www.hongdian.com

Connecting things
Hongdian

User Manual
4G Intelligent Gateway

We Hongdian provide full support to customers, contact us freely if any questions.

Hongdian Corporation

Address	Tower A, Hongdian Building, 100 Huabao Road, Pinghu, Longgang District, Shenzhen, China
Website	http://www.hongdian.com
Technical Support	+86-0755-88864288-4
Fax number	0755-83404677
Postalcode	518112

Copyright © Hongdian Corporation. All rights reserved.

All information in this user manual is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user manual by any means without written authorization from Hongdian Corporation.

Trademarks and Permissions

Connecting things Hongdian and DTU are the trademarks and logos of Hongdian Corporation. Other trademarks and logos mentioned in this manual belong to other organizations related. Hongdian Corporation does not own the rights of other trademarks and logos.

Caution

The content of this document may be updated from time to time due to product version updates or other reasons. Unless otherwise agreement, this document is intended as a guide for use only. All statements, information and recommendations in this document do not constitute any express or implied warranty.

Contents

1 The Configuration of Router.....
About this chapter.....
Overview.....
1.1 Basic configuration.....
1.1.1 Logging in to the WEB Configuration Page.....
1.2 Network settings.....
Overview.....
1.2.1 LAN.....
1.2.2 WAN.....
1.2.3 Modem.....
1.2.4 WLAN.....
1.2.5 Parameter select (Recommend to Single module dual SIM version).....
1.2.6 Network type.....
1.2.7 Link Backup.....
1.2.8 DHCP Service.....
1.3 Application Setting.....
Overview.....
1.3.1 ICMP check.....
1.3.2 DDNS configuration.....
1.3.3 GPS configuration.....
1.3.4 DTU configuration.....
1.3.5 SNMP configuration.....
1.3.6 M2M configuration.....
1.3.7 Schedule configuration.....
1.3.8 SMS Settings.....
1.3.9 Radius settings.....
1.4 Security Configuration.....
Overview.....
1.4.1 IP Filter.....
1.4.2 Domain Filter.....
1.4.3 MAC filter.....
1.4.4 Remote Access.....

1.4.5 Anti-attack.....
1.5 Forward configuration.....
Overview.....
1.5.1 NAT.....
1.5.2 Routing Configuration.....
1.5.3 QoS.....
1.5.4 Dynamic Routing (Optional).....
1.6 VPN configuration.....
Overview.....
1.6.1 VPDN configuration.....
1.6.2 Tunnel configuration.....
1.6.3 IPSec configuration.....
1.6.4 Open VPN Configuration.....
1.6.5 DMVPN Configuration.....
1.6.6 EOIP Configuration.....
1.7 System Management Configuration.....
Overview.....
1.7.1 Local Log.....
1.7.2 Remote Log.....
1.7.3 Clock.....
1.7.4 Account.....
1.7.5 Network Test.....
1.7.6 Files.....
1.8 Status.....
Overview.....
1.8.1 Base Information.....
1.8.2 LAN.....
1.8.3 WAN.....
1.8.4 Modem.....
1.8.5 WLAN.....
1.8.6 Routing Table.....
1.8.7 GPS.....
1.8.8 Traffic Statistics.....
1.9 RESET button function.....
2 Typical application.....
About this chapter.....
2.1 Overview.....
2.2 Link backup function.....
Application result.....
2.3 Parameter select function.....
2.4 VPN.....

2.5 Schedule.....

3 FAQ/Exception handling.....

About this chapter.....

3.1 Hardware Failure.....

3.1.1 All LED off.....

3.1.2 SIM Slot.....

3.1.3 Ethernet Connection.....

3.1.4 Antenna Connection.....

3.2 Dial Online Problem.....

3.2.1 Dial discontinue.....

3.2.2 No Signal.....

3.2.3 Cannot find SIM/UIM card.....

3.2.4 Poor Signal.....

3.2.5 Compress Protocol not match.....

3.3 VPN Problem.....

3.3.1 VPDN cannot connect.....

3.3.2 VPN cannot communicate.....

3.3.3 Router can communicate but subnet cannot.....

3.4 WEB config problem.....

3.4.1 Updating firmware failure.....

3.4.2 Backup setting problem.....

3.4.3 Updating patch failure.....

3.4.4 CFE Updating failure.....

3.4.5 Update failure in WEB GUI.....

3.4.6 Forget Router Password.....

1 The Configuration of Router

About this chapter

Section	Brief Introduction of Contents
5.1 Overview	the configuration of the 4G Intelligent Gateways in the WEB mode is introduced in this section briefly .
5.2 basic configuration	what the 4G Intelligent Gateways need to complete before performing advanced configuration is introduced in this section briefly.
5.3 Application	the 4G Intelligent Gateway application configuration, and how to configure it are introduced in this section briefly.
5.4 Security	the 4G Intelligent Gateway security configuration, and how to configure it are introduced in this section briefly .
5.5 Forward	the 4G Intelligent Gateway forwarding configuration, and how to configure it are introduced in this section briefly .
5.6 VPN	the 4G Intelligent Gateway VPN functions, and how to configure them are introduced in this section briefly .
5.7 System	The 4G Intelligent Gateway system management configuration, and the specific configuration and operation methods are introduced in this section briefly .
5.8 Status	This section briefly introduces the 4G Intelligent Gateway status query, and status query method.

Overview

4G Intelligent Gateway can be configured by WEB mode, which is easy to operate and intuitive. After the local connection configuration of the PC and the 4G Intelligent Gateways is completed according to the "Local Area Connection Configuration", you can start Internet Explorer or other browsers on the PC and log in to the 4G Intelligent Gateways for configuration.

1.1 Basic configuration

Through the "5.2.2 Network Settings", you can realize the basic functions of dial-up Internet access and access to the public network.

1.1.1 Logging in to the WEB Configuration Page

Step 1 Open the Internet Explorer browser of the configuration computer and enter "http://192.168.8.1/" in the address bar. Enter the authentication page of the user login identity, as shown in Figure 5-1.

Figure 1-1 The Local authentication page of the user login identity

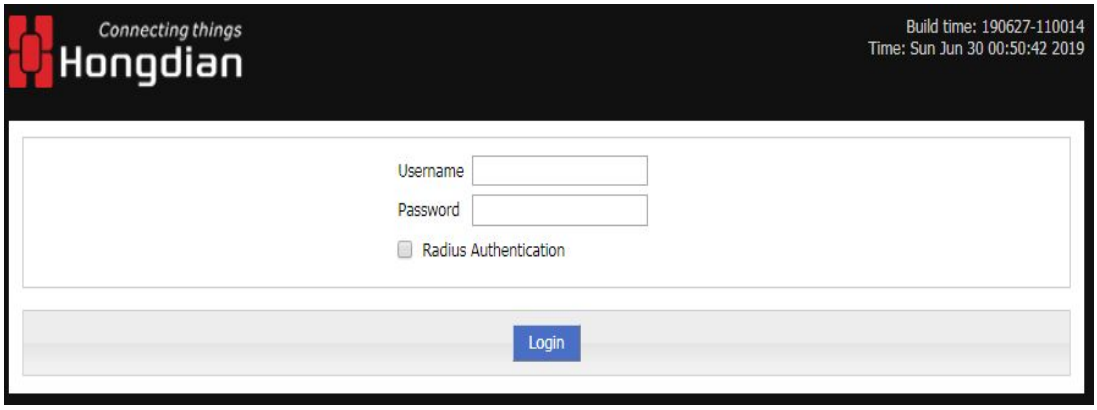
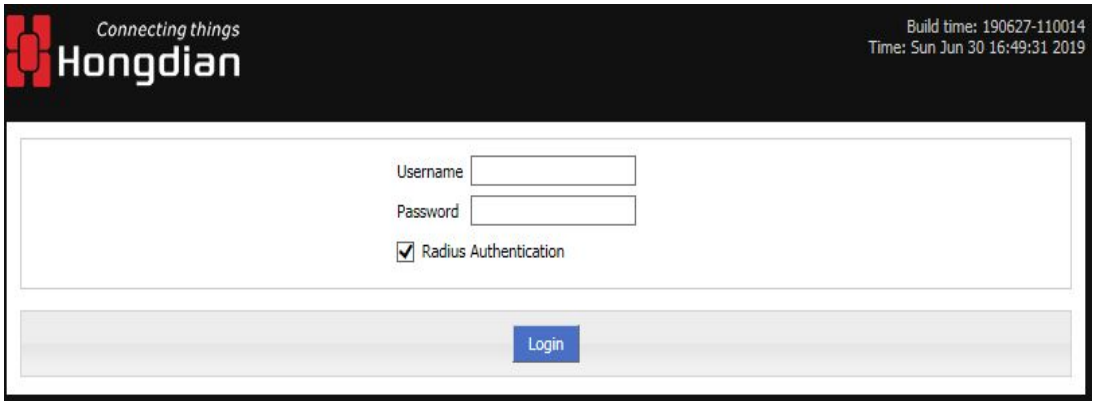


Figure 1-2 Identity authentication page for user Radius login



Step 2 To log in as Local, just enter "Username", "Password" and then click "Login" to log in to the WEB configuration page of 4G Intelligent Gateway.

Step 3 To log in as Radius, you need to select "Radius Authentication", then enter the radius username and password, and click "Login" to log in to the WEB configuration page of the 4G Intelligent Gateway.

NOTE

When logging into the system for the first time. The default username is admin and the password is admin. To change the password, please refer to "5.7.5 User Management".

---END

1.2 Network settings

Overview

The network settings mainly complete LAN, WAN, WLAN, mobile network, parameter selecting, network type, link backup, DHCP server and other configurations. After the configuration is completed, the basic network communication needs can be met.

1.2.1 LAN

The LAN port configuration is mainly used for the connection between the router and the lower device, so that the lower device can access the external network through the router, and at the same time ensure normal communication between the network segments connected to the router.

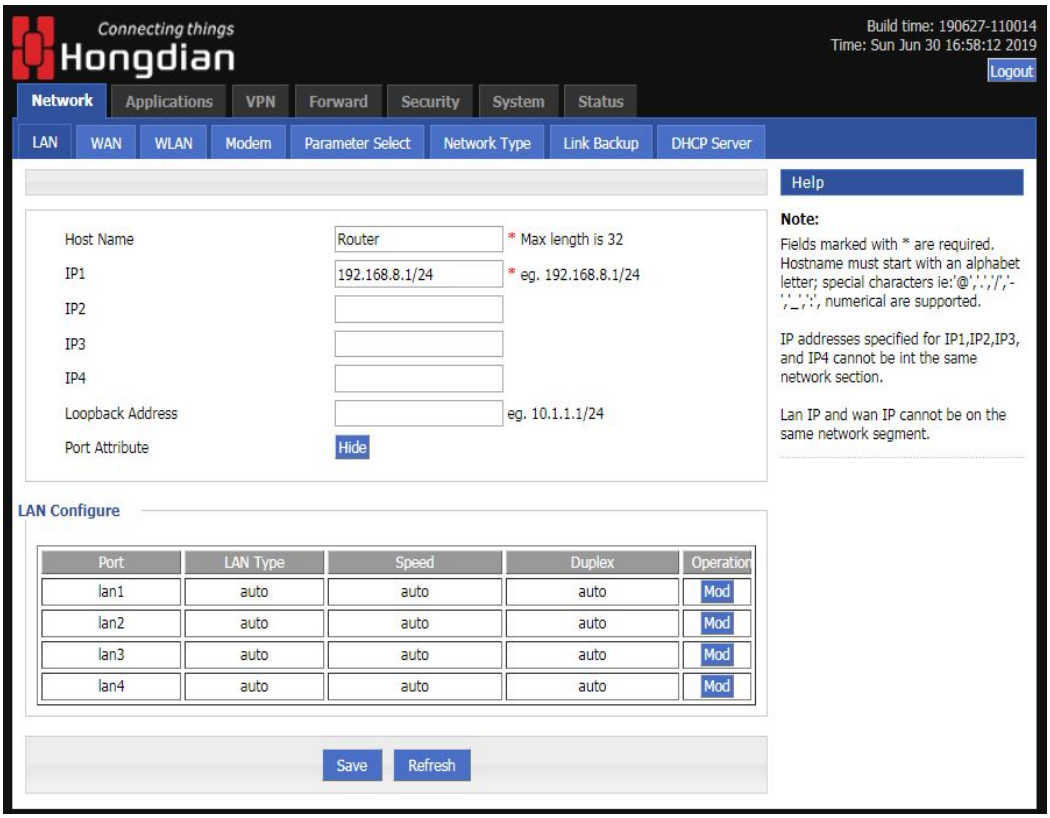
Step 1 Log in to the WEB configuration interface of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration page”.

Step 2 Click “Network > LAN”.

Open the page of LAN , as shown in Figure 5-3.

Figure 1-3 The page of LAN



Step 3 Set the connection parameters of the LAN port.

Table 1-1 The instruction of LAN Parameter

Parameter	Details	Operation
Host name	The name of router	Manual input, Maximum length limited to 32 word type character,Please refer to the “Parameter Specification Table” for input specifications.
IP1~4	Used to divide subnets, these subnets can communicate with each other, and IP1~4 represent 4 subnets.	Enter it manually. Format: A.B.C.D/M, please refer to "Parameter Specification Table" for input specifications.The default IP1: 192.168.8.1/24, and IP2~4 are input in the above format, but the contents between the two cannot be the same.
Loopback address	The virtual interface address of the router, which is configured and will not disappear due to the LAN interface being closed.	Enter it manually. Format: A.B.C.D/M, please refer to “Parameter Specification Table” for input specifications.
Lan Configure	Duplex mode and port rate for setting the lan port	The following pull frame selection method is used to select the port rate and duplex mode. The default is auto mode.

Step 4 Click Save to complete the configuration of connection type of the LAN port .

NOTE

When the user changes the IP1 address, if the page does not automatically jump, please make sure that the user's computer has the same network address as the modified LAN address, or set the computer to automatically obtain the IP, and then enter the new one in the browser.

---END

1.2.2 WAN

The WAN is mainly used to connect to the Internet through Ethernet. The connection modes are static IP, DHCP, and PPPoE.

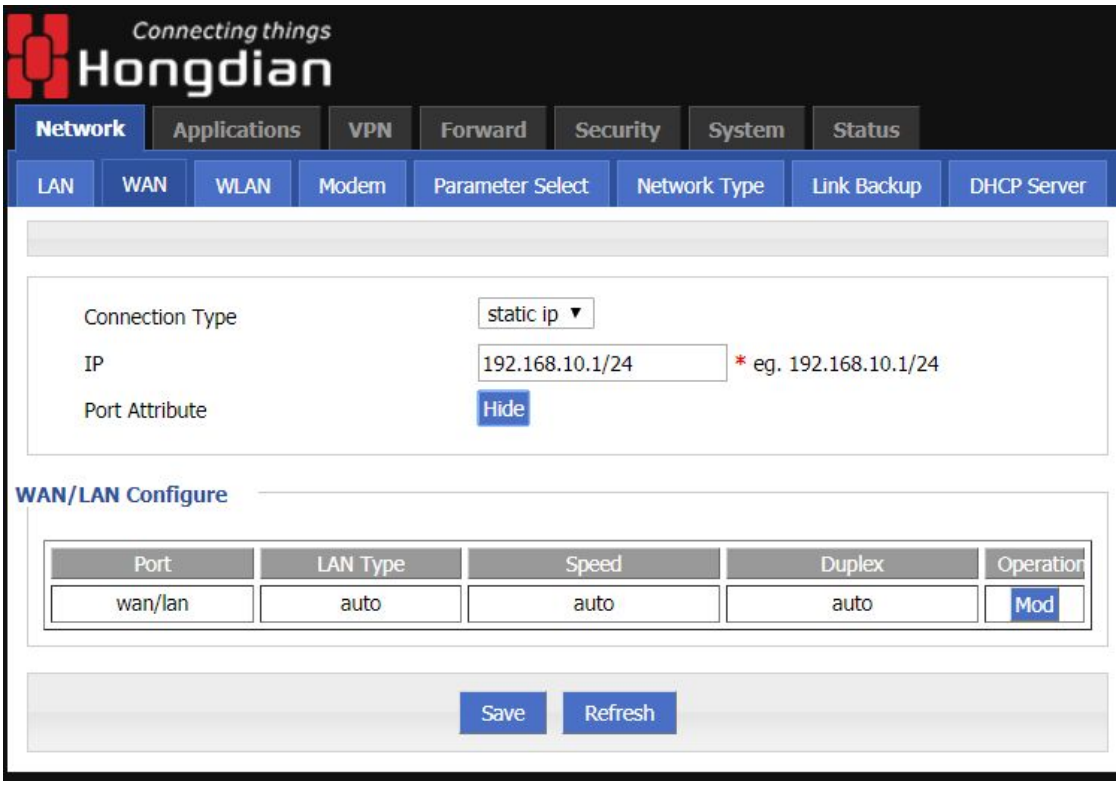
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration page”.

Step 2 Single click “network > WAN”.

Open the page of WAN , as shown in Figure 5-4.

Figure 1-1 The page of WAN



Step 3 Configure the connection type of the WAN port

The parameter description is shown in Table 5-2.

Table 1-1 The instruction of WAN connection type parameter

Parameter	Details	Operation
Connection Type	The connection type of the WAN.	Dropdown List Selection: • Static IP:manually configure the IP address of the interface. If you need to access the Internet through the WAN, you need to add the gateway, DNS, and default route to the network type. • DHCP: The DHCP client automatically obtains the IP address. If you need to access the Internet through the WAN, you need to add the default route configuration to the network type. • PPPoE: PPPoE dial-up obtains IP (usually an external ADSL modem for ADSL dial-up Internet access). If you need to access the Internet through the WAN, you need to add the default route configuration in the network type.
“Connection Type” select “Static IP”		
IP	Configure when "Connection Type" selects	Format: A.B.C.D/Mask Please refer to the”Parameter Specification Table”

Parameter	Details	Operation
	"Static IP".	for input specifications. For example: 192.168.10.1/24
“Connection Type” select “DHCP”		
IP	get IP address from DHCP	Select DHCP
“Connection Type” select “PPPoE”		
Interface Name	The unique identifier of an interface. It is used when other functions are invoked or associated with the interface. For example, you can configure the route of the interface and control the disable and enable of the interface.	PPPoE is not configurable. The interface name of the PPPoE configured on the web page is specified by the system. The interface name is: pppoe.
Service Name	Configure the PPPoE service name, which is usually used for identification and judgment between the client and the server. It is usually provided by the server. The ADSL dial-up is provided by the ISP.	General WORD type, maximum 64 bytes, can not be empty, please refer to "Parameter Specification Table" for input specifications.
Username/Pass word	The username/password used for PPPoE dialing is usually provided by the server. The ADSL dial-up is provided by the ISP.	Generally, the WORD type/CODE type, each of which has a maximum length of 64 bytes, is not empty. For the input specification, please refer to the "parameter specification table".
Advanced settings	Advanced parameters are used in special cases. It is usually not recommended. For the parameter description of "Advanced Settings", please refer to the related parameters in Table 5-3.	Click "Hide" to display the parameters of the advanced settings.
Wan Configure	Duplex mode and port rate for setting the wan port	The following pull frame selection method is used to select the port rate and duplex mode. The default is auto mode

Step 4 Single click “save” to complete the configuration of wan port.

---END

1.2.3 Modem

Mobile network is one of the core functions of 4G Intelligent Gateway. 4G Intelligent Gateway supports single-mode single-card dialing and single-mode dual-card backup dialing. It provides high-speed wireless broadband access for users. Internet access speeds of 3G can usually reach 1 to 5 Mbps, 3.5G networks can reach be up to 20 Mbps, and LTE can be up to nearly 100 Mbps.

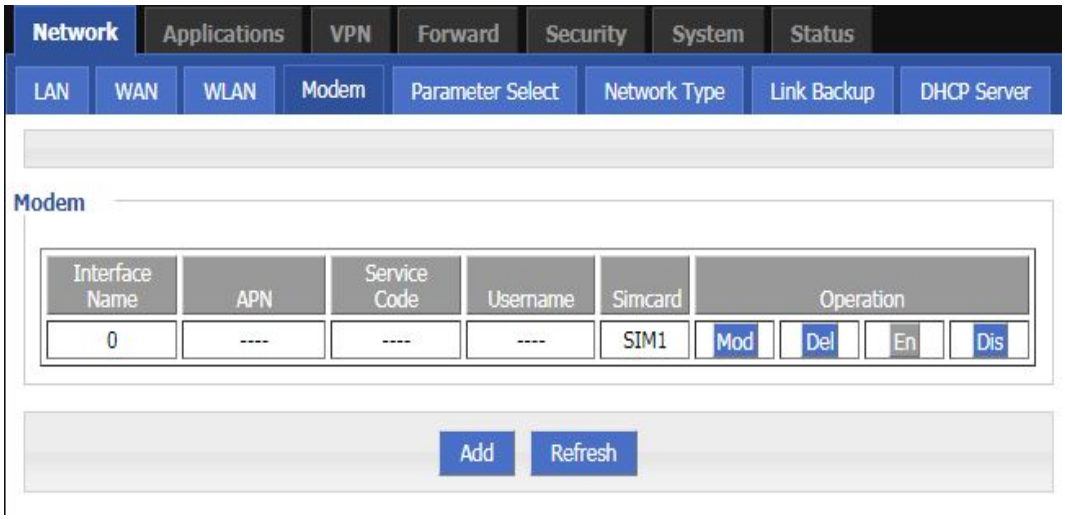
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Single click “Network > Modem”.

Open the page of Modem, as shown in Figure 5-5.

Figure 1-1 The page of Modem



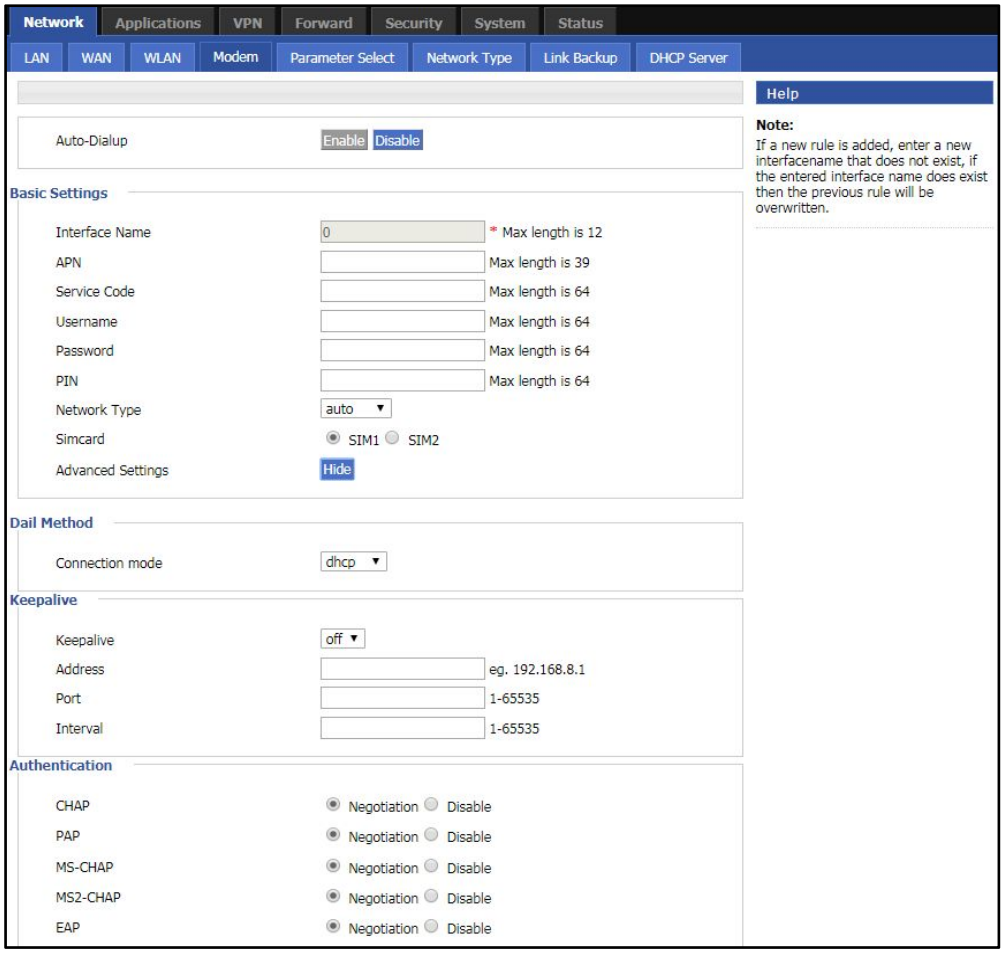
Step 3 “Add”, ”Edit”,” Delete”, “Enable”, and “Disable” actions for Mobile Network Parameters.

Action:

- Add

1. Click “Add” to display the Add page of modem Configuration, as shown in Figure 5-6..

Figure 1-2 The page of Modem(single-mode dual-card)



2. Add the "Modem" parameter. Table 5-3 describes the parameters of the modem.

Table 1-1 The instruction of the parameters of the modem

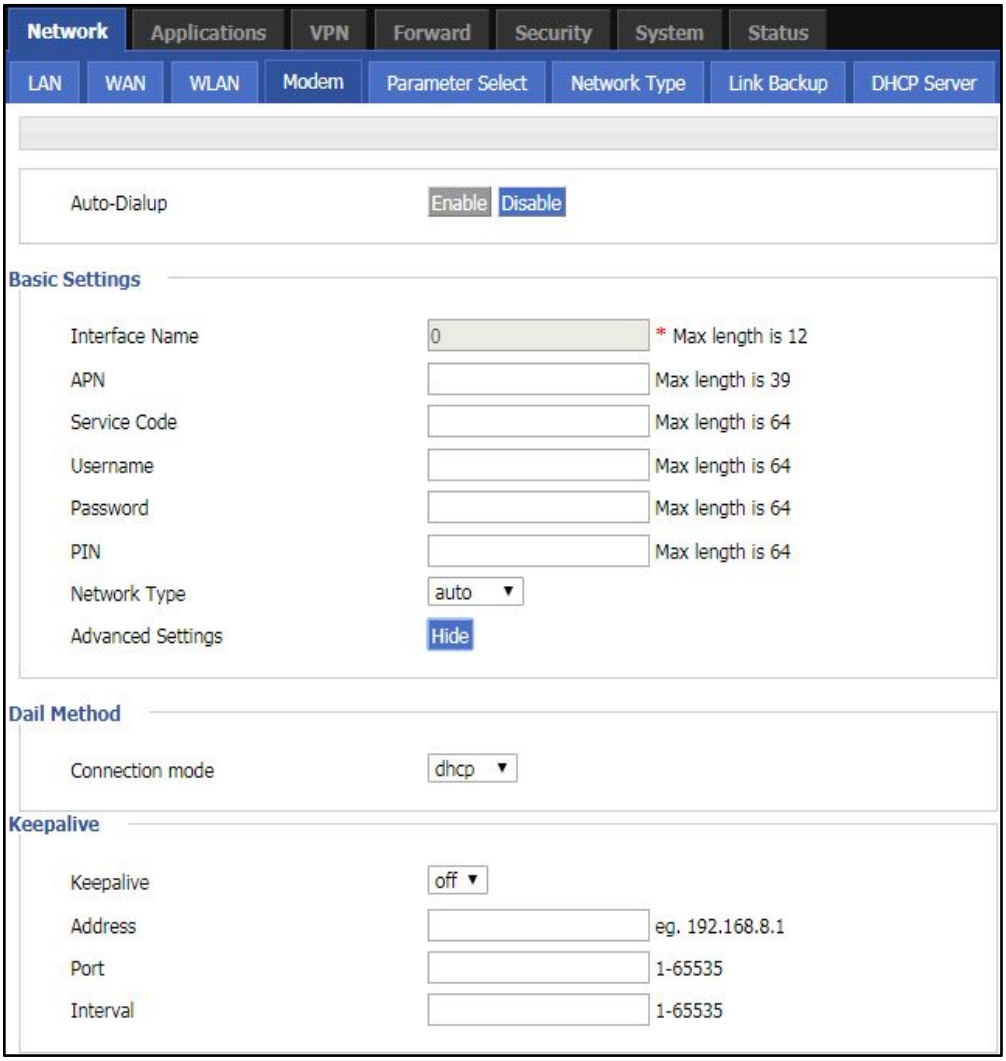
Parameter	Details	Operation
Auto-dialup	Enable the current modem parameter for modem dialing. Only one of the enabled modem parameters is running (random or other functions are controlled). When multiple sets of modem parameters are disabled, modem dialing is disabled.	Button selection: • Enable • Disable When the button is clicked, it will be grayed out to indicate that the current state is in effect. If "Enable" is grayed out, it indicates that the function or parameter is enabled.
APN	The unique identifier of an interface. It is used when other functions are invoked or associated with the interface. For example, you can configure the route of the interface and control the disable and enable of the interface.	Alphanumeric WORD type, up to 12 bytes, non-empty,please refer to"Parameter Specification Table" for input specifications.
Service Code	A type of code identifier for a network, usually a fixed network of	CODE type, maximum 64 bytes, please refer to "Parameter Specification Table" for input

Parameter	Details	Operation
	services has a fixed service code.	specifications.
Username /Password	The identity of the access operator network is used to access different private network services to isolate different private networks in the case of private network services.	WORD type / CODE type, each of which has a maximum length of 64 bytes, which are both present or empty at the same time.
PIN	Personal Identification Number, the identification password of the SIM card, the user can use the PIN code to unlock and lock the SIM card to prevent illegal users from using it.	Alphanumeric WORD type, please refer to "Parameter Specification Table" for input specifications.
SIM card (configuration items only in single-module dual-card mode)	Single-mode dual-card mode configuration option for specifying the SIM card when dialing.	Radio button selection • SIM1 • SIM2
Network Type	Use this option to force the required access network type to 2G or 3G/4G/5G. Usually used when a network is unstable or only wants to work on a network	The drop-down box option options include: • auto • wcdma • edge • fdd-lte • tdd-lte • td-scdma • evdo • cdma The drop-down box according to the type of the module will correspond to different network types, and AUTO means 2G/3G/4G/5G adaptation.
Connection mode	Used to select different connection methods to obtain an IP address from the base station	Drop-down box options: • pppd • dhcp • bridge The dhcp mode is used by default. The bridge mode can only be selected when it is in the EC25 series module.
Keepalive	Used to maintain a communication connection with the base station to prevent the base station from kicking off the modem	Keepalive function switch: • off • On The default is off Address is manually entered: Enter the service address detected by tcpping. If not entered, use the gateway address of the modem as the service address.

Parameter	Details	Operation
		Port is manually entered: Enter the corresponding port address. use port 22 by default. Interval is manually entered: Enter the Tcpping packet sending interval. Ithe default is 10 (seconds).
advanced settings	It is not recommended to configure the advanced parameters of PPP dialup. It is usually used when the private network service server has matching requirements. The dialing advanced options of VPDN and PPPoE are the same as the modem advanced options, as shown in Figure 5. 8 is shown.	Click to display the advanced settings.
Authentication (It needs to match the server when configuring. The default is all negotiation.)		
CHAP	Challenge-Handshake Authentication Protocol, a way to send real password when build ppp link, improved security	• Disable • Negotiation CHAP is prior to PAP
PAP	Password Authentication Protocol	• Disable • Negotiation
MS-CHAP	MS-CHAP Microsoft Challenge-Handshake Authentication Protocol Based on MPPE	• Disable • Negotiation
MS2-CHAP	MS-CHAP second version	• Disable • Negotiation
EAP	PPP Extensible Authentication Protocol	• Disable • Negotiation
Compress (It needs to match the server when configuring. The default is all disabled.)		
Compression Control Protocol	Negotiate which compress control protocol used on PPP link	• Disable • Negotiation
Address/Control Compression	Whether compress IP address	• Disable • Negotiation
Protocol Field Compression	Whether compress Whether compress IP address	• Disable • Negotiation
VJ TCP/IP Header	Whether allow TCP/IP to communicate by compressing VJ	• Disable • Negotiation

Parameter	Details	Operation
Compress		
Connection-ID Compression	Whether allow TCP/IP to communicate by compressing ID in the first	• Disable • Negotiation
More		
Debug	Enable PPP dialing log, default value is enable, in order to check more info about dialing, suggest no changing	• Disable • Negotiation
Peer's DNS	Auto get peer DNS when PPP dialing. DNS is necessary if want visit domain name. In order to forbid LAN pc visit domain name, you may disable it	• Disable • Negotiation
LCP interval/Retry	After PPP dialing succeed, LCP is needed to keep PPP link alive. Also it could be used to quickly spot network interrupt and reconnect	Value area : 1~512 Unit: second Default value: 30/5
MTU	the number of bytes of the maximum transfer unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
MRU	the number of bytes of the maximum receive unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
Local IP	Set the local IP address when PPP dialing, need ISP support	A.B.C.D, Example: 10.10.10.1
Remote IP	Set the remote IP address when PPP dialing, need the support of ISP	A.B.C.D, Example: 10.10.10.254
Professional	• nomppe • mppe required • mppe stateless • nodeflate • nobsdcomp • default-asyncmap	Do not suggest modify, please contact us for help if necessary

Figure 1-3 The page of Modem (Single module single SIM)



3. Click “Save” to complete the parameter configuration for Modem..

- Modify
  As shown in Figure 5-5, determine a parameter configuration record and click Modify to modify the parameter record. The parameter description is shown in Table 5-3.
- Delete
  As shown in Figure 5-5, determine a parameter configuration record and click Delete to delete the parameter record.
- Enable
  As shown in Figure 5-5, determine a parameter configuration record and click Enable to enable the parameter record.
- Disable

As shown in Figure 5-5, determine a parameter configuration record and click disable to disable the parameter record.

- Refresh
  Click “Refresh” to refresh the current page.

NOTE

When the button is gray, it indicates that the corresponding action is already in effect. When you click Enable, the Enable button is grayed out to indicate that the feature or parameter is currently enabled.

---END

1.2.4 WLAN

4G Intelligent Gateway provides two functions of WLAN AP and Station client. Through the AP function, 4G Intelligent Gateway can provide wireless LAN hotspots. Through the Station client function, 4G Intelligent Gateway can be connected to other AP device,The lower device of the 4G Intelligent Gateway can access the external network through the connected AP device.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration page”.

Step 2 Single click “Network > WLAN”.

Open the page of WLAN. When you select different WLAN working modes (AP, Station), the displayed pages are shown in Figure 5-8 and Figure 5-9. When the WLAN working mode selects the station, you need to scan the surrounding APs to select an AP to access, as shown in Figure 5-10.

Figure 1-4 The page of AP mode configuration

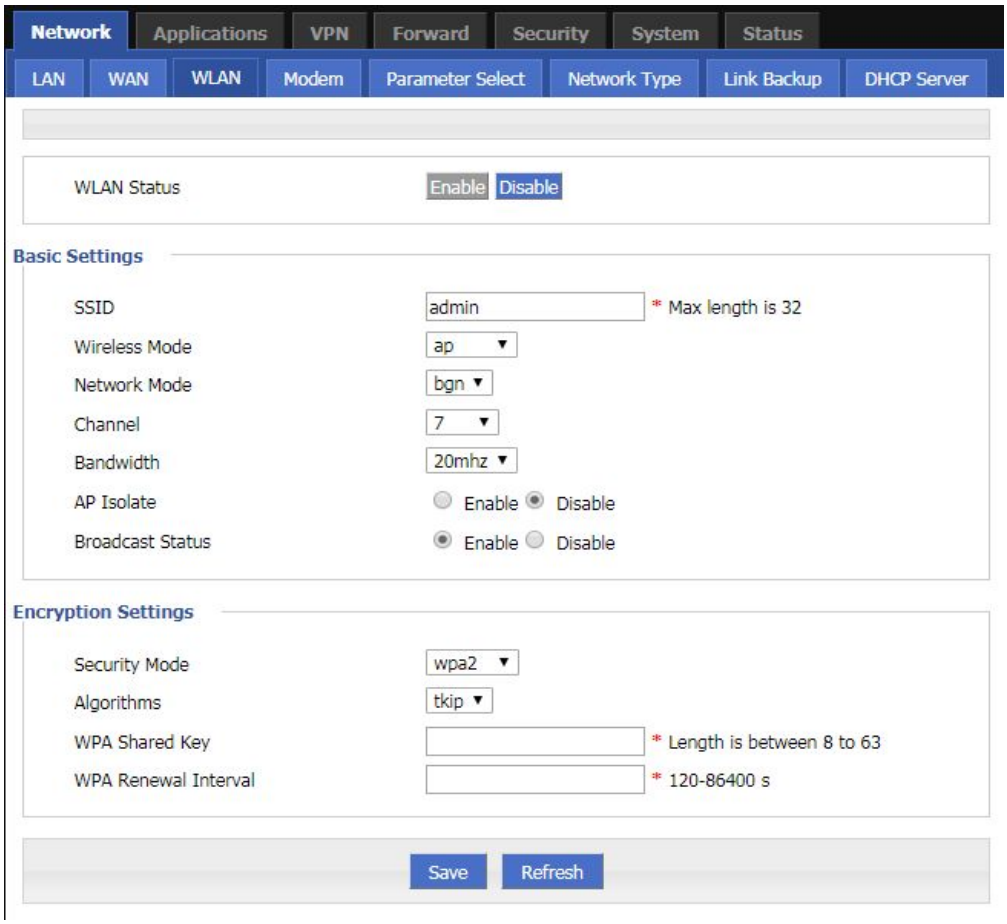


Figure 1-5 The page of Station mode configuration

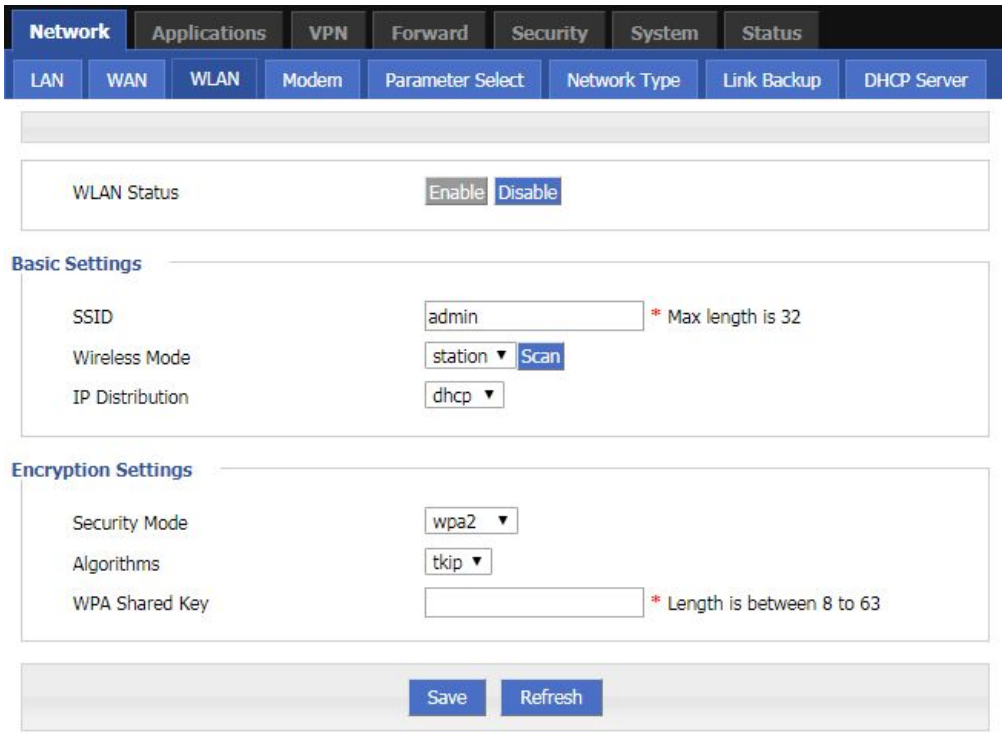
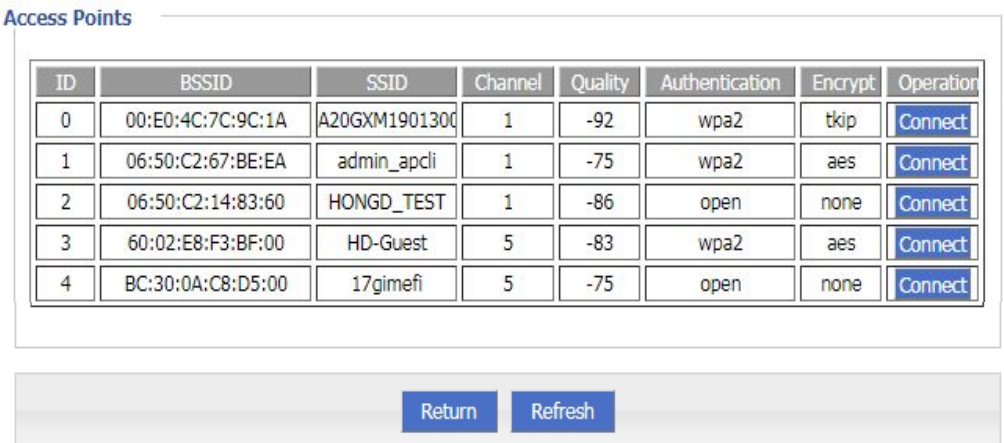


Figure 1-6 The Scanning page when selecting a station



Step 3 Configure parameters related to WLAN. The parameter description is shown in Table 5-4.

Table 1-1 The instruction of WLAN parameter

Parameter	Details	Operation
WLAN Status	Enable or disable WLAN feature	Dropdown List • Enable • Disable
Basic Setting		

SSID	The identity of the WLAN server.	General WORD type, maximum 32 bytes, please refer to "Parameter Specification Table" for input specifications.
Wireless Mode	WLAN work mode, support ap/station	Dropdown List • ap • station
Network Mode	WLAN network mode, different network models are quite different transmission rates, default bgn mixed mode. When operating mode is selected AP, the AP needs to manually set the network mode; When working mode selection station or repeater, AP network mode for the selected network mode, can not be modified manually.	Dropdown List • b represents the network rate of WLAN is 11Mbps • bg represents the network rate of WLAN is11Mbps,54Mbps(Auto- Negotiation) • bgn can support 11Mbps,54Mbps,150Mbps mixed mode
Channel	The working channel of the WLAN,which can be configured according to the specific needs of the network environment. The default is auto.	Dropdown List • auto • 1~11 Auto indicates channel adaptation. When there is no interference, channel 6 is used by default. When the same channel interference occurs, it automatically jumps to the channel with less interference.
Bandwidth	Bandwidth configuration when WLAN work at 802.11n	Dropdown List • 20MHz • 40MHz 40MHz represents high speed mode of 802.11n.
AP Isolate	The WLAN clients connected to the AP are isolated so that the clients cannot access each other.	Dropdown List • Enable • Disable
Broadcast Status	Used to configure the WLAN SSID is broadcasted so that clients can search the SSID, usually do not want other people to search and disable WLAN function, disable it means hidden SSID function in a network environment, users want to connect, you need to manually add the SSID	Dropdown List • Enable • Disable
IP Distribution(when Wireless Mode is	The address communicated with the AP when the H8922S4G Intelligent Gateway is connected to	Dropdown List • dhcp: get IP address from DHCP • static: manually set IP address

station)	the AP.	
IP(when Wireless Mode is station)	When "IP allocation" selects static, you need to configure the address to establish communication with the AP.	Format: A.B.C.D please refer to “Parameter Specification Table”for input specifications.
WLAN Encryption		
Security Mode	Configure the WLAN encryption mode to disable when cryptographic authentication is not required. WEP encryption is relatively easy to crack, it is recommended to use WPA encryption	Dropdown List • disable • wpa • wpa2
wpa/wpa2(WiFi Protected Access)		
Algorithms	Encryption algorithms • tkip • aes	Dropdown List
WPA Share Key	WLAN encryption key, used to connect the specified SSID	WORD or Number type, refer to "Parameter Specification Table"
WPA Renewal Interval	The time interval for the AP to verify the WLAN client key; if the verification is passed, the WLAN connection is continued, and if the verification fails, the WLAN connection is disconnected.	Value area: 120-86400 Units: Seconds

NOTE

When the working mode select station , 4G Intelligent Gateway will automatically match according to the selected AP and the corresponding encryption algorithm (to keep consistent with AP encryption); shared key update interval is required to fill in the connections of AP key and interval.

---END

1.2.5 Parameter select (Recommend to Single module dual SIM version)

4G Intelligent Gateway parameter switching function is a backup switching function independently developed by our company, with multi-function combination backup and switching. The main application scenarios are: multi-server mutual backup, multi-operator backup (in many countries, one SIM card supports multiple operators, one carrier is abnormally switched to another carrier), and application scenarios in which the functional parameters need to be bundled but they requires backup switching between each other.

