3onedata



ICPE5000-2A-5GT-2E-LV
Industrial-grade 5G Router
User Manual

Document Version: 01

Issue Date: 12/13/2023

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

Copyright © 2023 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

The industrial grade 5G router user manual describes this router:

- Product Features
- Product installation and deployment
- describes how to configure and maintain the device through the web-based NMS client
- The Web NMS client provides basic configurations, application configurations, VPN configurations, forwarding configurations, security configurations, and system management configurations

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".

Copyright © 3onedata Co., Ltd.

Format	Description
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: 'Light Blue'.
About this chapter	The section 'about this chapter' provide links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

Symbols

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

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

Format	Description
Add	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.
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	12/13/2023	Product release

Copyright © 3onedata Co., Ltd.

Contents

PREFACE 1
CONTENTS I
1 BASIC CONFIGURATION 1
1.1 CONFIGURING LOCAL CONNECTION 1
1.1.1 Configuring the PC 1
1.1.2 Configuration Check 4
1.2 BASIC CONFIGURATION 6
1.2.1 Accessing the WEB Configuration Page 6
1.2.2 LAN Configuration 8
1.2.3 Mobile network 9
1.2.4 WLAN Configuration 16
1.2.5 DHCP service configuration 22
1.2.6 port settings 23
1.2.7 VLAN configuration 24
1.2.8 Interface configuration 26
1.2.9 Port Mirror 30
1.2.10 Link management 31
2 APPLICATION CONFIGURATION 36
2.1 ONLINE RETENTION 36
2.2 SERIAL APPLICATION 38
2.3 DDNS CONFIGURATION 43
2.4 TRAFFIC STATISTICS 45
2.5 QOS 47
2.6 TIMED TASKS 48
2.7 LOCATION SERVICES 51
3 VPN CONFIGURATION 57
3.1 VPDN CONFIGURATION (L2TP/PPTP) 57
4.1.1 L2TP SERVER FUNCTION CONFIGURATION 63
3.2 N2N_ V2 CONFIGURATION 65
3.3 OPENVPN 67
3.4 IPSEC 71
3.5 GRE 75
3.6 EOIP 77
3.7 VXLAN 80

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

4 FORWARDING CONFIGURATION 83
4.1 NAT 83
4.2 ROUTING CONFIGURATION 85
4.3 DMZ 88
4.4 OSPF CONFIGURATION 89
5 SECURITY CONFIGURATION 92
5.1 FIREWALL 92
5.2 IP FILTERING 93
5.3 MAC FILTERING 96
5.4 DOMAIN NAME FILTERING 98
6 SYSTEM CONFIGURATION 102
6.1 USER MANAGEMENT 102
6.2 CONFIGURATION MANAGEMENT 103
6.3 FIRMWARE UPDATE 104
6.4 APP INSTALLATION 105
6.5 SYSTEM TIME 106
6.6 LOG MANAGEMENT 108
6.7 DIAGNOSIS 109
6.8 DEVICE CLOUD NETWORK MANAGEMENT 111
6.9 SERVICE CONFIGURATION 113
6.10 MODULE UPGRADE 115
7 SYSTEM STATE 118
7.1 SYSTEM 118
7.2 MOBILE NETWORK 119
7.3 WAN 120
7.4 LAN 121
7.5 DHCP CLIENT 122
7.6 WLAN STATUS 122
7.7 WLAN CONNECTED DEVICE 123
7.8 DDNS STATUS 124
8 CONFIGURATION EXAMPLE 126
8.1 VPN CONFIGURATION 126
8.1.1 L2TP VPN 126
9 FAQ 130
9.1 HARDWARE RELATED ISSUES 130
9.1.1 All indicator lights are not on 130
9.1.2 SIM card holder connection issue 130
9.1.3 Network port connection issue 131
9.1.4 Antenna connection issue 131
9.2 DIALING RELATED ISSUES 132
9.2.1 Dialing interruption 132
9.3 WEB CONFIGURATION OPERATION ISSUES 133
9.3.1 Unable to log in to the configuration page 133

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

9.3.2 Upgrade firmware failed 133
9.3.3 Router restarts repeatedly 134
10 APPENDIX 135
10.1 PARAMETER SPECIFICATION TABLE 135
10.2 TERM 136
11 MAINTENANCE AND SERVICE 138
11.1 INTERNET SERVICE 138
11.2 SERVICE HOTLINE 138
11.3 PRODUCT REPAIR OR REPLACEMENT 138

Copyright © 3onedata Co., Ltd.

1 Basic Configuration

1.1 Configuring Local Connection

Preconditions

- Supplies power to the router.
- The LAN network port of the router is connected to the PC through an Ethernet cable.

1.1.1 Configuring the PC

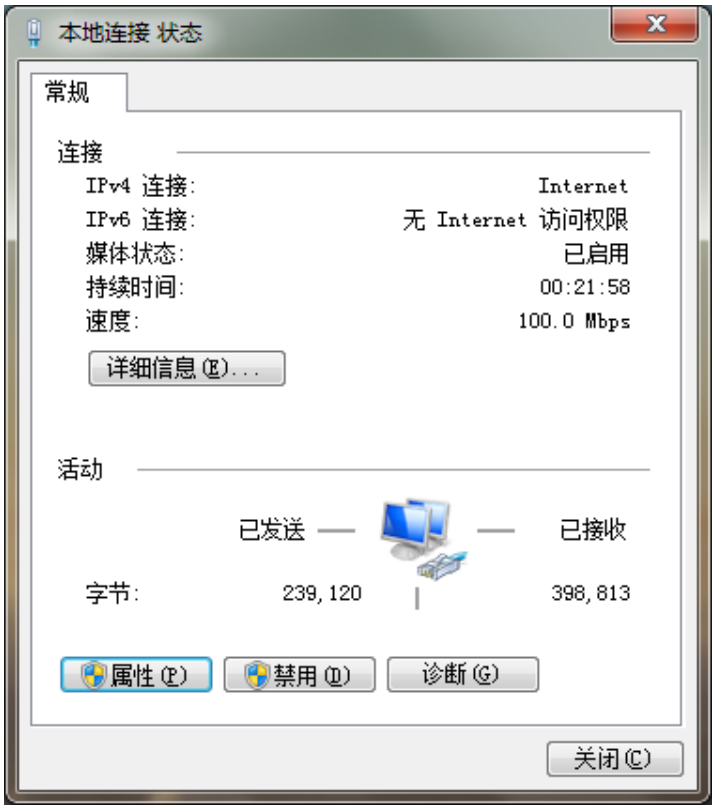
Operation Procedure

Step 1 Click“Initiate > Control panel > Network and sharing Center”，Double-click in the window that opens “Local connection”。

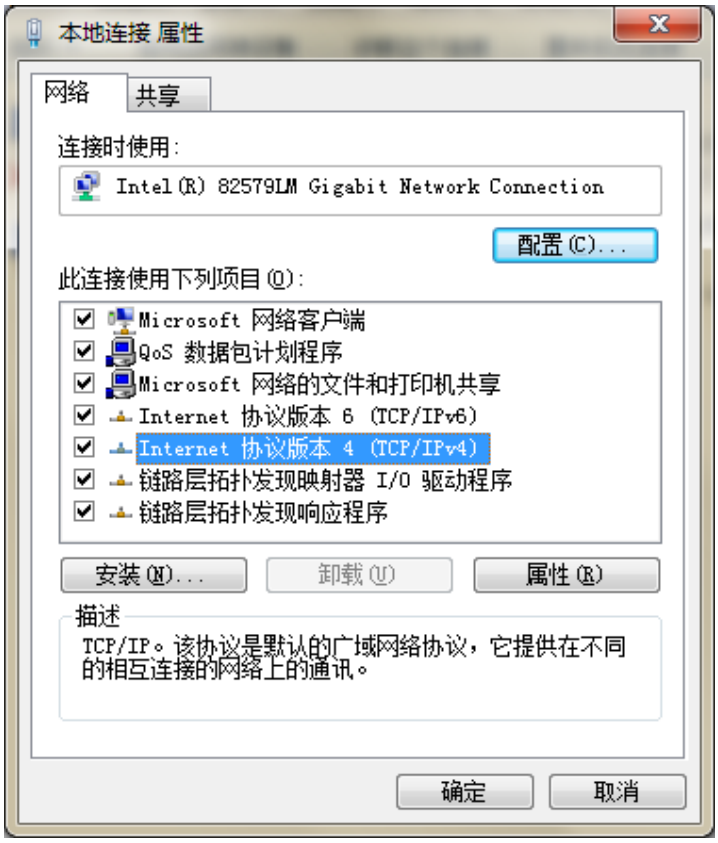


Copyright © 3onedata Co., Ltd.

Step 2 In the Local Area Connection Status window, click Properties.



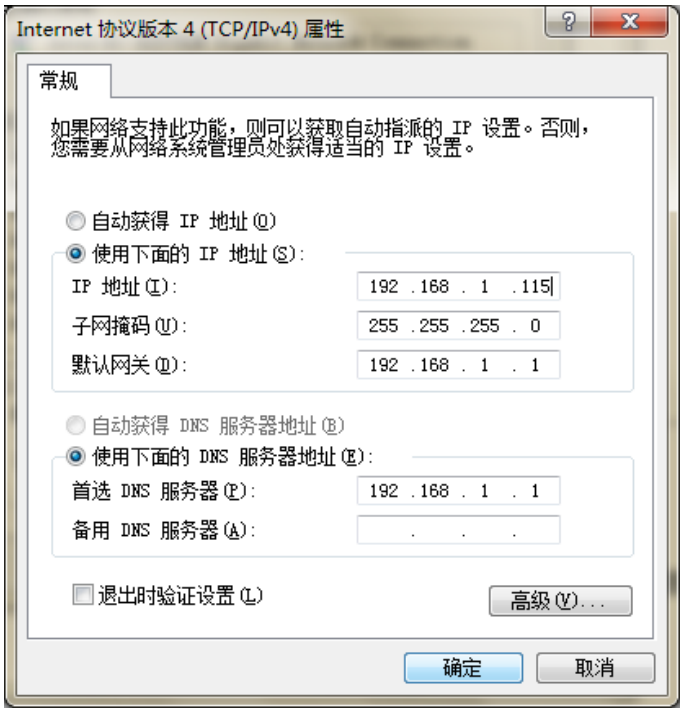
Step 3 Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.



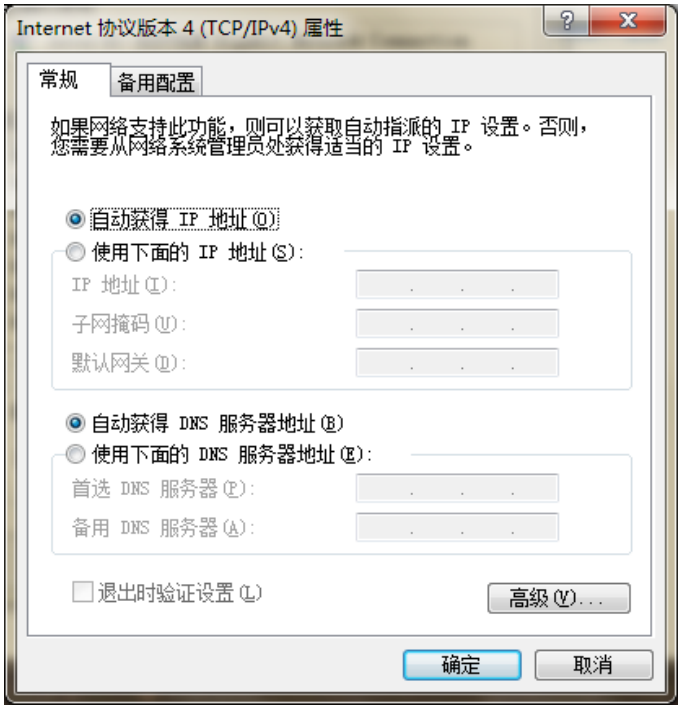
Copyright © 3onedata Co., Ltd.

Step 4 Configure the IP address of the PC by using two methods

Manually configure a static IP address for the PC that is on the same subnet as the router address, click, and configure Use the following IP address.



To automatically obtain an IP address from the DHCP server, click Obtain IP Address Automatically.



Copyright © 3onedata Co., Ltd.

1.1.2 Configuration Check

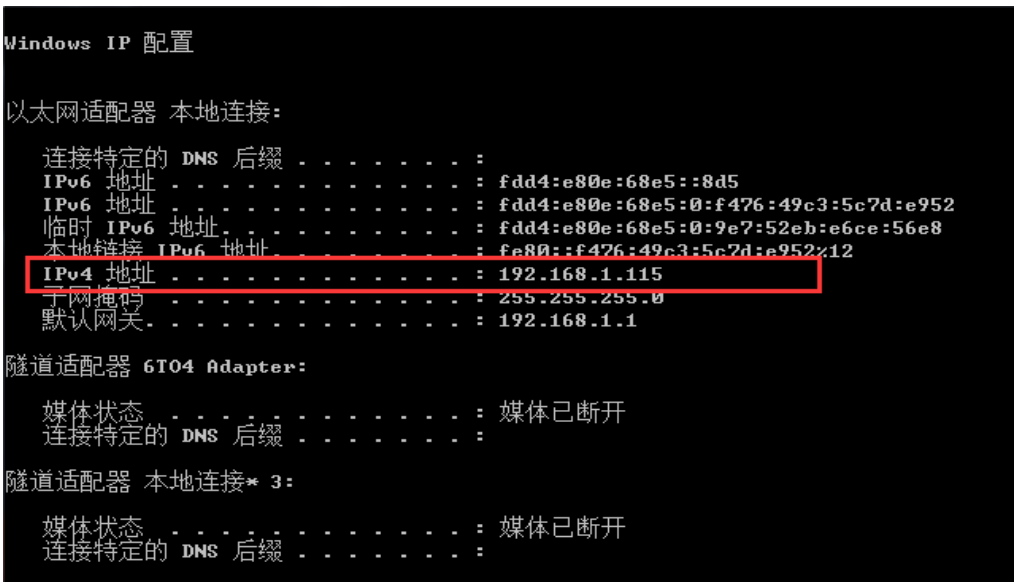
Operation procedure

Step 1 Click “Initiate > operation”，Enter cmd in the Run text box and press Enter. The Run window is displayed.



Step 2 Enter the ipconfig command in the Run window. The IP Address displayed in the ipconfig window is different for the two connection configuration methods. The IP Address displayed in the configuration method of the specified IP address is the IP address manually configured. The value is a random number from 2 to 254 in the IP Address displa

Result of specifying the IP mode ipconfig

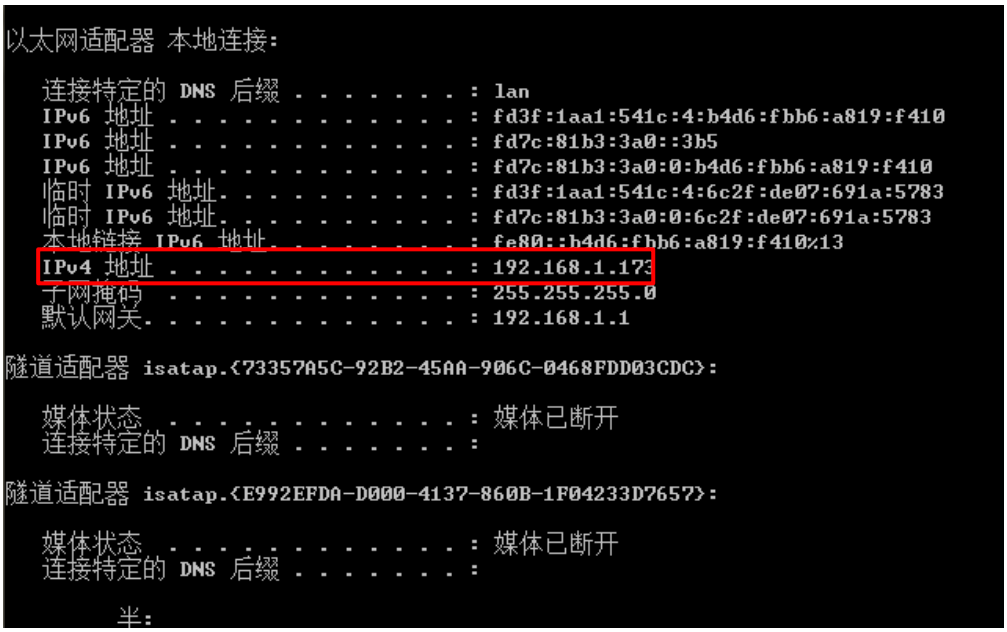


3onedata proprietary and confidential
Copyright © 3onedata Co., Ltd.

Step 3

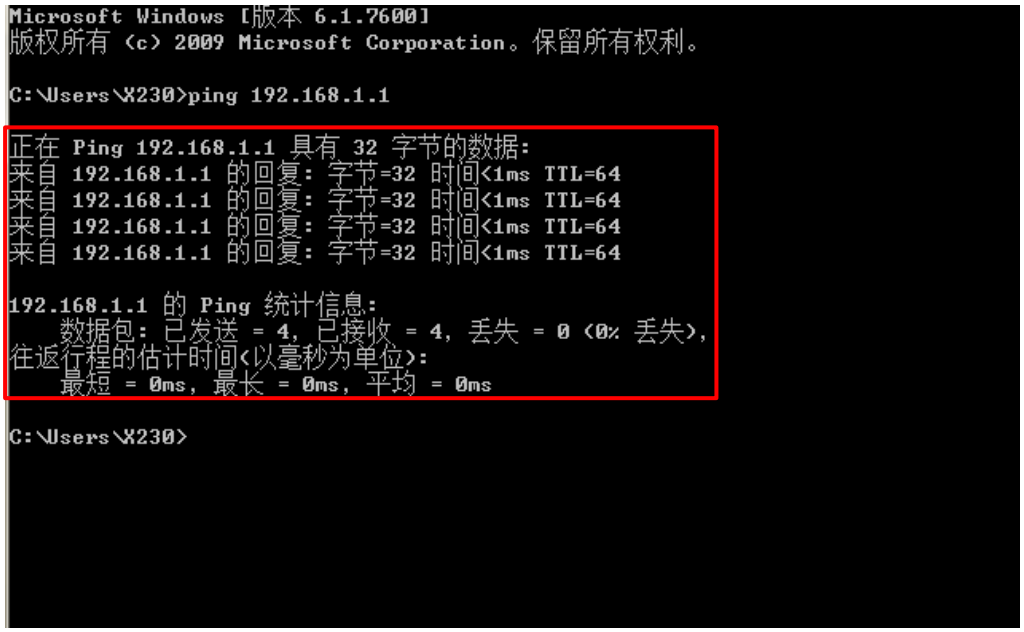
Step 4 yed in the configuration method of automatically obtaining IP addresses by

DHCP automatically obtains the execution result of ipconfig



DHCP.

Step 5 On the CLI, run ping 192.168.1.1. If the following information is displayed, the connection between the local computer and the router is normal.



——**Finish**

Copyright © 3onedata Co., Ltd.

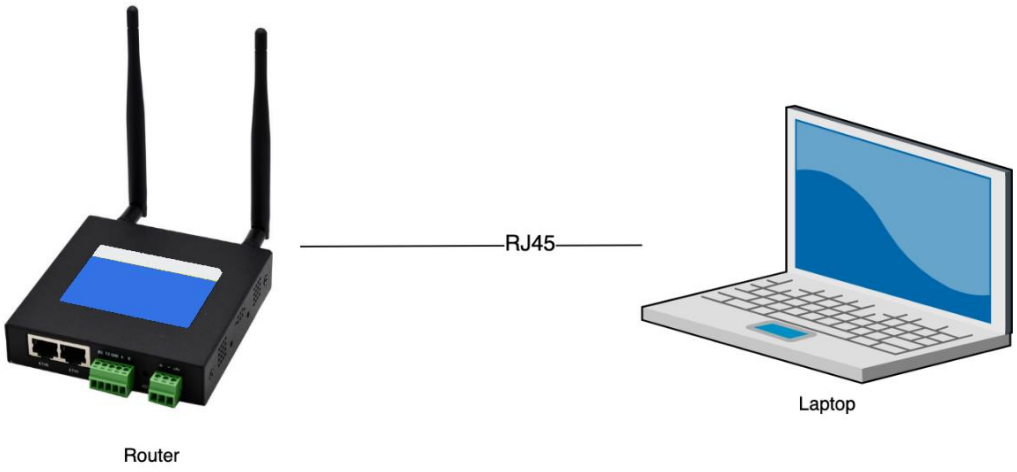
1.2 Basic Configuration

1.2.1 Accessing the WEB Configuration Page

Background Information

Users can directly log in to the web-based NMS using the device factory Settings to manage and maintain the device, or set the device IP address, web-based NMS parameters, and WEB users on the CLI as required, and then log in to the web-based NMS.

Users can use a PC to manage and configure the device through the Web-based NMS. Table 1-1 Description of port connections for each model



Model number	Interface description	Wiring instructions
ICPE5000 Series	ETH: indicates a LAN interface.	The PC is connected to the ETH port through a network cable.

pre-task

Before logging in to the WEB UI, complete the following tasks:

- You have configured an IP address for the access port.

Instructions

Copyright © 3onedata Co., Ltd.

The IP address of the device is 192.168.1.1, and the subnet mask is 255.255.255.0.

- The PC terminal is connected to the device through a network cable.

Instructions

If the PC cannot log in to the WEB UI by automatically obtaining an IP address, you are advised to set a static IP address in the same network segment as the device and then log in to the WEB UI.

- The device is running properly.
- The browser has been installed on the PC.

Operation procedure

Step 1 Open the chrome browser on the PC, enter the IP address of the router in the address box, http://192.168.1.1, and press Enter to access the user login authentication page.

Step 2 On the login page, enter the user name and password, and click OK.

Instructions

When logging in to the system for the first time, use the default user name and password. The default user name and password are admin. To change the password, see 7.1 User Management.

Step 3 After successful login, the home page is as shown in the following figure. On the home page, users can perform operations such as changing the language, restarting the router, and logging out.



Step 4 To log out of the current login, click Log Out at the upper right corner of the page to return to the user login page.

——**Finish**

Copyright © 3onedata Co., Ltd.

