

InHand Networks_VG710 User's Manual V1.2



Declaration

Thank you for choosing our product. Before using the product, read this manual carefully.

The contents of this manual cannot be copied or reproduced in any form without the written permission of InHand.

Due to continuous updating, InHand cannot promise that the contents are consistent with the actual product information, and does not assume any disputes caused by the inconsistency of technical parameters. The information in this document is subject to change without notice. InHand reserves the right of final change and interpretation.

© 2020 InHand Networks. All rights reserved.

Conventions

Symbol	Indication
	Indicates a button name, for example, the OK button.
""	Indicates a window name or menu name, for example, the pop-up window "New User".
>>	Separates a multi-level menu. For example, the multi-level menu File >> New >> Folder indicates the menu item "Folder" under the sub-menu "New", which is under the menu "File".
	Reminds readers to be careful. Improper action may result in loss of data or device damage.



Notes contain detailed descriptions and helpful suggestions.

Technical support:

43671 Trade Center Place, Suite 100, Dulles, VA 20166

T: +1 (703) 348-2988

www.inhandnetworks.com

Inquiry: info@inhandnetworks.com | Support: support@inhandnetworks.com

Chapter I routing

1 Overview

InHand VG710 is a new-generation 4G in-vehicle gateway oriented at the Internet of Vehicles (IoV). It provides fast and safe networks for automobiles and transport service vehicles, meeting the requirements of police vehicles, emergency command vehicles, engineering vehicles, medical vehicles, and logistics vehicles for fast mobile networks. It is used with a cloud-based remote vehicle management platform to provide ubiquitous accessible networks and uninterrupted operation supervision for logistics management, asset tracking, mobile office, and government security.

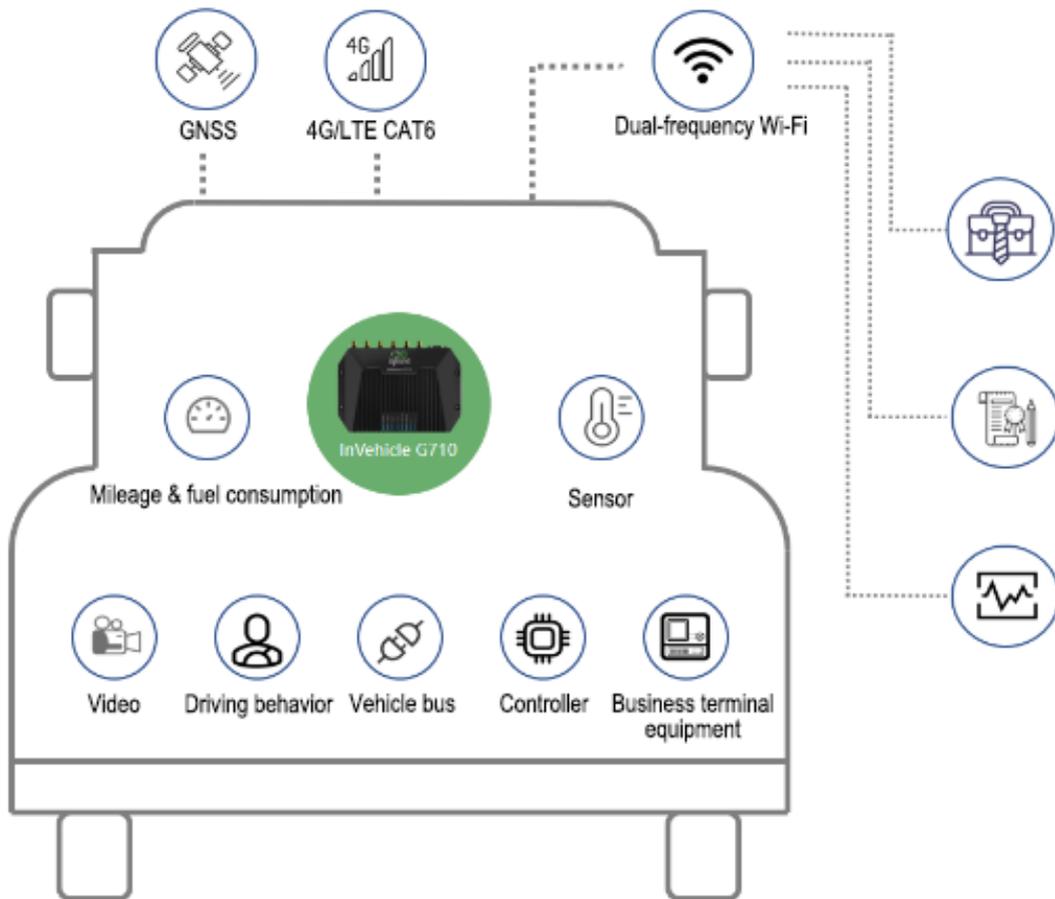


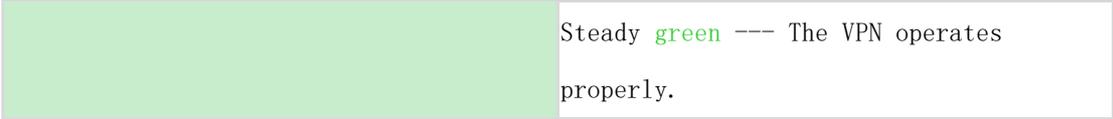
Fig. 1 Application case

2 Hardware

2.1 Indicator Description

VG710 Indicator	Status and Definition
System	<p>Steady off --- The device is powered off.</p> <p>Steady red --- The system is starting.</p> <p>Blinking green --- The system operates properly.</p> <p>Blinking red --- The system is faulty.</p> <p>Blinking blue --- The system is being upgraded.</p>
Cellular	<p>Steady off --- The dialup function is disabled.</p> <p>Blinking green --- Dialup is in progress.</p> <p>Steady green --- Dialup succeeds.</p> <p>Blinking red --- Dialup fails (no module or SIM card is detected).</p>
Signal	<p>Steady off --- The current dialup card has no signal.</p> <p>Steady red --- The current dialup card has weak signals (signal strength: ≤ 9 asu).</p> <p>Steady blue --- The current dialup card has moderate signals (signal strength: 10 - 19 asu).</p> <p>Steady green --- The current dialup card has strong signals (signal strength: ≥ 20 asu).</p>
GNSS	<p>Steady off --- GNSS is disabled.</p>

	<p>Blinking green --- Positioning is in progress.</p> <p>Steady green --- Positioning is completed.</p>
Wi-Fi 2.4G	<p>Used as an AP:</p> <p>Steady off --- The AP is disabled.</p> <p>Blinking green --- The AP operates properly.</p> <p>Used as a STA:</p> <p>Steady off --- The STA is disabled, or no AP is associated.</p> <p>Steady green --- Connection fails due to a wrong password after an AP is associated.</p> <p>Blinking green --- An AP is associated.</p>
Wi-Fi 5G	<p>Used as an AP:</p> <p>Steady off --- The AP is disabled.</p> <p>Blinking blue --- The AP operates properly.</p> <p>Used as a STA:</p> <p>Steady off --- The STA is disabled, or no AP is associated.</p> <p>Steady blue --- Connection fails due to a wrong password after an AP is associated.</p> <p>Blinking blue --- An AP is associated.</p>
U1 and U2	<p>U1:</p> <p>Steady off --- The APP is disabled.</p> <p>Steady green --- The APP is enabled.</p> <p>U2:</p> <p>Steady off --- The virtual private network (VPN) is disabled or abnormal.</p>



Steady **green** --- The VPN operates properly.

2.2 Restoring Default Settings via the Reset Button

To restore default settings via the Reset button, perform the following steps:

1. Power on the device and immediately press and hold the Reset button. After about 15s, only the System indicator is steady red.
2. When the System indicator turns off and becomes red again, immediately release the Reset button.
3. When the System indicator turns off, press the Reset button (ensure that it blinks red twice) and then release it. The device is restored to the default settings.

3 Default Settings

No.	Function	Default Settings
1	Dialup over the cellular network	<ul style="list-style-type: none">– Enabled (The Cellular indicator is steady green after dialup succeeds.) By default, the dual-SIM function is disabled, and SIM1 is enabled.
2	Satellite positioning and inertial navigation service	<ul style="list-style-type: none">– Enabled (The GNSS indicator is steady green after positioning succeeds.)– The inertial navigation function is enabled.
3	On-board diagnostics (OBD)	<ul style="list-style-type: none">– Enabled– The CANbus baud rate is automatically detected.– The OBD protocol is automatically detected.– OBD data is automatically scanned.
4	Default settings of Wi-Fi	<ul style="list-style-type: none">– The Wi-Fi 2.4G AP is enabled. The SSID

		<p>starts with VG710-, followed by six digits.</p> <ul style="list-style-type: none"> - The Wi-Fi 5G AP is enabled. The SSID starts with VG710-5G-, followed by six digits. - WPA2-PSK is used for authentication. - The password contains the last eight digits of the SN.
5	Default settings of Ethernet	<ul style="list-style-type: none"> - Four LAN ports are enabled. - The IP address is 192.168.2.1. - The subnet mask is 255.255.255.0. - The DHCP server is enabled. The IP address pool is 192.168.2.2 - 192.168.2.100, and IP addresses can be automatically allocated to downstream devices.
6	Network access control for the gateway	<ul style="list-style-type: none"> - HTTP and HTTPS are enabled, with the port

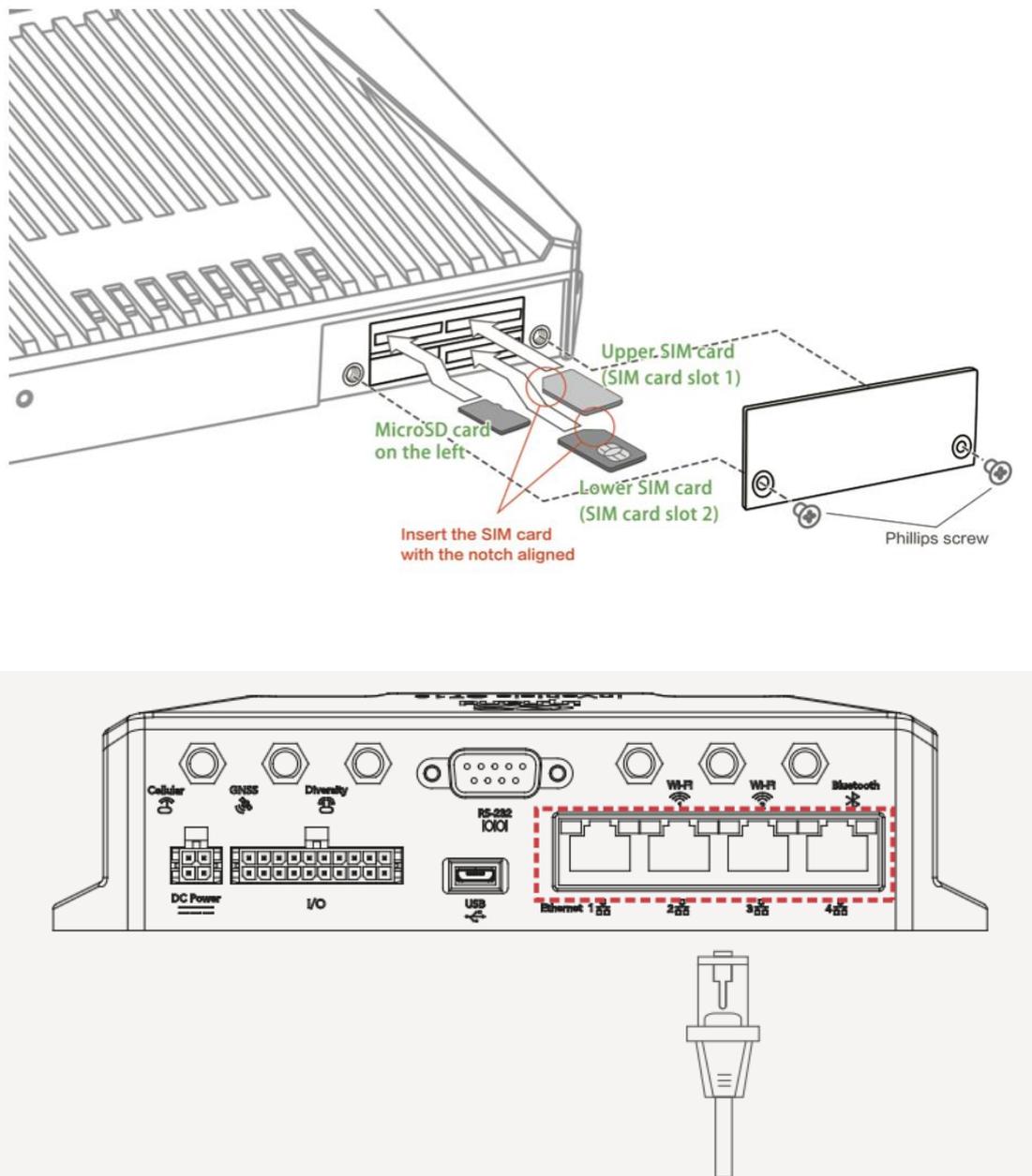
		<p>numbers of 80 and 443 respectively.</p> <ul style="list-style-type: none"> – Telnet is disabled. – SSH is disabled. – Access from the cellular network is allowed only over HTTPS.
7	User name and password	<ul style="list-style-type: none"> – adm/123456 (super administrator)
8	Power management	<ul style="list-style-type: none"> – shutdown-delay 30: The power-off delay is 30s. – standby-mode 1: The power-off function is enabled. – standby-check-interval 20 indicates the power check interval in standby mode. – standby-voltage 90: The standby threshold voltage is 9 V. – standby-resume-voltage 105: The threshold voltage for resuming normal operating in standby mode is 10.5 V.
9	I0	<ul style="list-style-type: none"> – Four digital output channels generate

		<p>output at low level by default, and the pull-up resistor is disabled.</p> <ul style="list-style-type: none"> – The pull-up resistor for six digital input channels is disabled.
10	Serial port	<ul style="list-style-type: none"> – RS232 <p>Baud rate: 9600 Data bits: 8 bits Parity bit: none Stop bit: 1 bit</p> <ul style="list-style-type: none"> – RS485 <p>Baud rate: 9600 Data bits: 8 bits Parity bit: none Stop bit: 1 bit</p>

4 Login and Network Access

4.1 Network Access via the Dialup Card

1. Insert the SIM card, connect the GNSS and cellular antennas, and connect the power supply and PC. Insert the diversity dialup antenna when the dialup card has poor signals.