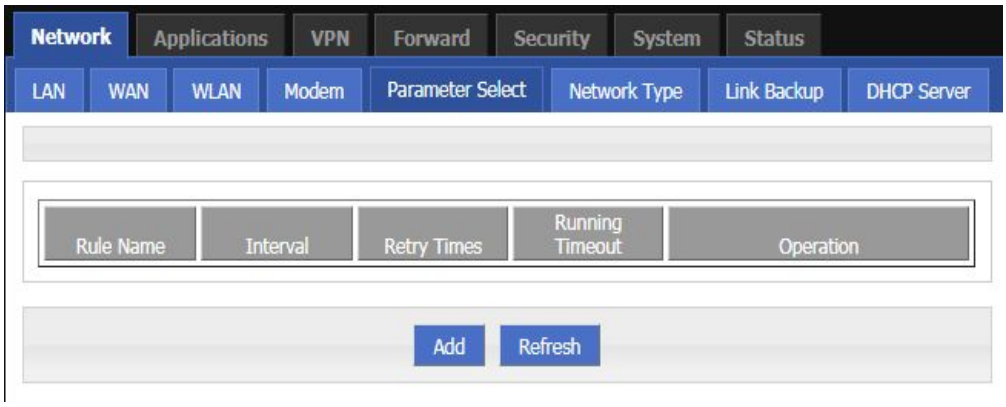
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration page”.

Step 2 Single click “Network > parameter select”.

Open the page of “Parameter Select” , as shown in Figure 5-11.

Figure 1-1 The page of “Parameter select”



Step 3 Configure the parameters related to Parameter Select.

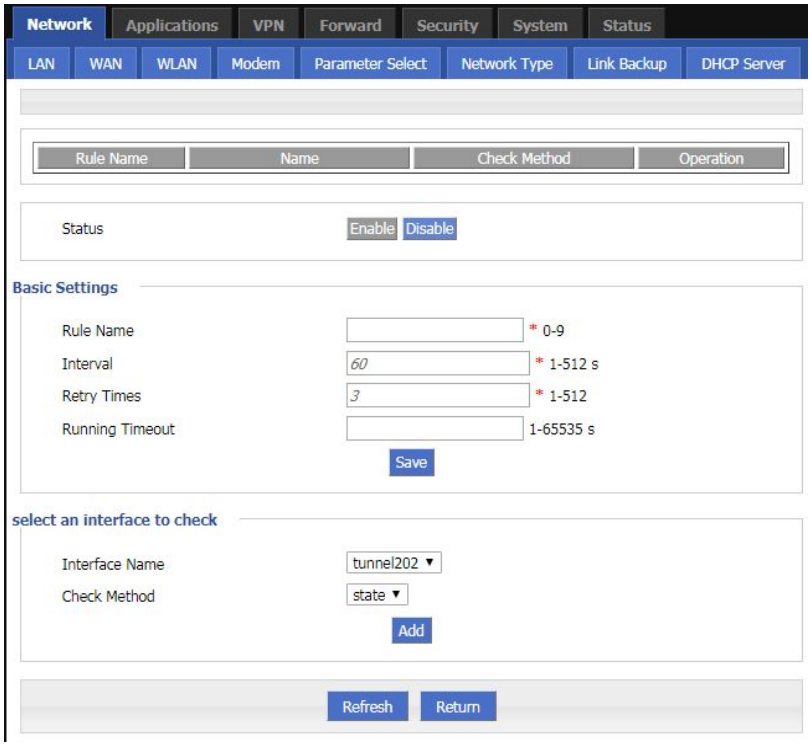
The "parameter rules" corresponding to "add", "edit", "delete", "enable", and "delete".

Action:

- Add

  1. Click “Add”. The configuration page of “Parameter Select” is displayed, as shown in Figure 5-12.

Figure 1-2 The configuration page of “Parameter Select”



2. Add a "parameter select" rule.

Table 1-1 The instruction of Parameter

Parameter	Details	Operation
Status	Enable the current rule. All enabled rules have only one rule running at a time, and the associated interfaces in all disabled rules are disabled. For example, select modem0, ipsec1, vpdn2 in rule0, and modem0, ipsec1, and vpdn2 are disabled if rule0 is disabled.	• Enable • Disable
Basic settings		
Rule name	Name identifier of a rule of parameter select , used to distinguish different rules.	Value area : [0,9]
Interval/Retry Times	The interval between detections and the maximum number of failures. If the number of failures reaches the configured number, switch to the next rule to work.	Value area : 1~512 Units: seconds/time Default: 60/3
Running timeout	It is used to limit the maximum working time of the current rule. This parameter is invalid in rule0. This parameter is configured in other rules and switches to rule0 after reaching the maximum working time. If it is not configured, it is switched in the order of rule. Configuration is not recommended when there is usually no strict master/slave requirement.	Value area : 1~65535 Units: seconds
Add interface detection rules		
Interface name	Name of the interface associated with the rule, such as the modem interface name: modem0, modem2.	The drop-down box option is automatically produced depending on the number of interface names currently configured in the system.
Check method	The detection method is divided into interface state detection and ICMP detection, and it is determined whether it is necessary to switch to the next rule by checking the status or the link (switching after reaching the maximum number of failures).	Dropdown List • state • icmp
Destination IP	It only needs to be configured when the icmp detection method is selected. It is used to configure the icmp detection destination address.	Format:A.B.C.D, please refer to the “Parameter Specification Table”for input specifications. For example: 192.168.8.2

3. Click "Add" to complete the rule addition.

- Delete
  Click “Delete” to delete the selected Parameter Select Rule.

- Enable
  Click "Enable" to enable and apply the Parameter select Rule.
- Disable

Click “Disable” to disable the Parameter Select Rule.

- Refresh
  Click “Refresh” to refresh the current page.

NOTE

To ensure that the user controls the uplink and downlink of the router, the 4G Intelligent Gateways provide multiple functions for the modem/modem2, such as parameter select, link backup, ICMP detection, task management, and trigger settings.The task management is to perform the action on the modem/modem2 and keep the state after the action is executed, and the parameter select, the link backup, and the ICMP detection all perform the action on the modem/modem2 but do not maintain the state. Therefore, the function of parameter select, ICMP detection, and task management trigger setting can only be performed on the modem/modem2 without conflict, and can be used together.
In addition, when using the parameter select and link backup functions at the same time, make sure that the two functions use different interface types. If you need to use, please contact our technical support staff.

---END

1.2.1 Network type

Provide the user with a configuration page for the default route.

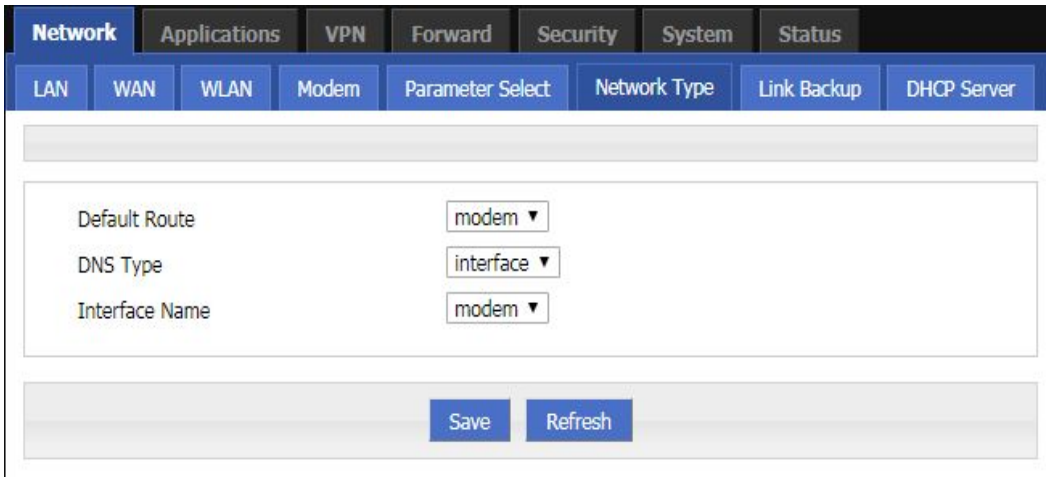
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration Interface”.

Step 2 Single click “Network > Network type”.

Open the page of “Network Type” , as shown in Figure 5-13.

Figure 1-1 the page of “Network Type”



Step 3 Configure parameters related to “Network Type”. The parameter description is shown in Table 5-6.

Table 1-1 The instruction of Parameter of “Network Type”

Parameter	Details	Operation
Default route	Default route	Dropdown List
Gateway	When the default route is wan and wan is static IP, you need to configure the next hop gateway address of the wan port address. If you need to access the domain name, you need to configure DNS.	Format:A.B.C.D Example: 192.168.10.254
DNS type	Configure the DNS type of the router. If you select an interface, you can obtain the DNS automatically by using interface dialing. If the WAN is static IP, you must manually set the DNS.	Dropdown List • interface • custom
DNS1/DNS2	Configured when the DNS type is selected as the custom. Manually configure the DNS address. You can configure up to two.	Format:A.B.C.D Example: 8.8.8.8
Interface name	Configured when the DNS type is selected as the interface. After the configuration, the router uses the DNS obtained by the interface associated with the DNS. Therefore, you need to pay special attention to whether the interface can obtain DNS.	Dropdown List • modem • eth1 • eth0 Eth0 indicates that the associated WAN port uses PPPoE dialup or DHCP to obtain DNS. Pay special attention to the eth0 is invalid when the WAN is a static IP address. If the PPP dialing configuration disables the peer DNS, the modem is invalid. eth1 indicates the DNS obtained by the WLAN.

Step 4 Single click “save” to complete the configuration of “Network Type “.

NOTE

When the "default route" selects the "eth0" interface and the WAN port is switched from DHCP or static IP to PPPoE, the default route of the router needs to click "Save" on the page of"Network Type" to take effect and display.

---END

1.2.2 Link Backup

The 4G Intelligent Gateways implement the multi-network link backup function in combination with the actual needs of the customer. They can implement mutual backup between wireless and wireless, wireless and wired links, and can quickly switch to backup when a link fails. The link ensures the connectivity and stability of the communication link of the lower computer, thus ensuring that the data service of the user is not affected. 4G

Intelligent Gateway supports both cold and hot backup modes. The advantage of hot backup is that it can communicate directly after link switching. However, the disadvantage is that communication costs will be generated when the backup link is online in real time, which increases the cost.

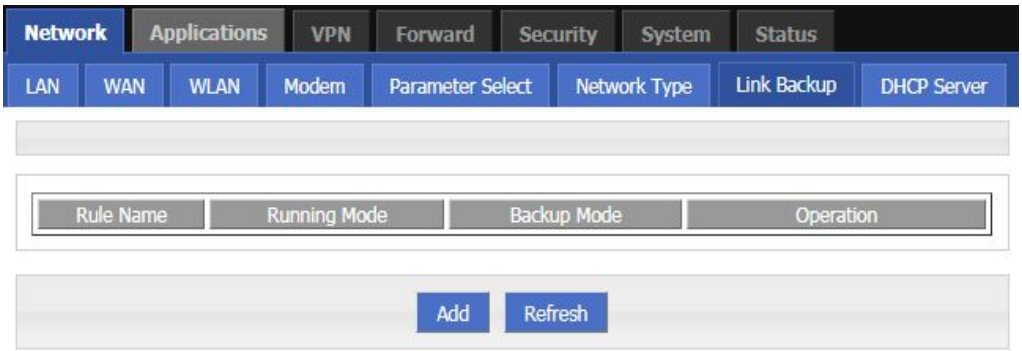
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Network>Link Backup”.

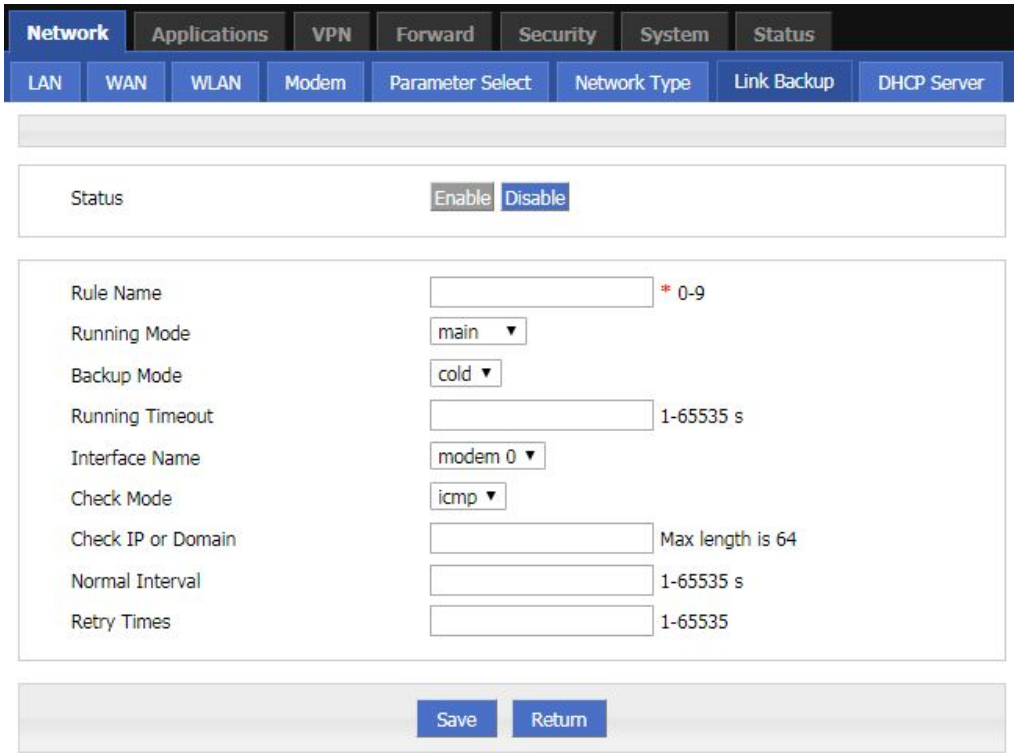
Open the page of Link Backup , as shown in Figure 5-14.

Figure 1-1 The page of “Link Backup”



Step 3 Click “Add” to open the page for adding the “Link Backup” rule, as shown in Figure 5-15.

Figure 1-2 The page for adding the “Link Backup” rule



Step 4 Configure parameters related to”Link Backup”. The parameter description is shown in Table 5-7.

Table 1-1 Link Backup Parameter

Parameter	Details	Operation
Status	Enable or Disable Link Backup feature	• Enable • Disable
Rule Name	Link Backup rule name identification Note: 0 can act as chain link or backup link, 1-9 only can act as backup link 1-9 can take the priority according to the number, the smaller the number the greater the priority	• Value area: 0-9
Running Mode	Link operate mode include: main: Link operate mode is main link backup: Link operate mode is backup link	Dropdown List • main • backup
Backup Mode	Backup mode include: cold and hot Hot refers to the corresponding link treatment enabled, the advantage of hot backup is switching fast, deficiency is when the link online will increase the cost of network overhead and charges. Cold refers to only the interface of current working link is enabled, and the others, as the interfaces of non-working link, are in offline state.	• Dropdown List • cold • hot
Running Timeout	• If the current link is main link, shows the main link stability time • if the current link is backup link, shows the shortest working time Note: Running timeout is only suitable for switching between master and slave	Value area:1-65535 Units: seconds
Interface Name	Interface used for link switching	Dropdown List • modem 0 • modem 1 • eth1 • eth0
Check Mode	Link detection mode, it supports icmp detection and wget detection mode (http)	Dropdown List • icmp • http The default mode is icmp
Check IP or Domain	Icmp: Detects the IP address or domain name through the ping packet. If the ping fails, the detection fails. Http: Detect ip address or domain name through wget mode, wget ip or domain name needs to bring http	WORD type, up to 64 characters, please refer to parameters regulation format
Interval/Retry Times	• The normal detection interval and the maximum number of failures of the link. The maximum number of failures arrives to switch the link.	• Value area:1-65535 • Units: seconds/times

Step 5 Single click “save” to complete the configuration of “Link Backup”.

NOTE

When the link backup function is enabled, the default route of the router is the default route of the link backup rule.When the link backup is the master-slave switchover, the master link is switched to the primary link as soon as the primary link is detected successfully.

---END

1.2.3 DHCP Service

The Dynamic Host Configuration Protocol (DHCP) is a network protocol for a local area network. After the DHCP function is enabled, the lower device can automatically obtain the dynamic IP.

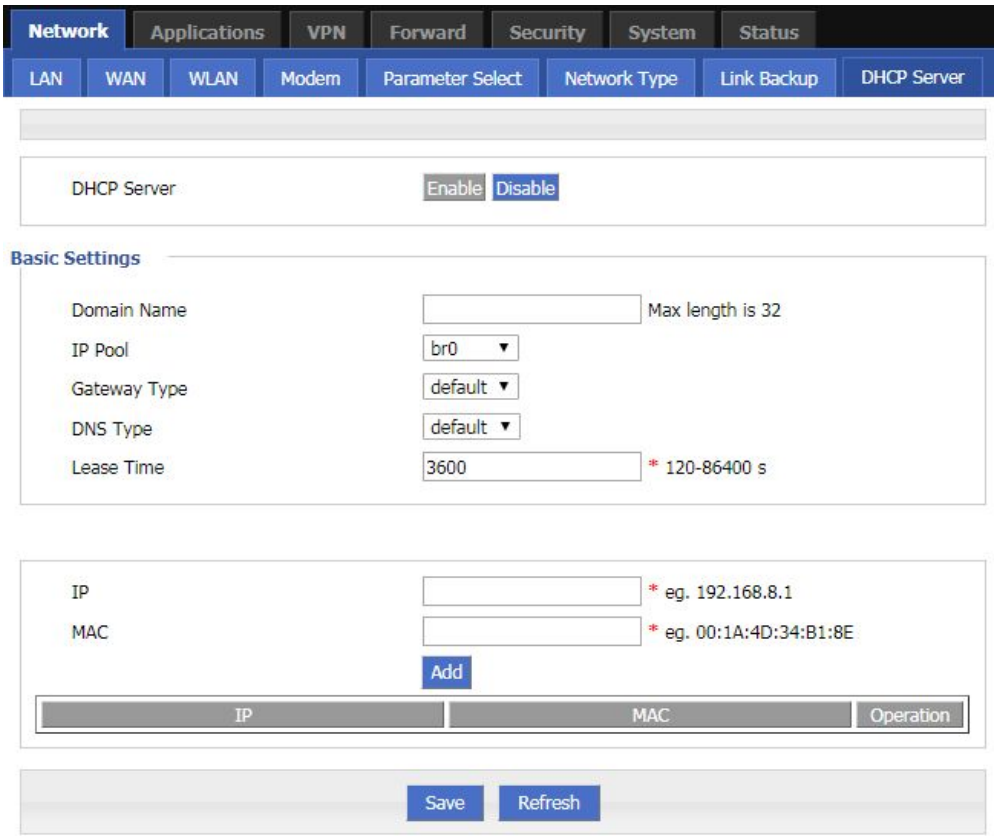
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Single click “Network > DHCP Server”.

Open the page of “DHCP Server” , as shown in Figure 5-16.

Figure 1-1 The page of “DHCP Server”



Step 3 Configure “DHCP Server” Settings.

.

Table 1-1 lists the DHCP server settings parameters

Parameter	Details	Operation
DHCP Server	Enable or Disable DHCP feature	• Enable • Disable
Basic Settings(DHCP is not recommended configure in the case of no special network requirement)		
IP Pool	The DHCP client can get the scope of IP address. The IP addresses range assigned for the DHCP client Selecting interface represents using network segment that the interface belongs to. This option can be configured to specify the IP address range of the lower machine, for example: only hope at most four machine can automatically obtain the IP	• Dropdown List • br0 • custom
Start IP	Configure the starting IP address of the DHCP address pool when the address pool is selected as custom.	Manual input Format: A.B.C.D/Mask Example: 192.168.8.2
End IP	Configure the ending IP address of the DHCP address pool when the address pool is selected as custom.	Manual input Format: A.B.C.D/Mask Example: 192.168.8.254
Gateway Type	DHCP client access gateway IP source, divided into default, br0, eth0, custom four categories, associated interface, the interface IP assigned to the DHCP client as a gateway	Dropdown List Default value: default
Gateway	When the gateway type selects custom, it is usually used when specifying the lower-end gateway IP.	Format: A.B.C.D Example: 192.168.8.1
DNS Type	DHCP client access to the DNS IP source, has a default, modem, eth0, br0, custom and so on, generally do not recommend to modify the configuration, especially under the dual modem application scenario configuration is not recommended	Dropdown List • default • modem • eth0 • br0 • custom Configuring for the default is based on DNS address which is allocated by the router itself
DNS1/DNS2	Configure the IP address of the DNS obtained by the DHCP client when the DNS type is Custom.	Format: A.B.C.D Example: 8.8.8.8
Lease Time	After the DHCP client obtain an IP on IP lease time, the client usually renegotiates obtain an IP address	Value area: 120-86400 Units: seconds

Parameter	Details	Operation
	lease time in more than half the time. IP lease time is mainly used to release idle IP to avoid that IP address resources are also occupied after the DHCP client shutdown	Default value: 3600
IP, MAC binding is used to assign a fixed MAC within the specified range of IP addresses		
IP	Binding with the specified MAC: when a DHCP client sends a DHCP request, the IP address with the client's MAC binding will be assigned to the DHCP client. The IP address will not be assigned to the other client with different MAC address even if it is not in use.	Manual input Format: A.B.C.D/Mask Example: 192.168.8.2
MAC	Configure DHCP to obtain an IP ,need to specify the DHCP client's MAC address	WORD Type MAC Format Example: 00:1A:4D:34:B1:8E

---END

1.1 Application Setting

Overview

Based on years of customer experience for different applications, besides SNMP, DDNS, 4G Intelligent Gateway has developed many functions for wireless network equipment, such as ICMP check, M2M terminal management function, task management function .

1.1.1 ICMP check

The wireless network has abnormal phenomena such as fake links (the IP address is dialed but the link is unreachable), and is usually maintained by LCP. The 4G Intelligent Gateways provide more reliable ICMP link detection in addition to this detection mode. The ICMP detection mainly detects the communication link through the ping packet detection mode, and performs the action set by the user when detecting the link abnormality, thereby realizing rapid recovery of the link and the system. The ICMP link detection is mainly used to detect the wireless link at the beginning of the design. The 4G Intelligent Gateways support the detection of tunnel links such as VPNs, support multi-rule simultaneous detection, and support up to 10 ICMP detection rules.

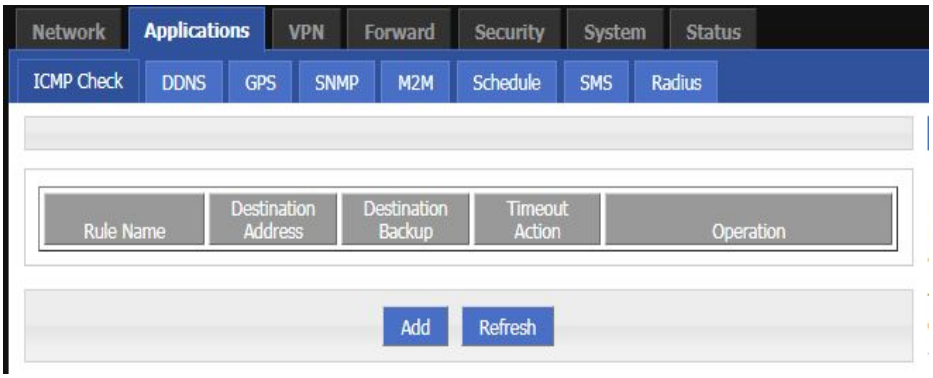
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, see “5.2.1 Logging In to the WEB Configuration page”.

Step 2 Click “applications > ICMP Check”.

Open the page of “ICMP Check” , as shown in Figure 5-17.

Figure 1-2 The page of “ICMP Check”

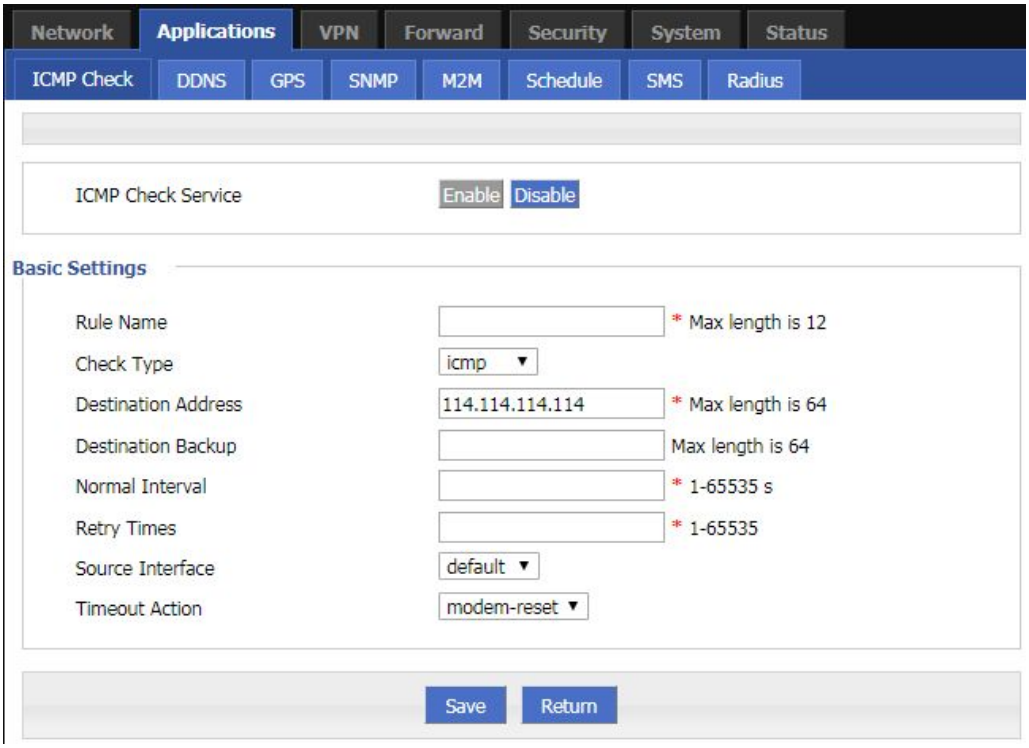


Step 3 "Add," "Edit," "Delete," "Enable," and "Disable" operations for "ICMP Detection."

Add

1. Click “Add”. The Add page of ICMP Detection is displayed, as shown in Figure 5-18.

Figure 1-3 The Add page of ICMP Detection



2. Configure parameters for the ICMP detection service. The parameter description is shown in Table 5-9.

Table 1-2 ICMP check rules Parameter instruction

Parameter	Details	Operation
ICMP check service	To enable or disable ICMP check rules, multiple rules can be used simultaneously, and one specific rule can be disabled	Button • Enable • Disable

Parameter	Details	Operation
Basic Config		
Rule Name	ICMP Check rule name, just to distinguish different rules	WORD type, max 12 bytes
Check Type	Destination address of ICMP check, it supports two methods of detecting ICMP and Domain.	Dropdown list: • icmp • domain
Destination Address	The destination address of the ICMP detection can be either IP or domain name. To set the domain name, you need to ensure that the router is configured correctly.	WORD type, max 64 bytes
Destination backup	A backup destination address of ICMP check, if “destination address” cannot be linked by ICMP check, the “destination backup” address will be checked, if still cannot linked, the router will recognize ICMP check fails	WORD type, max 64 bytes
Interval/Retry Times	Check time interval and max check failure times when link is OK, if check failure times reaches the max times, then “timeout action “ will be executed, e.g. “modem reset”	Value area : 1~65535 Unit: second/time
Source Interface	Router sends an ICMP detected packet's source address	Dropdown List options • br0 • modem • eth0
Timeout action	An action when check failure times reach max failure times. Can be modem-reset, reboot, custom	Dropdown List options • modem-reset: modem redials • modem2-reset: modem2 redials • reboot: router reboots • custom: customized action
Run commands	If “Timeout action” is “custom”, this shall be configured. Commands are BGO operation. It is not suggested to use, if need, please contact our technical engineers	WORD type, max 64 bytes

3. Single click “save” to finish the addition of a ICMP check rule.

NOTE

If the ICMP is normal, it is sent according to the ICMP detection interval. If an abnormality occurs, the ICMP packet is sent continuously according to the abnormal ICMP detection. If the detection destination address is unreachable, the backup address is detected. If the number of times the backup address fails to be detected also reaches the number of retransmissions, the router performs a "timeout action".

- Modify

As shown in Figure 5-18, determine a parameter configuration record and click Modify to modify the parameter record. The parameter description is shown in Table 5-9.

- Delete
  As shown in Figure 5-18, determine a parameter configuration record and click Delete to delete the parameter record.
- Enable
  As shown in Figure 5-18, determine a parameter configuration record and click Enable to enable the parameter record.
- Disable
  As shown in Figure 5-18, determine a parameter configuration record and click Disable to disable the parameter record.
- Refresh
  Click “refresh” to refresh the current page.

---END

1.1.2 DDNS configuration

DDNS is an abbreviation of Dynamic Domain Name System. The DDNS protocol provides a corresponding query function between dynamic IP and domain name. DDNS allows users to access the router's page through a domain name on any PC that can connect to the public network. Of course, the network corresponding to the SIM card used by the router must be a public network accessible address, so that the domain name can be accessed to access the router.

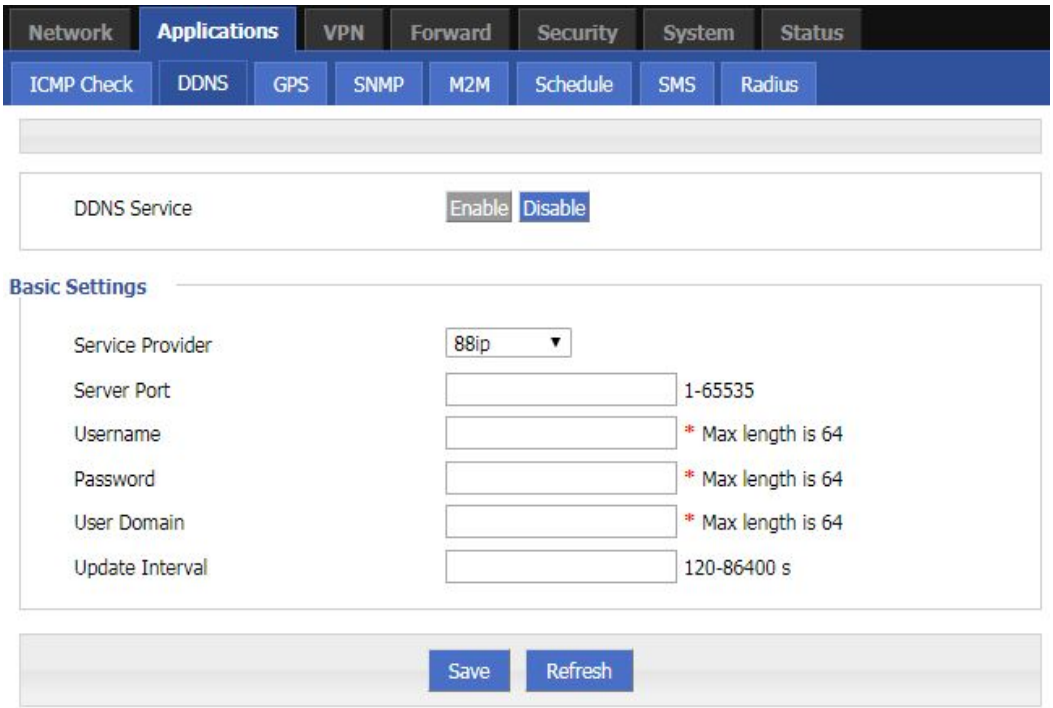
Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Applications” > “DDNS”.

Open the page of DDNS , as shown in Figure 5-19.

Figure 1-4 The page of DDNS



Step 3 Configure DDNS parameter. The parameter description is shown in Table 5-10.

Table 1-3 DDNS Parameter instruction

Parameter	Details	Operation
DDNS Service	Set whether enable DDNS service function	Button • Enable • Disable
Basic Config		
Service Provider	Select the DDNS service provider that router currently supports, don't support other providers	Dropdown List options • 322 • 88ip • dnsexit • dyndns • zoneedit • changeip • noip • dnsomatic • duckdns
Token	Enter when the Service Provider selects duckdns	Word type,Maximum 64 bytes.
Server Port	Set the port number of the DDNS server provided by the service provider. The default port number is 80	Value area: 1~65535 If empty, it means 80 port

Parameter	Details	Operation
Username/Pass word	Set user name/password of the DDNS service registered in the service provider	Normal WORD type/CODE type, Maximum 64 bytes.
User Domain	Set the domain of the DDNS service provided by the service provider	Normal WORD type, max 64 bytes
Update Interval	Set the interval of the DDNS client obtains new IP, suggest 240s or above	Value area: 120~86400 Unit: seconds

Step 4 Click “Save” to complete the configuration of DDNS.

NOTE

DDNS in China: 88IP (www.88ip.net), 3322 (www.3322.org)
DDNS outside of China: DNSEXIT (www.dnsexit.com), ZONEEDIT (www.zoneedti.com), CHANGEIP (www.changeip.com), DYNDNS (www.members.dyndns.org), NOIP (freeddns.noip.com), DNSOMATIC (www.dnsomatic.com), DUCKDNS (www.duckdns.org)
The IP address obtained from the SIM/UIM card service provider changes each time the router is restarted. If the user uses the DDNS domain name when logging in to the router remotely, the user can log in to the router page regardless of how the router's modemIP address changes.

---END

1.1.3 GPS configuration

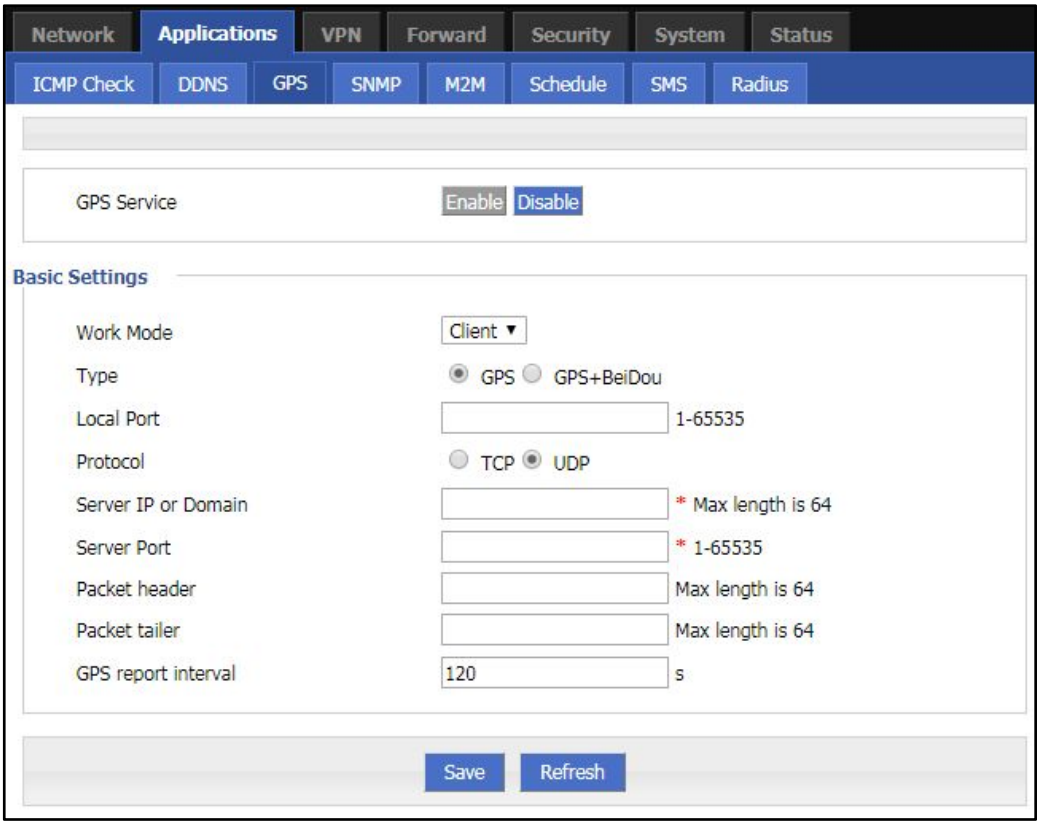
GPS (Global Positioning System) global positioning system for the geographical location of equipment, generally used in conjunction with electronic maps, can be used to monitor mobile vehicles or theft.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Applications >GPS” to open the page of “GPS”,as shown in Figure 5-20 .

Figure 1-5 The configuration page of “GPS”



Step 3 Configure GPS parameter.

Table 1-4 The instruction of GPS Parameter

Parameter	Details	Operation
GPS Service	Enable GPS service.	Radio button selection. • Enable • Disable
Basic settings		
Work Mode	The working mode of the router GPS function, the default "Client".	Drop-down box selection.
Type	GPS data positioning type selection, support GPS and GPS+BeiDou two ways	• Radio button selection. • GPS • GPS+BeiDou Only when the module type is EC25 series, the page can select GPS+BeiDou
Local Port	The router specifies the port used to report GPS data.	Value range: 1 to 65535
Protocol	The protocol used by the router for GPS data transmission. • TCP • UDP	Radio button selection

Parameter	Details	Operation
Server IP or Domain	IP address or domain name of the GPS server.	Format: A.B.C.D or word type
Server Port	The port used by the GPS server.	Value range: 1 to 65535
Packet header	Set the content in the GPS data message data header	Enter it manually. Maximum input length: 64 bits
Packet tailer	Setting content at the end of the data of the GPS data message	Enter it manually. Maximum input length: 64 bits
GPS report interval	GPS data packet transmission interval	Enter it manually. Value range: 1 to 65535 Unit: second Default 120

Step 4 Single click “save” icon to finish the configuration of GPS.

NOTE

Need to use with GPS antenna

---END

1.1.4 DTU configuration

H8922SS 4G Intelligent Gateway system has built-in communication function with registration center and data center, which can provide similar DTU (Data Transfer Unit), which is used to convert serial port data into IP data or convert IP data into serial port. The wireless terminal device that transmits data through the wireless communication network has the function of transparent data transmission function, and also provides a buffer function to avoid packet loss caused by switching after the data center is switched.

Step 1 Log in to the H8922SS 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Applications >DTU” to open the page of “DTU”,and select different working modes, as shown in Figure 5-21, and Figure 5-22.

CAUTION

- When you select Client in Work Mode, the Data Center Settings tab and the Heartbeat Settings tab are displayed, as shown in Figure 5-21.
- When”DDP Client”is selected in “Work Mode”, the “Data Center Settings”tab and the “Heartbeat Settings” tab will be displayed, and the parameter “Identity Code”will be displayed in “Basic Settings”, corresponding to Figure 5- 22.
- DDP client mode supports TCP and UDP protocols.
- Support TCP, UDP, MQTT when "client mode" is selected in "working mode"

Figure 1-6 The configuration page of DTU server

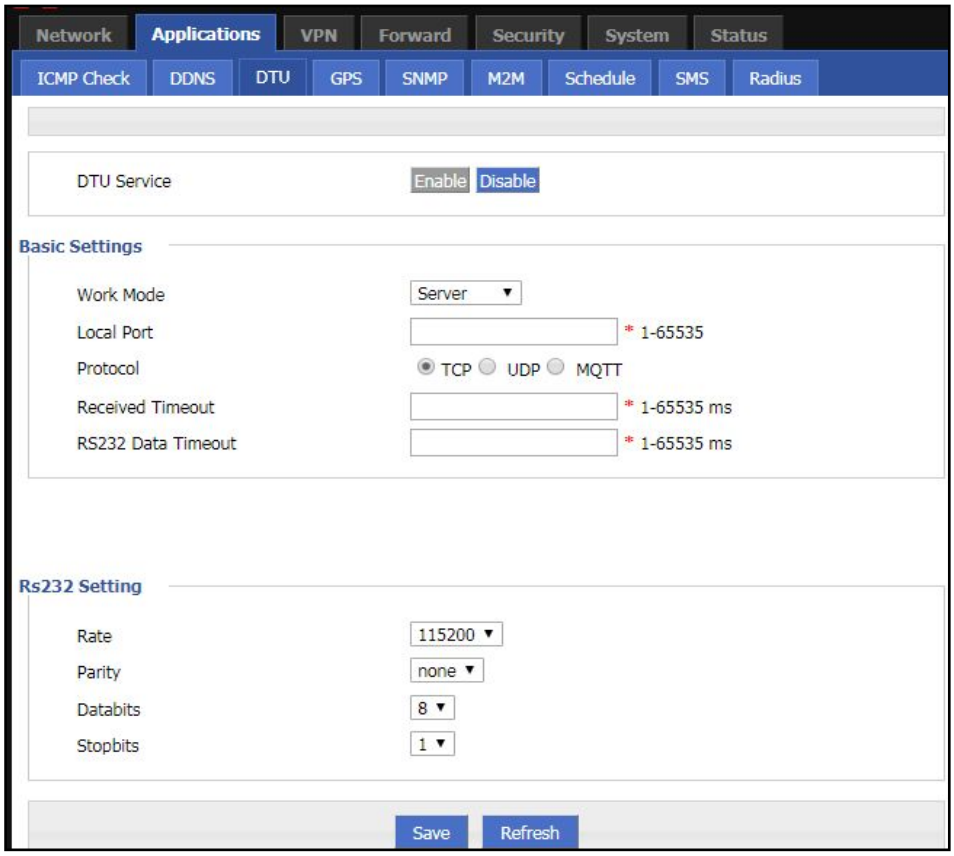


Figure 1-7 The configuration page of DTU client

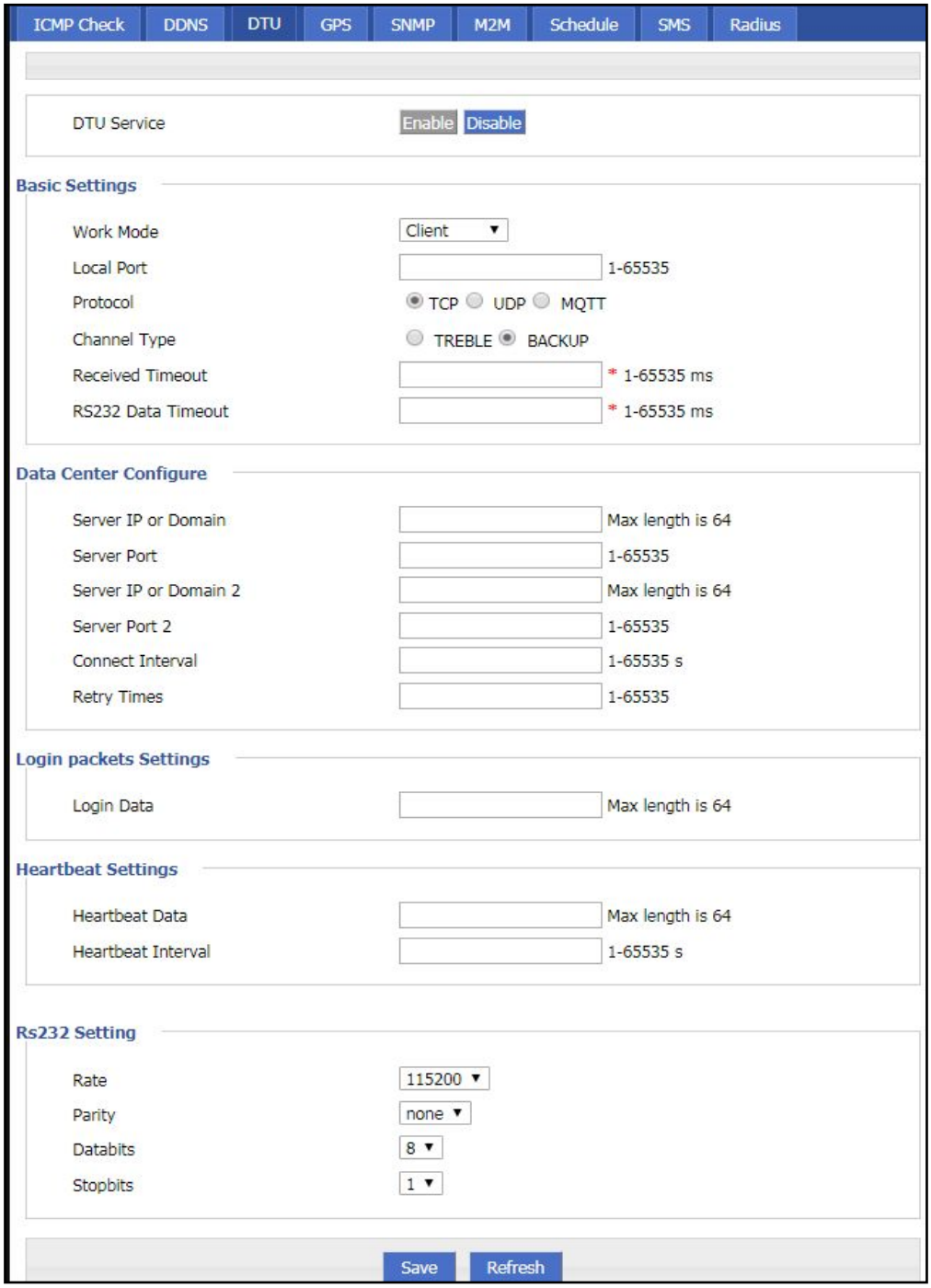
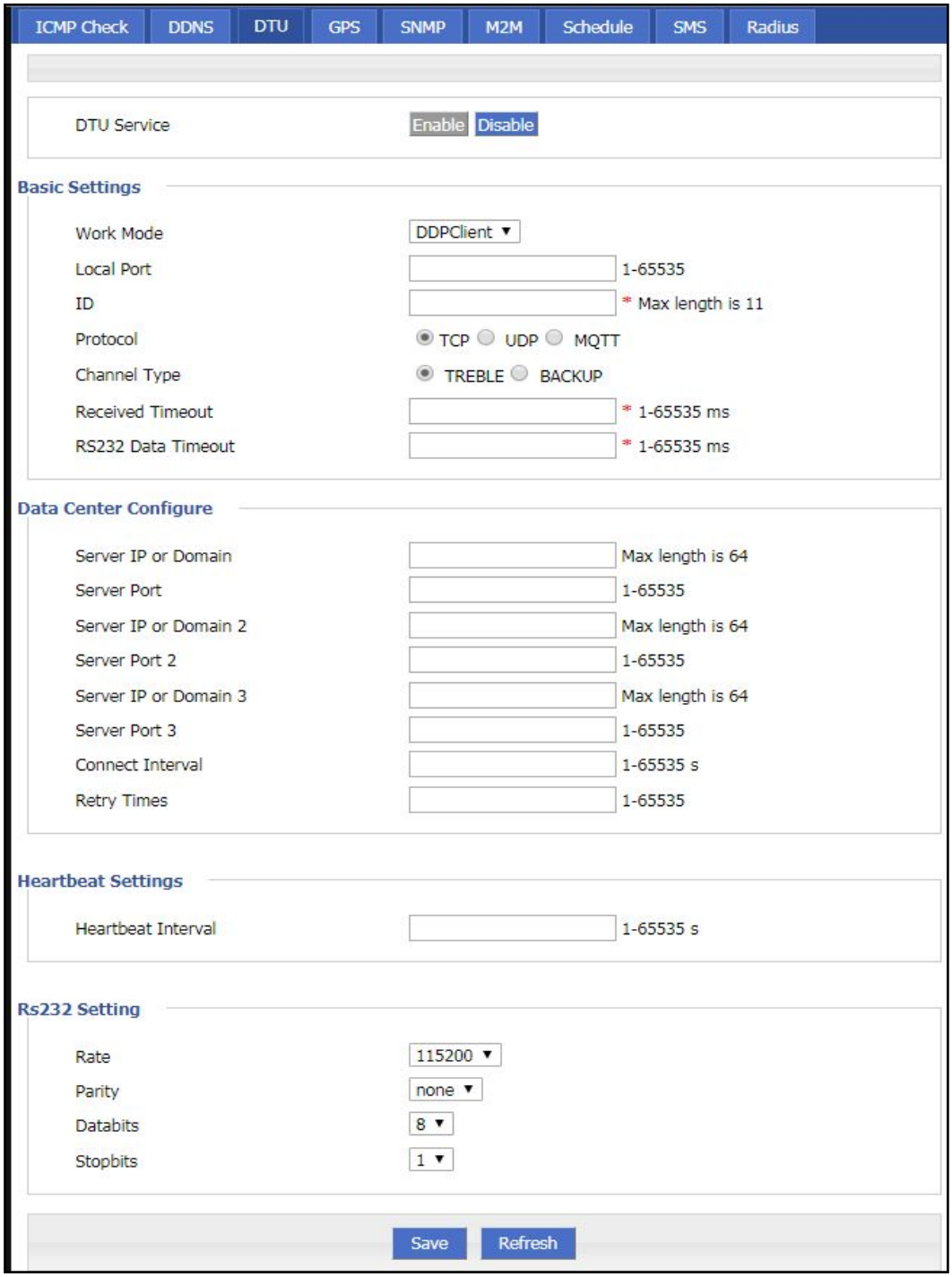


Figure 1-8 The configuration page of DDP



Step 3 If the DTU works in the server working mode, you need to configure the DTU as the parameter in the server working mode, as shown in Figure 5-20.