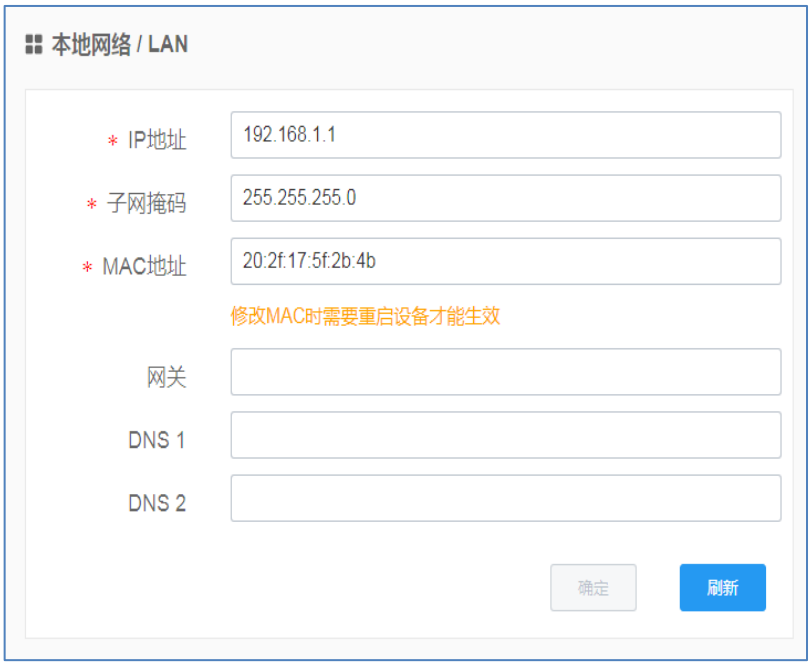
1.2.2 LAN Configuration

Background Information

The LAN interface is used to connect a router to a lower host computer. The lower host computer can access the Internet through the router and the network segments connected to the router can communicate with each other.

Operation procedure

Step 1 Log in to the WEB configuration page，Click “Network configuration > LAN configuration”，unpack “LAN” TAB.



Set LAN port connection parameters. Table 2-2 describes the parameters。

Table 1-2 Parameter description of LAN port connection types

Parameter name	Instructions	Configuration method
IP 地址	设置 LAN 口的 IP 地址。	在输入框中手动输入 格式：X.X.X.X 默认值：192.168.1.1
子网掩码	设置 LAN 口的子网掩码。	在输入框中手动输入 格式：X.X.X.X 默认值：255.255.255.0

Copyright © 3onedata Co., Ltd.

Parameter name	Instructions	Configuration method
MAC address	Set the MAC address of the LAN interface.	The format is not changed in normal cases XX:XX:XX:XX:XX:XX：
gateway	Set the IP gateway of the LAN port.	Enter manually in the input box format：X.X.X.X
DNS1	Set the preferred DNS server.	Enter manually in the input box format：X.X.X.X
DNS2	Example Set the standby DNS server.	Enter manually in the input box format：X.X.X.X

Step 5 Click OK to complete the configuration of the LAN port connection type.

——**Finish**

Instructions

If the page is not automatically redirected when you change the IP address of the LAN port, ensure that the PC has an IP address in the same network segment as the new LAN address, or set the PC to automatically obtain an IP address and enter the new LAN address in the browser.

1.2.3 Mobile network

Background Information

One of the core functions of Sanwang industrial wireless router, router through modem dial-up access to the Internet, to provide users with high-speed wireless broadband Internet access. 3G networks can usually reach 1 to 5Mbps Internet access rate, 3.5G networks can reach up to 20Mbps Internet access rate, 4G is up to nearly 100Mbps Internet access rate, 5G networks can reach 1000Mbps Internet access rate.

Copyright © 3onedata Co., Ltd.

Instructions

The ICPE5000 series support 5G-related configuration functions or dual SIM card functions

Operation procedure

Step 1 Log in to the WEB configuration page，Click “Network configuration > Mobile network”，The Mobile Network TAB is displayed.



Step 2 Set Mobile Network Parameters to Edit, Enable, and Disable. Table 2-4 describes the Mobile network parameters.

Table 1-4 Description of mobile network parameters

Parameter name	Instructions	Configuration method
enable	Whether to use mobile network functions.	● Select from the drop-down list ● Yes ● no
MODEM dial number	A code identification of the network, usually a standard network has a fixed service code, such as G network: *99***1#, C network: #777.	CODE type, a maximum of 64 bytes. For the input specification, see "Parameter Specification Table".

Copyright © 3onedata Co., Ltd.

Parameter name	Instructions	Configuration method
CID		Select from the drop-down list ● Profile 0~16
APN	Enter the access point for the cellular dial-up connection provided by your local Internet service provider.	Manual input
Authentication type	The router authentication type depends on the local ISP.	Select from the drop-down list ● Close ● PAP ● CHAP ● Automatic
User name/password	Enter the user name/password for the cellular dial-up connection provided by your local Internet service provider.	WORD type /CODE type. The value can contain a maximum of 64 bytes and can be null or exist at the same time
PIN code	The lock PIN of the SIM card provided by the carrier.	It is usually a 4-digit number
Enable dual SIM cards	Enable dual SIM cards	Select from the drop-down list ● yes ● no The main card can be SIM1 or SIM2

Step 3 Select Yes from the Display Advanced Configuration drop-down list to perform advanced mobile network configurations.

Copyright © 3onedata Co., Ltd.



Step 4 4 Set advanced parameters. Table 2-5 describes the parameters.

Table 1-5 Description of advanced mobile network configuration parameters

Parameter name	Instructions	Configuration method
5G access mode	5G networking mode is optional. The ICPE5000 series does not support this configuration.	Select from the drop-down list ● NSA+SA ● NSA ● SA
White card mode	Test card mode, belongs to the three major carriers SIM card does not need to be configured	Select from the drop-down list ● yes ● no

Copyright © 3onedata Co., Ltd.

Parameter name	Instructions	Configuration method
Priority registration network	Whether to preferentially register the network.	Select from the drop-down list ● yes ● no
agreement	The dial-up protocol usually uses auto. The router automatically selects the dial-up protocol according to the situation and forcibly selects pppd if necessary.	Select from the drop-down list ● auto ● pppd
Preferred network mode	Set the preferred network mode for routing.	Select from the drop-down list Automatic selection of 5G/4G/3G/2G ● NR only ● LTE+NR only ● LTE only ● Unicom 3G only ● Mobile 3G only ● Telecom 3G only ● GPRS only ● Only CDMA 1x
Enable the EHRPD	This function is available only for some EVDO networks.	Select from the drop-down list ● yes ● no
NAT	When a PC on a private network accesses the Internet, the NAT function must be enabled.	Select from the drop-down list ● yes ● no

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

Parameter name	Instructions	Configuration method
MTU	Maximum transmission unit of the interface. If the MTU is too small and the packet size is too large, too many fragments may be generated and packets may be discarded by the QoS queue. If the MTU value is too large, packets may be transmitted slowly or even lost.	Manually enter a value MTU The default value is 1500
Specify a subnet mask	You can modify the mask address of a mobile network interface	Enter manually in the input box format：X.X.X.X
Specified gateway	You can modify the gateway address of the mobile network interface	Enter manually in the input box format：X.X.X.X
Add default route	This function must be enabled when a PC on a private network accesses the Internet	Select from the drop-down list ● yes ● no
Gateway hop	Set the interface priority. The lower the value, the higher the interface priority	Normally, you do not need to change the priority. When multiple links are configured, you can set the priority by hop
DNS 1	Set the preferred DNS server.	Enter manually in the input box format：X.X.X.X
DNS 2	Example Set the standby DNS server.	Enter manually in the input box format：X.X.X.X

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

Parameter name	Instructions	Configuration method
PPP options	Dialing mode	
Log level	Filter detail log	DEBUG INFO NOTICE WARNING ERROR CRITICAL ALERT EMERG
Whether to lock base station	Support locking base station	Configure the relevant base station frequency, ID, carrier, BAND

Step 5 Configure online detection. Set the parameters as follows

Parameter name	Instructions	Configuration method
Master server	The primary server address must be reachable. The default address is empty, and both the primary and secondary servers are empty. That is, the probe is disabled	The format is X.X.X. x Default null
Standby server	The standby service address must be routable. The default address is empty, and both the active and standby servers are empty, indicating that probe is disabled	The format is X.X.X. x Default null
Interval time	Automatic detection interval, in seconds	Default 3 seconds
Timeout period	Setting the ICMP probe timeout period (The probe	Default 5 seconds

Copyright © 3onedata Co., Ltd.

Parameter name	Instructions	Configuration method
	timeout is automatically restarted)	
Maximum retry	Set the maximum number of retries for ICMP probe failures and dial up again when the maximum number of retries is reached.	Default 5 seconds
Strict detection	Enable detection or disable, strictly detect if the network cannot be detected within a specified time, the device will self-check and dial up the network again	Select from the drop-down list ● yes ● no
Forced offline restart	The system will be forcibly restarted if the number of retries exceeds the maximum	Select from the drop-down list ● yes ● no

Click OK to finish configuring mobile network parameters.

——**finish**

1.2.4 WLAN Configuration

Background Information

3Onedata Industrial wireless router provides AP mode and client mode two functions, through the function of AP mode, can provide you with wireless LAN hotspot, convenient access to the network, save the wiring trouble; You can enable the router to access other AP devices in client mode. In this way, the lower PC of the router can access the Internet through the connected AP devices.

Instructions

When client mode is selected, the router automatically matches the corresponding encryption mode and

Copyright © 3onedata Co., Ltd.

algorithm according to the selected AP (to keep the encryption mode consistent with that of the AP). For the shared key, enter the key for connecting to the AP. The ICPE5000 series does not support WIFI.

Operation procedure

Step 1 Log in to the WEB configuration page，Click “Network configuration >WLAN”，The WLAN Configuration TAB is displayed. Table 2-6 describes the displayed parameters.

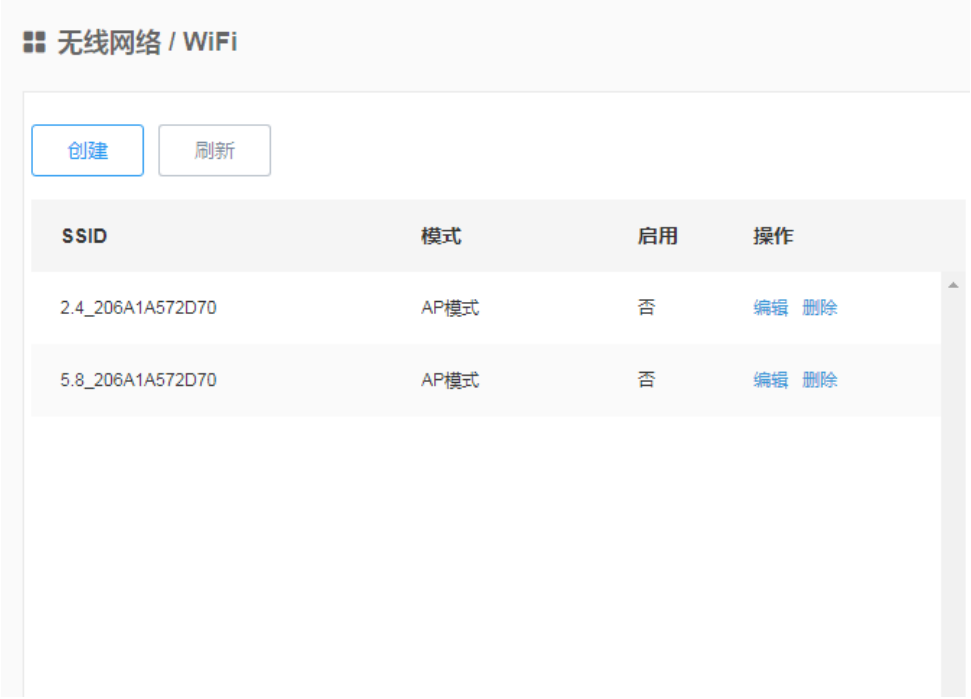


Table 1-6 WLAN parameters

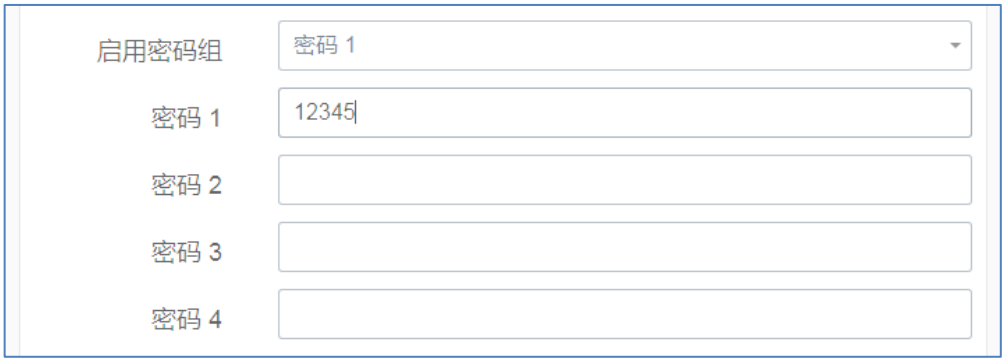
Parameter name	Instructions
SSID	Set a custom WiFi name.
mode	WLAN working mode: AP mode or client mode.
enable	Current WLAN status.
Controls	You can edit and delete the WLAN.

Step 2 Click Create to create a WLAN.

Copyright © 3onedata Co., Ltd.



Encryption mode Select "WEP Development Authentication", "WEP Shared Key"



Encryption Mode Select WPA, WPA2, WPA/WPA2.



Step 3 Step 3 Set WLAN parameters, as described in Table 2-7.

Table 1-7 WLAN parameters

Parameter name	Instructions	Configuration method

Parameter name	Instructions	Configuration method
enable	Whether the WLAN function is enabled.	Select from the drop-down list is no
mode	WLAN working mode: AP mode or client mode.	Select from the drop-down list ● AP mode ● Client mode
Enable trunk	Wireless relay mode, that is, wireless AP plays a relay role in the network connection, which can realize the relay and amplification of signals	Select from the drop-down list ● is ● no
MAC address	Set a user-defined MAC address	Custom
SSID	Set a custom WiFi name.	Enter a custom WiFi name
Hide SSID	This parameter is configured when AP mode is selected. This parameter is used to configure whether the WLANSSID is broadcast so that the client can search for the SSID. This parameter is usually disabled when the WLAN function is not searched and used by others. If the WLAN function is disabled, the SSID function is hidden from the network environment.	Select from the drop-down list ● is ● no
Radio power	Radio power 0dBm (1 mW) 4dBm (2 mW) 5dBm (3 mW) …… 19dBm (79 mW) 20dBm (100mW)	Select from the drop-down list Default is usually selected

Copyright © 3onedata Co., Ltd.

Parameter name	Instructions	Configuration method
passage	The WLAN working channel can be configured based on network requirements. The default value is 1. auto indicates channel self-adaptation. When there is no interference, channel 6 is used by default. When the same channel interferes, it automatically switches to the channel with less interference.	Select from the drop-down list ● auto ● 1～11
bandwidth	Bandwidth generally refers to the bandwidth that can be used to identify the data transmission capacity of signal transmission. The signal penetration of 20mhz is strong. The signal download capacity of 40mhz is strong	Select from the drop-down list ● 20mhz ● 40mhz
Network standard	WLAN network mode, the biggest difference between each network mode is that the transmission rate has a large difference, the default bgn mixed mode. If the working mode is AP, you need to manually set this parameter.	Select from the drop-down list ● n: 150Mbps ● bg: 11Mbps, 54Mbps adaptive ● bgn: Mixed modes of 11Mbps, 54Mbps and 150Mbps, adaptive according to the access LAN client
Low answer disconnect	No data interaction WIFI automatically disconnected	Select from the drop-down list ● is ● no

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

Parameter name	Instructions	Configuration method
Encryption mode	Configure the encryption mode of the WLAN. You can disable encryption when encryption authentication is not required. WEP encryption is relatively easy to crack, and WPA encryption is recommended.	Select from the drop-down list ● not encrypted ● WEPOpen authentication ● WEPShared key ● WPA ● WPA2 ● WPA/WPA2
WEP encryption (wired equivalent security, providing the same protection as wired LAN)		
Enable password group	Password group used to connect to the WLAN.	Select from the drop-down list ● Password 1 ● Password 2 ● Password 3 ● Password 4
Password	Enter the password for the access point the router wants to access.	Enter a custom password with more than 8 digits
WPA/WPA2 (WiFi Network Secure Access)		
algorithm	Encryption algorithm.	Select from the drop-down list ● Automatic ● Enforce CCMP (AES) encryption ● TKIP encryption is mandatory ● TKIP and CCMP (AES) encryption
cipher	Enter the password for the access point the router wants to access。	Enter a custom password with more than 8 digits

Step 4 Click OK to finish configuring WLAN parameters.

——**finish**

Copyright © 3onedata Co., Ltd.

1.2.5 DHCP service configuration

background information

Dynamic Host Configuration Protocol (DHCP) is a network protocol for a local area network that operates using the UDP protocol. After enabling the DHCP function, the lower computer can automatically obtain dynamic IP addresses, eliminating the hassle of modifying local IP addresses after gateway changes.

Operation steps

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



Step 2 Configure "DHCP Server Settings" with parameters as shown in Table 2-8.

Table 18 Parameter Description for DHCP Server Settings1-

Parameter Name	explain	Configuration method
Enable	Whether to use DHCP functionality.	Dropdown list selection ● yes ● no
Starting allocation base address	Configure the starting IP address of the DHCP address pool.	Default 100

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Number of Customers	The number of IP addresses that can be allocated from the starting address IP.	Default 150
Rental time unit	Time unit.	Dropdown list selection ● hour ● minute
Rental time	The DHCP client leases the IP after obtaining it.	Enter numerical values

Step 3 Configure the "DHCP Binding Table" with parameters as shown in Tables 2-9.

Parameter Name	explain	Configuration method
User IP address	Set a static specified IP address	Format X X. X.X
User MAC address	Set a static specified DHCP MAC address	Format XX: XX: XX: XX: XX: XX: XX

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

——**End**

1.2.6 port settings

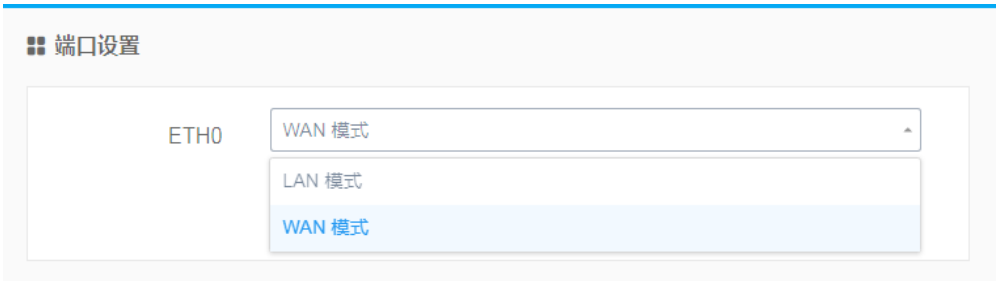
Explanation

The ICPE5000 series supports this feature

Operation steps

Step 5 After logging into the WEB configuration page, click "Network Configuration>Port Settings" to open the "Port Settings" tab.

Copyright © 3onedata Co., Ltd.



Step 6 Configure port parameters, as shown in Table 2-10.

Table 110 Parameter Description for Port Settings1-

Parameter Name	explain	Configuration method
LAN port	Select LAN port mode.	Dropdown list selection ● LAN mode ● WAN mode
WAN port	Select WAN port mode.	Dropdown list selection ● LAN mode ● WAN mode

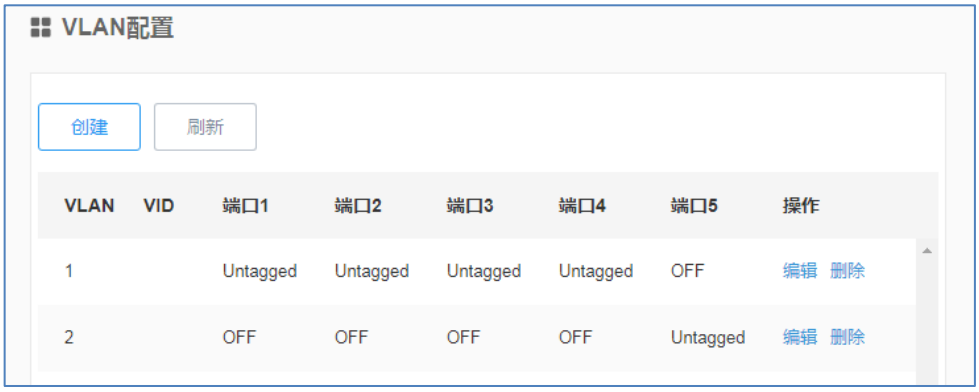
Step 7 Click "OK" to complete the configuration of port parameters.

——**End**

1.2.7 VLAN configuration

Operation steps

Step 8 After logging into the WEB configuration page, click "Network Configuration>VLAN Configuration" to open the "VLAN Configuration" tab.



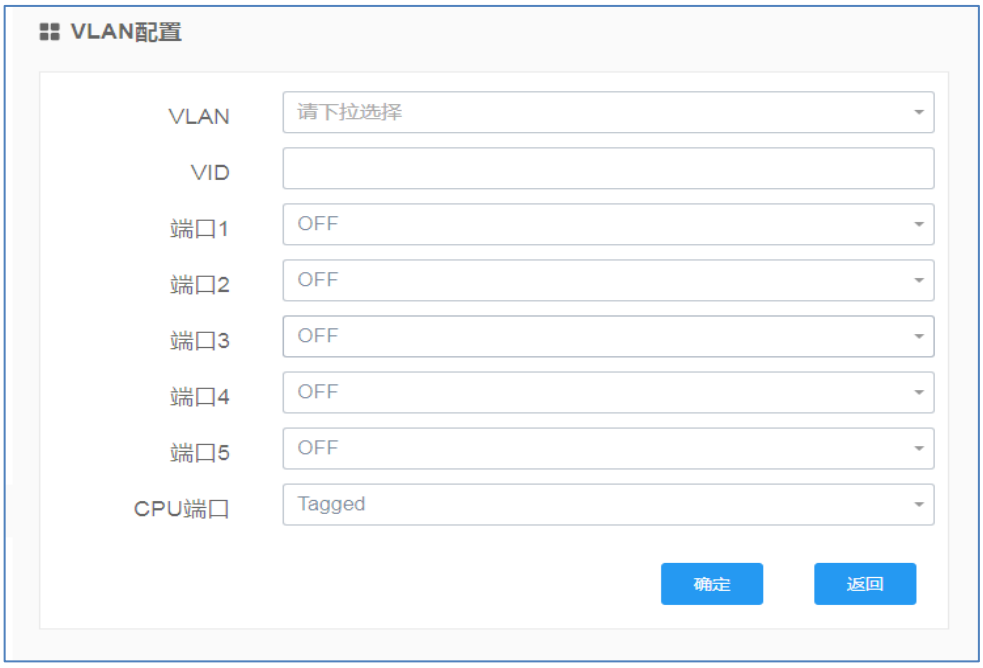
Step 9 The VLAN parameters are shown in Table 2-11.