Note:

Before inserting or removing the SIM card, unplug the power cable; otherwise, the operation will cause data loss or damage the gateway.

2. Assign an IP address to the PC, which is on the same network segment as the IP address of the gateway.

Method 1: Enable the PC to obtain an IP address automatically (recommended).

Method 2: Configure a fixed IP address on the same network segment as the gateway address for the PC.

Step: Select "Use the following IP address", enter any IP address in the range of 192.168.2.2 to 192.168.2.254 (different from the initial IP address 192.168.2.1 of the gateway), the subnet mask 255.255.255.0, and the default gateway address 192.168.2.1, and then click OK.

Internet Protocol Version 4 (TCP/IPv4) Properties



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

. . .

Subnet mask:

. . .

Default gateway:

. . .

Obtain DNS server address automatically

Use the following DNS server addresses

Preferred DNS server:

. . .

Alternate DNS server:

. . .

Validate settings upon exit

Advanced...

OK

Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:	192 . 168 . 2 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 2 . 1

Obtain DNS server address automatically

Use the following DNS server addresses

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	. . .

Validate settings upon exit

Advanced...

OK Cancel

Obtain an IP address automatically Use a fixed IP address

3. Open the browser, enter the default IP address 192.168.2.1 of the gateway in the address bar, and press Enter. (Edge Firefox or Chrome recommended)



4. Log in (if a blocking prompt is displayed, click "Advanced >> Continue"). Enter the default username adm and password 123456 to go to the web interface.



Method 3

Step 1: Connect to the device through the network cable or Wi-Fi (see the SSID and key on the nameplate). If you use Wi-Fi, the Wi-Fi indicator is steady on in green or blinks.

Step 2: Enter the default device IP address 192.168.2.1 in the address bar of the web browser to open the login page.

Step 3: Enter the default username adm and password 123456 to go to the web interface.

5. Click "Network >> Cellular", check "Enable", and click Apply & Save. If the network connection status is "Connected" and an IP address has been allocated, the SIM card has been connected to the network.

(Set the APN parameters for a private-network card.)

Network >> Cellular

Status Cellular

Enable

	SIM1	SIM2
Profile	<input type="text" value="auto"/>	<input type="text" value="auto"/>
Roaming	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PIN Code	<input type="text"/>	<input type="text"/>
Network Type	<input type="text" value="Auto"/>	
Static IP	<input type="checkbox"/>	
Connection Mode	<input type="text" value="Always Online"/>	
Redial Interval	<input type="text" value="10"/> s	
ICMP Detection Server	<input type="text"/>	
ICMP Detection Interval	<input type="text" value="30"/> s	
ICMP Detection Timeout	<input type="text" value="5"/> s	
ICMP Detection Max Retries	<input type="text" value="5"/>	
ICMP Detection Strict	<input type="checkbox"/>	
Show Advanced Options	<input type="checkbox"/>	

Profile

Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	3gnet	*99***1#	Auto	gprs	*****

Network >> Cellular

Status Cellular

Modem

Active SIM	SIM 1
IMEI Code	353593090129021
IMSI Code	460110923582245
ICCID Code	89860318040283846651
Signal Level	📶(29 asu -55 dBm)
RSRP	-85 dBm
RSRQ	-15 dB
Register Status	registered
Operator	CHN-CT
Network Type	4G
LAC	9B11
Cell ID	9D54212

Network

Status	Connected
IP Address	10.65.120.18
Netmask	255.255.255.252
Gateway	10.65.120.17
DNS	61.139.2.69 218.6.200.139
MTU	1500

6. Ping a common website in China with a ping detection tool. If there is data transmission, the device has been successfully connected to the network.

Tools >> Ping

Ping

Host	<input type="text" value="www.qq.com"/>	<input type="button" value="Ping"/>
Ping Count	<input type="text" value="4"/>	
Packet Size	<input type="text" value="32"/> Bytes	
Expert Options	<input type="text"/>	

```
PING www.qq.com (14.18.175.154): 32 data bytes
40 bytes from 14.18.175.154: seq=0 ttl=53 time=63.619 ms
40 bytes from 14.18.175.154: seq=1 ttl=53 time=52.125 ms
40 bytes from 14.18.175.154: seq=2 ttl=53 time=47.887 ms
40 bytes from 14.18.175.154: seq=3 ttl=53 time=47.264 ms

--- www.qq.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 47.264/52.723/63.619 ms
```

7. Enable the dual-SIM function when two SIM cards are used.

Network >> Cellular

Status Cellular

Show Advanced Options

Initial Commands

RSSI Poll Interval s(0: disable)

Dial Timeout s

MTU

Netmask

Infinitely Dial retry

Dual SIM Enable

Main SIM ▼

Max Number of Dial

Min Connected Time s(0: disable)

CSQ Threshold (0: disable)

CSQ Detect Interval (0: disable)

CSQ Detect Retries

Backup SIM Timeout s(0: disable)

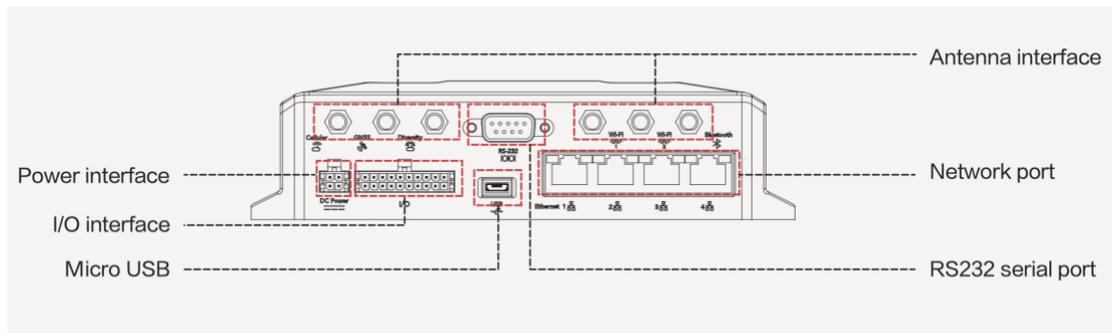
Debug

Profile

Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	3gnet	*99***1#	Auto	gprs	*****

4.2 Network Access via Wi-Fi

1. Complete the connection shown in the following figure. The Wi-Fi antenna is screwed into the panel Wi-Fi antenna interface. Connect to the device through the network cable or Wi-Fi (see the SSID and key on the nameplate). If you use Wi-Fi, the Wi-Fi indicator is steady on in green or blinks.



2. Assign an IP address to the PC, which is on the same network segment as the IP address of the gateway. Log in to the web page. For details, see [4.1 Network Access via the Dialup Card](#).

3. Click "Network >> Wi-Fi" and select Wi-Fi 2.4G or Wi-Fi 5G as a client. Enter the name, authentication method, and key of an available wireless access point (AP). Click Apply & Save.

Network >> Wi-Fi

Enable

Station Role: Client

Default Route:

SNAT:

SSID: Inhand

Auth Method: WPA2-PSK

Encrypt Mode: CCMP

WPA/WPA2 PSK Key: ●●●●●●●●●●●●●●●●

4. Click "Status". The current network status is "Connected", and an IP address is obtained successfully, indicating that the device has been successfully connected to the network via Wi-Fi.

Network >> Wi-Fi

Status

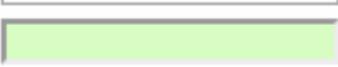
Wi-Fi 2.4G

Wi-Fi 5G

Wi-Fi 2.4G Status

Station Role	Client
Status	Connected
SSID	Inhand
MAC Address	00:18:05:10:30:31
Auth Method	WPA2-PSK
Encrypt Mode	CCMP
IP Address	192.168.100.44
Netmask	255.255.255.0
Gateway	192.168.100.1
DNS	61.139.2.69 202.98.96.68
Connection time	0 day, 00:01:21

5 Network Management

In parameter settings, a green text box  indicates a mandatory item, and a pure white text box

 indicates an optional item.

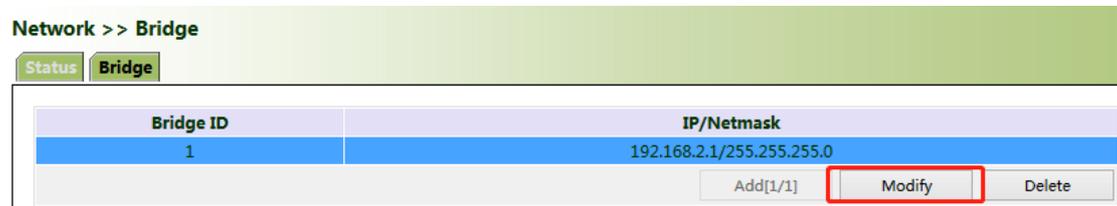
5.1 Network

5.1.1 Bridge Port

A bridge port is intended to connect two different physical LANs over a bridge, to enable storage and forwarding across LANs at the link layer.

Method for modifying the IP address of a bridge port and bridge members:

1. Click "Network >> Bridge" and select "Bridge >> Modify".



2. Modify the IP address of the bridge port or bridge members. Among the bridge members, dot11radiol and dot11radio2 are Wi-Fi 2.4G and Wi-Fi 5G ports respectively.

Network >> Bridge

Status **Bridge**

Bridge ID

Bridge

Primary IP

IP Address	<input type="text" value="192.168.2.1"/>
Netmask	<input type="text" value="255.255.255.0"/>

Secondary IP

IP Address	Netmask
<input type="text"/>	<input type="text"/>
<input type="button" value="Add[0/10]"/>	

Bridge Member

vlan 1	dot11radio 1	dot11radio 2
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

5.1.2 VLAN Port

A virtual LAN (VLAN) comprises a group of logical devices and users. These devices and users are not limited by physical locations, but can be organized based on functions, departments, applications, and other factors. They communicate with each other as if they are on the same network segment, which contributes to the name of VLAN.

Method for adding a port of VLAN 2:

1. Click "Network >> VLAN >> Configure VLAN Parameters >> Add". Set the virtual IP address of the port of VLAN 2 and select the member port of VLAN 2 as required. Click Apply & Save.

Network >> VLAN

VLAN Trunk **Configure VLAN Parameters**

VLAN ID

VLAN Virtual Interface

Primary IP

IP Address

Netmask

Secondary IP(s)

IP Address	Netmask
<input type="text"/>	<input type="text"/>

Add[0/10]

VLAN Member Ports

GE1/1	GE1/2	GE1/3	GE1/4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Apply & Save Cancel Back

2. Return to the VLAN list. The port of VLAN 2 has been successfully added.

Network >> VLAN

VLAN Trunk **Configure VLAN Parameters**

VLAN ID	GE1/1	GE1/2	GE1/3	GE1/4	Primary IP/Netmask
1	✓	✓	✓		
2				✓	192.168.3.1/255.255.255.0

Add[2/16] Modify Delete

Currently, VLAN ports of the device support two link types: access and trunk. An access port belongs to only one VLAN and is generally connected to a computer. A trunk port can be used for multiple VLANs and can receive messages from or send messages to multiple VLANs. It can be connected to a switch or a user's computer. You can select the link type as required on the "VLAN Trunk" page.

Network >> VLAN

VLAN Trunk

Configure VLAN Parameters

Port	Mode	Native VLAN
GE1/1	Access	1
GE1/2	Access	1
GE1/3	Trunk	1
GE1/4	Trunk	2

NOTE:

Native VLAN is only valid in trunking mode

Apply & Save

Cancel

5.1.3 ADSL Dialup (PPPoE)

Method for connecting the gateway to the PPPoE server:

1. Click "Network >> ADSL Dialup (PPPoE)", select the VG710 interface for connecting to the PPPoE server in the "Dial Pool" bar, and click Add.
2. Enter the user name, password, and pool ID of the PPPoE server in the "PPPoE List" bar. The pool ID must be the same as that in the "Dial Pool" bar. Click Add, and then click Apply & Save.

Network >> ADSL Dialup (PPPoE)

Status ADSL Dialup (PPPoE)

Dial Pool

Pool ID	Interface
1	bridge 1

Add[0/10]

PPPoE List

Enable	ID	Pool ID	Authentication Type	Username	Password	Local IP Address	Remote IP Address	Keepalive Interval	Keepalive Retry	Debug
✓	1	1	Auto	test	*****			120	3	No
<input checked="" type="checkbox"/>	2	1	Auto	test	●●●●●			120	3	<input type="checkbox"/>

Add[0/10]

Apply & Save

Cancel

5.1.4 Wi-Fi

The gateway can be used as an AP or a client. When it is used as an AP, other users can access the Internet through the gateway via Wi-Fi. When it is used as a client, the gateway connects to an AP for Internet access. The status bar shows the current Wi-Fi connection status of the gateway.

Network >> Wi-Fi

Status

Wi-Fi 2.4G

Wi-Fi 5G

Wi-Fi 2.4G Status

Station Role	Client
Status	Disconnected
SSID	Inhand
MAC Address	00:18:05:10:30:31
Auth Method	WPA2-PSK
Encrypt Mode	CCMP
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Connection time	0 day, 00:00:00

Wi-Fi 5G Status

Station Role	AP
Status	Enabled
SSID	VG710-5G-103032
MAC Address	00:18:05:10:30:32
Channel	36
Auth Method	WPA2-PSK
Encrypt Mode	CCMP

Method for providing network access services for wireless terminals when the gateway is used as an AP:

Click "Wi-Fi >> Wi-Fi 2.4 or Wi-Fi 5G" and select "AP" for "Station Role". Enter the SSID, authentication method, and key consistent with those of the wireless AP. Click Apply & Save.