Step 4 If the DTU works in the client/DDP client working mode, set the "working mode" to "DTU client" or "DDP client" and configure the corresponding parameters. As shown in Figure 5-21 and Figure 5-22. The parameter description is shown in Table 5-12.

Table 1-5 The instruction of DTU Parameter

Parameter	Details	Operation
DTU Service	Enable/disable the DTU service.	Single box Enable Disable
Basic settings		
Work Mode	DTU working mode, can be set to: ● Server: The router is used as a DTU server. ● Client: The router is used as a DTU client. ● DDP client: The router is used as a DDP client (the DDP protocol is our proprietary protocol).	Dropdown list selection: Server Client DDPClient
Local Port	The service port of DTU.	Enter it manually. Range 1-65535
ID(Attributes that need to be configured when the working mode is selected as the DDP client)	The identifier of the terminal used to distinguish the client of the DTU.	Manual input, the maximum length does not exceed 11 digits. WORD type
Protocol	The setting of the data transfer protocol type. TCP: The TCP protocol is a connection-oriented and reliable transmission protocol, which is suitable for occasions with high reliability requirements and low sensitivity to communication efficiency. UDP： The UDP protocol is a non-connected unreliable transmission protocol. It is applicable to scenarios where the efficiency requirements are relatively high and the reliability requirements are relatively low.。 MQTT： MQTT is a TCP-based publish-subscribe protocol. The initial purpose of the design is to provide extremely limited memory devices and network-unreliable communication with low network bandwidth, which is very suitable for IoT communication. MQTT can only be selected when it is in Client mode.	Radio button selection. You can choose according to your own needs.
Channel Type	The setting of data transfer channel type ● Three Centers: The three-center channel means that three main channels can be set, which can be online at the same time; the three channels are independent of each other. If channel 1 fails, it will not affect the communication of the other two channels. ● Active/standby: The active and standby channels refer to the DTU that can set a primary channel and a standby channel. When the primary channel fails, the DTU will automatically switch to the standby channel. When the standby channel has no data to send, it will try to connect to the primary channel again.。	Radio button selection. You can choose according to your own needs.

Parameter	Details	Operation
Received Packet Max Length	When the DDP client is selected as the working mode, it needs to be configured to indicate the maximum length of the packets that can be received when the UDP+DDP protocol is communicated. If the sent packet exceeds the maximum length, the DDP client discards the excess packet.	Enter it manually. Value range: 1 to 65535 Unit: Byte.
Received Timeout	The wait timeout for the DTU serial port to receive data from the data center. Read data within this time within the maximum packet length of the received packet. If there is data, it will be read all the time, and the data read during this time will be displayed at one time; if there is no data, it is greater than the timeout period. Then it is considered that the data is read and displayed to the DTU port serial port tool.	Enter it manually. Value range: 1 to 65535 Unit: milliseconds
RS232 Data Timeout	The waiting time for the DTU serial port to send data to the data center. If the data sent in this time has exceeded the maximum packet length of the UDP/TCP received packet, it will be sent immediately; if the maximum packet length of the UDP/TCP received packet is not exceeded, the data is waited until the last packet idle time is reached. And then send it together.	Enter it manually. Value range: 1 to 65535 Unit: milliseconds
Data center settings [Parameters only need to be configured in the "client", "DDP client" working mode] Note: When the working mode is "client" and the "transport protocol" is "TCP", you need to configure "service address 2" and "service port 2" when the working mode is "DDP client".		
Server IP or Domain	The IP address or domain name of the DTU Data Center Server (DSC).	Format:A.B.C.D Word type
Server Port	The port number of the DTU data center (must be the same as the service port set by the server).	Enter it manually. Range 1-65535
Server IP or Domain 2	The IP address or domain name of the DTU Data Center Server (DSC), used to reserve each other with the "Service Address".	Format:A.B.C.D Word type
Server Port 2	The port number of the DSC data center (must be the same as the service port set by the server).	Enter it manually. Range 1-65535
Server IP or Domain 3	The IP address or domain name of the DTU Data Center Server (DSC), used to reserve each other with the "Service Address".	Format:A.B.C.D Word type
Server Port 3	The port number of the DSC data center (must be the same as the service port set by the server).	Enter it manually. Range 1-65535
Connect Interval	The interval at which the client DTU and the server re-establish a connection after the connection fails.	Enter it manually. Value range: 1 to 65535 Unit: second
Retry Times	The maximum number of times the client DTU and the server try to connect after the connection fails.	Enter it manually. Value range: 1 to 65535 Unit: times
MQTT settings		
Broker Address	Message proxy server address	Enter it manually. Value range: up to 64

Parameter	Details	Operation
		characters
Broker Port	Message proxy server corresponding port	Enter it manually. Value range: 1 to 65535
Username/Password	Used for MQTT user authentication	Enter it manually. Value range: up to 64 characters
Client ID	The unique identifier of the client, the server is used to associate a session.	Enter it manually. Value range: up to 64 characters
Publish Topic	The topic is published, and the client that subscribes to the topic can receive the data published by the client.	Enter it manually. Value range: up to 64 characters
Subscribe Topic	Subscribe to the topic, you can receive the data from the client that posted the topic.	Enter it manually. Value range: up to 64 characters
QOS	QoS 0: "At most once", message publishing relies entirely on the underlying TCP/IP network. Messages distributed may be lost or duplicated. QoS 1: "At least once" to ensure that the message can arrive, but the message may be repeated. QoS 2: "Only once", ensuring that the message arrives only once.	The user selects the corresponding QOS level according to the actual scene.
Keepalive	.The goal is to maintain the reliability of the long connection and the confirmation of whether the two parties are online. .The client sets the duration of Keep Alive when connecting. If the server does not receive the client's message within 1.5 * KeepAlive time, it must disconnect the client's network connection.	Enter it manually. Value range: 5 to 120 Unit: second
Heartbeat settings		
Heartbeat Data	Set the heartbeat to send content (when no data is sent, every time the heartbeat time, the router sends the content once)	Enter it manually. Maximum input length: 64 bits
Heartbeat Interval	Set the interval for heartbeat sending (when no data is sent, the router will send heartbeat content every other time)。	Enter it manually. Value range: 1 to 65535 Unit: second
Serial port parameter setting (mainly used for correct connection between devices connected to the DTU port)		
Rate	The data transfer rate of the serial port.	Drop-down list selection. Set according to the actual serial port requirements of the DTU. Default: 115200
Parity	The way the data is verified.	Drop-down list selection. Set according to the actual serial port requirements of the DTU. Value range: None, Odd,

Parameter	Details	Operation
		Even Default: None (no parity)
Databits	Data transfer bit.	Drop-down list selection. Set according to the actual serial port requirements of the DTU. Value range: 5, 6, 7, 8 Default: 8
Stopbits	Data stop bit	Drop-down list selection. Set according to the actual serial port requirements of the DTU. Value range: 1, 2 Default: 1

1.1.5 SNMP configuration

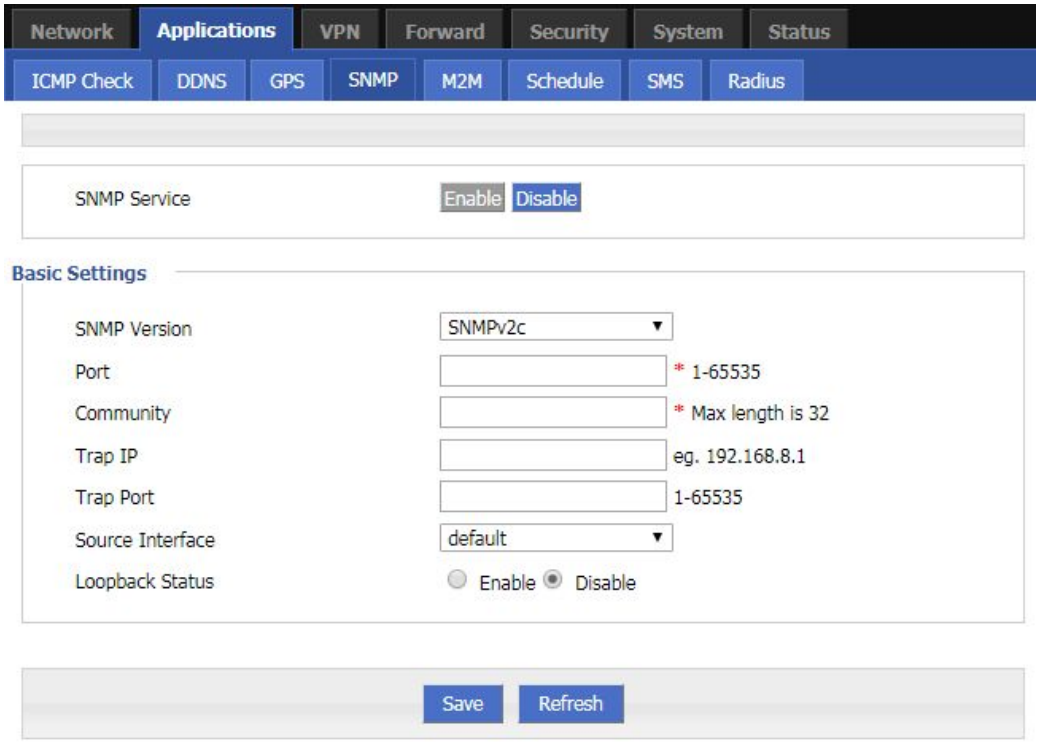
SNMP(Simple Network Management Protocol)can monitor routers remotely and get to know the status of routers (Support interface status check, like VPN, modem etc. MIB of our company shall be used).

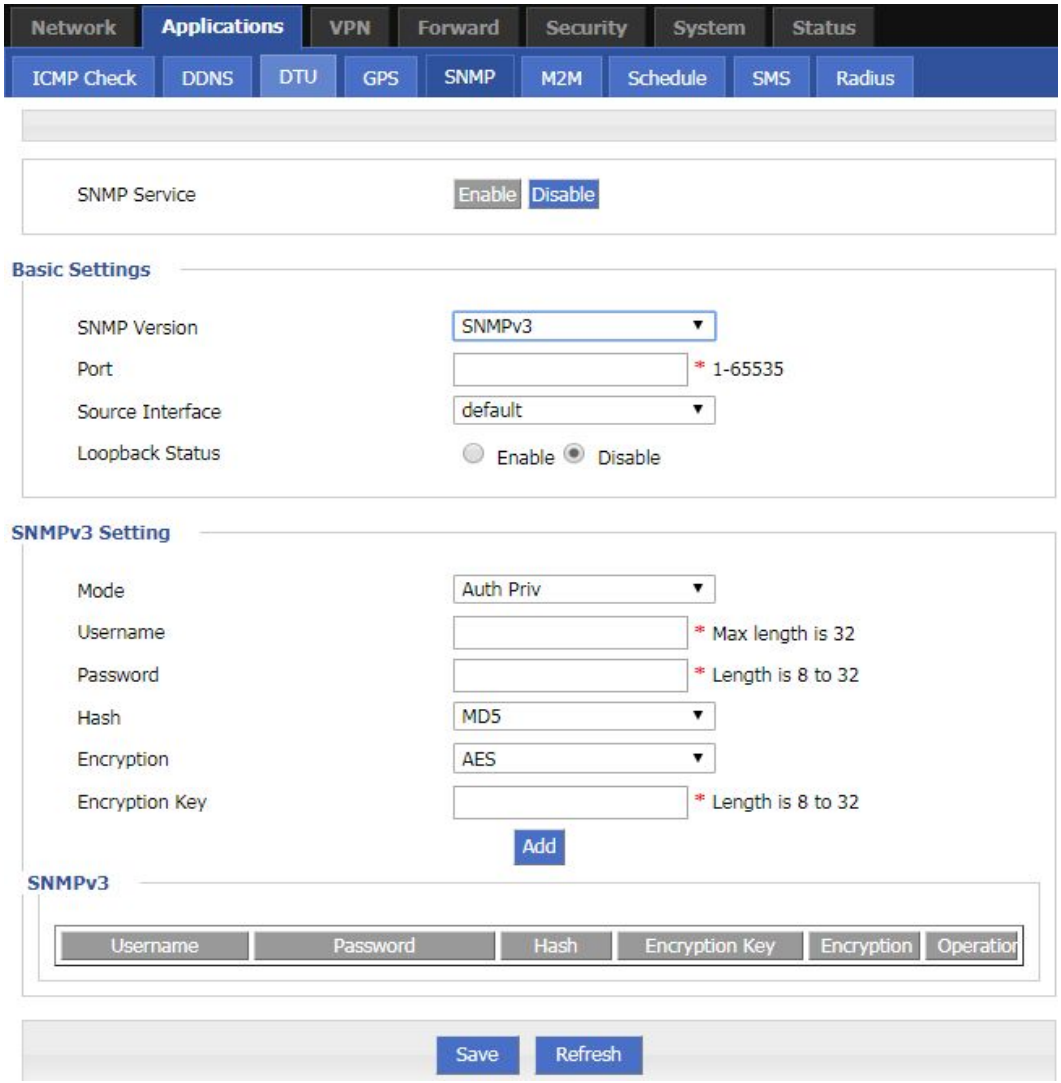
Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Applications >SNMP” to open the page of “SNMP”, as shown in Figure 5-21 .

Figure 1-9 The configuration page of "SNMP"(the V2 version configuration page above, the following figure is the V3 version configuration page)





Step 3 Configure SNMP parameter.

Table 1-6 The instruction of SNMP Parameter

Parameter	Details	Operation
SNMP service	To enable or disable SNMP service	Options: • Enable • Disable
Basic Config		
SNMP Version	SNMP version setting, support for SNMPV2c and SNMPV3	Dropdown list: • SNMPV2c • SNMPV3
Port	SNMP port, suggest to be default port161	Value area: 1~65535 Default: 161
Community	The community password of the SNMP service that the SNMP client connects to the	WORD type, Maxium 32 bytes

Parameter	Details	Operation
	router for identification	
Trap IP	Link-state router report server address	Manual input Format: A.B.C.D/Mask
Trap Port	Link-state router report server address's port	Value area: 1~65535 Default: 162
Loopback Status	Match with "LAN" page loopback address, in the "Loopback Status" to "Enable", means loopback address configuration successfully, the router reported Trap IP packet source address is the loopback address, If the "Loopback Status" to "Disabled" means router IP packet source address for the LAN port address	Options: • Enable • Disable
Source Interface (configured when SNMP version is selected for SNMPV3)	Used to specify the source address of the message packet when communicating with the SNMP tool.	Dropdown list: • default • br0 • modem • eth0
SNMPv3 Setting		
Mode	SNMP authentication encryption mode selection, support 3 modes: authentication + encryption, authentication + no encryption, no authentication + no encryption	Dropdown list: • Auth Priv • Auth NoPriv • NoAuth NoPriv
Usname/Password	User username and password authentication. The entered username and password must be the same as those set on the SNMP tool. Otherwise, the connection cannot be made.	Enter it manually. Username ranges from 1 to 32 characters. Password value range 8~32 characters
Hash (when Mode selects Auth Priv or Auth NoPriv, enter it)	Authentication mode selection, support MD5 and SHA	Dropdown list: • MD5 • SHA
Encryption (when Mode selects Auth Priv, enter it)	Encryption mode selection, support AES and DES	Dropdown list: • AES • DES
Encryption Key (enter when Mode selects Auth Priv)	Used to encrypt and decrypt data with the snmp tool	Enter it manually. The value ranges from 8 to 32 characters.

Step 4 Single click "save" icon to finish the configuration of SNMP.

NOTE

Trap: One of the five data types of the SNMP protocol, which refers to the trap message reported by the managed device, indicating that the device is faulty or changed. 4G Intelligent Gateway reports the type and content of the trap including: modem connection status and which interface, which SIM card dial, VPDN/TUNNEL/IPSec interface connection and disconnection.
The MIB library corresponding to SNMP can be downloaded from our website. If necessary, please contact our technical staff.

---END

1.1.6 M2M configuration

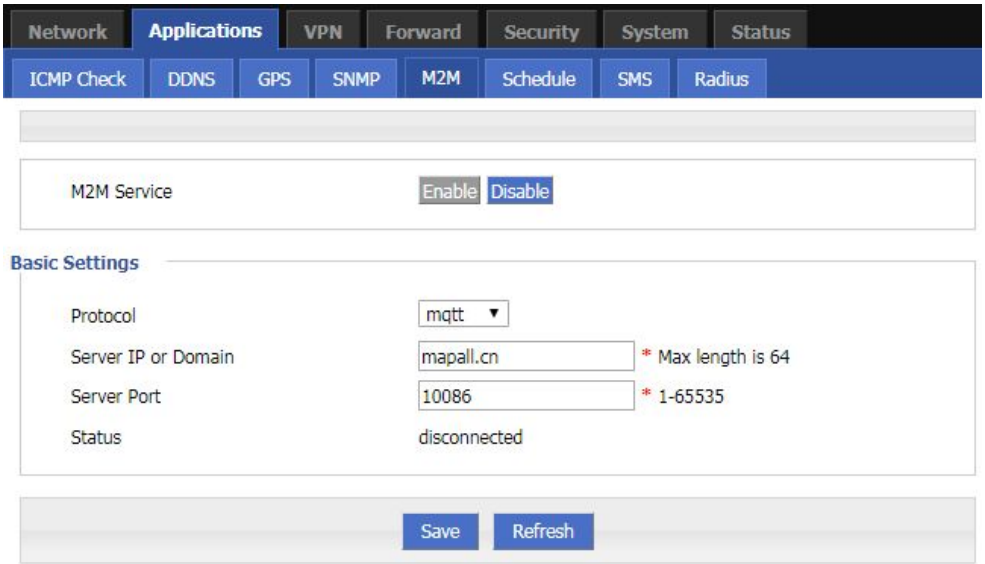
4G Intelligent Gateway has embedded a WMMP (Wireless Machine-to-Machine Protocol) protocol to realize communication with M2M (Machine-to-Machine) platform which can remotely monitor and manage the routers and its network, e.g. visit the router, patch upgrading, firmware upgrading, parameter configuration, monitor the network strength, time delay, flow. Its configuration is as follows:

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Applications > M2M” to open the page of “M2M” configuration. See below:

Figure 1-10 The page of “M2M” configuration



Step 3 Configure M2M parameter. Parameter instruction is shown in Table 5-13.

Table 1-7 The instruction of M2M Parameter

Parameter	Details	Operation
M2M service	To enable or disable M2M function. This function shall be used with our M2M platform	Button • Enable • Disable
Basic Config		

Parameter	Details	Operation
Protocol	Data transfer protocol selection between device and M2M platform	Dropdown list: • Mqtt • wmmp
Server IP or Domain	Set the server IP or domain of M2M platform	Normal WORD type, max 64 bytes
Server Port	WMMP port No, shall be the same with Port No of M2M platform server	Value area: 1~65535
Source Interface (selected when the protocol selects wmmp)	The source interface carried by the data communication between the router and the M2M platform. When using this function, you need to turn off the MASQ function, otherwise the message will be sent to change the source IP.	Dropdown list: • default • br0 • Modem • eth0
Status	Display the connection status	Connected to the platform shows connected, not connected to the platform, it shows disconnected

Step 4 Single click “save” icon to finish the configuration of “M2M”.

---END

1.1.7 Schedule configuration

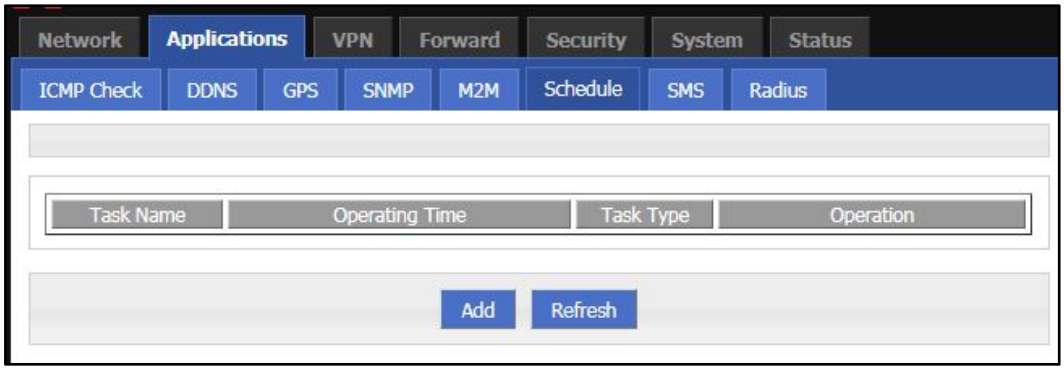
This application is to control the online time of the router to better manage network and save 3G/4G/5G flow. can add several online periods as per the user’s requirement (e.g. hours of some day). in addition, this application can support to begin some tasks at a time point (e.g. redial or reboot at 00:00). Supports up to 10 task rules.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

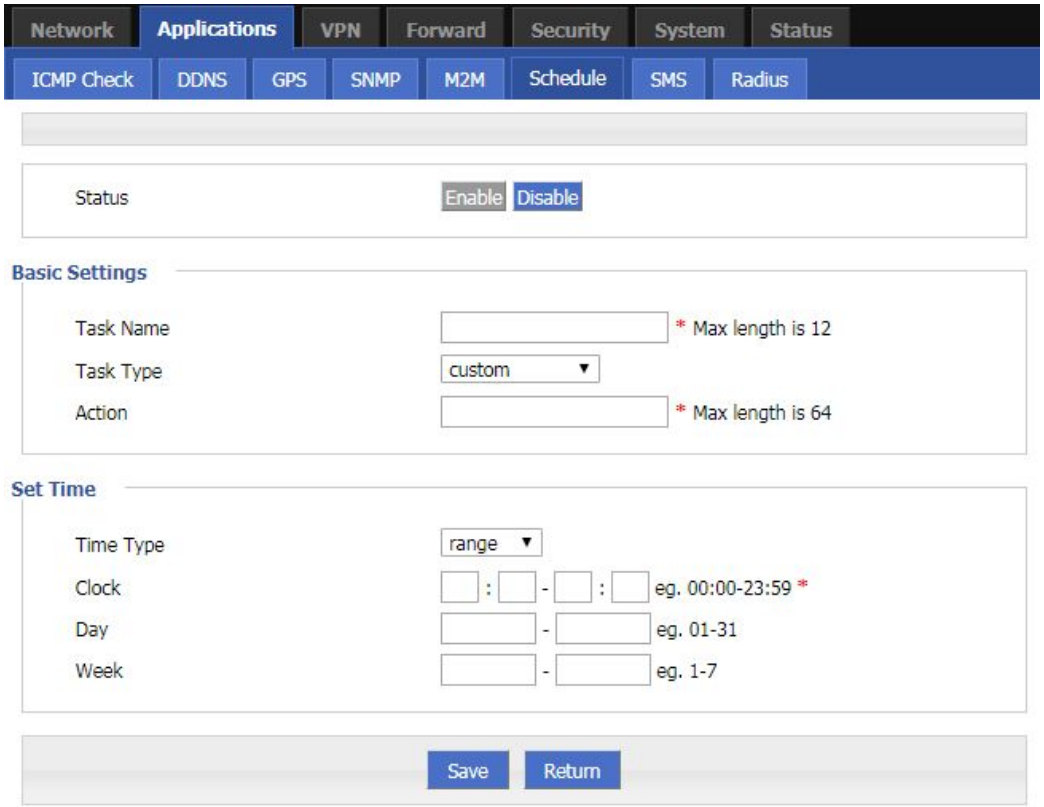
Step 2 Click “Applications > Schedule” to open the configuration page of “Schedule”.As shown in Figure 5-23.

Figure 1-11 The configuration page of "Schedule"



Step 3 To add a new task management rule, click "Add" to enter the task management rule settings page, as shown in Figure 5-24.

Figure 1-12 Task management rule settings page



Step 4 Configure task management rule parameters.

Table 1-8 Timing task parameter instruction

Parameter	Details	Operation
Status	Enable timing rules. Multiple rules can be run at the same time, or one rule can be disabled. In addition to the time-interval type of action tasks, other functions need to be used together with the NTP service. Otherwise, it is difficult to achieve	options • Enable • Disable

Parameter	Details	Operation
	reasonable time task control.	
Basic Config		
Task name	Name of a timing task	Maxium 12 bytes
Task type	Task type has action task and status task. Action task is for time point or time interval, while status task is for time period (for “modem-online” and “modem2-online”), which means that the modem will be online (if down, modem will automatically redial) during the configured time period. Modem will be offline (no dialing) for other time	Dropdown List options: • modem-online • modem2-online • reboot • custom if select “custom”, “schedule” will be shown to input command (can be dialup or other command). Maxium 64 bytes
Action	The command is a background operation command, which is usually not recommended. If you need to configure it, please contact our technical staff.	WORD type. Maxium 64 digits
Set time		
Time type	Range or interval for status task or action task	Dropdown List options: • range • interval
When “time type” select “range”		
Clock	To input hour and minute. When beginning and end hour and minute are the same, it means a time point for action task	Value area: [00:00,23:59] Format: HH:mm-HH:mm
Day	Days in a month for task	Value area: [01,31] Format: XX-XX
Week	Days in a week for task. When “day” and “week” are both input, it means only if both conditions meet, the task will begin	Value area: [1,7] Format: X-X 1 for Monday
When “time type” select “Interval”		
Interval	Time interval for action task	Value area: 1~65535 Unit: minutes

Step 5 Single click “save” icon to finish the configuration of “Schedule”.

When the time type of the task management is "range", you must first enable "system time", that is, the NTP service (task management does not support manual time); if the

time type is "interval", you do not need to enable "system time". To use "System Time",please see "5.7.4 System Time".

Due to the stability of the modem, the router has multiple functions for modem operation, such as task management, parameter switching, link backup, ICMP detection, trigger setting. where task management is to change the modem state, while other functions are Change the modem status but do not keep it, so please take into account other functions when using task management. If necessary, please contact our technical staff.

---END

1.1.8 SMS Settings

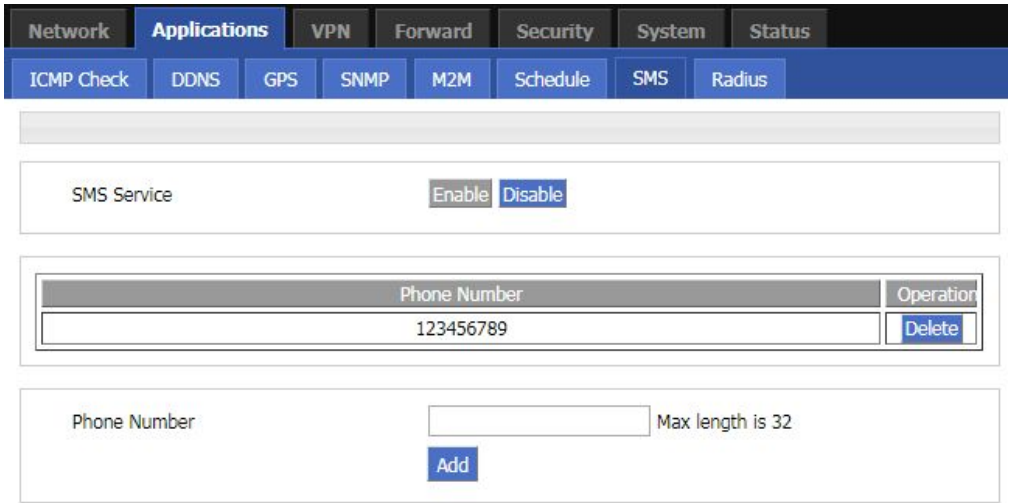
4G Intelligent Gateway SMS settings can enable the device SMS function. The mobile phone can use the SMS command to the device for information query, command configuration, and device restart. This feature is intended for users who are not comfortable with the device and who need to operate the device. This function can add a trust number, and the device will execute only the command issued by the added number. You can add up to 20 trust numbers.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Applications > SMS” to open the configuration of “SMS”.As shown in Figure 5-25.

Figure 1-13 The configuration of “SMS”



Step 3 Configure “SMS” parameter.

Table 1-9 The instruction of SMS Parameter

Parameter	Details	Operation
SMS Service	Turn on/off SMS service	Dropdown list: • Enable • Disable
Phone Number	Add a trust number, and only the added number can use the service	Enter it manually. The maximum length is 32 bits. For the input

Parameter	Details	Operation
	provided by the SMS function.	specifications, please refer to the “Parameter Specification Table”.

Step 4 Click "Add" to add the entered trust number

Step 5 Click delete to delete the added trust number.

NOTE

When no trust number is added, the SMS service function can be used for any mobile phone number;when there is a trusted number, only the trusted number can use the SMS service function.

---END

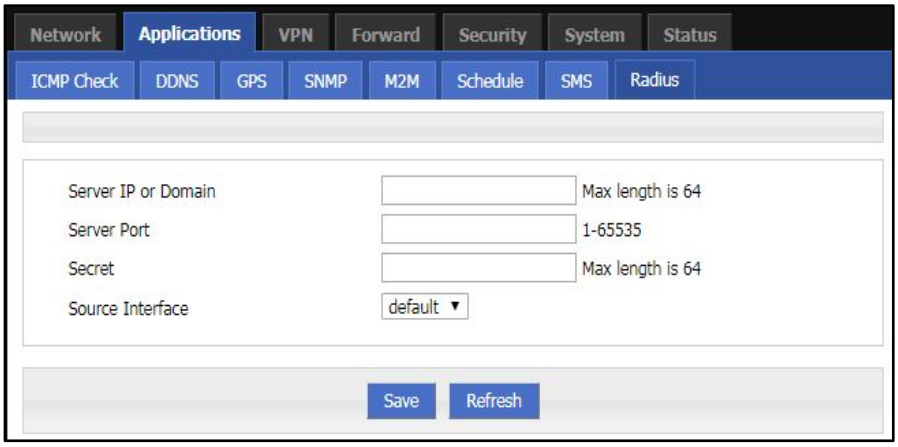
1.1.9 Radius settings

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Applications > Radius” to open the page of “Radius” .As shown in Figure 5-26.

Figure 1-14 The configuration page of Radius



Step 3 Configure the parameters of Radius.

Table 1-10 The instruction of Parameter of Radius

Parameter	Details	Operation
Server IP or Domain	Radius server address, support ip and domain	Enter it manually. Supports up to 64 characters. format i: A.B.C.D, the domain name is entered in the correct format of the domain name.
Server Port	Radius server listening port	Enter it manually. Input range: 1~65535
Secret	Communication key	Enter it manually.

Parameter	Details	Operation
	with the Radius server	Supports up to 64 characters
Source Interface	Server IP or domain for getting the GPS data	The source interface IP carried by the communication message with Radius, the MASQ function needs to be disabled when using this function, otherwise the source IP may be changed.

Step 4 Single click “save” to finish the configuration of “Radius”.

---END

1.2 Security Configuration

Overview

Security settings refer to the firewall function of the router and the prevention of network attacks.4G Intelligent Gateway supports five security settings: IP filter, domain filter and MAC address filter, Remote Access and network attacks.The user compares the IP address/port, MAC address, and domain name of the incoming router packet with the firewall rule added by the user, and performs a accepting or dropping action on the data packet matching the firewall rule to allow or prohibit certain network segment accesses the external network and allows/drops other users from accessing the router.And determining whether the data packet is a legitimate data packet by the characteristics of the received data packet to achieve the purpose of the device being free from network attacks.

1.2.1 IP Filter

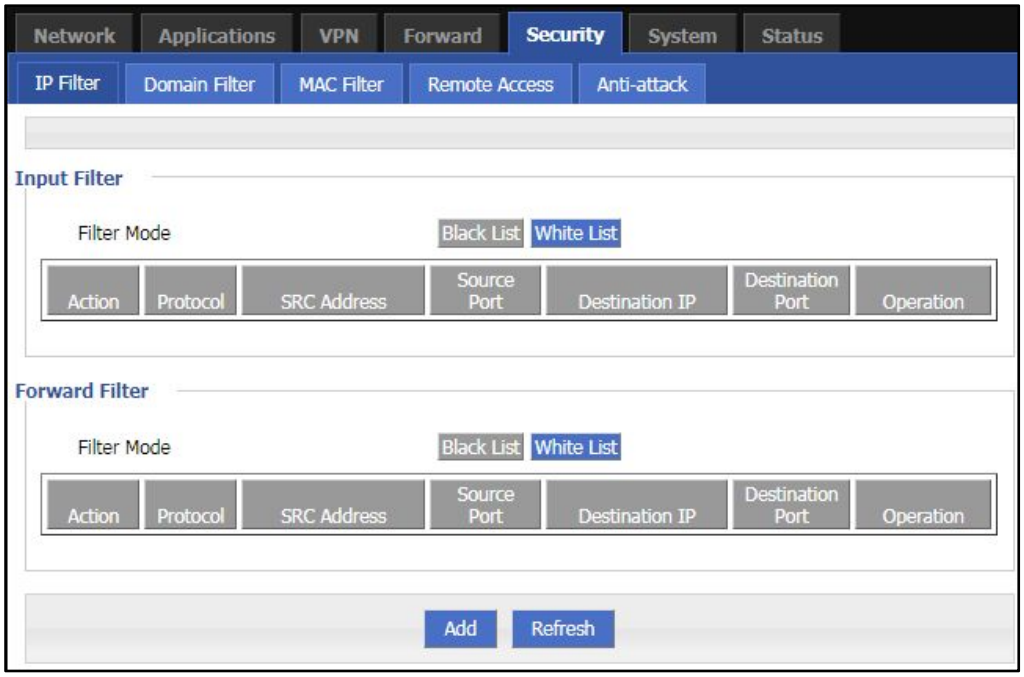
IP filter refers to judgment whether to allow router to forward the data according to filter rules, thus to manage internet surfing of PC in LAN. IP filter is used to allow part of PCs in LAN to visit external WAN network or forbidden some PCs from visiting specific website.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Security > IP Filter” to open the configuration page of”IP Filter”.As shown in Figure 5-27.

Figure 1-15 The configuration page of"IP Filter"



In the forwarding filtering rules.

- Black List: The default allows packet forwarding, in line with the list of "discarded" rules packet cannot be forwarded through the router.
- White List: The default refuses packet forwarding, in line with the list of "accept" rules packet can go through router forwarding.

Step 3 Click "Add" to add a new IP filter rule and configure IP filter parameter. There are two types of IP filter: "Input" and "Forward", as show in Figure 5-28 and Figure 5-29.

Figure 1-16 The configuration of "Input" type of IP filter

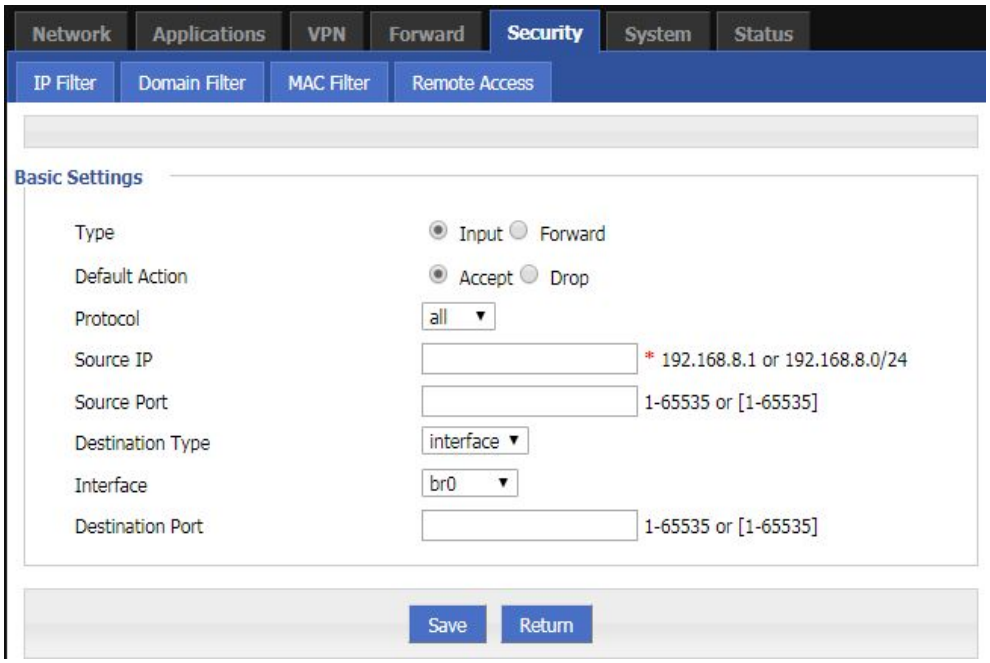


Figure 1-17 The configuration of “Forward” type of IP filter

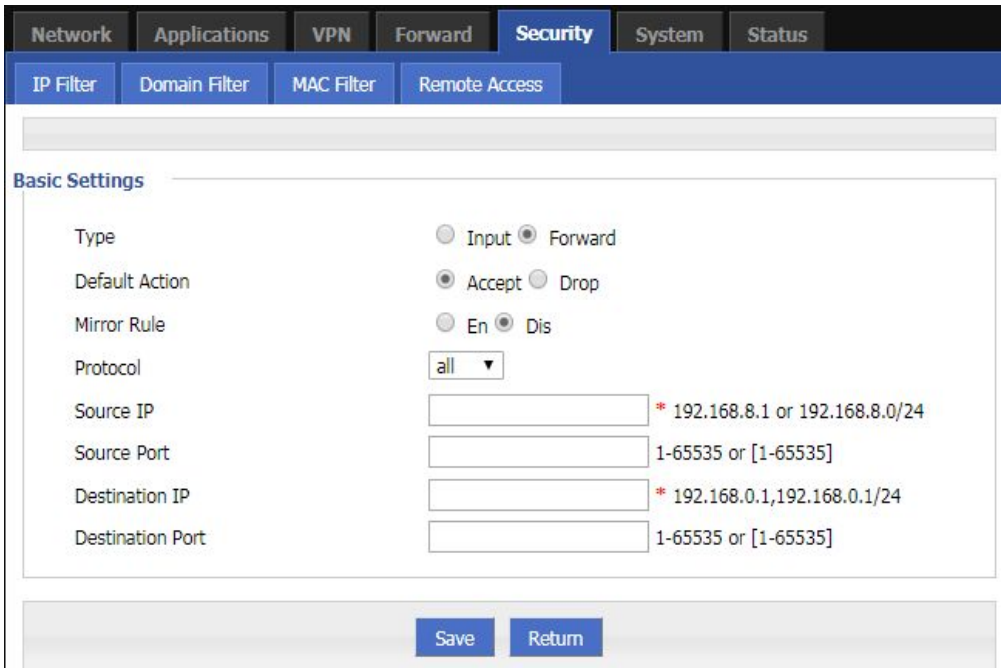


Table 1-11 The instruction of IP filter parameter

Parameter	Details	Operation
Type	Select a filter type, you can choose according to their needs, "Input" or "Forward" Input: whether to allow access to the router Forward: whether to allow the router forwarding	Dropdown List options • Input • Forward
Default Action	The default action rule. You can select "Accept" or " Drop " Accept: firewall to accept the package, which can be passed Drop: firewall discards the packet directly	Dropdown List options • Accept • Drop
Mirror Rule	When the filter type selects "Forward", it needs to be configured Enable: Base on the configured rules, system auto adds totally opposite rules in addition. Opposite rules mean all the source address/port and destination address/port are reverse in the rules Disabled: no treatment	Dropdown List options • Enable • Disable

Parameter	Details	Operation
Protocol	Protocol used by IP packets	• Dropdown List options • all • tcp • udp • icmp
Source IP	• The source IP address of the packet	Manual input Format: A.B.C.D/Mask Example: 92.168.8.1 or 192.168.8.1/24
Source Port	The source Port of the packet, when the protocol choose "icmp", it don't need to configure	Value area: 1-65535 or [1-65535], it can be a range, or a single port
When the IP Filter type select "Input"		
Destination Type	Design an IP packet access router interface	Dropdown List options • interface • any
Interface	Configure when Destination Type select "Interface", means the IP packet access the router interface	Dropdown List options • br0 • modem • eth0 • eth1
Destination Port	IP packet access router ports (when the protocol select "icmp", requires no configuration)	Value area: 1-65535 or [1-65535], it can be a range, or a single port
When the IP Filter type select "Forward"		
Destination IP	IP packet destination IP	Manual input Format: A.B.C.D/Mask
Destination Port	IP packet destination port	Value area: 1-65535 or [1-65535], it can be a range, or a single port

Step 4 Single click "save" to finish the configuration of IP Filter rule.

NOTE

The IP input rule indicates whether other devices are allowed to access the router. The destination address in the rule can only select the interface of the router. The IP forwarding rule indicates whether IP packets are allowed to be forwarded through the router. The destination address in the rule can be the interface address of the router. All other IP addresses except.
After the port is configured in the rule, select the "all" protocol to indicate that both "tcp" and "udp" protocols are selected. When the port is not configured in the rule, select "all" to indicate that "tcp" and "udp" are selected at the same time. "icmp" three protocols.

