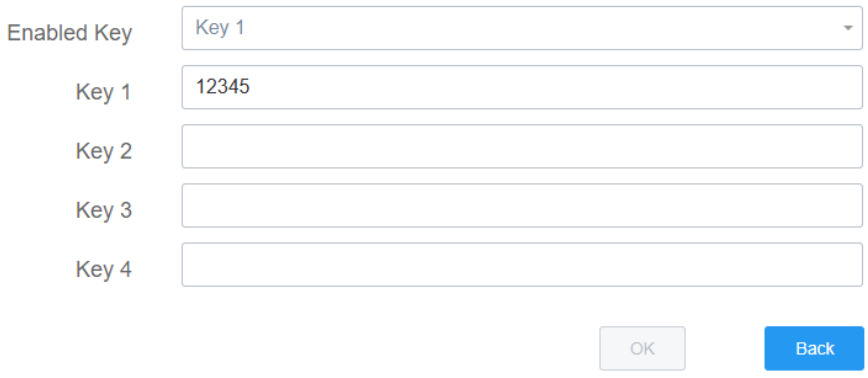
Copyright © 3onedata Co., Ltd.

The parameter name	explain
pattern	WLAN working mode, support AP mode / client mode.
start using	WLAN current state.
operate	Edit, Delete operations for WLAN.

Click Create to create a new WLAN.

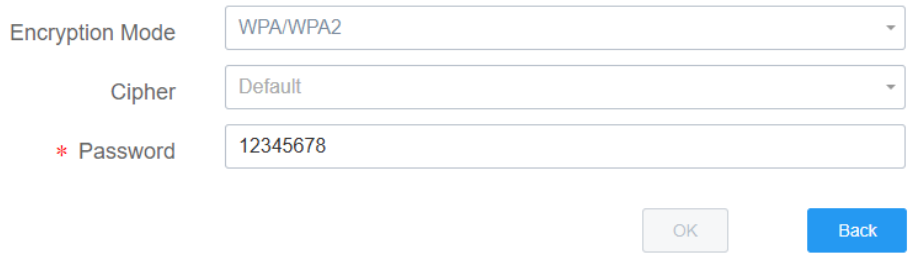


Select WEP Development Authentication, WEP Share and Key



For the encryption mode, select WPA, WPA 2, and WPA / WPA 2

Copyright © 3onedata Co., Ltd.



Relevant parameters of "WLAN", as shown in Table 2-7.

1-Table 27 Description of the WLAN parameters

The parameter name	explain	collocation
start using	Whether to use the WLAN function.	Drop-down list selection yes deny
pattern	WLAN working mode, support AP mode / client mode.	Drop-down list selection ● AP pattern ● Client mode
Enable Relay	Wireless relay mode, that is, wireless AP plays the role of relay in the network connection, can realize the signal relay and amplification	Drop-down list selection ● yes ● deny
MAC address	Set the custom MAC address	user-defined
SSID	Set the custom WiFi name.	Enter a custom WiFi name
hide SSID	Configure it when selecting the AP mode. Used to configure whether WLANSSID is broadcast so that the client can search the SSID, usually disabled when you do not want others to search and use the WLAN function, disabled means the SSID function is hidden in the network environment, the user needs to manually add the SSID to connect.	Drop-down list selection ● yes ● deny

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

The parameter name	explain	collocation
wireless power	wireless power 0dBm (1 mW) 4dBm (2 mW) 5dBm (3 mW) …… 19dBm (79 mW) 20dBm (100mW)	Drop-down list selection The default is usually selected
channel	The working channel of WLAN, configured according to the specific requirements of the network environment, the default 1. The auto represents the channel adaptation, and the channel 6 is used by default when there is no interference. When the same channel is disturbed, it automatically jumps to the channel with less interference.	Drop-down list selection ● auto ● 1～11
bandwidth	Frequency width generally refers to the bandwidth can be used to identify the signal transmission of data transmission ability 20 mhz signal penetration force 40 mhz signal download ability	Drop-down list selection ● 20mhz ● 40mhz
Network system	WLAN network mode, the biggest difference of each network mode is that the transmission rate is quite different, the default bgn mixed mode. Manual is required when working mode.	Drop-down list selection ● n ：150Mbps ● And bg: 11Mbps, 54Mbps adaptive ● Bgn: 11Mbps, 54Mbps, 150Mbps mixed mode, adaptive according to the connected LAN client
Low response disconnected	No data interaction WIFI, automatically disconnected	Drop-down list selection ● yes ● deny

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Encryption mode	Configure the encryption mode of WLAN, so without encryption when encryption verification is not required. WEP encryption is relatively easy to crack, so it is recommended to use WPA encryption mode.	Drop-down list selection ● No encryption ● The WEP Open Certification ● The WEP shared key ● WPA ● WPA2 ● WPA/WPA2
WEP encryption mode (cable equivalent confidentiality, providing protection equivalent to cable LAN)		
Enable password groups	Connect to the password group used by the WLAN.	Drop-down list selection ● Password 1 ● Password 2 ● Password 3 ● Password 4
password	Enter the password for the access point that the router wants to access.	Enter a custom password of more than 8 digits
WPA / WPA 2 (WiFi Network Security Access)		
algorithm	The algorithm used by the encryption.	Drop-down list selection ● voluntarily ● Force the use of the CCMP (AES) encryption ● Enforce the use of TKIP encryption ● TKIP and CCMP (AES) hybrid encryption
password	Enter the password for the access point that the router wants to access.	Enter a custom password of more than 8 digits

Click OK to complete the configuration of the WLAN parameter.

—— **finish**

1.7 DHCP, the service configuration

background information

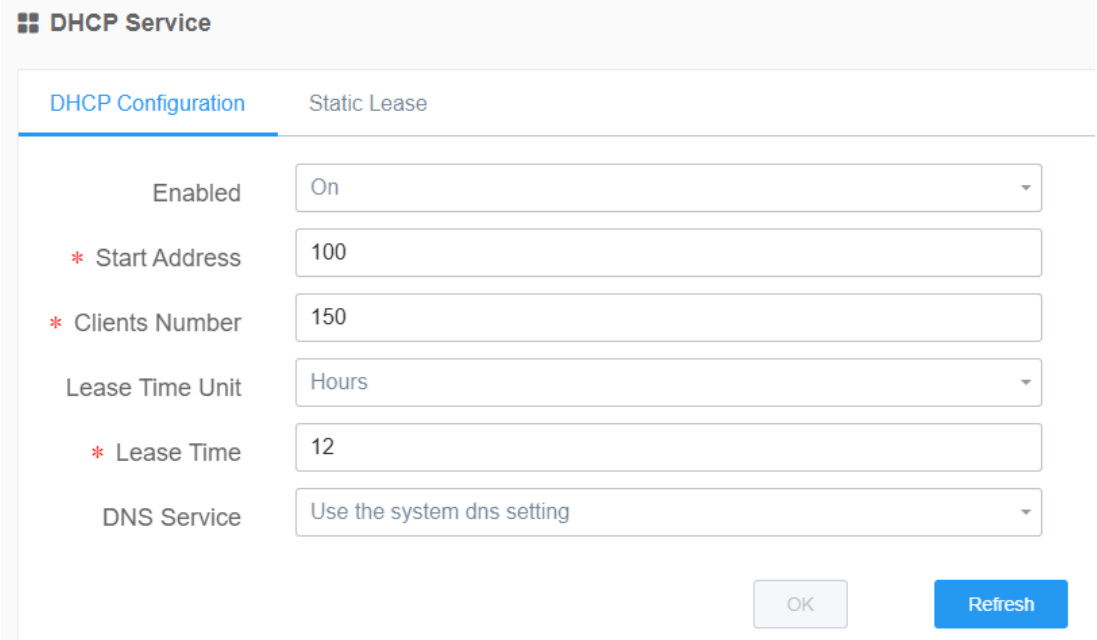
The Dynamic Host setup protocol (Dynamic Host Configuration Protocol, DHCP) is a LAN network protocol that works with the UDP protocol. After the DHCP function is

Copyright © 3onedata Co., Ltd.

enabled, the lower bit computer can automatically obtain the dynamic IP, eliminating the trouble of modifying the local IP after the gateway change.

operating steps

Step 1 After logging on to the WEB Configuration page, click Network Configuration> DHCP Services to open the DCHP Services tab.



Step 2 Configure the DHCP Server Settings, and the parameters are shown in Table 2-8.

1-Table 28 Description of the DHCP server settings

The parameter name	explain	collocation
start using	Use the DHCP function.	Drop-down list selection ● yes ● deny
Starting assignment of the base address	Configure the starting IP address for the DHCP address pool.	Default 100
Number of customers	Number of IP available later from the starting address IP.	Default 150
Rent time unit	hourly basis.	Drop-down list selection ● hour ● minute
reimbursed time	DHCP Client rents the IP time after acquiring the IP.	Enter the value

Step 3 Configure the "DHCP binding table" with parameters shown in Table 2-9.

The parameter name	explain	collocation

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
User IP address	Sets a statically specified IP address	form X.X.X.X
User MAC address	Set the MAC address for a statically specified DHCP	Format XX: XX: XX: XX: XX: XX

Step 4 Click OK to complete the configuration of the DHCP service parameters

—— **finish**

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

2 Application configuration

2.1 Keep online

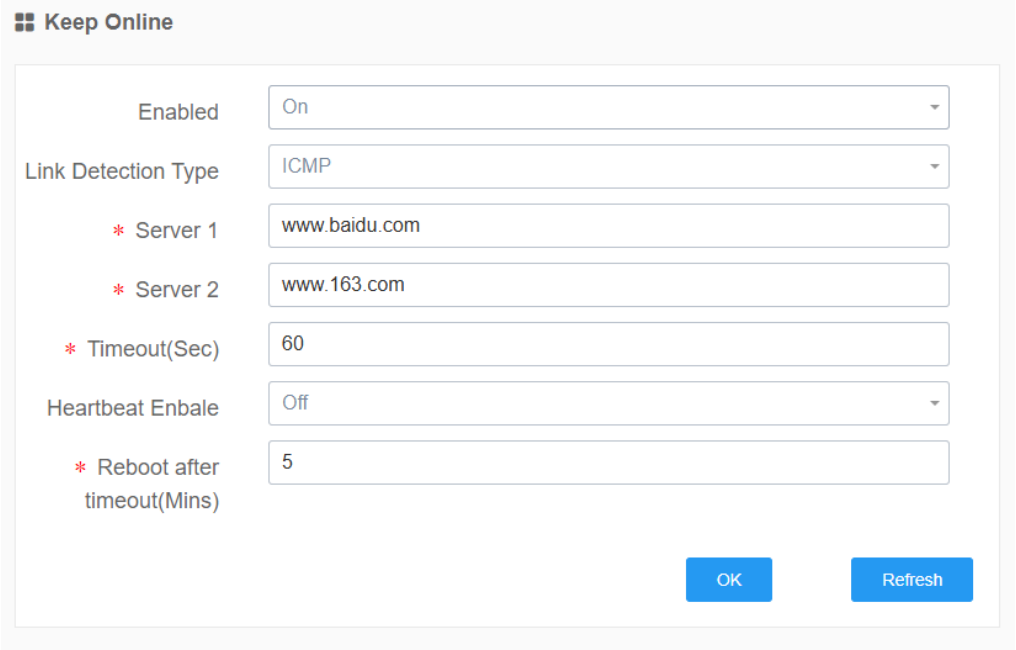
background information

Wireless network is false links (dial success and get IP, but the link) abnormal phenomenon, such as usually through LCP maintenance, three prosperous industrial wireless router in addition to support this detection method also provide more reliable ICMP link detection function, it through the ping package detection way detection communication link, when the user set action, realize the rapid recovery of link and system. At the beginning of the design, ICMP link detection is mainly used for the detection of wireless links. Sanwang industrial grade wireless router can support the detection of VPN and other tunnel links, and support multi-rule simultaneous detection, which greatly improves the recovery ability of product VPN tunnel and other link abnormalities.

operating steps

Step 1 After logging on to the WEB Configuration page, click Application Configuration> Online Hold to open the Online Hold tab.

Copyright © 3onedata Co., Ltd.



Step 2 Configure online hold parameters, as described in Table 3-1.

2-1Table 31 Description of the online retention rule parameters

The parameter name	explain	collocation
start using	Use the online Hold feature.	Drop-down list selection ● yes ● deny
Use the port	Using the port will determine the network status by accessing the port connection; if not checked, the ping package is detected through ICMP protocol.	Ports are not used by default
Server 1	The destination address to detect the network status can be the IP address or the domain name, set to the domain name needs to ensure that the router is configured with the correct DNS.	General W O R D type, maximum 64 bytes, input specification see" ”
Port 1	Port ports for connection when using the port.	Value range: 1 to 65535 Default 80
Server 2	The backup address of the network state, when the main address is not detected, if the backup address is not detected.	General W O R D type, maximum 64 bytes, input specification see"Parameter specification table”

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Port 2	Backup port.	Value range: 1 to 65535 Default 80
Timeout time	The time to detect the link timeout.	Default 30 seconds
Turn on the heartbeat test	Open the heartbeat detection not.	Drop-down list selection ● yes ● deny
Detection interval	Configuration to enable heartbeat detection.	Fill in the value
Off-line timeout restart	Network Exception timeout time	user-defined

Step 3 Click OK to complete the Online Hold configuration.

—— finish

2.2 Serial port application

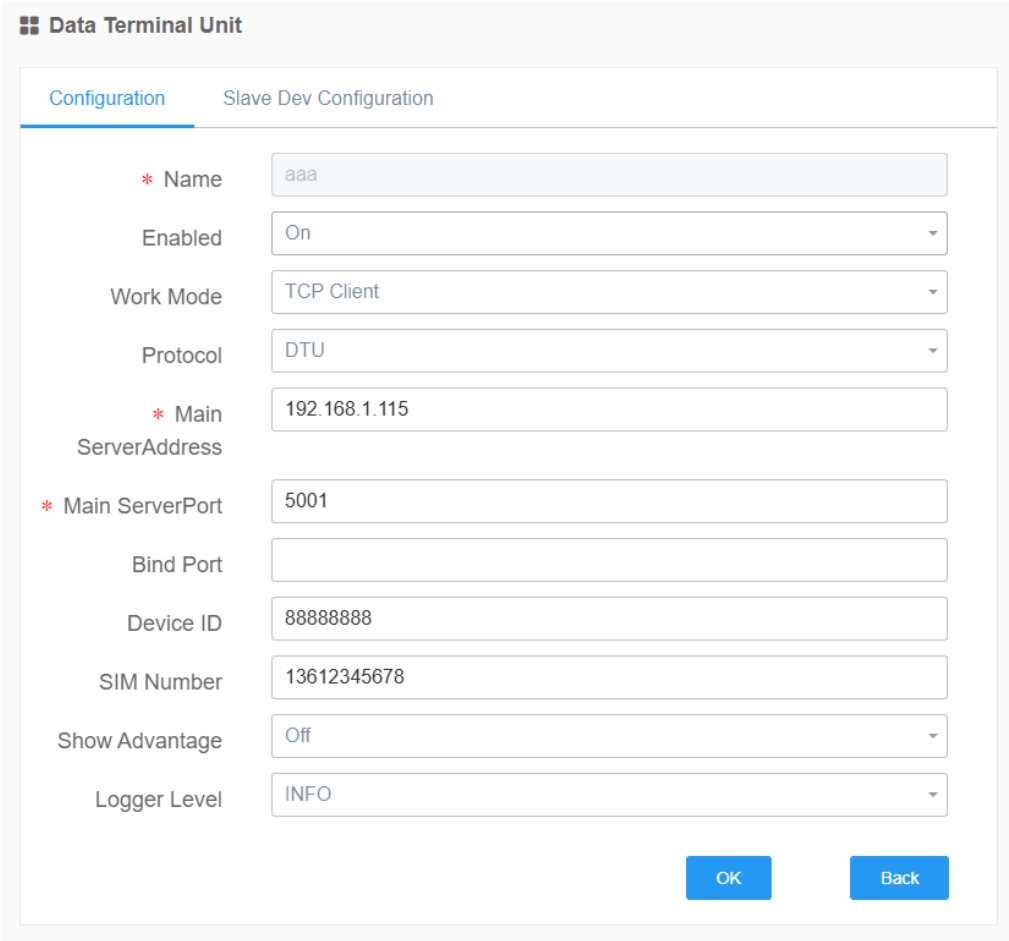
background information

The system has a built-in communication function with the registry center and the data center, which can provide a similar DTU function.

operating steps

Step 1 After logging on to the WEB Configuration page, click Apply Configuration> DTU to open the DTU tab.

Copyright © 3onedata Co., Ltd.



Step 2 If you are going to work in the DTU server operating mode, please configure the DTU parameters in the server operating mode, as described in Table 3-2.

2-Table 32 Description of the DTU parameters

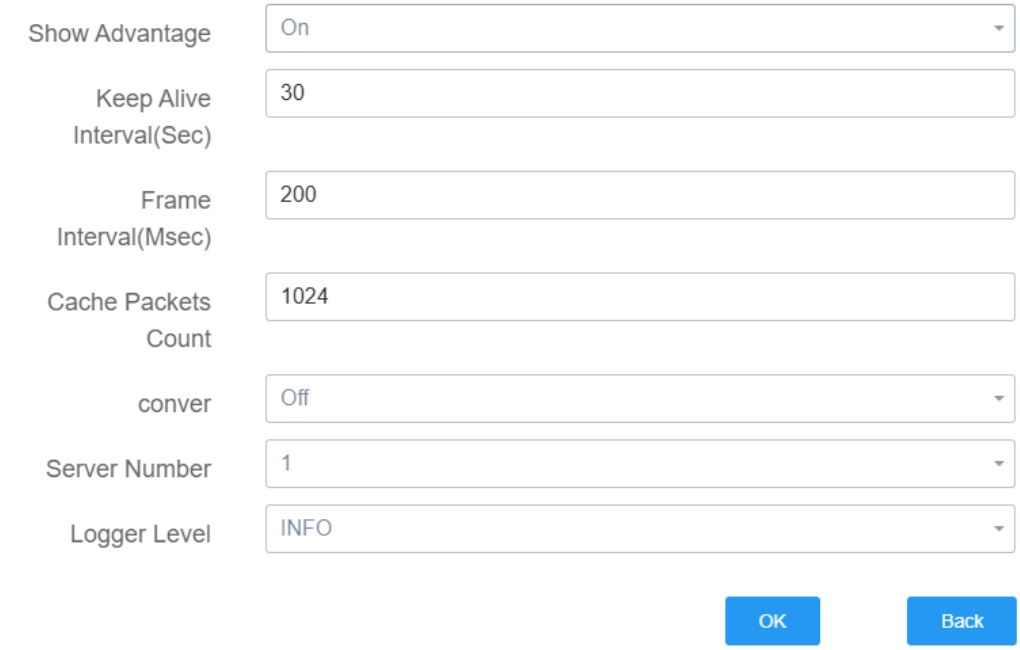
The parameter name	explain	collocation
start using	Whether to use the DTU function.	Drop-down list selection ● yes ● deny
String mouth selection	Serial port selection used by the DTU.	Drop-down list selection ● Console ● UART terminal
protocol	The protocol used by the DTU.	Drop-down list selection ● user-defined ● DTU ● MQTT ● HJ212 ● DC ● Modbus-Net-bridge ● 3H

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
primary center IP	The address of the DTU central server.	Enter manually in the input box form:X.X.X.X Default value: 192.168.1.115
Main center port	D T U Central server side port.	Value range: 0 to 65535
Baud rate	Select the serial port port rate.	Drop-down list selection ● 300 ● 600 ● 1200 ● … ● 57600 ● 115200
data bit	Serial port data transmission bits.	Drop-down list selection 5~8
check bit	Serial check bit.	Drop-down list selection ● None ● Odd ● Even
stop bit	Serial stop position.	Drop-down list selection ● 1 ● 2
equipment ID	Identification ID of the registry in the connected data.	8-bit 16-decimal number
SIM card number	Connect to the registered SIM card number in the data.	Enter the value

Step 3 In the Show Advanced Configuration drop-down box, select Yes for the DTU Advanced Configuration.

Copyright © 3onedata Co., Ltd.



Configure the advanced configuration parameters, which are described in Table 3-3.

2-Table 33 Description of the DTU advanced configuration parameters

The parameter name	explain	collocation
work pattern	D T U Working mode.	Drop-down list selection ● TCP, client ● UDP, client ● TCP, server
Heartbeat interval (seconds)	Time interval to the sending of the heartbeat packet.	Enter the numerical values manually
Data frame interval time (milliseconds)	Send each frame.	Manual input values
Maximum cache package number	Maximum number of cache packages.	Default: 1024
Is the escape	Escape heartbeat data	Drop-down list selection ● yes ● deny
Server number	The number of central servers, namely, the number of servers in effect.	Drop-down list selection ● 1~5
Server IP2	DTU central server address 2	manual input
Server port 2	DTU central server port 2	Value range: 0 to 65535

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Server IP3	DTU central server address 3	manual input
Server port 3	DTU central server terminal port 3	Value range: 0 to 65535
Server IP4	DTU central server address 4	manual input
Server port 4	DTU central server port 4	Value range: 0 to 65535
Server IP5	DTU central server address 5	manual input
Server port 5	DTU central server terminal port 5	Value range: 0 to 65535

Step 4 Click OK to complete the DTU, Server / client configuration.

—— **finish**

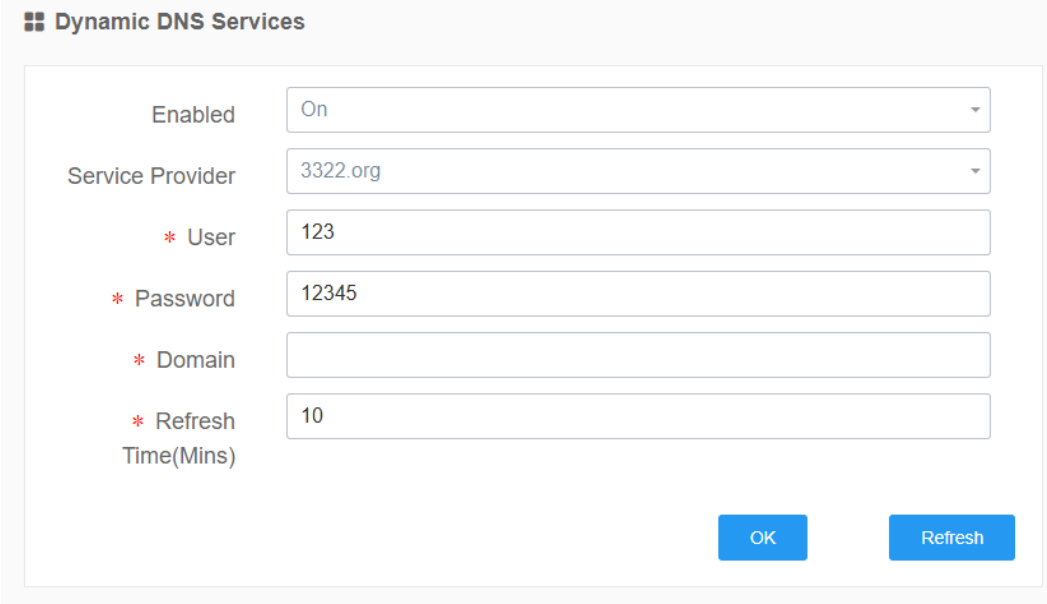
2.3 DDNS configure

background information

DDNS service allows a dynamic IP address to a fixed domain name resolution service provider, every time the user connected to the network when the client program will transfer the dynamic IP address of the host to the server program on the service provider host, server program is responsible for providing DNS service and implement dynamic domain name resolution, DDNS service allows you to assign a fixed domain name to the host dynamic WANIP, other users can access your host directly through the fixed domain name, rather than through the dynamic WANIP address. The router's dynamic WAN IP address is assigned directly by the ISP.

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

operating steps



After you login to the WEB configuration page, click Application Configuration> DDNS to open the DDNS Services tab.

Step 1 Configure the DDNS service parameters, and the parameters are described in Table 3-5.

2-2Table 35 DDNS, description of the parameters

The parameter name	explain	collocation
start using	Use the DDNS service.	Drop-down list selection ● yes ● deny
ISP internet	The domain name applied for corresponds to the domain name provider option. At present, our company does not support the DD N S service of domain name providers outside the list.	Drop-down list selection ● peanut shell ● dyndns.org ● changeip.com ● zoneedit.com ● free.editdns.net ● 3322.org ● …
User name / password	User name and password of the registered DD N S service provider domain name.	General W O R D type / C O D E type, with a maximum of 64 bytes

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
realm name	D D N S The domain name provided by the service provider, which corresponds to the IP of the router, usually visits the domain name to access the IP of the router.	General W O R D type, up to 64 bytes.
Refresh time (minutes)	The interval between the router and the DD N S domain name service provider updating DD N S related information, the service of some domain name provider is sending update data after the IP changes, the update interval depends on the DD N S service you buy, generally recommended more than 4 minutes.	Value range: 5~120 Unit: minutes Default: 10

Step 2 Click OK to complete the configuration of the DDNS service.