Network >> Wi-Fi

Status **Wi-Fi 2.4G** Wi-Fi 5G

Enable	<input checked="" type="checkbox"/>
Station Role	AP ▾
SSID Broadcast	<input checked="" type="checkbox"/>
AP Isolate	<input type="checkbox"/>
Bridge	<input checked="" type="checkbox"/>
Radio Type	802.11ng ▾
Channel	Auto ▾
SSID	VG710-103031
Auth Method	WPA2-PSK ▾
Encrypt Mode	CCMP ▾
WPA/WPA2 PSK Key	●●●●●●●●
Bandwidth	20MHz ▾
Stations Limit	

Apply & Save Cancel

Method for connecting to an AP for Internet access when VG710 is used as a client:

Select "Client", enter the Wi-Fi SSID and key, and click Apply & Save.

Network >> Wi-Fi

Status **Wi-Fi 2.4G** Wi-Fi 5G

Enable	<input checked="" type="checkbox"/>
Station Role	Client ▾
Default Route	<input checked="" type="checkbox"/>
SNAT	<input checked="" type="checkbox"/>
SSID	Inhand
Auth Method	WPA2-PSK ▾
Encrypt Mode	CCMP ▾
WPA/WPA2 PSK Key	●●●●●●●●

Apply & Save Cancel

Note: please click "apply & save" button to enable scan function

5.1.5 Loopback Port

Method for adding multiple loopback ports:

Click "Network >> Loopback >> Multi-IP Settings", configure any IP address for the gateway, click Add, and then click Apply & Save.

Network >> Loopback

Loopback

IP Address

Netmask

Multi-IP Settings

IP Address	Netmask
<input type="text"/>	<input type="text"/>

5.1.6 Layer 2 Switch

Check the network connection status of GE 1 to GE 4. LINK UP indicates that the network is connected. LINK DOWN indicates that the network is disconnected.

Network >> Layer2 Switch

Status

Port	Link Status	Speed	Duplex	PVID
GE1/1	LINK UP	1000M	FULL	1
GE1/2	LINK DOWN	---	---	1
GE1/3	LINK DOWN	---	---	1
GE1/4	LINK DOWN	---	---	1

5.2 OBD

OBD is used to collect vehicle condition data, obtain emission information, and perform fault diagnosis in real time. Vehicle condition data includes key parameters such as the fuel level, mileage, driving speed, engine speed, engine load, coolant temperature, and brake pressure. Emission information includes the

volume of AdBlue, the operating and monitoring status of various exhaust post-processing sensors (such as the exhaust gas sensor and diesel particle filter) and catalysts, etc. In fault diagnosis, standard fault codes of vehicles and description information can be obtained in real time, so that vehicle maintenance personnel can learn the vehicle health status in time and locate the faults. To collect vehicle data, the gateway is connected to the diagnostic port of the vehicle through the I/O port of the gateway over the OBD-II or J1939 cable. The cable accessories can be selected or customized during purchasing. For details about the access method, see Section 4.4 in the *VG710 Quick Start Guide*. After the gateway starts, the OBD service is automatically enabled to collect key vehicle condition data and fault code information.



注意

Note:

The power supply and OBD cable of the gateway shall be installed when the vehicle is off.

The vehicle status information is displayed on the OBD status page.

OBD Status:

CAN Link Status (ERROR-ACTIVE indicates that the gateway has successfully connected to the diagnostic port of the vehicle. Other status indicates that the connection is abnormal or the diagnostic port of the vehicle is not identified.)

CAN Baudrate (In OBD, the CAN baudrate is automatically adapted, generally 250 kbps or 500 kbps.)

CAN Bind ("OBD" (default) or "Custom")

OBD Connection Status ("Disconnected", "Connecting", or "Connected")

OBD Protocol Type (OBD-II or J1939)

Services >> OBD

Status

OBD Status

CAN Link Status	ERROR-ACTIVE
CAN Birtate	500 kbps
CAN Bind	OBD
OBD Connection Status	Connected
OBD Protocol Type	OBD-II

Scan OBD Data

Export OBD Report

Upload OBD Report

Scan OBD Data and Export OBD Report:

Click the Scan OBD Data button to generate a OBD data report containing detailed vehicle condition data and diagnostic information. Click the Export OBD Report button to save the generated OBD data report to the local storage.

OBD Data Stream: The real-time vehicle condition data is displayed.

Parameter Name	Value	Units
MIL Status	off	---
DTC Num	0	---
Fuel System Status	OL-Drive B2	---
Engine Load	29.02	%
Engine Coolant Temp	215.00	C
Fuel Pressure	0.00	kPa
Intake Manifold Pressure	0.00	kPa
Engine RPM	1010.75	RPM
Speed	132.00	km/h
Intake Manifold Temp	0.00	C
Throttle Position	18.43	%
OBD Standards	0x00000007	---
Engine Up Time	123.00	sec
MIL Activated Distance	0.00	km
Fuel Rail Pressure	0.00	kPa
Fuel Level	0.00	%
DTC Cleared Distance	0.00	km
Barometric Pressure	0.00	kPa
Battery Volt	0.00	V
Ambient Air Temp	0.00	C
MIL Activated Time	0.00	sec

OBD Ability:

Version of the OBD ability;

Type of the OBD protocol;

Vehicle identification number (VIN);

Valid variables and reference values that can be collected by the gateway.

▣ OBD Ability

Version 1.01
 Protocol OBD-II
 VIN 1A1JC5444R7252367

Valid Variable	Reference Value
MIL Status	0
DTC Num	0
Engine Load	100
Engine Coolant Temp	215
Fuel Pressure	0
Engine RPM	0
Speed	255
Throttle Position	0
Engine Up Time	6950
MIL Activated Distance	0
Fuel Level	0
DTC Cleared Distance	0
Battery Volt	0
Ambient Air Temp	0
MIL Activated Time	0
DTC Cleared Time	0
Engine Oil Temp	16
Fuel Rate	911.6

5.3 VPN Application

The VPN is intended to establish a private network on the public network for encrypted communication. A VPN gateway enables remote access by encrypting data packets and converting the destination address of data packets. The VPN can be realized by a server, hardware, or software, or in other ways. Compared with the traditional DDN private line or frame relay, the VPN provides a more secure and convenient remote access solution.

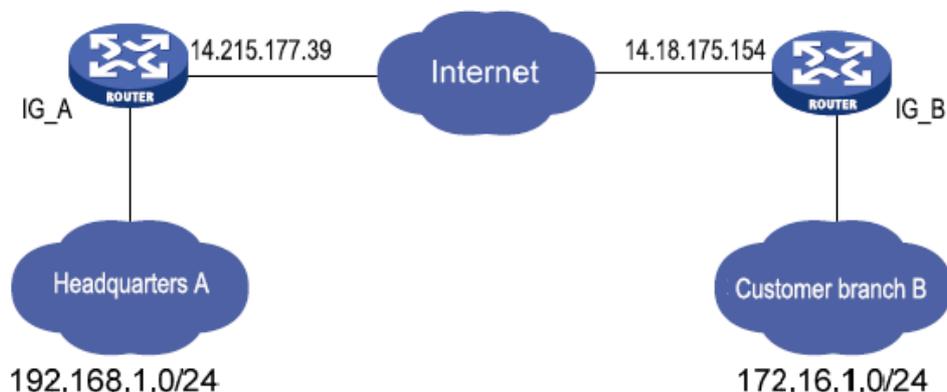
Common VPN application scenario: For example, an employee on a business trip accesses the enterprise's intranet. The employee connects to the enterprise's VPN server and then accesses the enterprise's intranet through the VPN server. Communication data

between the VPN server and the client is encrypted and can be regarded as being transmitted on a dedicated data network. This ensures data security.

5.3.1 IPsec

IPsec is a group of open network security protocols developed by IETF. At the IP layer, the data source authentication, data encryption, data integrity, and anti-replay functions are used to ensure the security of data transmission between communication parties on the Internet. This reduces the risk of leakage and eavesdropping, ensures the integrity and confidentiality of data, and ensures the security of service transmission for users.

Scenario: Data is transmitted between the subnet (192.168.1.0/24) of headquarters A and the subnet (172.16.1.0/24) of customer branch B through gateway A and gateway B. The transmission channels of gateway A and gateway B are encrypted over IPsec, to protect the security of data transmission between headquarters A and customer branch B.



Method for encrypting the transmission channels of gateway A and gateway B over IPsec:

Parameter settings:

Gateway A		Gateway B	
Set IKEv1/v2 parameters		Set IKEv1/v2 parameters	
ID	Custom	ID	Custom

Encryption algorithm	AES128		Encryption algorithm	Same as that of gateway A
Hash algorithm	SHA1		Hash algorithm	
Diffie-Hellman key exchange	Group2		Diffie-Hellman key exchange	
Lifecycle	86400		Lifecycle	
IPsec policy			IPsec policy	
Name	Custom		Name	Custom
Encapsulation	ESP		Encapsulation	Same as that of gateway A
Encryption algorithm	AES128		Encryption algorithm	
Authentication method	SHA1		Authentication method	
IPsec mode	Tunnel mode		IPsec mode	
IPsec tunnel configuration			IPsec tunnel configuration	
Peer address	Address where gateway B establishes the IPsec service		Peer address	Address where gateway A establishes the IPsec service
Interface	Interface for establishing the IPsec service		Interface	Interface for establishing the IPsec service
IKE version	IKE version used		IKE version	Same as that of gateway A
Authentication method	Shared key		Authentication method	

Local subnet	IP address of the subnet of gateway A		Local subnet	IP address of the subnet of gateway B
Peer subnet	IP address of the subnet of gateway B		Peer subnet	IP address of the subnet of gateway A

Detailed configuration steps:

1. Configure gateway A and gateway B.
 - (1) Add IKE and IPsec policies, and click Apply & Save.
 - (2) Add IPsec tunnels and click Apply & Save.

VPN >> IPsec

Status **IPsec Setting** IPsec Extern Setting

Enable

IKEv1 Policy

ID	Encryption	Hash	Diffie-Hellman Group	Lifetime
1	AES128	SHA1	Group2	86400
<input type="text"/>	<input type="text" value="AES128"/>	<input type="text" value="SHA1"/>	<input type="text" value="Group2"/>	<input type="text" value="86400"/>

IKEv2 Policy

ID	Encryption	integrity	Diffie-Hellman Group	Lifetime
<input type="text"/>	<input type="text" value="AES128"/>	<input type="text" value="SHA1"/>	<input type="text" value="Group2"/>	<input type="text" value="86400"/>

IPsec Policy

Name	Encapsulation	Encryption	Authentication	IPsec Mode
a	ESP	AES128	SHA1	Tunnel Mode
<input type="text"/>	<input type="text" value="ESP"/>	<input type="text" value="AES128"/>	<input type="text" value="SHA1"/>	<input type="text" value="Tunnel Mode"/>

IPsec Tunnels

Name	Status	Local Subnets	Remote Subnets	Interface	IKE Version
IPsec1_118.122.120.22	Connected	192.168.6.0/255.255.255.0	192.168.5.0/255.255.255.0	cellular 1	IKEv1

2. Access the IPsec status page. The IPsec VPN is established successfully if the page is shown as below.

VPN >> IPsec

Status IPsec Setting IPsec Extern Setting

Tunnel Status

Name	Destination Address	IkeStatus	Ike Timer	IPsec SAs
IPsec1_118.122.120.22	118.122.120.22	ESTABLISHED	established 126s; reauthentication in 85641s	192.168.6.0/24==192.168.5.0/24

IPsec SA Status

IPsec SA	Tunnel Name	Destination Address	Status	IPsec Timer	Tunnel Flow
192.168.6.0/24==192.168.5.0/24	IPsec1_118.122.120.22	118.122.120.22	INSTALLED	installed 126s rekeying in 2508s expires in 3474s	bytes-in 0 packets-in 0 bytes-out 0 packets-out 0



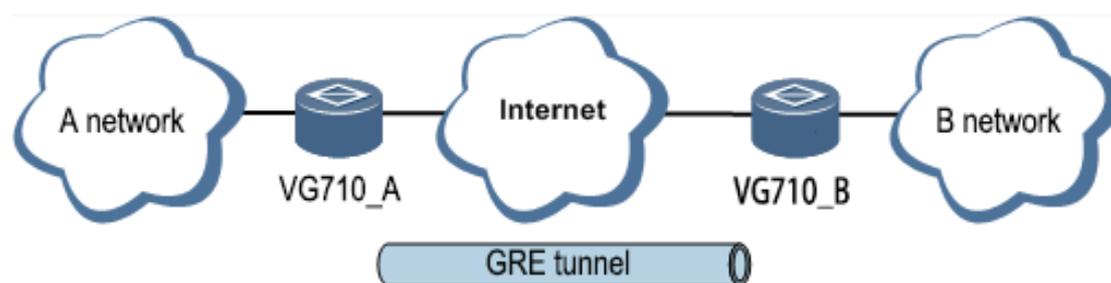
注意 Note:

The IPsec profile does not need to be configured for establishing an IPsec VPN, but needs to be configured for establishing a DM VPN.

5.3.2 GRE

The Generic Routing Encapsulation (GRE) protocol can be used to encapsulate datagrams of some network layer protocols, so that these encapsulated datagrams can be transmitted on the IPv4 network.

Scenario: GRE is enabled for VG710_A and VG710_B through the public network.



Method for enabling GRE for transmission channels of VG710_A and VG710_B:

1. Click "VPN >> GRE" and then click Add.

GRE Entry

Enable	Index	Local virtual IP	Local Address	Remote virtual IP	Peer Address	Key	NHRP Enable	IPsec Profile	Description
						Add[0/100]		Modify	Delete

2. Set "Index" as required. Select "Point to Point" or "Subnet" for "Network Type". Set "Local Virtual IP" and "Peer Virtual IP", ensuring that they are on the same network segment. Enter the source and peer IP addresses or interfaces and the key. Click Apply & Save.

VPN >> GRE

GRE

Enable	<input checked="" type="checkbox"/>
Index	1
Network Type	Point to Point ▾
Local Virtual IP	1.1.1.1
Peer Virtual IP	1.1.1.2
Source Type	Interface ▾
Local Interface	cellular 1 ▾
Peer IP	118.122.120.22
Key	<input type="text"/>
MTU	<input type="text"/>
NHRP Enable	<input type="checkbox"/>
IPsec Profile	Disable ▾
Description	<input type="text"/>

.....

3. Set VG710_B in the same way. The virtual and peer IP addresses of VG710_B must correspond to those of VG710_A, and the key must be the same as that of VG710_A.