Copyright © 3onedata Co., Ltd.

Table 12 VLAN List Parameter Description1-1

Parameter Name	explain
VLAN	VLAN port.
VID	The identification ID of the VLAN.
port	The status of each port.
operation	Can perform "edit" and "delete" operations on WLAN.

Step 10 Click "Create" to create a new VLAN.



Step 5 Configure the relevant parameters of VLAN, as shown in Table 2-12.

Table 112 VLAN Configuration Parameter Description1-

Parameter Name	explain	Configuration method
VLAN	Select the VLAN port.	Dropdown list selection ● VLAN 3-15
VID	The identification ID of the VLAN.	Alphanumeric WORD entry, please refer to "" for input specifications

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
port	Select the port status.	Dropdown list selection ● OFF ● Tagged ● Untagged
Port vid	No configuration is required when selecting to close the port.	Input numerical value, range of values from 0 to 4094
CPU port	Select CPU port status.	Dropdown list selection ● OFF ● Tagged ● Untagged

Step 6 Click "OK" to complete the configuration of VLAN parameters.

——**End**

1.2.8 Interface configuration

Operation steps

Step 11 After logging into the WEB configuration page, click "Network Configuration>Interface Configuration" to open the "Interface Configuration" tab. The interface list parameters are shown in Table 2-13.



Copyright © 3onedata Co., Ltd.

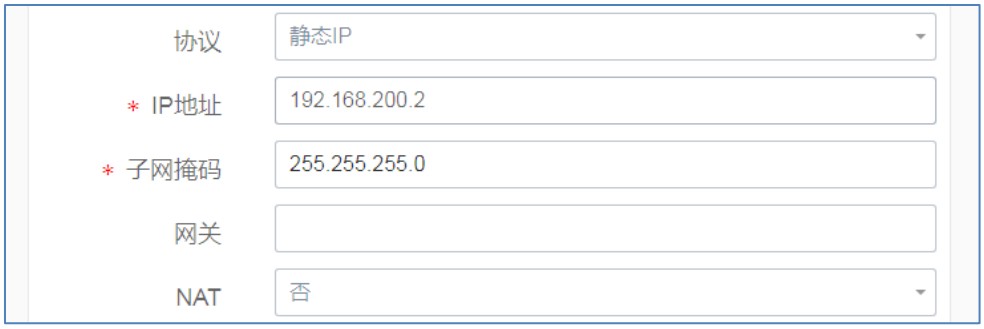


Table 113 Interface Parameter Description1-

Parameter Name	explain
VLAN	VLAN port.
VID	The identification ID of the VLAN.
IP address	Fill in the corresponding IP address
port	The status of each port.
operation	Can perform "edit" and "delete" operations on the interface.

Step 12 Click "Create" to create a new interface.

Copyright © 3onedata Co., Ltd.



Protocol selection "static IP"

Step 13 Configure interface parameters, as shown in Table 2-14.

Table 134 Interface Configuration Parameter Description1-2

Parameter Name	explain	Configuration method
Interface Name	Interface name.	WORD type, please refer to "" for input specificationsParameter specification table
protocol	The protocol used by the interface.	Dropdown list selection ● Static IP ● Dynamic DCHP
Use server to specify DNS	Whether to use the DNS specified by the server.	Dropdown list selection ● yes ● no
DNS 1	Set the preferred DNS server.	Manually enter in the input box Format: X X. X.X
DNS 2	Set up a backup DNS server.	Manually enter in the input box Format: X X. X.X
MAC address	The physical address of the interface.	Normally not modified, manually modified for special needs, format: XX: XX: XX: XX: XX: XX

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Interface type	Configure interface types.	Dropdown list selection ● Bridge ● None
License VLAN List	VLANs allowed for use.	Enter numerical values, multiple values separated by English status commas
Configure when selecting "static IP" for the protocol		
IP address	When selecting "Static IP" for "Protocol", it needs to be configured.	Interface type A B. C.D/M, please refer to "" for input specifications
Subnet Mask	WAN interface subnet mask.	Manually enter in the input box Format: X X. X.X Default value: 255.255.255.0
gateway	Specify the next hop address of the WAN interface.	When a WAN interface is needed as a switch, this option is optional and the format is the same as "IP address"
NAT	Do you want to enable NAT and address translation.	Dropdown list selection ● yes ● no

Step 7 Click "OK" to complete the configuration of the interface.

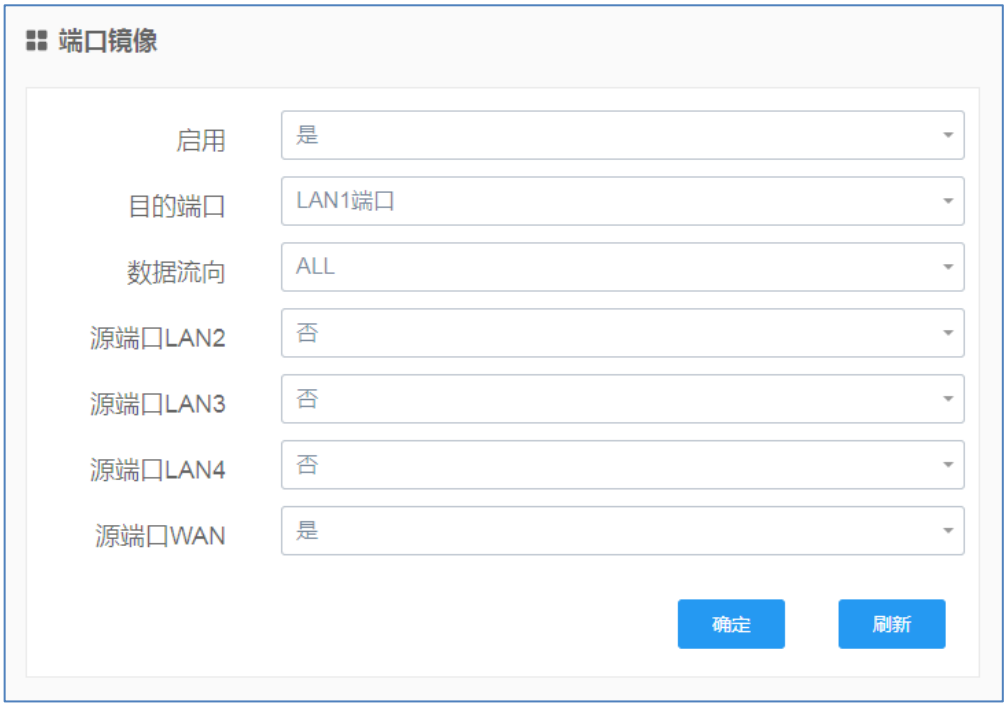
——**End**

Copyright © 3onedata Co., Ltd.

1.2.9 Port Mirror

Operation steps

Step 14 After logging into the WEB configuration page, click "Network Configuration>Port Mirroring" to open the "Port Mirroring" tab.



Step 15 Configure port mirroring parameters, as shown in Table 2-15.

Table 115 Explanation of Interface Mirror Parameters1-

Parameter Name	explain	Configuration method
Enable	Whether to use port mirroring.	Dropdown list selection ● yes ● no
Destination Port	Select the destination port for data forwarding, which cannot be used as the source port.	Dropdown list selection ● LAN1 port ● LAN2 port ● LAN3 port ● LAN4 port ● WAN port

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Data flow	Set the data flow direction, where RX is the input direction, TX is the output direction, and ALL is bidirectional.	Dropdown list selection ● close ● RX ● TX ● ALL
Source Port LAN2	Choose whether to monitor the data flow of this port. There can be multiple source ports.	Dropdown list selection ● yes ● no
Source Port LAN3	Choose whether to monitor the data flow of this port. There can be multiple source ports.	Dropdown list selection ● yes ● no
Source Port LAN4	Choose whether to monitor the data flow of this port. There can be multiple source ports.	Dropdown list selection ● yes ● no
Source Port WAN	Choose whether to monitor the data flow of this port. There can be multiple source ports.	Dropdown list selection ● yes ● no

Step 16 Click "OK" to complete the configuration of the interface image.

1.2.10 Link management

background information

The link management function supports the full utilization of multiple networking ports in the router, and enabling this function can achieve redundant switching of multiple networking links. In addition, it can also achieve functions such as bandwidth diversion and bandwidth stacking.

Explanation

The ICPE5000 series supports this feature

Copyright © 3onedata Co., Ltd.

Operation steps

Step 17 After logging into the WEB configuration page, click "Network Configuration>Link Management" to open the "Link Management" tab. The interface list parameters are shown in Table 2-16.

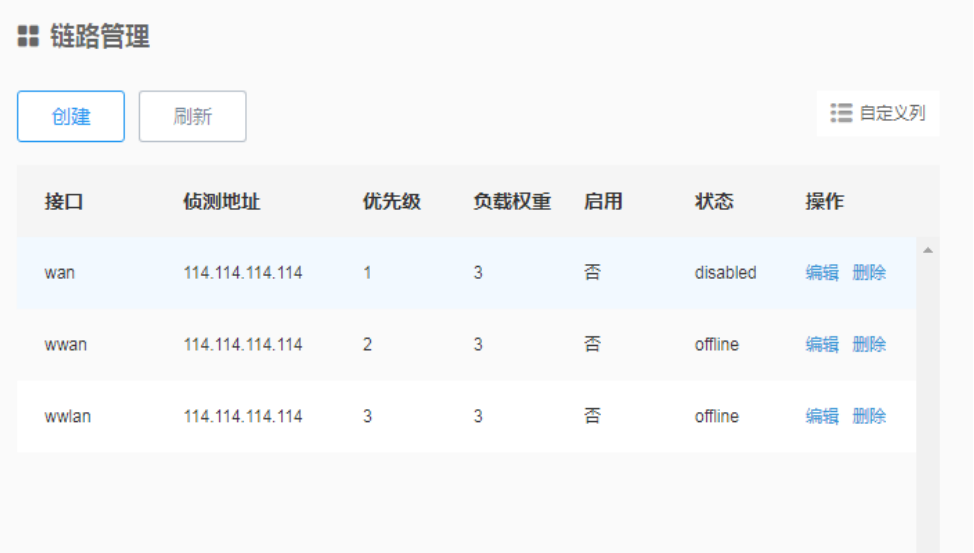


Table 116 Explanation of Interface Mirror Parameters1-

Parameter Name	explain
interface	Display the corresponding port name.
Detect address	Display the detection address for the corresponding port configuration.
priority	Display the priority value of the corresponding port.
Load weight	Display the load weight value of the corresponding port.
Enable	Display whether the port status is enabled.
state	The status of each port.
operation	Ports can be edited or deleted.

Step 18 Click "Edit" to edit the detailed link management parameters of the port, as shown in Table 2-17.

Copyright © 3onedata Co., Ltd.



Table 117 Description of Link Management Parameters1-

Parameter Name	explain	Configuration method
Enable	Whether to use link management.	Dropdown list selection ● yes ● no
Add detection route	Enabling this feature will add a policy route	Dropdown list selection ● yes ● no
interface	Display the name of the currently edited interface.	Unable to modify
Detect address	Fill in the detected IP address or domain name to determine if the port link is connected to the network normally.	Default 114.114.114.114

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Detection timeout	Based on the accumulated timeout time of the interface disconnection threshold item, determine whether the port link status has exceeded the communication timeout, in units of seconds.	Default 4 Value range: 1-255
Detection interval	The interval time for monitoring link status, measured in seconds.	Default 10 Value range: 5-255
Interface disconnection threshold	Determine whether the link has timed out response by pinging the number of address detections, in units of per occurrence.	Default 3 Value range: 1-255
Interface online threshold	Determine whether the link has returned to normal by pinging the address detection times, in units of per occurrence.	Default 2 Value range: 1-255
priority	Specify the usage priority of the port. The lower the value, the higher the priority. The high priority port link will be used as the main link for networking. When the main link is disconnected, the router will automatically switch to a lower priority link.	Default 1 Value range: 1-255
Load weight	By setting a numerical value, the bandwidth of the port is diverted, and the larger the value, the higher the traffic passing through the port link. To use this parameter, ensure that the priority of multiple ports is consistent.	Default 3 Value range: 1-255

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

Parameter Name	explain	Configuration method
Seamless switching	Is seamless switching enabled.	Dropdown list selection ● yes ● no

Step 19 Click "OK" to return to the higher-level configuration interface.

Step 20 Click "Submit Configuration" to save the configuration parameters for link management.

——**End**

Copyright © 3onedata Co., Ltd.

2 Application configuration

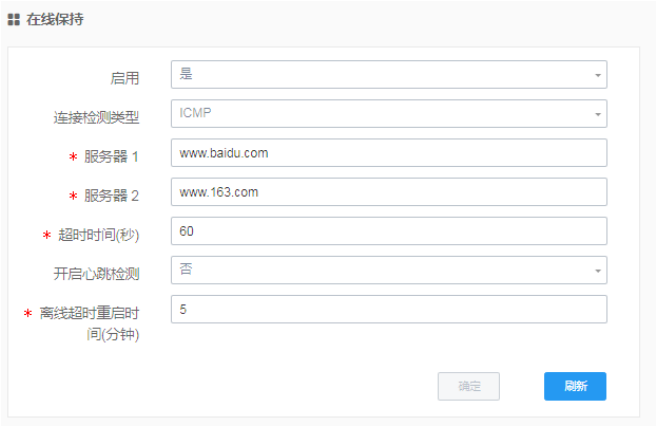
2.1 Online retention

background information

There are abnormal phenomena in wireless networks such as false links (successfully dialed and obtained IP, but the link is not connected), which are usually maintained through LCP and other methods. In addition to supporting this detection method, Sanwang industrial grade wireless routers also provide more reliable ICMP link detection function. It detects communication links through ping packet detection, and when detecting link abnormalities, it executes user set actions to achieve rapid recovery of links and systems. At the beginning of its design, ICMP link detection was mainly used to detect wireless links. Sanwang Industrial grade wireless routers can support detection of tunnel links such as VPN, and support simultaneous detection of multiple rules, greatly improving the recovery ability of product VPN tunnel and other link anomalies.

Operation steps

Step 1 After logging into the WEB configuration page, click "Application Configuration>Online Maintenance" to open the "Online Maintenance" tab.



Copyright © 3onedata Co., Ltd.

Step 2 Configure online maintenance parameters, as shown in Table 3-1.

Table 21 Explanation of Online Maintenance Rule Parameters2-1

Parameter Name	explain	Configuration method
Enable	Use online retention function.	Dropdown list selection ● yes ● no
Using Ports	Using a port will determine the network status by connecting through the access port; If not checked, it will be detected by sending ping packets using the ICMP protocol.	Default does not use port
Server 1	The destination address for detecting network status can be an IP address or a domain name. Setting it as a domain name requires ensuring that the router is configured with the correct DNS.	General WORD type, maximum 64 bytes, input specifications refer to ""
Port 1	Detect the port used for connection when using the port.	Value range: 1~65535 Default 80
Server 2	Detect the backup destination address for network status. If the primary address cannot be detected, check the backup address. If the backup address cannot be detected, it is determined that the detection has failed.	General WORD type, maximum 64 bytes, input specifications refer to ""parametergaugeFansurface

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Port 2	Backup port.	Value range: 1~65535 Default 80
Timeout time	Detect the timeout time of the link.	Default 30 seconds
Enable heartbeat detection	Is heartbeat detection enabled.	Dropdown list selection ● yes ● no
Detection interval	Configure when enabling heartbeat detection.	Fill in numerical values
Offline timeout restart	Network exception timeout	custom

Step 3 Click "OK" to complete the online retention configuration.

——**End**

2.2 Serial application

background information

The system has built-in communication functions with the registration center and data center, which can provide similar DTU functions.

Operation steps

Step 1 After logging into the WEB configuration page, click "Application Configuration>DTU" to open the "DTU" tab.

Copyright © 3onedata Co., Ltd.



Step 2 If you want to work in DTU server working mode, please configure the parameters of DTU in server working mode, as shown in Table 3-2.

Table 22 DTU Parameter Description2-

Parameter Name	explain	Configuration method
Enable	Whether to use DTU function.	Dropdown list selection ● yes ● no
Serial port selection	Select the serial port used by DTU.	Dropdown list selection ● Console ● UART terminal

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
protocol	The protocol used by DTU.	Dropdown list selection ● custom ● DTU ● MQTT ● HJ212 ● DC ● Modbus Net bridge ● 3H
Main Center IP	The address of the DTU central server.	Manually enter in the input box Format: X X. X.X Default value: 192.168.1.115
Main center port	DTU central server port.	Value range: 0-65535
Baud rate	Select the serial port baud rate.	Dropdown list selection ● 300 ● 600 ● 1200 ● ● 57600 ● 115200
Data bits	Serial port data transmission bit.	Dropdown list selection 5-8
Check bit	Serial port check bit.	Dropdown list selection ● None ● Odd ● Even
Stop bit	Serial port stop bit.	Dropdown list selection ● 1 ● 2
Device ID	Connect the registered identification ID in the data.	8-bit hexadecimal number

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
SIM card number	Connect the registered SIM card number in the data.	Enter numerical values

Step 3 Select "Yes" from the "Display Advanced Configuration" drop-down box to configure DTU Advanced.



Step 4 Configure advanced configuration parameters, as shown in Table 3-3.

Table 23 DTU Advanced Configuration Parameter Description2-

Parameter Name	explain	Configuration method
Working mode	DTU working mode.	Dropdown list selection ● TCP Client ● UDP client ● TCP server

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Heartbeat interval (seconds)	The time interval for sending heartbeat packets.	Manually entering numerical values
Data frame interval time (milliseconds)	The time interval for sending each frame of data.	Manually entering numerical values
Maximum number of cached packets	The maximum number of cached packets.	Default 1024
Whether to escape	Escape heartbeat data	Dropdown list selection ● yes ● no
Number of servers	The number of central servers refers to the number of effective servers.	Dropdown list selection ● 1-5
Server IP2	DTU Central Server Address 2	Manual input
Server Port 2	DTU Central Server Port 2	Value range: 0~65535
Server IP3	DTU Central Server Address 3	Manual input
Server Port 3	DTU Central Server Port 3	Value range: 0~65535
Server IP4	DTU Central Server Address 4	Manual input
Server Port 4	DTU Central Server Port 4	Value range: 0~65535
Server IP5	DTU Central Server Address 5	Manual input
Server Port 5	DTU Central Server Port 5	Value range: 0~65535

Step 5 Click "OK" to complete the DTU server/client configuration.

——**End**

Copyright © 3onedata Co., Ltd.

2.3 DDNS configuration

background information

DDNS, Dynamic Domain Name Server, is a dynamic domain name service. The DDNS service allows mapping a dynamic IP address to a fixed domain name resolution service provider. Every time a user connects to the network, the client program will transmit the dynamic IP address of the host to the server program located on the service provider's host through information transmission. The server program is responsible for providing DNS services and implementing dynamic domain name resolution. That is, the DDNS service allows you to assign a fixed domain name to the dynamic WANIP of the host, Other users can directly access your host through this fixed domain name, rather than through dynamic WAN IP addresses. The dynamic WAN IP address of the router is directly assigned by the ISP.

Operation steps

Step 1 After logging into the WEB configuration page, click "Application Configuration>DDNS" to open the "DDNS Services" tab.



Step 2 Configure DDNS service parameters, as shown in Table 3-5.

Table 22 DDNS Parameter Description2-2

Parameter Name	explain	Configuration method
Enable	Whether to use DDNS service.	Dropdown list selection ● yes ● no

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Service provider	The domain name provider option corresponding to the applied domain name is currently not supported by our company for DDNS services of domain name providers outside the list.	Dropdown list selection ● Peanut shell ● Dyndns.org ● Changeip.com ● Zonededit.com ● Free. editdns. net ● 3322.0rg ●
User name/password	Register the username and password for the DDNS service provider domain name.	General WORD/CODE type, maximum 64 bytes
domain name	The domain name provided by the DDNS service provider, which corresponds to the IP of the router, is usually accessed by accessing the domain name.	General WORD type, maximum 64 bytes.
Refresh time (minutes)	The interval between routers and DDNS domain name service providers to update DDNS related information. Some domain name providers send update data after an IP change, and the update interval depends on the DDNS service you purchased. It is generally recommended to wait for more than 4 minutes.	Value range: 5-120 Unit: minutes Default: 10

Step 3 Click "OK" to complete the configuration of the DDNS service.

——**End**

Copyright © 3onedata Co., Ltd.

explain

Every time the router restarts, the IP address obtained from the SIM card service provider will change. If the user uses the requested DDNS domain name when logging into the router remotely, regardless of how the router's modemIP address changes, the user can log in to the router page.