—— **finish**

explain

The IP address obtained from the SIM card service provider changes each time the router is restarted. If the user uses the applied DDNS domain name when logging in to the router remotely, the user can log in to the router page no matter how the router's modemIP address changes.

2.4 Traffic statistics

background information

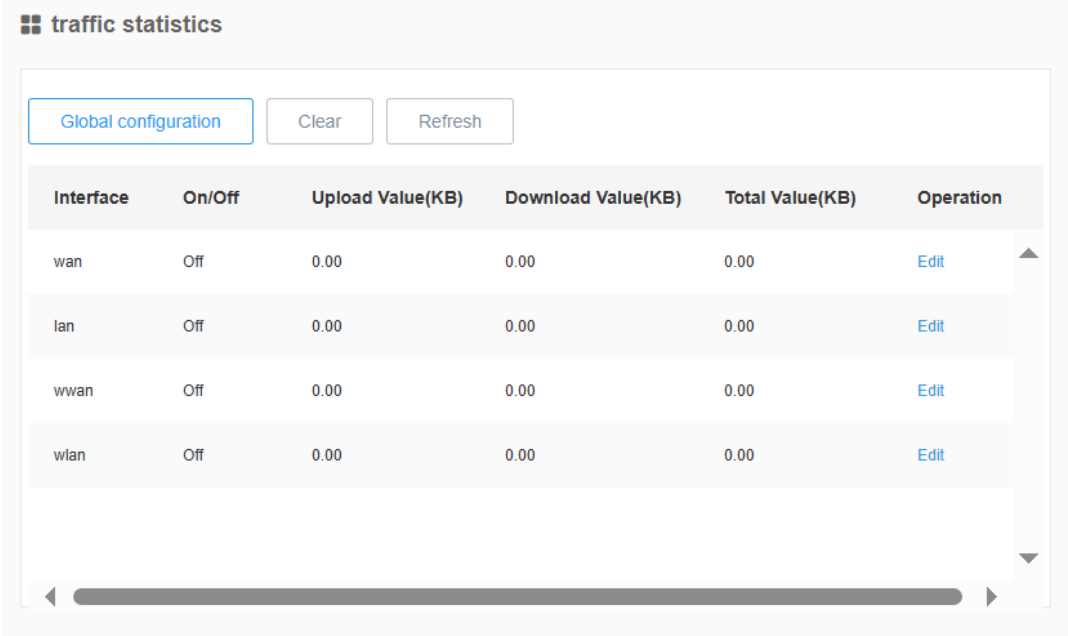
As a wireless router, most users are more concerned about the router traffic usage problem, so some functions are to count the traffic generated by the router wireless dial-up Internet access. The router will control the launch of the router according to the setting of the monthly traffic upper limit. When the router exceeds the monthly traffic upper limit, the router will disconnect the network, and users will be prohibited from accessing the external network to reach the limit of SIM card overtraffic. The traffic used at the beginning of each month will be cleared.

operating steps

Step 1 After logging into the WEB Configuration page, click Application Configuration>

Copyright © 3onedata Co., Ltd.

Traffic Statistics to open the Traffic Statistics tab.



Step 2 Configure flow statistics parameters, which are shown in Table 3-7.

2-3Table 37 Description of flow statistical parameters

The parameter name	explain	collocation
start using	Use the flow statistics function.	Drop-down list selection ● yes ● deny
WWAN Current Flow Rate (MB)	Set the traffic already used for the wireless WAN this month.	manual input Default: 0 unit:MB
Monthly WWAN Flow Upper Limit (MB)	Set the monthly flow threshold of the SIM card.	manual input Default: 1024 unit:MB
Save the f lash steps (MB)	The flow span when the flow statistics results are written to Flash, that is, the data is written to Flash after the accumulated flow used reaches the step length.	manual input. Default value 1 unit:MB
After the traffic exceeds the standard, limit the device to access the Internet	Whether the router restricts Internet access when the "current used traffic" exceeds the "monthly traffic limit".	Drop-down list selection ● yes ● deny

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

The parameter name	explain	collocation
WAN Current Flow Rate (MB)	Set the traffic already used on the WAN this month.	manual input Default: 0 unit:MB

Step 3 Click OK to complete the configuration of the traffic statistics.

—— **finish**

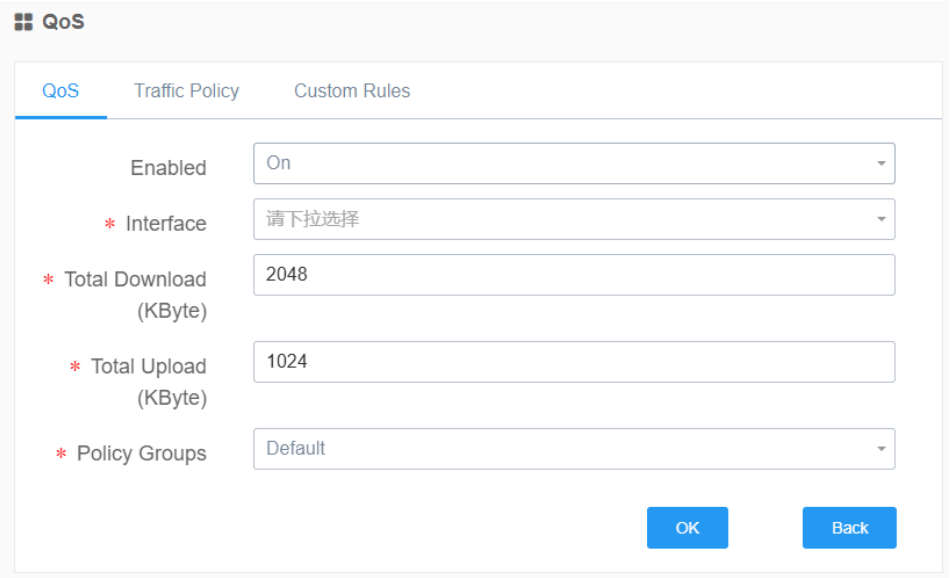
2.5 Qos

background information

The QoS function is mainly for the bandwidth control, allocating the bandwidth for download and upload on demand.

operating steps

Step 1 After logging on to the WEB Configuration page, click the Application Configuration> Qos to open the Qos tab.



Step 2 Qos parameters and parameter description are shown in Table 3-8.

2-4Table 38 Description of the Qos parameters

The parameter name	explain	collocation
start using	Whether to use the Qos feature.	Drop-down list selection ● yes ● deny
Download (KByte)	The size of the bandwidth of the user downlink.	Manual input values

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Upload (KByte)	The bandwidth size of the user uplink.	Manual input values

Step 3 Click OK to complete the configuration of the Qos.

—— **finish**

2.6 timed task

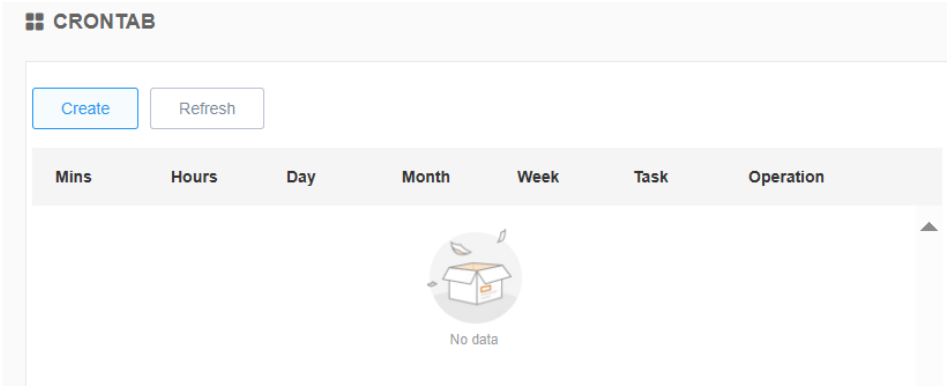
background information

As a wireless service gateway routing product, many customers hope to control the online duration of the router when using it, so as to better manage the network service and 3G / 4G / 5G charges. Sanwang industrial router task management can meet such needs of customers, customers can configure multiple online time periods (such as a few hours a day) according to their needs, in addition, it can also realize the task execution at the time point (such as dialing or restart the system at midnight every day).

operating steps

Step 1 After logging on to the WEB Configuration page, click Apply Configuration> Timing Tasks to open the Timing Tasks tab. The timing task list parameters are shown in Table 3-9.

2-5Table 39 Description of the timing task list parameters

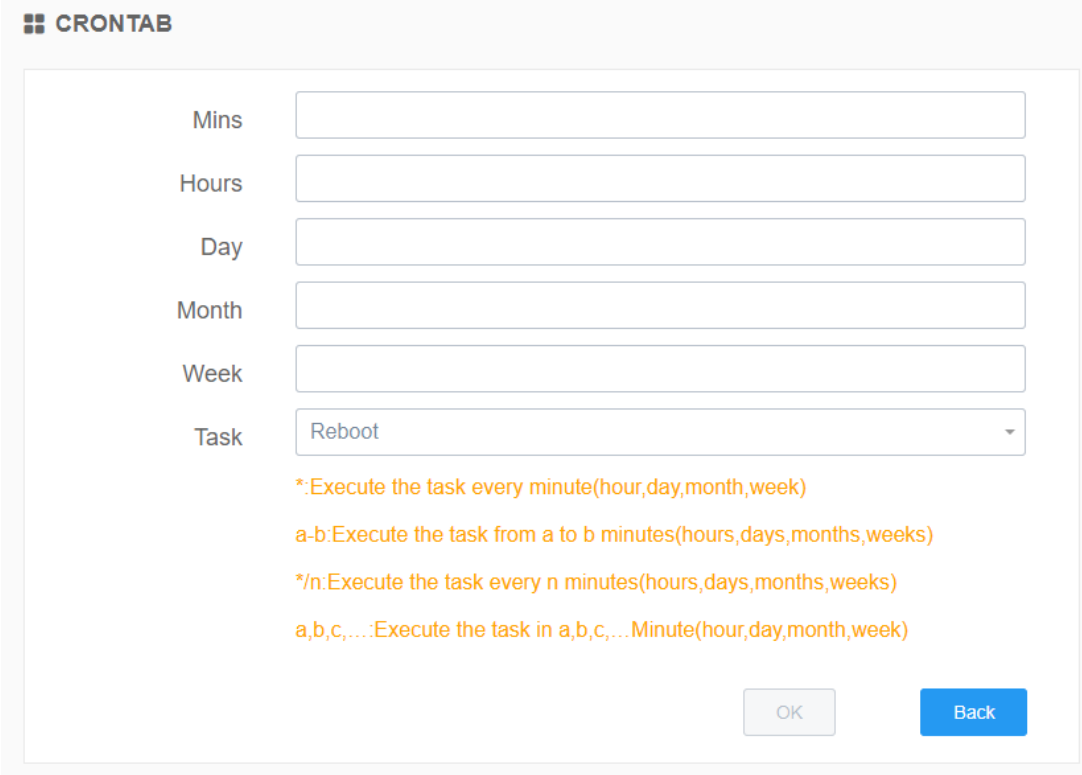


The parameter name	explain
minute	Time points for combination use, and every X minutes for independent use.
hour	Time points for combination use and every X hours for independent use.

Copyright © 3onedata Co., Ltd.

The parameter name	explain
date	One day of the month.
moon	month.
week	week.
assignment	The task of execution.
operate	You can edit and delete scheduled tasks.

Click Create to create a new timing task.



Step 2 The timing task parameters are shown in Table 3-10.

2-6Table 310 Description of the timing task rule parameters

The parameter name	explain	collocation
minute	Time points for combination use, and every X minutes for independent use.	● If the value is entered directly, it is the time point, and the value range is 0~59 ● If you add "* /" to the value X, perform the task every X minutes

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
hour	Time point for combined use, Every X hours for independent use.	● If the value is entered directly, it is the time point, and the value range is 0~23 ● If you add "* /" to the value X, perform the task every X hours
date	One day of the month.	Value range: 1~31, multiple dates are separated by ",""
moon	month.	Value range: 1~12, with "," separating them available for multiple months
week	week.	Value range: 1~7, separated by "," for multiple days, and "x-y" for consecutive days
assignment	The task of execution.	Drop-down list is optional: ● reboot ● close LAN ● open LAN

Step 3 Click OK to complete the configuration of the timing task.

—— **finish**

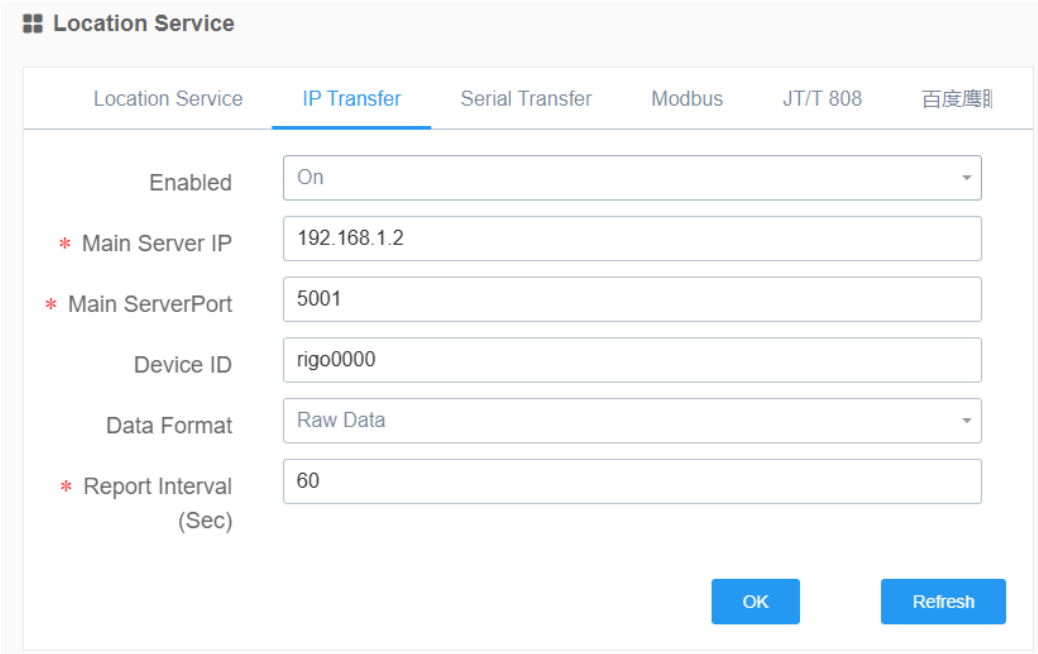
2.7 Location service

Note that the IRT2000-A1-1T1D-12-LV does not support the location service

operating steps

Step 1 After logging on to the WEB Configuration page, click Apply Configuration> Location Services to open the Location Services tab.

Copyright © 3onedata Co., Ltd.



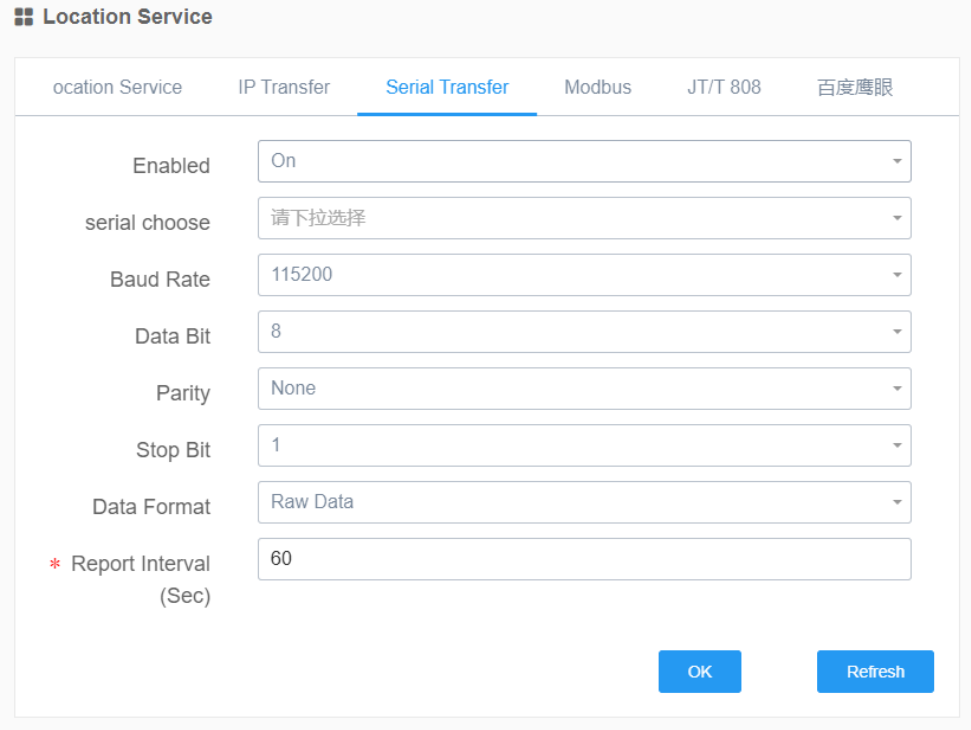
Step 1 Configure the location service parameters as described in Table 3-11.

2-7Table 311 Description of the location service IP forwarding parameters

The parameter name	explain	collocation
start using	Whether to use the location service.	Drop-down list selection ● yes ● deny
primary center IP	The address of the central server.	Enter manually in the input box form:X.X.X.X Default value: 192.168.1.2
Main center port	Central server side port.	Value range: 0 to 65535
equipment ID	Device ID number.	The 8-bit character
data type	Location data type.	Drop-down list selection ● initial data ● location data ● GPGGA ● GPRMC ● IEC101
GPS reporting interval (seconds)	Time interval for the reported location.	Value range: 1~500

Step 2 Configure the serial port forwarding parameters, which are shown in Table 3-12.

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



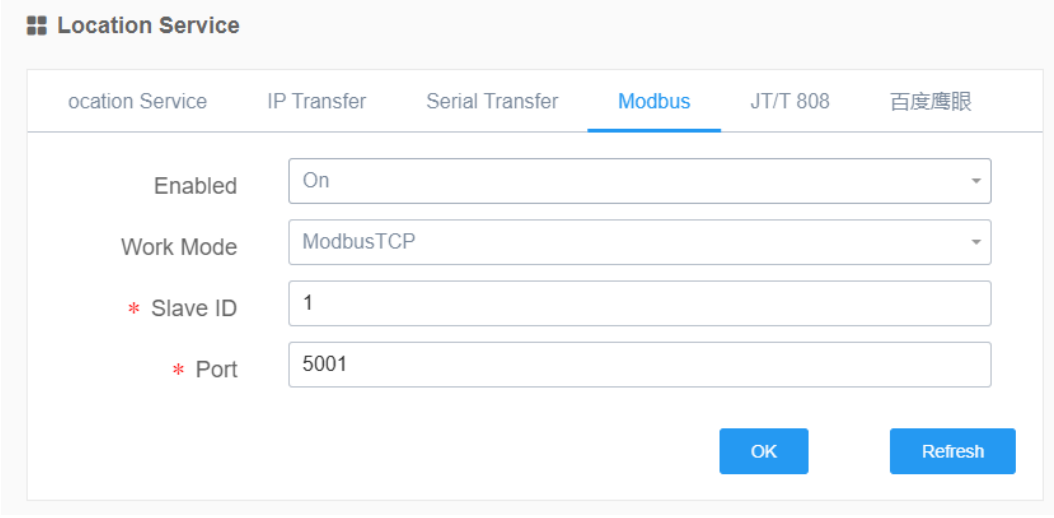
2-Table 312 Location service serial port forwarding, parameter description

The parameter name	explain	collocation
start using	Whether to use the location service.	Drop-down list selection ● yes ● deny
String mouth selection	Provide multi-serial port selection (some models only support console serial port interface)	Drop-down list selection ● console ● COM1 ● COM2 ● COM3 ● COM4
Baud rate	Select the serial port port rate.	Drop-down list selection ● 300 ● 600 ● 1200 ● … ● 57600 ● 115200
data bit	Serial port data transmission bits.	Drop-down list selection 5~8

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
check bit	Serial check bit.	Drop-down list selection ● None ● Odd ● Even
stop bit	Serial stop position.	Drop-down list selection ● 1 ● 2
data type	Location data type.	Drop-down list selection ● initial data ● location data ● GPGGA ● GPRMC ● IEC101
Reporting interval (seconds)	Report cycle unit of seconds	The default is 60 seconds

Step 3 Configure the location service Modbus parameter, as described in Table 3-13.



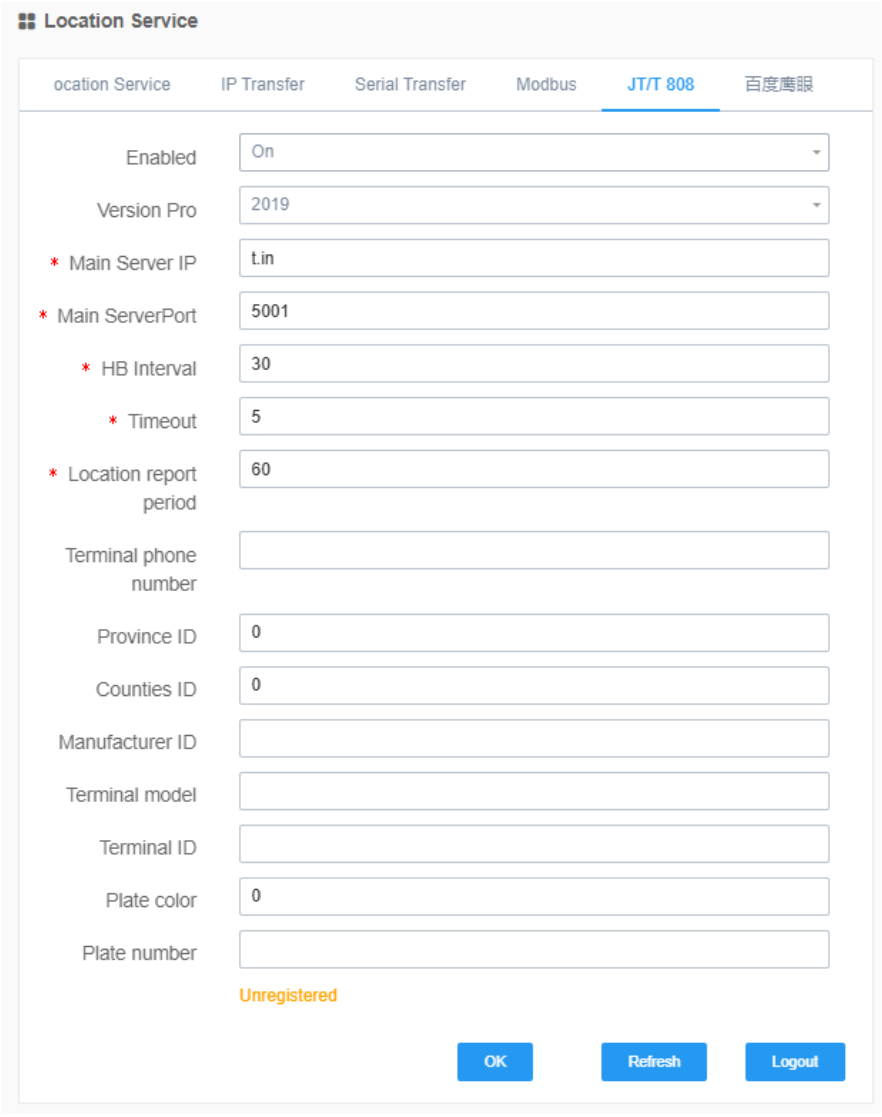
2-Table 313 Description of the location service Modbus parameters

The parameter name	explain	collocation
start using	Whether to use the location service.	Drop-down list selection ● yes ● deny
work pattern	ModbusTPC/ModbusRTU	Drop-down list selection ● ModbusTPC ● ModbusRTU

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
From the station number	The slave station number is 1 byte, and the value range is from 0 to FFH	That is between 1 and 255
port	Port number within the range of 0- - -65535	Port number within the range of 0- - -65535

Step 4 Configure the location service JT / T808, and the parameters are described in Table 3-14.