5.3.3 L2TP

The Layer 2 Tunneling Protocol (L2TP) is an industrial-standard Internet tunneling protocol used to encrypt network data streams.

Method for settings when the gateway is used as an L2TP client:

1. Click "VPN >> L2TP >> L2TP Client >> L2TP Class", enter a name of an L2TP class, and click Add.

VPN >> L2TP

Status **L2TP Client** L2TP Server

L2TP Class

Name	Authentication	Hostname	Challenge Secret
class1	No		
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Add[1/10]

2. Configure the pseudowire class: Enter a name of any pseudowire class. "L2TP Class" is the same as that on the "L2TP Class" page. Set "Source Interface" to the interface connecting to the server. Select L2TPV2 for "Protocol" and click Add.

Pseudowire Class

Name	L2TP Class	Source Interface	Data Encapsulation Method	Tunnel Management Protocol
Pse1	class1	cellular 1	L2TPV2	L2TPV2
<input type="text"/>	class1		L2TPV2	L2TPV2

Add[1/10]

3. Set L2TPV2 tunnel parameters: Enter the server's domain name or IP address for "L2TP Server". "Pseudowire Class" is the same as that on the "Pseudowire Class" page. Enter the user name and password created on the server. Set other parameters as required. Click Apply & Save.

VPN >> L2TP

Status **L2TP Client** L2TP Server

L2TPv2 Tunnel

Enable	ID	L2TP Server	Pseudowire Class	Authentication Type	Username	Password	Local IP Address	Remote IP Address
<input checked="" type="checkbox"/>	1	118.122.120.22	Pse1	Auto	test	*****		
<input checked="" type="checkbox"/>	2		Pse1	Auto				

Add[1/10]

L2TPv3 Tunnel

Enable	ID	Peer ID	Pseudowire Class	Protocol	Source Port	Destination Port	Xconnect Interface
<input checked="" type="checkbox"/>	1			IP			

Add[0/10]

L2TPv3 Session

Local Session ID	Remote Session ID	Local Tunnel ID	Local Session IP Address

Add[0/10]

Apply & Save Cancel

4. After gateway A and gateway B are configured, access the L2TP status page to view the L2TP connection status.

VPN >> L2TP English

Status **L2TP Client** L2TP Server

L2TP Client

Tunnel Name	L2TP Server	Status	Local IP Address	Remote IP Address	Local Session ID	Remote Session ID
virtual-ppp 1	118.122.120.22	Connected (141s)	6.6.6.2	6.6.6.1	-	-

5.3.4 OpenVPN

OpenVPN is realized based on the application-layer VPN of the OpenSSL library. It supports multiple authentication methods such as the certificate, key, and user name/password. Compared with the traditional VPN, it is simpler and easier to use.

Authentication methods:

Authentication method	Operation on the web page
None	No authentication is required.

User name/password	Enter the user name and password created on the OpenVPN server, click "VPN >> Certificate Management", and import the CA certificate, public key, and private key for authentication.
Pre-shared key	Enter the pre-shared key created on the OpenVPN server.
Digital certificate	Click "VPN >> Certificate Management" and import the CA certificate, public key, and private key.
Digital certificate/user name/password	Enter the user name and password created on the OpenVPN server, click "VPN >> Certificate Management", and import the CA certificate, public key, and private key for authentication.
Digital certificate/TLS authentication	Enter the pre-shared key created on the OpenVPN server, click "VPN >> Certificate Management", and import the CA certificate, public key, and private key for authentication.
Digital certificate/TLS authentication/user name/password	Enter the pre-shared key, user name, and password created on the OpenVPN server, click "VPN >> Certificate Management", and import the CA certificate, public key, and private key for authentication.

Method for settings when the gateway is connected to the OpenVPN server as a client:

OpenVPN can be configured manually, or OpenVPN configurations can be imported. In the following example, the authentication type is a digital certificate.

1. Set the OpenVPN parameters for the gateway as shown in the figure below, ensuring that the network parameters at both ends of the tunnel are consistent. Click Apply & Save.

VPN >> OpenVPN

Status **OpenVPN Client** **OpenVPN Server**

Enable

Index

OpenVPN Server	Port	Protocol Type
118.122.120.22	1194	udp
<input type="text"/>	<input type="text" value="1194"/>	<input type="text" value="udp"/>

Add[1/4]

Authentication Type

Description

Local IP Address

Remote IP Address

Show Advanced Options

Import Configuration

No file selected. **Browse...** **Import** **Export**

Apply & Save **Cancel**

2. Select a digital certificate for "Authentication Type", click "VPN >> Certificate Management", and import the CA certificate, public key, and private key.

3. Click Apply & Save. Return to the "Status" page and view the tunnel status.

VPN >> OpenVPN

Status **OpenVPN Client** **OpenVPN Server**

Tunnel Name	OpenVPN Server	Interface Type	Status	Local IP Address	Remote IP Address	Description
openvpn 1	118.122.120.22	tun	connected (0 day, 00:01:08s)	20.20.20.6	20.20.20.5	

5.3.5 Certificate Management

Certificates can be imported or exported on this page. Certificates are used for IPsec and OpenVPN services.

Method for importing a certificate:

Click "VPN >> Certificate Management >> Browse", select the certificate obtained from the certificate server, click Import *XX* Certificate, and then click Apply & Save.

The screenshot shows the "VPN >> Certificate Management" interface. At the top, there are tabs for "Certificate Management" and "ROOT CA". Below this, the "Certificate Management" section is visible. It includes several settings: "Enable SCEP (Simple Certificate Enrollment Protocol)" with an unchecked checkbox, "Protect Key" and "Protect Key Confirm" with empty text input fields, and "Revocation" with an unchecked checkbox. Below these settings is a table of actions:

No file selected.	Browse...	Import Public Key Certificate	Export Public Key Certificate
No file selected.	Browse...	Import Private Key Certificate	Export Private Key Certificate
No file selected.	Browse...	Import CA Certificate	Export CA Certificate
No file selected.	Browse...	Import CRL	Export CRL
No file selected.	Browse...	Import PKCS12 Certificate	Export PKCS12 Certificate

At the bottom of the form, there are two buttons: "Apply & Save" and "Cancel".

The screenshot shows the "VPN >> Certificate Management" interface with the "ROOT CA" tab selected. Below the tabs, there is a table with two columns: "CA Name" and "Issuer Name". Below the table, there is a section titled "Import Root CA Certificate" with a single row of actions:

CA Name	Issuer Name

Below the table, there is a section titled "Import Root CA Certificate" with a single row of actions:

No file selected.	Browse...	Import Root CA Certificate
-------------------	-----------	----------------------------

If no local certificate is available, check "Enable SCEP (Simple Certificate Enrollment Protocol)" to apply for a certificate online.

Method for applying for a certificate for the gateway online:

1. Click "VPN >> Certificate Management". Check "Enable SCEP (Simple Certificate Enrollment Protocol)" and "Force to re-enroll". Enter the certificate protection key and confirm it. Enter the URL of the

certificate server, the certificate name, and the FQDN. Click Apply & Save.

2. After the server issues the certificate, check the application status. If the application status is "Completion", the certificate application succeeds.

VPN >> Certificate Management

Certificate Management **ROOT CA**

Certificate Management

Enable SCEP (Simple Certificate Enrollment Protocol)	<input checked="" type="checkbox"/>
Force to re-enroll	<input type="checkbox"/>
Status	Initiation
Protect Key	●●●●●●
Protect Key Confirm	●●●●●●
Strict CA	<input type="checkbox"/>
Server URL	http://192.168.2.111/cersrv/mscep/mscep.dll
Common Name	VG7100116
FQDN	VG7100116@inhand.com.cn
Unit 1	
Unit 2	
Domain	
Serial Number	
Challenge	
Challenge Confirm	
Unstructured address	
RSA Key Length	1024 bits
Poll Interval	60 s

5.4 Services

5.4.1 DHCP (Automatic IP Address Allocation)

DHCP uses the client/server communication mode. The client submits a configuration application to the server, and the server returns the

IP address assigned to the client to realize the dynamic configuration of the IP address.

The DHCP server and DHCP forwarding function are mutually exclusive.

Method for settings when the gateway is used as a DHCP server:

Click "Services >> DHCP >> DHCP Server". In the "DHCP Server" bar, check "Enable", select an interface, set the start and end IP addresses, click Add, and then click Apply & Save.

The screenshot shows the "Services >> DHCP" configuration page. The "DHCP Server" tab is selected. A table lists the DHCP server configuration. The first row is highlighted with a red border and contains the following data:

Enable	Interface	Starting Address	Ending Address	Lease(Minutes)
<input checked="" type="checkbox"/>	bridge 1	192.168.2.2	192.168.2.100	1440
<input type="checkbox"/>				1440

Below the table is an "Add[1/10]" button.

Method for settings when the gateway is used as a DHCP client:

Click "Services >> DHCP >> DHCP Client", select the gateway interface, and click Apply & Save.

The screenshot shows the "Services >> DHCP" configuration page. The "DHCP Client" tab is selected. A dropdown menu is open, showing "Bridge 1" selected with a checkmark. Below the dropdown are two buttons: "Apply & Save" and "Cancel".

Method for enabling DHCP forwarding for the gateway:

DHCP forwarding is also referred to as a DHCP relay agent. It can process and forward DHCP information between different subnets and physical network segments.

Click "Services >> DHCP >> DHCP Relay", check "Enable", enter the server address, select the gateway interface, and click Apply & Save.

Services >> DHCP

Enable

DHCP Server 1	10.5.16.98
DHCP Server 2	<input type="text"/>
DHCP Server 3	<input type="text"/>
DHCP Server 4	<input type="text"/>
Relay Interface	bridge 1 ▾
Source IP	<input type="text"/>

5.4.2 DNS

The domain name service (DNS) is a distributed network directory service mainly used for mutual conversion between a domain name and an IP address.

Method for enabling the DNS server for the gateway:

Click "Services >> DNS >> DNS Server", enter the address of the DNS server, and click Apply & Save.

Services >> DNS

Primary DNS

Secondary DNS

Method for enabling DNS forwarding for the gateway:

As a DNS agent, the gateway forwards DNS request and response messages between the DNS client and the DNS server, and replaces the DNS client for domain name resolution.

If the DHCP service is enabled for the gateway, DNS forwarding is enabled by default and cannot be disabled.

Click "Services >> DNS >> DNS Relay", check "Enable DNS Relay", set the mapping between the domain name and the IP address, click Add, and then click Apply & Save. After the settings are completed, when a DNS client on the LAN requests a host domain name in the list, the DNS agent server returns the corresponding IP address to the client.

Services >> DNS

DNS Server **DNS Relay**

Enable DNS Relay

Static [Domain Name <=> IP addresses] Pairing

Host	IP Address 1	IP Address 2
www.sohu.com	10.5.16.98	

Add[0/128]

Apply & Save Cancel

5.4.3 DDNS

The dynamic domain name server (DDNS) maps the dynamic IP address of the gateway to a fixed DNS. Each time a user connects to the Internet, the client program transmits the dynamic IP address of the host to the server program on the server host through information transfer. The server program provides the DDNS service and realizes dynamic domain name resolution. In this way, you can access the Internet by entering the domain name, even if the IP address is changed.

Method for enabling the DDNS service for the gateway:

1. If the Custom service is used, set "Method Name" as required, select "Custom" for "Service Type", and enter the DDNS expression

"http://user name:password@ddns.oray.com/ph/update?hostname=hostname" of the server for "Url". This expression is only for reference. The actual URL is provided by the service provider (usually available on the official website of the service provider). Click Add.

If a common domain name server other than the Custom service is used, set "Method Name" and "Service Type" as required, enter the user name, password, and host name obtained from the server, and click Add.

If "Disable" is selected, the DDNS service is not used.

2. Select the gateway interface, enter the name of the DDNS update method, click Add, and then click Apply & Save to apply the DDNS update method to the gateway interface.

Services >> DDNS

Status DDNS

DDNS Method List

Method Name	Service Type	Url	Username	Password	Hostname	Period minutes
ddns1	Custom	http://mangonew2:abc123@ddns.oray.com/ph/update?hostname=h2340c9004.iask.in				1

Add[1/4]

Specify A Method To Interface

Interface	Method
bridge 1	ddns1
cellular 1	

Add[1/3]

Apply & Save Cancel

3. Wait several minutes after the DDNS settings are applied and saved. Then ping the host name (domain name) of the domain name server to confirm the successful application of the DDNS service.