--END

1.2.2 Domain Filter

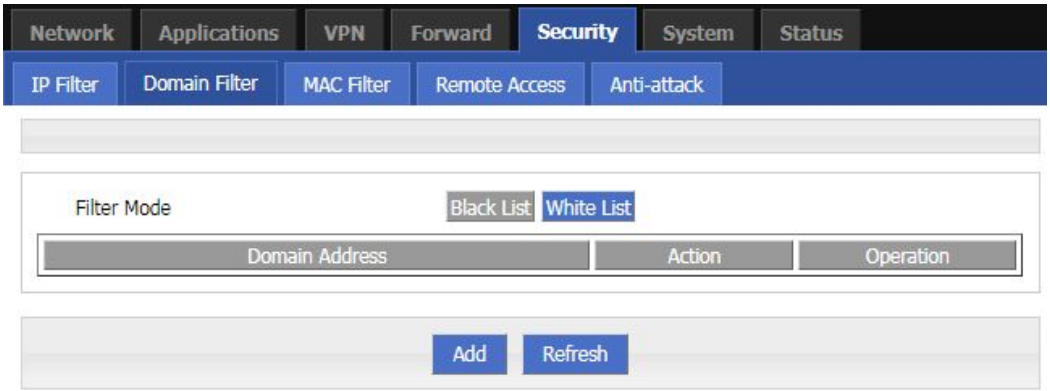
Domain filter support black list and white list. It is used to forbid PCs in LAN from visit some websites or allows them to visit specific websites.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Security> Domain Filter” to open the configuration of “Domain Filter”.As shown in Figure 5-30.

Figure 1-18 The configuration of Domain filter



- Black list: websites in the blacklist cannot be visited. Click “black list” to forbid visiting the websites in the list.
- White list: only the websites in the white list can be visited, while other websites cannot be visited. Click “White list” to activate it.

Step 3 Click “ADD” to add a new domain filter rule and configure domain filtering parameter.

Figure 1-19 The configuration page of Domain filter

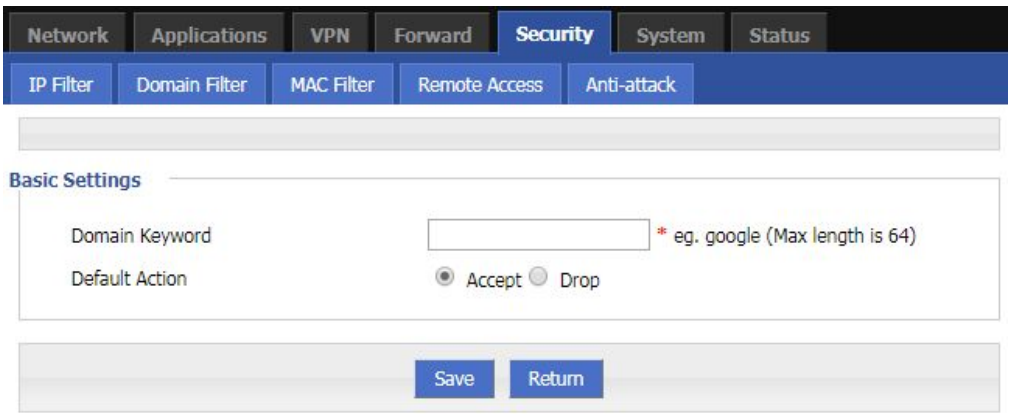


Table 1-12 The instruction of Domain Filter parameter

Parameter	Details	Operation
Domain keyword	Keyword of domain for filter	WORD type, max 64 digits. E.g. www.google.com, the keyword is “google”.

Default action	Actions to filter the keyword	• Accept. • Drop

Step 4 Single click “Save” to finish configuring a rule.

--END

1.2.3 MAC filter

MAC filter also supports black and white lists, which are usually used to control host access to routers. In addition to this function, the 4G Intelligent Gateways can also restrict the external network access rights of specific MAC hosts, or only allow hosts with specific MAC addresses to access the external network.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Security> MAC Filter” to open the configuration page of “MAC Filter”. See below:

Figure 1-20 The configuration page of MAC Filter

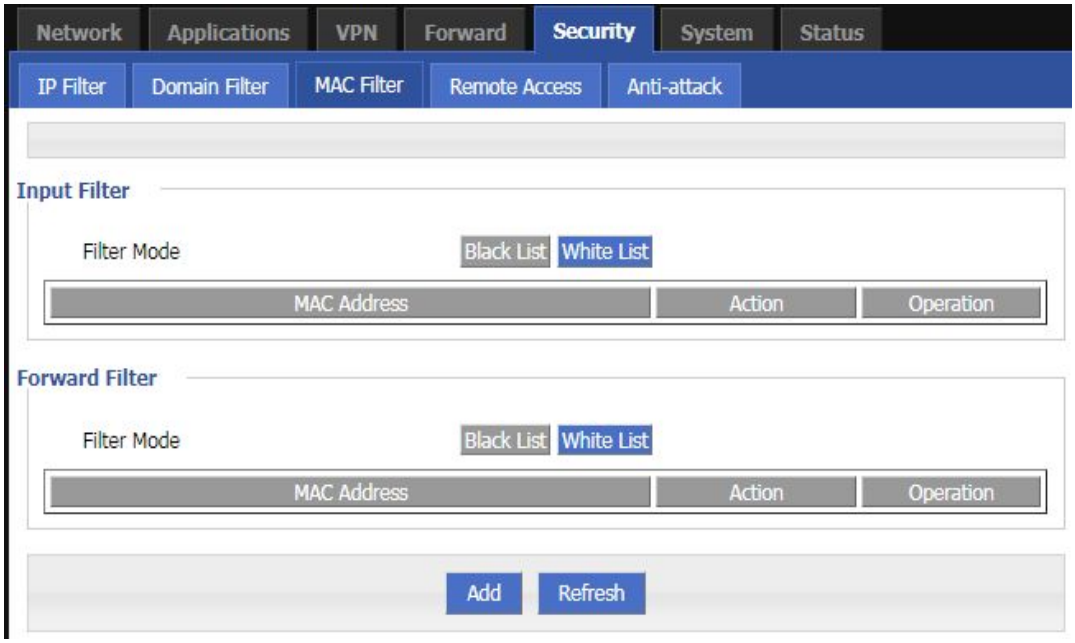


Table 1-13 MAC Filter explanation

Parameter	Details	Operation
Input configuration		
Input Filter	To activate MAC input filtering black list / white list.	• Blacklist: rules in blacklist cannot visit router, other MACs can visit router. • White list: rules in white list can visit router, other MACs cannot visit router.
Forward configuration		
Forward Filter	To activate MAC forward filtering	• Blacklist: rules in blacklist cannot visit external network, other MACs can visit external network

Parameter	Details	Operation
	black list / white list.	through router. • White list: rules in white list can visit external network, other MACs cannot visit external network through router.

Step 3 Click "Add" to add a new MAC filter rule and configure MAC filtering parameter. See below:

Figure 1-21 The configuration of MAC Filter

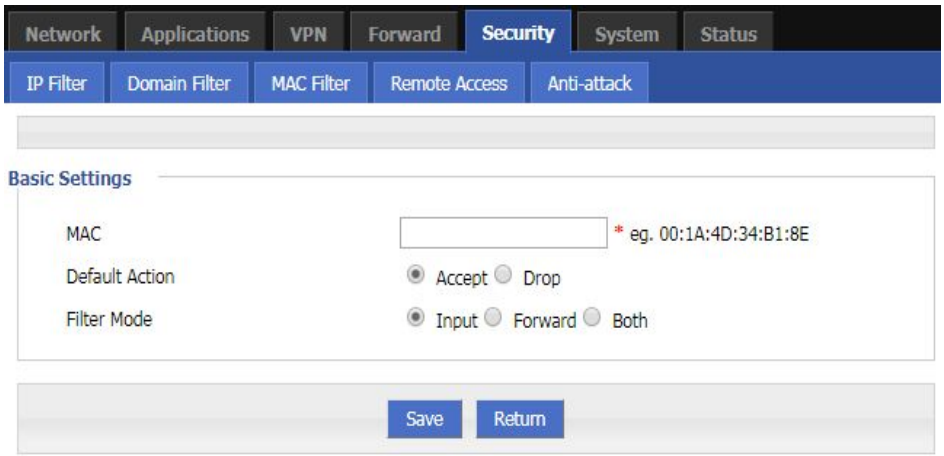


Table 1-14 The instruction of MAC Filter Parameter

Parameter	Details	Operation
Basic Settings		
MAC	MAC to be filtered	WORD type MAC format: XX:XX:XX:XX:XX:XX
Default Action	Default actions of the rule. Can be "accept" or "Drop": • Accept: to accept all packages from this MAC. • Drop: to drop all packages from this MAC.	To choose "accept" or "Drop"
Filter mode	To choose "Input", "Forward" or "Both". • Input: all packages visiting router. • Forward: all packages forwarded by router. • Both: both Input and forward.	To choose "Input", "Forward" or "Both".

Step 4 Single click "save" to finish the configuration of MAC filter.

---END

1.2.4 Remote Access

For security reasons, the ports 80, 23, 5123, and 443 of the router are usually disabled by default. In order to facilitate the configuration of the router through a specific interface, the port opening function is added.

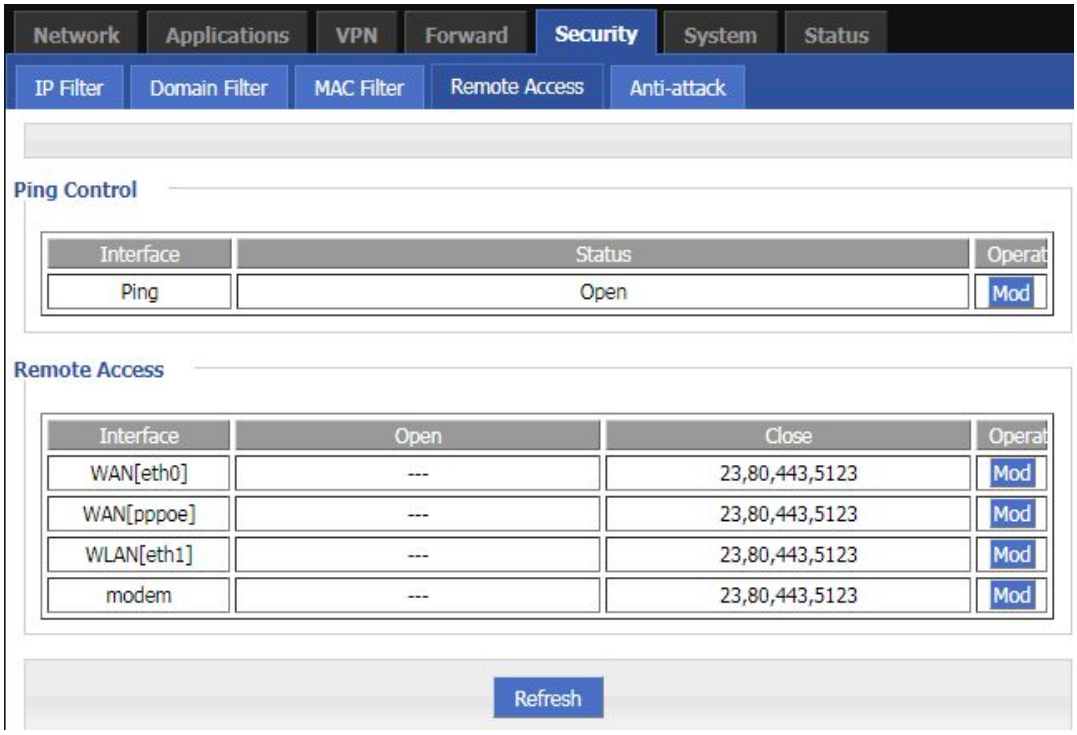
In addition, some customers have banned ping service requirements, and the page has added a ping function that prohibits all ports except the br0 port.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click "Security>Remote Access". Open the configuration page of “Remote Access”, see below:

Figure 1-22 The page of “Remote Access”



Step 3 Click "Mod" to open or close the 80 (HTTP), 23 (CLI), 5123 (SSH), 443 (HTTPS) ports of different interfaces. See below:

Figure 1-23 The editing page to open Ports

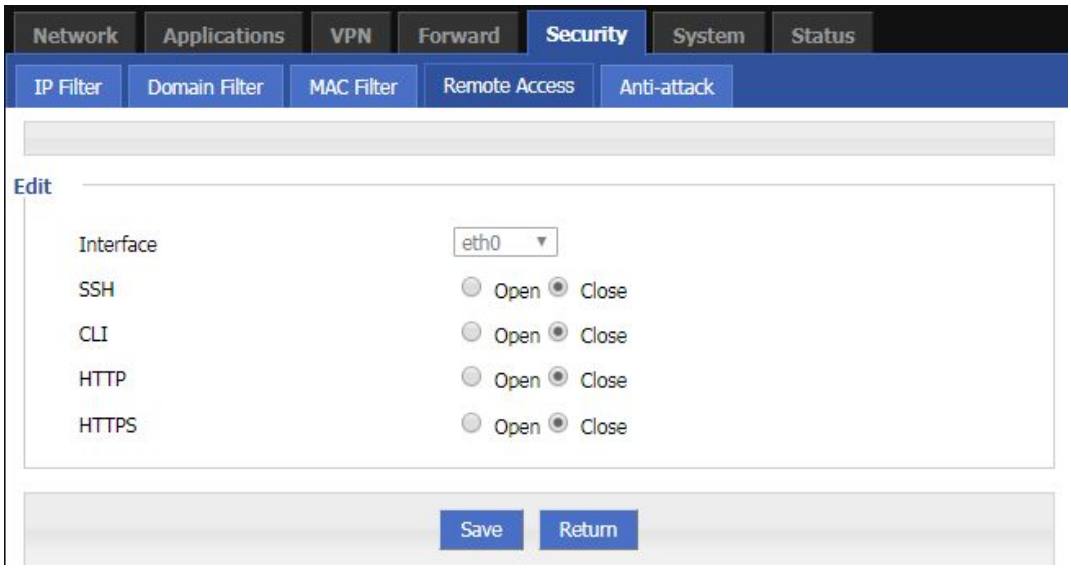


Table 1-15 Description of port open configuration parameters

Parameter	Details	Operation
Interface	The interface that needs to be configured for the port. The default is not to choose.	No action required
SSH	The SSH port can be chosen to open or close .	Radio button selection. • Open • Close
CLI	The CLI port can be chosen to open or close .	Radio button selection. • Open • Close
HTTP	The HTTP port can be chosen to open or close .	Radio button selection. • Open • Close
HTTPS	The HTTPS port can be chosen to open or close .	Radio button selection. • Open • Close

Step 4 Click Save to complete the configuration of opening or closing the port on the interface.

Step 5 Click the “Mod” button to enable or disable the ping function, see below:

Figure 1-24 The editing page to ping

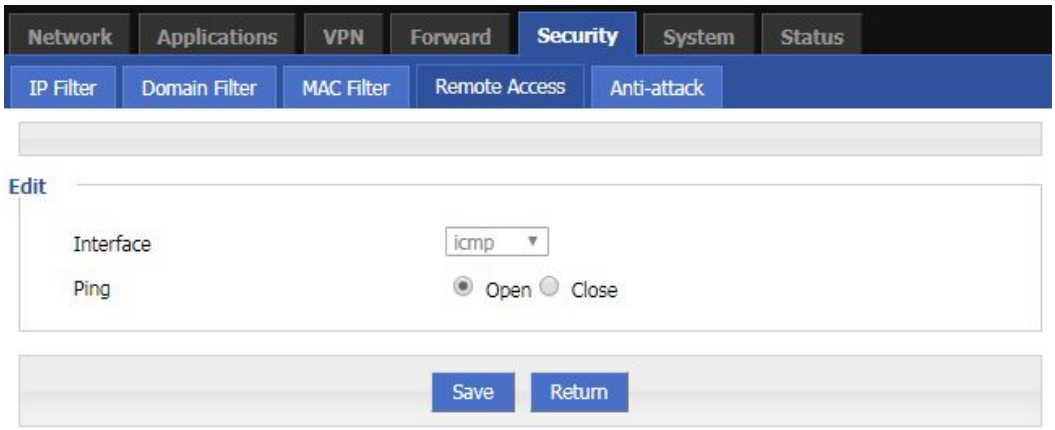


Table 1-16 Description of port open configuration parameters

Parameter	Details	Operation
Interface	The interface that needs to be configured for the port. The default is not to choose.	No action required
ping	The ping can be chosen to turn ping on or off	Radio button selection. • Open • Close

Step 6 Click Save to complete the configuration that the ping function is open or closed.

---END

1.2.5 Anti-attack

A DDoS attack is a common type of network attack. If the attacked object is severe, the entire network may be paralyzed. The device provides DDoS attack defense. This allows the device to reduce this network attack. In addition, port scanning is also used by some hackers to attack the device. A large number of port scans also occupy a large amount of resources of the device. The device provides a function of prohibiting port scanning, which enables the device to reduce illegal port scanning.

Step 1 Log in to the 4G Intelligent Gateway WEB configuration page.

For details, see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click "Security>Anti-attack".

Open the configuration page of “Anti-attack”. See below:

Figure 1-25 The configuration page of “Anti-attack”

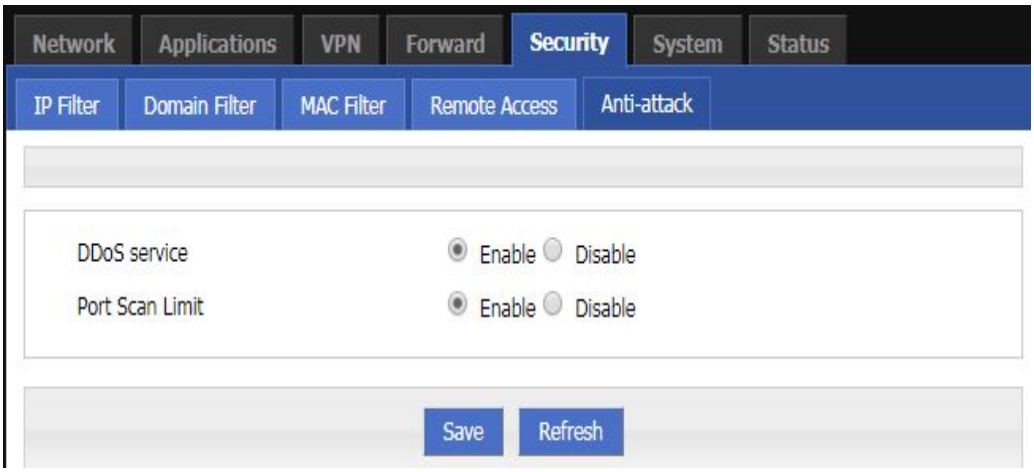


Table 1-17 The instruction of Parameter for Anti-attack

Parameter	Details	Operation
DDoS service	The DDos can be chosen to enable or disable.	Radio button selection. • Enable • Disable
Port Scan Limit	The function of port Scan Limit can be chosen to enable or disable.	Radio button selection. • Enable • Disable

Step 3 Click "Save"to finish the configuration of “Anti-attack” .

---END

1.3 Forward configuration

Overview

Forward function of 4G Intelligent Gateway includes NAT, Routing, dynamic routing (RIP, OSPF,BGP) (optional) and QoS .

1.3.1 NAT

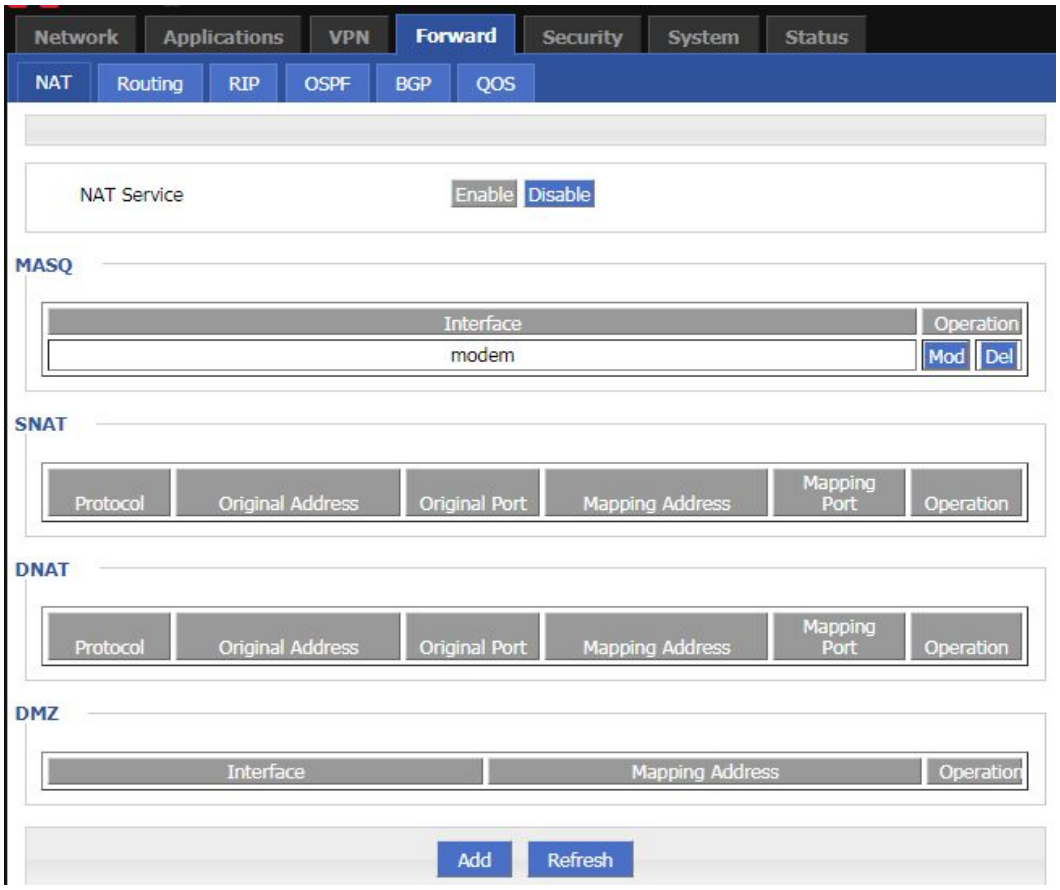
1.3.1.2 The configuration of DNAT rule

The DNAT is a destination address replacement and is used to replace the destination address inside the external network access router with the address set by the user.

Step 1 Click "Forward>NAT".

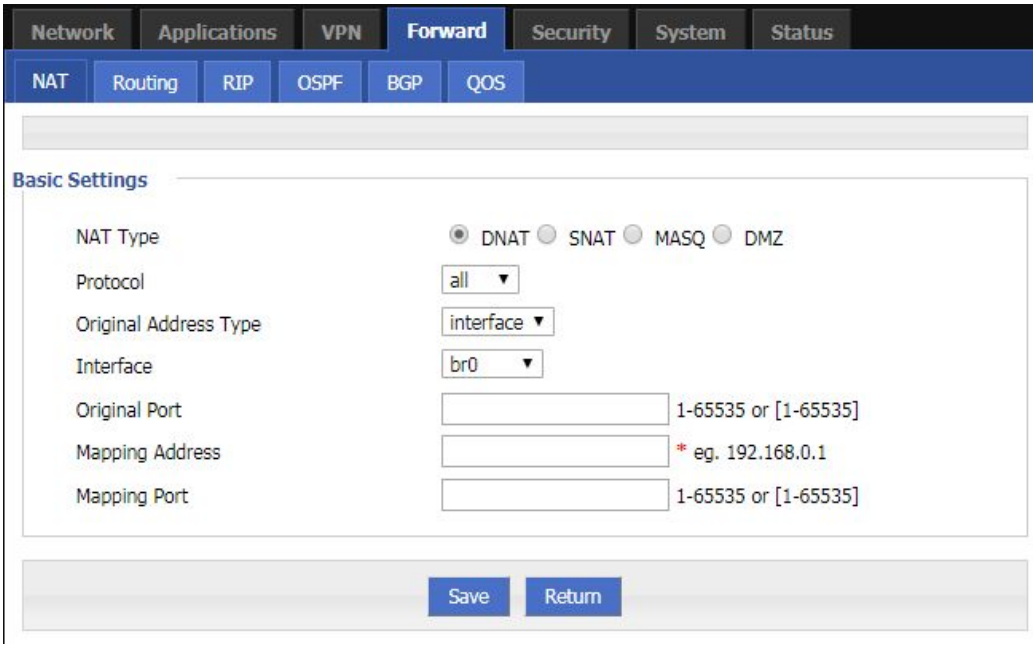
Open the configuration page of “NAT”. See below:

Figure 1-26 The configuration page of “NAT”



Step 2 Click the "Add" button and select a new DNAT rule with the conversion type "DNAT", see below:

Figure 1-27 The configuration page of DNAT rule



Step 3 Configure parameters for the DNAT rule.

Table 1-18 DNAT Parameter instruction

Parameter	Details	Operation
Basic Settings		
Protocol	The destination address translation is performed for which protocol packet.	Select from dropdown List: • all • tcp • Udp • icmp
Original Address Type	The external address, the address needs to be converted	Dropdown List • interface • static
Interface (when the initial address type select “interface” , needs to be configured)	Indicates the external address of IP packets to an interface of the router	Dropdown List • br0 • modem • eth0 • eth1
Original Address (when the initial address type select “static”, needs to be configured)	The external address, the address needs to be converted	Manual input Format1: A.B.C.D Format2: A.B.C.D/Mask
Original port	The port of external IP, the port need to be replaced	Value area: 1~65535
Mapping address	Internal IP address	Format:A.B.C.D e.g. 192.168.8.1
Mapping port	The port of Internal IP address	Value area :1~65535

Step 4 Single click “save” to finish the configuration.

NOTE

When a port is configured in the DNAT rule, the protocol selects "all" to select two protocols "tcp" and "udp"; when no port is configured in the DNAT rule, the protocol selects "all" to select "tcp" and "udp" , "icmp" three kinds of agreements.

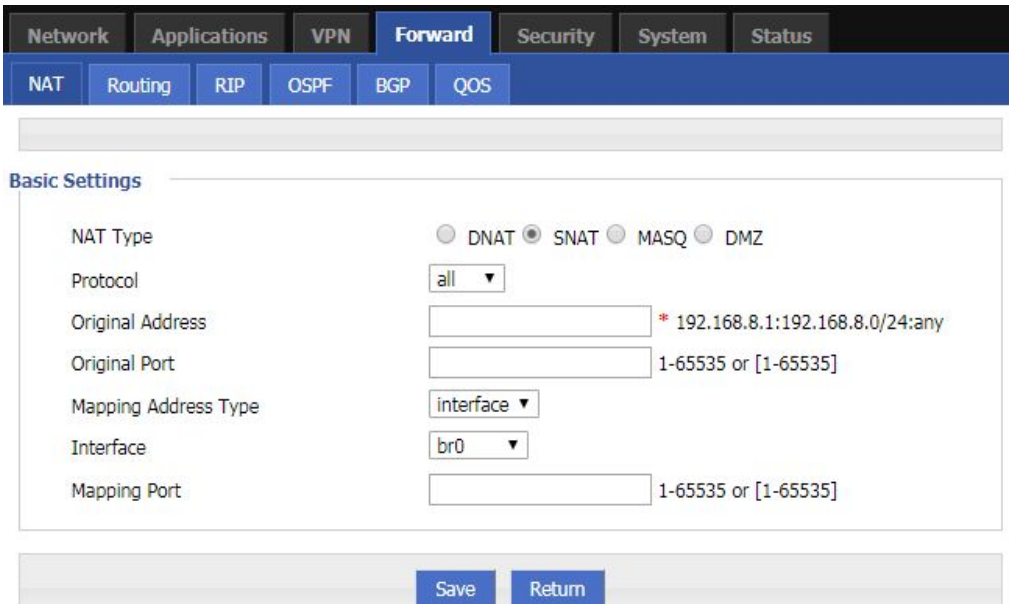
1.3.1.3 The configuration of SNAT rule

SNAT is the source address translation, and its role is to translate source address of IP packets into another address.

Step 1 Click “Forward > NAT” to open the configuration page of “NAT”.

Step 2 After the conversion type is set to SNAT, the configuration page. See below:

Figure 1-1 The configuration page of SNAT rule



Step 3 Configure the paraneter of SNAT rule.

Table 1-1 The instruction of parameters of SNAT rule

Parameter	Details	Operation
Protocol	The destination address translation is performed for which protocol packet.	Dropdown List • all • tcp • udp • icmp
Original Address	The source address need to be replaced	Manual input Format1: A.B.C.D Format2: A.B.C.D/Mask
Original Port	Source address port to be replaced.	Value area: 1-65535 or [1-65535], it can be a range, or a single port
Mapping Address Type	The type of new source address after the source address is replaced	Dropdown List • interface • static
Interface	Select the interface of the router as source address after replacement	• Dropdown List • br0 • modem • eth0 • eth1

Parameter	Details	Operation
Mapping Address	New source address after source address replacement	Format: A.B.C.D
Mapping Port	The new port which replaces the original port of source address.	Value area: 1-65535 or [1-65535], it can be a range, or a single port

Step 4 Single click “save” to finish the configuration of SNAT rule.

NOTE

When a SNAT rule is configured with port specified, selecting “all” in protocol means selecting two protocols contain "tcp", "udp"; when a SNAT rule is configured with no port specified, selecting “all” in protocol means selecting three protocols contains "tcp", "udp","icmp".

---END

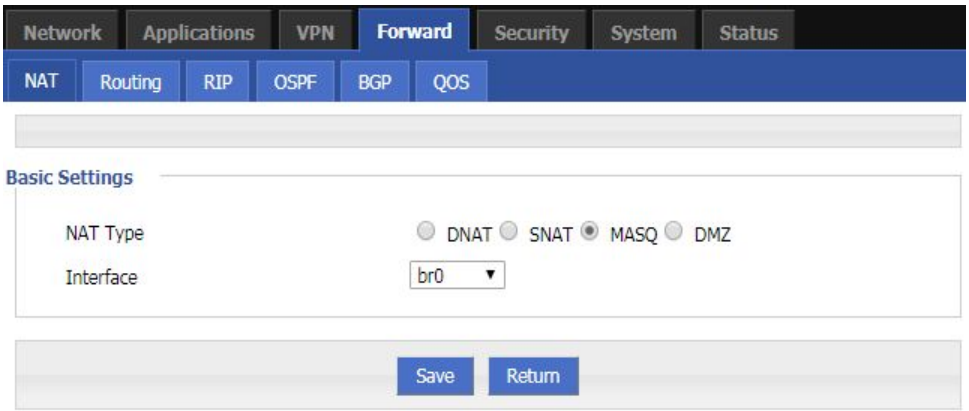
1.3.1.4 The configuration of MASQ rule

MASQ is also MASQUREADE, address masquerading, which converts the source IP address of all packets forwarded by the router into the IP address set by the user. The routers support the conversion of the source IP address of a packet to an interface address of the router.

Step 1 Click “Forward > NAT” .

open the configuration page of “NAT”and choose Convert Type as MASQ. See below:

Figure 1-1 The configuration page of MASQ



Step 2 Configure the parameters of MASQ rule.

Table 1-1 The instruction of parameters of MASQ rule

Parameter	Details	Operation
Interface	Select the IP of an interface as the communication address between the router LAN	Select from Dropdown List:

Parameter	Details	Operation
	and the outside.	• br0 • modem • eth0 • eth1

Step 3 Single click “save” to finish the configuration of MASQ.

NOTE

MASQ rule: the source address of all packets in the LAN need to be transferred into the specific ip address of the router, so the PC from the LAN can send packets out; If MASQ rule in the router will be deleted, the router LAN of the PC cannot communicate with external network.

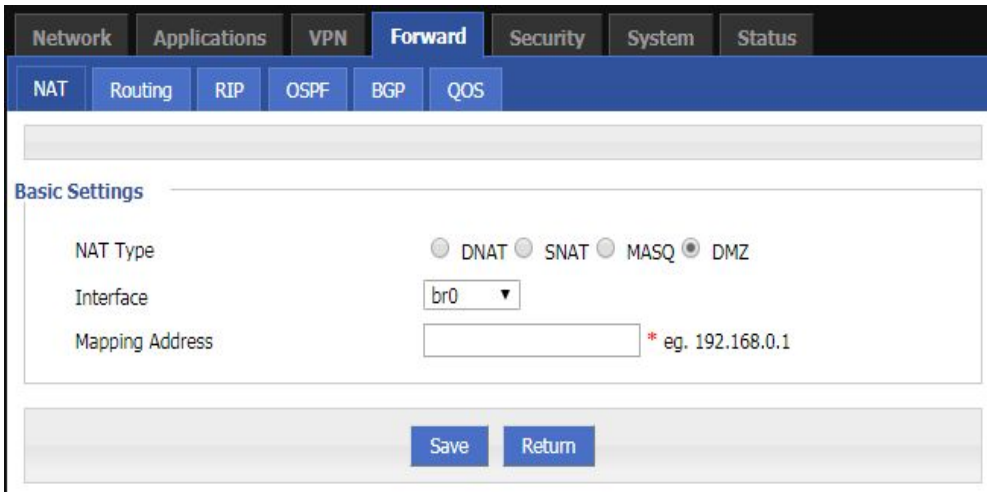
---END

1.3.1.5 The configuration of MASQ rule

DMZ is the abbreviation of "demilitarized zone" in English, and the Chinese name is "quarantine zone", also known as "demilitarized zone". It is to solve the problem that the external network can not access the internal network server after installing the firewall, and set up a buffer between the non-secure system and the security system. This buffer is located in the small network area between the internal network of the enterprise and the external network. In this small network area, you can place some server facilities that must be exposed, such as enterprise web servers, FTP servers, and forums. On the other hand, through such a DMZ area, the internal network is more effectively protected, because this kind of network deployment has an additional level for the attacker compared to the general firewall scheme.

Step 1 Click “Forward > DMZ”. See below:

Figure 1-2 The configuration page of DMZ



Step 2 Configure the parameters of DMZ rule.

Table 1-2 The instruction of parameters of DMZ rule.

Parameter	Details	Operation
Interface	Select the IP of an interface as the communication	Select from Dropdown

Parameter	Details	Operation
	address between the router LAN and the outside.	List: • br0 • modem • eth0 • eth1
Mapping Address	The address after the original destination address is replaced.	Format: A.B.C.D

Step 3 Single click “save” to finish the configuration of DMZ.

---END

1.3.1 Routing Configuration

Routing provides a specific forwarding path for routers to forward packets, which must be manually configured by the user. A route is classified into a static route and a policy route. The static route is a route based on the destination address.Priority is configured. The smaller the priority of the static route of the same destination, the higher the priority is selected.The policy routing is based on the source address selection route (the router detects the source address of the received forwarding packet, and then selects the corresponding policy route forwarding according to the source address), and the policy routing priority is distinguished by 3 to 252 numbers. The smaller the number, the higher the priority. There is also a priority between static routes and policy routes: policy routes take precedence over static routes.

Step 1 Click “Forward > Routing” to open the configuration page of “Routing” . See below:

Figure 1-1 The configuration page of “Routing”

Step 2 Click “Add” to add a new static route, configuration page. See below:

Figure 1-2 The configuration page of Static Routing

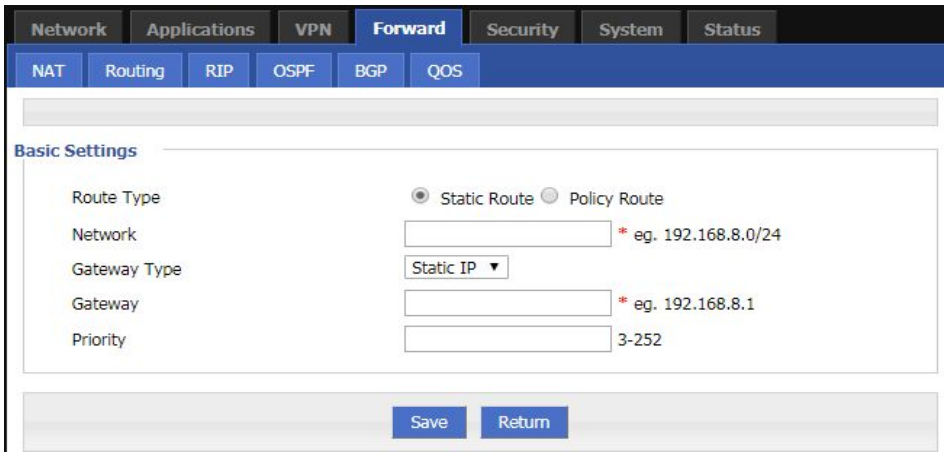


Figure 1-3 The configuration page of Policy Routing

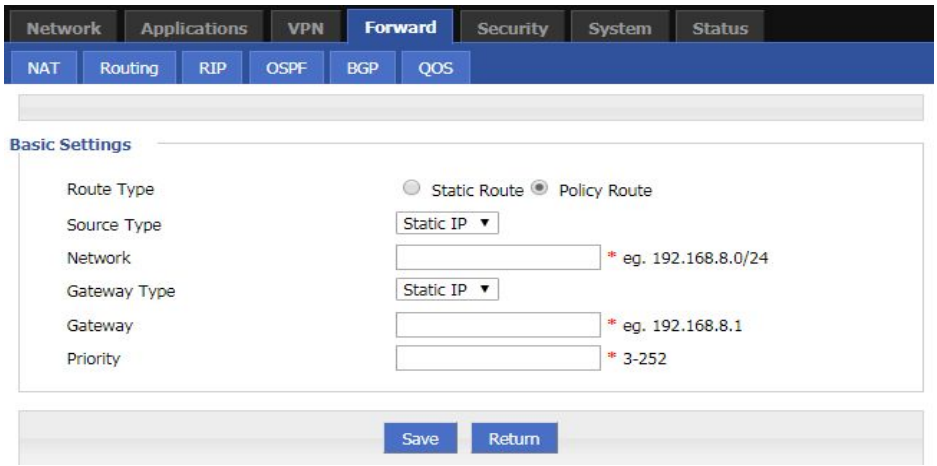


Table 1-1 The instruction of parameters of Routing

Parameter	Details	Operation
Basic Setting		
Routing Type	To select “Static Route” or “Policy Route”	• Dropdown List
When Routing Type is “Static Route”		
Network	Set the destination IP address and subnet mask of static route	Manual input Format1: A.B.C.D/Mask
Gateway Type	Specify gateway type of static routing, includes: • interface • static IP	Dropdown List • Static IP • Interface
Gateway	Set a next hop IP address of static route, IP address of the adjacent router interface	Dropdown List • If the gateway type selects static IP, gateway need to manually input, format:

Parameter	Details	Operation
		A.B.C.D • If the gateway type select interface, the gateway needs to select from dropdown list
Priority	Static route priority configuration	Enter it manually. Range: 3-252 The smaller the value, the higher the priority
When Routing Type is “Policy Route”		
Source Type	Set source address type of policy route	Dropdown List • Static IP Interface
Network	It can be configured when “static IP” is selected in source type, by adding IP address or subnet manually.	Manual input Format1: A.B.C.D/Mask
Source Interface	When source type is policy route, need to manually set source network address of policy router	Dropdown List • modem • eth0 • eth1
Gateway Type	Set the next hop IP of policy route	Dropdown List • static ip • Interface
Gateway	When the gateway type select "Static IP" to fill in the IP address, when gateway type is "interface", it will use the selected interfaces as gateway	Manual input Format1: A.B.C.D/Mask
Priority	Set policy routing priority, the priority lower the number, the higher the priority	Value area: [3,252]

Step 3 Single click “save” to finish the static routing setting.

NOTE

Static routing will forward according to the destination address of the packet, if the router received the packet (e.g. source address is 1.1.1.1 destination address is 2.2.2.2), it will forward the packet to next hop according to the route which meets with the destination address (2.2.2.2).

It will forward the packet to next hop according to the route which meets with the destination address (2.2.2.2).

Policy routing will forward according to the source address of the packet, if the router received the packet (e.g. source address is 1.1.1.1 destination address is 2.2.2.2), it will forward the packet to next hop according to the route which meet with the source address (1.1.1.1).

Policy routing has higher priority than static routing, policy-based routing priority regardless of how much.

---END

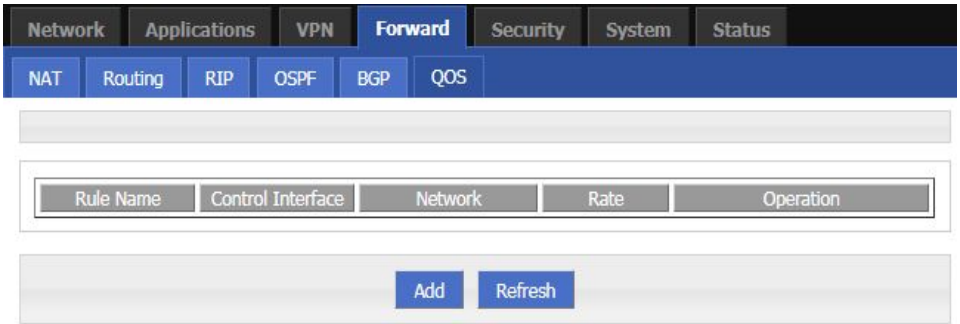
1.3.2 QoS

QoS (Quality of Service) quality of service, is a security mechanism for the network, is a technique to solve the network bandwidth allocation and network priority and other issues. When the network is overloaded or congested, QoS to ensure that critical traffic is not delayed or dropped, while ensuring the efficient operation of the network, our 4G Intelligent Gateway supports custom QoS services.

Step 1 Click “Forward > Qos”.

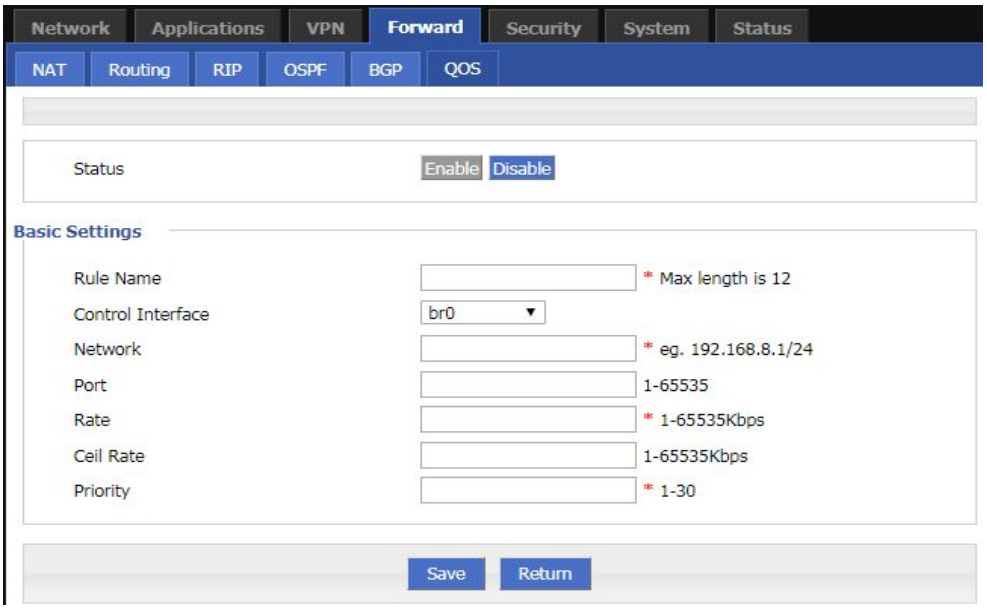
Step 2 Open the configuration page of “Qos”. See below:

Figure 1-4 The page of QoS



Step 3 Click "Add" to create a new QoS rule. See below:

Figure 1-5 The configuration page of QoS



Step 4 Configure QoS parameters. See below:

Table 1-2 QoS parameter instruction

Parameter	Details	Option
Rule Name	QoS rule name	The max to 12 characters Only set when adds a new rule and the

Parameter	Details	Option
		follow-up can not be modified The rule name can not be repeated, otherwise the rule will be covered after the rule is added in front of the cover
Control Interface	The interface type of QOS, include:	Dropdown List • br0 • Modem • eth0
Network	The network address that flow in and out via the QOS interface, is the object of speed limit.	Full in destination address and subnet mask Manual input Format1: A.B.C.D/Mask
Port	The network interface of QOS	Value area: 1-65535 You can not configure the port, if not the configuration represents all ports
Rate	Transmission rate of the network address settings	Value area: 1~65535 Units: Kbps
Ceil Rate	In ensuring the basic rate and the spare bandwidth, the maximum bandwidth of the network address of the communication can be obtained with higher priority will be given priority redundant bandwidth	Value area: 1~65535 Units: Kbps
Priority	Set the precedence of the rules	Value area: [1,30]

Step 5 Single click “save” to finish QOS setting.