2.4 Traffic statistics

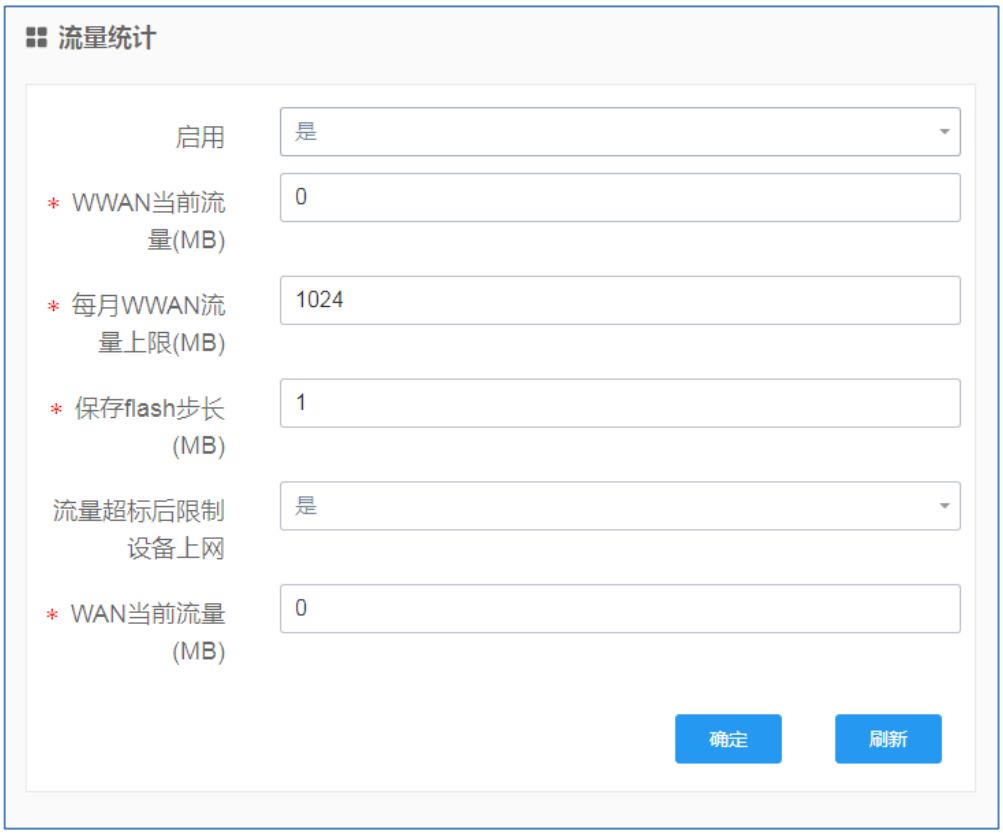
background information

As a wireless router, most users are concerned about the usage of router traffic, so some functions are to calculate the traffic generated by the router during wireless dial-up internet access. The router will control the online operation of the router based on the monthly traffic limit. When the router exceeds the monthly traffic limit, the router will disconnect from the network and prohibit users from accessing the external network. If the SIM card exceeds the limit, the used traffic at the beginning of each month will be reset to zero.

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

Operation steps

Step 1 After logging into the WEB configuration page, click "Application Configuration>Traffic Statistics" to open the "Traffic Statistics" tab.



Step 2 Configure traffic statistics parameters, as shown in Table 3-7.

Table 23 Explanation of Traffic Statistics Parameters2-3

Parameter Name	explain	Configuration method
Enable	Whether to use traffic statistics function.	Dropdown list selection ● yes ● no
WWAN Current Traffic (MB)	Set the traffic already used by the wireless wide area network this month.	Manual input Default: 0 Unit: MB
Monthly WWAN traffic limit (MB)	Set the monthly SIM card traffic threshold.	Manual input Default: 1024 Unit: MB

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Save Flash Step Size (MB)	The traffic span when writing the traffic statistics results into Flash, that is, the data is written into Flash after the cumulative usage of traffic reaches a step size.	Manual input. Default value 1 Unit: MB
Restricting devices from accessing the internet after exceeding traffic limits	Does the router restrict internet access when the amount of data used this month exceeds the monthly data limit.	Dropdown list selection ● yes ● no
Current WAN traffic (MB)	Set the traffic already used by the wide area network this month.	Manual input Default: 0 Unit: MB

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

——**End**

2.5 QoS

background information

The QoS function is mainly aimed at controlling bandwidth, allocating download and upload bandwidth as needed.

Operation steps

Step 1 After logging into the WEB configuration page, click "Application Configuration>QoS" to open the "QoS" tab.



Step 2 Configure QoS parameters, as shown in Table 3-8.

Table 24 QoS parameter description2-4

Parameter Name	explain	Configuration method
Enable	Whether to use QoS function.	Dropdown list selection ● yes ● no
Download (KByte)	The bandwidth size of the user's downlink.	Manually entering numerical values
Upload (KByte)	The bandwidth size of the user's uplink.	Manually entering numerical values
Privileged TCP	Specify unlimited speed port	Fill in ports that are not restricted by speed
Privileged UDP	Specify unlimited speed port	Fill in ports that are not restricted by speed

Step 3 Click "OK" to complete the QoS configuration.

——**End**

2.6 Timed tasks

background information

As a wireless service gateway routing product, many customers hope to control the online duration of the router when using it, in order to better manage network services and 3G/4G/5G tariffs. The task management of Sanwang industrial grade routers can meet the needs of customers. Customers can configure multiple online time periods according to their needs (such as a certain number of hours on a certain day). In addition, it can also achieve task execution at time points (such as redialing or restarting the system at midnight every day).

Operation steps

Step 1 After logging into the WEB configuration page, click "Application Configuration>Timed Tasks" to open the "Timed Tasks" tab. The scheduled task list parameters are shown in Table 3-9.

Copyright © 3onedata Co., Ltd.



Table 25 Parameter Description of Timed Task List2-5

Parameter Name	explain
minute	When used in combination, it is a time point, and when used independently, it is every X minutes.
hour	When used in combination, it is a time point, and when used independently, it is every X hours.
date	On a certain day of a certain month.
month	Month.
week	Week.
task	The task to be executed.
operation	Can perform "edit" and "delete" operations on scheduled tasks.

Step 2 Click "Create" to create a new scheduled task.

Copyright © 3onedata Co., Ltd.



Step 3 Configure timed task parameters, as shown in Table 3-10.

Table 26 Explanation of Timed Task Rule Parameters2-6

Parameter Name	explain	Configuration method
minute	When used in combination, it is a time point, and when used independently, it is every X minutes.	● If a numerical value is directly entered, it is a time point, with a value range of 0~59 ● If "*/" is added before the value X, the task will be executed every X minutes
hour	When used in combination, it is a time point, When used independently, it is every X hours.	● If a numerical value is directly entered, it is a time point, with a value range of 0-23 ● If "*/" is added before the value X, the task will be executed every X hours
date	On a certain day of a certain month.	Value range: 1-31, multiple dates can be separated by ","

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
month	Month.	Value range: 1-12, multiple months can be separated by ","
week	Week.	Value range: 1-7, available for multiple days, separated by "x", available for consecutive days "x-y"
task	The task to be executed.	Dropdown list options: ● Reboot ● Turn off LAN ● Enable LAN

Step 4 Click "OK" to complete the configuration of the scheduled task.

——**End**

2.7 Location Services

Explanation: The ICPE5000 series supports location services

Operation steps

Step 1 After logging into the WEB configuration page, click "Application Configuration>Location Services" to open the "Location Services" tab.



Step 2 Configure location service parameters, as shown in Table 3-11.

Table 27 Description of Location Service IP Forwarding Parameters2-7

Parameter Name	explain	Configuration method
Enable	Whether to use location services.	Dropdown list selection ● yes ● no
Main Center IP	The address of the central server.	Manually enter in the input box Format: X X. X.X Default value: 192.168.1.2
Main center port	Central server port.	Value range: 0-65535
Device ID	Device ID number.	8-digit characters
data type	Location data type.	Dropdown list selection ● raw data ● Location data ● GPGGA ● GPRMC ● IEC101
GPS reporting interval (seconds)	The time interval for reporting the location.	Value range: 1~500

Step 3 Configure the serial port forwarding parameters, as shown in Table 3-12.



Table 212 Description of Serial Port Forwarding Parameters for Location Services2-

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Enable	Whether to use location services.	Dropdown list selection ● yes ● no
Serial port selection	Provide multiple serial port options (some models only support console serial port interface)	Dropdown list selection ● Console ● COM1 ● COM2 ● COM3 ● COM4
Baud rate	Select the serial port baud rate.	Dropdown list selection ● 300 ● 600 ● 1200 ● ● 57600 ● 115200
Data bits	Serial port data transmission bit.	Dropdown list selection 5-8
Check bit	Serial port check bit.	Dropdown list selection ● None ● Odd ● Even
Stop bit	Serial port stop bit.	Dropdown list selection ● 1 ● 2
data type	Location data type.	Dropdown list selection ● raw data ● Location data ● GPGGA ● GPRMC ● IEC101

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Reporting interval (seconds)	Reporting cycle in seconds	Default 60 seconds

Step 4 Configure the Modbus parameters for the location service, as shown in Table 3-13.



Table 213 Description of Modbus Parameters for Location Services2-

Parameter Name	explain	Configuration method
Enable	Whether to use location services.	Dropdown list selection ● yes ● no
Working mode	ModbusTPC/ModbusRTU	Dropdown list selection ● ModbusTPC ● ModbusRTU
Slave station number	The station number is 1 byte, with a value range of 0 to FFH	Between 1 and 255
port	Port numbers within the range of 0-65535	Port numbers within the range of 0-65535

Step 5 Configure location service JT/T808, and the parameter specifications are shown in Table 3-14.

Copyright © 3onedata Co., Ltd.



Table 214 Location Service JT/T 8 08 Parameter Description2-

Parameter Name	explain	Configuration method
Enable	Whether to use location services	Dropdown list selection ● yes ● no
Protocol version	Transport Vehicle Satellite Status System Agreement 2019/2013	Dropdown list selection ● 2019 ● 2013
Main Center IP	The address of the central server	Manually enter in the input box Format: X X. X.X Default value: 192.168.1.2
Main center port	Central server port	Value range: 0-65535
Heartbeat cycle	Send heartbeat every N seconds	Value range: 0-4294967295
Timeout time	Detection of link timeout time	Value range: 0-4294967295

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

Parameter Name	explain	Configuration method
Position reporting interval	Position interval reporting cycle	Value range: 0-4294967295

Step 6 Configure the location service Baidu Eagle Eye parameters, as shown in Table 3-15.



Table 215 Description of Baidu Eagle Eye Parameters for Location Services2-

Parameter Name	explain	Configuration method
Enable	Whether to use location services	Dropdown list selection ● yes ● no
Service ID		
name		
Token		
Update interval time	Data update time	Value range: 1~999999999 seconds

explain

Baidu Eagle Eye related configuration information needs to be obtained and filled in through the Baidu platform.

Copyright © 3onedata Co., Ltd.

3 VPN configuration

3.1 VPDN configuration (L2TP/PPTP)

background information

VPDN, also known as Virtual Private Dial-up Networks, is a type of VPN service based on dial-up users. The dial-up access method is a secure virtual private network established by combining the carrying function of IP networks with corresponding authentication and authorization mechanisms. It is a technology that has rapidly developed in recent years with the development of the Internet. VPDN supports both L2TP and PPTP protocols.

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

L2TP (Layer Two Tunneling Protocol) is an abbreviation for Layer Two Tunneling Protocol, which is a type of VPDN (Virtual Private Dialup Network) technology specifically used for channel transmission of Layer Two data. L2TP provides a means of remote access control, where users dial into the company's local network access server (NAS) through PPP to access the company's internal network, obtain IP addresses, and access network resources with corresponding permissions. The employee dials into the company network as securely and conveniently as if on the company LAN.

Operation steps

Step 1 After logging into the WEB configuration page, click on "VPN Configuration>L2TP/PPTP" and click on the "Client Creation" tab. The

Copyright © 3onedata Co., Ltd.

parameter description of the VPDN channel list is shown in Table 4-1.



Table 31 VPDN Channel List Parameter Description3-1

Parameter Name	explain
Interface Name	The name of the VPDN rule.
protocol	The protocol adopted by VPDN.
server	The server IP address or domain name used for access.
user name	Authorized legitimate access users to access the server.
Enable	Is the VPDN channel rule enabled.
state	The current status of the VPDN channel rule.
operation	Can perform "edit" and "delete" operations on scheduled tasks.

Step 2 Click "Create" to create a new VPDN channel.

Copyright © 3onedata Co., Ltd.



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

Table 32 VPDN Rule Parameter Description3-2

Parameter Name	explain	Configuration method
Enable	Is VPN connection enabled.	Dropdown list selection ● yes ● no
Interface Name	The name of the VPDN rule.	Suggest using easily recognizable names. Such as city city, specific events, etc

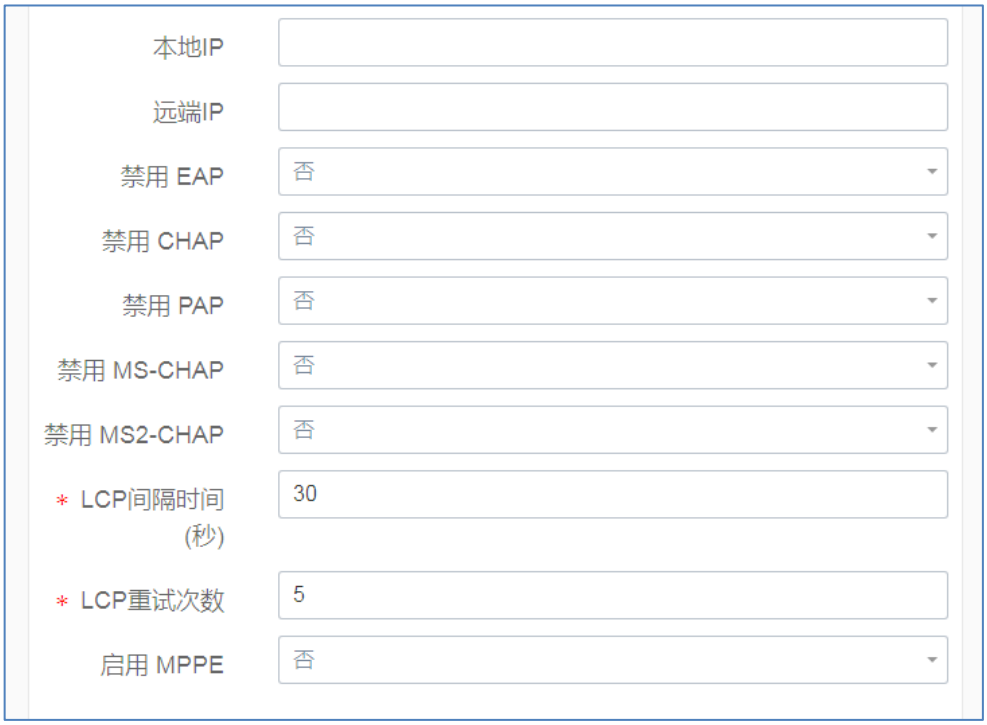
Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
protocol	The protocol adopted by VPDN.	Dropdown list selection ● PPTP ● L2TP
server	The server IP address or domain name used for access.	Fill in the IP address or domain name of the server used for access
User name/password	Authorized legal access users and passwords for accessing the server.	Fill in the authorized legal access username/password for accessing the server
Add default route	After a successful VPN connection, set the default route to this VPN tunnel.	Dropdown list selection ● yes ● no
Add tunnel routing	Add a route that allows the other subnet to access this terminal network.	Dropdown list selection ● yes ● no
NAT	Whether to use NAT function.	Dropdown list selection ● yes ● no
MTU	Set the maximum transmission unit.	Manually entering numerical values The default value is 1500
Gateway Hop	Set the hop count of the gateway after VPN connection.	Manual input
Use server to specify DNS	Whether to use the server's DNS.	Dropdown list selection ● yes ● no
Reconnection interval (seconds)	The time interval for device reconnection.	Manual input

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

Parameter Name	explain	Configuration method
Do not enable after restart	After the router restarts, the VPN will be shut down.	Dropdown list selection ● yes ● no

Step 4 Select "Yes" from the "Display Advanced Configuration" dropdown box to configure VPDN advanced.



Configure advanced configuration parameters, as shown in Table 4-3.

Table 33 VPDN Advanced Configuration3-3

Parameter Name	explain	Configuration method
Local IP	Set the local static tunnel IP address.	Manually enter in the input box Format: X X. X.X
Remote IP	Set the static tunnel IP address for the opposite end.	Manually enter in the input box Format: X X. X.X
Disable EAP	Do not use EAP certification.	Dropdown list selection ● yes ● no

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Disable CHAPs	Do not use CHAP authentication.	Dropdown list selection ● yes ● no
Disable PAP	Do not use PAP authentication.	Dropdown list selection ● yes ● no
Disable MS-CHAP	Do not use MS-CHAP certification.	Dropdown list selection ● yes ● no
Disable MS2 CHAP	Do not use MS2 CHAP authentication.	Dropdown list selection ● yes ● no
LCP interval time (seconds)	The time interval for sending LCP packet requests.	Manually entering numerical values
LCP retry count	Send LCP packet request timeout retry count.	Manually entering numerical values
Enable MPPE	Enable Microsoft peer-to-peer encryption protocol.	Dropdown list selection ● yes ● no
Enable stateless MPPE	Stateless MPPE, configured when MPPE is enabled.	Dropdown list selection ● yes ● no
Enable MPPE40	MPPE 40 bit encryption, configured when MPPE is enabled.	Dropdown list selection ● yes ● no
Enable MPPE128	MPPE 128 bit encryption, configured when MPPE is enabled.	Dropdown list selection ● yes ● no

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

4.1.1 L2TP Server Function Configuration

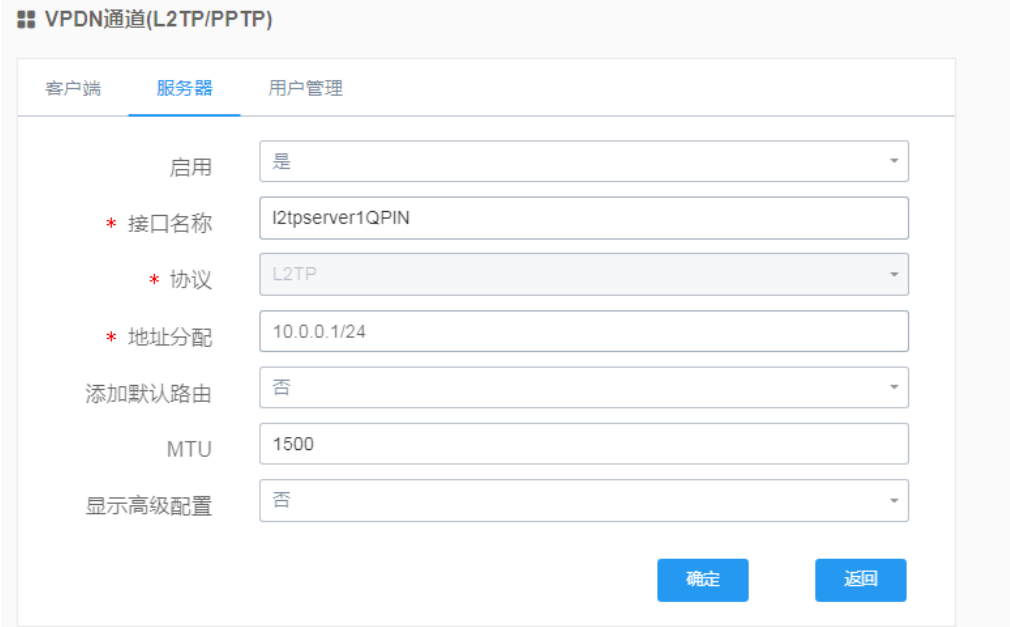
background information

L2TP servers are deployed at the enterprise headquarters and typically serve as gateways for the enterprise headquarters. The L2TP server receives user information transmitted by the L2TP client, verifies the identity of the accessed user, responds to L2TP tunnel connection requests initiated by the L2TP client, and jointly establishes an L2TP connection with the L2TP client.

Operation steps

Step 1 After logging into the WEB configuration page, click "VPN Settings>L2TP/PPTP Settings". The parameter description of the VPDN channel list is shown in Table 4-1.





Copyright © 3onedata Co., Ltd.

Table 34-1 L2TP Server Configuration List Parameter Description3-4

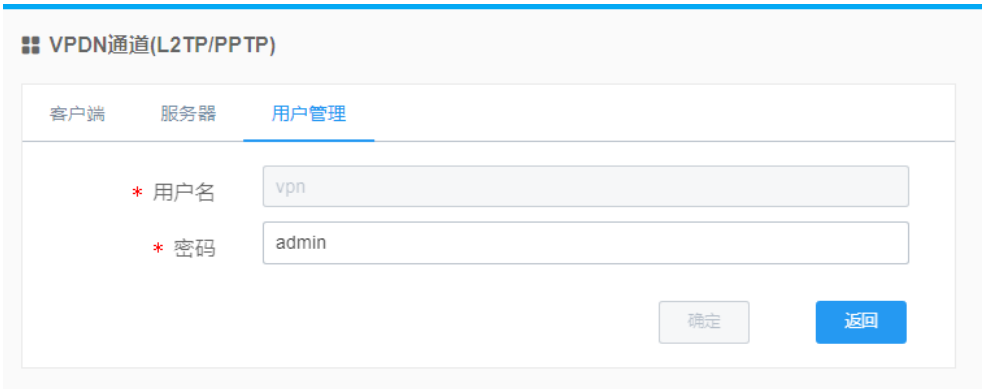
Parameter Name	explain
Enable	Dropdown list selection ● yes ● no
Interface Name	The name of the VPDN rule.
protocol	L2TP
Address allocation	Set the private IP address and address pool for the L2TP server. The gateway IP serves as the gateway address for L2TP clients, and the subnet mask determines the IP address resources dynamically allocated to L2TP clients.
Add default route	Dropdown list selection ● yes ● no
MTU	Set maximum transmission unit and manually input values The default value is 1500

Step 2 The parameter description of the user management configuration table is shown in Table 4-1-2.



Copyright © 3onedata Co., Ltd.

Table 35-1 L2TP username configuration list parameter description Table 4-1-3 shows3-5



Parameter Name	explain
user name	The username of the remote dial-up user.
password	Password for remote dial-up users

Step 3 Click "OK" to complete the L2TP server configuration.