Services >> DDNS

Status DDNS

Bridge 1

Method	ddns1
Hostname	
IP Address	118.122.120.22
Last Update	2020-01-16 15:27:33, 118.122.120.22
Last Response	2020-01-16 15:27:33, successful update for 118.122.120.22 (h2340c9004.iask.in)

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\achalabhishek>ping h2340c9004.iask.in

Pinging 10.0.0.126 with 32 bytes of data:
Reply from 118.122.120.22: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\achalabhishek>_
```

5.4.4 SMS

The short message service (SMS) is enabled for gateway restart and manual dialup via SMS messages. Some gateways can receive alarm information in the SMS whitelist.

Method for controlling gateway restart and manual dialup via SMS messages

Click "Services >> SMS" and check "Enable". In the "SMS Access Control" bar, set "ID" as required, select "permit" for "Action", enter the phone number, and click Apply & Save. When you activate the dialup port via SMS, after the configuration is completed, you can send the **reboot** command to restart the gateway by using the mobile phone number, or send the **cellular 1 ppp up/down** command to make the gateway redial or interrupt the dialup.

Services >> SMS

Basic

Enable

Mode

Poll Interval s(0: disable)

SMS Access Control

ID	Action	Phone Number
<input type="text" value="1"/>	<input type="text" value="permit"/>	<input type="text" value="18211697833"/>

5.4.5 GPS

Position: You can view the current positioning information.

Services >> GPS

Position	Enable GPS	GPS IP Forwarding	GPS Serial Forwarding
Time			
GPS Time	2020-1-16 15:39:3		
Position			
Latitude	30°35.246500' N		
Longitude	104°3.253280' E		
Speed			
Speed	0.1860 Knots (1knot = 1.852km/h)		

Method for enabling GPS for the gateway:

Click "Services >> Enable GPS", check "Enable", and click Apply & Save. By default, GPS is enabled for the gateway.

Services >> GPS

Position	Enable GPS	GPS IP Forwarding	GPS Serial Forwarding
Enable	<input checked="" type="checkbox"/>		
Debug GPS Model	<input type="checkbox"/>		
<hr/>			
Apply & Save		Cancel	

Method for forwarding GPS data to the server over IP when VG710 is used as a client:

Click "Services >> GPS IP Forwarding", check "Enable", select "Client" for "Type", enter the server address and port in the "Destination IP Address" bar, click Add, and then click Apply & Save.

Services >> GPS

Position	Enable GPS	GPS IP Forwarding	GPS Serial Forwarding
Enable <input checked="" type="checkbox"/>			
Type	Client ▾		
Transmit Protocol	TCP Protocol ▾		
Connection Type	Long-lived ▾		
Keepalive Interval	100	s(60-180)	
Keepalive Retry	10	times(5-10)	
Min Reconnect Interval	15	s(15-180)	
Max Reconnect Interval	180	s(180-3600)	
Source Interface	▾		
Trap Interval	30	s(1-86400)	
Include RMC	<input checked="" type="checkbox"/>		
Include GSA	<input checked="" type="checkbox"/>		
Include GGA	<input checked="" type="checkbox"/>		
Include GSV	<input checked="" type="checkbox"/>		
Message Prefix	<input type="text"/>		
Message Suffix	<input type="text"/>		
Destination IP Address			
Server Address		Server Port	
<input type="text"/>		<input type="text"/>	
		<input type="button" value="Add[0/100]"/>	

Method for forwarding GPS data over IP when VG710 is used as a server:

Click "Services >> GPS IP Forwarding", check "Enable", select "Server" for "Type", and click Apply & Save.

Services >> GPS

Position	Enable GPS	GPS IP Forwarding	GPS Serial Forwarding
Enable	<input checked="" type="checkbox"/>		
Type	Server		
Connection Type	Long-lived		
Keepalive Interval	60	s(60-180)	
Keepalive Retry	5	times(5-10)	
Local Port	10001		
Trap Interval	30	s(1-86400)	
Include RMC	<input checked="" type="checkbox"/>		
Include GSA	<input checked="" type="checkbox"/>		
Include GGA	<input checked="" type="checkbox"/>		
Include GSV	<input checked="" type="checkbox"/>		
Message Prefix			
Message Suffix			
<hr/>			
Apply & Save		Cancel	

Method for forwarding GPS data by VG710 through a serial port:

Click "Services >> GPS Serial Forwarding", check "Enable", and select a serial port type based on the data transmission port used. Ensure that the baud rate, data bits, parity bit, and stop bit are the same as the current settings. Click Apply & Save.

Services >> GPS

Position	Enable GPS	GPS IP Forwarding	GPS Serial Forwarding
Enable	<input checked="" type="checkbox"/>		
Serial Type	RS232	▼	
Baudrate	9600	▼	
Data Bits	8 bits	▼	
Parity	None	▼	
Stop Bit	1 bit	▼	
Software Flow Control	<input type="checkbox"/>		
Include RMC	<input checked="" type="checkbox"/>		
Include GSA	<input checked="" type="checkbox"/>		
Include GGA	<input checked="" type="checkbox"/>		
Include GSV	<input checked="" type="checkbox"/>		
<hr/>			
Apply & Save	Cancel		

5.4.6 QoS

Quality of service (QoS) is a network security mechanism that enables a network to provide better services for designated network communication by using various basic technologies. It is a technology for solving problems such as network delays and blocking.

Method for setting the egress maximum bandwidth for the gateway through QoS control:

Click "QoS >> Traffic Control >> Apply QoS", select the gateway interface, enter the egress maximum bandwidth, click Add, and then click Apply & Save.

Apply QoS

Interface	Ingress Max Bandwidth (Kbps)	Egress Max Bandwidth (Kbps)	Ingress Policy	Egress Policy
cellular 1	1000	1000		
bridge 1				

Method for applying the ingress and egress policies for the gateway through QoS control:

1. Add a network link classifier. Click "QoS >> Traffic Control >> Classifier", check "Any Packets", set the source and destination addresses of the link, select transmit protocols for QoS control, and click Add.
2. Set transmission policies. Click "QoS >> Traffic Control >> Policy", enter a custom policy name for "Name", enter the classifier name for "Classifier", set the guaranteed bandwidth, maximum bandwidth, and policy priority, and click Add.
3. Click "QoS >> Traffic Control >> Apply QoS", select the gateway interface, enter the policy name for "Ingress Policy" and "Egress Policy", click Add, and then click Apply & Save.

Services >> QoS

Traffic Control

Classifier

Name	Any Packets	Source	Destination	Transmit Protocol
1	<input checked="" type="checkbox"/>	any	any	any

icmp igmp tcp udp gre
 esp ah ospf vrrp l2tp

Policy

Name	Classifier	Guaranteed Bandwidth (Kbps)	Max Bandwidth (Kbps)	Priority
p1	1	500	800	medium

Apply QoS

Interface	Ingress Max Bandwidth (Kbps)	Egress Max Bandwidth (Kbps)	Ingress Policy	Egress Policy
cellular 1	1000	1000		p1
bridge 1				

5.4.7 Traffic Control

Method for enabling traffic control for the gateway:

Click "Services >> Traffic Control", enable traffic control, set traffic control parameters, and click Apply & Save. After the settings are completed, the system generates an alarm, stops forwarding, or disables the interface when the traffic exceeds the limit according to the settings on this page.

Services >> Data Usage

Status **Data Usage**

Data Usage

Monitoring	<input checked="" type="checkbox"/>
Daily Limit	<input type="text"/> KB ▾
Start Hour	0 ▾ Hour
When Over Daily Limit	Only Reporting ▾
Monthly Limit	<input type="text"/> MB ▾
Start Day	1 ▾ Days
When Over Monthly Limit	Only Reporting ▾

Tips:
If this function is enabled, the Cellular Connection Mode will be automatically set to Always Online.

5.5 Firewall

5.5.1 ACL

The access control list (ACL) is an access control technology based on packet filtering. It can filter the packets on the interface based on preset conditions and allow them to pass or discard them.

Common scenario: By default, all devices on the LAN (bridge 1) can access the Internet, except the device with the IP address of 192.168.2.100.

Method for setting VG710:

1. Click "Firewall >> ACL >> Add". Enter the ID and sequence number. A smaller sequence number indicates a higher priority. Select "deny" for "Action". Set "Source IP" to "192.168.2.100" and "Source

Wildcard" to "0.0.0.0". Leave "Destination IP" empty, which indicates 0.0.0.0/0, that is, all IP addresses. Click Apply & Save.

Firewall >> ACL

ACL

Type	<input type="text" value="extended"/>
ID	<input type="text" value="101"/>
Sequence Number	<input type="text" value="100"/>
Action	<input type="text" value="deny"/>
Match Conditions	
Protocol	<input type="text" value="ip"/>
Source IP	<input type="text" value="192.168.2.100"/>
Source Wildcard	<input type="text" value="0.0.0.0"/>
Destination IP	<input type="text"/>
Destination Wildcard	<input type="text"/>
Fragments	<input type="checkbox"/>
Log	<input type="checkbox"/>
Description	<input type="text"/>

Apply & Save

Cancel

Back

2. Return to the ACL page, add the rule with the ID of 101 to the management rule of bridge 1, and click Add. Click Apply & Save.

Firewall >> ACL English

ACL

Default Filter Policy

Access Control List

ID	Sequence Number	Action	Protocol	Source	Destination	More Conditions	Description
100	10	permit	ip	any	any		
101	100	deny	ip	192.168.2.100	any		
192	10	permit&log	tcp	any	any; port=443		
192	20	deny	tcp	any	any; port=80		
192	30	deny	tcp	any	any; port=23		
192	40	deny	tcp	any	any; port=22		
192	50	deny	tcp	any	any; port=53		
192	60	deny	udp	any	any; port=53		

Add Modify Delete

Interface List

Interface	In ACL	Out ACL	Admin ACL
bridge 1	none	none	101