NOTE

QoS is mainly used to allocate the average bandwidth for the users which access Internet through the router, or assigned specific users with more bandwidth. If the router is connected with two subnets: 192.168.8.1/24 and 192.168.9.1/24, the router QOS can control the rate of these two subnets; If the router's bandwidth is relatively well-off, the router can adjust the bandwidth based on priority and redundancy of two subnets, that is, the router meets the high priority redundancy bandwidth firstly, then meets the low priority subnet redundancy bandwidth.

---END

1.3.3 Dynamic Routing (Optional)

RIP configuration

RIP protocol (Routing Information Protocol) is the most widely IGP (Interior Gateway Protocol), it was designed for the same technology used in small networks, and therefore adapt to most of the campus

network and used in a continuous regional networks that the rate change is not big, 4G Intelligent Gateway supports RIP v2 protocol. For more complex environments, generally do not use the RIP protocol.

Step 1 Click “Forward > RIP”.

Step 2 Open the configuration page of “RIP”. See below:

Figure 1-6 The configuration of RIP

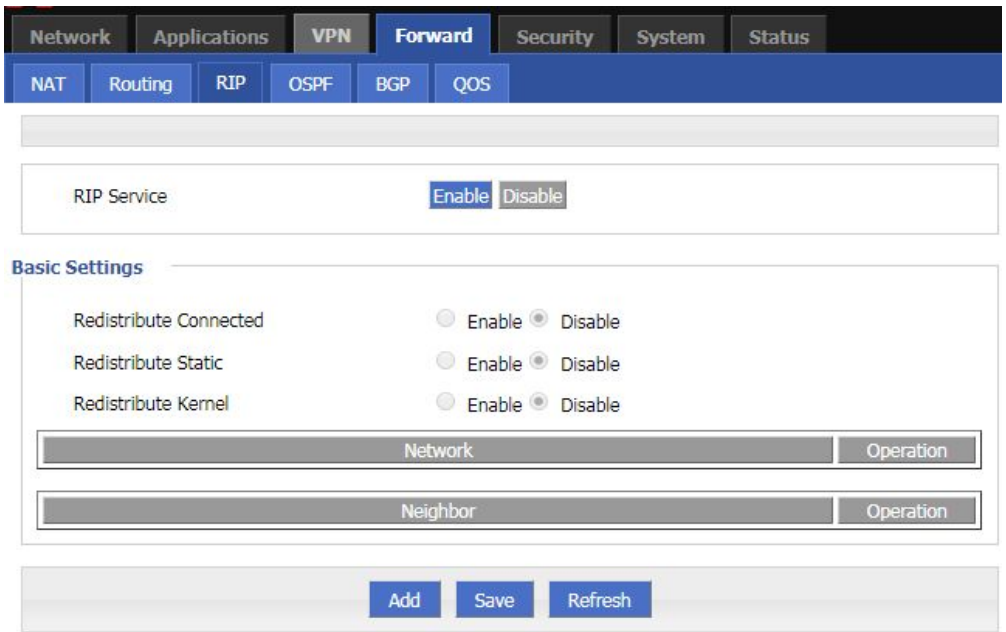
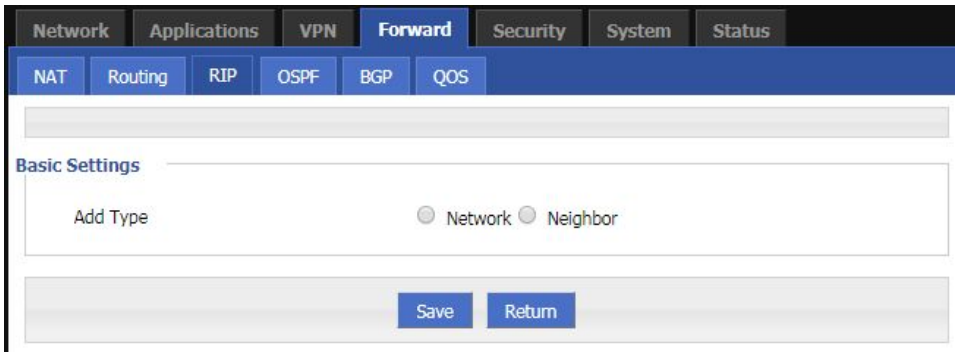


Table 1-3 RIP Parameter Instruction

Parameter	Details	Operation
RIP Service	Enable or disable RIP Service	Click the button to select. • Enable • Disable
Redistribute Connected	Whether to redistribute direct routes to RIP	Click the button to select. • Enable • Disable
Redistribute Static	Whether to redistribute static routes to RIP	Click the button to select. • Enable • Disable
Redistribute Kernel	Whether to redistribute kernel routes to RIP	Click the button to select. • Enable • Disable

Step 3 Click “Add” to add a new RIP route, configuration page. See below:

Figure 1-7 The configuration page of RIP route



Step 4 Configure RIP route parameter instruction. See below:

Table 1-4 RIP parameter instruction

Parameter	Details	Operation
Add Type	Add the type of RIP route	Click the button to select Add Type • When it is "Network", need to configure destination network address. • When it is "Neighbor", need to configure neighbor's IP address
Network(directly connect to the router)	Add the destination network of RIP route	Add the destination network of RIP route Format: A.B.C.D/Mask
Neighbor(directly connect to the router)	Add the neighbor's IP address of RIP route	Add the neighbor's IP address of RIP route Format: A.B.C.D

Step 5 Single click "save" to finish RIP route setting.

NOTE

RIP is an interior gateway protocol. If the communications between the two routers do not go through another router, the two routers are adjacent. The RIP protocol specifies that no information exchange between non-adjacent routers.

Routers exchanging information is all the information currently known to the router. That is its own routing table. At a fixed time to exchange routing information (such as every 30 seconds), then the router receives the routing information to update the routing table.

RIP protocol "distance" also known as "hops " (hop count), because each through a router hop count is incremented. The RIP judges a better router according to the less routing hops, as the "shorter distance". RIP allows a path can contain up to 15 routers. Therefore, when the distance reach to 16 hops, it means the destination unreachable. RIP visible only for small Internet.

---END

OSPF configuration

OSPF (Open Shortest Path First) protocol is one of the (Interior Gateway Protocol), the most widely used IGP, for a single AS (autonomous system) in the routing decisions for large networks. OSPF business can be based whether the user needs to be configured at the factory 4G Intelligent Gateway.

Step 1 Click "Forward > OSPF".

Step 2 Open the configuration page of “OSPF” . See below:

Figure 1-8 The configuration page of OSPF

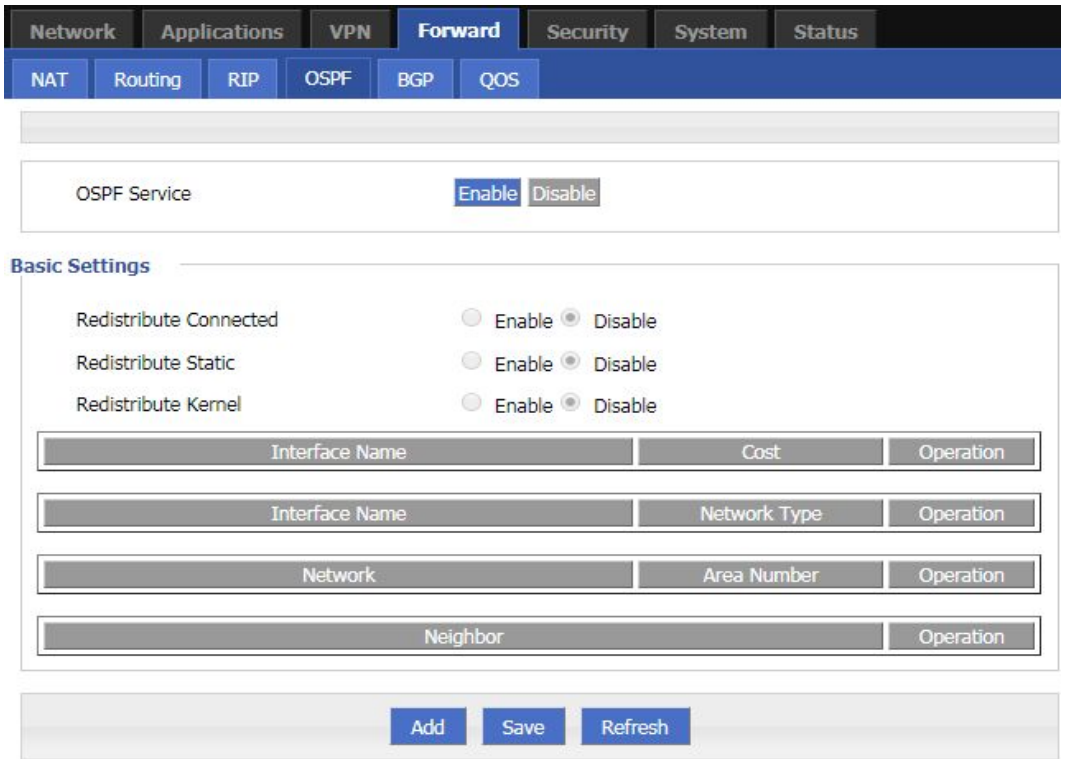
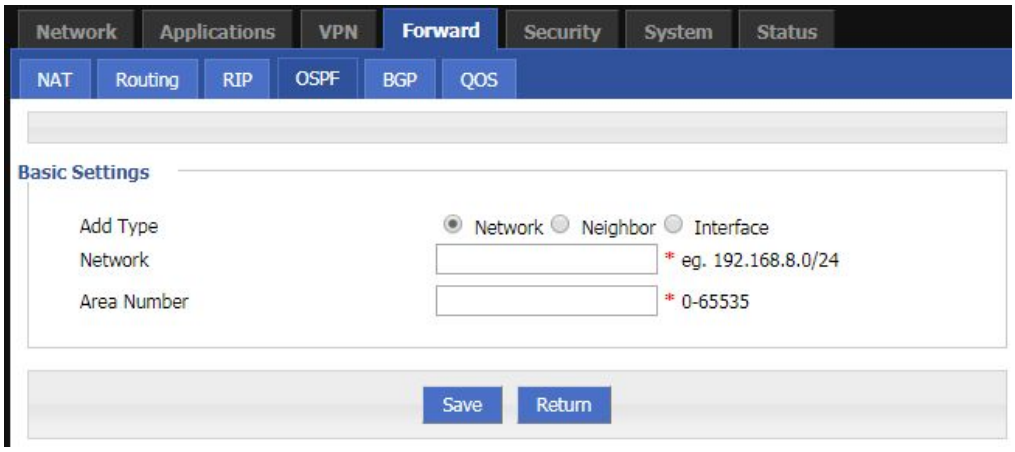


Table 1-5 OSPF parameter instruction

Parameter	Details	Operation
OSPF Service	Enable or disable OSPF Service	Click the button to select • Enable • Disable
Redistribute Connected	Whether to redistribute direct routes to OSPF	Click the button to select • Enable • Disable
Redistribute Static	Whether to redistribute static routes to OSPF	Click the button to select • Enable • Disable
Redistribute Kernel	Whether to redistribute kernel routes to OSPF	Click the button to select • Enable • Disable

Step 3 Click “Add” to add a new OSPF route, configuration page. See below:

Figure 1-9 The configuration of OSPF route



Step 4 Configure OSPF route parameter instruction. See below:

Table 1-6 OSPF route parameter instruction

Parameter	Details	Option
When Add Type is “Network”,		
Network	Set the network address as ospf sending address	Manual input Format1: A.B.C.D/Mask
Area Number	Used to identify the network (only the routers with the same domain address can exchange routing information)	Manual input Value area:[0,65535]
When Add Type is “Neighbor”,		
Neighbor	The router can reach in the next hop	Manual input Format1: A.B.C.D/Mask
When Add Type is “Interface”,		
Interface Name	The interface of the router	• Dropdown List • br0 • modem • eth1 • eth0
Interface Attribute	Configure the router interface attribute, include cost and network	• Click the button to select • cost • network
Cost	Configure the cost of the router interface, used to learn routing table	Manual input Value area:1-65535
Network Type (when the interface attribute is network)	Configure the network type of the router interface	• Dropdown List • broadcast • non-broad • point-to-multipoint • point-to-point

Step 5 Single click “save” to finish OSPF route setting.

NOTE

OSPF is a link-state (Link-state) routing protocol, commonly used for the same routing domain. Here, the routing domain is an autonomous system, which refers to the routers can switch routing information through a unified network switching or routing protocol routing policy in the AS, all OSPF routers maintains an identical description of the database structure AS, which is stored in the database link status information corresponding routing domain, OSPF router is through this database to calculate its OSPF routing table.

As a link-state routing protocol, OSPF link state broadcast data LSA (Link State Advertisement) sent to all routers in an area, which is different from the distance vector routing protocols. Distance vector routing protocol passed some or all routing information of the routing table to the adjacent routers.

---END

BGP configuration

Border Gateway Protocol (BGP) is a routing protocol for an autonomous system running on TCP. BGP is the only protocol used to handle networks like the size of the Internet, and the only protocol that can properly handle multiple connections between unrelated routing domains. BGP is built on the experience of EGP. The main function of the BGP system is to exchange network reachability information with other BGP systems. Network reachability information includes information about the listed autonomous systems (AS). This information effectively constructs a topology map of the AS interconnect and thereby clears the routing loop while implementing policy decisions at the AS level.

Step 1 Click “Forward > BGP”.

Step 2 Open the configuration page of “BGP”. See below:

Figure 1-10 The page of BGP

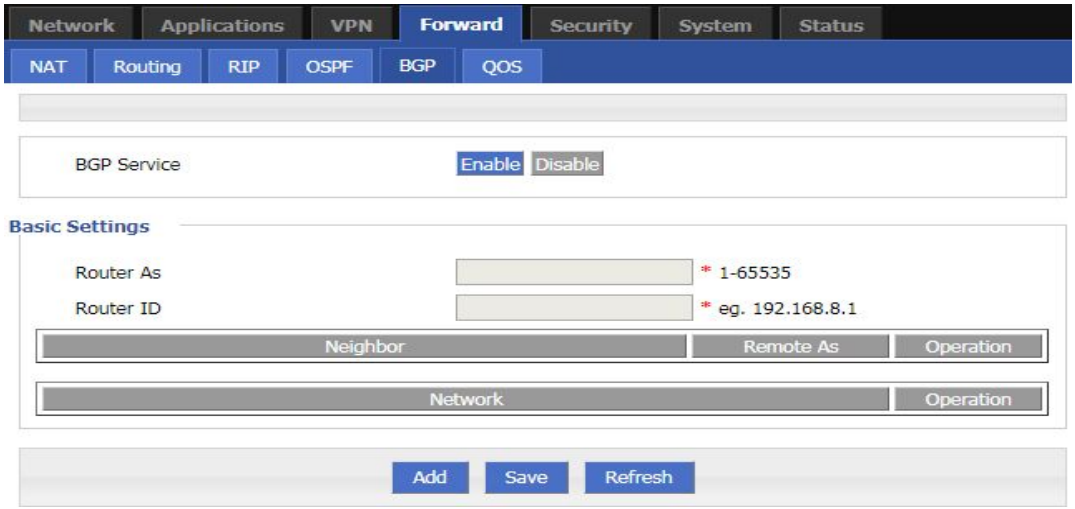


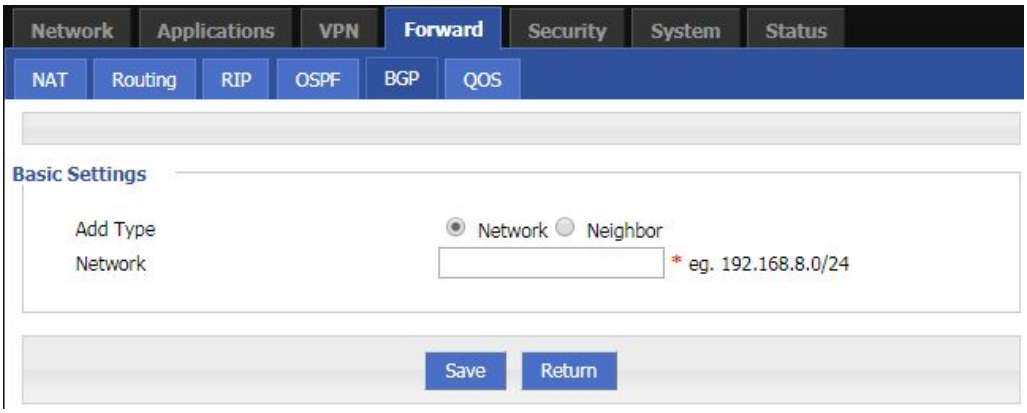
Table 1-7 BGP configuration parameter instruction

Parameter	Details	Option
BGP Service	BGP function is turned on	Button selection: • Enable • Disable Gray status indicates the currently selected status
Router As	The router is configured with the system number. The same AS is called IBGP. The different AS is called EBGP.	Manual input Value area:[0,65535]
Router ID	Route ID, which is used in BGP when routing	Manual input Format1: A.B.C.D

Step 3 Click “Save” to finish the basic settings of BGP.

Step 4 Click “Add” to create a new BGP rule. See below:

Figure 1-11 The configuration page of BGP



Step 5 Configure the rule parameters of the route mode. See below:BGP rule parameter instruction

Parameter	Details	Option
When "Notification Type" selects "Network"		
Network	Set a network segment as the notification address of the router BGP.	Format: A.B.C.D
When "Notification Type" selects "Neighbor"		
Neighbor	The address of the device that the router can reach at one hop.	Manual input Format: A.B.C.D
Remote As	Set the peer peer AS number to be the same as the local AS number to establish an IBGP neighbor. The local AS number is inconsistent with the local AS number.	Manual input Value area:[0,65535]
Advanced Settings	Advanced option switch	Click to expand. The default is the collapsed state
Update Source	BGP update source interface selection. The update source is the interface used by BGP to establish a tcp connection when BGP establishes a neighbor. If not specified, the physical network port of the interconnect is used by default.	Dropdown list: • br0 • loopback • modem • eth0 • Eth1
Log-neighbor-changes	Print log when neighbor status changes	Dropdown list: • Enable • Disable
Auto Summary	Automatic route aggregation switch	Dropdown list: • Enable • Disable

Synchronization	BGP synchronization switch	Dropdown list: • Enable • Disable

Step 6 Click “Save” to complete the configuration of the BGP rule.

NOTE

BGP (Border Gateway Protocol) is a distance vector routing protocol that implements reachable routes between ASs (Autonomous System) and selects the best route.

BGP advantages:

BGP guarantees the security, flexibility, stability, reliability and efficiency of the network in many aspects.

BGP adopts authentication and GTSM to ensure network security.

BGP provides a variety of routing policies, which can flexibly route routes and guide neighbors to advertise routes according to policies.

BGP provides route aggregation and route aging to prevent network flapping and effectively improve network stability.

BGP uses TCP as its transport layer protocol (destination port number 179) and supports association with BGP and BFD, BGP tracking, and BGP GR and NSR to improve network reliability.

In the scenario where the number of neighbors is large, the number of routes is large, and most of the neighbors have the same egress policy, BGP uses the group-packaging technology to greatly improve the performance of BGP packet delivery.

---END

1.4 VPN configuration

Overview

VPN (Virtual Private Network) is a kind of secure local area network based on the Internet. Currently, the 4G Intelligent Gateways not only support the separate use of the five VPN protocols L2TP/PPTP/GRE/IPIP/IPSEC/OpenVPN, but also support VPN service is set up on the VPN, that is, VPN OVER VPN, such as GRE over IPSec, IPSec over PPTP/L2TP/GRE/IPIP. Multi-layer VPN settings can better report the security of user communication data.

1.4.1 VPDN configuration

VPDN English is Virtual Private Dial-up Networks, also known as virtual private dial-up network. It is a kind of VPN service and is a virtual private dial-up network service based on dial-up users. That is, dial-up access to the Internet is a secure virtual private network that is built using the bearer function of the IP network combined with the corresponding authentication and authorization mechanism. It is a technology that has developed rapidly in recent years with the development of the Internet.

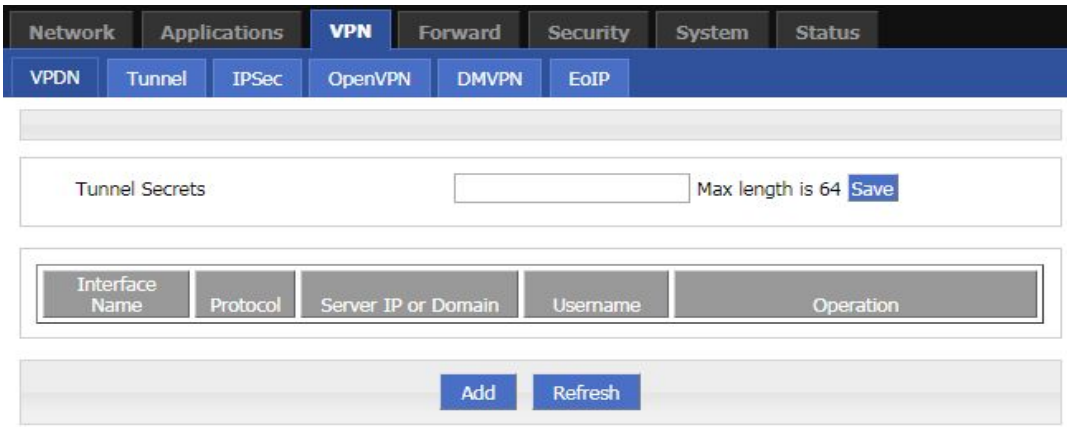
VPDN supports both L2TP and PPTP protocols.

Point to Point Tunneling Protocol (PPTP) is a network technology that supports multi-protocol virtual private networks. It is also a Layer 2 protocol. Through this protocol, remote users can securely access the corporate network through Windows mainstream operating systems and other systems equipped with peer-to-peer protocols, and can dial into the local ISP to securely connect to the corporate network through the Internet.

L2TP (Layer Two Tunneling Protocol) Abbreviation for Layer 2 Tunneling Protocol, which is a kind of VPDN (Virtual Private Dial-Up Networking) technology, which is used for channel transmission of Layer 2 data. L2TP provides a means of remote access control. A typical application scenario is: a company employee dials into the company's local network access server (NAS) through PPP, thereby accessing the company's internal network, obtaining an IP address and accessing it. Network resources for the corresponding permissions. The employee's access to the company's network is as safe and convenient as a corporate LAN.

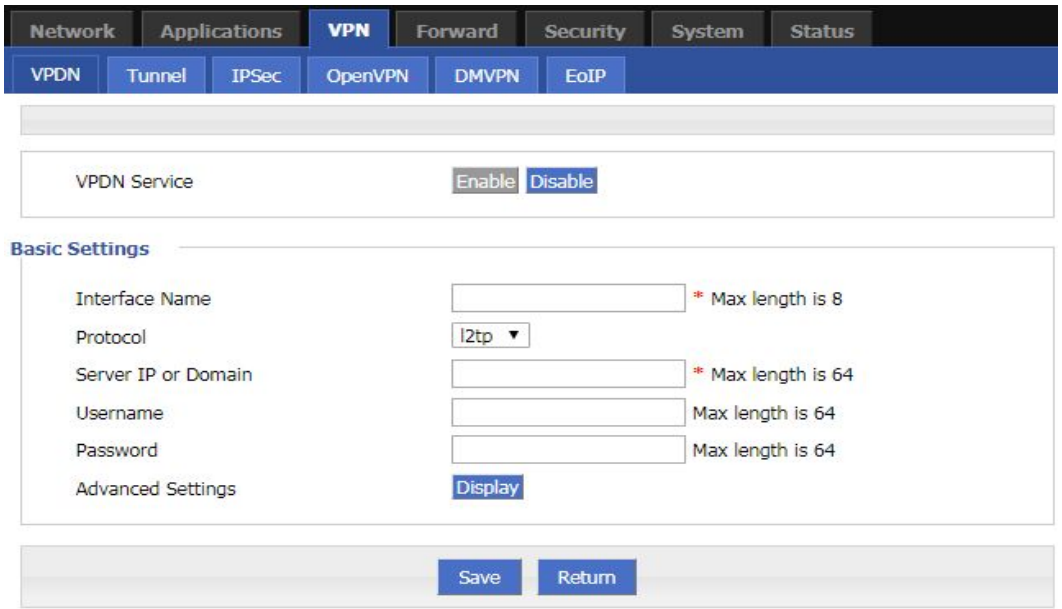
Step 1 Click “VPN > VPDN” to open the configuration page of “VPDN”.

Figure 1-12 The configuration page of VPDN



Step 2 Click “Add” to add a new VPDN rule.As shown in Figure 5-58.

Figure 1-13 VPDN rule configuration



Step 3 Configure VPDN rule parameter. See below:

Table 1-8 VPDN rule parameter instruction

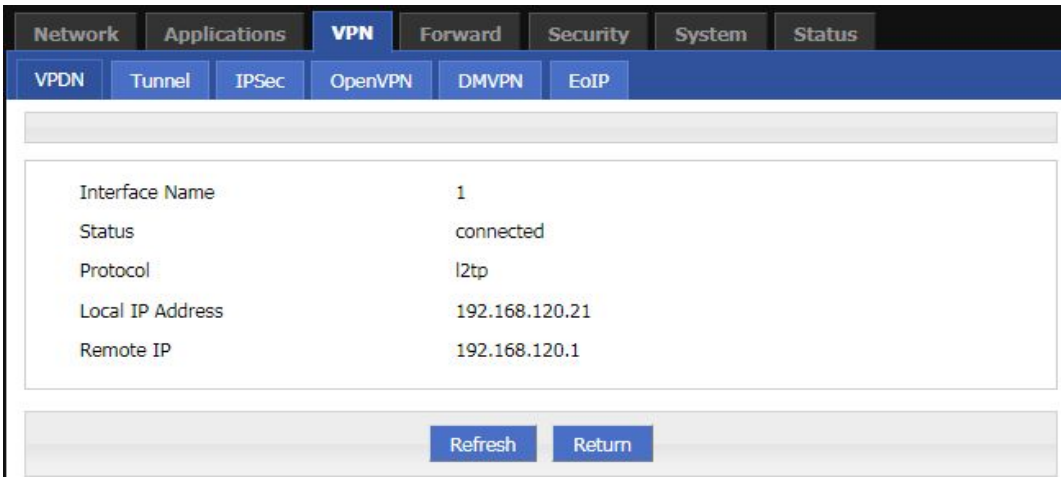
Parameter	Details	Operation
VPDN service	To enable or disable the VPDN rule	single button: • Enable • Disable
Basic Settings		
Interface name	Name of this VPDN rule	Cannot be modified after save.
protocol	VPDN protocol includes • L2TP • PPTP	Select from Dropdown List, cannot be modified after save.
Service IP or Domain	IP or domain of server to be visited	To input the IP or domain of server to be visited. Maxium 64 bytes
Username	Username of server to be visited	To input the username. Maxium 64 bytes
Password	Password of server to be visited	To input password. Maxium 64 bytes
Advanced settings	Advanced parameter of PPP link	Click “Display”
Authentication & Encryption (matching with the server when configuring, defaults to negotiation)		
CHAP	Challenge-Handshake Authentication Protocol, a way to send real password when build ppp link, improved security	• Disable • Negotiation CHAP is prior to PAP
PAP	Password Authentication Protocol	• Disable • Negotiation
MS-CHAP	MS-CHAP Microsoft Challenge-Handshake Authentication Protocol Based on MPPE	• Disable • Negotiation
MS2-CHAP	MS-CHAP second version	• Disable • Negotiation
EAP	PPP Extensible Authentication Protocol	• Disable • Negotiation
Compress (configuration needs to match the server, the default is all disabled)		
Compression Control Protocol	Negotiate which compress control protocol used on PPP link	• Disable • Negotiation

Parameter	Details	Operation
Address/Control Compression	Whether compress IP address	• Disable • Negotiation
Protocol Field Compression	Whether compress Whether compress IP address	• Disable • Negotiation
VJ TCP/IP Header Compress	Whether allow TCP/IP to communicate by compressing VJ	• Disable • Negotiation
Connection-ID Compression	Whether allow TCP/IP to communicate by compressing ID in the first	• Disable • Negotiation
more		
Debug	Enable PPP dialing log, default value is enable, in order to check more info about dialing, suggest no changing	• Disable • Negotiation
Peer's DNS	Auto get peer DNS when PPP dialing. DNS is necessary if want visit domain name. In order to forbid LAN pc visit domain name, you may disable it	• Disable • Negotiation
LCP Interval/LCP Retry	After PPP dialing succeed, LCP is needed to keep PPP link alive. Also it could be used to quickly spot network interrupt and reconnect	Value area : 1~512 Unit: second Default value: 30/5
MTU	the number of bytes of the maximum transfer unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
MRU	the number of bytes of the maximum receive unit by PPP interface, sometimes financial data has request on this	Value area : 128~16364 byte
Local IP	Set the local IP address when PPP dialing, need ISP support	A.B.C.D, Example: 10.10.10.1
Remote IP	Set the remote IP address when PPP dialing, need the support of ISP	A.B.C.D, Example: 10.10.10.254
Professional	• nomppe • mppe required • mppe stateless • nodeflate • nobsdcomp • default-asyncmap	Do not suggest modify, please contact us for help if necessary

Step 4 Single click “save” icon to finish.

After a VPDN rule is added, router will build VPN communication with service address automatically. To see the tunnel status, click “View” in “Tunnel” tab.

Figure 1-14 L2TP tunnel status



---END

1.4.2 Tunnel configuration

Tunnel technology transfers data between the networks through the Internet infrastructure. In the whole process of transmission, when the encapsulated data package delivered on a public Internet, the logic path which the packet passes through is called tunnel. GRE and IPIP Tunnel configuration supports two modes.

GRE (Generic Routing Encapsulation, Generic Routing protocol encapsulation) specifies how to use a network protocol to another network protocol encapsulation method. The main purpose of the GRE protocol, there are two: internal protocol encapsulation and private address encapsulation.

IPIP tunnel is a simple agreement between two routers for IP packet encapsulation, IPIP tunnel interface will be like a physical interface in the interface list, many routers including Cisco, basically support the agreement. This agreement enables multiple network distribution possible.

Step 1 Log in to the 4G Intelligent Gateway configuration page.

For details on how to log in to the device, see 5.2.1 “Logging In to the WEB Configuration page”.

Step 2 Click “VPN > Tunnel” to open the configuration page of “Tunnel” .

Step 3 Click Add to add a new tunnel rule. See below:

Figure 1-15 Tunnel configuration

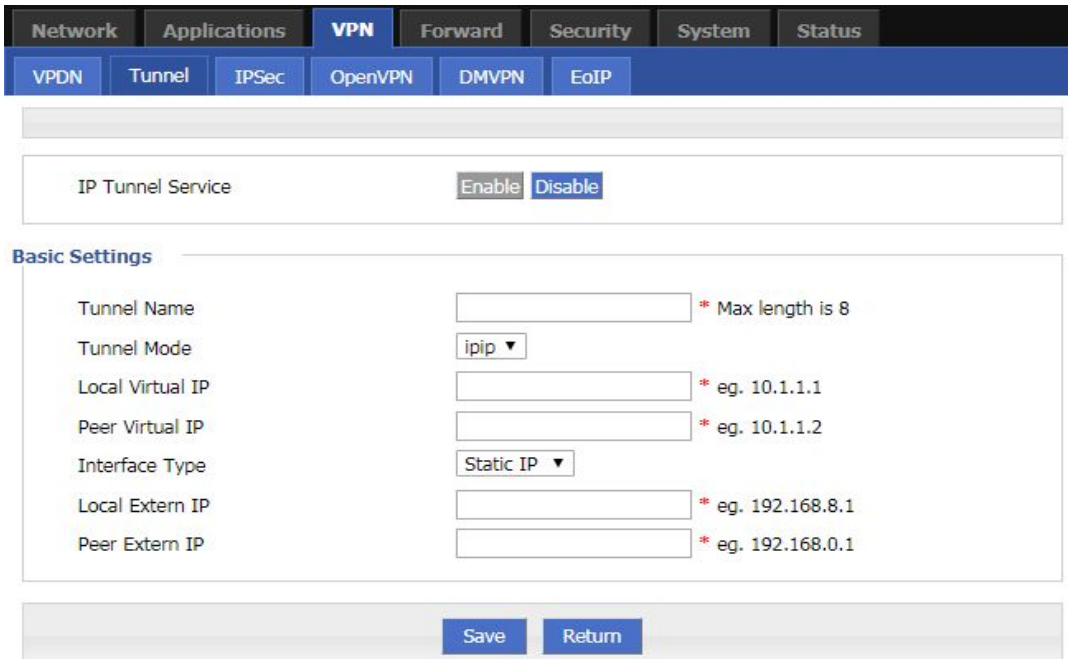


Table 1-9 Tunnel rule parameter instruction

Parameter	Details	Operation
IP Tunnel Service	To enable or disable IP tunnel service	Button selection: • Enable • Disable
Basic Settings		
Tunnel name	Name of the tunnel, cannot be modified after save	An easily identifiable name is recommended. Modifications are not allowed after saving. The maximum support input is 8 characters.
Tunnel Mode	Tunnel mode:	Select from Dropdown List: • Gre • ipip
Local virtual IP	Virtual IP address of local tunnel	Format: interface type A.B.C.D/M.
Peer virtual IP	Virtual IP address of peer tunnel	Format: interface type A.B.C.D/M.
Interface type	To choose “interface” or “static IP”	Select from Dropdown List. • Static IP • Interface

Parameter	Details	Operation
Local Extern interface	This parameter will need to be set if “interface” is selected in “interface type”. Choose any connected interface as external interface	Select from Dropdown List. • modem • eth0
Local extern IP	This parameter need to be set if “static IP” is selected for “interface type”. It is to set IP address to external network	Format: interface type A.B.C.D/M.
Peer extern IP	External interface IP of counterpart network tunnel. Usually a public IP address, also can be a LAN IP	Format: interface type A.B.C.D/M.
Tunnel Key	When the tunnel mode is set to gre, the tunnel key is set to unlock the tunnel. The two sides of the tunnel must be set consistently.	Enter it manually. Input range: 0~4294967295
Keep-alive Interval	The tunnel keepalive detection mechanism is used to detect whether the physical link of the tunnel is connected. This area is used to set the sending time of keepalive packets.	Enter it manually. Input range: 1~32767
Keep-alive Retry	The tunnel keepalive detection mechanism is used to detect whether the physical link of the tunnel is connected. This is used to set the keepalive message connection to be received several times, and the tunnel is disconnected.	Enter it manually. Input range: 1~255

Step 4 Single click “save” icon to finish.

---END

1.4.3 IPSec configuration

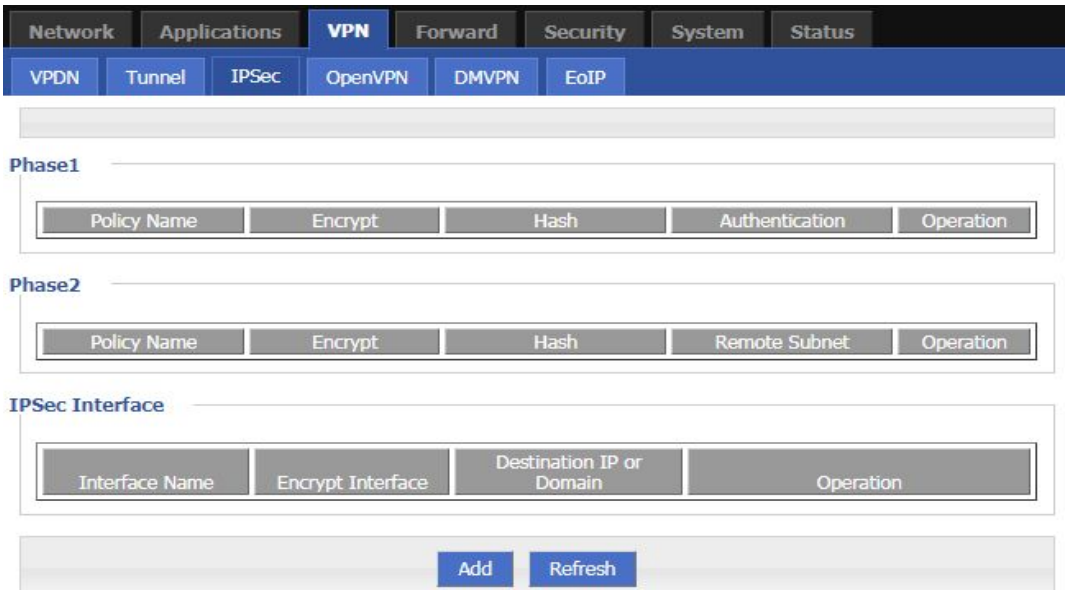
IPSec (IP_SECURITY) is a protocol built on top of the Internet Protocol (IP) layer. It enables two or more hosts to communicate in a secure manner. IPSec is the long-term direction of secure networking. It provides proactive protection through end-to-end security to prevent attacks from private networks and the Internet. The IPSec in the and 4G Intelligent Gateways uses the common phase1 to negotiate with most IPSec servers. The 4G Intelligent Gateways also support IPSec through other interfaces (such as pulling them through the modem), eliminating the need for manual operation by the user. IPSec has two modes: tunnel mode and transmission mode.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

Step 2 Click "VPN>IPSEC"

Open the IPSec Configuration page. See below:

Figure 1-16 The page of IPSec



Step 3 Click "Add" to add a new IPSec rule. There are 3 phases for IPSec configuration:

1. Phase 1 parameter

Figure 1-17 IPSec phase 1 configuration

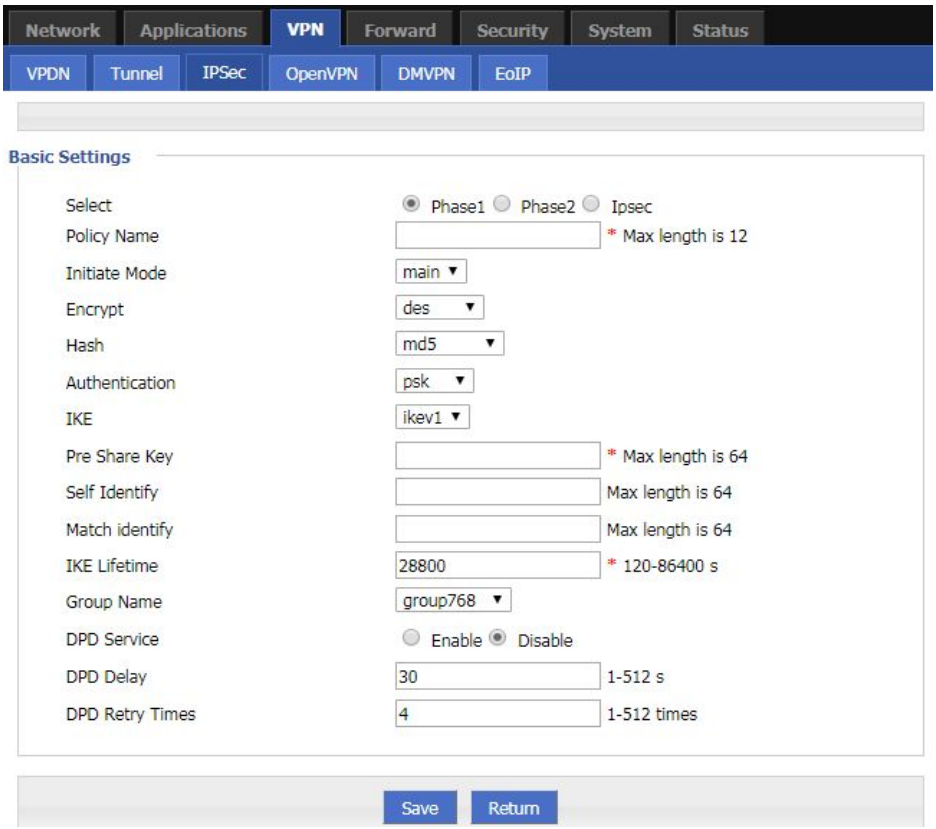


Table 1-10 The instruction of parameters of IPSec Phase 1

Parameter	Details	Operation
Basic Settings		
Select	Set the phase type of IPSec, including the first phase, the second phase, and the third phase.	Select “Phase 1”
Policy Name	The name of this stage is mainly used for the matching of the third stage.	To input the name of phase 1. Cannot be changed after save. Supports up to 12 characters of input.
Initial Mode	The first phase of IPSec negotiation mode, including "main" (main mode) and "aggr" (barbaric mode).	Select from Dropdown List, “aggr” is recommended
Encrypt	First stage encryption method selection.	Select from Dropdown List • des • 3des • aes256 • aes192 • aes128
Hash	First stage hash algorithm selection.	Select from Dropdown List • md5 • sha1 • sha2_256
Authentication	The first stage of the certification method selection.	Select from Dropdown List: • psk • Rsasig • xauth
IKE	The first phase of the IKE version selection.	Select from Dropdown List: • ikev1 • Ikev2
Pre Share Key	To set pre share key	Max 24 letters
Self Identify	Configure the IPSEC local ID to indicate the identity of the local end. If not configured, the IP address is used.	You can fill in the IPSec local ID. It must be the same as the peer ID preset by the IPSec peer server. Maxium 64 bytes.
Match Identify	Configure the IPSEC peer ID to indicate the peer identity. If not configured, the IP address is used.	can fill in the IPSec peer ID, which is the same as the local ID of the IPSec peer server. Word type,Maxium 64 bytes.
IKE Lifetime	Life time of IKE key	Value area: 120~86400 Unit: second

Parameter	Details	Operation
Group Name	Configured here as the key length for the first phase of IKE negotiation.	Select from Dropdown List • group768 • group1024 • group1536 • group2048 • group3072 • Grouo4096
DPD Service	To enable DPD service,The DPD peer detection needs to be supported by the peer server. It is used to check whether the IKE environment is normal. If the IKE environment is abnormal, the IKE environment is renegotiated to ensure the security and connectivity stability and connectivity of the IPSec environment.	Dropdown list: • Enable • Disable Click "Enable" to enable the peer detection service.
DPD Delay	To set DPD check interval time	Manual input Value area : 1~512 Unit: second
DPD Retry Times	Max times to continuous DPD check failure.	Manual input Value area: 1~512 Unit: times

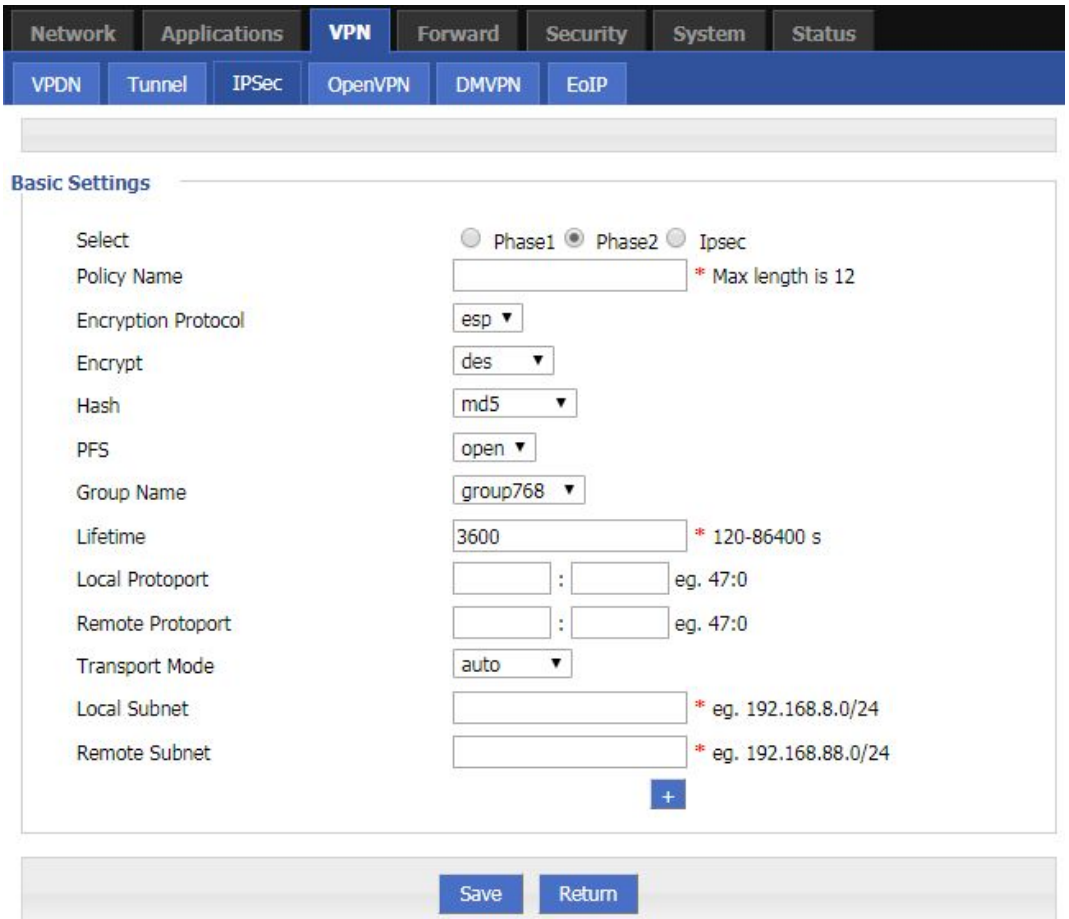
Single click "save" to finish the configuration of phase 1 .