——End

3.2 N2N_ V2 configuration

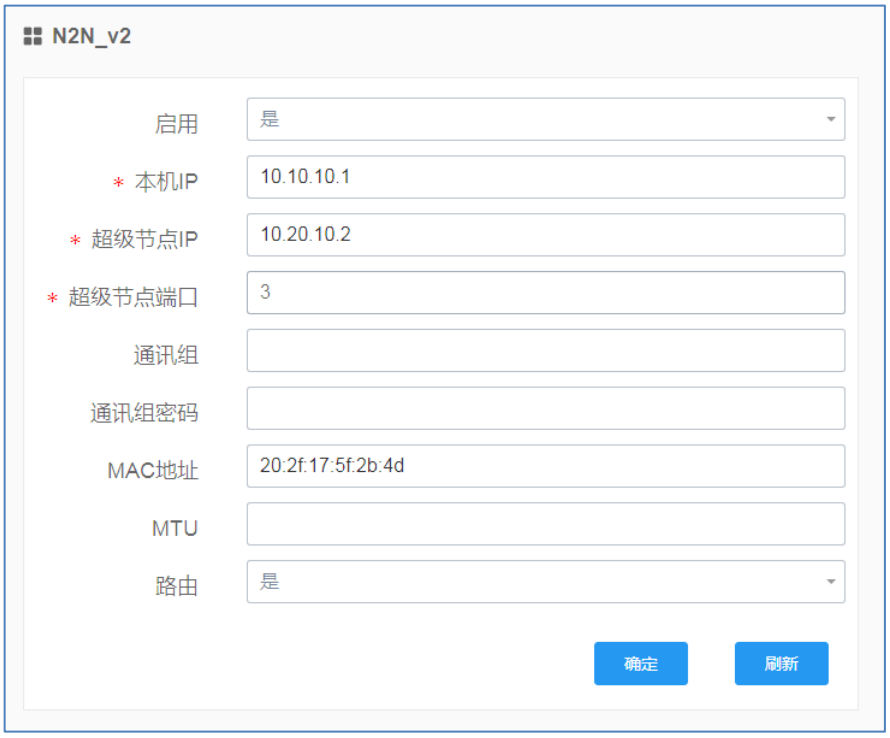
background information

N2N aims to provide decentralized, unmanaged, secure, and stable network connectivity, regardless of the user's location, IP address, and network type. Simply put, it means no need for a public IP, no need to configure NAT, and no need to penetrate firewalls.

Operation steps

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

Copyright © 3onedata Co., Ltd.



Step 2 Configure N2N_ The v2 parameter is described in Table 4-4.

Table 36 N2N_ V2 parameter description3-6

Parameter Name	explain	Configuration method
Enable	Whether to use N2N_ V2 connection.	Dropdown list selection ● yes ● no
Local IP	Set an internal IP address.	Manually enter in the input box Format: X X. X.X
Super node IP	Connect the IP of the super node.	Manually enter in the input box Format: X X. X.X
Super node port	Connect the port of the super node.	Value range: 0~65535
Distribution group	The name of the N2N communication organization.	Fill in the name characters of the distribution group

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Distribution group password	The password used by the distribution group.	Fill in the legal access password for accessing the distribution group authorization
MAC address	The physical address of the interface of the N2N node.	Normally not modified, manually modified for special needs, format: XX: XX: XX: XX: XX: XX
MTU	Maximum data transmission unit. Default: 1500.	Manually entering numerical values
route	Add a default route for the N2N interface.	Dropdown list selection ● yes ● no

Step 3 Click "OK" to complete N2N_ Configuration of v2.

——**End**

3.3 OPENVPN

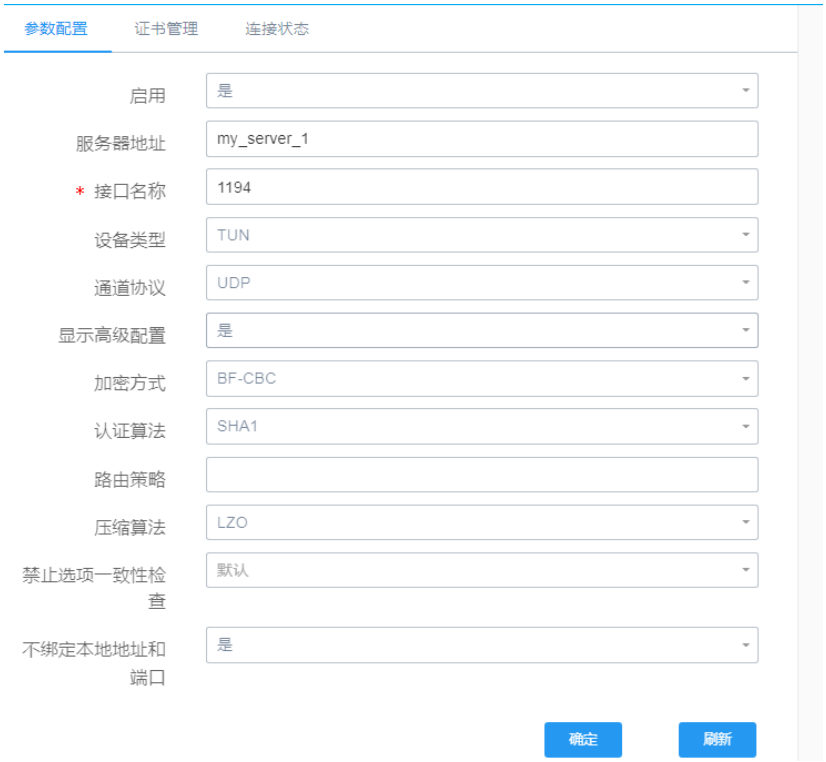
background information

All communication in OPENVPN is based on a single IP port, and UDP protocol communication is recommended by default, while also supporting TCP. The official port assigned by IANA (Internet Assigned Numbers Authority) to OPENVPN is 1194. In OPENVPN, if a user accesses a remote virtual address (belonging to the address family used by the virtual network card, different from the real address), the operating system will send data packets (TUN mode) or data frames (TAP mode) to the virtual network card through a routing mechanism. After receiving the data and processing it, the service program will send it out from the external network through SOCKET. This completes a one-way transmission process, and vice versa. When the remote service program receives data from the external network through SOCKET, performs corresponding processing, and then sends it back to the virtual network card, the application software can receive it.

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

Operation steps

Step 1 After logging into the WEB configuration page, click "VPN Settings>OPENVPN" to open the "OPENVPN" tab.



Step 2 Configure OPENVPN parameters, as shown in Table 4-5.

Table 37 OPENVPN Parameter Description3-7

Parameter Name	explain	Configuration method
Enable	Whether to use OPENVPN connection.	Dropdown list selection ● yes ● no
server address	The domain name of the peer IP address or remote OPENVPN server.	Manual input
Interface Name	The port of the server.	Value range: 0~65535
Equipment type	Channel device type.	Dropdown list selection ● TUP ● TAP

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Channel Protocol	Channel protocol, selected according to application requirements.	Dropdown list selection ● UDP ● TCP
Routing strategy	The current routing strategy being used.	Manual input
Using LZO compression	Whether to use LZO compression algorithm.	Dropdown list selection ● YES ● NO
Encryption method	Is data encryption required	Dropdown list selection ● BF-CBC ● RC2-40-CBC ● CACT5-CBC ● RC2-64-CBC .....
Authentication algorithm	Is data encryption required	Dropdown list selection ● SHA1 ● RSA-MD5 ● MD5 .....
Prohibit option consistency check	Do not use option consistency check.	Dropdown list selection ● yes ● no
Unbind local address and port	Do not bind local addresses and ports.	Dropdown list selection ● yes ● no

Step 3 Configure certificate management configuration parameters, as shown in Table 4-6.

Copyright © 3onedata Co., Ltd.



Table 38 Description of Advanced Configuration Parameters for OPENVPN3-8

Parameter Name	explain	Configuration method
Certified CA certificate	CA certificate.	Select Upload Delete uploaded certificate Update uploaded certificates
TA certificate	TA certificate.	Select Upload Delete uploaded certificate Update uploaded certificates
Local certificate	Local certificate.	Select Upload Delete uploaded certificate Update uploaded certificates
Local private key	Local key.	Select Upload Delete uploaded certificate Update uploaded certificates

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

——**End**

Copyright © 3onedata Co., Ltd.

3.4 IPSEC

background information

IPSec VPN refers to a VPN technology that uses the IPSec protocol to achieve remote access. IPSec, also known as Internet Protocol Security, is a security standard framework defined by the Internet Engineering Task Force (IETF) to provide end-to-end encryption and authentication services for public and private networks. IPSEC is a relatively complete and systematic VPN technology that specifies a series of protocol standards.

Operation steps

Step 1 After logging into the WEB configuration page, click "VPN Settings>IPSEC" to open the "IPSEC" tab.



Copyright © 3onedata Co., Ltd.



Step 2 Configure IPSEC parameters, as shown in Table 4-7.

Table 39 IPSEC parameter description3-9

Parameter Name	explain	Configuration method
Enable	Whether to use IPSEC function.	Dropdown list selection yes no
Negotiation mode	Choose IKE's negotiation mode. If the IP address at one end of the IPSEC tunnel is automatically obtained.	Dropdown list selection Active mode aggressive mode
Start mode		Dropdown list selection automatic trigger Add

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Opposite address	Set the peer IP address or domain name.	Just fill in the IP address or domain name of the peer address
IKE authentication mode	Choose the authentication mode negotiated by IKE.	Dropdown list selection ● IKE-PSK ● IKE-PSK-XAUTH
Encapsulation mode	Select data packet encapsulation format	Dropdown list selection ● tunnel mode ● transmission mode
Shared Key	The key used.	Manual input, with a maximum length of 64 bit WORD string. Please refer to "" for input specifications
Local subnet	Enter the local subnet address and mask included in IPSEC.	Interface type A B. C.D/M, please refer to "" for input specifications
Terminal network	Enter the terminal network address and mask contained in IPSEC.	Interface type A B. C.D/M, please refer to "" for input specifications
Local identification	Local address identification.	Manual input
Opposite identification	Opposite address identification.	Manual input
Enable PDP detection	Is PDP testing used.	Dropdown list selection ● yes ● no

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
PDP action	PDP heartbeat selection	Dropdown list selection ● clean up ● keep ● Reconnection
Detection interval (seconds)	PDP detection time interval	Manually entering numerical values
Exceeding the time limit	Detection exceeded the time limit.	Manually entering numerical values
Encryption method	Choose the encryption method for the first stage.	Dropdown list selection ● AES128 ● AES192 ● AES256 ● 3des ● Des
Hash algorithm	Choose a hash algorithm.	Dropdown list selection ● Md5 ● Sha1 ● Sha256 ● Sha384 ● Sha512
DH group	Select DH grouping for IKE negotiation.	Dropdown list selection ● Group 1 (768) ● Group 2 (1024) ● Group 5 (1536) ● Group 14 (2048) ● ● Group 18 (8192)

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

Parameter Name	explain	Configuration method
IKE lifecycle	Set the survival time in IKE negotiation. Before the SA expires, IKE negotiates a new SA; Once a new SA is established, it will take effect immediately; The old one will be cleared immediately after expiration.	Manually entering numerical values

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

——**End**

3.5 GRE

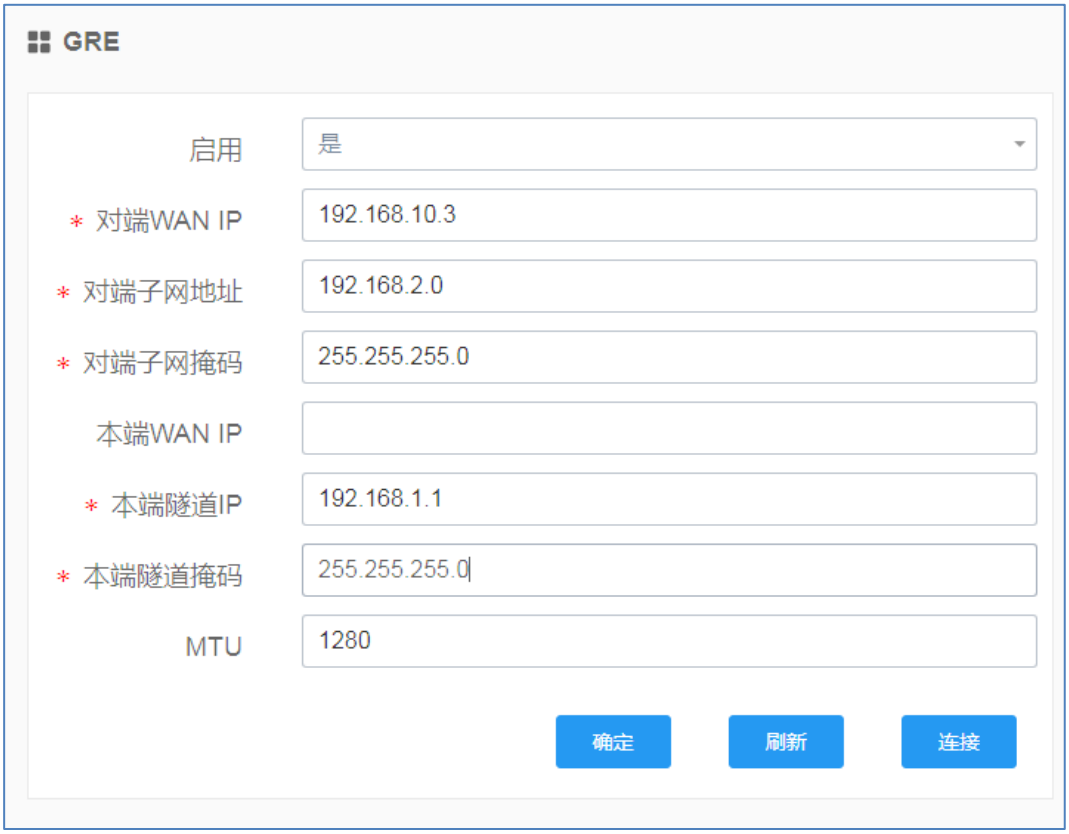
background information

GRE VPN (General Routing Encapsulation), also known as General Routing Encapsulation Protocol, encapsulates datagrams of certain network layer protocols (such as IP and IPX), allowing these encapsulated datagrams to be transmitted in another network layer protocol (such as IP). GRE is the third layer tunneling protocol of VPN (Virtual Private Network), which uses a technology called Tunnel between protocol layers.

Operation steps

Step 1 After logging into the WEB configuration page, click "VPN Settings>GRE" to open the "GRE" tab.

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



Step 2 Configure the GRE parameters, as shown in Table 4-8.

Table 310 Description of GRE Parameters3-10

Parameter Name	explain	Configuration method
Enable	Whether to use the GRE function.	Dropdown list selection ● yes ● no
Opposite WAN IP	Set the IP address of the opposite end of the GRE tunnel.	Manually enter in the input box Format: X X. X.X
Terminal network address	Set the subnet address of the peer IP of the GRE tunnel.	Manually enter in the input box Format: X X. X.X
Mask for terminal network	Set the terminal network mask for the GRE tunnel.	Manually enter in the input box Format: X X. X.X

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

Parameter Name	explain	Configuration method
Local WAN IP	Set the local IP address of the GRE tunnel.	Manually enter in the input box Format: X X. X.X
Local tunnel IP	Set the subnet address of the local IP of the GRE tunnel.	Manually enter in the input box Format: X X. X.X
Local tunnel mask	Set the local terminal network mask for the GRE tunnel.	Manually enter in the input box Format: X X. X.X
MTU	Set the maximum transmission unit.	Manually entering numerical values The default value is 1500

Step 3 Click "OK" to complete the configuration of GRE.

3.6 EoIP

background information

EoIP (Ethernet over IP) tunneling is an Ethernet tunneling protocol established between the IP transport layers of two routers. The EoIP interface performs similarly to Ethernet transmission. When the router's bridging function is enabled, all Ethernet data traffic (all Ethernet protocols) will be bridged, that is, the same local area network will cross the IP layer to achieve remote layer 2 network interconnection.

Operation steps

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

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



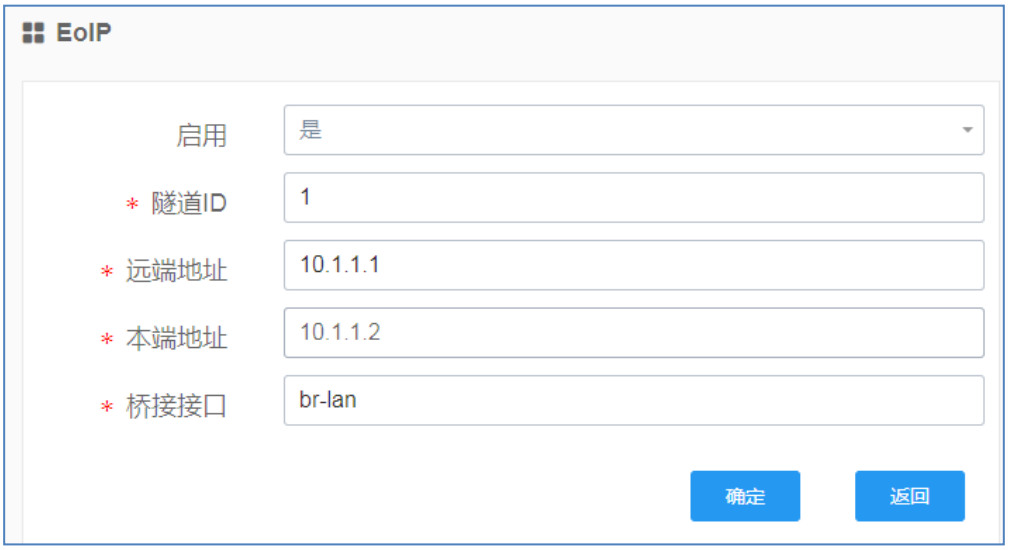
The EOIP list parameters are explained in Table 4-9.

Table 4-9 Explanation of EoIP List Parameters

Parameter Name	explain
Tunnel ID	Display the tunnel ID number for this configuration item.
Bridge interface	Display the interface name bridged by this configuration item.
Remote address	Display the remote address configured for this configuration item.
Local address	Display the local address configured for this configuration item.
Enable	Display whether the configuration item status is enabled.
operation	The configuration item can be edited or deleted.

Step 2 Click "Create" to create a new EoIP tunnel.

Copyright © 3onedata Co., Ltd.



Step 3 Configure EoIP parameters, as shown in Table 4-10.

Table 4-10 EoIP parameter description

Parameter Name	explain	Configuration method
Enable	Whether to use EoIP function.	Dropdown list selection ● yes ● no
Tunnel ID	Set the EoIP tunnel ID number, and the tunnel ID numbers on both ends must be consistent.	Manually enter in the input box Format: X X. X.X
Remote address	Set the WAN IP address of the opposite end of the EoIP tunnel.	Manually enter in the input box Format: X X. X.X
Local address	Set the local WAN IP address for the EoIP tunnel.	Manually enter in the input box Format: X X. X.X
Bridge interface	Configure the interface name that needs to be bridged.	Fill in the name of the router network interface that needs to be bridged. The default setting is the br lan interface.

Copyright © 3onedata Co., Ltd.

Step 4 Click "OK" to complete the parameter configuration of the EoIP function.

——**End**

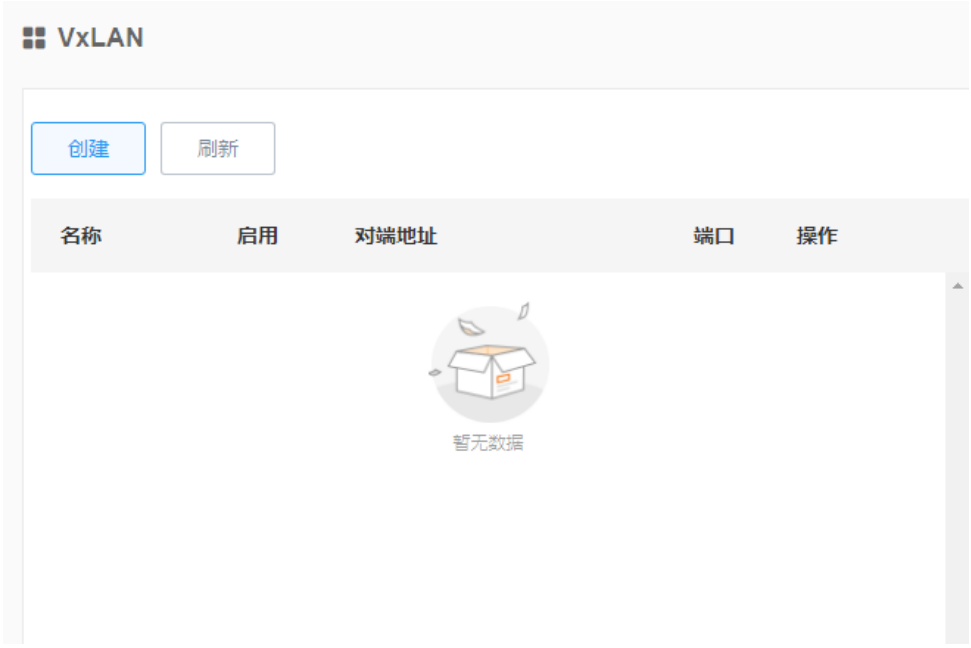
3.7 VXLAN

background information

VXLAN is a network virtualization technology that can improve the scalability of large-scale cloud computing during deployment, and is an extension of VLAN. VXLAN is a powerful tool that can penetrate the third layer network and expand the second layer. It can address the portability limitations of VMS (Virtual Memory System) by encapsulating traffic and extending it to the third layer gateway, allowing it to access servers on external IP subnets

Operation steps

Step 1 After logging into the WEB configuration page, click "VPN Settings>VXLAN" to open the "VXLAN" tab. The parameter description of VXLAN list is shown in Table 4-11.



Step 2 Click "Create" to create a new VXLAN tunnel.

Copyright © 3onedata Co., Ltd.



Step 3 Configure VXLAN parameters, as shown in Table 4-12.

Table 4-12 VXLAN Parameter Description

Parameter Name	explain	Configuration method
Enable	Whether to use VXLAN function.	Dropdown list selection ● yes ● no
Interface Name	The name of this VXLAN rule	custom
Opposite address	Set the peer IP address or domain name.	Just fill in the IP address or domain name of the peer address
port	Connection port	4789 by default
VID	Display the ID number of the configuration item.	Value range: 0~16777215
MTU	Maximum transmission unit	Manual configuration
NAT	address translation	Dropdown list selection ● yes ● no

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

Parameter Name	explain	Configuration method
Bridge interface	nothing	Default LAN

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

4 Forwarding configuration

4.1 NAT

Operation steps

Step 1 After logging into the WEB configuration page, click "Forwarding Settings>NAT" to open the "NAT" tab. The NAT list parameter description is shown in Table 5-1.