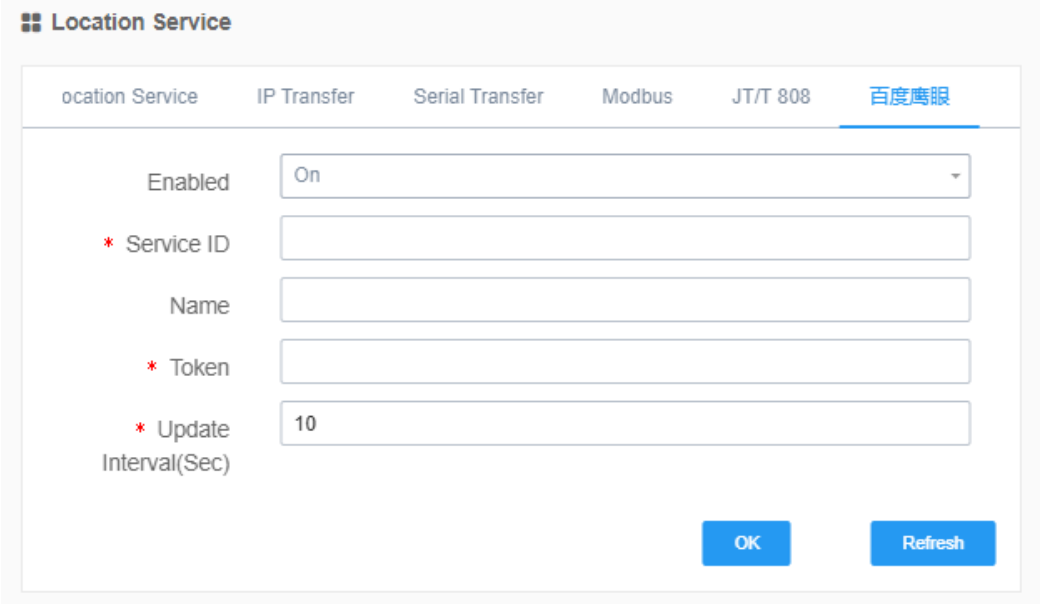
2-Table 314 Location service JT / T 8 08 reference, number description

The parameter name	explain	collocation

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
start using	Whether to use the location service	Drop-down list selection ● yes ● deny
Protocol version	Transport Vehicle Satellite Status System Agreement 2019 / 2013	Drop-down list selection ● 2019 ● 2013
primary center IP	The address of the central server	Enter manually in the input box form:X.X.X.X Default value: 192.168.1.2
Main center port	Central server side port	Value range: 0 to 65535
Heartbeat cycle	Send a heartbeat in between N seconds	Range of values: 0-4294967295
Timeout time	The time to detect the link timeout	Range of values: 0-4294967295
Location reporting interval	Location interval reporting cycle	Range of values: 0-4294967295

Step 5 The parameters are shown in Table 3-15.



2-Table 315 Description of Baidu Eagle Eye

The parameter name	explain	collocation

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
start using	Whether to use the location service	Drop-down list selection ● yes ● deny
serve ID		
name		
T oken		
Update interval time	Data update time	The values range from 1 to 999999999 seconds

explain

Baidu Eagle eye related configuration information should be obtained through Baidu platform and filled in the relevant configuration.

Copyright © 3onedata Co., Ltd.

3 VPN configure

3.1 VPDN configuration (L 2 TP / PPTP)

background information

VPDN English for Virtual Private Dial-up Networks, also known as virtual private dial-up network, is a kind of VPN service, is a virtual private dial-up network service based on dial-up users. That is, surfing the Internet by dial-up access is a secure virtual private network established by using the carrying function of IP network combined with the corresponding authentication and authorization mechanism. It is a technology developed rapidly with the development of Internet in recent years. VPDN supports two protocols, L 2 TP and PPTP.

PPTP (Point to Point Tunneling Protocol) Point-to-point tunnel protocol is a network technology that supports multi-protocol virtual private network, which is also the second layer protocol. Through this protocol, remote users can securely access the company network through Windows mainstream operating systems and other systems equipped with peer-to-peer protocols, and dial up to local ISPs to securely link to the company network through Internet.

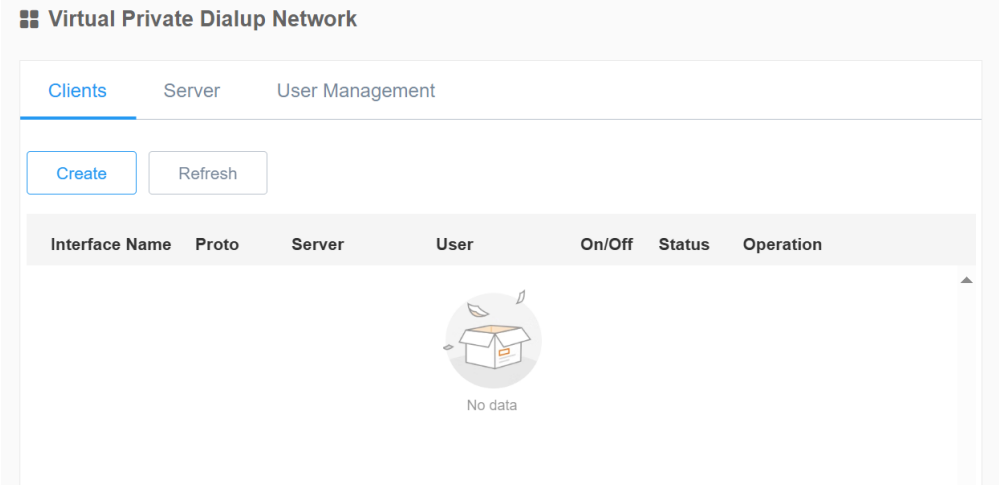
L 2 TP (Layer Two Tunneling Protocol) second layer channel protocol, which is a VPDN (virtual private dial-up network) technology, is dedicated to the channel transmission of the second layer of data. L 2 TP provides a means of remote access control, the user dials the company's local network access server (NAS) through PPP to access the company's internal network, obtain the IP address and access the corresponding permission of network resources. The employee dial into the company network as safe and convenient as in the company LAN.

operating steps

Step 1 After logging on to the WEB Configuration page, click "VPN Config" > L 2 TP / PPTP ", click the Client Create tab. List of VPDN channel parameters are shown in

Copyright © 3onedata Co., Ltd.

Table 4-1.

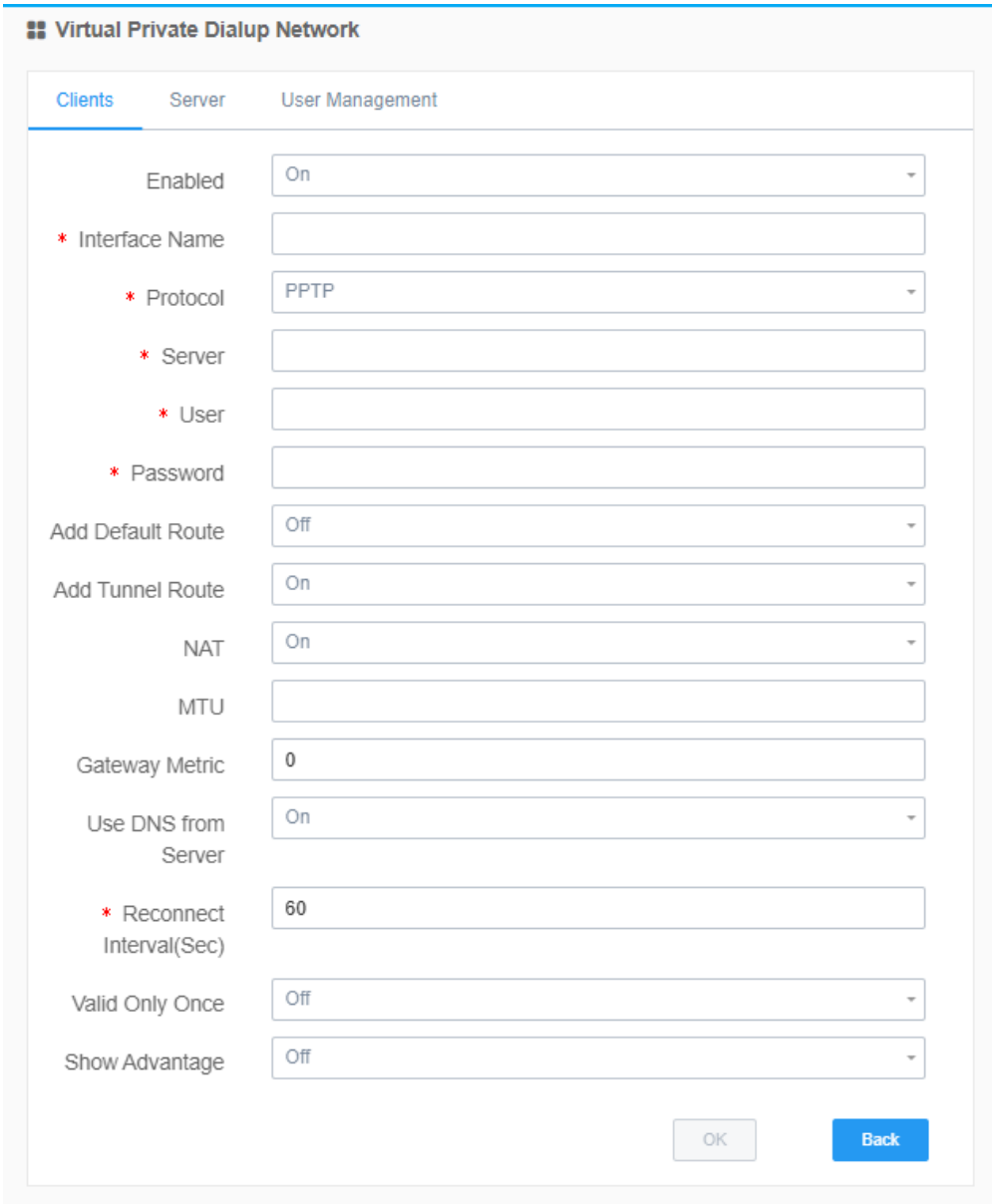


3-1Table 41 List of VPDN channels

The parameter name	explain
The interface name	The name of the VPDN rule.
protocol	The protocol adopted by the VPDN.
server	Server IP address or domain name used for access access.
user name	A legitimate access user authorized by the access server.
start using	Whether the VPDN channel rule is enabled.
state	The VPDN channel rule is in its current state.
operate	You can edit and delete scheduled tasks.

Step 2 Click Create to create a new VPDN channel.

Copyright © 3onedata Co., Ltd.



Step 3 Configure the VPDN rule parameters, as described in Table 4-2.

3-2Table 42 Description of the parameters of the VPDN rules

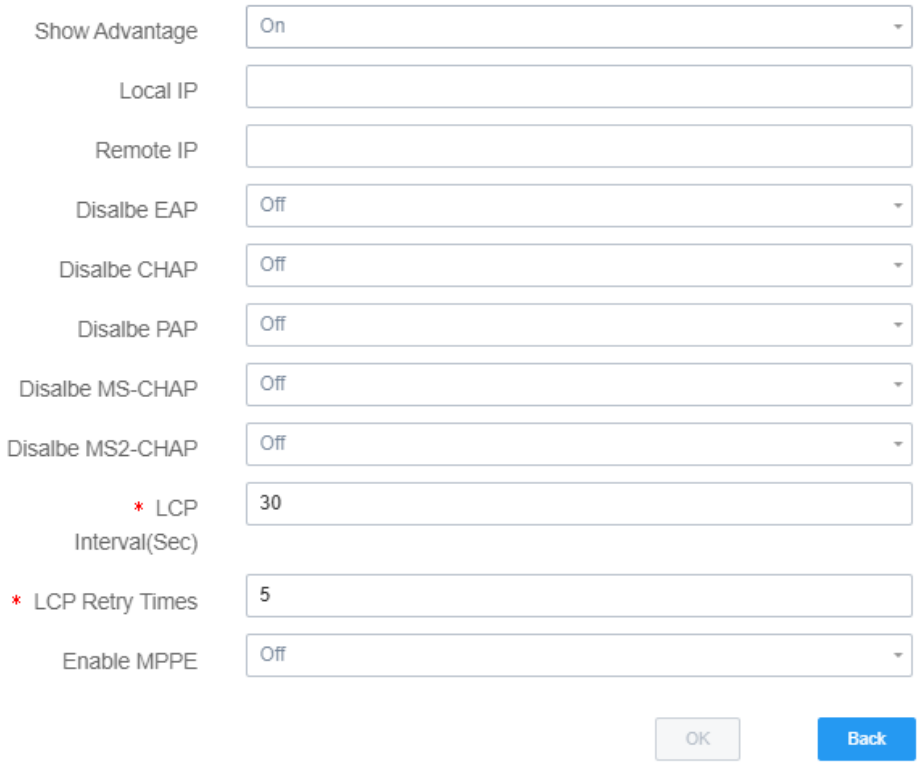
The parameter name	explain	collocation
start using	Whether the VPN connection is enabled.	Drop-down list selection ● yes ● deny
The interface name	The name of the VPDN rule.	Easy identifiable names are recommended. Such as city-city, specific events, etc
protocol	The protocol adopted by the VPDN.	Drop-down list selection ● PPTP ● L2TP

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
server	Server IP address or domain name used for access access.	Fill the server IP address or domain name for access
User name / password	Legal access user and password as authorized by the access server.	Fill in the legal access user name / password authorized by the access server
Add default routing	After the VPN connection is successful, the default route is set to this VPN tunnel.	Drop-down list selection ● yes ● deny
Add tunnel routing	Add a route that gives the opposing subnet access to the local subnet.	Drop-down list selection ● yes ● deny
NAT	Whether to use the NAT function.	Drop-down list selection ● yes ● deny
MTU	Set the maximum transmission unit.	Manual input values The default value is 1500
Gateway jump point	Set the number of jumps of the gateway after the VPN connection.	manual input
Use the server to specify the DNS	Whether to use the server's DNS.	Drop-down list selection ● yes ● deny
Reconnection interval (seconds)	Time interval between equipment reconnection.	manual input
It is not enabled after restart	After the router restart, the VPN will be closed.	Drop-down list selection ● yes ● deny

Step 4 In the Show Advanced Configuration drop-down box, select Yes for the VPDN Advanced configuration.

Copyright © 3onedata Co., Ltd.



Configure the advanced configuration parameters, which are described in Table 4-3.

3-3Table 43 VPDN, advanced configuration

The parameter name	explain	collocation
this locality IP	Set up the local static tunnel IP address.	Enter manually in the input box form:X.X.X.X
far-end IP	Set up the opposite-end static tunnel IP address.	Enter manually in the input box form:X.X.X.X
forbidden EAP	EAP authentication.	Drop-down list selection ● yes ● deny
forbidden CHAP	The CHAP certification is not used.	Drop-down list selection ● yes ● deny
forbidden PAP	PAP authentication.	Drop-down list selection ● yes ● deny
The MS-CHAP is disabled	The MS-CHAP certification is not used.	Drop-down list selection ● yes ● deny

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
The MS2-CHAP is disabled	The MS2-CHAP certification is not used.	Drop-down list selection ● yes ● deny
LCP interval time (seconds)	The time interval between sending the LCP package request.	Manual input values
Number of LCP	Send LCP package request timeout retry times.	Manual input values
start using MPPE	Enable the Microsoft peer-to-peer encryption protocol.	Drop-down list selection ● yes ● deny
Stateless MPPE is enabled	Stateless MPPE, which is configured when MPPE is enabled.	Drop-down list selection ● yes ● deny
Enable the MPPE40	MPPE 40 Bit encryption, which is configured when MPPE is enabled.	Drop-down list selection ● yes ● deny
Enable the MPPE128	MPPE 128 Bit encryption, which is configured when MPPE is enabled.	Drop-down list selection ● yes ● deny

3.2 L 2 TP server function configuration

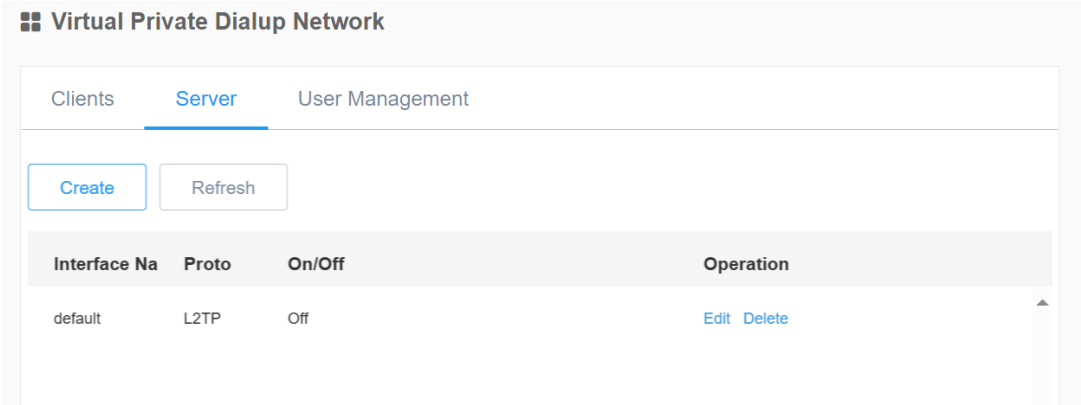
background information

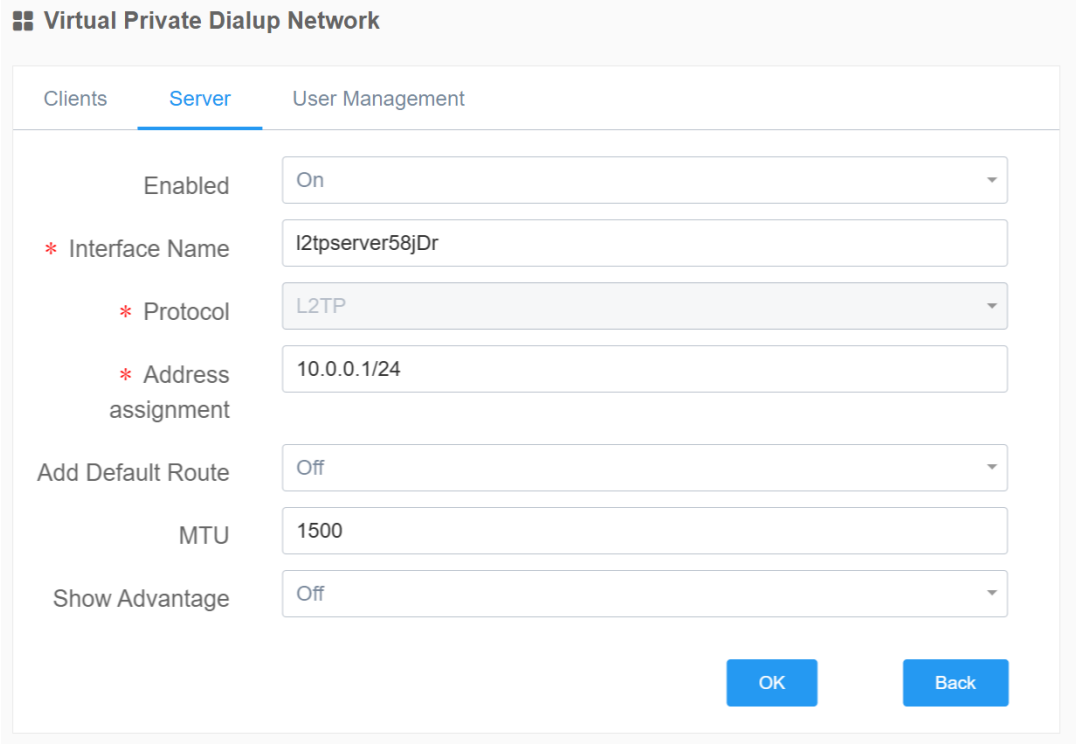
The L 2 TP server is deployed at the corporate headquarters and usually serves as a gateway to the corporate headquarters. The L 2 TP server receives the user information transmitted by the L 2 TP client, authenticates the connected user identity, responds to the L 2 TP tunnel connection request initiated by the L 2 TP client, and establishes the L 2 TP connection together with the L 2 TP client.

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

operating steps

Step 1 After logging on to the WEB configuration page, click "" VPN Settings" > L 2 TP / PPTP setting ", the description of the VPDN channel list parameters are shown in Table 4-1-1.



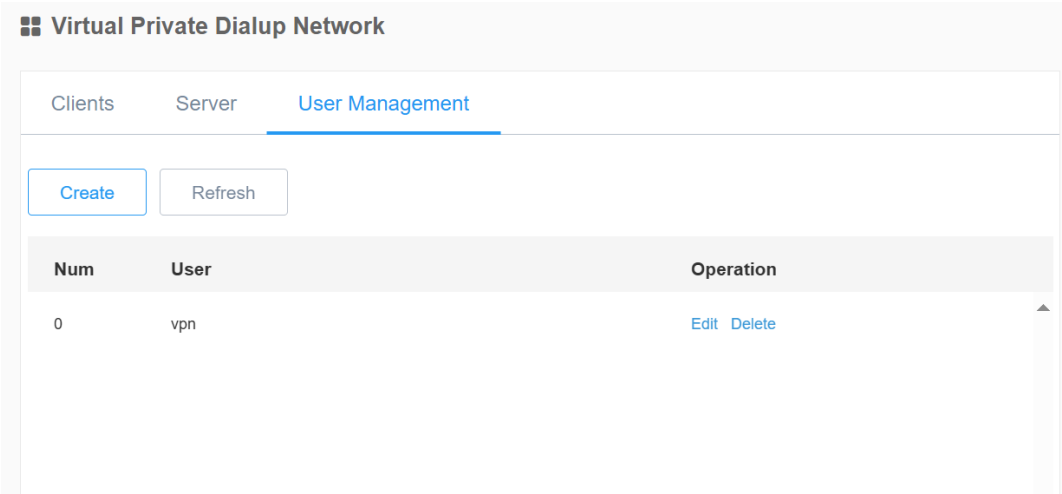


Copyright © 3onedata Co., Ltd.

34Table 41-1 Description of the parameters of the L 2 TP server configuration list

The parameter name	explain
start using	Drop-down list selection ● yes ● deny
The interface name	The name of the VPDN rule.
protocol	L2TP
address assignment	Set up the private network IP address and address pool of the L 2 TP server. Gateway IP " is the gateway address of the L 2 TP client, and the Subnet mask determines the dynamic allocation to L 2 TP and the IP address resource of the client.
Add default routing	Drop-down list selection ● yes ● deny
MTU	Set the maximum transmission unit and enter the value manually The default value is 1500

Step 2 The parameters of the user management configuration table are described in Table 4-1-2.



35Table 41-1 L 2 TP username configuration list parameters are shown in Table 4-1-3

The parameter name	explain

Copyright © 3onedata Co., Ltd.

The parameter name	explain
user name	The user name of the remote dial-up user.
password	Password of the remote dial user

Step 3 Click OK to complete the L 2 TP server configuration.

—— **finish**

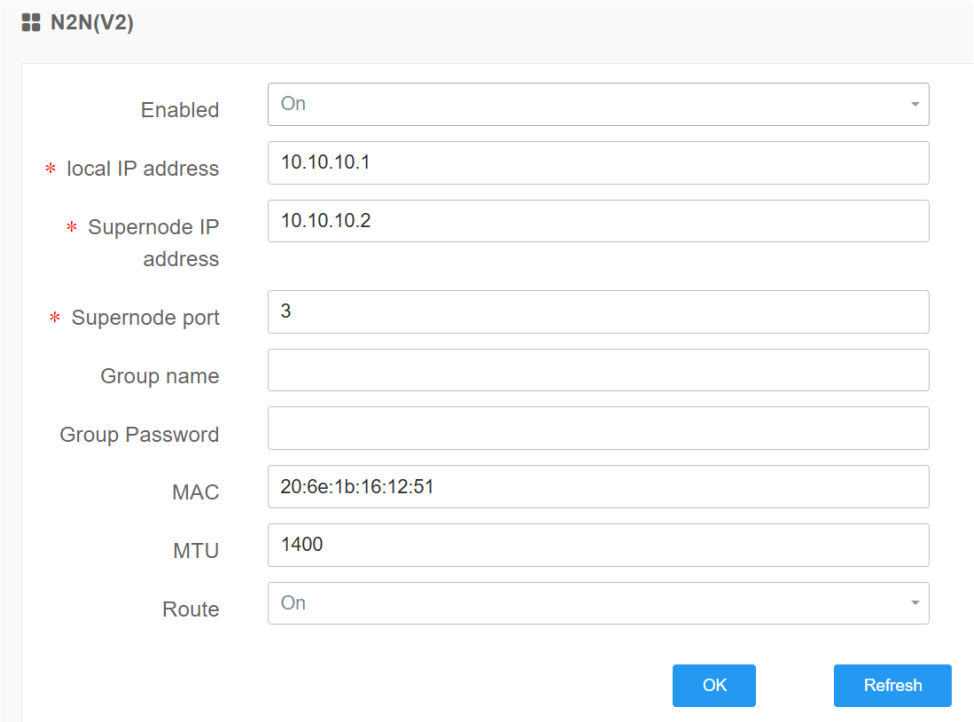
3.3 The N2N_v2 configuration

background information

The N2N is designed to provide a decentralized, management-free, secure, and stable network connection, regardless of the user's location, IP address, and network type. Generally speaking, there is no need for public network IP, do not need to configure NAT, through the firewall.

operating steps

Step 1 After logging on to the WEB configuration page, click VPN Settings> N2N_v2 to open the N2N_v2 tab.



Step 2 Configure the N2N_v2 parameter, and the parameter description is shown in Table 4-4.

3-6Table 44 Description of N 2 N _ v 2 parameters

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
start using	Whether to use the N2N_v2 connection.	Drop-down list selection ● yes ● deny
local IP	Set up an Intranet IP address.	Enter manually in the input box form:X.X.X.X
Supernode IP	The IP that connects the supernode.	Enter manually in the input box form:X.X.X.X
Super node port	The port to connect the supernode.	Value range: 0 to 65535
Communication group	Name of the N2N communication organization.	Filled in the name character of the distribution group
Communication group password	Password used by the distribution group.	Filling in the legal access password authorized by the access distribution group
MAC address	Interface physical address of the N2N node.	Normal does not modify, manual modification when there are special needs, format: XX: XX: XX: XX: XX: XX
MTU	Maximum data transmission unit. Default: 1500.	Manual input values
route	Add a default route for the N2N interface.	Drop-down list selection ● yes ● deny

Step 3 Click OK to complete the configuration of N2N_v2.