cellular 1	none	none	none

5.5.2 NAT

Network address translation (NAT) can be used when some hosts on a private network have been assigned with local IP addresses (that is, private IP addresses used only on the private network), but expect to communicate with hosts on the Internet (without encryption).

Common scenario: A user expects to access a camera on the LAN of the device through the public network to view the current driving conditions of the vehicle. The camera address is 192.168.2.100, and the open port 18000 provides video services.

1. Click "Firewall >> NAT", and select "DNAT" for "Action", and "Outside" for "Source Network". Select "IP PORT to IP PORT" or "INTERFACE PORT to IP PORT" for "Translation Type". The public IP address obtained through dial-up is not fixed, so "INTERFACE PORT to IP PORT" is more convenient. Select "TCP" for "Transmit Protocol" because video services are transmitted over TCP. Select "cellular 1" (dialup interface for the cellular network) for "Interface" and set "Port" to "20000". Set "IP Address" and "Port" under "Translated Address" to "192.168.200" and "18000" respectively. Click Apply & Save.

The gateway redirects the TCP service destined for port 20000 of the cellular 1 interface to the internal IP address 192.168.2.100 and port 18000, to enable access to the internal services.

Firewall >> NAT

NAT

Action	DNAT ▾
Source Network	Outside ▾
Translation Type	INTERFACE PORT to IP PORT ▾
Transmit Protocol	TCP ▾
Match Conditions	
Interface	cellular 1 ▾
Port	20000 - <input type="text"/>
Translated Address	
IP Address	192.168.2.100
Port	18000 - <input type="text"/>
Description	<input type="text"/>
Log	<input type="checkbox"/>

5.5.3 MAC-IP Binding

After MAC-IP binding, the PC can access the public network through the gateway only by using the IP address bound to the MAC address of the PC.

Method for binding the MAC address and IP address of a connected device:

1. Click "Firewall >> ACL" and select "Block" for "Default Filter Policy".

Firewall >> ACL

ACL

Default Filter Policy: Block

Access Control List

ID	Sequence Number	Action	Protocol	Source	Destination	More Conditions	Description
100	10	permit	ip	any	any		
192	10	permit&log	tcp	any	any; port=443		
192	20	deny	tcp	any	any; port=80		
192	30	deny	tcp	any	any; port=23		
192	40	deny	tcp	any	any; port=22		
192	50	deny	tcp	any	any; port=53		
192	60	deny	udp	any	any; port=53		

Interface List

Interface	In ACL	Out ACL	Admin ACL
cellular 1	none	none	192

2. Click "Firewall >> MAC-IP Binding", check "Enable", enter the MAC address and IP address of the connected device, click Add, and click Apply & Save.

Firewall >> MAC-IP Binding

MAC-IP Binding

Enable

MAC-IP Binding List

MAC Address	IP Address	Description
01:03:00:30:00:00	192.168.2.1	
00:00:00:00:00:00		

Add[0/20]

Apply & Save Cancel

5.6 Routing

5.6.1 Static Routing

Set the destination network, subnet mask, and interface or gateway as required.

Routing >> Static Routing

Route Table **Static Routing**

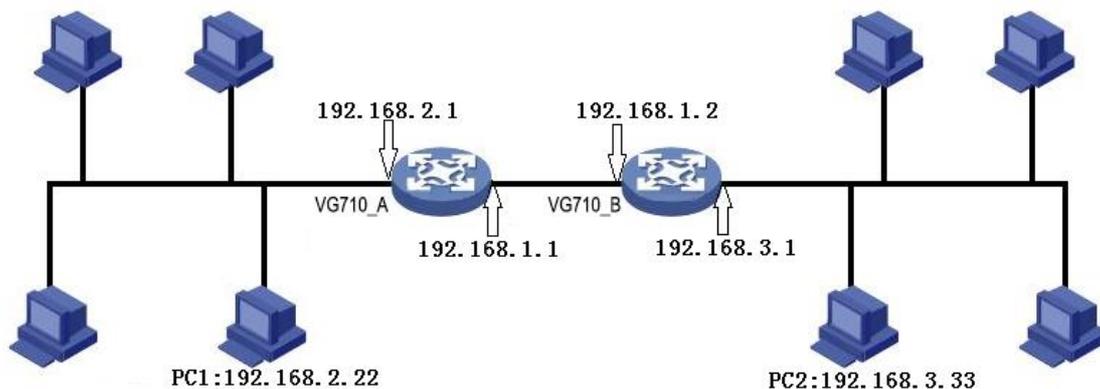
Destination	Netmask	Interface	Gateway	Distance	Track id
0.0.0.0	0.0.0.0	cellular 1		255	
192.168.10.0	255.255.255.0	bridge 1			

Add[1/128]

Apply & Save Cancel

5.6.2 Dynamic Routing

Scenario: Enable dynamic routing between two LANs for mutual communication between them. The topology is shown below.



5.6.2.1 RIP

The Routing Information Protocol (RIP) is a simple internal dynamic routing protocol mainly used on small-scale networks.

Method for enabling dynamic routing between VG710_A and VG710_B over RIP in the scenario:

1. Configure VG710_A. Click "Routing >> Dynamic Routing >> RIP", check "Enable", and configure VG710_A in the "Network" bar to announce the routing entry of VG710_A.

Routing >> Dynamic Routing

Route Table **RIP** OSPF BGP Filtering Route

Enable	<input checked="" type="checkbox"/>
Update Timer	30 s
Timeout Timer	180 s
Garbage Collection Timer	120 s
Version	Default ▾
Show Advanced Options	<input type="checkbox"/>

Network

IP Address	Netmask
192.168.1.0	255.255.255.0
192.168.2.0	255.255.255.0
<input type="text"/>	
<input type="text"/>	
<input type="button" value="Add[0/64]"/>	

2. Configure VG710_B.

Routing >> Dynamic Routing

Route Table

RIP

OSPF

BGP

Filtering Route

Enable

Update Timer s

Timeout Timer s

Garbage Collection Timer s

Version ▾

Show Advanced Options

Network

IP Address	Netmask
192.168.1.0	255.255.255.0
192.168.3.0	255.255.255.0
<input type="text"/>	<input type="text"/>

3. After the configuration is completed, check whether PC 1 can communicate with PC 2. If yes, the dynamic route is added successfully. The RIP route learned by VG710_B is shown in the figure below.

Routing >> Dynamic Routing

Route Table | RIP | OSPF | BGP | Filtering Route

Type: All

Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	10.25.227.169	cellular 1	255/0	
C	10.25.227.168	255.255.255.252		cellular 1	0/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.1.0	255.255.255.0		bridge 1	0/0	
R	192.168.2.0	255.255.255.0	192.168.1.1	bridge 1	120/2	00:00:15
C	192.168.3.0	255.255.255.0		vlan 2	0/0	

5. 6. 2. 2 OSPF

The Open Shortest Path First (OSPF) protocol is a link-status-based internal gateway protocol mainly used on large-scale networks.

Method for enabling dynamic routing between VG710_A and VG710_B over OSPF in the scenario:

1. Configure VG710_A. Click "Routing >> Dynamic Routing >> OSPF", check "Enable", enter a valid IP address for "Router ID", and configure VG710_A in the "Network" bar to announce the routing entry of VG710_A.

Routing >> Dynamic Routing

Route Table | RIP | OSPF | BGP | Filtering Route

Enable

Router ID 192.168.1.1

Route Advanced Options

Interface

Interface	Network	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay
	Broadcast	10	40	5	1

Add[0/100]

Interface Advanced Options

Network

IP Address	Netmask	Area ID
192.168.2.0	255.255.255.0	0
192.168.1.0	255.255.255.0	0

Add[0/64]

2. Set parameters for VG710_B.

Routing >> Dynamic Routing

Route Table | RIP | **OSPF** | BGP | Filtering Route

Enable

Router ID 192.168.1.2

Route Advanced Options

Interface

Interface	Network	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay
	Broadcast	10	40	5	1

Add[0/100]

Interface Advanced Options

Network

IP Address	Netmask	Area ID
192.168.3.0	255.255.255.0	0
192.168.1.0	255.255.255.0	0

Add[0/64]

3. After the configuration is completed, check whether PC 1 can communicate with PC 2. If yes, the dynamic route is added successfully. The OSPF route learned by VG710_B is shown in the figure below.

Routing >> Static Routing

Route Table | **Static Routing**

Type: All

Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	10.25.227.169	cellular 1	255/0	
C	10.25.227.168	255.255.255.252		cellular 1	0/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.1.0	255.255.255.0		bridge 1	0/0	
O	192.168.2.0	255.255.255.0	192.168.1.1	bridge 1	110/20	00:00:12
C	192.168.3.0	255.255.255.0		vlan 2	0/0	

5. 6. 2. 3 BGP

Method for enabling dynamic routing between VG710_A and VG710_B over BGP in the scenario:

1. Configure VG710_A. Click "Routing >> Dynamic Routing >> BGP", check "Enable", and set "AS number" as required.

Routing >> Dynamic Routing

Route Table **RIP** **OSPF** **BGP** **Filtering Route**

Enable

AS number (1-4294967295)

Router ID

Keepalive Time s(0-65535)

Hold Time s(0-65535)

2. In the "Neighbor" bar, click Add, enter the IP address 192.168.1.2 of VG710_B, set "AS number" as required, and click Apply & Save.

Neighbor

IP Address	AS number	EBGP Multihop	Password	Update Time Interval	Keepalive Time	Hold Time	Update Source Interface	Default Originate	Disable Peer	Next Hop Attribute	Distribute List Filter	Prefix List Filter	Descrip
192.168.1.2	100				60	180		FALSE	FALSE	FALSE			

3. Enter a valid IP address for "Router ID", configure VG710_A in the "Network" bar, and click Add, to announce the routing entry of VG710_A. Then click Apply & Save.

Routing >> Dynamic Routing

Route Table **RIP** **OSPF** **BGP** **Filtering Route**

Enable

AS number (1-4294967295)

Router ID

Keepalive Time s(0-65535)

Hold Time s(0-65535)

Show Advanced Options

Network

IP Address	Netmask
192.168.2.0	255.255.255.0

4. Set parameters for VG710_B. The parameters are the same as or corresponding to those of VG710_A.

Routing >> Dynamic Routing English

Route Table | RIP | OSPF | **BGP** | Filtering Route

Enable

AS number (1-4294967295)

Router ID

Keepalive Time s(0-65535)

Hold Time s(0-65535)

Show Advanced Options

Network

IP Address	Netmask
192.168.3.0	255.255.255.0

Add[1/32]

Neighbor

IP Address	AS number	EBGP Multihop	Password	Update Time Interval	Keepalive Time	Hold Time	Update Source Interface	Default Originate	Disable Peer	Next Hop Attribute	Distribute List Filter	Prefix List Filter	Descrip
192.168.1.1	50				60	180		FALSE	FALSE	FALSE			

Add[1/32] | Modify | Delete

5. After the configuration is completed, check whether PC 1 can communicate with PC 2. If yes, the dynamic route is added successfully. The BGP route learned by VG710_B is shown in the figure below.

Routing >> Dynamic Routing

Route Table | RIP | OSPF | **BGP** | Filtering Route

Type:

Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
S	0.0.0.0	0.0.0.0	10.25.227.169	cellular 1	255/0	