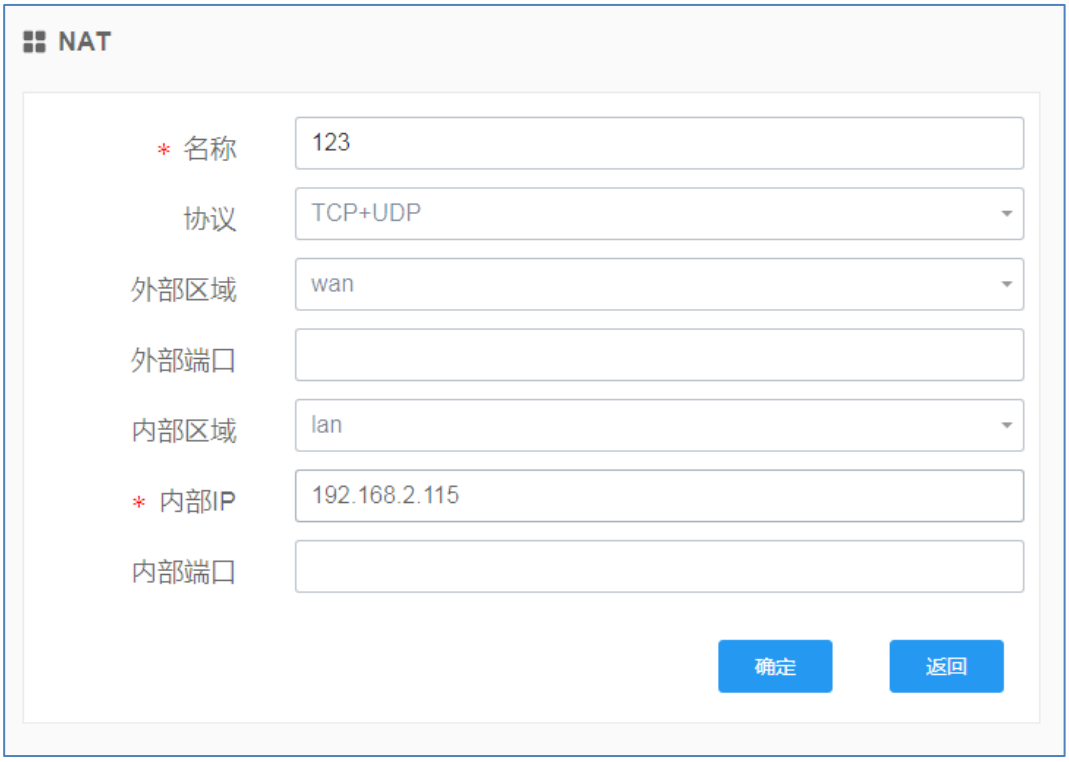
Table 41 NAT List Parameter Description4-1

Parameter Name	explain
name	NAT rule name.
protocol	The protocol used for address translation packets.
External area	External network.
External port	The port used by the external network.
Internal area	Internal network.
Internal IP	The IP address of the internal network.

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
Internal port	The port used by the internal network.
operation	Can perform "edit" and "delete" operations on NAT rules.

Step 2 Click "Create" to create a new NAT rule.



Configure NAT rule parameters, as shown in Table 5-2.

Table 42 NAT Parameter Description4-2

Parameter Name	explain	Configuration method
name	Set the NAT rule name.	Alphanumeric WORD entry, please refer to "" for input specifications
protocol	For which protocol of data packet to perform destination address translation.	Dropdown list selection ● TCP+UDP ● TCP ● UDP

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
External area	External network.	Dropdown list selection ● Wan
External port	The port used by the external network.	Value range: 1~65535 or [1~65535], which can be a range or a single port
Internal area	Internal network.	Dropdown list selection ● Lan
Internal IP	The IP address of the internal network.	Manually enter in the input box Format: X X. X.X
Internal port	The port used by the internal network.	Value range: 1~65535 or [1~65535], which can be a range or a single port

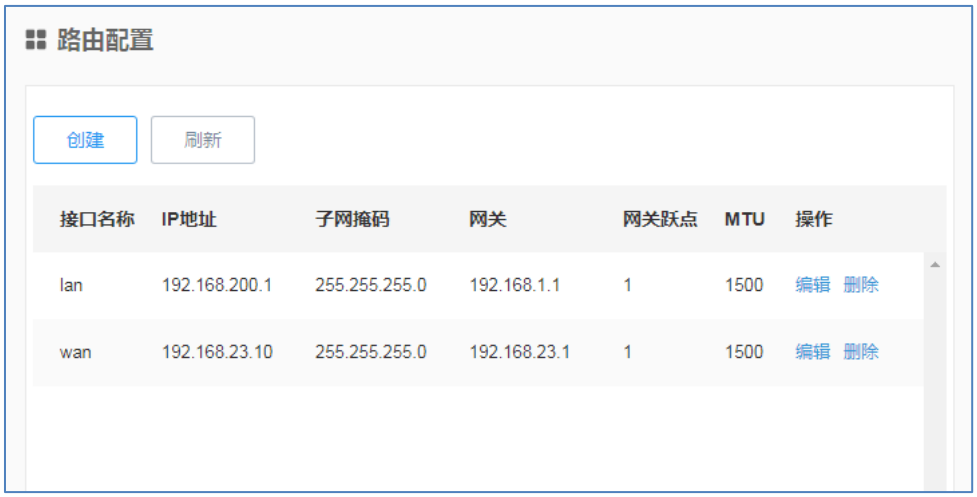
Step 3 Click "OK" to complete the NAT rule configuration.

——**End**

4.2 Routing configuration

Operation steps

Step 1 After logging into the WEB configuration page, click "Forwarding Settings>Routing Configuration" to open the "Routing Configuration" tab. The routing list parameters are explained in Table 5-3.



Copyright © 3onedata Co., Ltd.

Table 43 Description of Routing Configuration List Parameters4-3

Parameter Name	explain
Interface Name	The name of the routing interface.
IP address	The IP address of the destination host or destination network for routing rules.
Subnet Mask	The subnet mask of the routing destination host or destination network.
gateway	The IP address of the routing rule gateway.
Gateway Hop	Gateway metric.
MTU	Maximum transmission unit.
operation	Can perform "edit" and "delete" operations on scheduled tasks.

Step 2 Click "Create" to create a new routing rule.



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

Table 44 Description of Routing Configuration Parameters4-4

Parameter Name	explain	Configuration method

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Interface Name	The name of the routing interface.	Dropdown list selection ● Gretunnel ● Gretunnel_ Static ● Lan ● N2n ● Open_ VPN1 ● Open_ VPN2 ● Wan ● Wwan
IP address	Enter the IP address of the destination host or destination network.	Manually enter in the input box Format: X X. X.X
Subnet Mask	Enter the subnet mask of the destination host or destination network.	Manually enter in the input box Format: 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 data that matches the destination address and subnet mask to the gateway.	Manually enter in the input box Format: X X. X.X
Gateway Hop	Gateway metric.	Manually entering numerical values
MTU	Set the maximum transmission unit.	Manually entering numerical values

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

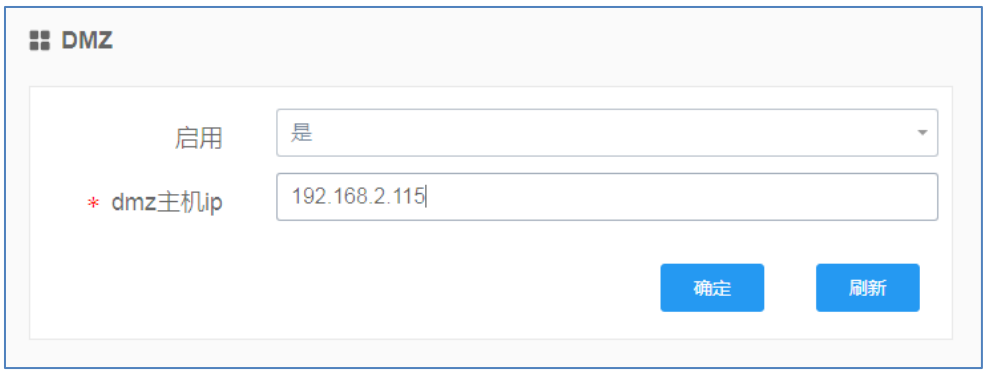
——**End**

Copyright © 3onedata Co., Ltd.

4.3 DMZ

Operation steps

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



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

Table 45 DMZ Configuration Parameter Description4-5

Parameter Name	explain	Configuration method
Enable	Whether to use DMZ function.	Dropdown list selection ● yes ● no
DMZ host IP	The IP address of the DMZ host.	Manually enter in the input box Format: X X. X.X

Step 3 Click "OK" to complete the DMZ configuration.

——**End**

Copyright © 3onedata Co., Ltd.

4.4 OSPF configuration

Operation steps

Step 1 After logging into the WEB configuration page, click "Forwarding Settings>OSPF" to open the "OSPF" tab.



Step 2 Configure OSPF parameters, as shown in Table 5-6.

Table 46 OSPF Configuration Parameter Description4-6

Parameter Name	explain	Configuration method
Enable	Whether to use OSPF function.	Dropdown list selection ● yes ● no
Routing ID	Routing local identifier	Format: XXX XXX XXX XXX
SPF calculation interval	Set the delay time for SPF calculation	0-255 (seconds)

Step 3 The parameter description of the regional configuration list is shown in Table 5-7.



Copyright © 3onedata Co., Ltd.

Table 47 OSPF Configuration Parameter Description4-

Parameter Name	explain
Region ID	Set OSPF area ID number 0 as the backbone area and the others as the regular area

Step 4 The network configuration parameters are explained in Table 5-8.

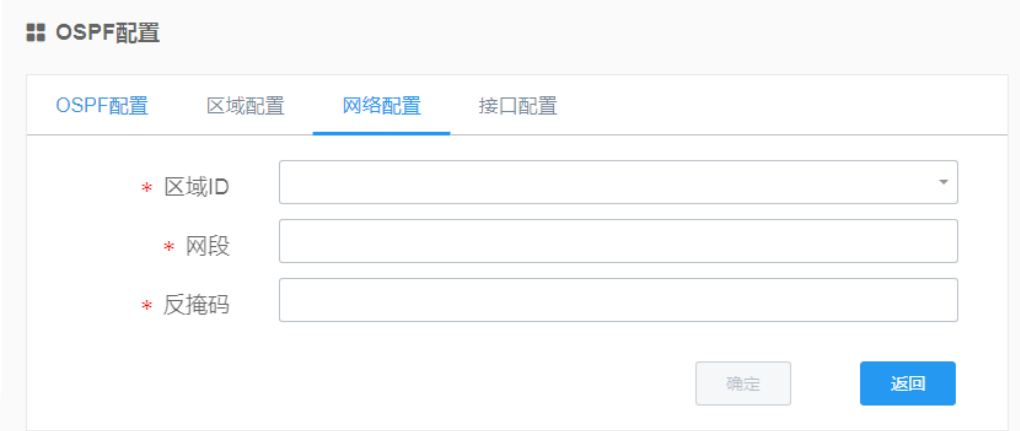


Table 49 Network Configuration Parameter Description4-

Parameter Name	explain
Region ID	Set OSPF area ID number 0 as the backbone area and the others as the regular area
Network segment	Declare all interface network segment addresses for routing
Anti mask	Wildcard mask such as 0.0.0.255

Step 5 The interface configuration parameters are explained in Table 5-10.

Copyright © 3onedata Co., Ltd.



Table 411 Network Configuration Parameter Description4-

Parameter Name	explain
Interface Name	The output interface is not optional
Interface overhead	Legal value: 0-65535
Certification type	Users can choose between simple authentication and MD5 to set the authentication mode used in the OSPF area. If simple authentication mode is selected, it is also necessary to configure a simple authentication password and confirm the password again. If you choose MD5 authentication mode, you also need to configure the 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 for sending Hello messages. If the Hello intervals between adjacent routers are different, a neighbor relationship cannot be established. Legal values: 1-65535
Retransmission time interval (seconds)	Must be greater than 0, must be within 3601

Step 1 Click "OK" to complete the OSPF configuration.

——**End**

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

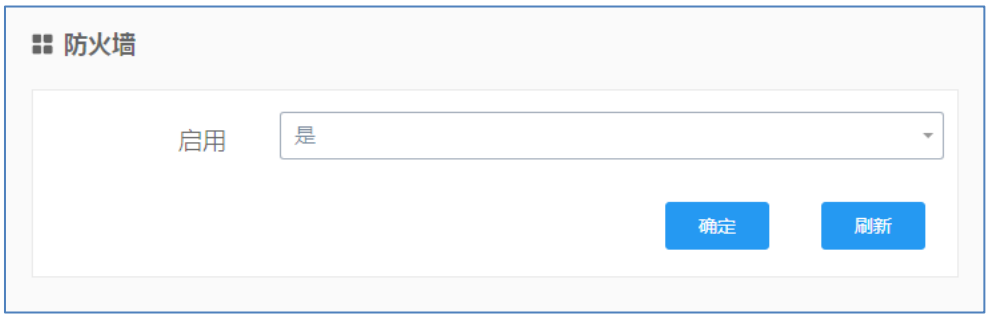
5 Security configuration

Security settings are the firewall function of a router. By analyzing the IP address/MAC address of data packets entering the router, comparing it with the firewall rules added by the user, and performing receive or discard actions on data packets that match the corresponding firewall rules, users can achieve secure access. Sanwang Industrial grade wireless routers support IP filtering and MAC filtering security settings. Users can set security rules to allow/prohibit certain network segments from accessing the external network, and allow/prohibit other users from accessing the router.

5.1 firewall

Operation steps

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



Step 2 Configure firewall parameters, as shown in Table 6-1.

Table 51 Description of firewall configuration parameters5-1

Parameter Name	explain	Configuration method

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Enable	Choose whether to enable the firewall.	Dropdown list selection ● yes ● no

Step 3 Click "OK" to complete the firewall configuration.

——**End**

5.2 IP filtering

background information

IP filtering refers to the use of filtering rules by routers to determine whether external devices are allowed to access the router and whether data packets are allowed to be forwarded through the router, thereby achieving management of router devices and internet behavior management of local area network devices. IP filtering is usually used to allow only a certain group of hosts to access the external network or to prohibit a certain group of hosts from accessing a specific network.

Operation steps

Step 2 After logging into the WEB configuration page, click "Security Settings>IP Filtering" to open the "IP Filtering" tab. The IP filtering list parameters are explained in Table 6-2.



Table 52 IP Filter List Parameter Description5-2

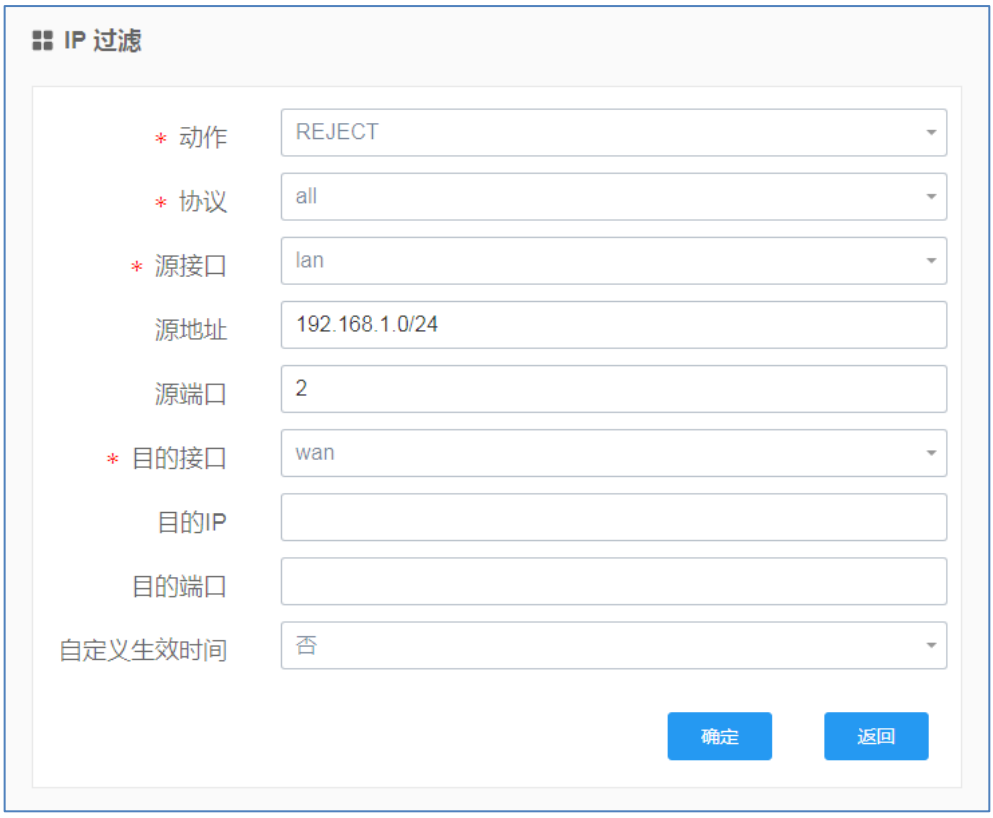
Parameter Name	explain

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
Filter type	Dropdown list selection ● Whitelist ● Blacklist ● custom
action	The filtering rules for access.
protocol	The protocol used for accessing.
source address	Specify the source address for accessing the source.
Source Port	Specify the source port for accessing the source.
Destination IP	The target address to be accessed by accessing the source.
Destination Port	The target port to be accessed by accessing the source.
time	Customize the effective time.
operation	You can edit or delete IP filtering rules.

Step 3 Click "Create" to create a new IP filtering rule.

Copyright © 3onedata Co., Ltd.



Configure IP filtering parameters, as shown in Table 6-3.

Table 53 IP filtering parameters5-3

Parameter Name	explain	Configuration method
action	Select the filtering rules for access.	Radio box selection ● ACCESS ● PROJECT ● DROP
protocol	Choose the protocol used for access. If unsure of the current access protocol, it is recommended to choose "all".	Dropdown list selection ● TCP ● Udp ● Tcpudp ● All
Source interface	Specify the interface for accessing the source.	Dropdown list selection ● Wan ● Lan
source address	Specify the source address for accessing the source.	Manually enter IP address, subnet segment, or specified IP range

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Source Port	Specify the source port for accessing the source.	Value range: 1-65535 or [1-65535]; It can be a range or a single port
Destination interface	Specify the router interface for IP packet access.	Dropdown list selection ● Wan ● Lan
Destination IP	The target address to be accessed by accessing the source can be an IP device connected to the router.	Manually enter IP address, subnet segment, or specified IP range
Destination Port	The target port to access the source can be an IP device connected to the router.	Value range: 1-65535 or [1-65535]; It can be a range or a single port
Custom effective time	Do you want to customize the effective time.	Dropdown list selection ● yes ● no

Step 4 Click "OK" to complete the configuration of the IP filtering rule.

——**End**

5.3 MAC filtering

background information

MAC filtering is commonly used to control host access to routers, using whitelists to allow only hosts with specific MAC addresses to manage and access routers. In addition to implementing this function, the Sanwang industrial grade wireless router can also restrict the external network access permissions of specific MAC hosts, or only allow specific MAC hosts to access the external network.

Operation steps

Step 1 After logging into the WEB configuration page, click "Security Settings>MAC Filtering" to open the "MAC Filtering" tab. The MAC filter list parameters are explained in Table 6-4

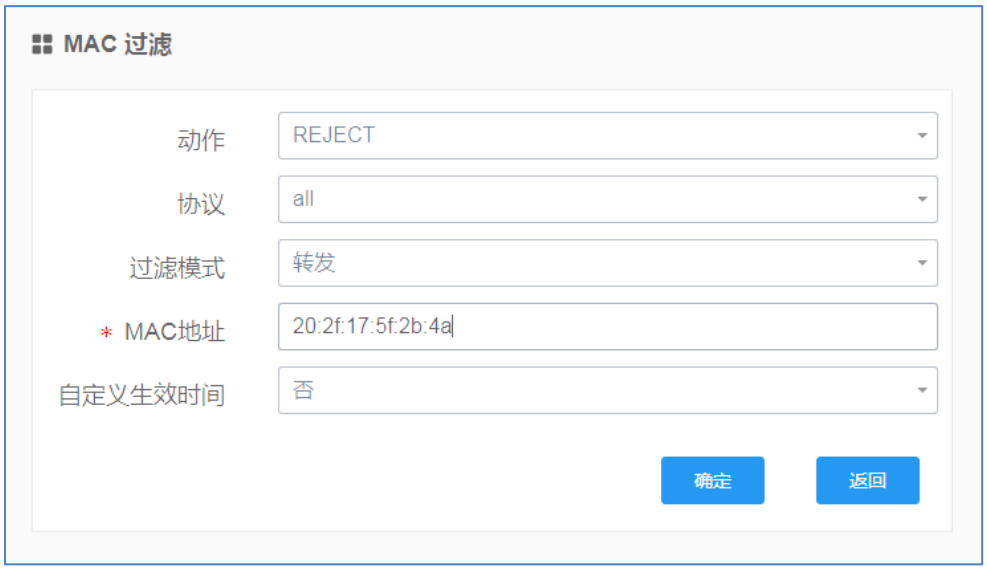
Copyright © 3onedata Co., Ltd.



Table 54 MAC Filter List Parameter Description5-4

Parameter Name	explain
action	The filtering rules for access.
protocol	The protocol used for accessing.
Filtering mode	MAC filtering mode.
MAC address	MAC addresses that need to be filtered.
time	Customize the effective time.
operation	You can edit or delete IP filtering rules.

Step 2 Click "Create" to create a new MAC filtering rule.



Step 3 Configure MAC filtering parameters, as shown in Table 6-5.

Table 55 MAC filtering parameters5-5

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
action	Select the filtering rules for access.	Dropdown list selection ● ACCESS ● PROJECT ● DROP
protocol	Choose the protocol used for access. If unsure of the current access protocol, it is recommended to choose "all".	Dropdown list selection ● TCP ● UDP ● TCPUDP ● ALL
Filtering mode	The filtering mode of this rule.	Dropdown list selection ● transmit ● input
MAC address	MAC addresses that need to be filtered.	WORD type MAC format: XX: XX: XX: XX: XX: XX: XX input, please refer to ""
Custom effective time	Do you want to customize the effective time.	Dropdown list selection ● yes ● no

Step 4 Click "OK" to complete the configuration of the MAC filtering rule.

5.4 Domain name filtering

background information

The domain name filtering function can set access restrictions on websites, and specific filtering rules can be set through the black and white list function to achieve a safe and reliable domain name access environment.

Copyright © 3onedata Co., Ltd.