CAUTION

In above parameters, "Initial Mode", "Encrypt", "Hash", "Authentication" "Pre Share Key", "IKE Lifetime", "Group Name"DH Group" need to match parameter of IPSec server. "Self Identify" and "Match Identify" needs to match "match Identify" and "Self Identify" of IPSec sever respectively.

2. Parameter configuration for the second phase. See below:

Figure 1-18 The configuration page of IPSec phase 2



See below parameters instruction of the second phase of the IPSec rule.

Table 1-11 The parameters of the second phase of the IPSec rule

Parameter	Details	Operation
Basic Settings		
Select	Set the phase type of IPSec, including the first phase, the second phase, and the third phase.	Radio button selection. The second phase of the rule is added here, so select "Phase 2".
Policy Name	The name of this stage is mainly used for the matching of the third stage.	To input the name of phase 2. Cannot be changed after save
Encryption Protocol	Supports esp	Select the authentication encryption protocol to set from the drop-down list
Encrypt	The choice of the second stage encryption method.	Select from Dropdown List • des • 3des • aes256 • aes192 • aes128

Parameter	Details	Operation
Hash	The second stage of hash algorithm selection	Select from Dropdown List • md5 • sha1 • Sha2_256
Group Name	Used when perfect forward encryption is enabled, here configured as the key length for IPSec second-phase SA negotiation.	Select from Dropdown List • group768 • group1024 • group1536 • group2048 • group3072 • Grouo4096
PFS	Enabling or disabling perfect forward encryption, enabling perfect forward encryption increases system overhead, but increases IPSec security.	Select from Dropdown List Select open or close according to the settings of the peer IPSec server.
Lifetime	IPSec SA key life time	Value area: 120~86400 Unit: second
Local Protoport	Configure the protocol and port that the local end needs to encrypt.	Manual input, the front box enters the protocol code, and the rear box enters the port.
Remote Protoport	Configure the protocol and port that the peer needs to encrypt.	Manual input, the front box enters the protocol code, and the rear box enters the port.
Transport Mode	Supports tunnel, transport and auto.	Select from Dropdown List • auto • Transport • tunnel
Local Subnet	Set local subnet	No need to set for “transport” mode, only for “auto” and “tunnel”. Format: A.B.C.D/M
Remote Subnet	To set local subnet	No need to set for “transport” mode, only for “auto” and “tunnel”. Format: A.B.C.D/M

Single click “save” to finish the configuration of phase 2 .

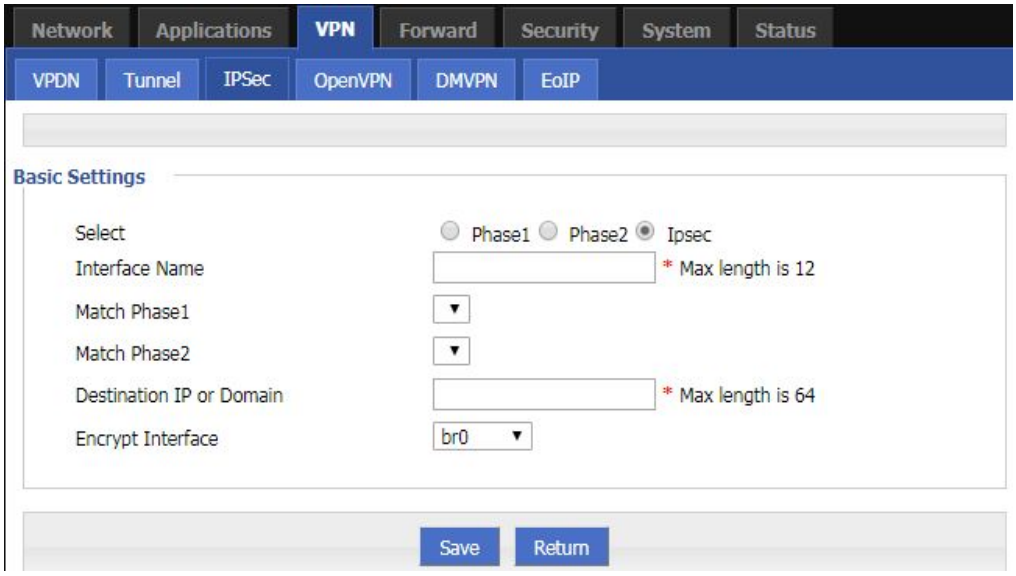
CAUTION

Among the above parameters, the transmission protocol, encryption method, hash algorithm, DH group, perfect forward encryption, key lifetime, etc. must be consistent with the IPSec server configuration; if the transmission mode is set to automatic or tunnel mode, the local subnet and the remote terminal network must be consistent with the configuration of the remote subnet and local subnet in the IPSec server.

The protocol code of the local protocol port and the remote protocol port must be the same, indicating that one protocol is encrypted. When the local protocol port and the remote protocol port are configured, IPSec encrypts the protocol and port, and other communications are not encrypted. When this parameter is not configured, it means that IPSec encrypts all communications.

3. Match phase parameter configuration. See below:

Figure 1-19 The matching phase configuration page



set the matching phase parameters of the IPSec rule. After the configuration is complete, click “Save”.

NOTE

When the encrypted interface selects br0 and the br0 interface has multiple addresses, the address selected by IPSec is the IP1 address of br0.

Table 5-41 describes the parameters of the matching phase of the IPSec rule.

Table 1-12 The parameters of the matching phase of the IPSec rule.

Parameter	Details	Operation
Basic Settings		
Select	Set the phase type of IPSec, including the first phase, the second phase, and the third phase.	Radio button selection. The rule added here is the matching phase, so select "IPSec".
Interface Name	The name of this stage is mainly used for the matching of the third stage.	A maximum of 12-bit strings are allowed. Fill in the name of the stage. Cannot be modified after saving
Match Phase1	To select a matching name of “phase1”	Select from Dropdown List. Select the policy name for the first

Parameter	Details	Operation
		phase configuration.
Match Phase2	To select a matching name of “phase2”	Select from Dropdown List Select the policy name for the second phase configuration.
Destination IP or Domain	IP or domain name of the IPSec peer server.	Fill in the IP or domain name of the IPSec peer server. Maximum allowable input of 64-bit strings.
Encryption Interface	To select binding interface of IPSec. to bind VPDN/modem/br0 as local interface of IPSec initial can support IPSec OVER VPDN. In addition, after binding, IPSec rule will change as per the charge of binding interface. Thus can resume link of IPSec dialing interface and keep IPSec linked as soon as possible	Select from Dropdown List

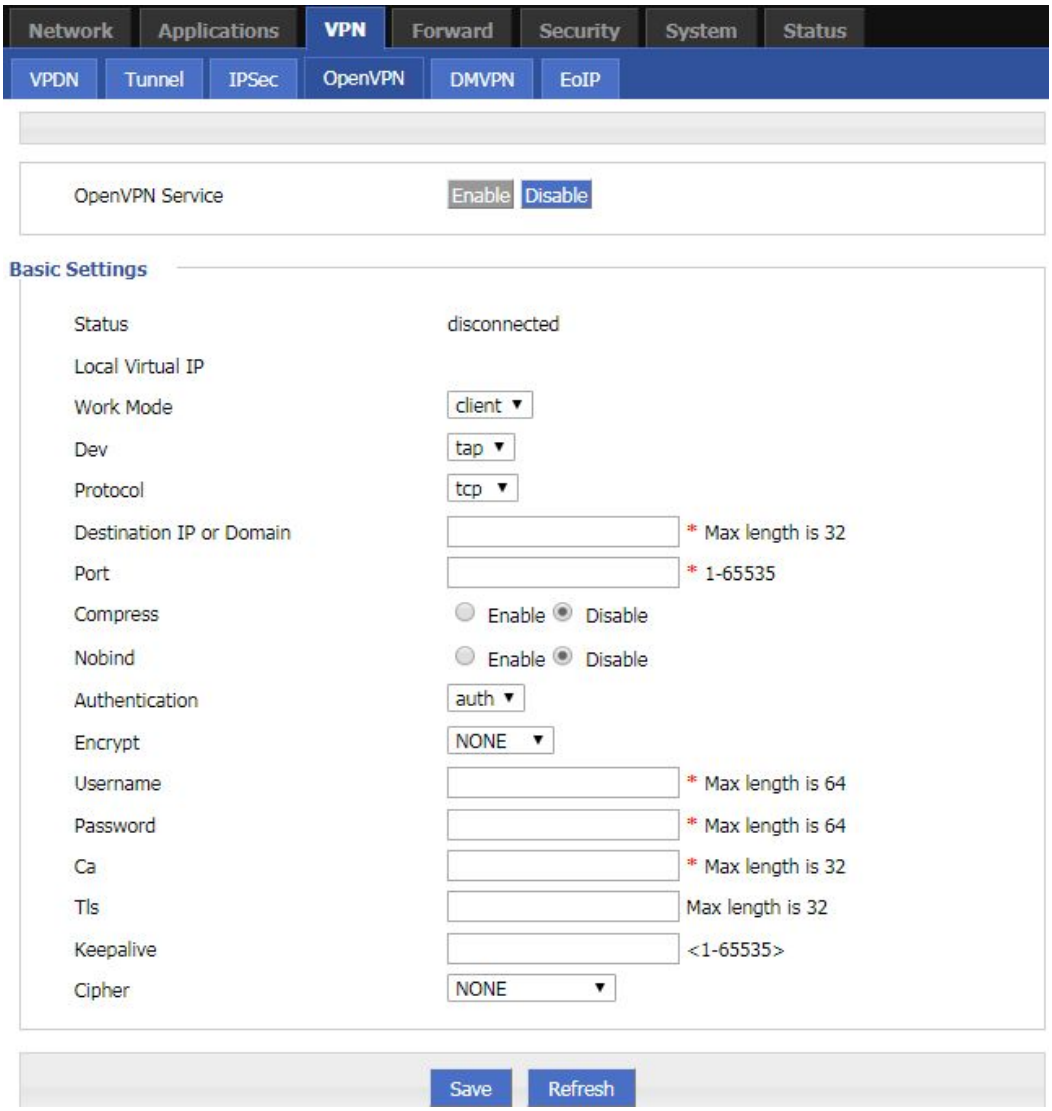
---END

1.4.4 Open VPN Configuration

OpenVPN is the VPN achievement based on the OpenSSL library's application layer. Compared with the traditional VPN, it is simple and easy to use. OpenVPN all the communications are based on a signal IP port, and it use the UDP protocol transports default and recommended. It can also support the TCP protocol. OpenVPN connection can through most of the proxy servers and work well in the NAT environment. Its server side has the function of pushing some network configuration information (including IP address, route configuration and so on) to the client side. OpenVPN offers two types of interfaces for networking via the universal TUN/TAP driver. It can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. Port 1194 is the official IANA (Internet Assigned Numbers Authority) assigned port number for OpenVPN.

Step 1 Click "VPN > OpenVPN"to open the configuration page of "OpenVPN". See below:

Figure 1-20 The configuration page of OpenVPN



Step 2 Set the parameters of Open VPN. See below:

Table 1-13 The instruction of the parameters of OpenVPN

Parameter	Detail	Operation
OPENVPN Service	Enable OPENVPN Service.	Click button options: • Enable • Disable
Basic Setting		
Status	OpenVPN connection status display	There are two states: disconnected, connected
Local Virtual IP	Display of virtual interface IP address after OpenVPN connection	Display the IP address of the virtual interface

Parameter	Detail	Operation
Work Mode	Supports two working modes: ● Client mode: client type mode ● Multi mode: peer to peer working mode (peer is non-server)	Dropdown list options: • client • multi Select the required working mode from dropdown list.
Dev	Dev represents the network interface type, and supports two types: • Tun(OSI Layer 3):Simulates network layer device to operate the third layer data packets, such as IP packets • Tap(OSI Layer 2):Equates to an Ethernet device to operate the second layer data packets, such as Ethernet data frame.	Dropdown list options: • tun • tap Select the required working mode from dropdown list. Demand consistent with peer.
Protocol	• Data transfer protocol type settings: ● TCP protocol: A kind of connection oriented reliable transmission protocol, which is suitable for the occasions where the reliability requirement is high and the communication efficiency is not high. ● UDP protocol: A kind of non - connection unreliable transmission protocol, which is suitable for the scene with relatively high efficiency and relatively low reliability.	Dropdown list options: • tcp • udp Select the required working mode from dropdown list. Demand consistent with peer.
Destination IP or domain	Specifies connected server address	WORD type， max 32 bytes. Demand consistent with peer.
Port	Specifies connected server port	Value range: 1~65535 • Default: 1194 Demand consistent with peer.
Compress	Compression protocol: configure whether VPN connection compression is opened. If the server is open, the client must open.	Click button options: • Enable • Disable
Nobind	Configure whether to bind to the specific local port.	Click button options: • Enable • Disable
Authentication	Configuring the VPN data transfer mode: ● SSL: encrypt the network connection in transport layer, high safety factor. ● Text: transport with text form during transmission, low safety factor ● Auth: username + password + ca verification, high security factor	Dropdown list options: • auth • ssl • text Select the required data transfer type from dropdown list.

Parameter	Detail	Operation
Encrypt	Data encryption method	Dropdown list options: • NONE • MD5 • SHA1 • SHA224 • SHA256 • SHA384 • SHA512
Ca	Specifies the file path for the client CA certificate	WORD type， max 32 bytes.
Key	Specifies the private key path for the current client	WORD type， max 32 bytes.
Cert	Specifies the certificate file path for the current client	WORD type， max 32 bytes.”。
Tls	Open TLS, if the server is open, the client must also open. TLS: secure transport layer protocol (TLS) to provide confidentiality and data integrity between two communication applications. The protocol consists of two layers: the TLS record protocol (TLS Record) and the TLS handshake protocol (TLS Handshake)	WORD type， max 32 bytes.
Keep alive	The message keepalive mechanism between it and the OpenVPN server.	Enter it manually. Input range: 1~65535 Unit: second
Cipher	SSL's encryption algorithm system.	Drop box options: • NONE • BF-CBC • DES-CBC • RC2-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • RC2-40-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC

Click “Save” to finish the configuration of OpenVPN.

---END

1.4.5 DMVPN Configuration

Dynamic Multipoint VPN, dynamic multipoint VPN. DMVPN is a MGRE+NHRP+IPSEC solution that is a simple, dynamic, and scalable way. DMVPN supports spoke dynamic addresses, adding new spokes, without changing the hub configuration. The spoke to spoke dynamic generation tunnel is triggered by traffic and is encrypted using IPSec.

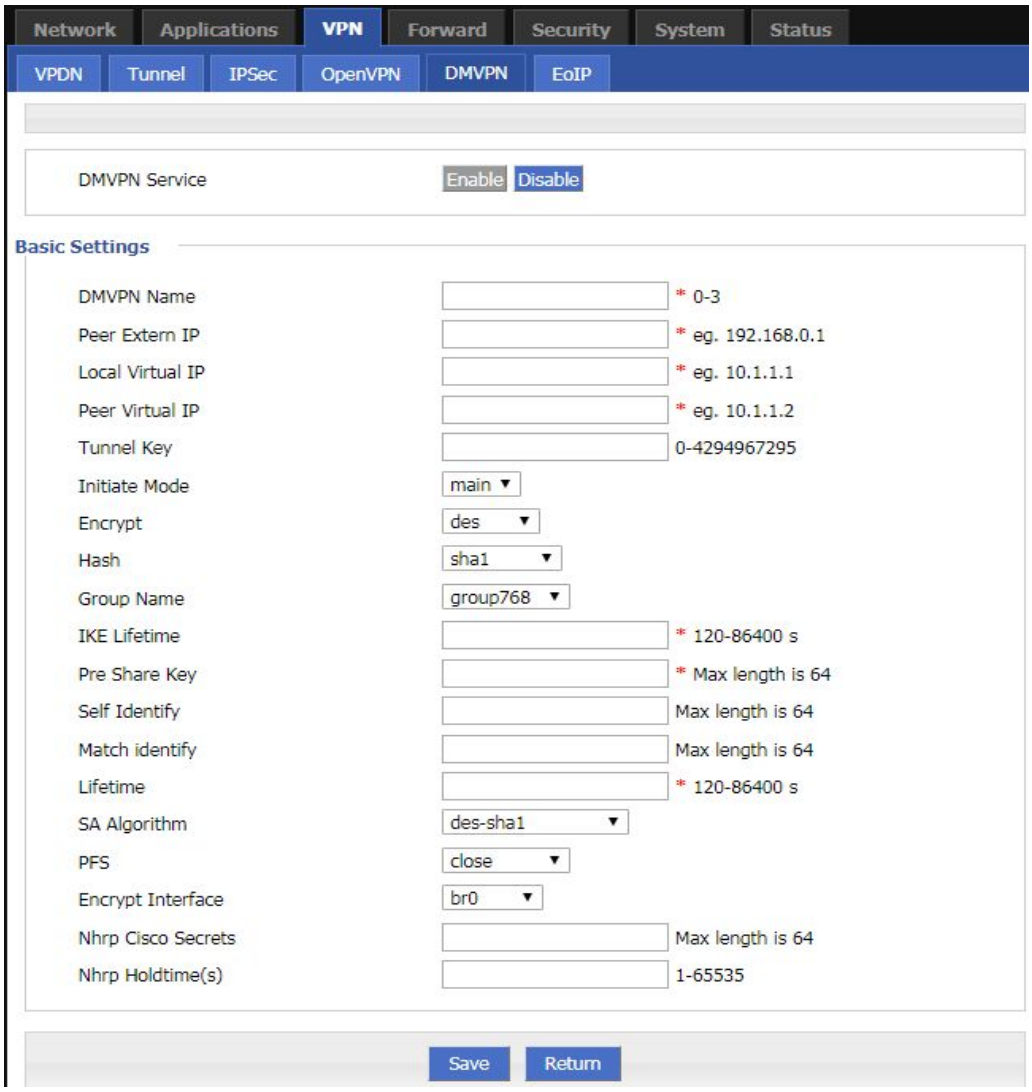
Step 1 Click "VPN > DMVPN".

Step 2 Open the page of “DMVPN” . See below:

Figure 1-21 The page of “DMVPN”

Step 3 Click Add to add a new DMVPN rule. See below:

Figure 1-22 The configuration page of "DMVPN"



Step 4 Configure DMVPN rule parameters. See below:

Table 1-14 The instruction of the parameters of DMVPN

Parameter	Detail	Operation
DMVPN Service	DMVPN service switch	Button selection: • Enable • Disable Gray status indicates the currently selected status
Basic settings		
DMVPN Name	DMVPN rule name input	Enter it manually. Input range: 0~3
Peer Extern IP	The external interface IP of the peer network of the tunnel is usually the	Fill in the external interface IP of the tunnel peer network.

Parameter	Detail	Operation
	IP address of the public network. It can also be the IP address of different intranets.。	Format:A.B.C.D
Local Virtual IP	The virtual IP address of the local tunnel.	Enter it manually. Format:A.B.C.D
Peer Virtual IP	The virtual IP address of the local tunnel.	Enter it manually. Format:A.B.C.D
Tunnel Key	Used to unlock the tunnel. The two sides of the tunnel must be set consistently.	Enter it manually. Input range: 0~4294967295
Initiate Mode	The first phase of IPSec negotiation mode, including "main" (main mode) and "aggr" (barbaric mode).	Drop-down list selection. • main • aggr Select the startup mode to be set from the drop-down list. Generally, both ends have NAT and use USERID to suggest "savage mode".
Encrypt	The choice of the first stage encryption method	Drop-down list selection. • des • 3des • aes256 • aes192 • aes128
Hash	The choice of the first stage hash algorithm	Drop-down list selection. • md5 • sha1 • sha2_256
Group Name	Configured here as the key length for the first phase of IKE negotiation.	Drop-down list selection. • group768 • group1024 • group1536 • group2048 • group3072 • group4096
IKE Lifetime	The lifetime of the IKE key.	Fill in the appropriate key life cycle. Value range: 120~86400 Unit: second
Pre Share Key	Set the pre-shared key.	Fill in the pre-shared key preset by the IPSec peer server. An alphanumeric string of up to 64 characters in length.

Parameter	Detail	Operation
Self Identify	Configure the IPSEC local ID to indicate the identity of the local end. If not configured, the IP address is used.	You can fill in the IPSec local ID. It must be the same as the peer ID preset by the IPSec peer server. WORD type.An alphanumeric string of up to 64 characters in length.In addition, the local identifier supports space input.
Match identify	Configure the IPSEC peer ID to indicate the peer identity. If not configured, the IP address is used.	You can fill in the IPSec peer ID. It must be the same as the local ID preset by the IPSec peer server. WORD type.An alphanumeric string of up to 64 characters in length.In addition, the peer identifier supports space input.
Lifetime	Key lifetime of the IPSec SA (IPSec SA).	Fill in the life cycle of the appropriate key. Value range: 120~86400 Unit: second
SA Algorithm	The choice of the second stage encryption and hash combination	Drop-down list selection. • des-sha1 • des-sha2_256 • des-md5 • 3des-sha1 • 3des-sha2_256 • 3des-md5 • aes128-sha1 • aes128-sha2_256 • aes128-md5 • aes192-sha1 • aes192-sha2_256 • aes192-md5 • aes256-sha1 • aes256-sha2_256 • aes256-md5
PFS	After the key length is selected, the perfect forward encryption is automatically enabled. This is configured as the key length of the IPSec second-phase SA negotiation.	Drop-down list selection. • close • group768 • group1024 • group1536 • group2048 • group3072 • group4096
Encrypt Interface	Select the binding interface of IPSec	Drop-down list selection. • modem • eth0 • br0 In addition, when a virtual interface is configured, such as l2tp, tunnel, etc., it can

Parameter	Detail	Operation
		also be selected in the drop-down list.
Nhrp Cisco Secrets	The NHRP next hop routing resolution protocol is used to solve point-to-multipoint environmental data communication problems. Fill in the NHRP key here, and it needs to be consistent with the peer.	Enter it manually. Maximum support input of 64 characters.
Nhrp Holdtime(s)	NHRP retention time	Enter it manually. Input range: 1~65535

Step 5 Click"Save" to complete the configuration of DMVPN rule.

---END

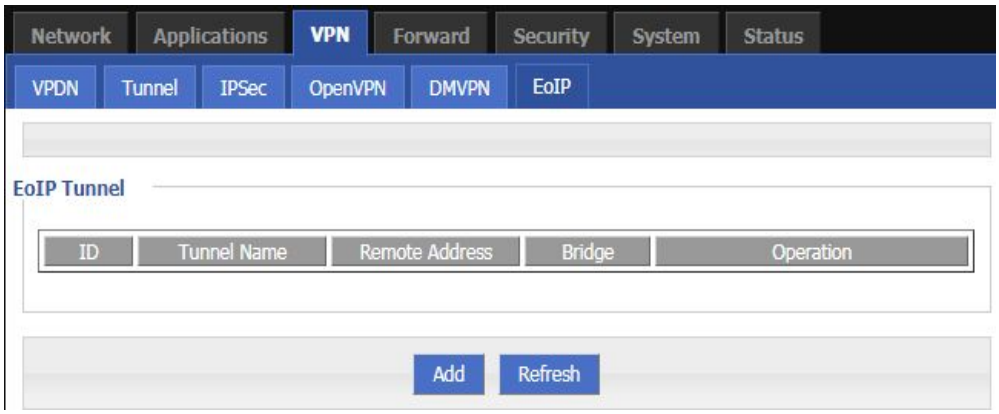
1.4.6 EOIP Configuration

An EoIP (Ethernet over IP) tunnel is an Ethernet tunneling protocol established between the IP transport layers of two routers. It is a free protocol of MikroTik RouterOS. The EoIP interface behaves like an Ethernet transport. When the bridge function of the router is enabled, all Ethernet data traffic (all Ethernet protocols) will be bridged as if there is physical between the two routers (with bridging enabled). The switch interface is the same as the fiber transceiver.

Step 1 Click"VPN>EOIP".

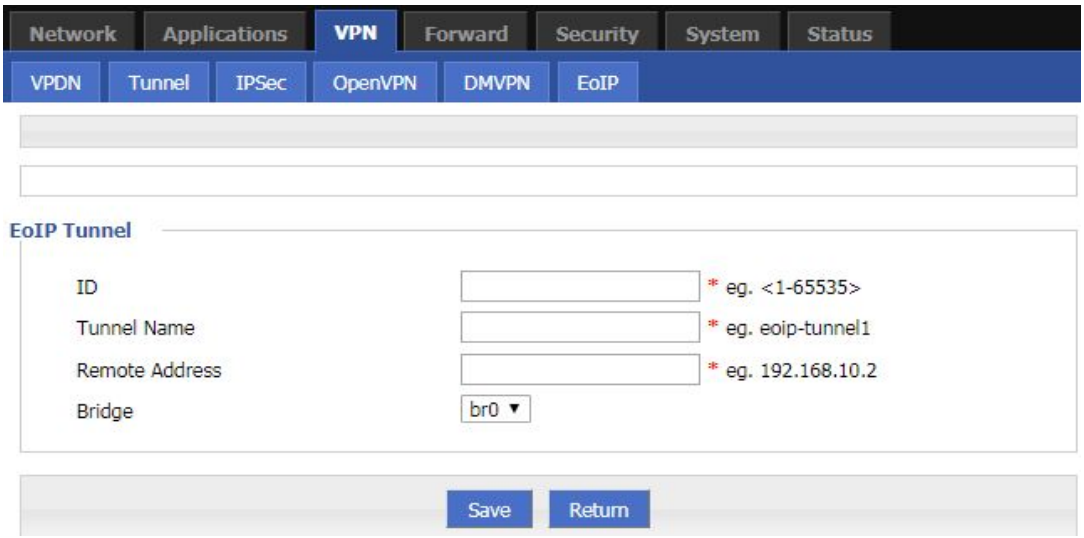
Step 2 Open the page of "EOIP". See below:

Figure 1-23 The page of "EOIP"



Step 3 Click "Add" to add a new EOIP rule. See below:

Figure 1-24 The configuration page of "EOIP"



Step 4 Configure parameters for EOIP rules. See below:

Table 1-15 The instruction of the parameters of EOIP

Parameter	Detail	Operation
ID	Input of EOIP ID value	Enter it manually. Input range: 1~65535 ID cannot be modified after saving
Tunnel Name	Input of EOIP's Tunnel Name	Enter it manually. Maximum support for inputting 64 characters. Can be modified after saving.
Remote Address	Input of the peer address	Enter it manually. Format:A.B.C.D
Bridge	EOIP bridge port selection	Currently only supports br0.

Step 5 Click "Save" to finish the configuration of EOIP rule.

---END

1.5 System Management Configuration

Overview

4G Intelligent Gateway system management function is mainly to carry out some daily maintenance operations on the system. For example, through the log to analyze the operation of the system, management of user account information, network testing, and upgrade of system files.

1.5.1 Local Log

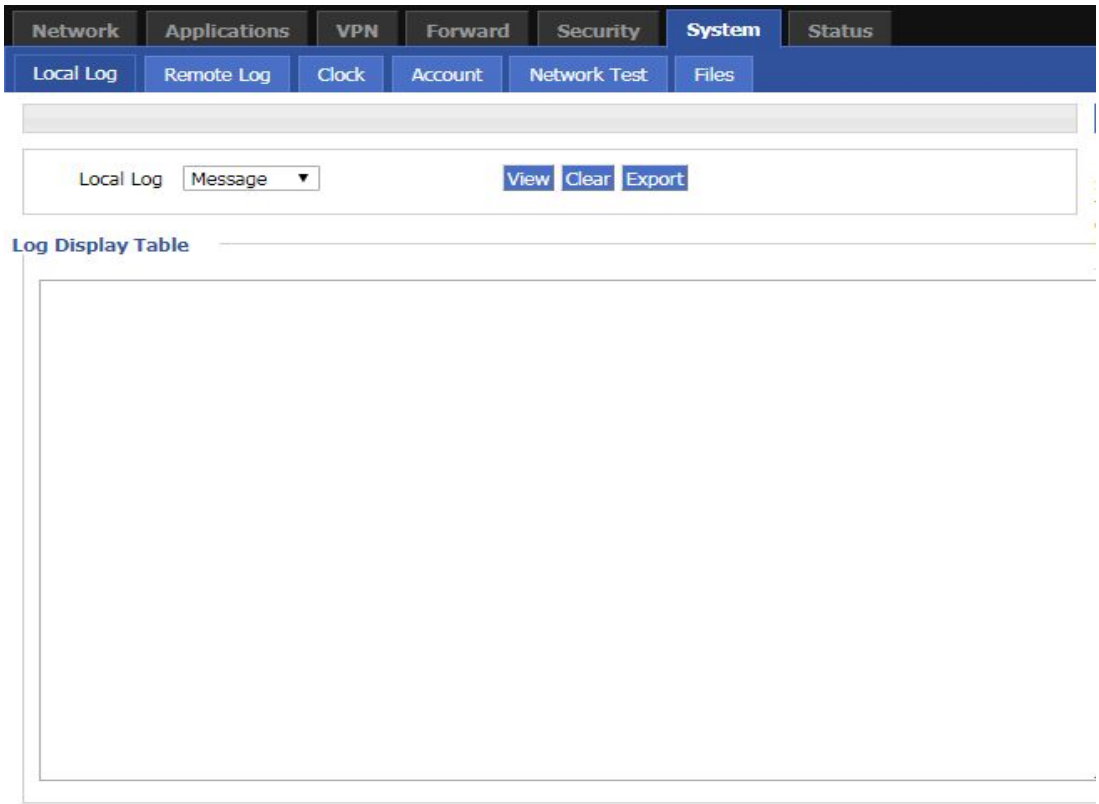
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “System>Local Log”.

Open the configuration page of”Local Log”. See below:

Figure 1-25 Local Log tab



Step 3 Select type of “Local Log” and then click “View” to see log.

Click “Clear” to clear the log info in the “Log Table”, and click “Export” to export log in your local PC.

There are 3 kinds of log:

- Message: system log, to record the running log of router, usually for most of users.
- Application: application program log, to record the Open or close of some application programs.
- Kernel: kernel log of router, usually for R&D engineers.

---END

1.5.2 Remote Log

The remote log is mainly used to connect to the remote log server. The router can upload the local log to the remote log server. The configuration steps are as follows:

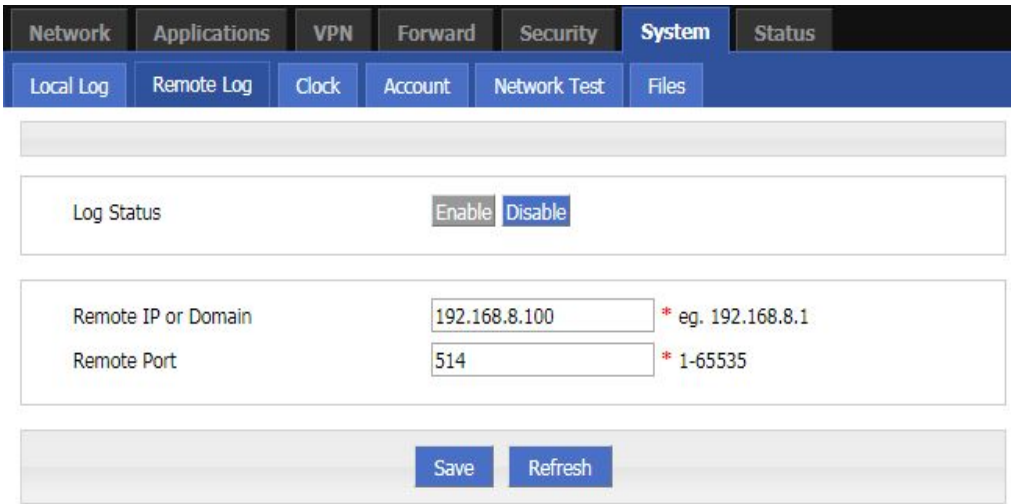
Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “System>Remote Log”.

Open the configuration page of”Remote Log”. See below:

Figure 1-26 The configuration page of Remote Log



Step 3 Configure parameters for the system log. See below:

Table 1-16 The instruction of Remote log parameter

Parameter	Details	Operation
Log Status	To enable or disable remote log	Click “Enable”to enable the remote log.
Remote IP or Domain	IP address of the remote log server (either the IP address of the LAN side PC or the public network address).	To input the IP address or domain to receive log
Remote Port	Port number of the remote log server.	Default port: 514

Step 4 Single click “save” to finish the configuration of “Remote Log” parameter.

NOTE

A software tool Syslog is used to receive remote log in server. Syslog can be downloaded at website of http://www.hongdian.com.

---END

1.5.3 Clock

4G Intelligent Gateway supports NTP (Network Time Protocol) network protocol timing. When the NTP network is paired, the system time of the router can be ensured to correspond to the actual time. The functions such as task management can be executed at the correct time. Specific steps are as follows.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “System > Clock” to open the page of “Clock”. See below:

Figure 1-27 “NTP” Time Synch.

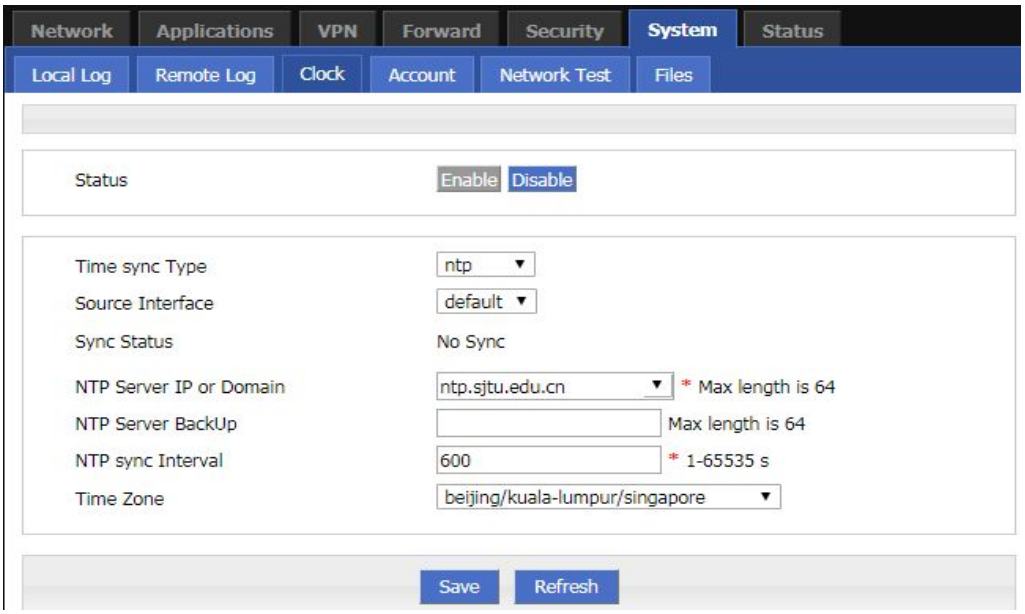
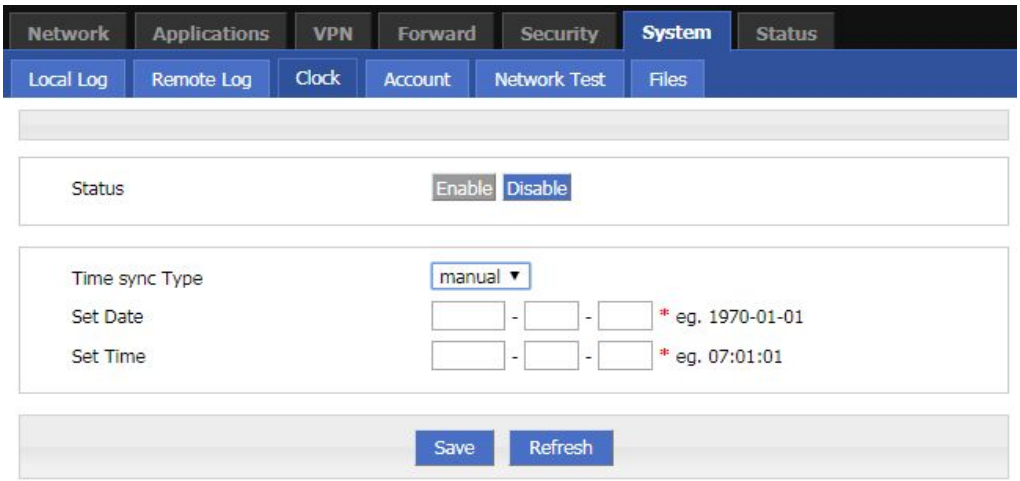


Figure 1-28 Manually configure Time Sync Type



Step 3 Configure parameters for system time.

The parameter description is shown in Table 5-46.

Table 1-17 Clock Parameter instruction

Parameter	Details	Operation
Status	To enable to disable Time Synchronization service	• To click “Enable” or “Disable”

Time Synch. Type	Type to synchronize system time	Select from Dropdown List: • Ntp(correcting time via the network) • manual(using the manual method for proofreading time)
When select “NTP” in “Time Synch. Type”		
Source Interface	The original interface with the NTP server	Select from Dropdown List: • modem • eth0 • Br0
Sync Status	Display of NTP status	NTP synchronization successfully displays "Sync success" NTP synchronization failed to display "No Sync"
NTP Server IP or Domain	IP or domain of NTP server	Select from Dropdown List
NTP Server Backup	Backup NTP server	Manual input server domain or IP address
NTP Synch. Interval	Interval for NTP client to check time with NTP Server. E.g. every 10 minutes	Value area: 1~65535 Unit: second Default: 600 s
Time Zone	Time Zone	Select from Dropdown List
Time Zone Number	For “Custom” option in “Time Zone”. E.g. +8 or -4	WORD type
When select “Manual” in “Time Synch. Type”(This page only shows the configured time, the system real time is in the upper right corner of the WEB page)		
Set Date	To set date	YYYY-MM-DD e.g. 1970-01-01
Set Time	To set time	HH:MM:mm E.g. 07:01:01

Step 4 Single click “save” to finish the configuration of remote log .

---END

1.5.4 Account

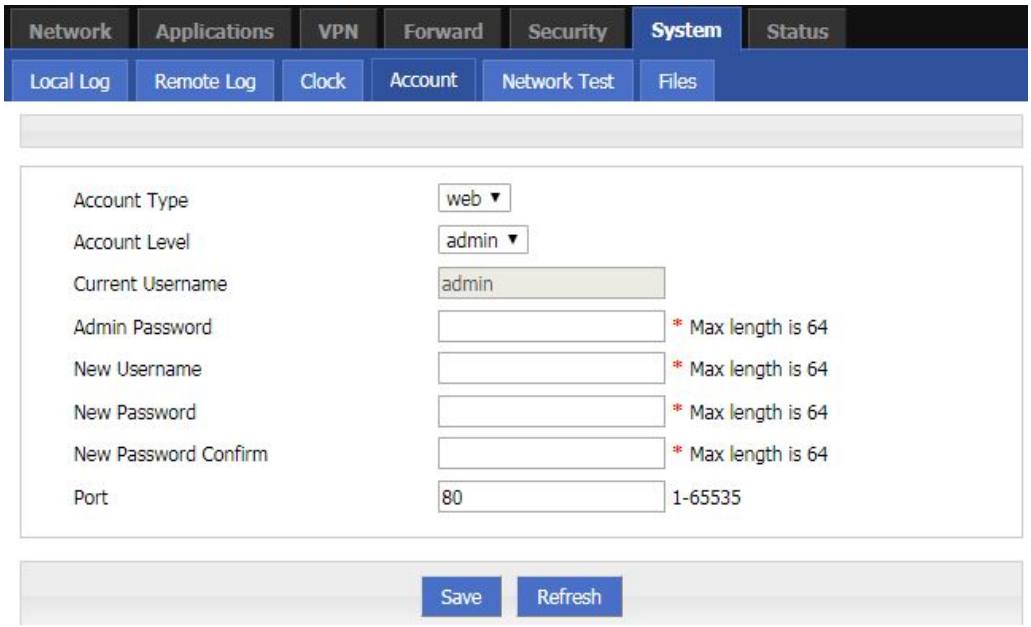
“Account” User provides the ability for users to modify the username/password. At the same time, user management can modify the access port of the router's WEB and block other users from accessing the route.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “System > Account” to open the page of “Account”.AS shown in figure 5-74.

Figure 1-29 The page of Account



Step 3 Configure parameters of account.

The parameter description is shown in Table 5-47.

Table 1-18 The instruction of Account parameter

Parameter	Details	Operation
Account Type	Visit the router on web	Select from Dropdown List
Account Level	Level of account to login router	Select from Dropdown List • Admin: can view and change the parameter. • Guest: can view parameter and export log and use “Network Test”.
Current Username	Current username	Cannot be configured,Displayed as the currently logged in user.
Admin password	Current password	Enter the login password of the currently logged in user.
New Username	New username	Manual input, max 64 word type.
New Password	New password	Manual input, max 64 word type.
New password confirm	To confirm the new password	Manual input, max 64 word type.
Port	The port on which the user logs in to the router page.	Manual input Value area 1~65535

Parameter	Details	Operation
		Default: 80

NOTE

“Account” only provides the user's modification function, and does not provide functions such as adding and deleting.

If the "port" parameter has not been modified, you can log in to the router page by directly entering the IP address of the router. If the port is modified to other numbers and the modification is successful, you need to enter the IP address of the router to log in to the router page.

The admin can only modify the password of the admin itself, but cannot modify the password and parameters of the guest; the guest itself has no function of “Account”.

Step 4 Click “Save” to finish configuration.After the save is successful, the page will automatically jump to the login page, and the user needs to enter the modified username/password to enter.

---END

1.5.5 Network Test

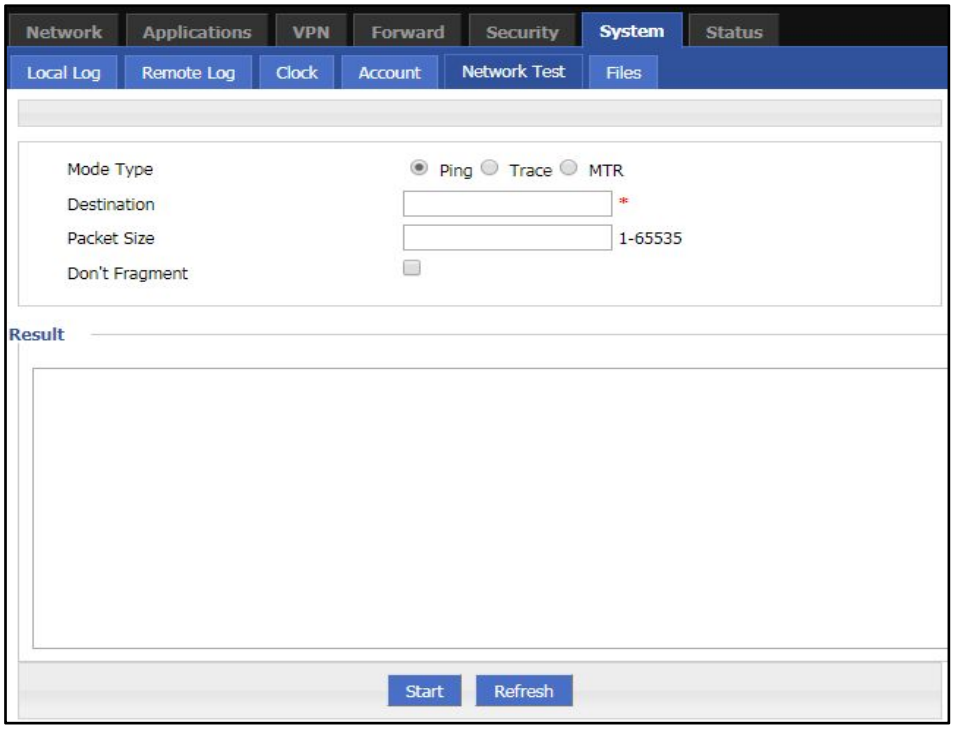
The network test includes the commonly used Ping function and Traceroute function. The specific steps are as follows:

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “System > Network Test” to open the page of “Network Test” . See below:

Figure 1-30 The configuration page of Network Test



Step 3 Input IP address or domain to be tested in “Destination”, click “Ping, to check whether the router can be linked with destination. See below:

Table 1-19 The instruction of parameters of Network Test

Parameter	Details	Operation
Mode Type	Choose a different type of network test.	single button: • Ping • Trace • MTR
Destination	Set the destination IP address or domain name to use for testing.	Fill in the destination IP address or domain name to be used for testing.
Packet Size	When the type of network detection is "Ping" and "MTR", the size of the packet can be set.	Enter it manually. Input range: 1~65535
Don't Fragment	When the network detection type is "Ping", you can set whether the ping packet carries the DF identifier. DF is the identification bit of the slice.	Single box. Unchecked by default
Reslove Names	When the network detection type is "MTR", you can set whether to perform name resolution.	Single box. Unchecked by default
start	Click “start” to start the selected network detection mode.	No

NOTE

Trace: Traceroute. Through Traceroute, we can know what path the computer from the computer to the other end of the Internet is. It takes a long time to send a small packet to the destination device until it returns. Each device Traceroute on one path is measured 3 times. The output includes the time (ms) of each test and the name of the device (if any) and its IP address.