—— **finish**

3.4 OPENVPN

background information

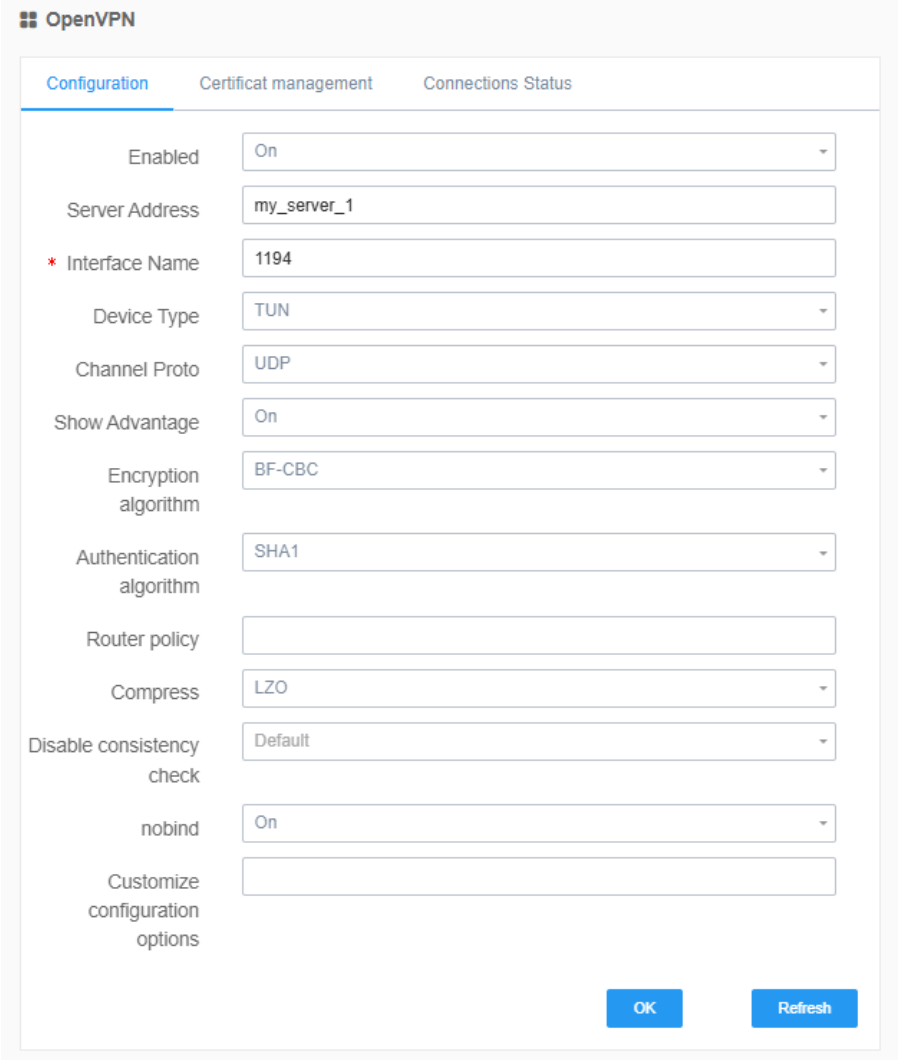
OPENVPN All communications are based on a single IP port, default and UDP protocol communication is recommended, and TCP support. The official port of (Internet Assigned Numbers Authority) designated by IANA to the OPENVPN is 1194. In OPENVPN, if the user access a remote virtual address (address series belonging to the virtual network card, different from the real address), the operating system will send packets (TUN mode) or data frame (TUN mode (TAP mode) to the virtual network card through the routing mechanism, the service program receives the data

Copyright © 3onedata Co., Ltd.

and conduct the corresponding processing, will be sent from the external network through the SOCKET. This completes a process of one-way transmission, and vice versa. When the remote service program receives the data from the external network through the SOCKET, and conducts the corresponding processing, it will be sent back to the virtual network card, then the application software can receive it.

operating steps

Step 1 After logging on to the WEB Configuration page, click VPN Settings> OPENVPN to open the OPENVPN tab.



Step 2 Configure OPENVPN parameters, parameter description are shown in Table 4-5.

3-7Table 45 Description of the OPENVPN parameters

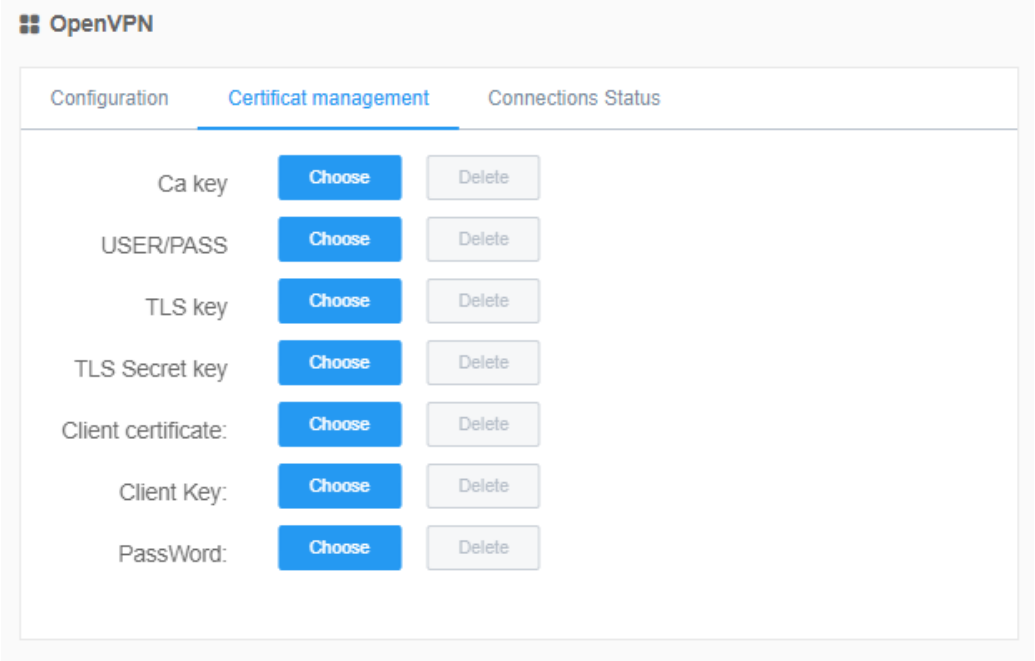
The parameter name	explain	collocation
start using	Whether to use the OPENVPN connection.	Drop-down list selection ● yes ● deny

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Server address	The opposite-end IP address or the domain name of the remote OPENVPN server.	manual input
The interface name	The port of the server.	Value range: 0 to 65535
device type	Channel device type.	Drop-down list selection ● TUP ● TAP
Channel protocol	Channel protocol, selected according to the application requirements.	Drop-down list selection ● UDP ● TCP
Routing strategy	Routing policy is currently in use.	manual input
Compress with the LZO	Whether to use the LZO compression algorithm.	Drop-down list selection ● YES ● NO
way of encryption	Whether to encrypt the data	Drop-down list selection ● BF-CBC ● RC2-40-CBC ● CACT5-CBC ● RC2-64-CBC .....
Certification algorithm	Whether to encrypt the data	Drop-down list selection ● SHA1 ● RSA-MD5 ● MD5 .....
Disable the option consistency check	No option consistency check is used.	Drop-down list selection ● yes ● deny
Local addresses and ports are not bound	Local addresses and ports are not bound.	Drop-down list selection ● yes ● deny

Step 3 Configure the certificate management configuration parameters as described in Table 4-6.

Copyright © 3onedata Co., Ltd.



3-8Table 46 Description of the OPENVPN advanced configuration parameters

The parameter name	explain	collocation
Certified of CA certificate	CA certificate.	Choose to upload Delete the uploaded certificate Update of the uploaded certificate
TA certificate	TA certificate.	Choose to upload Delete the uploaded certificate Update of the uploaded certificate
Local certificate	Local certificate.	Choose to upload Delete the uploaded certificate Update of the uploaded certificate
Local private key	Local key.	Choose to upload Delete the uploaded certificate Update of the uploaded certificate

Step 4 Click OK to complete the configuration of the OPENVPN.

—— **finish**

3.5 IPSEC

background information

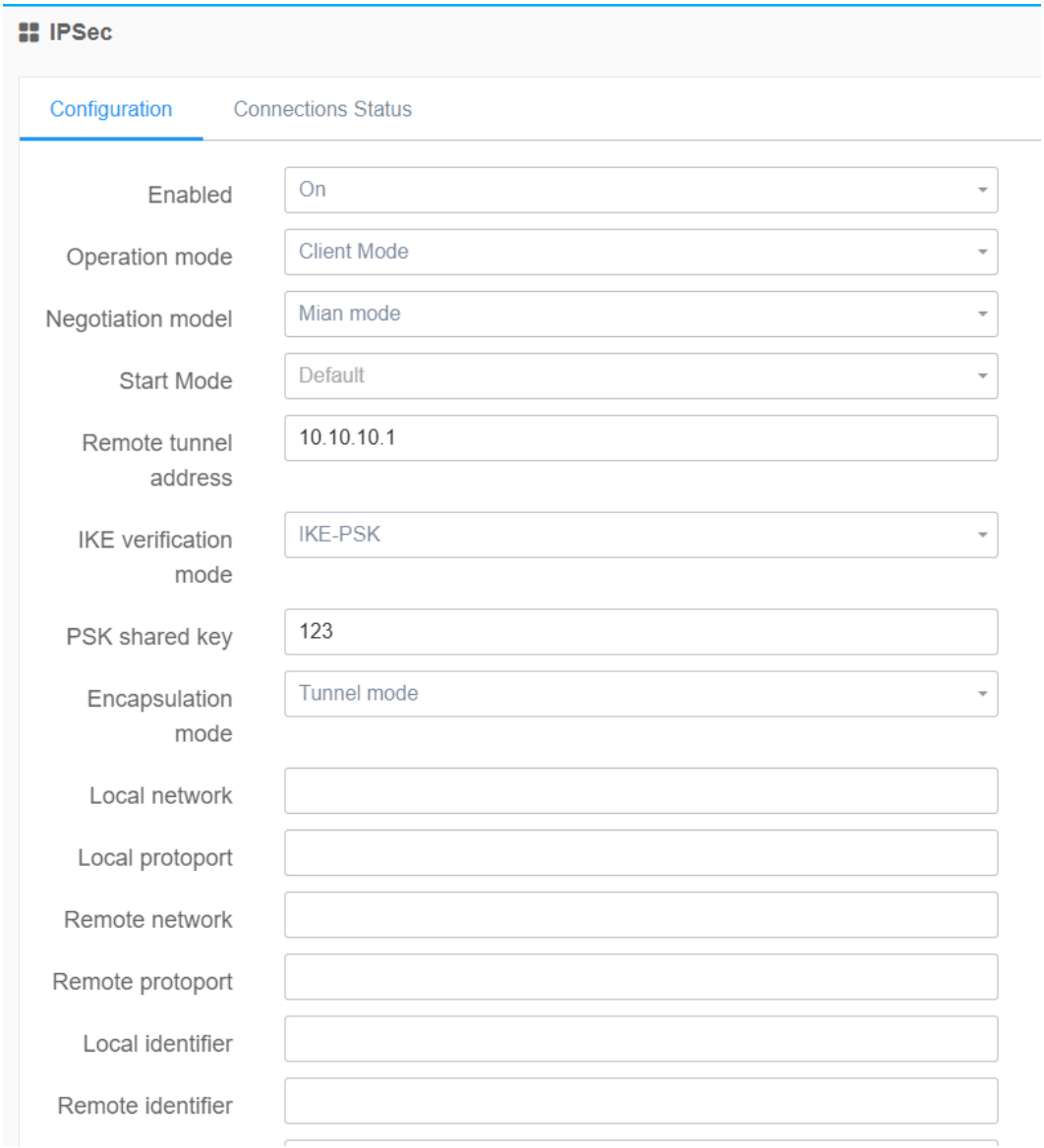
IPSec VPN refers to a VPN technology that uses IPSec protocol to realize remote access. IPSec, called Internet Protocol Security, is a security standard framework

Copyright © 3onedata Co., Ltd.

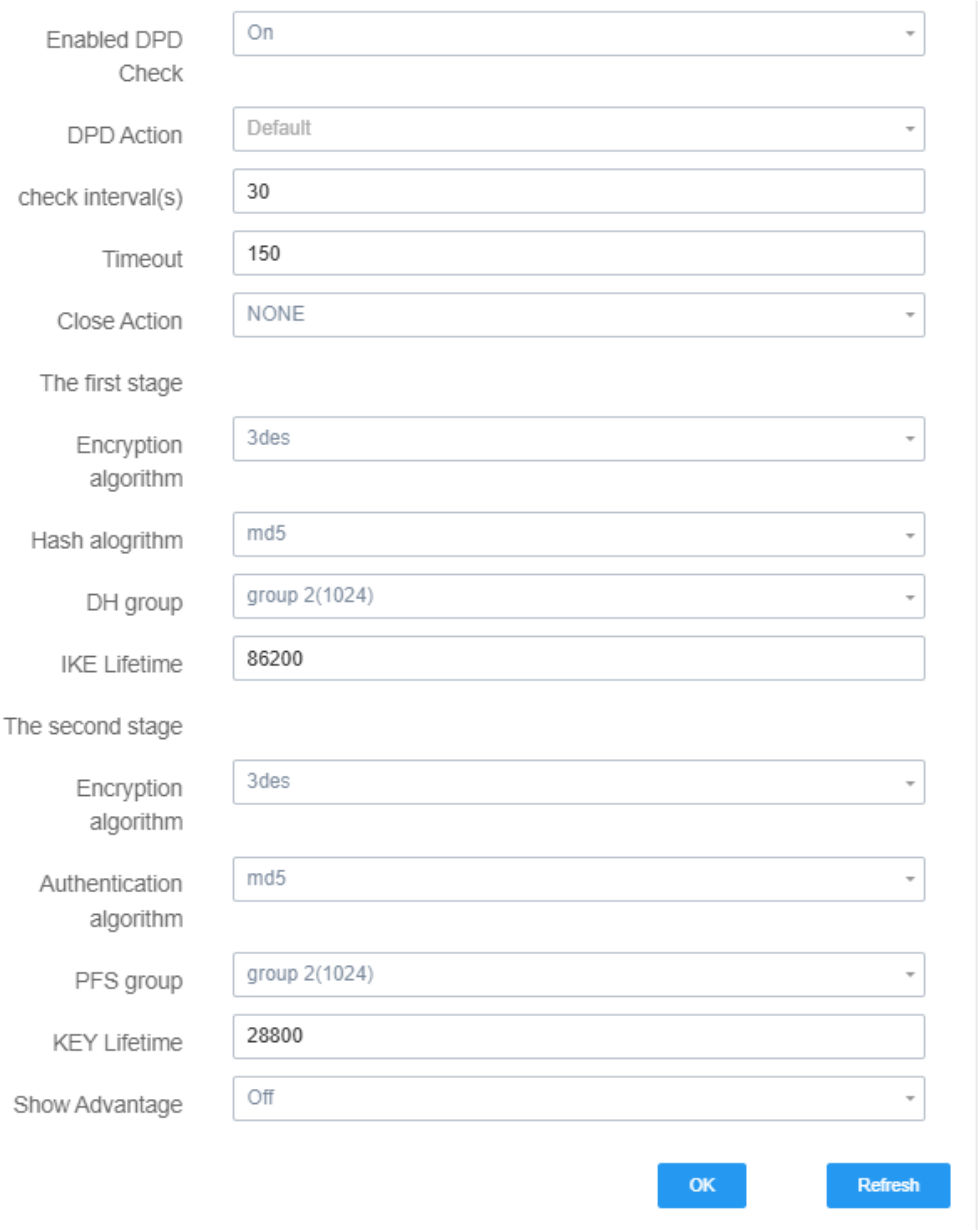
defined by Internet Engineering Task Force (IETF) to provide end-to-end encryption and authentication services for public and private networks. IPSEC Is a relatively complete system of VPN technology, it stipulates a series of protocol standards.

operating steps

Step 1 After logging on to the WEB Configuration page, click VPN Settings> IPSEC to open the IPSEC tab.



Copyright © 3onedata Co., Ltd.



Step 2 Configure the IPSEC parameters as described in Table 4-7.

3-9Table 47 Description of the IPSEC parameters

The parameter name	explain	collocation
start using	Whether to use the IPSEC function.	Drop-down list selection yes deny
Negotiation mode	Select the negotiation mode of IKE. If IPSEC, the IP address at one end of the tunnel is automatically acquired.	Drop-down list selection Active mode Savage mode

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Start mode		Drop-down list selection voluntarily detonate by contact add
The paired-end address	Set up the paired-end IP address or the domain name.	Fill in the IP address or domain name of the paired-end address
The IKE authentication mode	Select the authentication mode that the IKE negotiated.	Drop-down list selection ● IKE-PSK ● IKE-PSK-XAUTH
Packaging mode	Select the data packet encapsulation format	Drop-down list selection ● Tunnel mode ● transmission mode
Share the key	The key used.	WORD string, up to 64-bit, see" "
Local subnetwork	Enter the local subnet address and mask that the IPSEC contains.	Interface type A.B.C. D / M, for the input specification, see" "
To the terminal network	Enter the opposite-terminal subnet address and mask that the IPSEC contains.	Interface type A.B.C. D / M, for the input specification, see" "
This end of the logo	Local address identification.	manual input
The paired-end identification	Pend address identification.	manual input
Enable the PDP detection	Whether to use the PDP test.	Drop-down list selection ● yes ● deny
PDP movement	The PDP heartbeat selection	Drop-down list selection ● clean up ● keep ● reconnection
Detection interval (seconds)	The PDP detection time interval	Manual input values
More than time	Detection over time.	Manual input values

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
way of encryption	Select the encryption mode for the first stage.	Drop-down list selection ● aes128 ● aes192 ● aes256 ● 3des ● des
Hash algorithm	Select the hash algorithm.	Drop-down list selection ● md5 ● sha1 ● sha256 ● sha384 ● sha512
DH group	Select the DH grouping to apply to the IKE negotiation.	Drop-down list selection ● group 1（768） ● group 2（1024） ● group 5（1536） ● group 14（2048） ● … ● group 18（8192）
IKE life cycle	Set the survival time in the IKE negotiation. IKE negotia new SA before the SA expires; the new SA is established; the old one is cleared immediately after expiration.	Manual input values

Step 3 Click OK to complete the configuration of the IPSEC.

—— **finish**

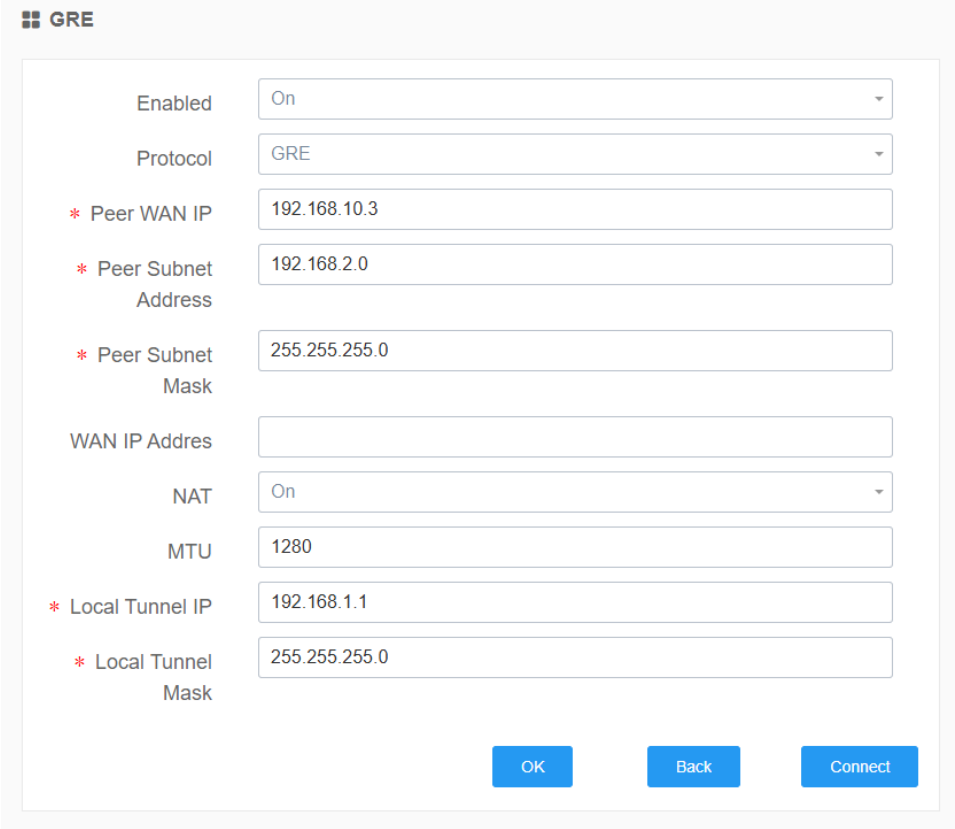
3.6 GRE

background information

GRE VPN (Generic Routing Encapsulation), the general routing encapsulation protocol, is the encapsulation of some network layer protocols (such as IP and IPX), so that these encapsulated datagram can be transmitted in another network layer protocol (such as IP). GRE is the third layer tunnel protocol of VPN (Virtual Private Network), where a technology called Tunnel (tunnel) is used between the protocol layers.

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

operating steps



Step 1 After logging on to the WEB Configuration page, click the VPN Settings> GRE to open the GRE tab.

Step 2 GRE parameters and parameter description are shown in Table 4-8.

3-10Table 48 Description of the GRE parameters

The parameter name	explain	collocation
start using	Whether to use the GRE function.	Drop-down list selection ● yes ● deny
Paired-end, WAN IP	Set up the opposite-end IP address of the GRE tunnel.	Enter manually in the input box form:X.X.X.X
Addresses to terminal network	Set the subnet address of the opposite-end IP of the GRE tunnel.	Enter manually in the input box form:X.X.X.X
Propair terminal network mask	Set the opposite-terminal subnet mask of the GRE tunnel.	Enter manually in the input box form:X.X.X.X
Local end of the WAN IP	Set up the local IP address of the GRE tunnel.	Enter manually in the input box form:X.X.X.X

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Local-end tunnel IP	Set the subnet address of the local IP of the GRE tunnel.	Enter manually in the input box form:X.X.X.X
Tunnel mask at this end	Set the local subnet mask for the GRE tunnel.	Enter manually in the input box form:X.X.X.X
MTU	Set the maximum transmission unit.	Manual input values The default value is 1500

Step 3 Click OK to complete the GRE configuration.

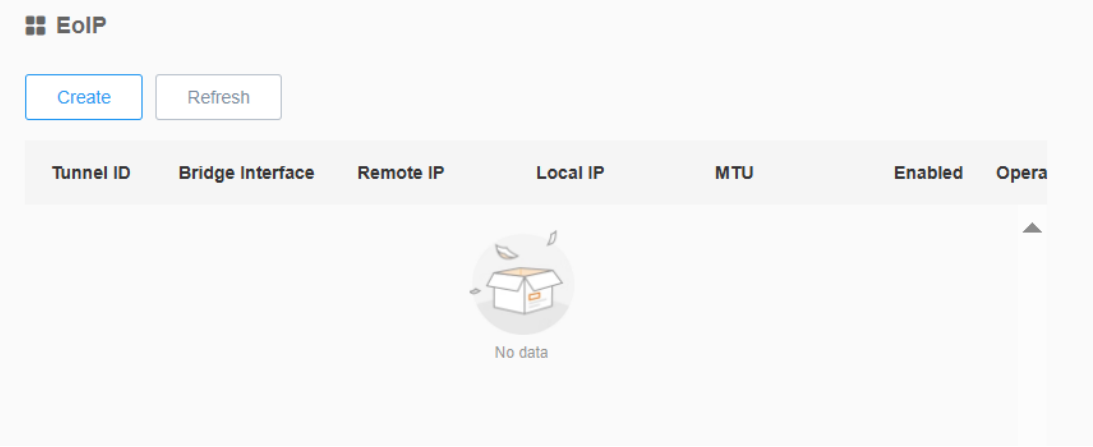
3.7 EoIP

background information

The EoIP (Ethernet over IP) tunnel is an Ethernet tunnel protocol built between the IP transmission layers of the two routers. The EoIP interface is similar to Ethernet transmission. When the bridging function of the router is enabled, all Ethernet data traffic (all Ethernet protocols) will be bridging, that is, the same LAN spans the IP layer to realize the remote second layer network interconnection.

operating steps

Step 1 After logging on to the WEB configuration page, click the VPN Settings> EoIP to open the EoIP tab.



The EOIP list parameters are described in Table 4-9.