Operation steps

Step 1 After logging into the WEB configuration page, click "Security Settings>Domain Name Filtering" to open the "Domain Name Filtering" tab. The description of domain name filter list parameters is shown in Table 6-6.



Table 56 Domain name filtering parameters5-

Parameter Name	explain
Enable	Choose whether to enable domain name filtering. Dropdown list selection ● yes ● no
Filter type	Select the filtering type. Dropdown list selection ● Blacklist ● Whitelist
name	Display the name of the domain name filtering configuration item.

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
domain name	Display the filtered domain names for the current configuration item.
Enable filtering	Display whether the configuration item is enabled.
operation	Domain name filtering rules can be edited or deleted.

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



Step 3 Configure domain name filtering parameters, as shown in Table 6-7.

Table 57 Domain name filtering parameters5-

Parameter Name	explain	Configuration method
name	Custom rule name.	No more than 32 arbitrary characters
domain name	Fill in the first level domain name that needs to be filtered.	Fill in a valid domain name without the need to fill in the www prefix, otherwise it will affect the filtering effect. Fill in a domain name that does not exceed 32 characters.

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Enable filtering	Choose whether to enable the filtering rule.	Dropdown list selection ● yes ● no

Step 4 Click "OK" to return to the "Domain Name Filtering" tab.

Step 5 Select "Filter Type" according to your needs. If "blacklist" is selected, access to the filtering rule's domain name is prohibited; If "whitelist" is selected, only domain names with filtering rules can be accessed, and access to other domains is prohibited.

——**End**

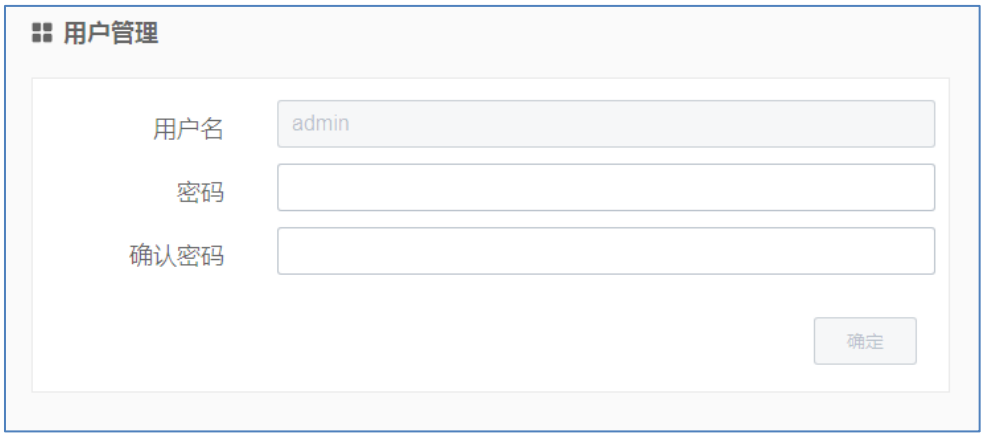
Copyright © 3onedata Co., Ltd.

6 system configuration

6.1 user management

Operation steps

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



Step 2 Configure user management parameters, as shown in Table 7-1.

Table 61 User Management Parameters6-1

Parameter Name	explain	Configuration method
password	The user's modified password.	Manually input a Word string with a maximum length of 32 bits. Please refer to "" for input specificationsParameter specification table

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Confirm password	Confirm the password after the user changes it.	Manually input a Word string with a maximum length of 32 bits. Please refer to "" for input specificationsParameter specification table

Step 3 After completing the modification, click "OK". After successful saving, the page will automatically redirect to the login interface. Users need to enter the modified username/password to enter.

——**End**

explain

Some models or firmware versions have changed the "System Configuration" - "User Management" function to "User Management" in the root directory of the function menu.

6.2 configuration management

Operation steps

Step 1 After logging into the WEB configuration page, click "System Configuration>Configuration Management" to open the "Configuration



Step 2 Backup/Recovery" tab.

Copyright © 3onedata Co., Ltd.

Step 3 Click "Download Configuration" to export the configuration file to the local area and achieve the backup function of files/parameters.

Step 4 Click "Restore Factory Default" to restore the factory configuration.

take care

Restoring the factory configuration will clear all current configurations.

Step 5 Click "Select", browse the local configuration file that needs to be imported, and click "Update" to complete the file import. If there is an error or file loss in the router parameters, the "import" function can be used to restore the parameters.

——**End**

explain

After importing the backup file, the system automatically restarts and takes effect only after restarting the system.

6.3 Firmware update

background information

The router supports upgrading system files through local network methods. Before upgrading, please ensure that you have obtained the target file for the system update and store the updated file on a computer on the local area network.

Operation steps

Step 1 After logging into the WEB configuration page, click "System Configuration>Firmware Upgrade" to open the "Firmware Upgrade" tab.



Copyright © 3onedata Co., Ltd.

explain

Select the "Keep Configuration" checkbox to keep the parameters set by the user on the page. It is not recommended to close the page when upgrading files. After the upgrade is completed, the page will automatically redirect. If it is a remote upgrade, after upgrading the file, the router modem will redial and obtain a new IP address. At this time, the page will not automatically jump due to incorrect IP address.

Step 2 Click "Select", browse the local file to select the firmware file that needs to be updated, and click "Update" to start the system upgrade.

——**End**

take care

During the upgrade process, please ensure that the router is powered on normally; If the router loses power, the upgrade will fail

explain

After the upgrade is completed, please clear the browser cache before opening the router configuration page.

6.4 APP installation

Operation steps

Step 1 After logging into the WEB configuration page, click "System Configuration>APP Installation" to open the "APP Installation" tab. The parameter description of the APP installation list is shown in Table 7-2.

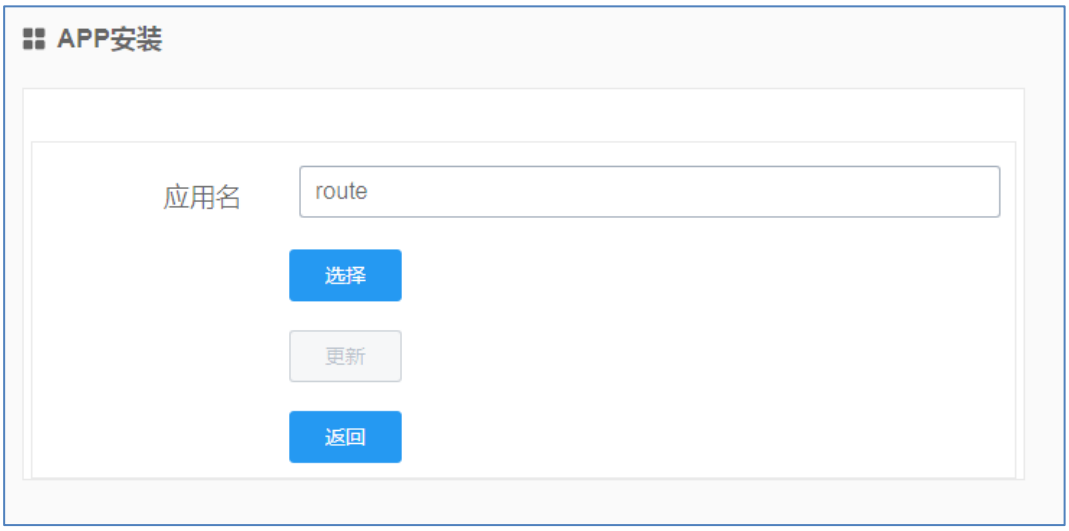


Table 62 APP Installation List Parameter Description6-2

Parameter Name	explain

Parameter Name	explain
Application Name	The name of the installed app.
Version number	The version number of the installed APP.
operation	You can edit or 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", and start installing the APP.

——**End**

explain

Some models and firmware versions have renamed "APP installation" to "Application installation", which only supports the installation of IPK format programs.

6.5 system time

Operation steps

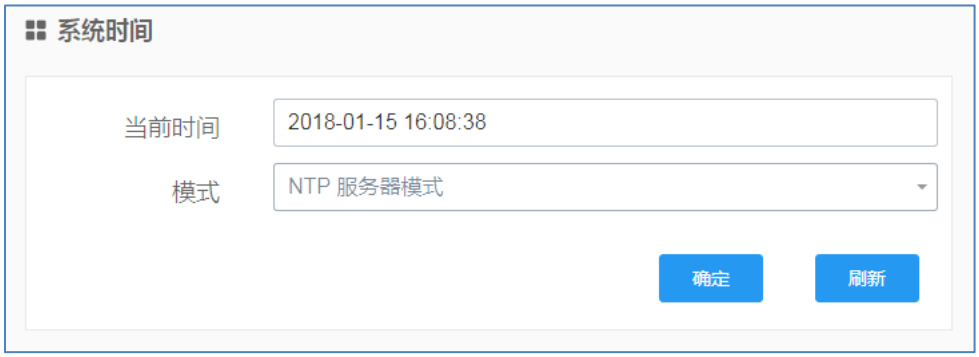
Step 1 After logging into the WEB configuration page, click "System Configuration>System Time" to open the "System Time" tab.

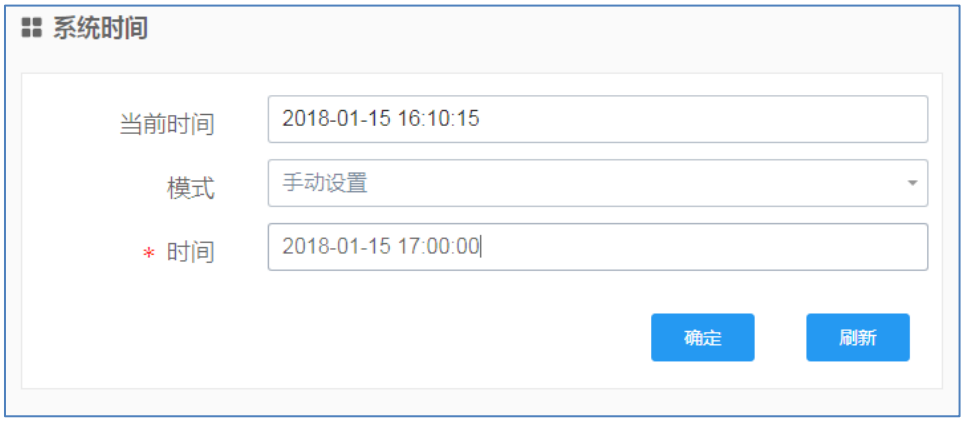
Mode selection "NTP client mode"

Copyright © 3onedata Co., Ltd.



Mode selection "NTP server mode"





Mode selection "Manual settings"

Step 2 Configure the system time, and the parameter specifications are shown in Table 7-3.

Table 63 Explanation of System Time Parameters6-3

Parameter Name	explain	Configuration method

Parameter Name	explain	Configuration method
current time	The current time of the system.	Unconfigurable, automatically generated by the system
mode	Select the system time mode.	Dropdown list selection ● NTP client mode ● NTP server mode ● Manual settings
Display when selecting "NTP client mode" for "mode"		
server address		Manual input
time zone	The current time zone.	Dropdown list selection ● CST-1 ● CST-2 ● ● CST-12
Display when selecting "Manual Settings" in "Mode"		
time	Manually set the time.	Manual input Format: YYYY-MM-DD hh: mm: ss

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

——**End**

6.6 Log management

Operation steps

Step 1 After logging into the WEB configuration page, click "System Configuration>Log Management" to view the router's log information.

Copyright © 3onedata Co., Ltd.



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

Table 64 System Debugging Parameters6-4

Parameter Name	explain
Refresh	View real-time logs on the page
Export system logs	Export historical logs
Export kernel logs	Export Historical Kernel Logs

Step 3 Click "OK" to complete the system debugging configuration.

——**End**

6.7 diagnosis

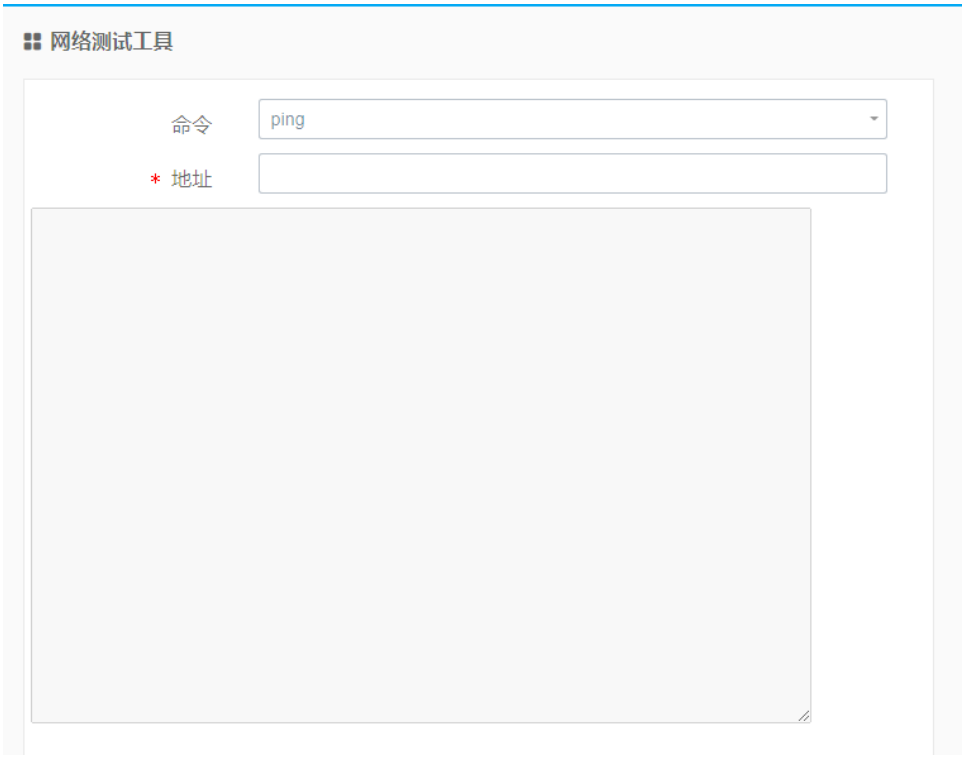
background information

Network testing, including commonly used Ping and Traceroute functions.

Copyright © 3onedata Co., Ltd.

Operation steps

Step 1 After logging into the WEB configuration page, click on "System Configuration>Diagnosis" to open the "Diagnosis" tab



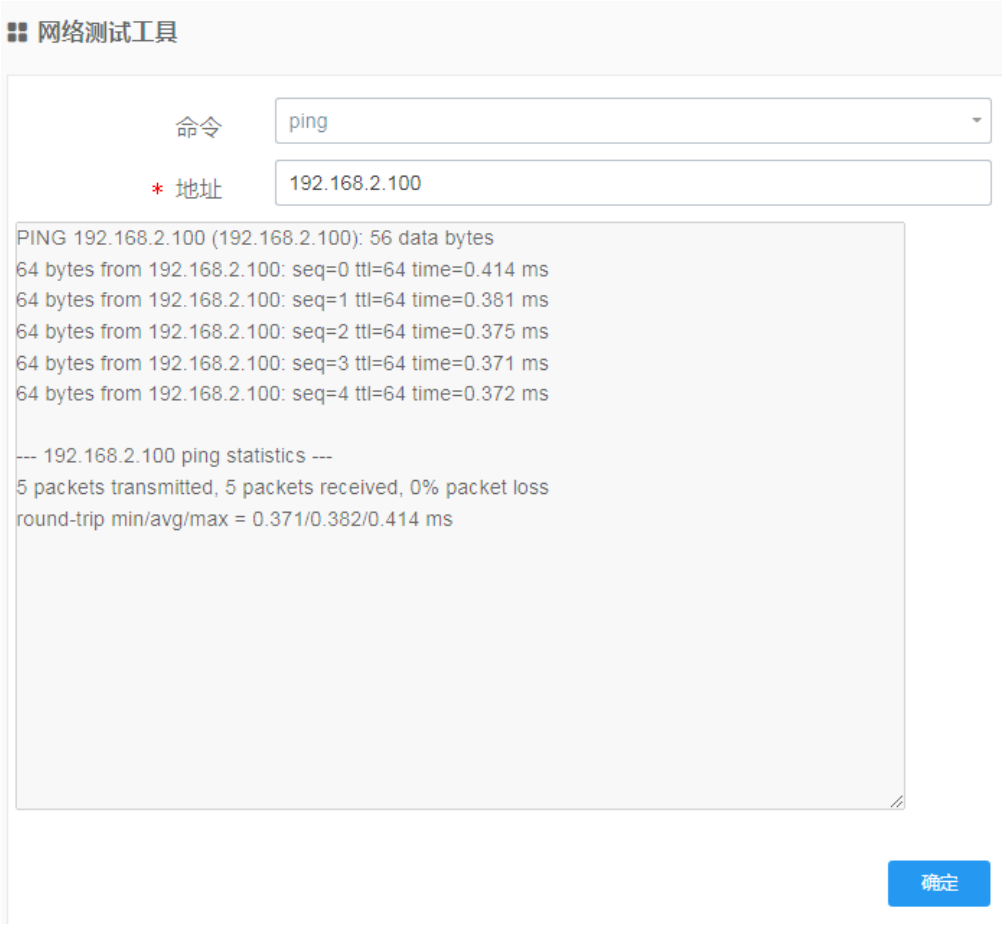
Step 2 Select the command and enter the IP address or domain name to be tested in the "Address" box. The parameter specifications are shown in Table 7-7.

Table 65 Diagnostic Function Parameters6-5

Parameter Name	explain	Configuration method
command	Select the test command.	Dropdown list selection ● Ping: Test network connectivity ● Tracert: Test the number of hops a router reaches its destination address
address	Set the destination IP address or domain name for testing.	Fill in the IP address or domain name of the destination address to be used for testing

Copyright © 3onedata Co., Ltd.

Step 3 Click "OK" to view the results in the box below.



——**End**

explain

Tracert: also known as traceroute, through which we can know the path that information takes from your computer to the host on the other end of the Internet; Measure how long it takes to send small packets to the destination device until they return. Each device Traceroute on a path needs to be tested three times. The output results include the time (ms) of each test, the name of the device (if any), and its IP address.

6.8 Device cloud network management

background information

The Sanwang industrial grade wireless router system is equipped with a communication function with the M2M platform through the WMMP protocol, which can achieve remote maintenance and management of devices and monitoring and

Copyright © 3onedata Co., Ltd.

management of on-site network status through the platform, such as viewing device information, upgrading patches, upgrading firmware, etc., and checking the network signal strength, latency, traffic, etc. of the devices. Support connecting to the Sanwang Cloud Device Management Platform for remote configuration and router management. Please refer to the "Cloud Device Management Platform User Manual - Official Version 1.0". Support connecting to the Sanwang GoConnect Remote Maintenance Platform for remote connection and access to router mounted devices or lower level machines. Please refer to the "GoConnect Remote Maintenance System User Manual V1.0".

Operation steps

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



Step 2 Configure the cloud network management parameters for the device, as shown in Table 7-8.

Table 68 Description of Cloud Network Management Parameters for Devices6-

Parameter Name	explain	Configuration method
Enable	To use the device cloud network management service, this function needs to be used in conjunction with our network management platform.	Dropdown list selection ● yes ● no

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Cloud server address	The IP address or domain name of the network management platform server.	WORD type, maximum 64 bytes, input specifications refer to ""Parameter specification table
Cloud server port	The port number used by the network management platform server.	Value range: 0-65535 Default 1883 port
Device ID	The identification ID for connecting to the network management platform.	Assign from the management platform
Register an account	Manage platform accounts for devices	Platform account
Site name	Used to identify device points when using multiple devices	custom

Step 3 Click "OK" to complete the network management configuration.

——**End**

6.9 Service configuration

background information

Service configuration can customize and modify the device's WEB management port number, and enable or disable RFC1918 filtering, Telnet, and SSH functions.

Operation steps

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

Copyright © 3onedata Co., Ltd.



Step 2 Configure service configuration parameters, as shown in Table 7-9.

Table 69 Description of Service Configuration Parameters6-

Parameter Name	explain	Configuration method
WEB HTTP port	Customize and modify the device's WEB login port number.	Default 80
RFC1918 filtering	After activation, the device's dedicated LAN address will be denied external access.	Dropdown list selection ● yes ● no
Enable Telnet	Choose whether to enable Telnet functionality.	Dropdown list selection ● yes ● no
Enable SSH	Choose whether to enable SSH functionality.	Dropdown list selection ● yes ● no
Enable Console	Is the console enabled or disabled? The serial port cannot enter the console	Dropdown list selection ● yes ● no

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Online light control	There are two ways to determine the online light: 1. Keep 4G connected online successfully and ping the corresponding address normally. The online light is always on 2. Mobile network 4G network successfully connected online, always on	Dropdown list selection Online retention Mobile network

Step 3 Click "OK" to complete the service configuration.

——**End**

6.10 Module Upgrade

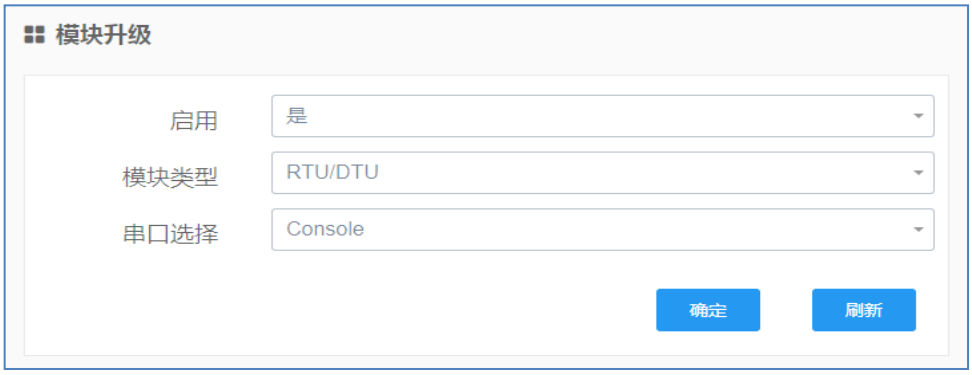
background information

The module upgrade function supports firmware version differential package upgrades for some communication modules.

Operation steps

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

Enable selection "Yes"



Copyright © 3onedata Co., Ltd.

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



Step 2 Configure module upgrade parameters, as shown in Table 7-10.