---END

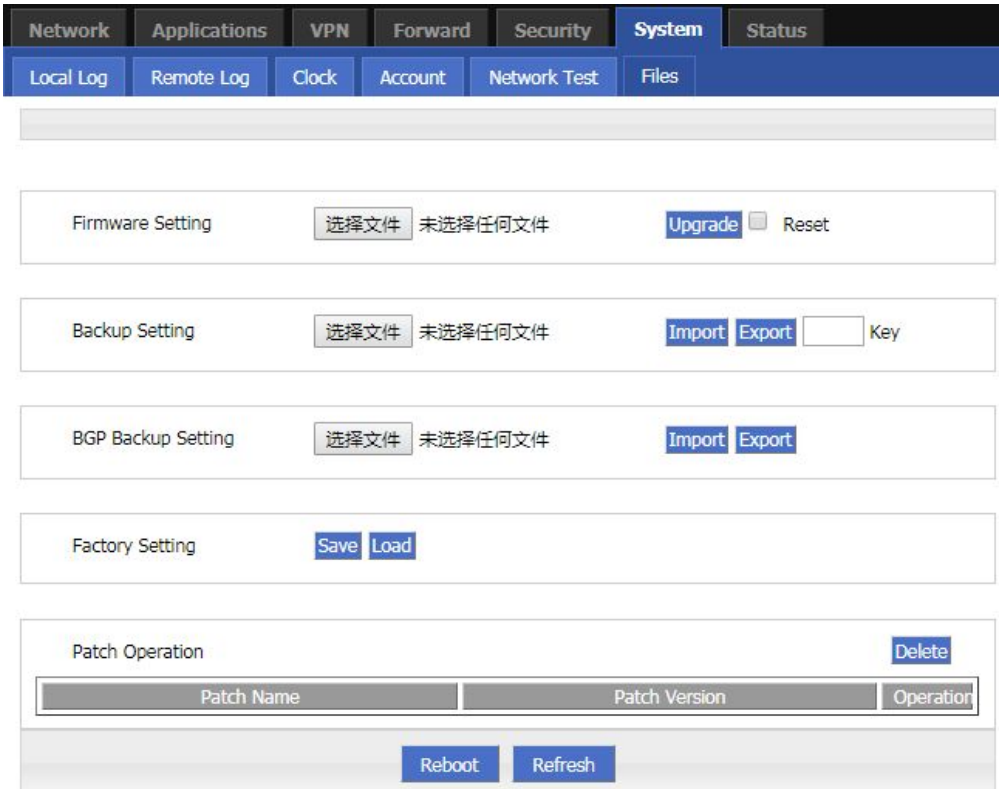
1.5.6 Files

Firmware Setting

The supports upgrading the system files on the local network. Before upgrading, please make sure that you have obtained the target file of the system update and have saved the update files on the computer on the LAN.

Step 1 Click “System > Files” to open the page of “Files”.As shown in figure 5-76.

Figure 1-31 The page of Files



Step 2 Click Browse, select the upgrade file locally, and click Upgrade to start the upgrade. If "Restore Default" is selected, the configuration of the router will be restored to the factory settings after the patch or program is upgraded; if it is not selected, only the patch or program will be upgraded, and the parameter configuration of the router will be maintained.

---END

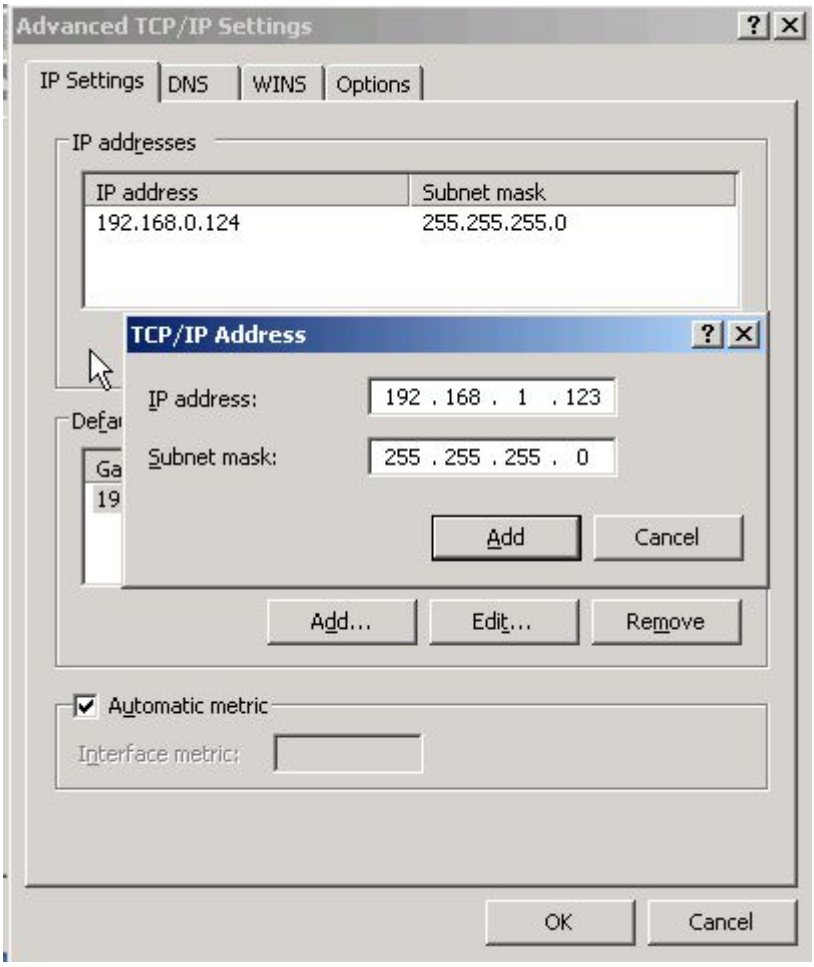
Upgrade in CFE mode

When the program is upgraded to the router (generally, the program upgrade is a comprehensive replacement upgrade), if the file size exceeds 6MB or the upgrade fails through the WEB configuration page, you can choose to upgrade in CFE mode. The specific upgrade operation mode is as follows.

Step 1 Add an IP address of the 192.168.1.X network segment on the PC. See below:

For details, see “4.2 Local Connection Configuration”.

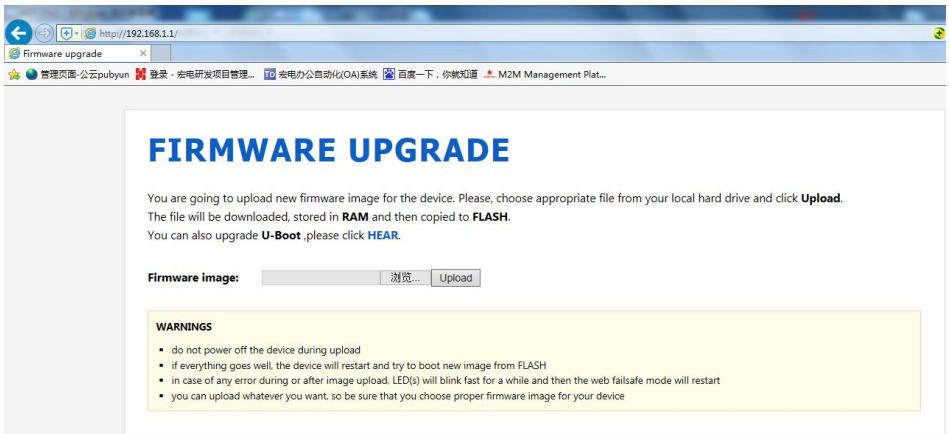
Figure 1-32 Add an IP address



Step 2 Press the RESET interface. Do not release it. Hold it, meanwhile power on router(After power-on, keep pressing the “RESET”button for 2 to 5 seconds or more and then release the “RESET”button

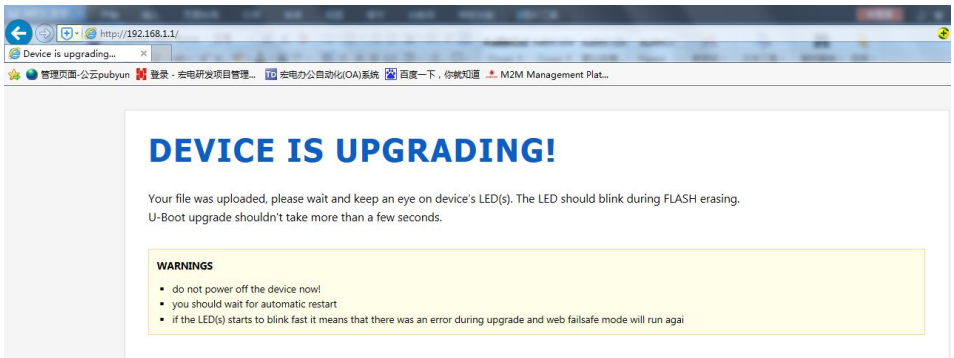
Step 3 Enter http://192.168.1.1 into the upgrade page in the browser of the PC, as shown below:

Figure 1-33 The page of upgrading in CFE mode



Step 4 Click “Browse” and select the upgrade file on the local PC, and then click Upload to start the upgrade. See below:

Figure 1-34 The Page being upgraded in CFE mode



The upgrade process will last for about 3 to 6 minutes. Please wait patiently and observe the SYS indicator of the device. If the SYS indicator is on, the program upgrade is successful.

TIP

You can also PING br0 address on your PC (ping 192.168.8.1 –t). if Ping ok, upgrading is OK.

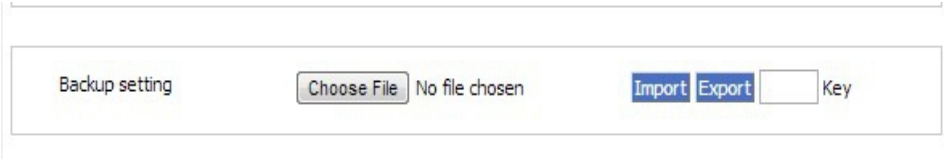
---END

Backup setting

The series routers support backup and recovery of configuration files. See below:

- Click “Browse”to view the configuration file that needs to be imported locally, and click “Import” to complete the import of the file. If the parameters of the router are incorrect or the file is lost, you can use the "Import" function to restore the parameters.
- Click “Export” to export the configuration file to the local file to implement file/parameter backup.

Figure 1-35 Backup setting page



NOTE

After the backup file is imported, the system automatically restarts a Key: adding a key when exporting a file, you need to enter the key when importing the file. Otherwise, the router will be garbled; the key can be left blank. If the key is entered incorrectly during import, the router page will not be accessible and the key must be 8 digits.

BGP backup settings

The routers of the series support backup and recovery of BGP configuration files, as shown in Figure 5-81.

- Click “Browse” to view the BGP configuration file that needs to be imported locally. Click “Import” to complete the import of the file. If the router parameters are incorrect or the file is lost, you can use the "Import" function to restore the parameters.
- Click Export to export the BGP configuration file to the local device to implement file/parameter backup.

Figure 1-36 The page of BGP Backup setting

Factory setting

4G Intelligent Gateway has function to resume factory configuration. Users can set the configuration to factory mode, and also can set the current configuration into default configuration and generate a default factory configuration file in router. To resume this default factory setting, users can click “Load” in “factory setting”. If the default factory configuration file is deleted, the router will be resumed back to initial factory setting.

- Set as default: Save the current configuration as the default factory configuration.
- Restore default: Restore the factory configuration.

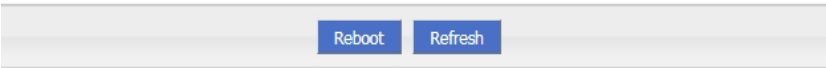
View patch information

Figure 1-37 Patch file status bar

- Delete: Delete all patch files.

Reboot

Click the "Restart" button to restart the system.



1.6 Status

Overview

4G Intelligent Gateway provides status display information. Through the status page, you can quickly view the basic information, network status, and routing table information of the router.

1.6.1 Base Information

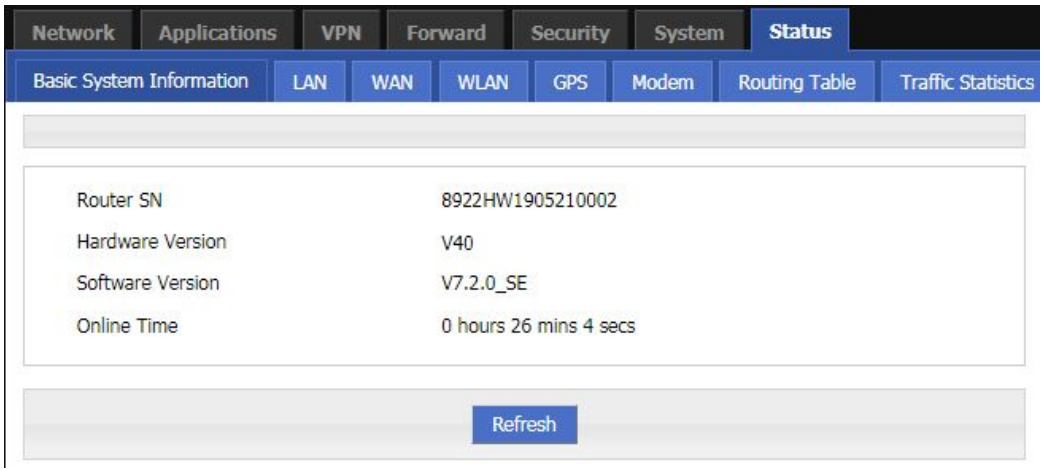
You can learn the basic information of the 4G Intelligent Gateway system by viewing the basic information of the 4G Intelligent Gateway. The specific operation method is as follows.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status > Base System information” to open the page of “Base Information”.

Figure 1-38 The page of Base system Information



NOTE

Click “Refresh” to re-detect the latest parameters of the system and display it to the current page.

Table 1-20 The instruction of parameter of Base information

Parameter	Details	Operation
Router SN	Serial number information of the device	Not available
Hardware Version	Hardware version information of the device	Not available
Software Version	Operating system and application software version information corresponding to the product	Not available
Online Time	Online time information of device	Not available

1.6.2 LAN

By viewing the "LAN Status" information of the 4G Intelligent Gateway, you can learn the basic information of the "LAN Status" of the 4G Intelligent Gateway. The specific operation method is as follows.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status > LAN” to open the page of “LAN”.As shown in figure 5-84.

Figure 1-39 The page of “LAN”

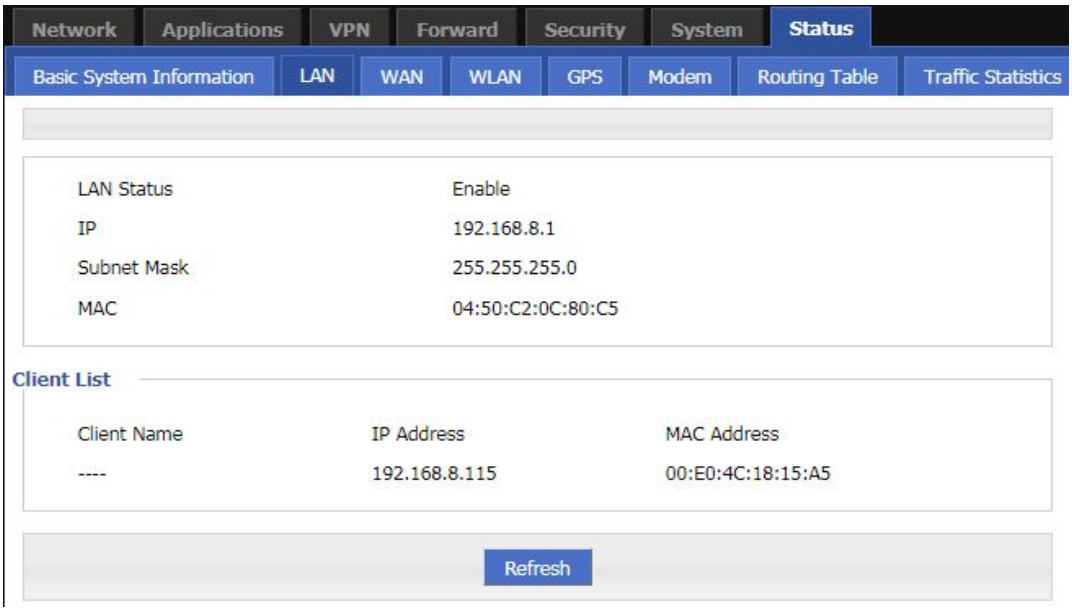


Table 1-21 The instruction of LAN

Parameter	Details	Operation
LAN status	Displays whether the status of the current LAN interface function is enabled or disabled.	Not available
IP	Displays the IP address configured for the LAN port.	Not available
Subnet Mask	Displays the network address where the configured LAN interface is located.	Not available
MAC	Displays the physical address of the LAN network port. This address is generally fixed and unique.	Not available
Client List	List of client information connected to the device through the LAN port	Not available

---END

1.6.3 WAN

By viewing the "WAN Status" information of the 4G Intelligent Gateway, you can learn the basic information of the "LAN Status" of the 4G Intelligent Gateway. The specific operation method is as follows.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details, please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status > WAN” to open the page of “WAN”. Because the WAN port has three forms of static IP/DHCP/PPPOE, when the WAN port is in any of these three forms, the WAN status displays the WAN information in this form. See below:

Figure 1-40 WAN status in static IP form

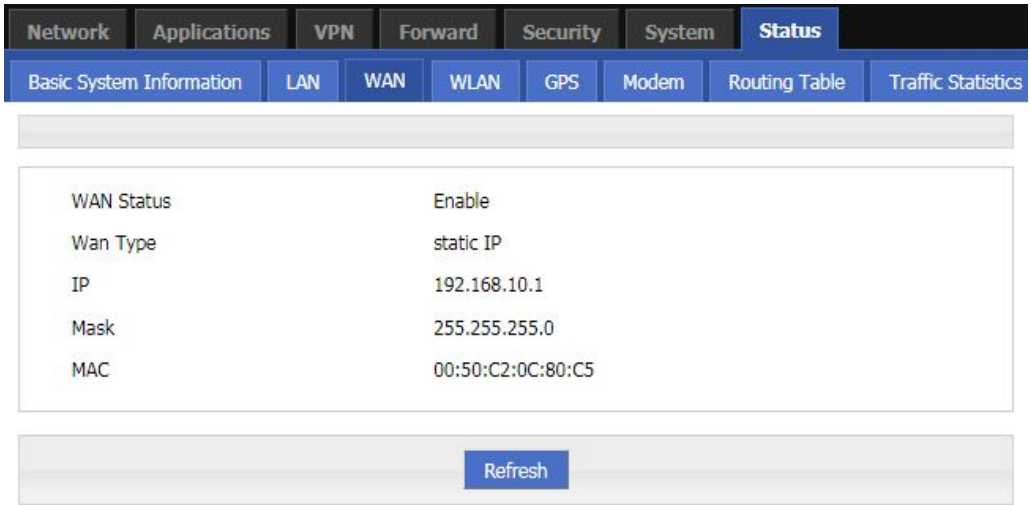


Figure 1-41 WAN status in DHCP form

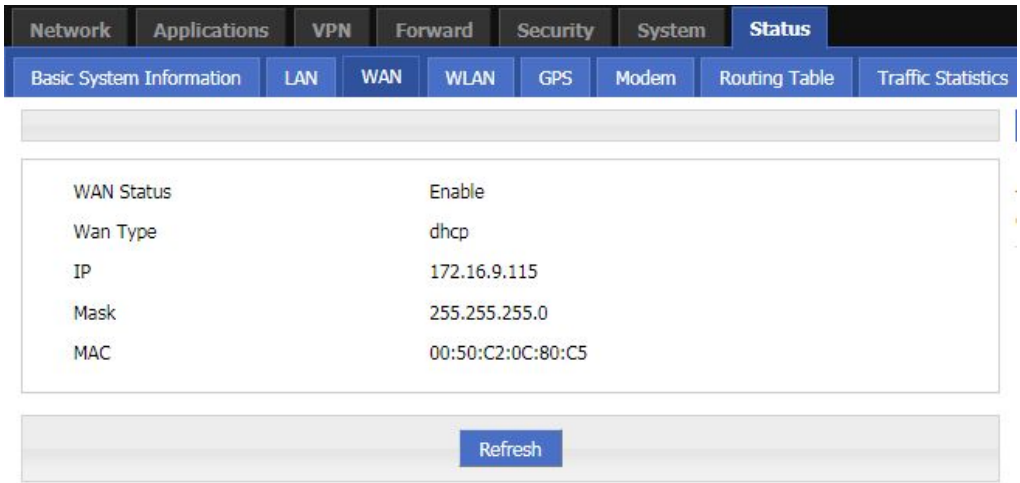


Figure 1-42 WAN status in PPPoE form

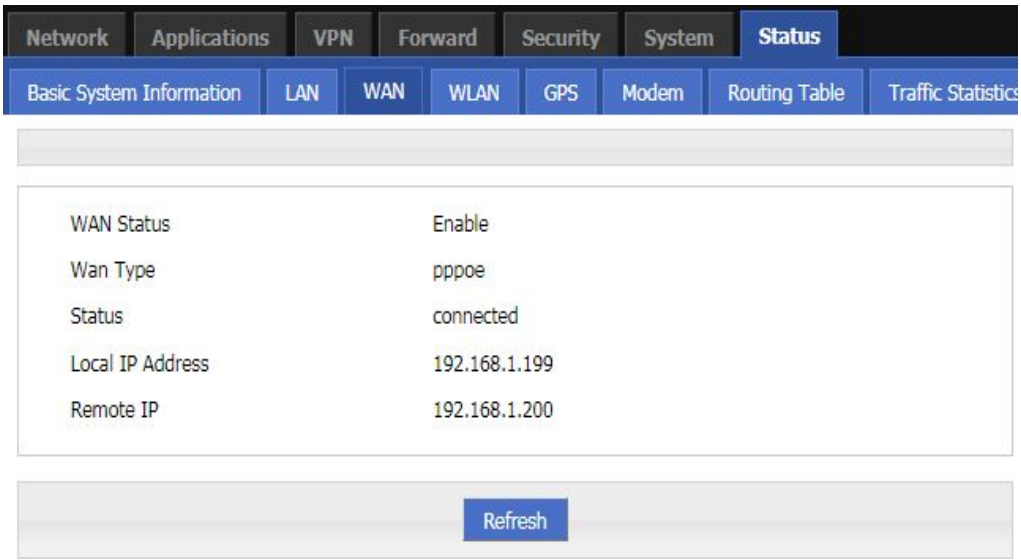


Table 1-22 The instruction of parameters of WAN status

Parameter	Details	Operation
WAN Status	Shows whether the status of the current WAN interface function is enabled or disabled.	Not available
Wan Type	Displays the type of the current WAN interface.	Not available
Status	Displays the configured local IP address of the WAN port.	Not available
Local IP Address	Displays the network address where the configured WAN interface is located.	Not available
Remote IP	Displays the physical address of the LAN NIC, which is generally fixed and unique.	Not available
Status display when the WAN port adopts PPPoE mode		
Status	To show the link status of WAN interface in PPPoE mode	Not available
Local IP	To show the router IP distributed by PPPoE	Not available
Remote IP	To show IP of PPPoE server	Not available

---END

1.6.4 Modem

By querying the status of the “modem”, you can learn about the "mobile network status" and "mobile network device information". Therefore, it is determined whether the network and the device are normal according to the relevant state. It is also conducive to analysis and problem solving of abnormal situations.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status > Modem” to open the page of “Modem”. As shown in figure 5-88. The parameter description is shown in Table 5-52.

Figure 1-43 The page of Modem Status

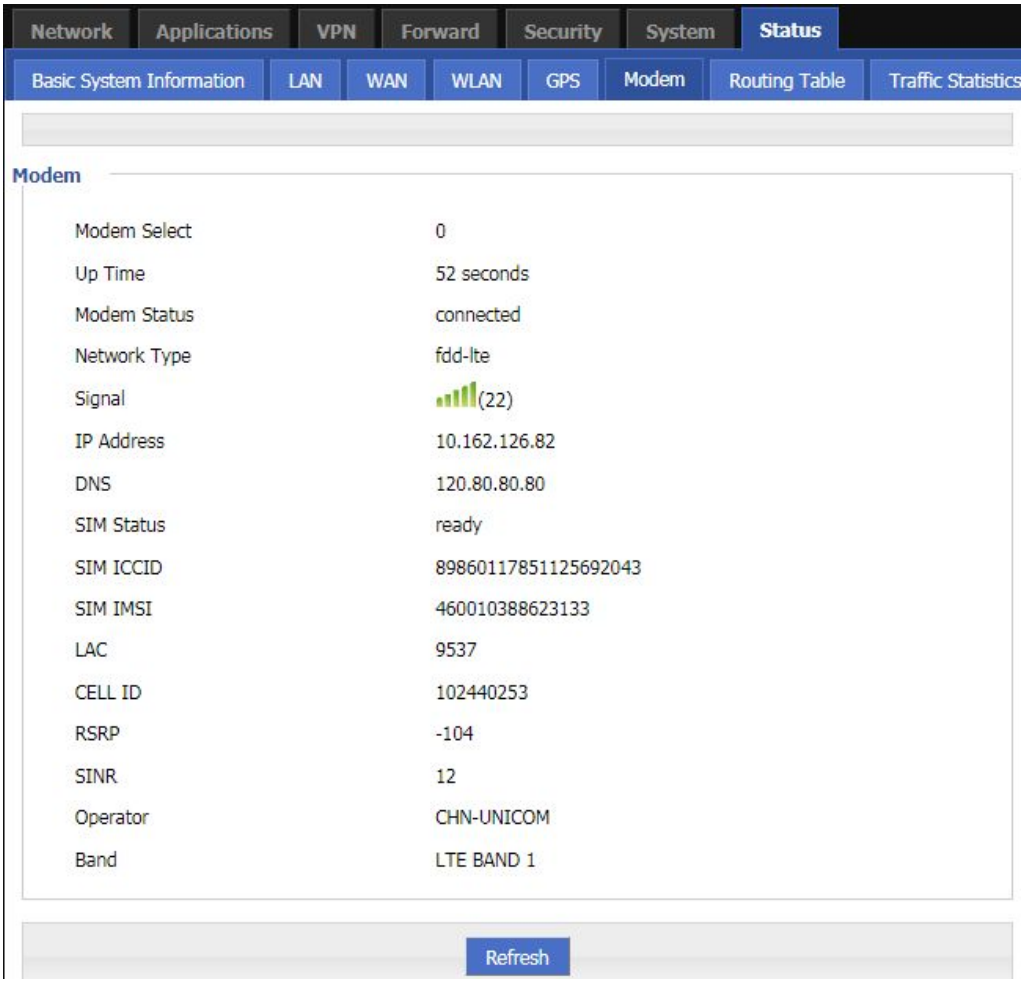


Table 1-23 The instruction of parameter of Modem

Parameter	Details	Operation
Modem Select	The name of the Modem rule that is currently dialed by the mobile network.	Not available
Up Time	The online duration of the 4G Intelligent Gateway after dialing the line is displayed.	Not available
Modem Status	H8922S4G Intelligent Gateway connection status with the wireless network. Contains both connected and disconnected states.	Not available
Network Type	The type of network corresponding to the SIM card currently in effect.	Not available
Signal	The signal strength of the wireless network. Value range: 1 to 31 If there is no signal, the dialing cannot be successful.	Not available

Parameter	Details	Operation
IP Address	4G Intelligent Gateway obtained the external network IP address when dialing.	Not available
DNS	4G Intelligent Gateway obtains the preferred DNS address when dialing.	Not available
SIM Status	The working status of the SIM corresponding to the card slot currently used by the 4G Intelligent Gateway.	Not available
SIM ICCID	The ICCID number of the SIM card.	Not available
SIM IMSI	The IMSI number of the SIM card.	Not available
LAC	The location area code used by Modem dialing.	Not available
CELL ID	The cell ID used by Modem dialing.	Not available
RSRP	The received power of the reference signal dialed by Modem. Only displayed when 4G/5G dialing.	Not available
SINR	The ratio of the signal dialed by Modem to the interference plus noise. Only displayed when 4G/5G dialing.	Not available
Operator	Modem dial-up carrier.	Not available
Band	The frequency band used by Modem dialing.	Not available

---END

1.6.5 WLAN

You can learn the basic information about the WLAN of the router by viewing the WLAN Status information of the 4G Intelligent Gateway. The specific operation method is as follows.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status > WLAN”. The 4G Intelligent Gateways have WLAN and station modes. See below:

Figure 1-44 Status page in ap mode

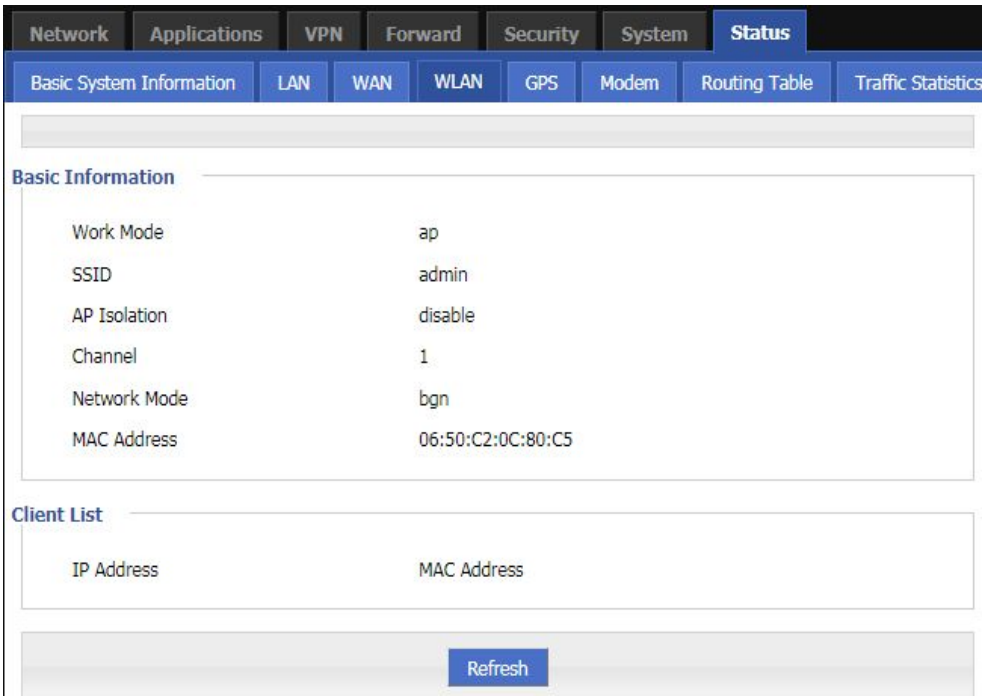


Figure 1-45 Status page in station mode

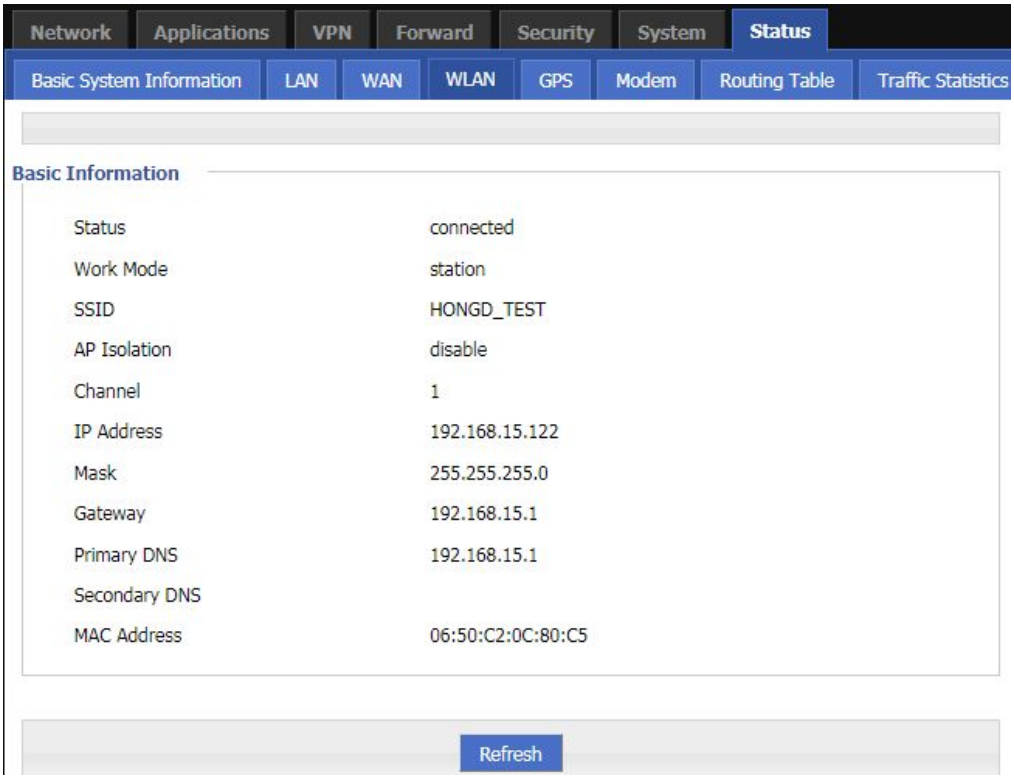


Table 1-24 The instruction of Parameter in ap mode

Parameter	Details	Operation
Basic information		
Work Mode	The working mode of the WLAN.	Not available
SSID	Representation of ap.	Not available
AP Isolation	The isolation status of the WLAN client device.	Not available
Channel	The working channel of ap.	Not available
Network Mode	The network mode currently used by ap.	Not available
MAC Address	The MAC address of the device.	Not available
Client information		
IP address	IP address of the WLAN client.	Not available
MAC address	MAC address of the WLAN client.	Not available

Table 1-25 The instruction of Parameter in station mode

Parameter	Details	Operation
Basic information		
Status	The state of the other APs connected to the WLAN when it is stationed.	Not available
Work Mode	Station mode	Not available
SSID	AP ID of the router connection	Not available
Channel	Working channel of the AP connected to the router	Not available
IP Address	IP address assigned to the router by the connected AP of the router	Not available
Mask	Subnet mask assigned to the router by the connected AP of the router	Not available
Gateway	The default gateway assigned to the router by the connected AP of the router	Not available
Primary DNS	The preferred DNS address assigned to the router by the connected AP of the router	Not available
Secondary DNS	The backup DNS address assigned to the router by the connected AP of the router	Not available
MAC Address	MAC address of the connected AP of the router	Not available

---END

1.6.6 Routing Table

By querying the status of the routing table, you can learn the routing information of the 4G Intelligent Gateway.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status > Routing Table” to open the page of “Routing Table”. See below:The page of Routing table

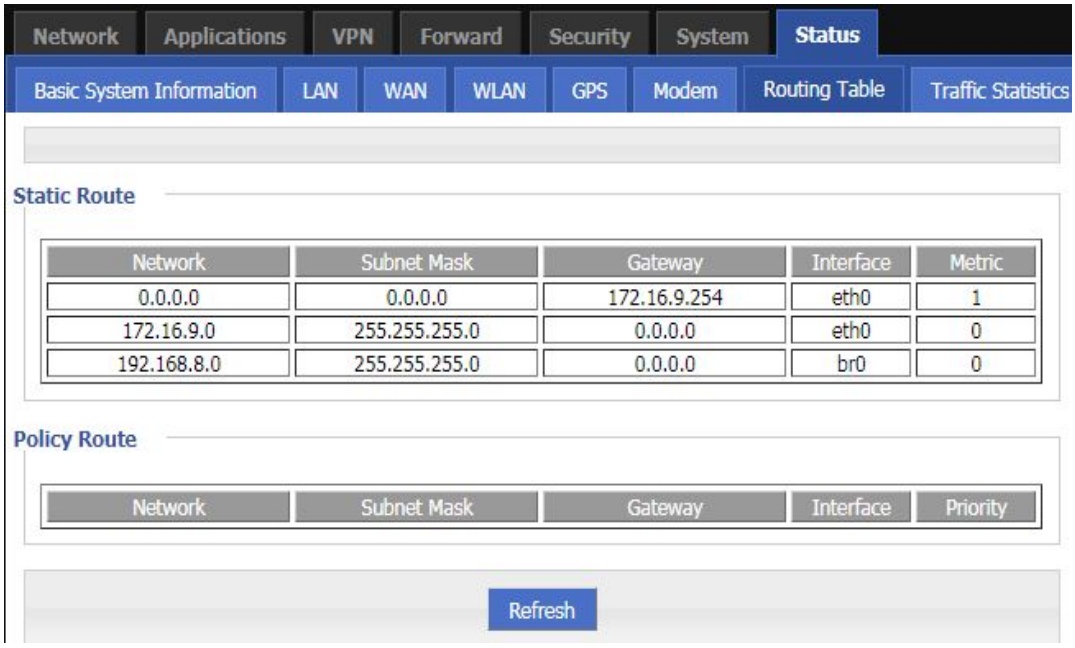


Table 1-26 The instruction of Routing table Parameter

Parameter	Details	Operation
Static route		
Network	IP address the router can reach	Not available
Subnet Mask	IP network the router can reach. It is used together with “Network”	Not available
Gateway	Next hop IP address which the router will reach	Not available
interface	Interface from router to gateway	Not available
metric	Route No which the router reaches destination IP	Not available
Policy route		
Priority	Priority the router select route	Not available

---END

1.6.7 GPS

By querying the status of the routing table, you can learn the GPS information of the 4G Intelligent Gateway.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status>GPS”. See below:

Figure 1-46 The page of GPS

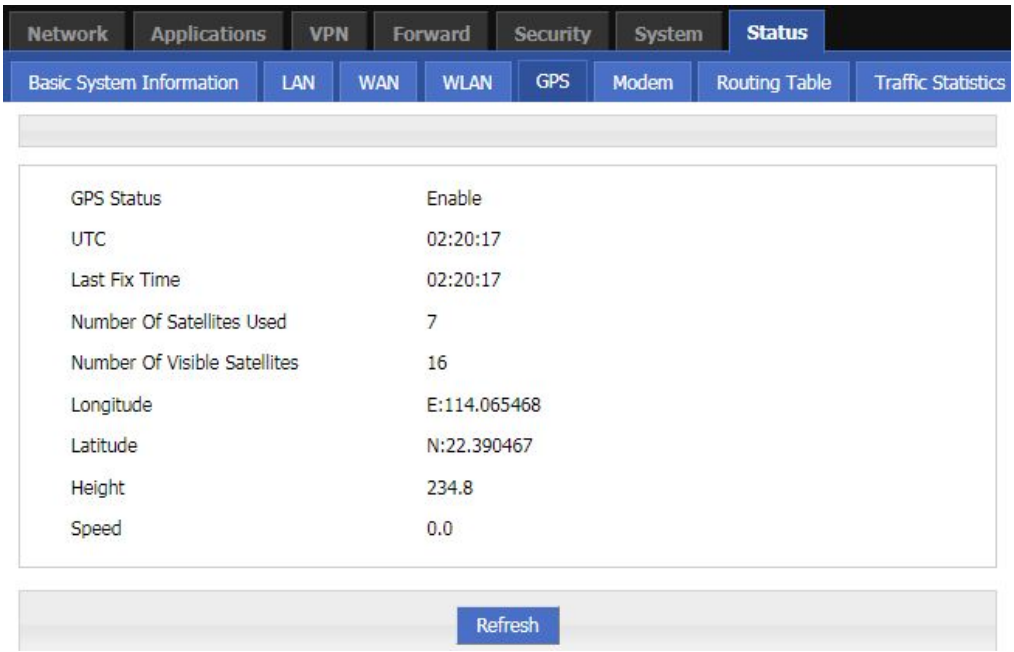


Table 1-27 The instruction of GPS Parameter

Parameter	Details	Operation
GPS Status	Display of the on state of the GPS.	Not available
UTC	Display of world standard time.	Not available
Last Fix Time	The display of the last specified time.	Not available
Number Of Satellites Used	The display of the number of satellites used by GPS.	Not available
Number Of Visible Satellites	Display of the number of satellites available for GPS.	Not available
Longitude	Display of device longitude information.	Not available
Latitude	Display of device dimension information.	Not available
Height	The height of the device from sea level. Unit M.	Not available
Speed	Parallel speed of the device.	Not available

--END

1.6.8 Traffic Statistics

By querying the status of the routing table, you can learn the traffic statistics of the 4G Intelligent Gateways.

Step 1 Log in to the WEB configuration page of the 4G Intelligent Gateway.

For details ,please see “5.2.1 Logging In to the WEB Configuration Page”.

Step 2 Click “Status>Traffic Statistic”. See below:

Figure 1-47 The page of modem Traffic Statistic

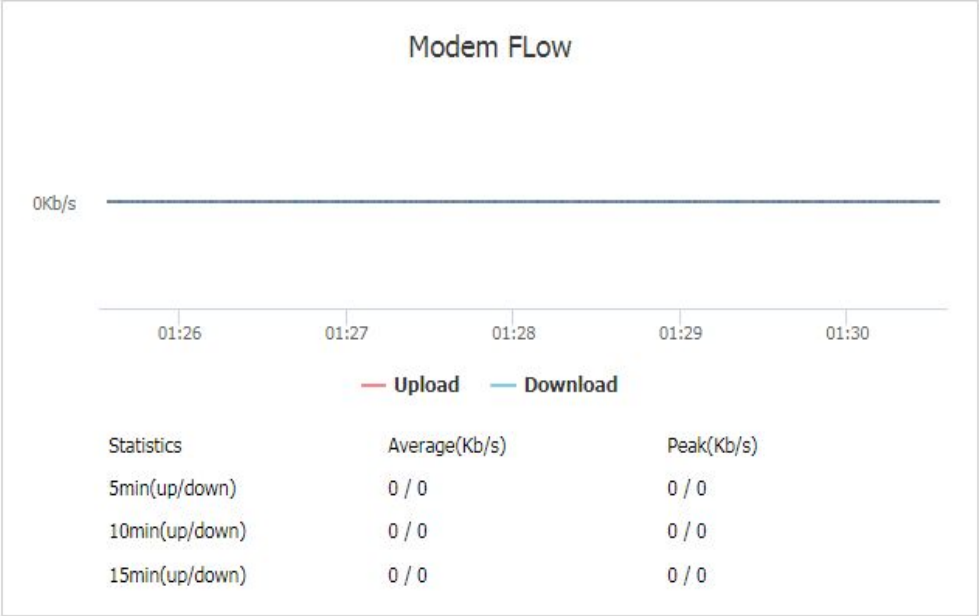


Figure 1-48 The page of WAN Traffic Statistic

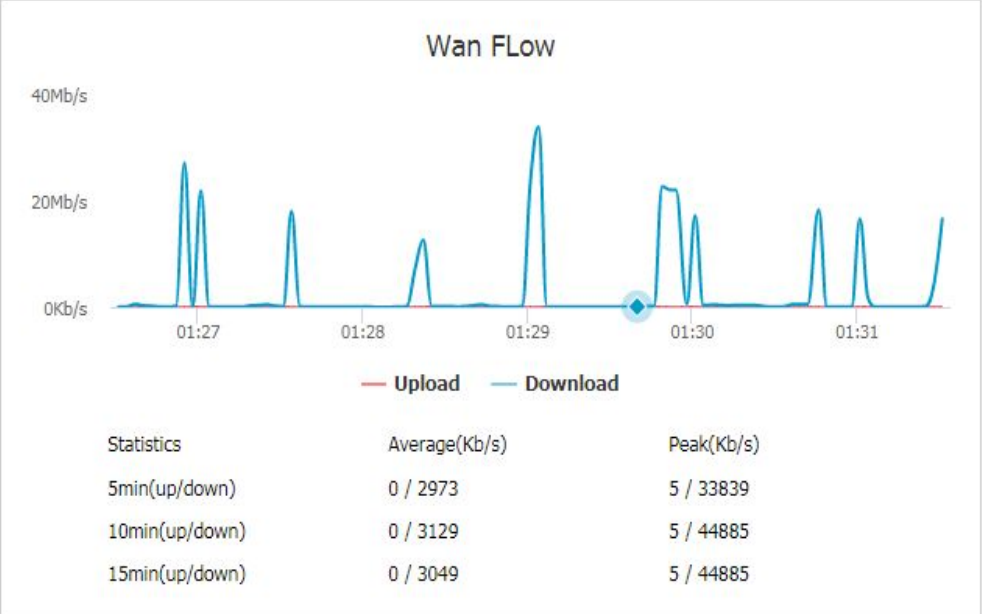


Figure 1-49 The page of LAN Traffic Statistic

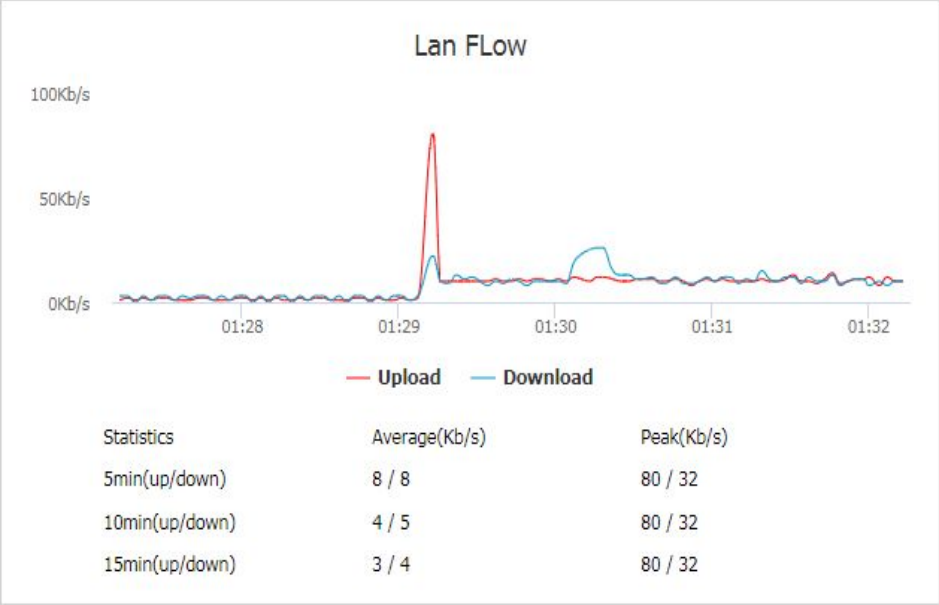


Table 1-28 The instruction of Traffic Statistic

Parameter	Details	Operation
Flow chart	The traffic usage information of the interface is displayed in real time through the picture. The speed of uploading and downloading can be seen through the picture, the red line indicates uploading, and the blue line indicates download。	Not available
Statistics	It can display the average speed of uploading and downloading within 5min, 10min, and 15min, and the peak speed.	Not available
Average(Kb/s)	Display of average speed information.	Not available
Peak(Kb/s)	Display of peak speed information.	Not available

--END

1.7 RESET button function

"RESET" button is on the rear panel and next to power interface. This button can be used when the router is in use or when the router is turned on. Three are 3 functions to press "RESET" button when the router is in use:

- Press "RESET" for about 0~5 seconds, router will reboot.
- Press "RESET" 5-15 seconds, the router will reboot, meanwhile, the router will be resumed to default factory setting configuration.
- Press "RESET" over 15 seconds, the router will reboot, and get into CFE upgrading. The router is resumed to default factory setting configuration.
- Press button when the router is turned on:
- Press "RESET" button and turn on the router, and keep pressing "RESET" for 2 seconds. The router will get into CFE upgrading mode.