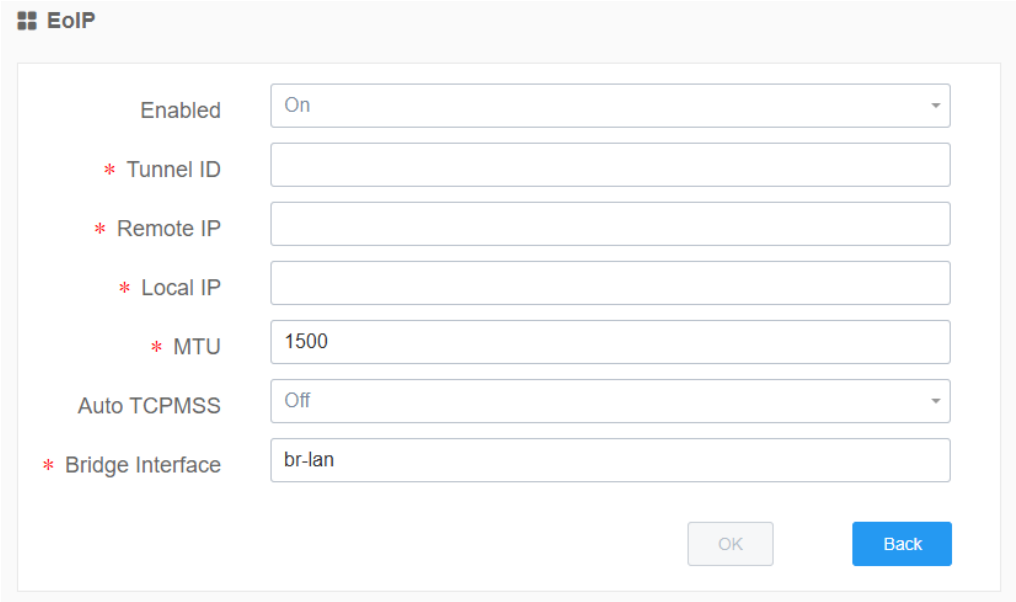
Table 4-9 Description of the EoIP list parameters

The parameter name	explain
tunnel ID	Displays the tunnel ID number for the CI.

Copyright © 3onedata Co., Ltd.

The parameter name	explain
Bridge interface	Displays the interface name that the CI bridges on.
Far end address	Displays the remote address configured by the configuration key.
Address at this end	Displays the local address configured by the configuration key.
start using	Disows whether the key status is enabled.
operate	The CI can be edited or deleted.

Step 2 Click Create to create a new EoIP tunnel.



Step 3 Configure the IP parameters for EoP, as described in Table 4-10.

Table 4-10 EoIP, with a description of the parameters

The parameter name	explain	collocation
start using	Whether to use the EoIP function.	Drop-down list selection ● yes ● deny
tunnel ID	Set the EoIP tunnel ID number, both ends of the tunnel ID number must be consistent.	Enter manually in the input box form:X.X.X.X
Far end address	Set up the opposite-end WAN IP address of the EoIP tunnel.	Enter manually in the input box form:X.X.X.X

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Address at this end	Set up the local WAN IP address of the EoIP tunnel.	Enter manually in the input box form:X.X.X.X
Bridge interface	Configure the interface name that requires bridging.	Fin the router network interface name that needs to be bridging. The default settings are for the br-lan interface.

Step 4 Click OK to complete the parameter configuration for the EoIP functionality.

—— **finish**

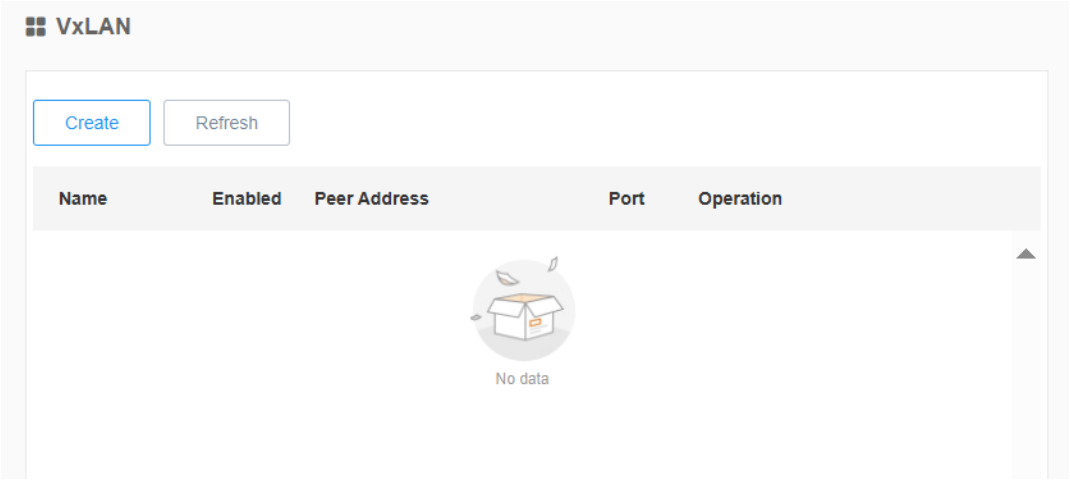
3.8 VXLAN

background information

VXLAN Is a network virtualization technology that can improve the expansion problem of large cloud computing during deployment, and is an extension of vlan. VXLAN Is a powerful tool that extends the second layer through a three-layer network. It addresses the portability limitations of VMS (Virtual Memory Systems) by packaging traffic and extending it to a tier 3 gateway, enabling access to servers on an external IP subnet

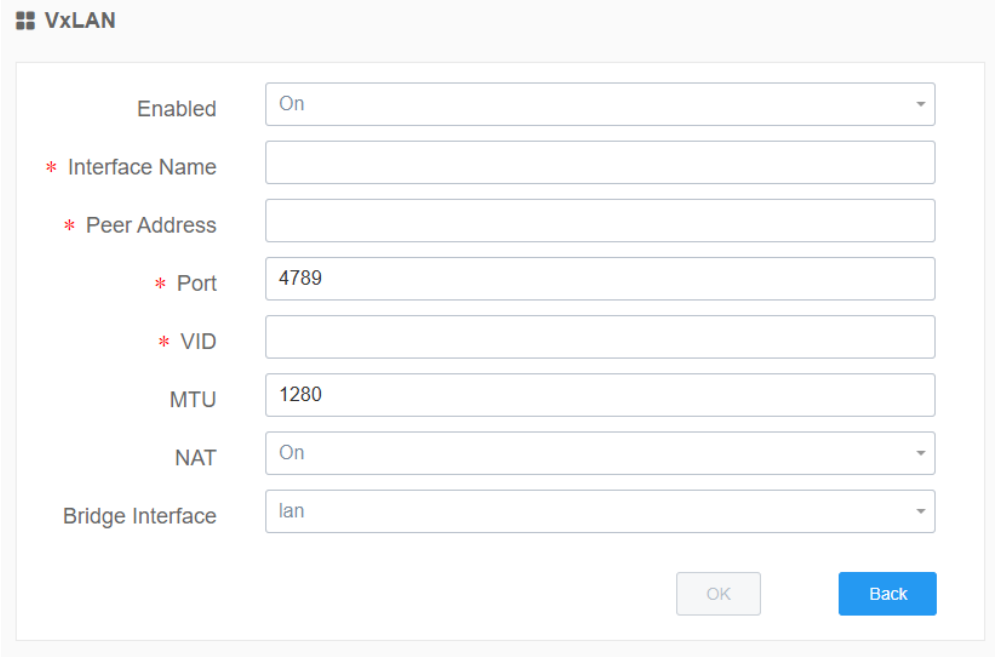
operating steps

Step 1 After logging on to the WEB Configuration page, click VPN Settings> VXLAN to open the VXLAN tab.



Step 2 Click Create to create a new VXLAN tunnel.

Copyright © 3onedata Co., Ltd.



Step 3 Configure the VXLAN parameters, the parameter description is shown in Table 4-12.

Table 4-12 Description of the VXLAN parameters

The parameter name	explain	collocation
start using	Whether to use the VXLAN function.	Drop-down list selection ● yes ● deny
The interface name	This article is a VXLAN, and the name of the rule	user-defined
The paired-end address	Set up the paired-end IP address or the domain name.	Fill in the IP address or domain name of the paired-end address
port	Connection port	4,789, by default
VID	Displays the ID number of the configuration item.	Value range from 0 to 16777215
MTU	Maximum transmission unit	Manual configuration
NAT	address translation	Drop-down list selection ● yes ● deny
Bridge interface	not have	default LAN

Copyright © 3onedata Co., Ltd.

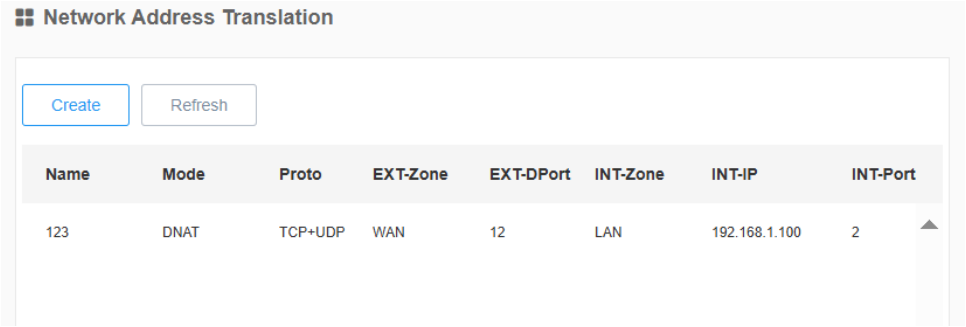
4 Forward configuration

4.1 NAT

operating steps

Step 1 After logging on to the WEB Configuration page, click the Forward Settings> NAT to open the NAT TAB. The descriptions of the NAT list parameters are shown in Table 5-1.

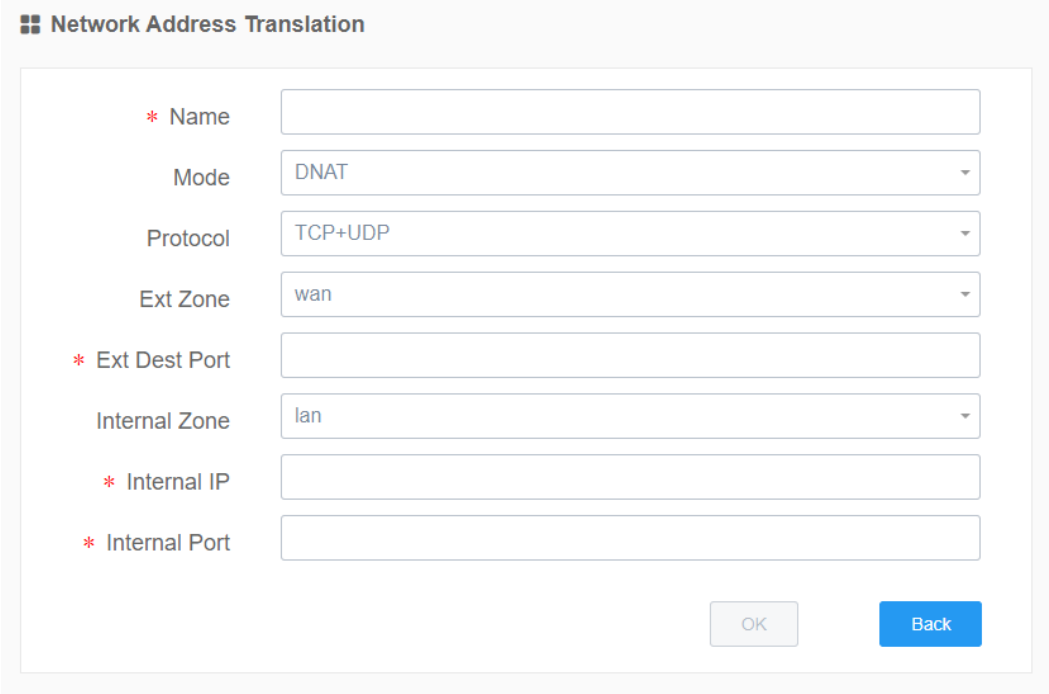
4-1Table 51 Description of the NAT list parameters



The parameter name	explain
name	The NAT rule name.
protocol	Address-transformed packets using the protocol.
exterior zone	outer net.
External port	Ports used by the exnet.
interior zone	inner-mesh.
interior IP	The IP address of the Intranet.
Internal port	Ports used by the Intranet.
operate	Edit and Delete NAT rules.

Step 2 Click Create to create a new NAT rule.

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



Step 3 Configure the NAT rule parameters, and the parameters description are shown in Table 5-2.

4-2Table 52 Description of the NAT parameters

The parameter name	explain	collocation
name	Set the NAT rule name.	Alphanumeric WORD item, input specification see" ”
protocol	Target address conversion for which protocol packet.	Drop-down list selection ● TCP+UDP ● TCP ● UDP
exterior zone	outer net.	Drop-down list selection ● wan
External port	Ports used by the exnet.	Value range: 1~65535 or [1~65535], it can be a range or a single port
interior zone	inner-mesh.	Drop-down list selection ● lan
interior IP	The IP address of the Intranet.	Enter manually in the input box form:X.X.X.X

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Internal port	Ports used by the Intranet.	Value range: 1~65535 or [1~65535], it can be a range or a single port

Step 4 Click OK to complete the NAT rule configuration.

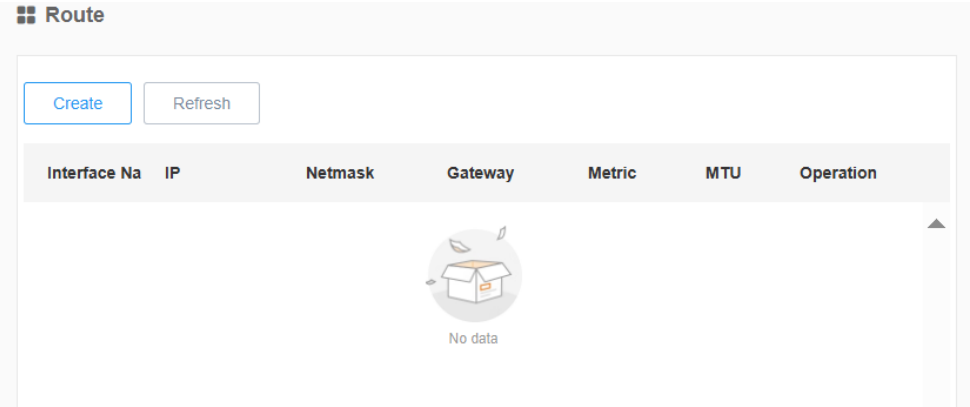
—— **finish**

4.2 Routing configuration

operating steps

Step 1 After logging in to the WEB Configuration page, click the Forward Settings> Routing Configuration page to open the Routing Configuration tab. Description of the routing list parameters are shown in Table 5-3.

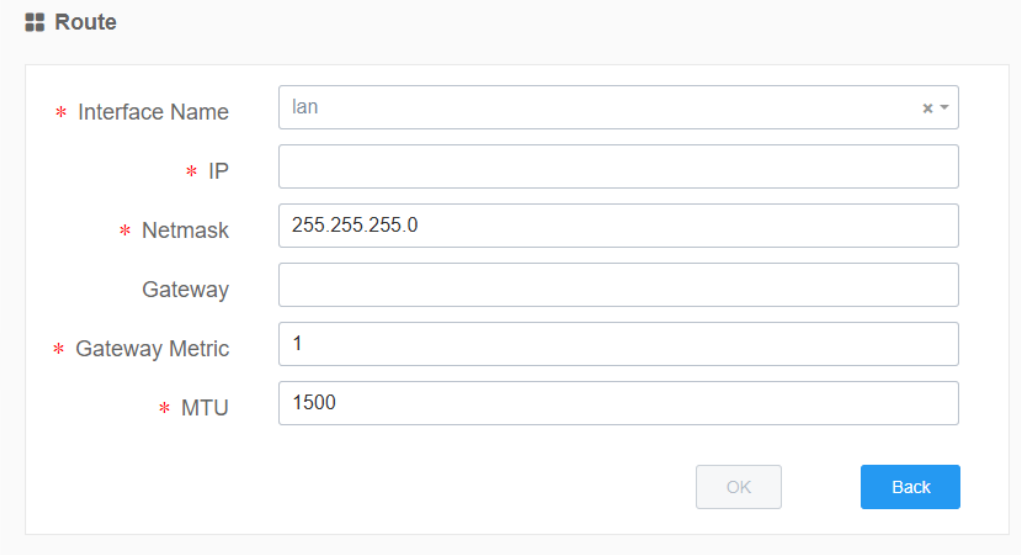
4-3Table 53 Description of the routing configuration list parameters



The parameter name	explain
The interface name	The name of the routing interface.
IP address	IP address of the host or destination of the network.
subnet mask	A subnet mask of the routing destination host or the destination network.
gateway	The IP address of the route-rule gateway.
Gateway jump point	Gateway jump point number.
MTU	Maximum transmission unit.
operate	You can edit and delete scheduled tasks.

Step 2 Click Create to create a new routing rule.

Copyright © 3onedata Co., Ltd.



Step 3 Configure the routing mode rule parameters, as described in Table 5-4.

4-4Table 54 Description of the routing configuration parameters

The parameter name	explain	collocation
The interface name	The name of the routing interface.	Drop-down list selection ● gretunnel ● gretunnel_static ● lan ● n2n ● open_vpn1 ● open_vpn2 ● wan ● wwan
IP address	Enter the IP address of the destination host or the destination network.	Enter manually in the input box form:X.X.X.X
subnet mask	Enter a subnet mask for the destination host or the destination network.	Enter manually in the input box form:X.X.X.X Default value: 255.255.255.0
gateway	Enter the IP address of the routing rule gateway, and the router will forward all the data matching the destination address and the subnet mask to the gateway.	Enter manually in the input box form:X.X.X.X
Gateway jump point	Gateway jump point number.	Manual input values
MTU	Set the maximum transmission unit.	Manual input values

Copyright © 3onedata Co., Ltd.

Step 4 Click OK to complete the configuration of the routing rule.

—— **finish**

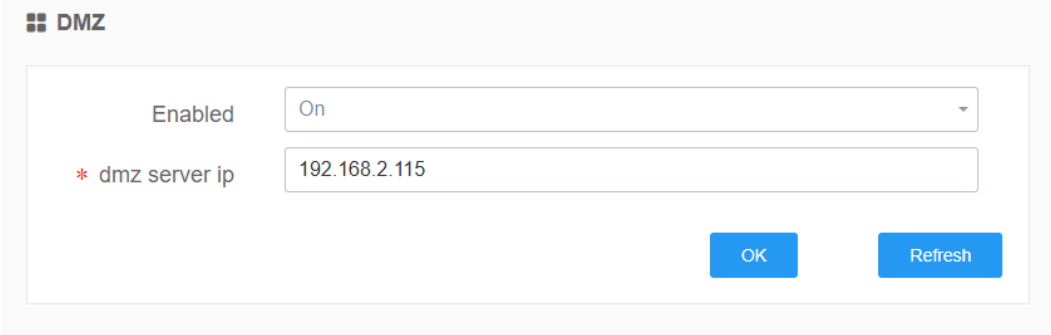
4.3 DMZ

operating steps

Step 1 After logging into the WEB configuration page, click the Forward Settings> DMZ to open the DMZ tab.

Step 2 Configure the routing mode rule parameters, as described in Table 5-5.

4-5Table 55 Description of the DMZ configuration parameters



The parameter name	explain	collocation
start using	Use the DMZ function.	Drop-down list selection ● yes ● deny
The DMZ host IP	DMZ, the IP address of the host.	Enter manually in the input box form:X.X.X.X

Step 3 Click OK to complete the DMZ configuration.

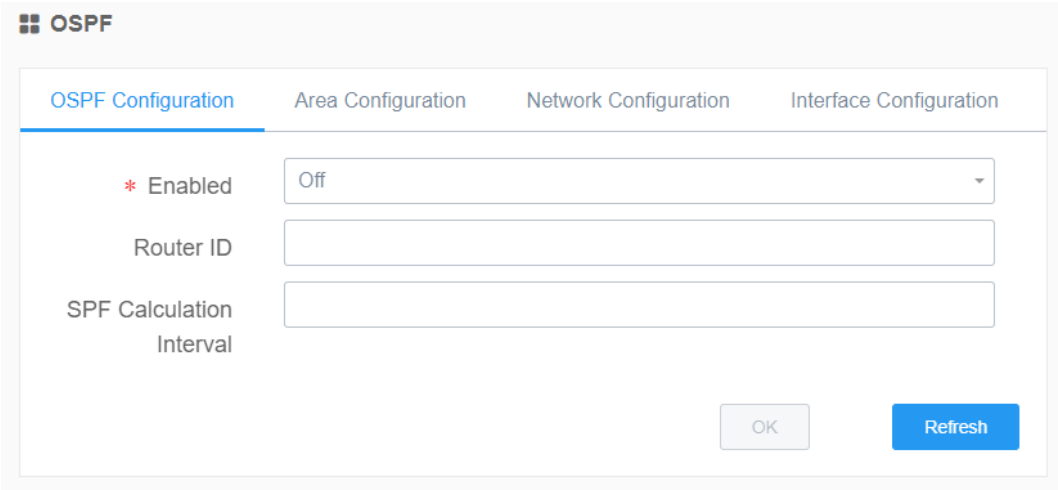
—— **finish**

Copyright © 3onedata Co., Ltd.

4.4 OSPF configure

operating steps

Step 1 After logging on to the WEB configuration page, click the Forward Settings> OSPF to open the OSPF tab.

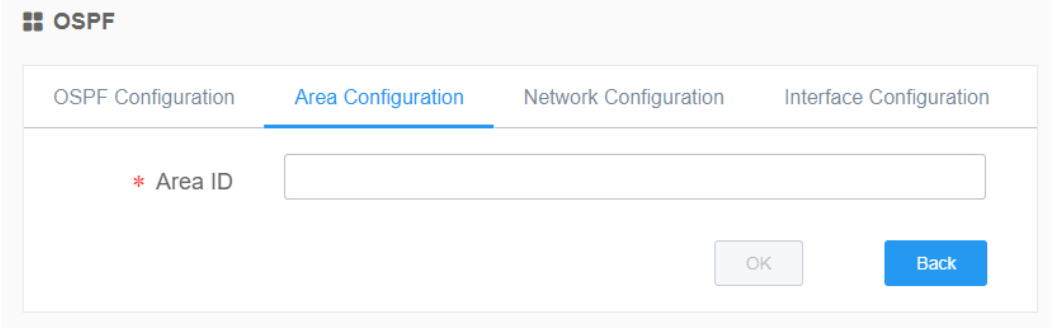


Step 2 OSPF parameters and parameter description are shown in Table 5-6.

4-6Table 56 Description of the OSPF configuration parameters

The parameter name	explain	collocation
start using	Whether to use the OSPF feature.	Drop-down list selection ● yes ● deny
route ID	Routing this end identification	form:XXX.XXX.XXX.XXX
SPF counting period	Set the delay time for the SPF calculation	0~255 (sec)

Step 3 Regional configuration list parameters are described in Table 5-7.

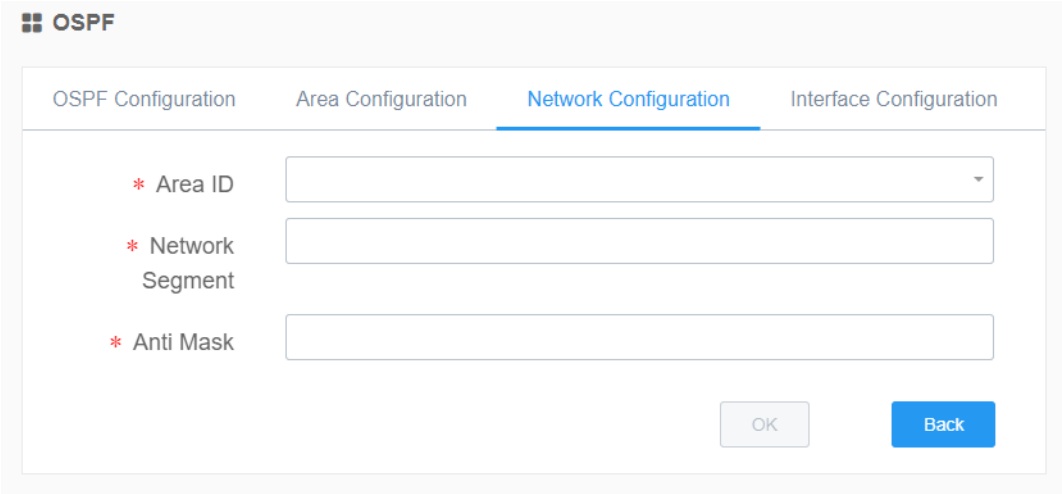


Copyright © 3onedata Co., Ltd.

4-Table 57 Description of the OSPF configuration parameters

The parameter name	explain
region ID	Set the OSPF area ID 0 as the backbone and other regular

Step 4 The description of the network configuration parameters are shown in Table 5-8.