Table 69 Description of Service Configuration Parameters6-

Parameter Name	explain	Configuration method
Enable	Choose to enable or disable the module upgrade function.	Dropdown list selection ● yes ● no
Module type	Select the type of module that needs to be upgraded. Only differential package upgrades for specific models of devices or communication modules are supported.	Dropdown list selection ● RTU/DTU ● Module ME3630

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Serial port selection	Select the communication serial port.	Dropdown list selection ● Console
Module status	Display the status of the currently upgraded device or communication module.	Click the status refresh button to update the status ● Ready ● Checking ● Upgrade ● Successful ● Failed
Select file upgrade	Select the correct differential upgrade package for updating.	After selecting the upgrade package, click the update button

Step 3 When the "Module Status" column displays Successful, the module upgrade is completed.

——**End**

Copyright © 3onedata Co., Ltd.

7 system state

7.1 system

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

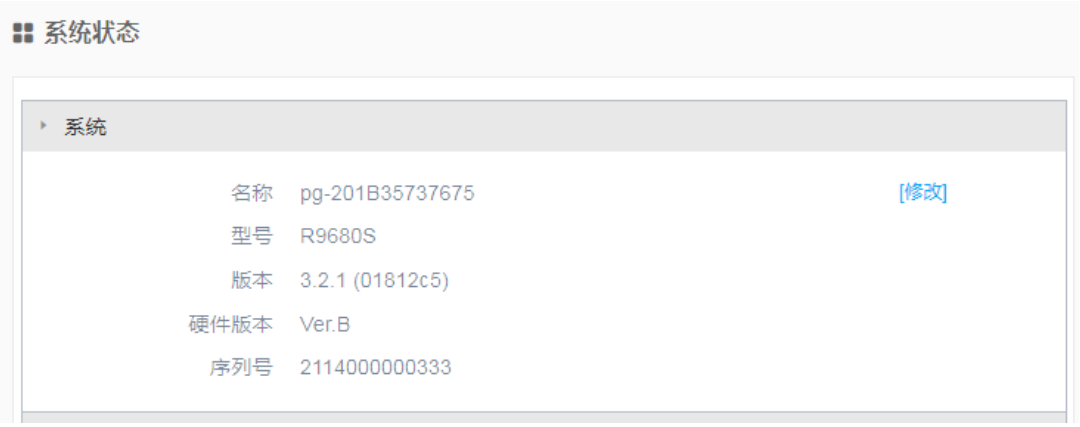


Table 71 System Information Parameter Description7-1

Parameter Name	explain
name	The name of the currently connected device.
model	The current connected device model.
Version number	Web network management configuration version.
Hardware version	Ver. A \ Ver. B versions have hardware differences

Copyright © 3onedata Co., Ltd.

7.2 Mobile network

This section displays the mobile network status information of the router. The description of mobile network status parameters is shown in Table 8-2.



Table 72 Explanation of Mobile Network Status Parameters7-2

Parameter Name	explain
module	The module used by the router.
IMEI	Router ID code.
Operators	Identify the current SIM card operator
Network format	The type of network used by mobile networks.
SIM card status	The current status of the SIM card.
Dual SIM card	Is the dual card function enabled
Current SIM card	Identify the current insertion position of the SIM card
IMSI	Mobile user identification code.
ICCID	SIM card number.
Base station number	The base station number to which the current device is connected.

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
Mobile signal	The strength of the mobile signal.
state	Is the device connected to a mobile network.

7.3 WAN

This section displays the wide area network status information of the router. The description of WAN status parameters is shown in Table 8-3.



Table 73 Explanation of WAN State Parameters7-3

Parameter Name	explain
protocol	WAN connection type.
MAC address	The MAC address of the WAN interface.
address	The IP address of the WAN interface.
Subnet Mask	The subnet mask of the WAN interface.
gateway	Gateway for WAN interface.
DNS 1	Set the preferred DNS server.

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
DNS 2	Set up a backup DNS server.
Port activated	The port number used by the WAN.
receive	WAN interface receives packet size.
send	WAN interface sends packet size.
Connected	WAN connected time.

7.4 LAN

This section displays the LAN status information of the router. The description of LAN status parameters is shown in Table 8-4.



Table 74 Description of LAN State Parameters7-4

Parameter Name	explain
protocol	The protocol used by LAN.
MAC address	The MAC address of the LAN interface.
address	The IP address of the LAN interface.
Subnet Mask	The subnet mask of the LAN interface.
Port activated	The port number used by the LAN.

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
receive	The size of data packets received by the LAN interface.
send	The size of data packets sent by the LAN interface.
Connected	LAN connected time.



7.5 dhcp client

This section displays the DHCP client information of the router. The DHCP client parameter specifications are shown in Table 8-5.

Table 75 DHCP Client Parameter Description7-5

Parameter Name	explain
host name	DHPC client name.
IP address	The IP address of the DHCP client.
MAC address	The MAC address of the DHCP client.
Remaining lease term	The DHCP client obtains the remaining lease time for the IP address.

7.6 WLAN status

This section displays the WLAN status information of the router. The description of WLAN status parameters is shown in Table 8-6.

Copyright © 3onedata Co., Ltd.



Table 76 WLAN Status Parameter Description7-6

Parameter Name	explain
mode	The working mode of WLAN.
equipment	Device name.
passageway	The working channel of WLAN.
rate	The transmission rate of WLAN.
signal	The current signal size of WLAN.
SSID	The identity of the WLAN server.
Network format	The network mode of WLAN.

7.7 WLAN connected device

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



Table 77 Description of WLAN Connected Device Parameters7-7

Parameter Name	explain

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
MAC address	The MAC address of the connected device.
Network	The WLAN name of the connection.
signal	Device connection signal.
noise	Signal-to-noise ratio
Receiving rate	The device receives bandwidth.
Sending rate	Device sending bandwidth.

7.8 DDNS status

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

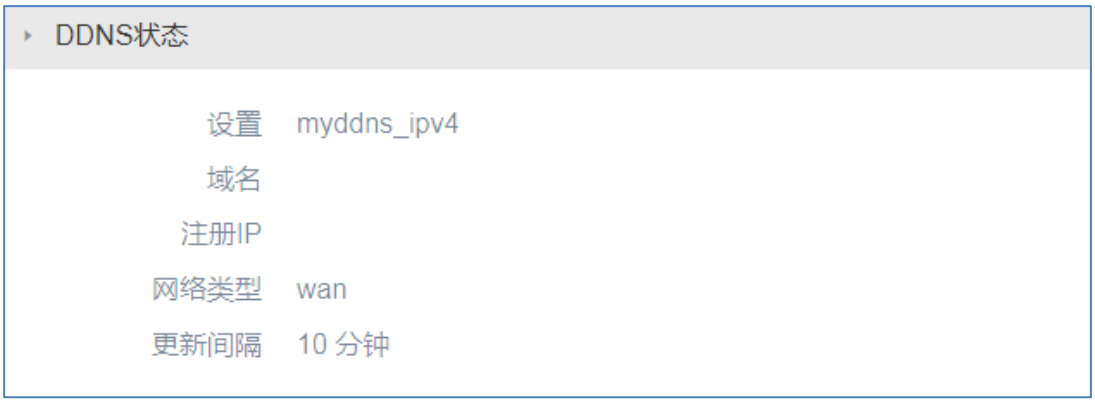


Table 78 Description of DDNS State Parameters7-8

Parameter Name	explain
set up	
domain name	The domain name provided by the DDNS service provider.
Register IP	Get address
Network type	The network type used by the DDNS service.

Copyright © 3onedata Co., Ltd.

Parameter Name	explain
update interval	The interval between the router and the DDNS domain name service provider to update DDNS related information.

Copyright © 3onedata Co., Ltd.

8 Configuration Example

8.1 VPN configuration

8.1.1 L2TP VPN

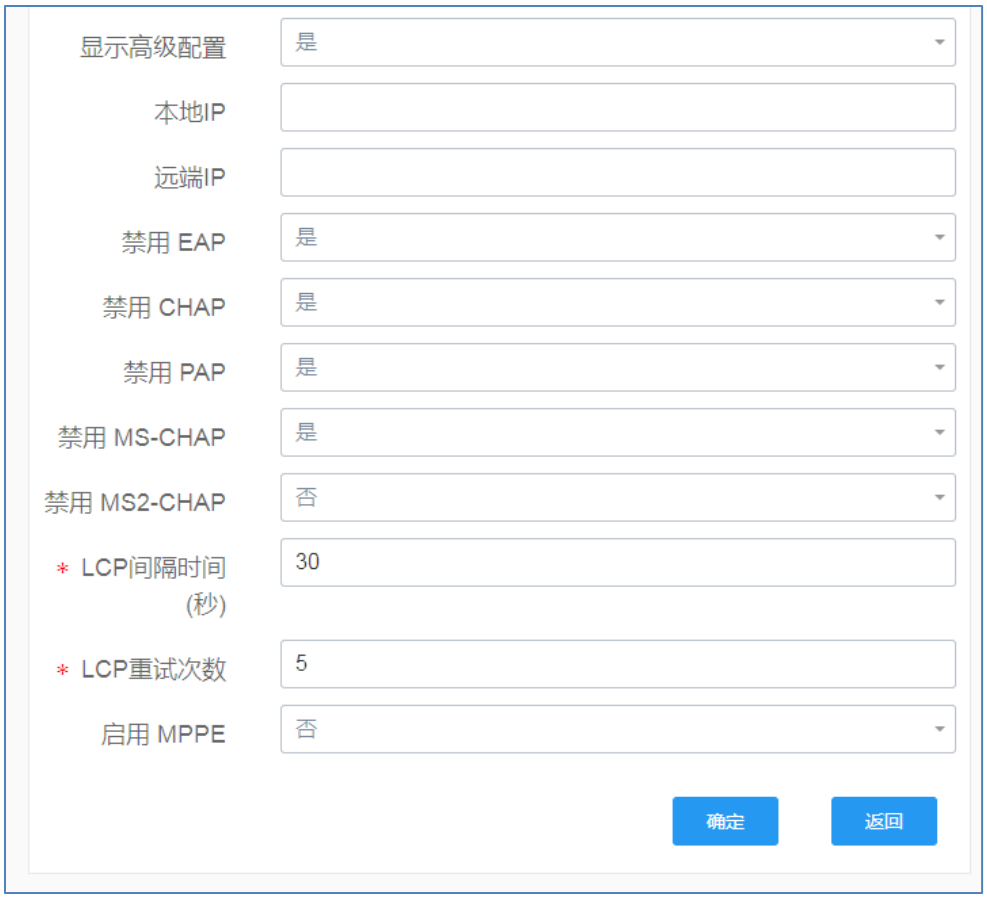
Operation steps

Step 1 After logging into the WEB configuration page, click "VPN Configuration>VPDN Configuration", open the "VPDN Configuration" tab, and click "Create".



Copyright © 3onedata Co., Ltd.

1



Step 2 Configure VPN server parameters, as shown in Table 9-1.

Table 81 L2TP VPN Configuration Parameter Description8-1

Parameter Name	explain	Configuration method
Enable	Is VPN connection enabled.	Select "Yes" from the dropdown list
Interface Name	The name of the VPDN rule.	Enter company VPN
protocol	The protocol adopted by VPDN.	Select "L2TP" from the dropdown list
server	The server IP address or domain name used for access.	Fill in the IP address or domain name of the server used for access

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
User name/password	Authorized legal access users and passwords for accessing the server.	Fill in the authorized legal access username/password for accessing the server
Add default route	After a successful VPN connection, set the default route to this VPN tunnel.	Select "No" from the dropdown list
Add tunnel routing	Add a route that allows the other subnet to access this terminal network.	Select "Yes" from the dropdown list
NAT	Whether to use NAT function.	Dropdown list selection ● yes ● no
MTU	Set the maximum transmission unit.	Manually entering numerical values The default value is 1500
Gateway Hop	Set the hop count of the gateway after VPN connection.	Manual input
Use server to specify DNS	Whether to use the server's DNS.	Select "Yes" from the dropdown list
Reconnection interval (seconds)	The time interval for device reconnection.	Manual input
Do not enable after restart	After the router restarts, the VPN will be shut down.	Select "No" from the dropdown list
Advanced configuration		
Local IP	Set the local static tunnel IP address.	Manually enter in the input box Format: X X. X.X

Copyright © 3onedata Co., Ltd.

Parameter Name	explain	Configuration method
Remote IP	Set the static tunnel IP address for the opposite end.	Manually enter in the input box Format: X X. X.X
Disable EAP	Do not use EAP certification.	Select "Yes" from the dropdown list
Disable CHAPs	Do not use CHAP authentication.	Select "Yes" from the dropdown list
Disable PAP	Do not use PAP authentication.	Select "Yes" from the dropdown list
Disable MS-CHAP	Do not use MS-CHAP certification.	Select "Yes" from the dropdown list
Disable MS2 CHAP	Do not use MS2 CHAP authentication.	Select "No" from the dropdown list
LCP interval time (seconds)	The time interval for sending LCP packet requests.	Manually entering numerical values
LCP retry count	Send LCP packet request timeout retry count.	Manually entering numerical values
Enable MPPE	Enable Microsoft peer-to-peer encryption protocol.	Dropdown list selection ● yes ● no

Step 3 If the VPN status is connected, it is complete.

——End

Copyright © 3onedata Co., Ltd.

9 FAQ

9.1 Hardware related issues

9.1.1 All indicator lights are not on

Problem phenomenon

All indicator lights on the router are not on.

Cause analysis

Possible reasons are as follows:

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

Solution

- 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, please plug the power cord into the power port.

9.1.2 SIM card holder connection issue

Problem phenomenon

The SIM card holder is unable to insert the SIM card properly, and all indicator lights on the router are not on.

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

Cause analysis

Possible reasons are as follows:

- The SIM card holder is damaged.
- The SIM card is inserted in the wrong direction.

Solution

- If the SIM card holder is damaged, please contact our technical support engineer to see if repair is required.
- If the insertion direction of the SIM card is incorrect, please confirm that the SIM card chip is aligned with the slot chip end and inserted into the card holder.

9.1.3 Network port connection issue

Problem phenomenon

The ETH/GE port indicator light is not on and the router page cannot be accessed.

Cause analysis

Possible reasons are as follows:

- Incorrect network cable connection
- The network cable is damaged
- The PC network card is working abnormally or disabled

Solution

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

9.1.4 Antenna connection issue

Problem phenomenon

The antenna cannot be installed properly.

Cause analysis

Possible reasons are as follows:

- The antenna does not meet the accessory requirements.

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

- The antenna connection is incorrect.

Solution

- If the antenna does not meet the requirements, please replace it with one that meets the requirements.
- If the antenna connection is incorrect, please reconnect the antenna.

9.2 Dialing related issues

9.2.1 Dialing interruption

Problem phenomenon

Interruption during device dialing process, unable to dial up for internet access.

Cause analysis

Possible reasons are as follows:

- Poor SIM card contact
- Is the SIM card activated or is it overdue
- Does the device support SIM card network types
- The power supply does not meet the requirements
- PIN function enabled and PIN code set incorrectly

Solution

- If the antenna does not meet the requirements, please replace it with one that meets the requirements.
- If the antenna connection is incorrect, please reconnect the antenna.
- If the SIM card network type is incorrect, please replace the corresponding type of SIM card according to the module.
- If the SIM card is not activated, please activate it. If the SIM card is overdue, recharge the SIM card.
- If the power supply does not meet the requirements, please replace it with a power supply that meets the requirements.
- If it is a PIN code configuration error, please use the correct PIN code.

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

9.3 WEB configuration operation issues

9.3.1 Unable to log in to the configuration page

Problem phenomenon

Unable to log in to the web configuration page normally.

Cause analysis

Possible reasons are as follows:

- Browser incompatibility
- The IP address of the accessed router is incorrect

Solution

- If the browser is incompatible, please use Google Chrome or IE10 or higher versions of the browser.
- Check the IP address obtained by the computer. The router IP and computer IP are in the same network segment.
- If you forget to configure the interface IP address, please hold down the Reset button with a needle for 5 seconds and wait for the router to restart. After restarting, enter 192.168.1.1 in the browser to log in to the configuration page.

9.3.2 Upgrade firmware failed

Problem phenomenon

Upgrading firmware found that the upgrade was not successful.

Cause analysis

Possible reasons are as follows:

- When upgrading, the device is affected by other functions and restarts automatically (such as when the wireless module cannot dial the number)
- The power supply does not meet the requirements
- The model and format of the firmware upgrade are incorrect
- During the upgrade process, the router loses power

Solution

- If the upgrade fails due to being affected by other features during the upgrade and

Copyright © 3onedata Co., Ltd.

restarting, please close other features and upgrade again.

- If the power supply does not meet the requirements, please replace it with a power supply that meets the requirements.
- If the firmware model is being upgraded and the format is incorrect, please replace it with an upgraded firmware with the correct format that matches the Sanwang 4G Router.
- If the router loses power during the upgrade process, please ensure that the power supply to the router is normal.

9.3.3 Router restarts repeatedly

Problem phenomenon

Router restarts repeatedly

Cause analysis

Possible reasons are as follows:

- Communication failure with server address set for online retention function

Solution

- If online retention is set, click "Application Configuration>Online Retention", open the "Online Retention" tab, turn off this function, or fill in the IP address of the server that can communicate normally.

Copyright © 3onedata Co., Ltd.

10 appendix

10.1 Parameter specification table

Parameter type	Value range
General WORD type	Contains numbers, letters, special characters (@,., \,/, -, _,:), all other types are illegal characters, such as username
Alphanumeric Word type	Contains letters, numbers, and other illegal characters, such as modem
The initial letter is generally in Word format	Alphanumeric type with a letter as the first character, such as host name
CODE type	Any character other than spaces, such as svc code
LINE type	Any character that can contain spaces, such as description, password (password that does not allow spaces is of CODE type)
A. B.C.D type	0.0.0. 0~255.255.255.255, ABCD is 0~255, such as IP address configuration
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.255, x.x.x.0 are all illegal
A. B.C.D/M type	0.0.0. 0/0 to 255.255.255.55/32, ABCD from 0 to 255, M from 0 to 32, as configured for subnet

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

Parameter type	Value range
A. B.C.D/M 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 and x.x.x.0 are both illegal, and are illegal when M is 0 and 32, such as configuring the interface IP address
Digital range type	If 1 to 512, it means that the value is any number from 1 to 512 (including 1 and 512)

10.2 term

I

IPSEC Internet Protocol Security (IPSec) is an open standard framework structure that ensures confidential and secure communication over Internet Protocol (IP) networks by using encrypted security services.

L

L2TP L2TP (Layer 2 Tunneling Protocol) is an industrial standard Internet tunneling protocol with functions similar to PPTP protocol, such as encrypting network data streams. However, there are also differences, such as PPTP requiring the network to be an IP network, and L2TP requiring point-to-point connections for data packets; PPTP uses a single tunnel, while L2TP uses multiple tunnels; L2TP provides header compression and tunnel verification, while PPTP does not support it.

router A device that selects routing for information flow or data packets.

M

Modem A general term for the combination of modulators and demodulators. A conversion interface that enables digital data to be transmitted on analog signal transmission lines.

R

Copyright © 3onedata Co., Ltd.

RIP2 RIP/RIP2/RIPng: Routing Information Protocol, as an internal gateway protocol or IGP (Internal Gateway Protocol), is a routing protocol applied to AS systems. RIP is primarily designed to work with moderately sized networks using similar technologies. Therefore, through wiring connections with minimal speed changes, RIP is more suitable for simple campus and regional networks, but not for complex network situations. RIP 2 is derived from RIP and is a supplementary protocol to the RIP protocol. It is mainly used to expand the amount of useful information loaded in RIP 2 while increasing its security performance. RIP 2 is a UDP based protocol. Under RIP2, each host sends and receives packets from UDP port 520 through a routing process. The default routing update cycle for the RIP protocol is 30 seconds.

W

WMMP The WMMP (Wireless M2M Protocol) protocol is an application layer protocol designed to facilitate data communication between M2M terminals and M2M platforms, between M2M terminals, and between M2M platforms and application platforms in M2M services.

Copyright © 3onedata Co., Ltd.

11 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;

11.1 Internet Service

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

11.2 Service Hotline

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

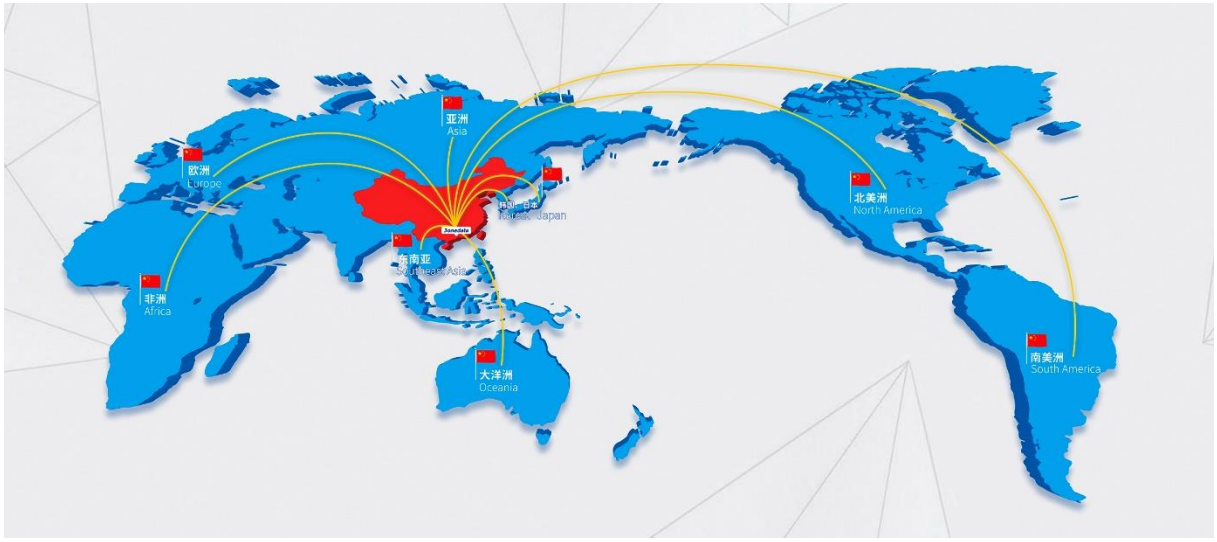
11.3 Product Repair or Replacement

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.

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



3onedata Co., Ltd.

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