---END

2 Typical application

About this chapter

Chapter	Brief introduction of content
6.1 Overview	This section briefly introduces several typical application functions of the 4G Intelligent Gateway.
6.2 Link backup function	This section briefly introduces a typical application example of the Router trigger setting function.
6.3 Parameter select function	This section briefly introduces a typical application example of the 4G Intelligent Gateway parameter select function.
2.4 VPN	This section briefly introduces the 4G Intelligent Gateway VPN application examples.
6.4 Schedule	This section briefly introduces the practical application examples of the 4G Intelligent Gateway task management functions.

2.1 Overview

The 4G Intelligent Gateways are widely used. The commonly used functions include on-demand dialing, parameter link backup, and VPN. The following are some typical application scenarios provided by the 4G Intelligent Gateway systems.

2.2 Link backup function

Scene introduction

4G Intelligent Gateway supports link switching between wireless and wireless, wireless and wired. When the working link of the router fails, it can quickly switch to other links and continue to work on the switched link.

For example, the shopping mall POS card needs a stable network to ensure that if the wired network used by the POS fails, the 4G Intelligent Gateway can quickly switch to the wireless network to ensure the normal operation of the POS card card service.

Parameter configuration

In this scenario, you need to perform the configuration of Link Backup. For details, see "Link Backup."

Figure 2-1 Main link (wan) configuration

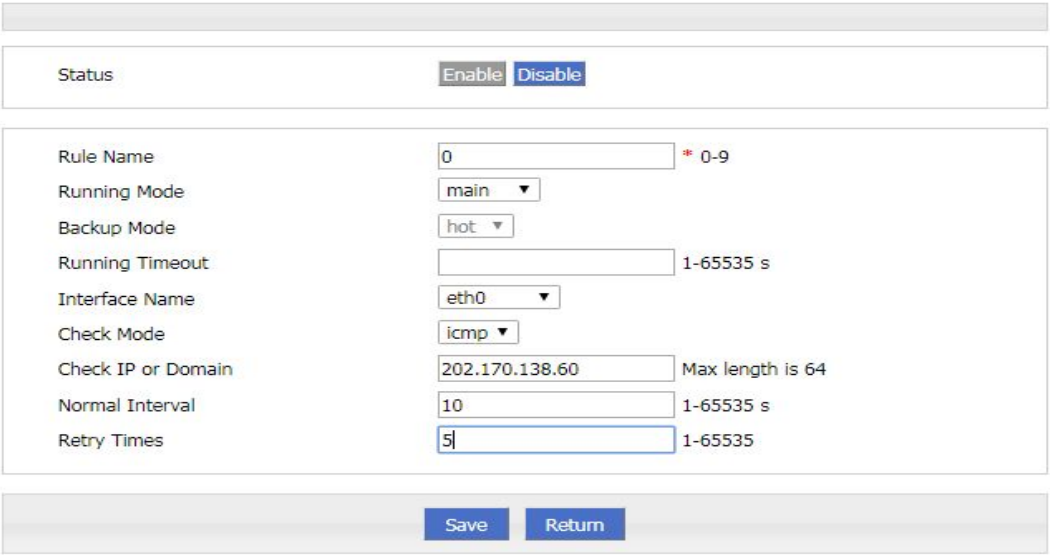
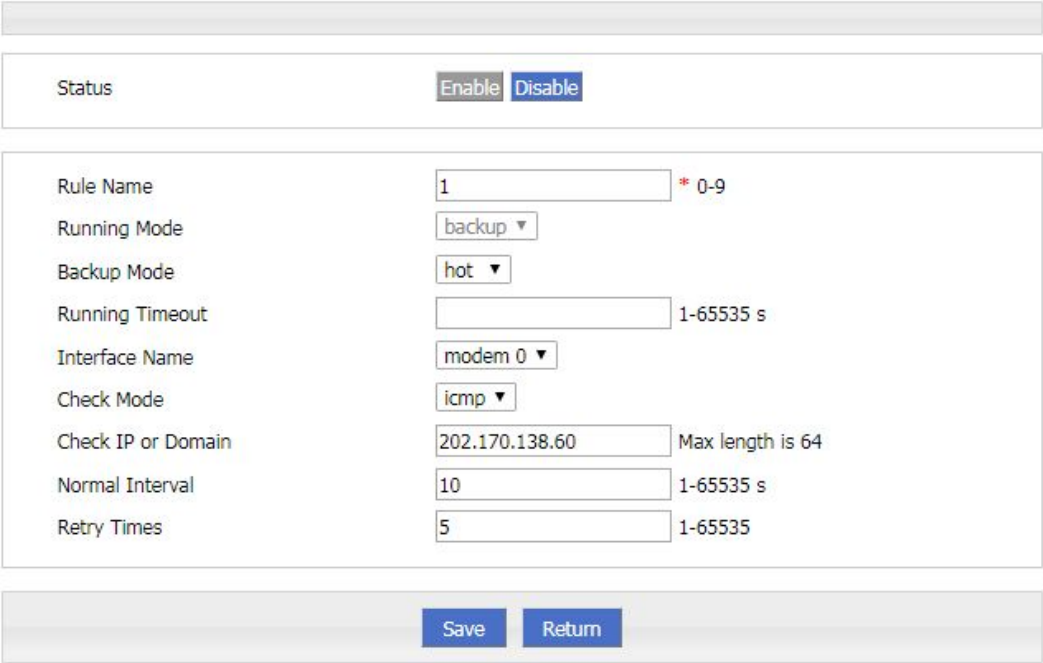


Figure 2-2 Backup link (modem) configuration



Application result

After all the parameters are configured, the default route of the router goes to the eth0 (WAN) interface of the primary link. If the router can ping the IP address of 202.170.138.60, the router will always work on the primary link. As shown in Figure 6-3, the backup link modem is always online. If the wired network (WAN port) fails to ping 202.170.138.60 due to a fault, the router will switch the link to the modem after multiple failures, so that the services of the lower computer can be performed normally, as shown in below.

Figure 2-3 The primary link is detected normally and works on the primary link

```
##### rule[0], main link[vpdnpppoe], icmp check begin #####{linkbackup.c->739}
**** ICMP send icmp packet successful ****{icmp.c->219}
>>>> ICMP recv one packet success!>>>>{icmp.c->304}
##### rule[0], main link[vpdnpppoe], icmp check end #####{linkbackup.c->741}
now checking rule[0], check main link[vpdnpppoe] ret[0](0:success, <0:failed){linkbackup.c->744}
```

Static Route

Network	Subnet Mask	Gateway	Interface	Metric
192.168.8.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	vpdnpppoe	0

Figure 2-4 The primary link fails to be detected and is switched to the backup link.

```
**** ICMP send icmp packet successful ****{icmp.c->219}
recv_icmp_pack:select time out{icmp.c->98}
**** ICMP Recv icmp packet timeout ****{icmp.c->299}
**** ICMP send icmp packet successful ****{icmp.c->219}
recv_icmp_pack:select time out{icmp.c->98}
**** ICMP Recv icmp packet timeout ****{icmp.c->299}
##### rule[0], main link[vpdnpppoe], icmp check end #####{linkbackup.c->741}
now checking rule[0], check main link[vpdnpppoe] ret[-2](0:success, <0:failed){linkbackup.c->744}
switch from [rule:0] main [link:vpdnpppoe] to [rule:1] backup [link:modem]{linkbackup.c->475}
```

Static Route

Network	Subnet Mask	Gateway	Interface	Metric
192.168.8.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	modem	0

2.3 Parameter select function

Scene introduction

4G Intelligent Gateway provides parameter switching function to switch between working or temporarily stopped links. For example, when the working L2TP link fails to work properly for some reason, it can switch to the standby PPTP or IPSec link. The 4G Intelligent Gateways switch multiple links according to the configured parameter switching rules to ensure the reliability of network communication.

Configuration

In this scenario, you need to perform parameter select. For the configuration procedure, see Parameter select.

Figure 2-5 Interface configuration

VPDN | Tunnel | IPSec | OpenVPN | DMVPN | EoIP

Tunnel Secrets [ ] Max length is 64 Save

Interface Name	Protocol	Server IP or Domain	Username	Operation				
2	pptp	192.168.8.6	1234	Mod	Del	View	En	Dis
1	l2tp	192.168.8.6	1234	Mod	Del	View	En	Dis

Add Refresh

Figure 2-6 The configuration of parameter select 1

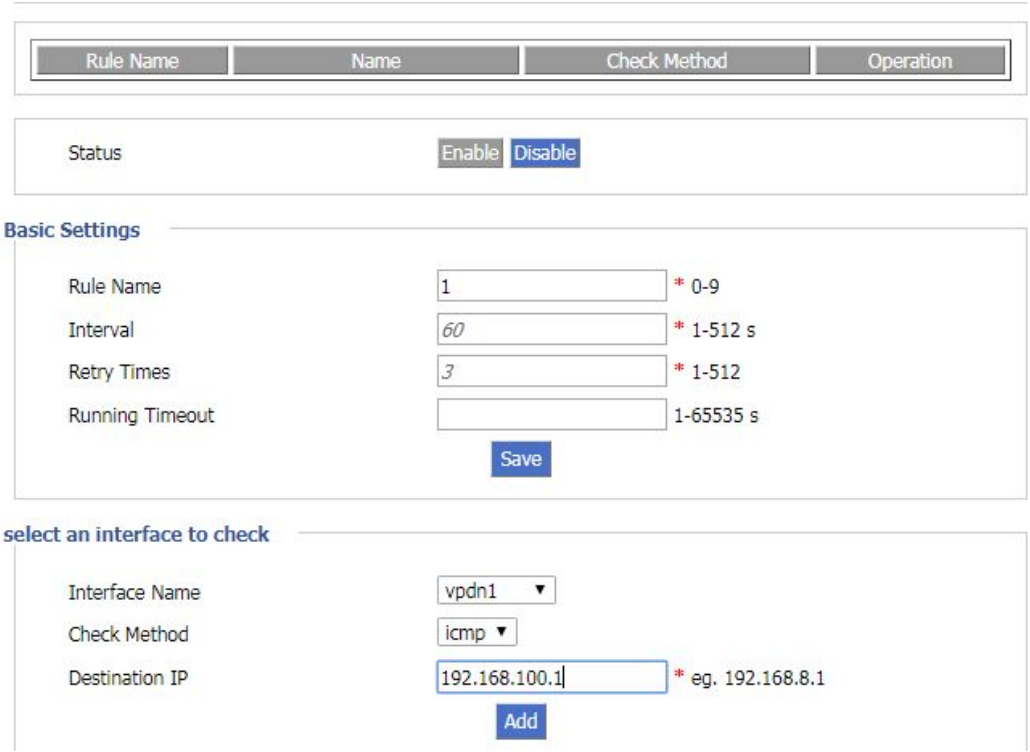
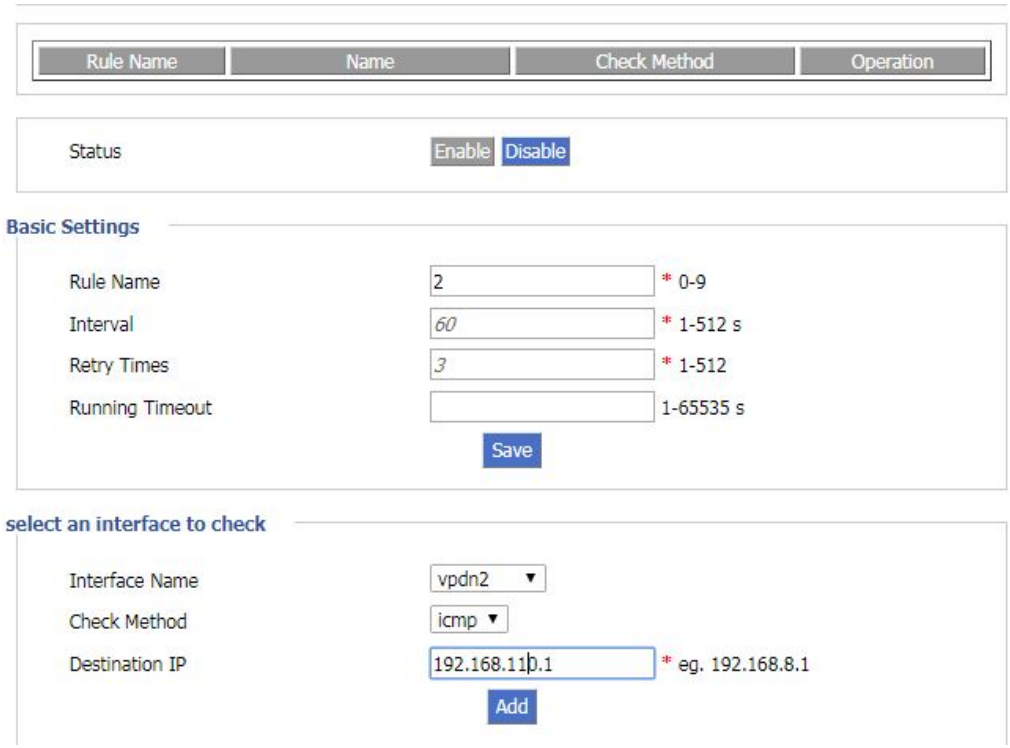


Figure 2-7 The configuration of parameter select 2

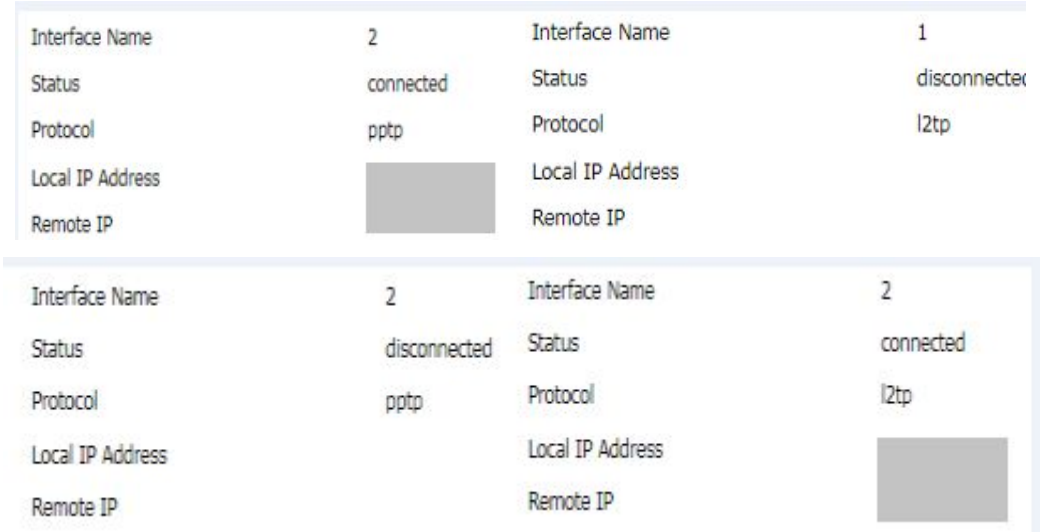


When the working L2TP link is disconnected from the server for some reason, the router performs the parameter "check icmp" in the parameter switch, and pings the configured destination IP to detect whether the router is disconnected from the network operator. After failing to ping the destination IP address three times, the router will switch to the PPTP link, maintain the connection with the server, and continue to work.

Application result

Initially, the PPTP link is used, and then the L2TP connection is disconnected. After the ping 192.168.100.1 fails, the router switches to the L2TP link and maintains the connection with the server, as shown in Figure 6-8.

Figure 2-8 The result of parameter select



2.4 VPN

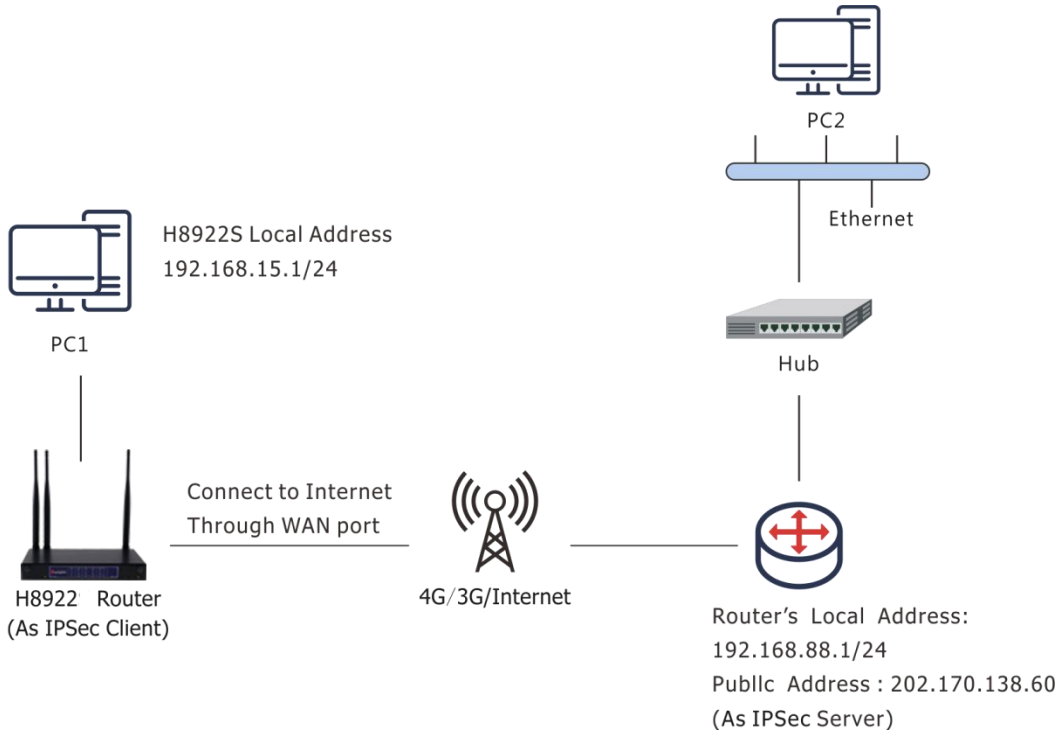
Scene introduction

VPN is a virtual private network, which is a secure local area network based on the Internet. Currently, the 4G Intelligent Gateway supports L2TP/PPTP/GRE/IPIP/IPSec/OpenVPN six protocol VPNs.

L2TP is an abbreviation of Layer 2 channel protocol. It is a kind of VPDN (Virtual Private Dial-Up Networking) technology, which is used for channel transmission of Layer 2 data. L2TP provides a means of remote access control. The typical application scenario is that a company employee dials into the company's local network access server (NAS) through L2TP to access the company's internal network, obtain an IP address, and access it. Network resources for the corresponding permissions. The employee's access to the company's network is as safe and convenient as a corporate LAN.

Here, IPSec is used to establish a communication link between employees and the company to ensure that employees work as if they are accessing the corporate LAN, as shown in Figure 6-9.

Figure 2-9 Establishing IPSec communication



PC1 establishes an IPSec link with the company's router through the VPN function of and uses tunnel mode communication. The LAN address on the side is 192.168.86.1/24, and the LAN address on the router side of the company is 192.168.99.1/24. Through the established IPSec connection, the two LANs can communicate securely.

Parameter configuration

In this scenario, you need to configure the VPN function. For the configuration procedure, see 5.6.4 IPSec Settings. Figure 6-10, Figure 6-111, and Figure 6-12 show the configuration.

Figure 2-10 IPSec Phase 1

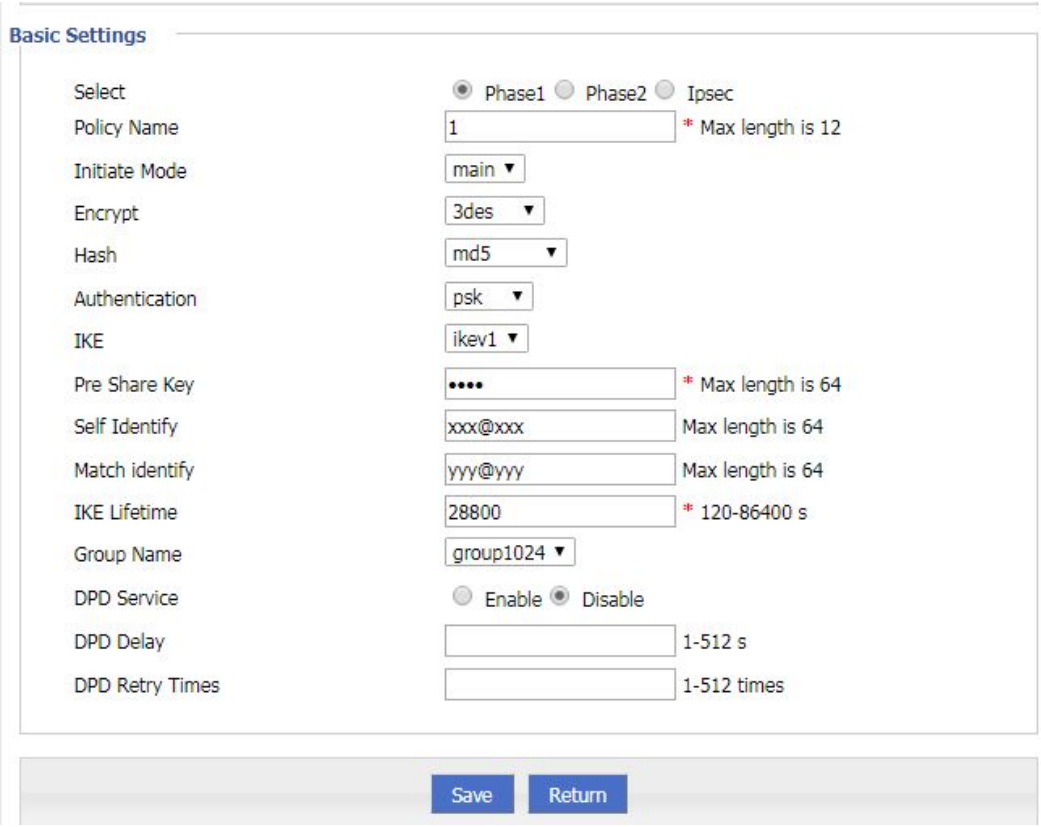


Figure 2-11 IPSec Phase 2

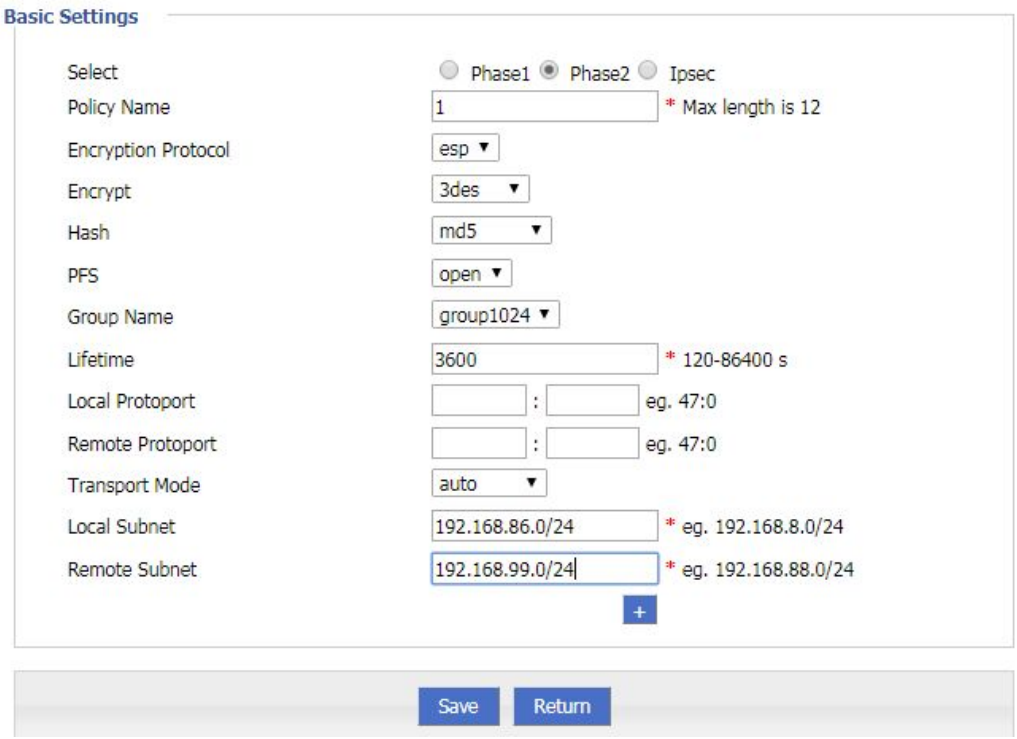
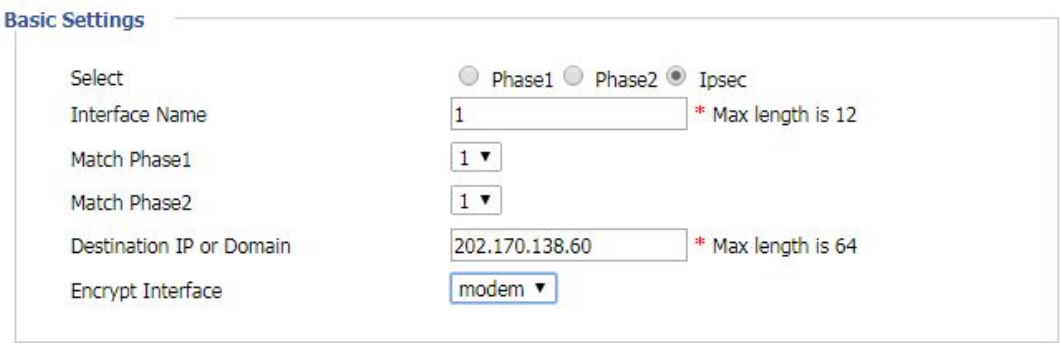


Figure 2-12 IPSec

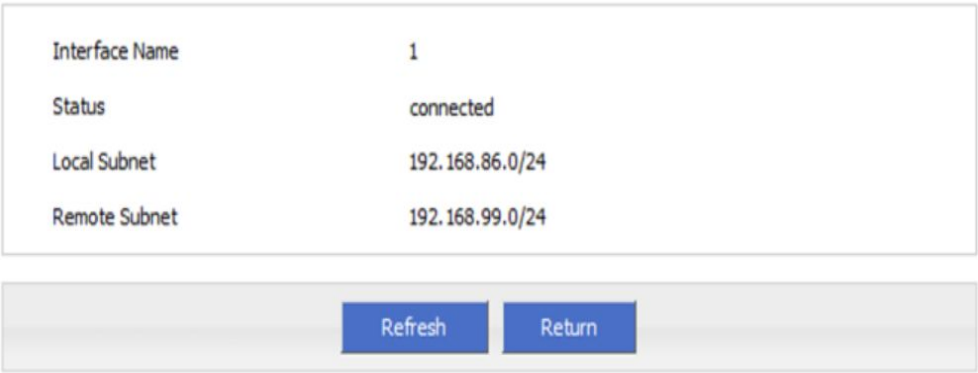


The same configuration should be used on the router of the company. The difference is that the configuration of the local end identifier, the peer end identifier, the local subnet, and the terminal network are opposite to those of the 4G Intelligent Gateway.

Application result

AAfter configuring the parameters of the 4G Intelligent Gateway, and the company router, the two negotiate and establish an IPSec connection, as shown in Figure 6-13. At this point, the LANs in the two places can access the remote LAN as if they were accessing the local area network. At the same time, you can ping the company subnet through this terminal network.

Figure 2-13 IPSec status



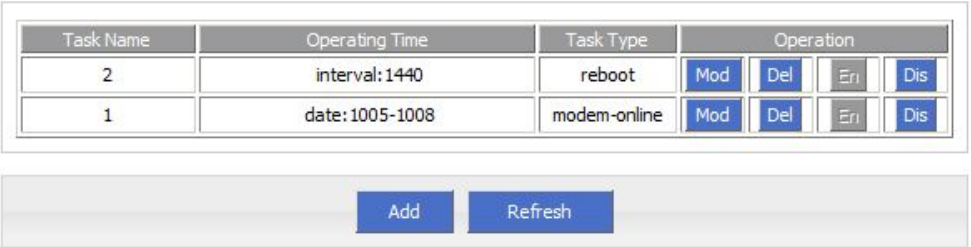

```
~ # ping 192.168.99.1 -I 192.168.86.1
PING 192.168.99.1 (192.168.99.1) from 192.168.86.1: 56 data bytes
64 bytes from 192.168.99.1: seq=0 ttl=255 time=1569.360 ms
64 bytes from 192.168.99.1: seq=1 ttl=255 time=769.937 ms

--- 192.168.99.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 769.937/1169.648/1569.360 ms
```

2.5 Schedule

Scene introduction

4G Intelligent Gateway support timing task, by setting timing task, at certain time, router will operate reboot, online command. Etc. Easier the customer operation. I assume set the router online at certain time and keep a moment, then reboot every 24 hours. You could set like below.

Figure 2-14 schedule



Task Name	Operating Time	Task Type	Operation			
2	interval:1440	reboot	Mod	Del	En	Dis
1	date:1005-1008	modem-online	Mod	Del	En	Dis

Add Refresh

Application result

Router will be online at 10:05 AM and keep online until 10:08, then offline at 10:09.

And router will reboot every 24 hours count began last reboot.

Figure 2-15 Router online

```
10:04:57 time[912]: ntpclient -h clock.via.net -s return 1{time.c->109}
10:04:57 time[912]: open the file(/tmp/ntp_first.mark) success!{time.c->254}
10:04:57 time[912]: NTP failed!{time.c->274}
10:04:59 pppd[345]: sent [LCP EchoReq id=0xf magic=0x5511fa91]
10:05:00 pppd[345]: rcvd [LCP EchoRep id=0xf magic=0xc1caf26e]
10:05:05 modem[969]: got SIG_TERM signal{modem.c->605}
10:05:05 modem[969]: argument error{hp_chat.c->533}
10:05:05 modem[1019]: modem_parameter_init :: boot!{modem.c->702}
10:05:05 modem[1019]: modem name is (0, 0){modem.c->294}
10:05:05 modem[1020]: find the modem(ZTE-AD3812:10){modemcheck.c->185}
10:05:06 modem_mg[229]: search usb device{modem_mg.c->1489}
10:05:06 modem[1020]: open the device(/dev/ttyUSB2) succeed{hp_chat.c->326}
```

Figure 2-16 Router off line

```
10:09:02 pppd[1067]: Terminating on signal 15
10:09:02 pppd[1067]: Connect time 3.0 minutes.
10:09:02 pppd[1067]: Sent 445 bytes, received 2660 bytes.
10:09:03 netdown[1336]: ppp interface modem down{netdown.c->37}
10:09:03 netdown[1336]: killall -SIGUSR2 modem{netdown.c->47}
10:09:03 pppd[1067]: Script /usr/sbin/pppdown-run started (pid 1335
10:09:03 pppd[1067]: sent [LCP TermReq id=0x2 "User request"]
10:09:03 pppd[1067]: rcvd [LCP TermAck id=0x2]
10:09:03 pppd[1067]: Connection terminated.
```

Figure 2-17 Router reboot

```
10:12:01 timing[1484]: timing: Reboot the system{hp_misc.c->984}
```

---END

3 FAQ/Exception handling

About this chapter

Chapter	Content
7.1 Hardware failure	Possible hardware failure during using 4G Intelligent Gateway and how to handle them
7.2 Dial online problem	Possible problem during dialing and how to handle them
3.3 VPN	Possible problem when connecting VPN
3.4 WEB config problem config problem	Possible WEB config problem and how to handle them

3.1 Hardware Failure

3.1.1 All LED off

3.1.1.1 Phenomenon

Router LED all dark

3.1.1.2 Possible Reason

- Power supply does not match, it should be 5-36VDC
- No power supply

3.1.1.3 Solution

- Make sure the power supply is 5~36VDC
- Check the power adapter and cable connection

3.1.2 SIM Slot

3.1.2.4 Phenomenon

Cannot insert SIM card

3.1.2.5 Possible Reason

- SIM slot damaged
- SIM card wrong direction

3.1.2.6 Solution

- SIM slot damaged, please contact us to repair
- Check the SIM card direction, please make sure the SIM goldfinger is up

3.1.3 Ethernet Connection

3.1.3.7 Phenomenon

LAN LED dark, cannot visit router WEB GUI

3.1.3.8 Possible Reason

- Ethernet cable connection problem
- Ethernet cable damage
- PC end network card abnormal

3.1.3.9 Solution

- Re-connect Ethernet cable
- Change a Ethernet cable
- Check network card setting on PC end

3.1.4 Antenna Connection

3.1.4.10 Phenomenon

Cannot connect antenna

3.1.4.11 Possible Reason

- Antenna type do not match
- Wrong connection

3.1.4.12 Solution

- Please check antenna interface, should be SMA-J
- Please check antenna type, there are 3G/4G/5G and WIFI, GPS antenna, do not mix them

3.2 Dial Online Problem

3.2.1 Dial discontinue

3.2.1.13 Phenomenon

4G Intelligent Gateway discontinue during dialing, dial failure

3.2.1.14 Possible Reason

- SIM card network type do not match
- SIM charges owed
- Power supply do not match
- Modem setting wrong

3.2.1.15 Solution

- Change to a suitable SIM card
- Recharge SIM card
- Change to suitable power supply
- Change Modem setting, please check related chapter

3.2.2 No Signal

3.2.2.16 Phenomenon

4G Intelligent Gateway modem status show no signal

3.2.2.17 Possible Reason

- Antenna connect wrong
- Modem cannot online
- Modem offline

3.2.2.18 Solution

- Connect suitable antenna
- Modem cannot online, check SIM and modem setting
- Modem offline, check router setting, like wake up setting, ICMP setting, check if there are any setting make router offline

3.2.3 Cannot find SIM/UIM card

3.2.3.19 Phenomenon

4G Intelligent Gateway cannot find SIM/UIM card

3.2.3.20 Possible Reason

- SIM card damage

- SIM bad contact

3.2.3.21 Solution

- Replace SIM card
- Re-install SIM card

3.2.4 Poor Signal

3.2.4.22 Phenomenon

4G Intelligent Gateway no signal or poor signal

3.2.4.23 Possible Reason

- Antenna connect wrong
- Area signal weak

3.2.4.24 Solution

- Check the antenna and re-connect it.
- Contact Telecom Operator to confirm signal problem
- Change to high-gain antenna

3.2.5 Compress Protocol not match

3.2.5.25 Phenomenon

4G Intelligent Gateway dial failure, log shows compress protocol not match

3.2.5.26 Possible Reason

Modem compress protocol do not match with server end

3.2.5.27 Solution

Change compress protocol setting

3.3 VPN Problem

3.3.1 VPDN cannot connect

3.3.1.28 Phenomenon

VPDN cannot connect

3.3.1.29 Possible Reason

- VPDN port work abnormal
- VPDN parameter wrong
- VPDN peer server abnormal

3.3.1.30 Solution

- Make sure Modem is online
- Set the correct port to VPDN
- VPDN parameter wrong
- Check VPDN peer server

3.3.2 VPN cannot communicate

3.3.2.31 Phenomenon

VPN already connect, but cannot communicate

3.3.2.32 Possible Reason

- Router table config wrong
- VPN peer server config wrong

3.3.2.33 Solution

- Add related Router table
- Check VPN peer server setting

3.3.3 Router can communicate but subnet cannot

3.3.3.34 Phenomenon

Router can communicate but subnet cannot

3.3.3.35 Possible Reason

- VPN peer server config wrong
- Local Router has no MASQ
- Wrong local route table

3.3.3.36 Solution

- Check VPN peer server setting
- Local Router has no MASQ, please manual add VPN port MASQ
- Wrong local route table, set right route table

3.4 WEB config problem

3.4.1 Updating firmware failure

3.4.1.37 Phenomenon

Updating firmware failure

3.4.1.38 Possible Reason

- Auto reboot during updating 4G Intelligent Gateway
- Power supply problem
- Wrong firmware
- Power off during updating router

3.4.1.39 Solution

- Check setting, disable the function which may cause reboot
- Change to a suitable power supply
- Ask technical support for suitable firmware
- Power off during updating router, please make sure power supply normal

3.4.2 Backup setting problem

3.4.2.40 Phenomenon

Router import backup setting failure

3.4.2.41 Possible Reason

- Backup setting file format wrong
- No reboot after backup setting

3.4.2.42 Solution

- Choose a right file to import
- Must reboot after import setting, then parameters available

3.4.3 Updating patch failure

3.4.3.43 Phenomenon

Updating fix patch failure, after updating, view fix patch and found no fix patch

3.4.3.44 Possible Reason

- Patch format wrong
- Patch name too complicated

3.4.3.45 Solution

- Check patch format, change to a right one
- Change the patch name to a simple one

3.4.4 CFE Updating failure

3.4.4.46 Phenomenon

CFE updating failure, firmware edition no change

3.4.4.47 Possible Reason

- Power supply do not match
- Firmware version or format do not match
- Power off during updating process

3.4.4.48 Solution

- If power supply do not match, please change then update again
- If firmware version, format do not match, please change then update again
- If power off during updating, please update again

3.4.5 Update failure in WEB GUI

3.4.5.49 Phenomenon

Updating by WEB GUI, failed and cannot visit WEB GUI again

3.4.5.50 Possible Reason

Firmware oversize cause updating failure

3.4.5.51 Solution

Using CFE mode to update again, and router will restore to factory mode. If after CFE updating, still cannot visit WEB GUI, please contact us for repairing

3.4.6 Forget Router Password

3.4.6.52 Phenomenon

Forget router login password

3.4.6.53 Possible Reason

User has changed the password

3.4.6.54 Solution

After router power on, push and hold RESET button over 10 seconds then release, then re-power on router, router will back to factory mode (Username/Password both admin), but patch will reserve

CAUTION

When router is power on, press and hold RESET button around 1s, router will reboot and kept all setting.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

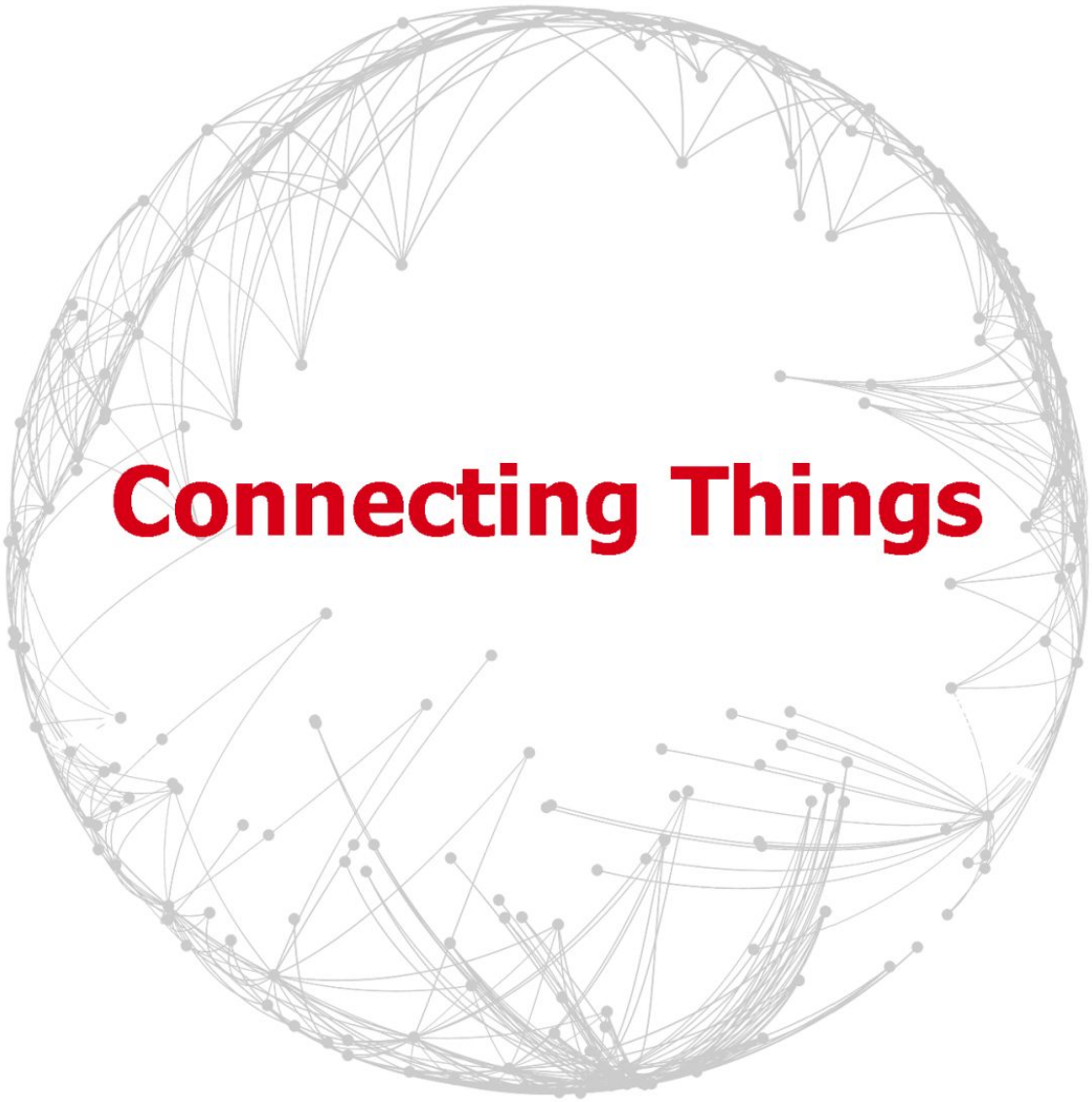
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF Exposure Information

To comply with FCC RF exposure compliance requirements, this grant is applicable to only mobile configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.



Contact US

Hongdian Corporation

Add：F14-F16, Tower A, Building 14, NO.12, Ganli 6th Road, Longgang District, Shenzhen 518112, China

Tel：+86-755-88864288 Fax：-86-755-83404677

CSH：400-00-64288 E-mail：Sales@hongdian.com