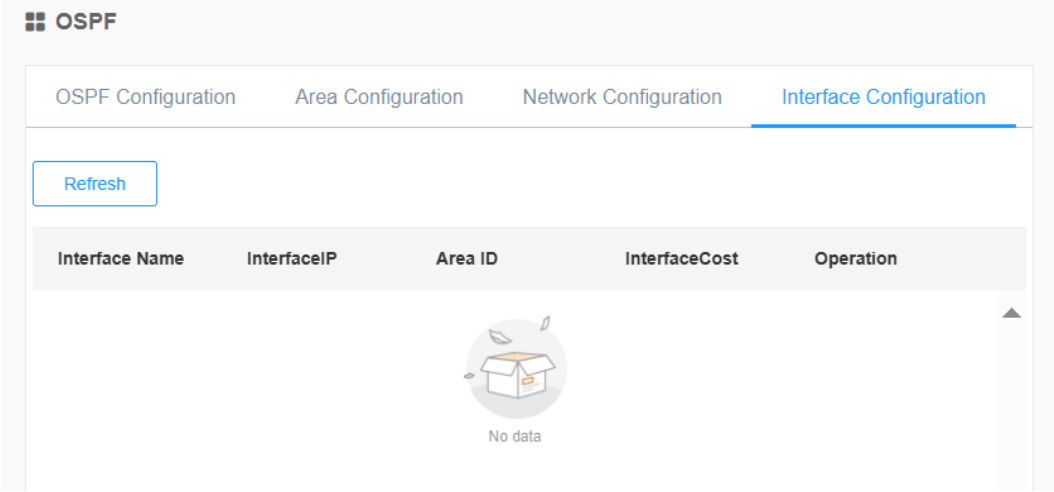


4-Table 59 Description of the network configuration parameters

The parameter name	explain
region ID	Set the OSPF area ID 0 as the backbone and other regular
network segment	Declaration route all interface segment addresses
Anti mask code	wildcard mask as 0.0.0.255

Copyright © 3onedata Co., Ltd.

Step 5 Description of the interface configuration parameters are shown in Table 5-10.



4-Table 511 Description of the network configuration parameters

The parameter name	explain
The interface name	The exit interface cannot be selected
interface overhead	Legal value: 0-65535
Certification type	Users can choose: simple authentication, set the authentication mode used in the OSPF area of md 5. If you choose the simple authentication mode, you also need to configure a simple authentication password and confirm the password again. If you choose MD5 authentication mode, you also need to configure MD5, key value and password, and confirm the password again.
DR priority	Must be greater than-1 and less than 256
Transmission delay time (seconds)	Must be greater than 0 and less than 501
Hello Message interval (seconds)	The time interval of sending Hello message. If the Hello interval of two adjacent routers is different, the legal value of neighbor relationship cannot be established: 1-65535
Retransmission time interval (seconds)	Must be greater than 0, must be at 3601

Step 1 Click OK to complete the OSPF configuration.

—— **finish**

Copyright © 3onedata Co., Ltd.

5 Security configuration

Security setting is the firewall function of the router. By analyzing the IP address / MAC address of the packet entering the router, comparing with the firewall rules added by the user, and receiving or discarding the packets matching the corresponding firewall rules, so as to achieve the effect of user security access. Sanwang industrial grade wireless router supports IP filtering, MAC filtering security Settings, users can set security rules to complete allow / prohibit some network segments to access the external network, allow / prohibit other users to access the router, etc.

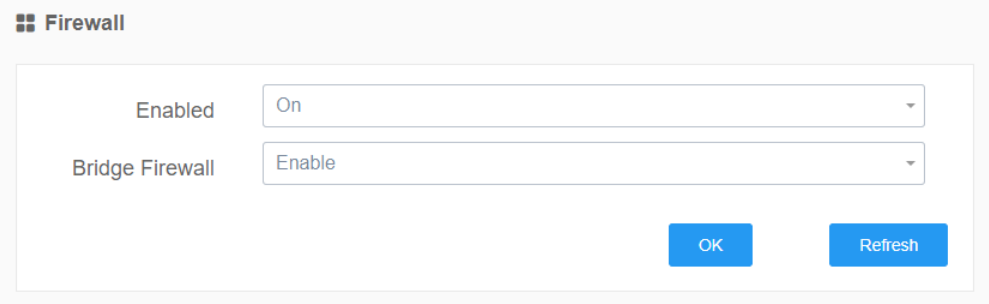
5.1 firewall

operating steps

Step 1 After logging on to the WEB configuration page, click Security> Firewall to open the Firewall tab.

Step 2 Configure the firewall parameters as described in Table 6-1.

5-1Table 61 Description of the firewall configuration parameters



The parameter name	explain	collocation
start using	Select whether to enable the firewall.	Drop-down list selection ● yes ● deny

Copyright © 3onedata Co., Ltd.

Step 3 Click OK to complete the firewall configuration.

—— **finish**

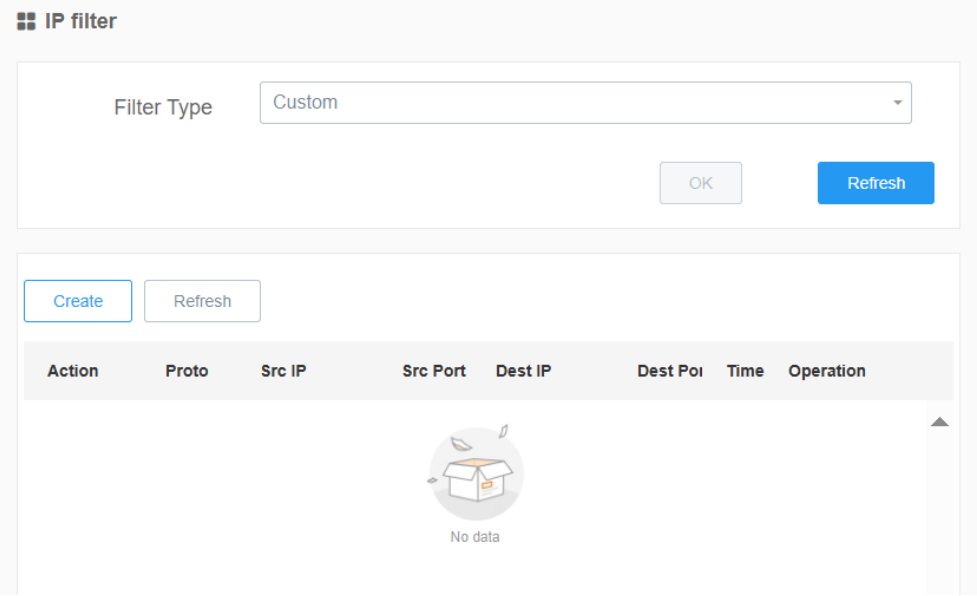
5.2 IP filter

background information

IP filtering refers to the router to determine whether to allow external devices to access the router and whether to allow packets to forward through the router, so as to realize the management of the router device and the Internet behavior management of the LAN device. IP filtering is usually used to allow only a part of the host to access the external network or prohibit a part of the host from accessing a particular network.

operating steps

Step 1 After logging on to the WEB configuration page, click Security Settings> IP Filter to open the IP Filter tab. Description of the IP filter list parameters are shown in Table 6-2.



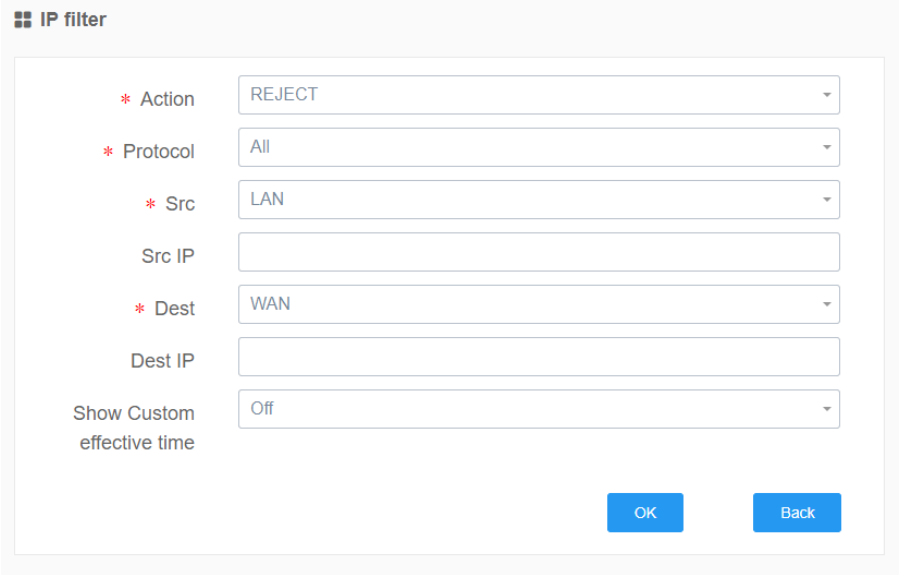
5-2Table 62 Description of the parameters of the IP filter list

The parameter name	explain
Filter type	Drop-down list selection ● white list ● blacklist ● user-defined
movement	Filtering rules for the access.
protocol	The protocol used for the access.
source address	Specifies the source address to access the source.

Copyright © 3onedata Co., Ltd.

The parameter name	explain
Source port	Specifies the source port that access the source.
purpose IP	The destination address that the access source wants to access.
destination port	Access to the destination port that the source wants to access.
time	Customize the effective time.
operate	You can edit and delete IP filtering rules.

Step 2 Click Create to create a new IP filtering rule.



Configure the IP filtering parameters as described in Table 6-3.

5-3Table 63 IP Filter parameters

The parameter name	explain	collocation
movement	Select the filtering rule for the access.	Radio box selection ● ACCEPT ● REJECT ● DROP
protocol	Select the protocol used for access, and if the current access protocol is unclear, it is recommended to select "all".	Drop-down list selection ● tcp ● udp ● tcpudp ● all
Source interface	Specifies the interface to access the source.	Drop-down list selection ● wan ● lan

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
source address	Specifies the source address to access the source.	Manually enter an IP address, a subnet segment, or specify an IP range
Source port	Specifies the source port that access the source.	Value range: 1~65535 or [1-65535]; it can be a range or a single port
Purpose interface	Specifies the router interface for the IP packet access.	Drop-down list selection ● wan ● lan
purpose IP	The target address to access the source can be the IP device under the router.	Manually enter an IP address, a subnet segment, or specify an IP range
destination port	The target port to access the source can be the IP device under the router.	Value range: 1~65535 or [1-65535]; it can be a range or a single port
Customize the effective time	Whether to customize the effective time.	Drop-down list selection ● yes ● deny

Step 3 Click OK to complete the IP filtering rule configuration.

—— **finish**

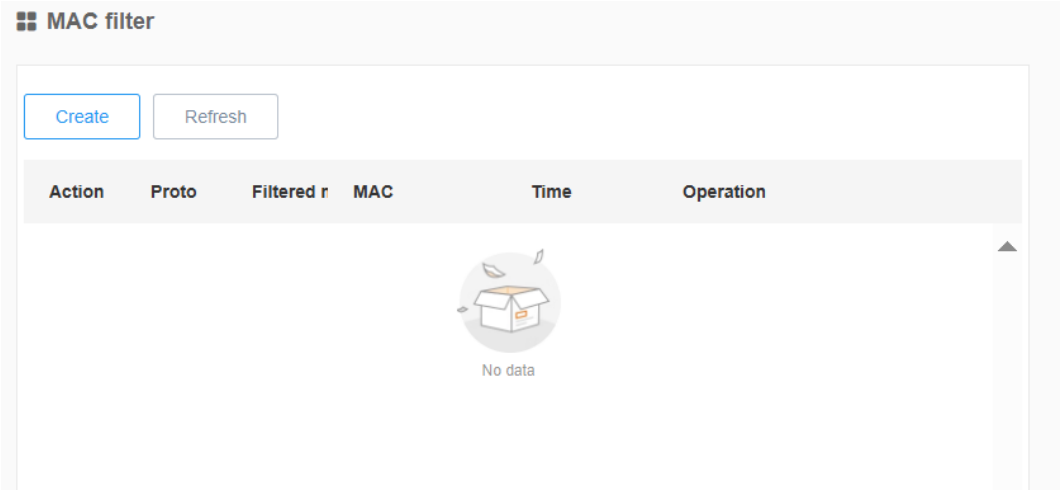
5.3 MAC filter

background information

MAC filtering is usually used to control host access to the router, with whitelists so that only MAC-specific hosts can manage and access the router. In addition to implementing this function, the Sanwang industrial-grade wireless router can also limit the external network access rights of a specific MAC host, or only allow a specific MAC host to access the external network.

Copyright © 3onedata Co., Ltd.

operating steps



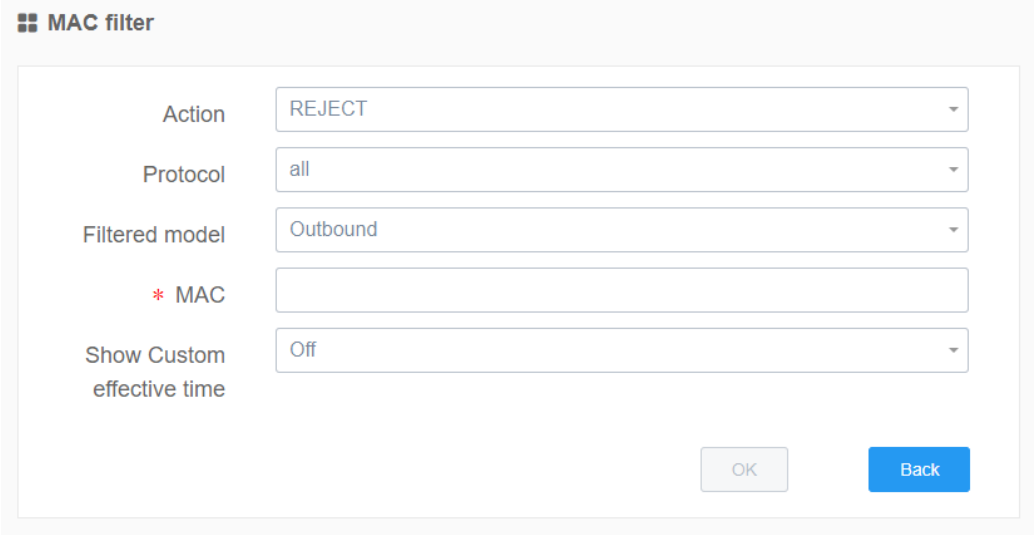
After logging on to the WEB configuration page, click Security Settings> MAC Filter to open the MAC Filter tab. The MAC filter list parameters are described in Table 6-4.

5-4Table 64 Description of MAC filter list

The parameter name	explain
movement	Filtering rules for the access.
protocol	The protocol used for the access.
filtered model	The MAC filter mode.
MAC address	MAC, the MAC address to be filtered.
time	Customize the effective time.
operate	You can edit and delete IP filtering rules.

Step 1 Click Create to create a new MAC filtering rule.

Copyright © 3onedata Co., Ltd.



Step 2 Configure the MAC filtering parameters as described in Table 6-5.

5-5Table 65 MAC Filter parameters

The parameter name	explain	collocation
movement	Select the filtering rule for the access.	Drop-down list selection ● ACCEPT ● REJECT ● DROP
protocol	Select the protocol used for access, and if the current access protocol is unclear, it is recommended to select "all".	Drop-down list selection ● TCP ● UDP ● TCPUDP ● ALL
filtered model	The filtering mode of the rule.	Drop-down list selection ● retransmission ● import
MAC address	The MAC address for the MAC to filter.	WORD type MAC format: XX: XX: XX: XX: XX: XX Input see"Parameter specification table"
Customize the effective time	Whether to customize the effective time.	Drop-down list selection ● yes ● deny

Step 3 Click OK to complete the MAC filtering rule configuration.

Copyright © 3onedata Co., Ltd.

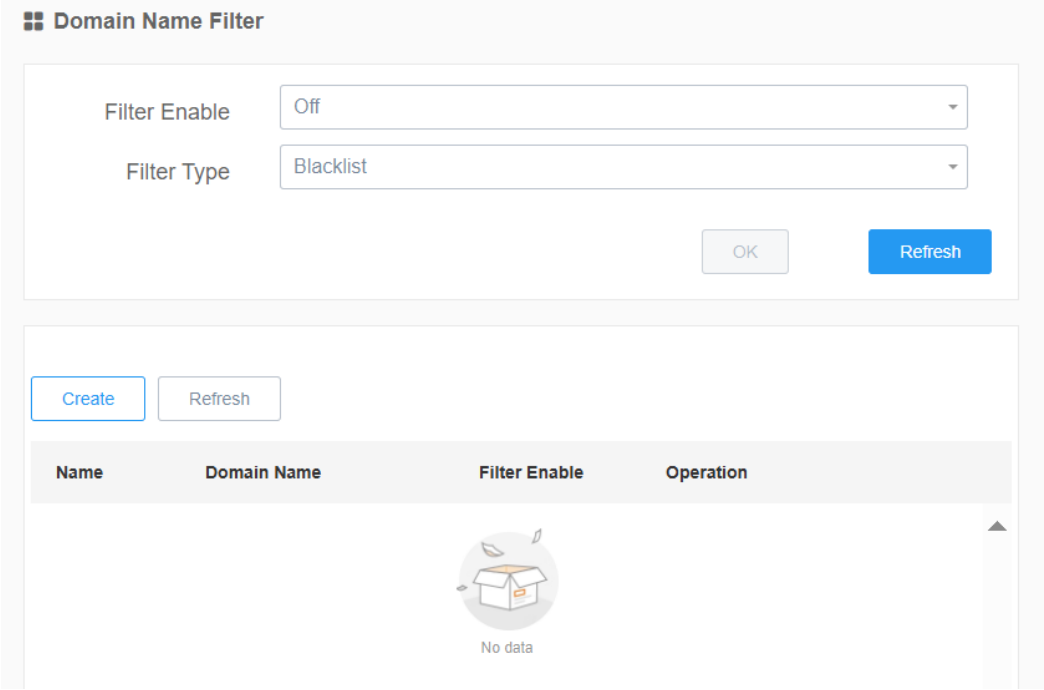
5.4 Domain name filtering

background information

Domain name filtering function can set the access restrictions to the website, through the black and white list function to set up specific filtering rules, to achieve a safe and reliable domain name access environment.

operating steps

Step 1 After logging on to the WEB configuration page, click Security Settings> Domain Filter to open the Domain Filter tab. The parameters of the domain name filter list are described in Table 6-6.



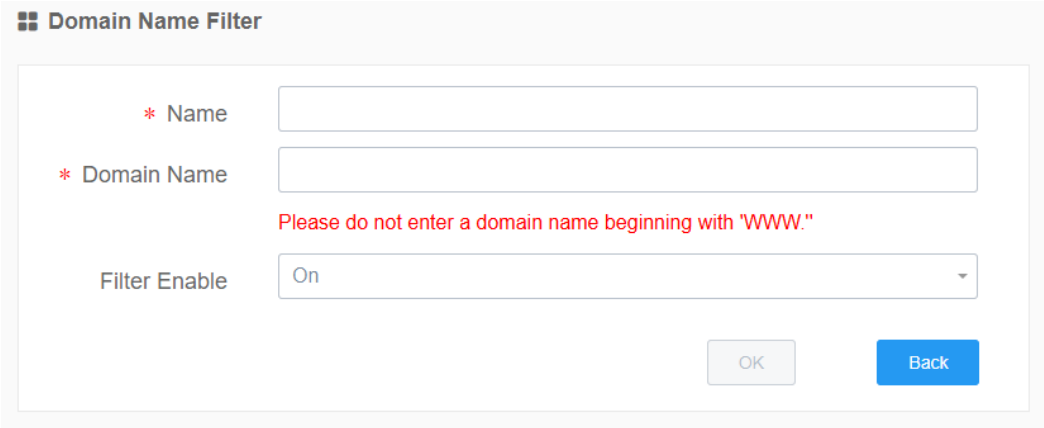
5-Table 66 Domain name filtering parameters

The parameter name	explain
start using	Select whether to enable the domain name filtering function. Drop-down list selection ● yes ● deny
Filter type	Select the filter type. Drop-down list selection ● blacklist ● white list

Copyright © 3onedata Co., Ltd.

The parameter name	explain
name	Displays the name of the domain name filtering configuration item.
realm name	Displays the domain name where the current configuration key is filtered.
Enable filtering	Shows whether the configuration key is enabled.
operate	You can edit and delete operations for domain name filtering rules.

Step 2 Click Create to create a new domain name filtering rule.



Step 1 Configure the domain name filtering parameters, which are described in Table 6-7.

5-Table 67 Domain name filtering parameters

The parameter name	explain	collocation
name	Custom rule name.	No more than 32 arbitrary characters
realm name	Fill in the primary domain name that needs to be filtered.	Fill in the legal domain name, do not need to fill in the www prefix, otherwise it will affect the filtering effect. Fill no more than 32 characters.
Enable filtering	Select whether to enable the filtering rule.	Drop-down list selection ● yes ● deny

Step 2 Click OK to return to the Domain Name Filter tab.

Step 3 Depending on the requirements, select the Filter Type. If the "blacklist" is selected, the domain name of the filtering rule is banned; if the "whitelist" is selected, only the domain name of the filtering rule can be accessed, and the other domain names can be banned.

—— **finish**

Copyright © 3onedata Co., Ltd.

6 System configuration

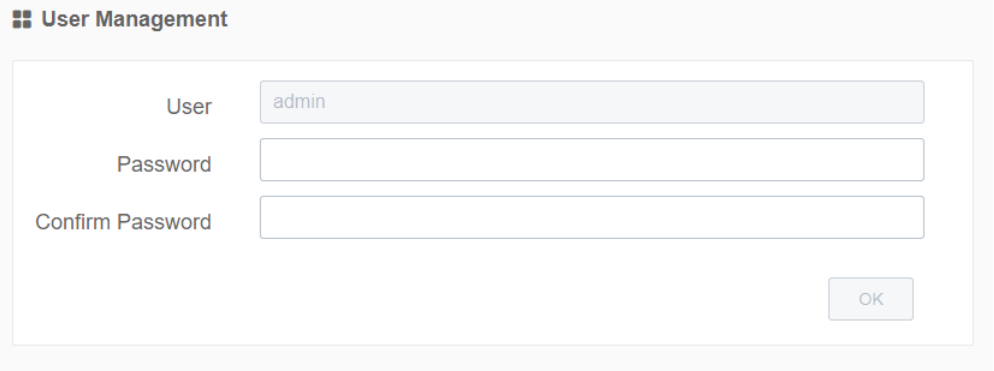
6.1 user management

operating steps

Step 1 After logging on to the WEB Configuration page, click System Configuration> User Management to open the User Management tab.

Step 2 Configure the user management parameters, which are described in Table 7-1.

6-1Table 71 User management parameters



The parameter name	explain	collocation
password	The password is modified by the user.	Manual input, up to 32-bit WORD string, input specification see"Parameter specification table"
confirm password	The confirmation password after the user changes the password.	Manual input, up to 32-bit WORD string, input specification see"Parameter specification table"

Step 3 After the modification, click "OK", and the page will automatically jump to the login interface. The user needs to enter the modified user name / password to enter.

—— **finish**

Copyright © 3onedata Co., Ltd.

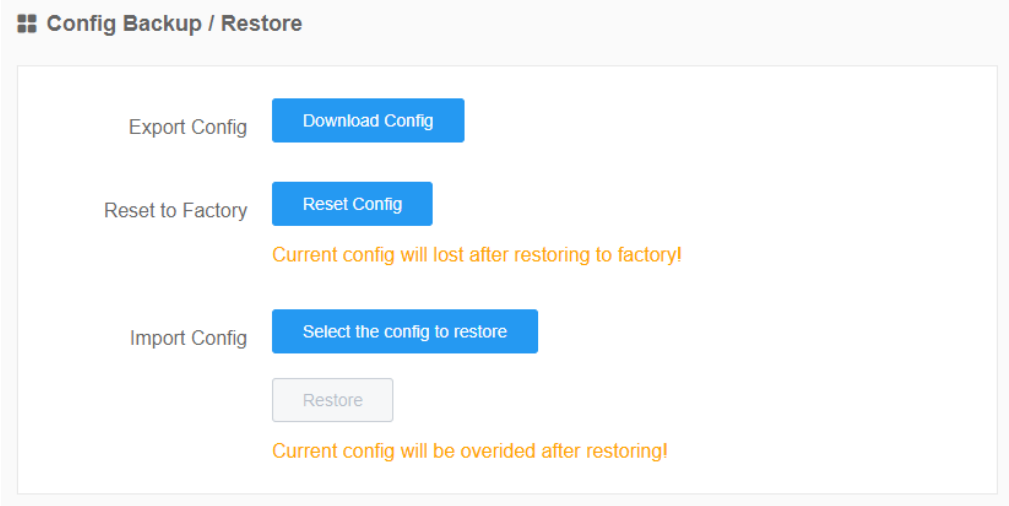
explain

Some model or firmware versions have changed the System Configuration-User Management feature to User Management at the root of the feature menu.

6.2 configuration management

operating steps

Step 1 After logging on to the WEB Configuration page, click System Configuration> Configuration Management to open the Configuration Backup / Restore tab.



Click Download Configuration to export the configuration file to the backup function of file / parameters.

Step 2 Click Restore factory Default to restore the factory configuration.

pay attention to

Restoring the factory configuration cleans up all of the current configurations.

Step 3 Click Select to browse the local profile that needs to be imported, and click Update to complete the file import. If the router parameter is wrong or the file is lost, the Import function can be used to restore the parameter.

—— **finish**

explain

After importing the backup file, the system is automatically restarted and takes effect only after the system is restarted.

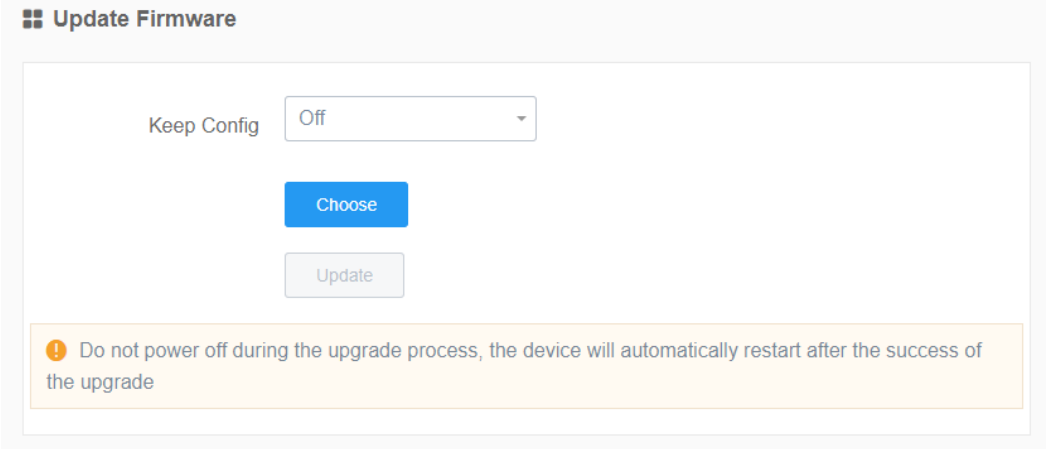
Copyright © 3onedata Co., Ltd.

6.3 firmware upgrade

background information

The router supports local network upgrade system files. Before the upgrade, you determine the target file for the system update and store the update file on the computer with the LAN.

operating steps



After logging on to the WEB Configuration page, click System Configuration> Firmware Upgrade to open the Firmware Upgrade tab.

explain

Select the Retention Configuration check box to retain the parameters set by the user on the page. When upgrading a file, it is not recommended to close the page. After the upgrade is completed, the page will automatically jump. If it is a remote upgrade, after upgrading the file, after the router modem dials again and gets the new IP address, the page will not be automatically due due to the incorrect IP address.

Step 1 Click Select, browse the local file to select the firmware file to update, and click Update to start the upgrade.

—— **finish**

pay attention to

During the upgrade, ensure that the router is powered normally; if the router is powered, the upgrade will fail

explain

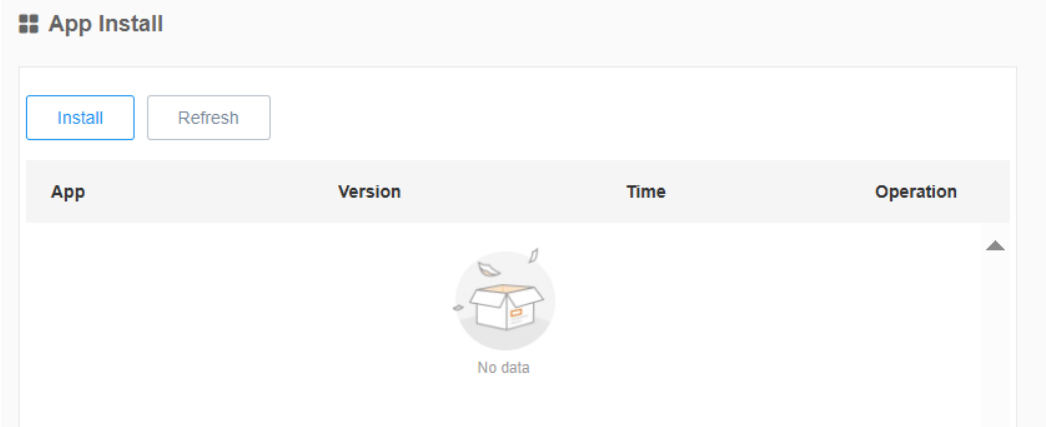
Copyright © 3onedata Co., Ltd.

After the upgrade is complete, clear the browser cache before opening the Router Configuration page.

6.4 APP install

operating steps

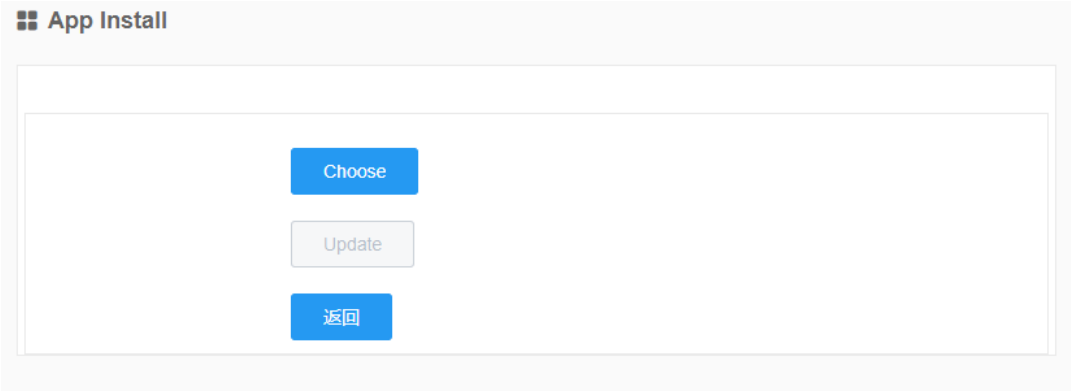
Step 1 After logging on to the WEB Configuration page, click System Configuration> APP Installation to open the APP Setup tab. The parameters of the APP installation list are described in Table 7-2.



6-2Table 72 Description of the parameters of the APP installation list

The parameter name	explain
apply names	Name of the APP being installed.
version number	The APP version number that was installed.
operate	You can edit and delete IP filtering rules.

Step 2 Click Install to install a new APP.



Step 3 Manually enter the application name, click Select, browse the local file to select the installation package, click Update to start installing the APP installation.

—— **finish**

Copyright © 3onedata Co., Ltd.

explain

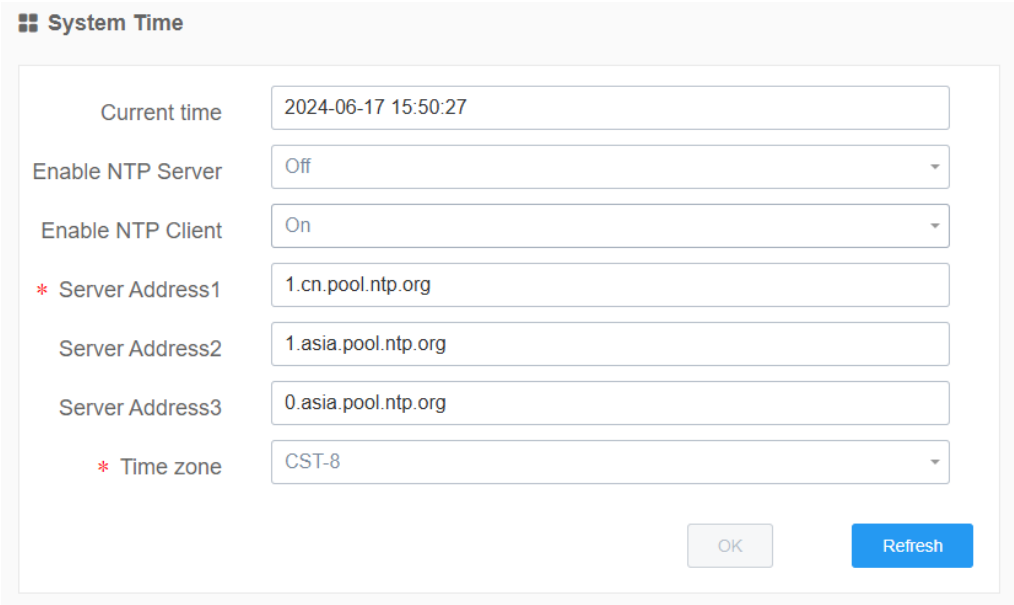
Some models and firmware versions have been renamed APP Installation to Application Installation, which only supports the installation of ipk formats.

6.5 System time

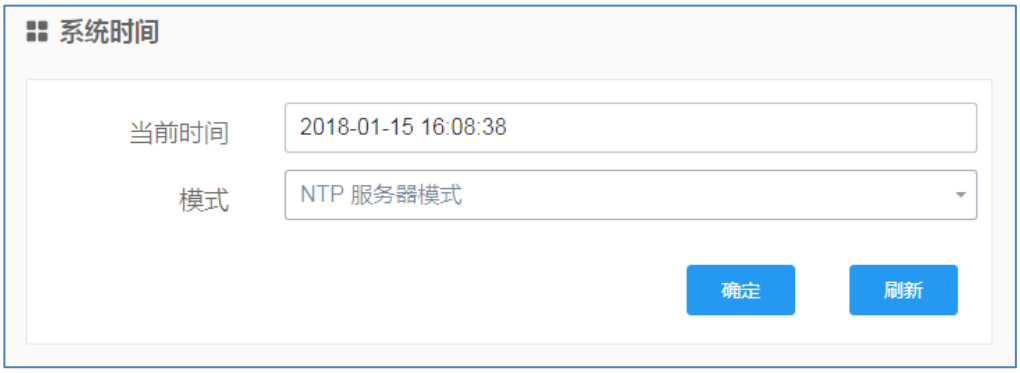
operating steps

Step 1 After logging on to the WEB Configuration page, click System Configuration> System Time to open the System Time tab.

Mode Select the NTP Client Mode



Mode Select the NTP Server Mode



Step 2 Configure system time, parameters are shown in Table 7-3.

6-3Table 73 Description of the system time parameters

The parameter name	explain	collocation

The parameter name	explain	collocation
present time	System current time.	Not being configurable, the system is automatically generated
pattern	Select the system time mode.	Drop-down list selection ● The NTP client mode ● The NTP server mode ● Manual setting
The Mode is displayed when the NTP Client Mode is selected		
Server address		manual input
time zone	The current time zone.	Drop-down list selection ● CST-1 ● CST-2 ● … ● CST-12

Step 3 Click OK to complete the configuration of the system time.

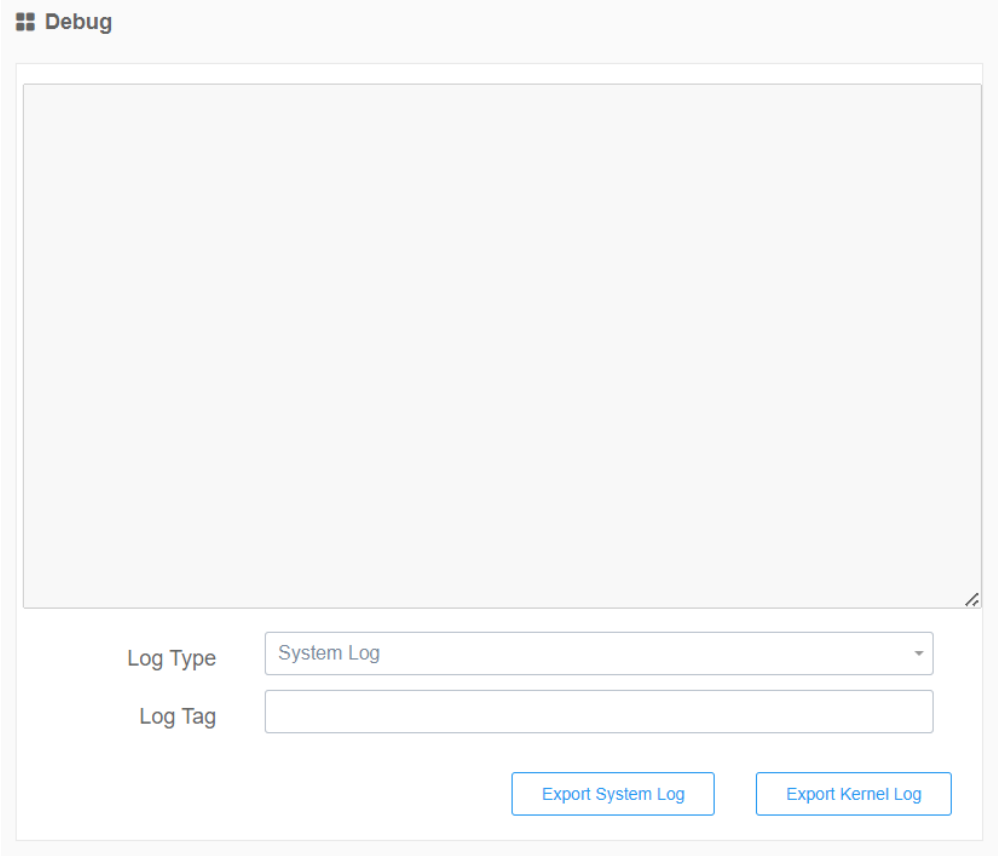
—— **finish**

6.6 Log management

operating steps

Step 1 After logging on to the WEB Configuration page, click System Configuration> Log Management to view the log information of the router.

Copyright © 3onedata Co., Ltd.



Step 2 Configure the system debugging parameters as shown in Table 7-5.

6-4Table 75 System debugging parameters

The parameter name	explain
renovate	Page to view the live logs
Export system logs	Export history logs
Export kernel logs	Export the history kernel logs

Step 3 Click OK to complete the system debugging configuration.

—— **finish**

6.7 diagnose

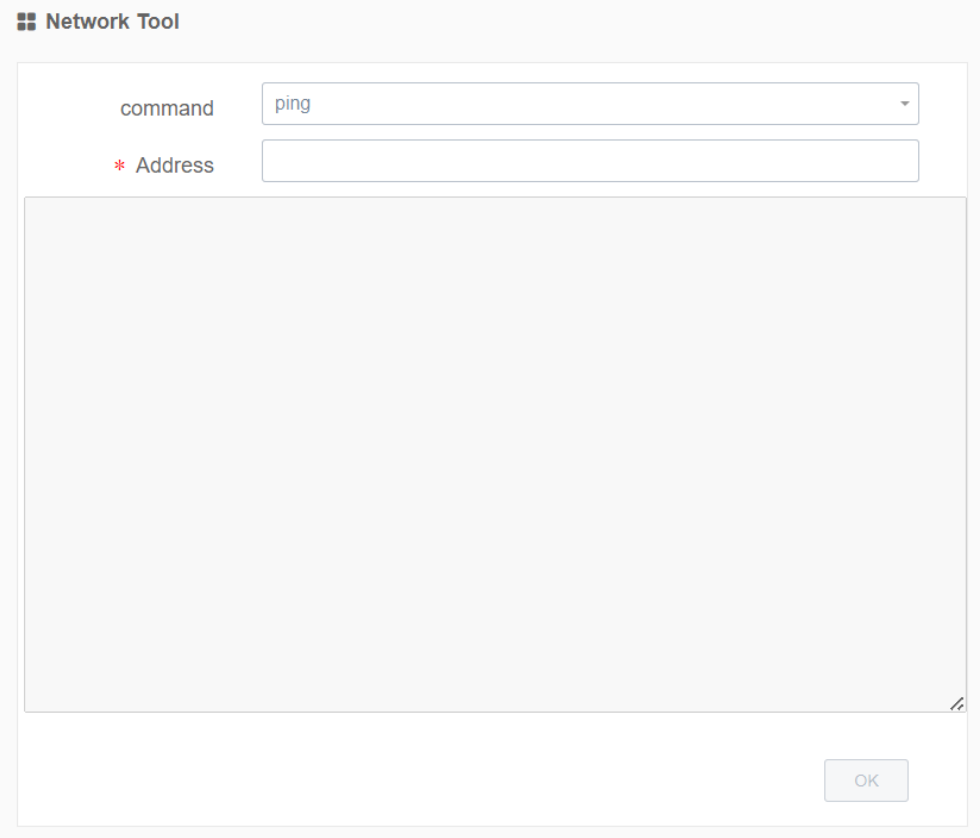
background information

Network testing, including the commonly used Ping feature and the Traceroute functions.

operating steps

Step 1 After logging into the WEB Configuration page, click System Configuration> Diagnostics to open the Diagnostics tab

Copyright © 3onedata Co., Ltd.

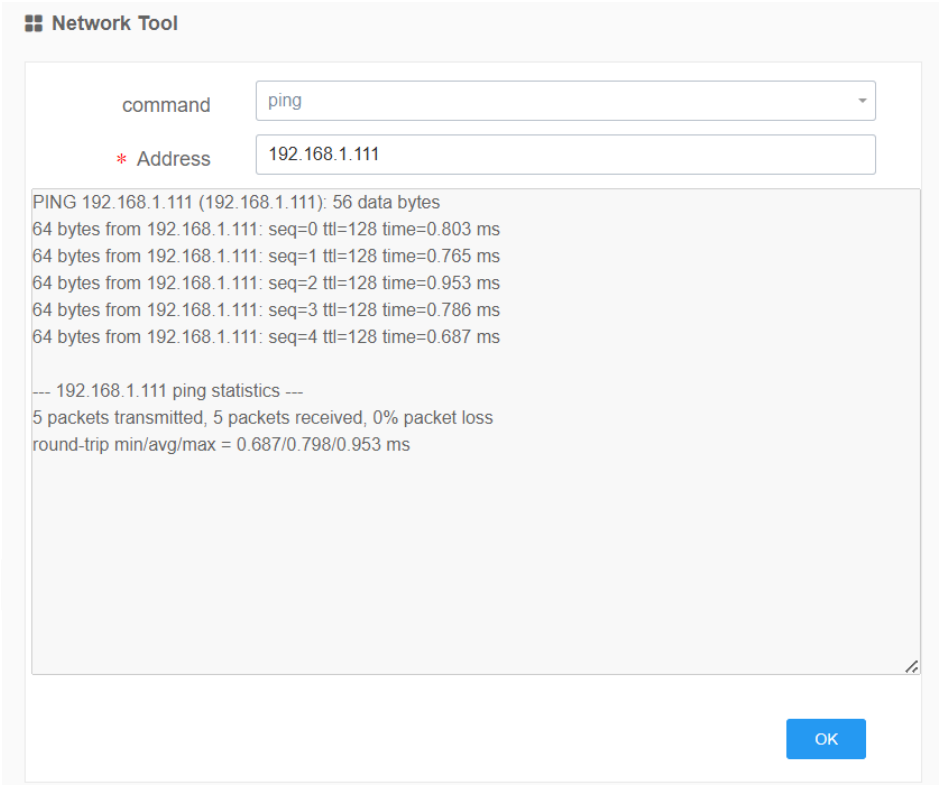


Step 2 Select the command to enter the IP address or domain name to test in the Address box, described in Table 7-7.

6-5Table 77 for diagnostic functional parameters

The parameter name	explain	collocation
order	Select the test command.	Drop-down list selection ● ping: Test network connectivity ● tracert: Test the number of jumps to the destination address
address	Sets the destination IP address or domain name used for testing.	Fill in the IP address or domain name of the destination address to be used for the test

Copyright © 3onedata Co., Ltd.



Click OK to view the results in the box below.

—— finish

explain

Trace rt: traceroute, through Traceroute we can know what path the information takes from your computer to the other host of the Internet; measure how long it takes to send a small packet to the destination device until it returns. Each device Traceroute on one path should be measured three times. The output includes the time (ms) of each test and the name of the device (if any) and its IP address.

Copyright © 3onedata Co., Ltd.

6.8 Device cloud network pipe

background information

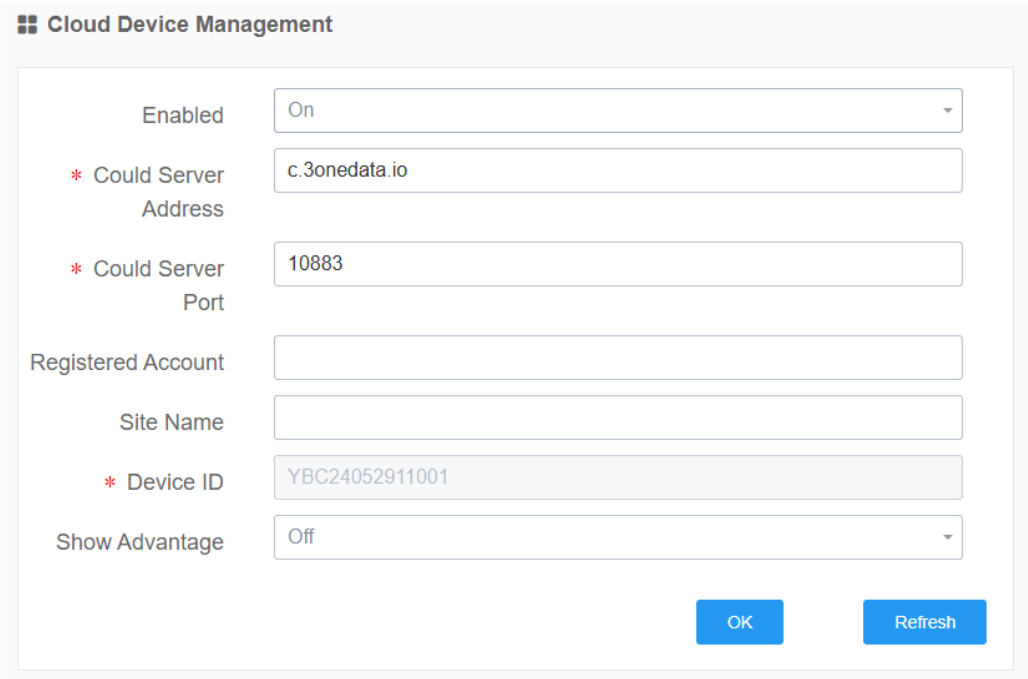
Sanwang industrial wireless router system has built-in communication function with M2M platform through WMMP protocol, which can realize the remote maintenance and management of the equipment and the monitoring and management of the field network status through the platform, such as viewing the equipment information, upgrading patches, upgrading firmware, etc., and checking the network signal strength, delay and flow of the equipment. Support connecting sanwang cloud equipment management platform for remote configuration and management router, please refer to "cloud equipment management platform user manual-official version 1.0", support connecting sanwang GoConnect remote maintenance platform for remote connection and access to the router device or machine, please refer to "GoConnect remote maintenance system manual-V1.0".

operating steps

Step 1 After logging in to the WEB configuration page, click System Configuration> Device Cloud Network Management and open the Device Cloud Network tab.

Step 2 Configure the parameters, which are shown in Table 7-8.

6-Table 78 Description of device cloud network management parameters



The parameter name	explain	collocation

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
start using	Using the device cloud network management service, this function should be used in conjunction with our network management management platform.	Drop-down list selection ● yes ● deny
Cloud server address	IP address or domain name of the network platform server.	WO RD Type, up to 64 bytes, see "" for input specificationParameter specification table"
Cloud server terminal	The port number used by the network platform server.	Value range: 0 to 65535 Default 1883 port
equipment ID	Identification ID connecting to the network management platform.	Assign it from the management platform
register an account	Manage the platform account number of the device	Platform account
Site name	Multiple devices are used to identify the equipment points	user-defined

Step 3 Click OK to complete the network configuration.

—— **finish**

6.9 service configuration

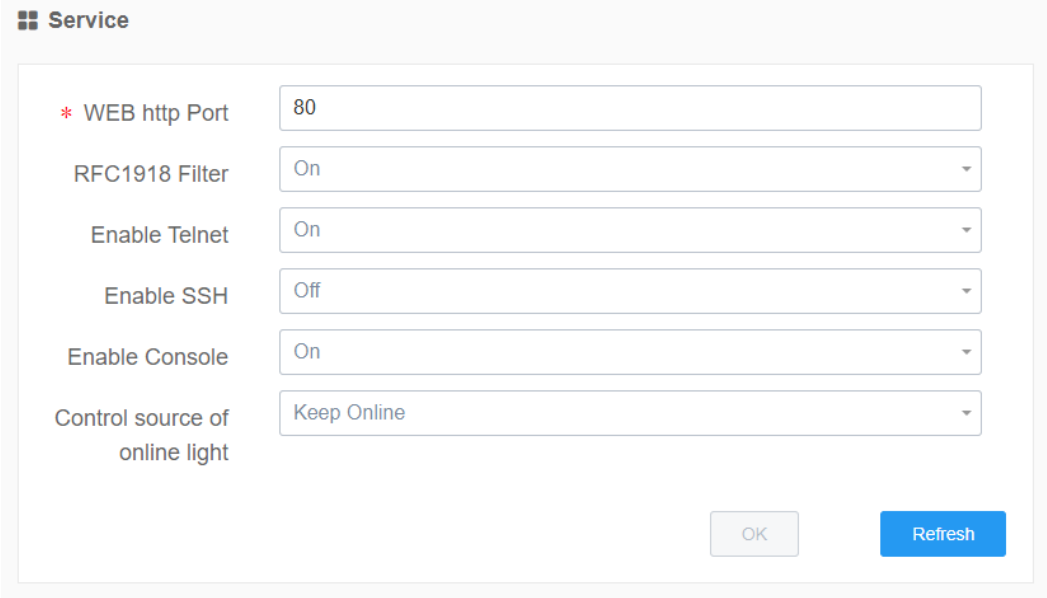
background information

The service configuration can customize the device WEB management port number to set the RFC1918 filtering, Telnet, and SSH functions on or off.

operating steps

Step 1 After logging on to the WEB Configuration page, click System Configuration> Service Configuration to open the Service Configuration tab.

Copyright © 3onedata Co., Ltd.



Step 2 Configure the service configuration parameters, which are described in Table 7-9.

6-Table 79 Description of the service configuration parameters

The parameter name	explain	collocation
The WEB http Port	Customize the modified device WEB landing port number.	Default 80
RFC1918 Filter-out	When enabled, the device-specific LAN address will be denied external access.	Drop-down list selection ● yes ● deny
Enable the Telnet	Select whether to enable the Telnet function.	Drop-down list selection ● yes ● deny
start using SSH	Select whether to enable the SSH feature.	Drop-down list selection ● yes ● deny
Enable the console	Turn the console To close the function serial port cannot enter the console	Drop-down list selection ● yes ● deny

Copyright © 3onedata Co., Ltd.

The parameter name	explain	collocation
Online light control	Through two ways to judge the online light 1, online to maintain the 4G network success and can be normal ping through the corresponding address online always bright 2, mobile network 4G network networking success online Chang bright	Drop-down list selection Keep online mobile network

Step 1 Click OK to complete the service configuration.

—— **finish**

6.10 Module upgrade

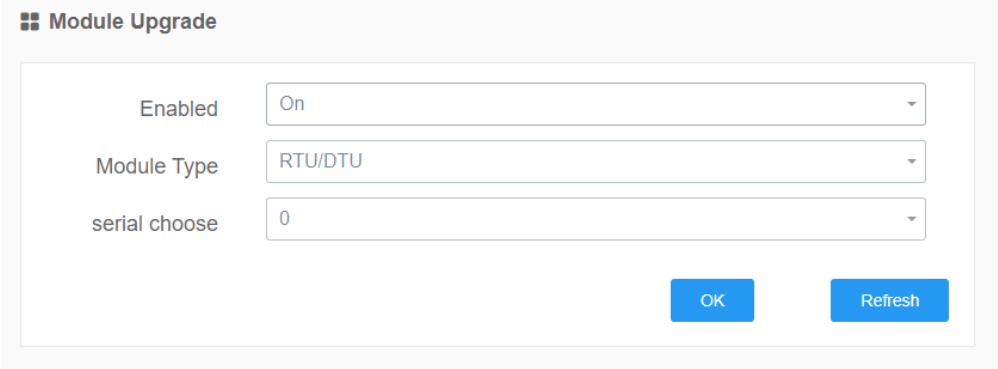
background information

Module upgrade function supports the firmware version differential package upgrade of some communication modules.

operating steps

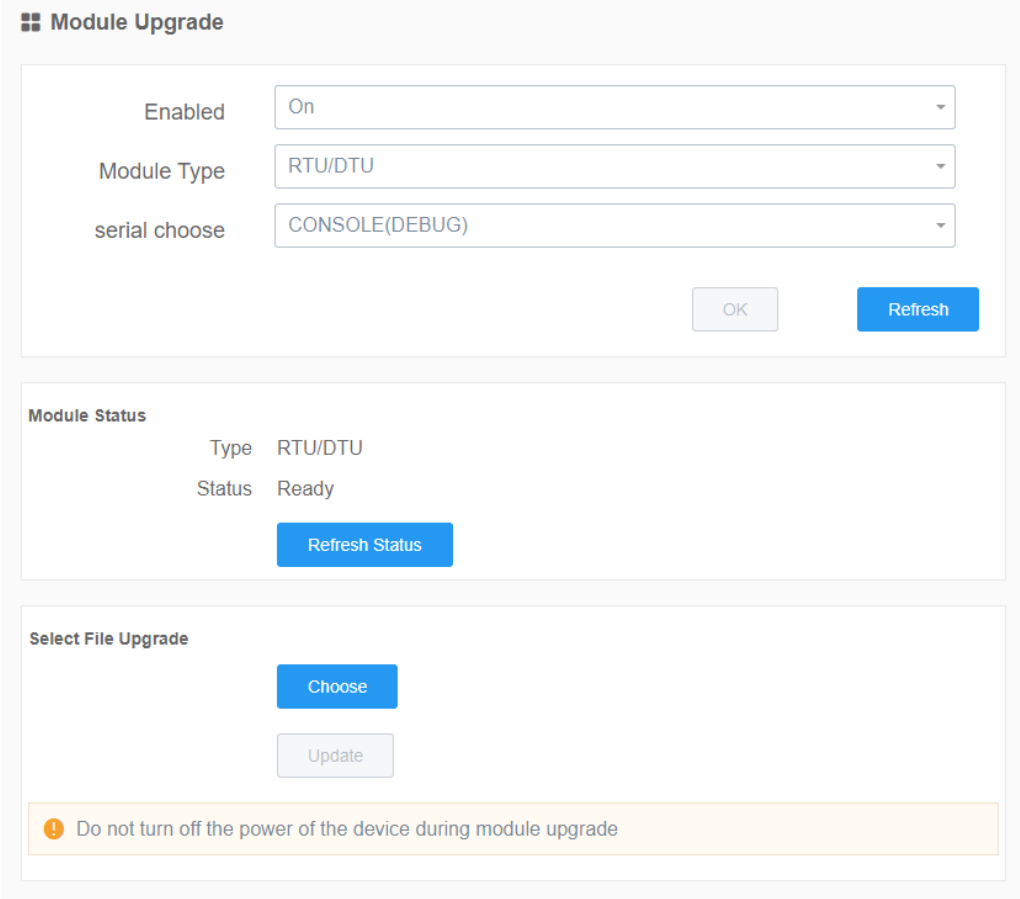
Step 1 After logging on to the WEB Configuration page, click System Configuration> Module Upgrade to open the Module Upgrade tab.

Enable the selection of Yes



Click the "OK" button, and the "Module Status" and "Select File Upgrade" columns appear on the page

Copyright © 3onedata Co., Ltd.



Step 2 Configure the module upgrade parameters as described in Table 7-10.

6-Table 79 Description of the service configuration parameters

The parameter name	explain	collocation
start using	Select to Enable or close the module upgrade function.	Drop-down list selection ● yes ● deny
Module type	Select the module type that you need to upgrade for. Differential package upgrades are supported only for specific types of devices or communication modules.	Drop-down list selection ● RTU/DTU ● Module-ME3630
String mouth selection	Select the communication serial port.	Drop-down list selection ● Console

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

The parameter name	explain	collocation
Module state	Displays the status of the currently upgraded device or communication module.	Click on the status refresh button to update the status ● Ready ● Checking ● Upgrade ● Successful ● F ail
Select file upgrade	Select the correct Differential upgrade package for the update.	After selecting the upgrade package, click the update button

Step 1 When the Module Status bar displays the Successful, the module upgrade is completed.

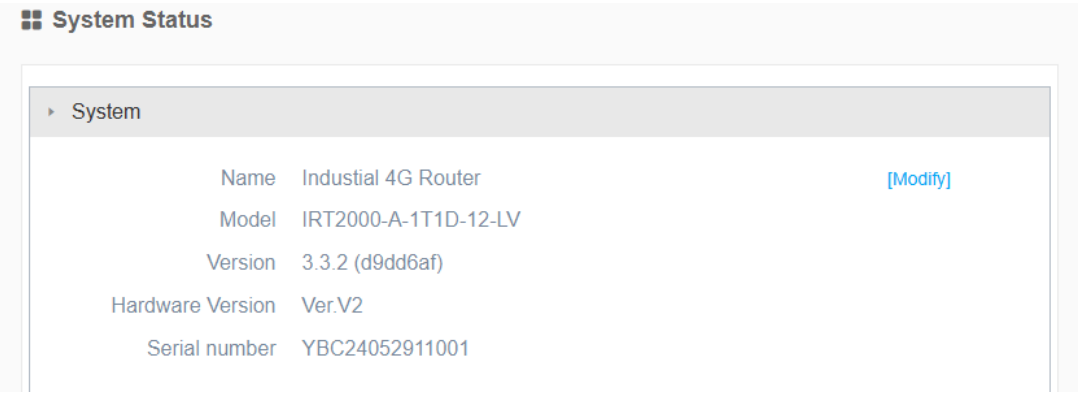
—— **finish**

Copyright © 3onedata Co., Ltd.

7 System mode

7.1 system

This section displays the system information for the router. The description of the system information display parameters is shown in Table 8-1.



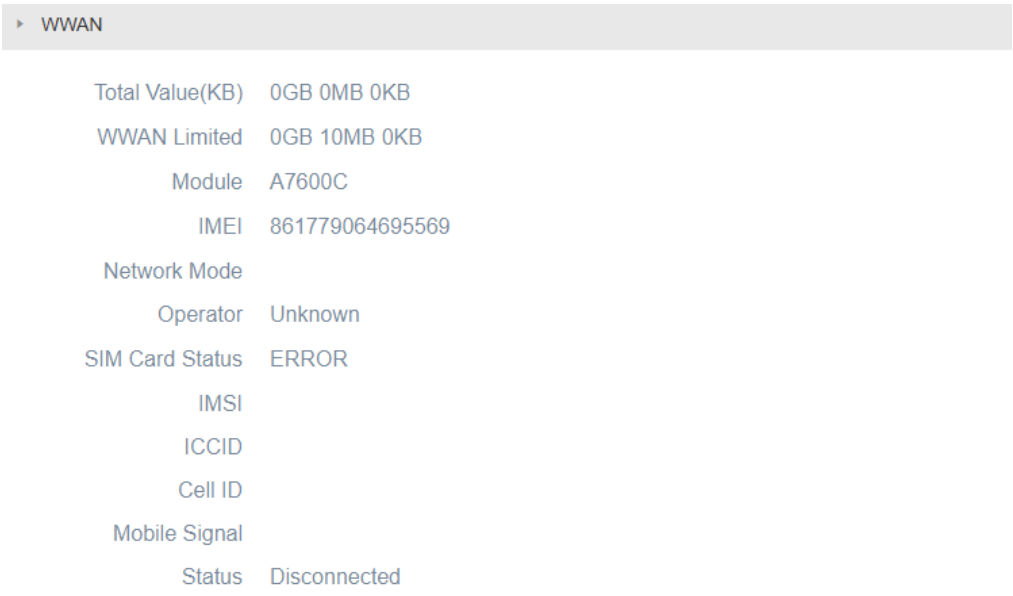
7-1Table 81 Description of the system information parameters

The parameter name	explain
name	The current connection device name.
model	Current connected device model number.
version number	The Web network management configuration version.
Hardware version	Ver.A\Ver. Version B hardware

Copyright © 3onedata Co., Ltd.

7.2 mobile network

This section displays the mobile network status information of the router. The descriptions of the mobile network state parameters are shown in Table 8-2.



7-2Table 82 Description of the status parameters of the mobile network

The parameter name	explain
module	The module used by the router.
IMEI	Router identity code.
carrieroperator	Identify the current SIM card operator
Network system	Type of network used by the mobile network.
SIM, card status	Current status of the SIM card.
Dual SIM card	Whether the dual-card function is enabled
Current SIM card	Identify the current insertion position of the SIM card
IMSI	Mobile user identification code.
ICCID	The SIM card number.
Base station number	Number of the base station connected to the current device.
movable signal	Mobile signal strength.

Copyright © 3onedata Co., Ltd.

The parameter name	explain
state	Whether the device is connected to the mobile network.

7.3

7-3Table 84 Description of the LAN state parameters

The parameter name	explain
protocol	The protocol used by the LAN.
MAC address	LAN, the MAC address of the interface.
address	LAN, the IP address of the interface.
subnet mask	Subnet mask of the LAN interface.
The port was activated	Port number used by the LAN.
receive	The LAN interface receives the packet size.
transmit by radio	The LAN interface sends the packet size.
Has been connected	LAN is connected time.



7.4 DHCP client

This section displays the DHCP client information for the router. D Description of the HCP client parameters are shown in Table 8-5.

7-4Table 85 Description of the DHCP client parameters

The parameter name	explain
host name	The DHPC client name.
IP address	DHCP, the IP address of the client.

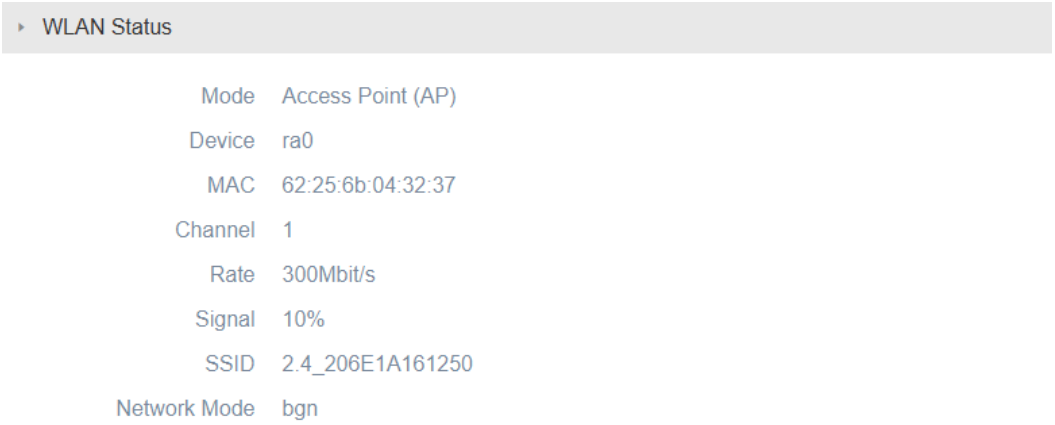
Copyright © 3onedata Co., Ltd.

The parameter name	explain
MAC address	DHCP, the MAC address of the client.
The remaining lease term	DHCP Client has the remaining rental time for IP after acquiring IP.

7.5 WLAN state

This section displays the WLAN status information for the router. The WLAN status parameters are described in Table 8-6.

7-5Table 86 Description of the WLAN status parameters



The parameter name	explain
pattern	Working mode of the WLAN.
equipment	device name.
channel	The WLAN's work channel.
speed	Transmission rate of the WLAN.
signal	Current signal size for the WLAN.
SSID	Identity of the WLAN server.
Network system	Network mode of the WLAN.

7.6 The WLAN has been connected to the device

This section displays the WLAN-connected device information for the router. The parameter descriptions of the WLAN connected devices are shown in Table 8-7.

7-6Table 87 Description of the parameters of the WLAN connected devices

Copyright © 3onedata Co., Ltd.



The parameter name	explain
MAC address	The MAC address of the connected device.
N etwork	The WLAN name of the connection.
signal	Device connection signal.
noise	noise-signal ratio
Receive rate	Device receiving bandwidth.
Send rate	Device transmission bandwidth.

7.7 DDNS state

This section displays the DDNS status information of the router. The DDNS status parameters are described in Table 8-8.

7-7Table 88 Description of the DDNS status parameters



The parameter name	explain
set up	
realm name	Domain name provided by the DDNS service provider.
register IP	Get the address
Network type	Type of network used by the DDNS services.
Update interval	The interval between the router and the DDNS domain name service provider updating the DDNS related information.

Copyright © 3onedata Co., Ltd.

8 FAQ

8.1 Hardware problems

8.1.1 All indicator lights are inactive

Problem phenomenon

All the indicator lights of the router are inactive.

analysis of causes

Possible reasons are as follows:

- The power supply does not meet the requirements.
- The power supply source is not connected to the router power supply port.

resolvent

- If the power supply does not meet the requirements, please ensure that the power supply is 12V.
- If the router power port is connected to the power supply, plug the power cord into the power port.

8.1.2 The SIM card holder connection issue

Problem phenomenon

The SIM holder cannot be inserted into the SIM card normally, and all the indicators of the router are not on.

analysis of causes

Possible reasons are as follows:

- The SIM holder is damaged.
- SIM, the card was inserted in the wrong orientation.

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

resolvent

- If the SIM holder is damaged, please contact our technical support engineer if we need to report for repair.
- If the SIM card is inserted in the wrong direction, please confirm that the SIM and the card chip are inserted at the slot chip end.

8.1.3 Network port connection problem

Problem phenomenon

The ETH / GE port light is not on and the router page cannot access.

analysis of causes

Possible reasons are as follows:

- Improper network cable connection
- The network cable has been damaged
- The PC network card is working abnormally or is disabled

resolvent

- If the network cable connection is incorrect, reconnect the network cable.
- If the network cable is damaged, replace the network cable.
- If the PC network card is abnormal, replace the network card or enable the network adapter

8.1.4 Antenna connection problem

Problem phenomenon

The antenna cannot be installed normally.

analysis of causes

Possible reasons are as follows:

- The antenna does not meet the fitting requirements.
- Incorrect antenna connection.

resolvent

- If the antenna does not meet the requirements, please replace the qualified antenna.
- If the antenna is not connected correctly, reconnect the antenna.

Copyright © 3onedata Co., Ltd.

8.2 Dial class problem

8.2.1 Dial interrupt

Problem phenomenon

Interruption during the device dialing process, unable not dial up the Internet.

analysis of causes

Possible reasons are as follows:

- Poor SIM card contact
- Whether the SIM card is opened or is overdue
- Whether the device supports the SIM card network type
- The power supply does not meet the requirements
- PIN is enabled and PIN code is set

resolvent

- If the antenna does not meet the requirements, please replace the qualified antenna.
- If the antenna is not connected correctly, reconnect the antenna.
- If the SIM network type is incorrect, replace the SIM network type according to the module.
- If the SIM card is not open, please open it. If the SIM card is overdue, recharge the SIM card.
- If the power supply does not meet the requirements, please replace the required power supply supply.
- If the PIN code is configured, use the correct PIN code.

8.3 The WEB configuration action class problem

8.3.1 Unable to log on to the configuration page

Problem phenomenon

Unable not log on to the WEB configuration page.

analysis of causes

Possible causes are as follows:

- Browser is not compatible
- Wrong router IP address accessed

resolvent

- If the browser is incompatible, use Google browser or IE 10 or above.

Copyright © 3onedata Co., Ltd.

- View the IP address obtained by the computer, the router IP and the computer IP are the same network segment.
- If you forget to configure the IP address of the interface, please use, hold the Reset button for 5 seconds, and wait for the router to restart. After restart, enter 192.168.1.1 to log in the configuration page.

8.3.2 Failed to upgrade firmware

Problem phenomenon

Upgrade firmware found no upgrade success.

analysis of causes

Possible reasons are as follows:

- When upgrading, the device is restarted due to other functions (such as the wireless module can not dial the number to automatically restart)
- The power supply does not meet the requirements
- The model and format of the upgraded firmware are incorrect
- The router is powered off during the upgrade process

resolvent

- If the upgrade fails due to the restart, turn down the other features and upgrade again.
- If the power supply does not meet the requirements, please replace the required power supply supply.
- If the upgrade firmware model and format is not correct, please replace the upgrade firmware with the correct format that matches the Sanwang 4G Router.
- If the router is powered off during the upgrade, ensure that the router power supply is normal during the upgrade.

8.3.3 The router is restarted repeatedly

Problem phenomenon

The router is restarted repeatedly

analysis of causes

Possible reasons are as follows:

- The server address communication for the online Hold function settings failed

resolvent

- If online Hold is set, click Application Configuration> Online Hold, open the Online Hold tab, turn off the function or fill in the normally communicating server IP address.

Copyright © 3onedata Co., Ltd.

9 Appendix

9.1 Parameter specification table

parameter type	span
General WORD type	Contains numbers, letters, and special characters (@,., \, /, -, _,:), Other types are illegal characters, such as username
Alphanumeric word type	Contains letters, numbers, and other characters are illegal characters, such as modem
The initial letter is generally word type	alphanumeric letter: such as hostname
CODE mould	Any character other than a space, such as svc-code
LINE mould	Any characters that can contain spaces, such as description, password (password not allowed is CODE type)
A.B.C. D mould	0.0.0.0~255.255.255.255, the ABCD is 0~255, such as the configuration of the IP address
A.B.C. D interface type	0.x.x.x 、127.x.x.x 、169.254.x.x 、255.x.x.x 、224.x.x.x 、x.x.x.255、x.x.x.0 All illegal
A.B.C. D/M mould	0.0.0. 0/0~255.255.255.255/32, ABCD 0-255 and M 0 to 32, as in subnet configuration
A.B.C. D / M, and the interface type	0.x.x.x 、127.x.x.x 、169.254.x.x 、255.x.x.x 、224.x.x.x 。x.x.x.255， x.x.x.0 is illegal, M is 0 and 32, such as configuration of interface IP address
Digital range type	As in 1~512, the value is any number from 1~512 (including 1 and 512)

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

9.2 term

I

IPSEC	Internet Protocol Security (IPSec) is an open standard framework that ensures confidential and secure communication on the Internet protocol (IP) network.

L

L2TP	L 2 TP (Layer 2 Tunneling Protocol) is an industry-standard Internet tunnel protocol that functions similar to the PPTP protocol, such as encrypted network data flows. However, there are also differences, such as PPTP requires IP network, L 2 TP requires packet point-to-point connection; PPTP uses a single tunnel, L 2 TP uses multiple tunnels; L 2 TP provides Baotou compression and tunnel verification, but PPTP does not support.
router	Device ted routing for information flow or data grouping.

M

Modem	General term of the modulator and demodulator taken together. A conversion interface that enables the digital data to be transmitted on the analog signal transmission line.

R

RIP2	RIP / RIP2 / RIPng: Routing Information Protocol) As an internal gateway protocol or IGP (internal gateway protocol), the routing protocol applies to AS systems. RIP is designed to work with moderately sized networks. Therefore, RIP is relatively suitable for simple campus network and regional network, but it is not suitable for complex network situation. RIP 2 comes from RIP and belongs to the supplementary protocol of RIP protocol. RIP 2 is mainly used to expand the amount of useful information loaded with RIP 2 information while increasing its security performance. RIP 2 is a UDP-based protocol. Under RIP2, each host sends and accepts packets from the UDP port 520 through a routing process. The default routing update cycle for the RIP protocol is 30 seconds.

W

Copyright © 3onedata Co., Ltd.

WMMP	WMMP (Wireless M2M Protocol) protocol is an application layer protocol designed to realize the data communication process between M2M, M2M in service, M2M platform, M2M platform, and M2M platform and application platform.

Copyright © 3onedata Co., Ltd.

10 Maintenance and Service

Since the date of product delivery, our company provides 5-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

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

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

10.1 Internet Service

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

10.2 Service Hotline

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

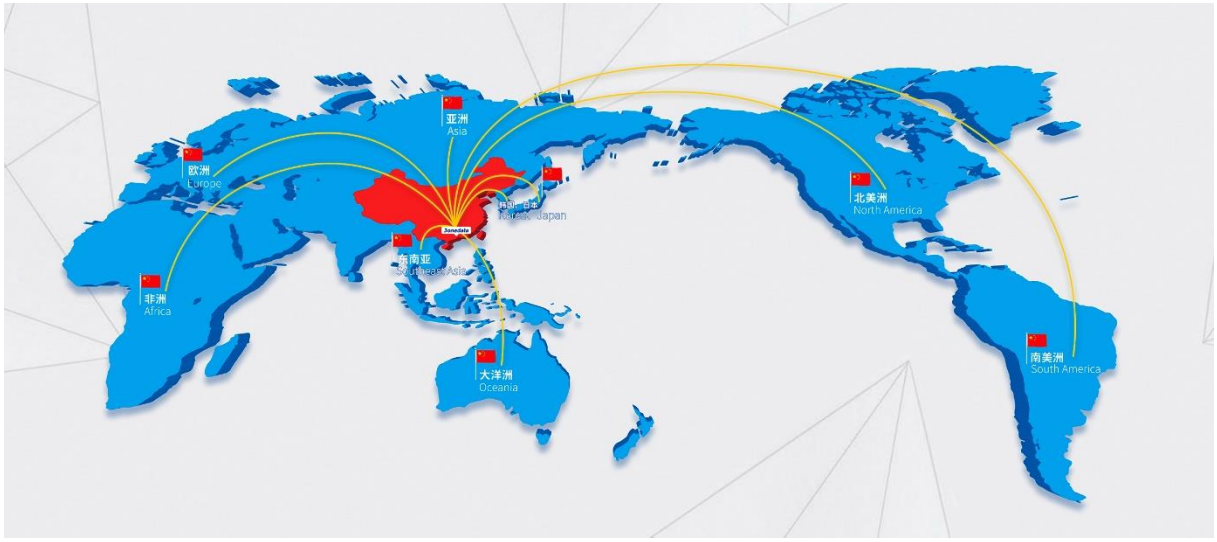
10.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem.

Copyright © 3onedata Co., Ltd.

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 Co., Ltd.

Headquarter Address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology Support:	tech-support@3onedata.com
Service Hotline:	4008804496
Official Website:	http://www.3onedata.com