C	10.25.227.168	255.255.255.252		cellular 1	0/0	
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.1.0	255.255.255.0		bridge 1	0/0	
B	192.168.2.0	255.255.255.0	192.168.1.1	bridge 1	20/0	00:04:52
C	192.168.3.0	255.255.255.0		vlan 2	0/0	

5.7 Link Backup

5.7.1 SLA

The service level agreement (SLA) is used to detect whether the link between the gateway and the ISP fails.

Method for adding an SLA entry for the gateway:

Click "Link Backup >> SLA >> Add", enter the detected IP address for "Destination Address", set other parameters as required, click Add, and then click Apply & Save.

Timeout (ms) indicates the duration for determining a detection failure. **Consecutive** indicates the number of detection failures resulting in a link failure.

Link Backup >> SLA

Status SLA

SLA Entry

Index	Type	Destination Address	Data size	Interval(s)	Timeout(ms)	Consecutive	Life	Start-time
1	icmp-echo	118.122.120.22	56	30	5000	5	forever	now
2	icmp-echo		56	30	5000	5	forever	now

Add[0/10]

Apply & Save Cancel

5.7.2 Track

Currently, linkage is enabled between the track module and the following application modules: VRRP, static routing, and interface backup. If detection succeeds, the corresponding track entry is in the Positive state. If detection fails, the corresponding track entry is in the Negative state.

Method for adding a track entry for VG710:

Click "Link Backup >> Track >> Track", set "Index" as required, select "sla", "interface", or "vrrp" for "Type", set "SLA/VRRP ID" based on the ID in the SLA list, set "Negative Delay (s)" and "Positive Delay (s)" as required, click Add, and then click Apply & Save.

Negative Delay (s): In case of an abnormal state, switching can be delayed based on the delay setting (0 indicates immediate switching).

Positive Delay (s): When a failure is recovered, switching can be delayed based on the delay setting (0 indicates immediate switching).

Link Backup >> Track

Status **Track**

Track Object

Index	Type	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s)
1	sla	1		0	0
2	sla	1		0	0

Add[0/10]

Track Action

Index	Control Service	Action
	ipsec	positive-start/negative-stop

Add[0/10]

Apply & Save Cancel

Method for adding an IPsec track entry for VG710:

Click "Link Backup >> Track >> Track" and set "Index" as required.

"positive-start/negative-stop" means starting the IPsec service when the track detection state is Positive and stopping the IPsec service when the track detection state is Negative.

Link Backup >> Track

Status **Track**

Track Object

Index	Type	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s)
1	sla	1		0	0
2	sla	1		0	0

Add[0/10]

Track Action

Index	Control Service	Action
1	ipsec	positive-start/negative-stop
	ipsec	positive-start/negative-stop

Add[0/10]

Apply & Save Cancel

5.7.3 VRRP

Scenario: Multiple gateways are connected to a network at the same time. Gateway A acts as the host, and gateway B acts as a backup for gateway A. When gateway A fails, gateway B temporarily replaces gateway A as the host.

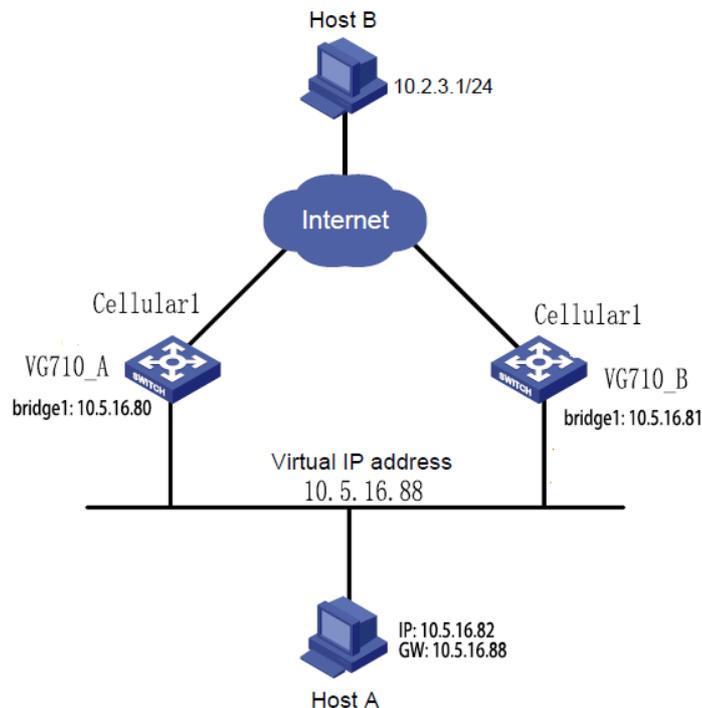
1. Networking requirement

Host A uses the VRRP backup group comprising gateway A and gateway B as its default gateway to access host B on the Internet.

Information of the VRRP backup group:

- The backup group ID is 1.
- The IP address of the virtual gateway of the backup group is 10.5.16.88.
- Gateway A acts as the master gateway.
- Gateway A acts as a backup gateway that can be preempted.

2. Networking diagram



Gateway	Ethernet port	IP address of the port	Priority	Work mode
---------	---------------	------------------------	----------	-----------

	connected to host A	connected to host A		
VG710_A	bridge 1	10.5.16.80	110	Preemption
VG710_B	bridge 1	10.5.16.81	100	Preemption

Method for settings when VG710_A acts as the master gateway and VG710_B as a backup gateway:

1. Configure VG710_A.

Click "Link Backup >> VRRP", set "Virtual Route ID" as required, select the gateway interface of VG710_A, enter the virtual IP address, set the interface priority to 110, and click Add.

Link Backup >> VRRP

Status VRRP

Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
<input checked="" type="checkbox"/>	1	bridge 1	10.5.16.88	110	1	<input checked="" type="checkbox"/>	

Add[0/10]

Apply & Save Cancel

In the navigation tree, click "Link Backup >> VRRP >> Status" and view the VRRP status.

Link Backup >> VRRP

Status VRRP

Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	bridge 1	Master	110	-

2. Configure VG710_B.

Click "Link Backup >> VRRP", set the interface priority to 100, and click Add.

Link Backup >> VRRP

Status **VRRP**

Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
✓	1	bridge 1	10.5.16.88	100	1	✓	
<input checked="" type="checkbox"/>	<input type="text"/>	bridge 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="text"/>

Add[1/10]

Apply & Save **Cancel**

In the navigation tree, click "Link Backup >> VRRP >> Status" and view the VRRP status.

Link Backup >> VRRP

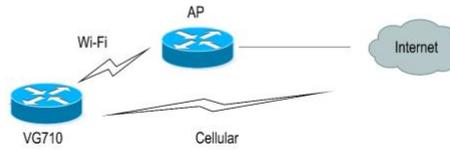
Status **VRRP**

Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	bridge 1	Backup	100	-

Under normal circumstances, VG710_A performs gateway functions. When VG710_A is shut down or fails, VG710_B performs gateway functions. The preemption mode is intended to enable VG710_A to continue to act as the master gateway after it recovers.

5.7.4 Interface Backup

Scenario: VG710 accesses the Internet via Wi-Fi, and an interface backup is created to enable VG710 to access the Internet through dial-up upon Wi-Fi failure. The topology is shown below.



Method for creating an interface backup for the gateway:

1. Enable VG710 to access the Internet via Wi-Fi.

Network >> Wi-Fi

Status
Wi-Fi 2.4G
Wi-Fi 5G

Enable	<input checked="" type="checkbox"/>
Station Role	Client ▾
Default Route	<input checked="" type="checkbox"/>
SNAT	<input checked="" type="checkbox"/>
SSID	<input style="width: 100%;" type="text" value="Inhand"/>
	Scan
Auth Method	WPA2-PSK ▾
Encrypt Mode	CCMP ▾
WPA/WPA2 PSK Key	<input style="width: 100%; text-align: center;" type="password" value="●●●●●●●●●●●●●●●●"/>

Apply & Save
Cancel

2. Click "Link Backup >> SLA >> SLA >> Add" to add an ICMP detection entry. Set the IP address to the host address that can be detected over ICMP on the public or private network, for example, the public IP address 118.122.120.22. Click Apply & Save.

Link Backup >> SLA

Status **SLA**

SLA Entry

Index	Type	Destination Address	Data size	Interval(s)	Timeout(ms)	Consecutive	Life	Start-time
1	icmp-echo	118.122.120.22	56	30	5000	5	forever	now
2	icmp-echo		56	30	5000	5	forever	now

Add[1/10]

Apply & Save Cancel

3. Click "Link Backup >> Track >> Track >> Add" to add a track entry. Select "sla" for "Type" and "dot1lradiol" for "Interface", click Add, and then click Apply & Save.

Link Backup >> Track

Status **Track**

Track Object

Index	Type	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s)
1	sla	1		0	0
2	sla	1		0	0

Add[0/10]

Track Action

Index	Control Service	Action
	ipsec	positive-start/negative-stop

Add[0/10]

Apply & Save Cancel

4. Click "Link Backup >> Interface Backup >> Add", select "dot1lradiol" for "Main Interface" and "cellular1" for "Backup Interface", and click Apply & Save.

Link Backup >> Interface Backup

Status **Interface Backup**

Main Interface	Backup Interface	Startup Delay	Up Delay	Down Delay	Track id
dot11radio 1	cellular 1	60	0	0	1
dot11radio 1	cellular 1	60	0	0	1

Add[0/10]

Apply & Save Cancel

5. Click "Routing >> Static Routing >> Add" and add two routes for network access through the "dot11radio1" and "cellular1" interfaces. A smaller value of "Distance" indicates a higher priority.

Routing >> Static Routing

Route Table **Static Routing**

Destination	Netmask	Interface	Gateway	Distance	Track id
0.0.0.0	0.0.0.0	cellular 1		255	
0.0.0.0	0.0.0.0	dot11radio 1		244	
118.122.120.22	255.255.255.0	dot11radio 1		243	1

Add[2/128]

Apply & Save Cancel

6. Trigger a Wi-Fi failure. According to the preset link detection policy, VG710 accesses the Internet through dial-up via the cellular port, and when Wi-Fi recovers, immediately switches to Wi-Fi for Internet access.

5.8 Wizards

The "Wizards" module incorporates some common communication parameters, simplifying the operations.

5.8.1 New Cellular

After a common network interface card (NIC) is inserted, click "Wizards >> New Cellular >> Apply & Save" and access the status page

to view the network connection status of the device. The device is connected to the network.

Wizards >> New Cellular

New Cellular

Dial-up parameters

Auto ▾

NAT



Apply & Save

Cancel

Network >> Cellular

Status

Cellular

Modem

Active SIM	SIM 1
IMEI Code	353593090129021
IMSI Code	460110923582245
ICCID Code	89860318040283846651
Signal Level	📶(27 asu -59 dBm)
RSRP	-85 dBm
RSRQ	-14 dB
Register Status	registered
Operator	CHN-CT
Network Type	4G
LAC	9B11
Cell ID	9D54211

5.8.2 New IPsec Tunnel

A dedicated virtual tunnel is established between the gateway and other devices or cloud platforms on the network.

Method for establishing an IPsec tunnel for the gateway:

Click "Wizards >> New IPsec Tunnel", set "Map Interface" to an interface ("bridge": bridge interface; "cellular": dialup interface; "dot11radio": Wi-Fi interface) for which you want to establish a tunnel, enter the peer IP address for "Destination Address", and enter the subnet IP addresses and masks at both ends of the tunnel. In Phase 1, enter the IDs at both ends of the tunnel and the connection key, and click Apply & Save.

Wizards >> New IPsec Tunnel

New IPsec Tunnel

Basic Parameters

Tunnel ID	1 ▾
Map Interface	cellular 1 ▾
Destination Address	118.122.120.22
Negotiation Mode	Main Mode ▾
Local Subnet	192.168.2.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.3.0
Remote Netmask	255.255.255.0

Phase 1 Parameters

IKE Policy	3DES-MD5-DH2 ▾
IKE Lifetime	86400 s
Local ID Type	IP Address ▾
Local ID	
Remote ID Type	IP Address ▾
Remote ID	
Authentication Type	Shared Key ▾
Key	●●●●●●

Phase 2 Parameters

IPSec Policy	3DES-MD5-96 ▾
IPSec Lifetime	3600 s

5.8.3 IPsec Experts' Configuration

This function is available only for specific users. To activate this function, contact the technical support personnel.

5.8.4 New L2TPv2 Tunnel

Method for creating an L2TPv2 tunnel for the gateway:

Set the parameters of the L2TP server and the local/remote addresses.
Click Apply & Save.

Wizards >> New L2TPv2 Tunnel

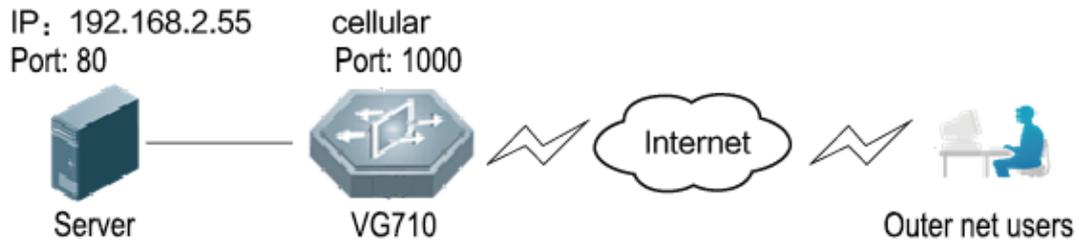
New L2TPv2 Tunnel

ID	<input type="text" value="1"/>
L2TP Server	<input type="text" value="118.122.120.22"/>
Source Interface	<input type="text" value="cellular 1"/>
Username	<input type="text" value="test"/>
Password	<input type="password" value="•••••"/>
Authentication Type	<input type="text" value="Auto"/>
Hostname	<input type="text"/>
Enable Challenge Secret	<input type="checkbox"/>
Local IP Address	<input type="text"/>
Remote IP Address	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Netmask	<input type="text" value="255.255.255.0"/>
Link Detection Interval	<input type="text" value="60"/> s
Max Retries for Link Detection	<input type="text" value="5"/>
NAT	<input type="checkbox"/>
MTU	<input type="text" value="1500"/>
MRU	<input type="text" value="1500"/>

5.8.5 New Port Mapping

Port mapping is to map a port of a host on the intranet to a port of a host on the extranet to provide corresponding services. When a user accesses the port on the extranet, the server automatically maps the request to the internal machine on the corresponding LAN.

Scenario: Users on the extranet cannot directly access a web server on the intranet. In this case, a port mapping can be created on the gateway so that the gateway automatically transfers the data to port 80 of the web server on the intranet when a user on the extranet accesses port 1000 via the cellular interface of the gateway.



Method for creating a port mapping for the gateway:

Click Wizards >> New Port Mapping". Enter the gateway interface for "Outside Interface", gateway port for "Service Port", IP address of the internal host for "Internal Address", and port ID of the internal host for "Internal Port". Click Apply & Save.

Wizards >> New Port Mapping

New Port Mapping

Transmit Protocol	TCP ▾
Outside Interface	cellular 1 ▾
Service Port	1000
Internal Address	192.168.2.55
Internal Port	80
Description	

Apply & Save Cancel

6 APP Management

App function is an important part of the gateway to realize edge computing. The prerequisite for using this feature is to install the python SDK.

6.1 APP

Step 1: click "APP>>APP management • > > Open Python app management", click apply and save.

Export and import the compiled app installation package. After importing the app installation package, the system will automatically decompress and install it.

The screenshot shows the inhand APP Management interface. The left sidebar contains navigation options: Administration, Network, Services, Link Backup, Routing, Firewall, VPN, APP, Industrial, Tools, and Wizards. The main content area is titled 'APP >> APP' and has a 'Status' tab set to 'APP Management'. Under 'APP Management', there are three checkboxes: 'Enable APP Manager' (checked), 'Enable IDE Debug' (unchecked), and 'Enable Extended Flash' (unchecked). Below this is the 'Import APP Package' section with a file selection area and 'Browse...' and 'Upload' buttons. The 'APP Configuration' section contains a table with the following data:

Enable	ID	APP Name	APP Version	SDK Version	Logfile Size(MB)	Operation Method			
<input type="checkbox"/>	1	flexapi_mqtt_demo	1.0.1_H	2.3.15	1	Import Config	Export Config	Export App	Uninstall
<input type="checkbox"/>	2	WiFiControl	1.1.0	0.2.0	1	Import Config	Export Config	Export App	Uninstall
<input type="checkbox"/>	3	HelloWorld	1.0.0	0.2.0	1	Import Config	Export Config	Export App	Uninstall
<input type="checkbox"/>	4	ble_adv	1.0.4	2.3.13	1	Import Config	Export Config	Export App	Uninstall
<input type="checkbox"/>	5	AWS_pubsub_demo	1.0.0	2.3.12	1	Import Config	Export Config	Export App	Uninstall

Below the table is the 'APP Management' section with 'Start All', 'Stop All', and 'Restart All' buttons. At the bottom, there is a table header 'ID APP Name Operation Method' and two buttons: 'Apply & Save' and 'Cancel'.

Step 2: click running status. If the app management running status is running, the operation is successful

APP >> APP

APP Management

APP Manager Status: Running

Python Version: Python3

SDK Version: 2.3.15

Debug Server Status: Stopped

APP Filesystem Use%: 11% of 6537 MB

Data/Log Filesystem Use%: 11% of 6537 MB

Extended Memory Card: Unrecognized

APP Running Status

ID	APP Name	APP Version	SDK Version	State	Uptime	Action
1	flexapi_mqtt_demo	1.0.1_H	2.3.15	running	pid 12981, uptime 0:00:13	<input type="button" value="Clear Log"/> <input type="button" value="Show Log"/> <input type="button" value="Download Log"/>

6.2 Docker

The docker SDK is installed before using the docker function .

Step 1: click "app>>docker>> enable", enter the user name, password and port number in the input box, click apply and save

APP >> Docker

Docker Management

Enable:

Version: 18.06.2-ce

Username:

Password:

Port:

Download Log:

[Go to the docker management page](#)

[Save Configuration](#)

6.3 Third party cloud platform

The gateway device connects to the cloud platform as a client to realize communication, and obtains data in real time according to the corresponding configuration of the gateway device to achieve the purpose of data interaction.

6.3.1 MQTT protocol connection to cloud platform

Step 1: click "APP>> third party cloud platform > >mqtt>> enable", select the address and port of the cloud platform server, click apply and save.

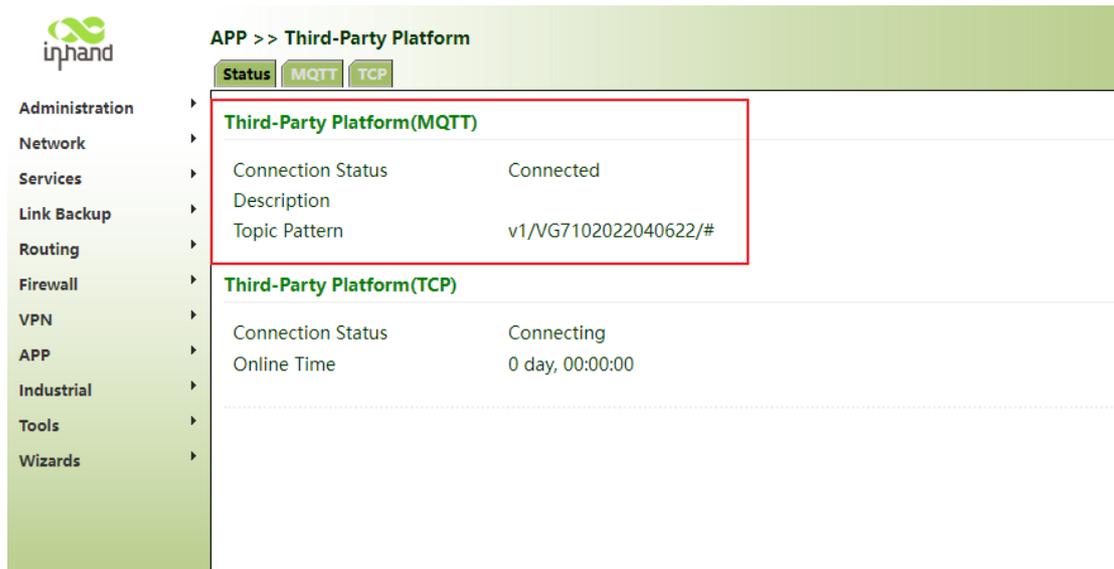
Which fields are sent to the platform by default, and the FlexAPI config can be modified

The screenshot shows the inhand web interface for configuring the MQTT protocol connection to a third-party cloud platform. The left sidebar contains a navigation menu with categories: Administration, Network, Services, Link Backup, Routing, Firewall, VPN, APP (highlighted), Industrial, Tools, and Wizards. The main content area is titled "APP >> Third-Party Platform" and has three tabs: Status, MQTT (selected), and TCP. The configuration form includes the following fields and options:

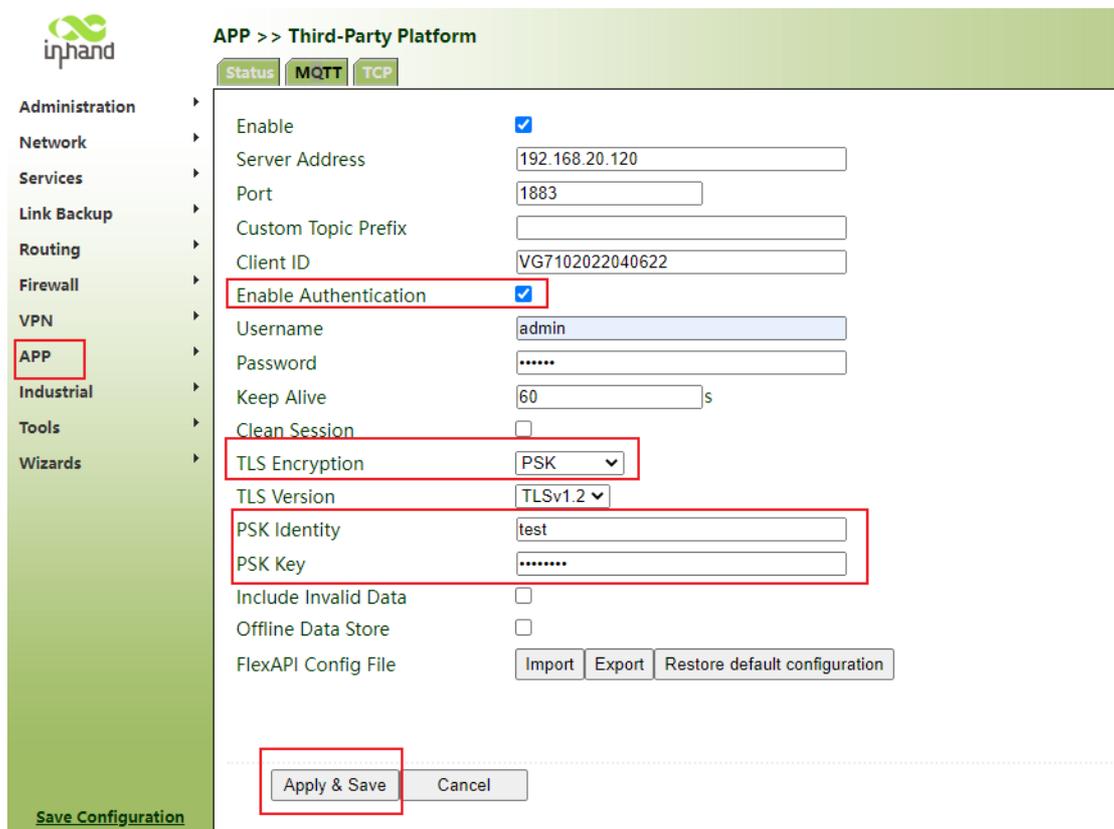
- Enable:
- Server Address:
- Port:
- Custom Topic Prefix:
- Client ID:
- Enable Authentication:
- Keep Alive: s
- Clean Session:
- TLS Encryption:
- Include Invalid Data:
- Offline Data Store:
- FlexAPI Config File:

At the bottom of the form, there are two buttons: "Apply & Save" (highlighted with a red box) and "Cancel".

Step 2: click status. If the connection status is connected, the connection is successful.

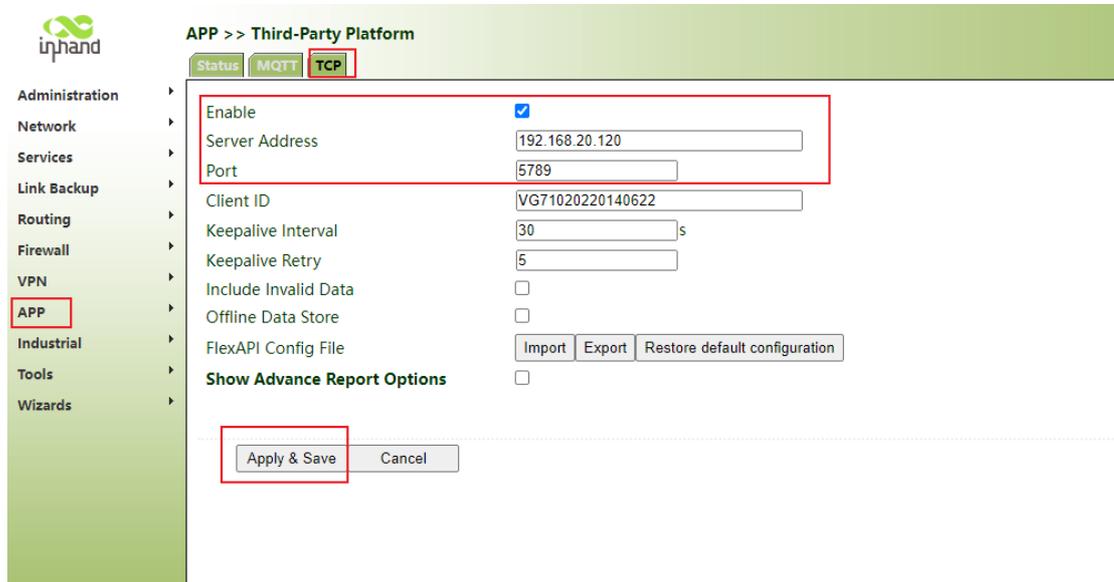


Note: if the server needs authentication and encryption, it needs to be enabled correspondingly. Click "app>> third party cloud platform > >mqtt>> enable", select the address and port of the cloud platform server, and enable mqtt authentication and TLS encryption.

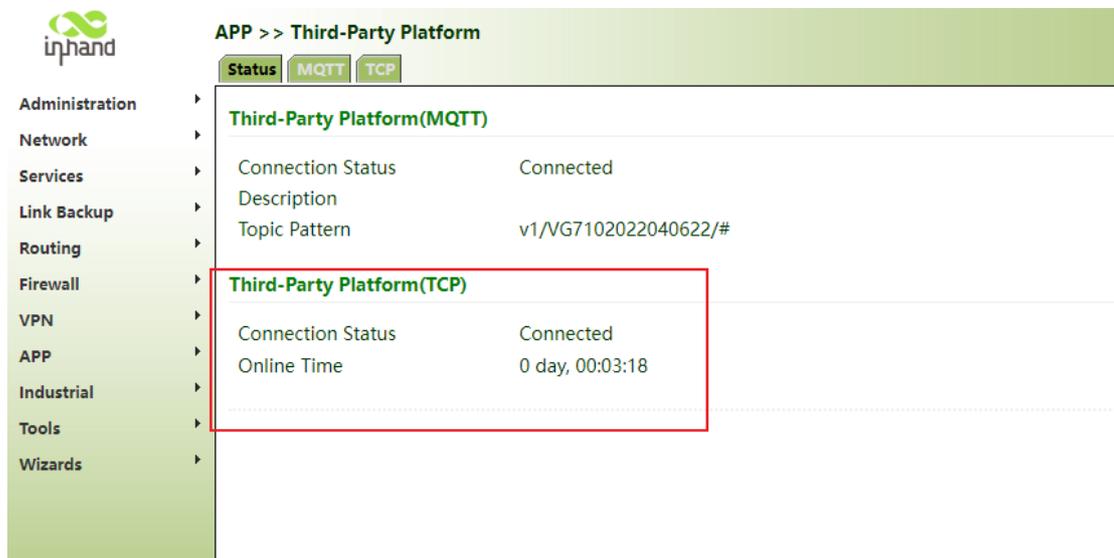


6.3.2 TCP protocol connection to cloud platform

Step 1: click "app>> third party cloud platform > >tcp>> enable", select the address and port of the cloud platform server, click apply and save



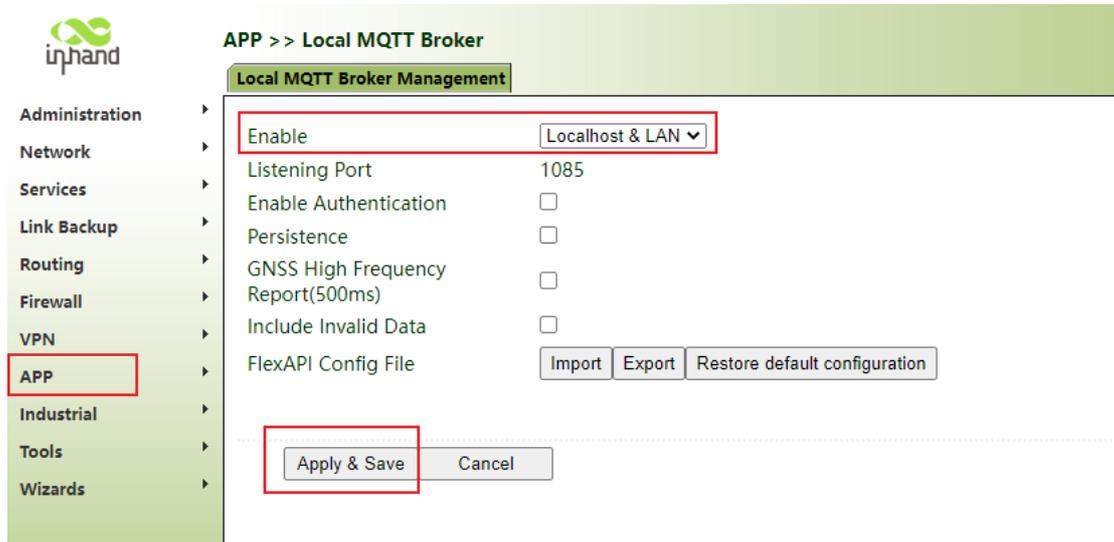
Step 2: click status. If the connection status is connected, the connection is successful.



6.4 Local MQTT Agent

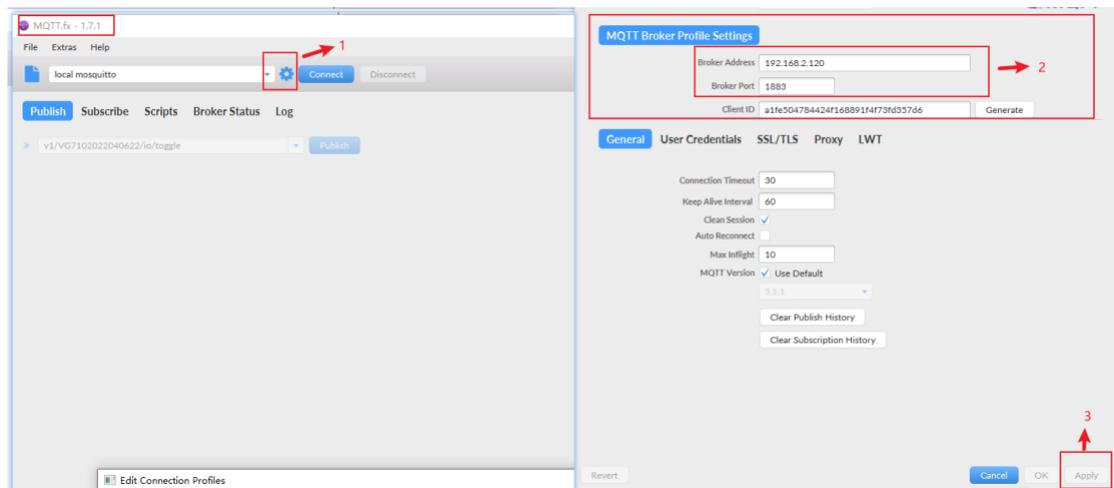
The gateway device acts as an mqtt server to proxy messages. When users need messages, they use the mqtt client to subscribe to information. Python App or Docker program use gateway info, Subscribe to messages from the local mqtt agent.

Step 1: click "app>> local mqtt agent >> enable local / local & Lan", click apply and save

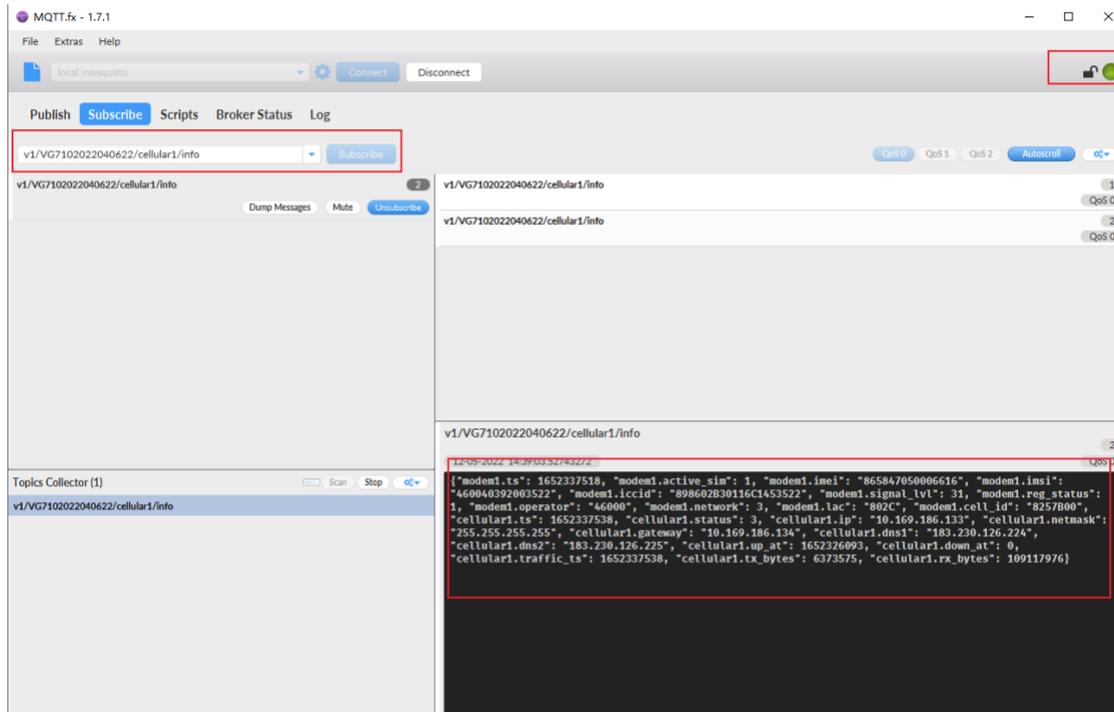


Step 2: use mqtt client information: server address, port, authentication and other information

This document uses mqtt Take FX test tool as an example.



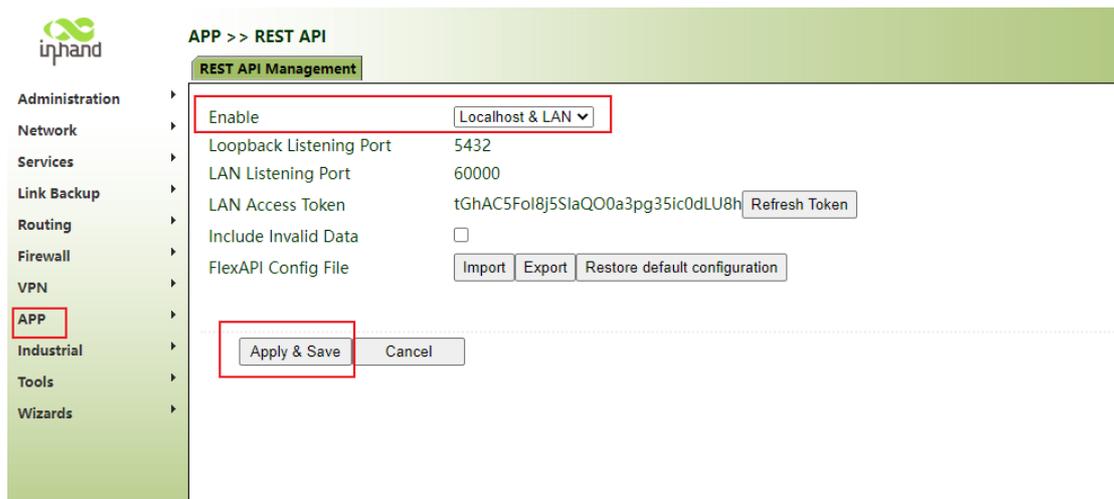
Step 3: click Connect. If the icon turns green, it means the connection is successful. Then subscribe to the information according to the topic document. The gateway will return data in JSON format. For example, subscribe to cellular information



6.5 REST API

In addition to using mqtt and TCP to obtain data, users can also use rest APIs to call data according to interface documents

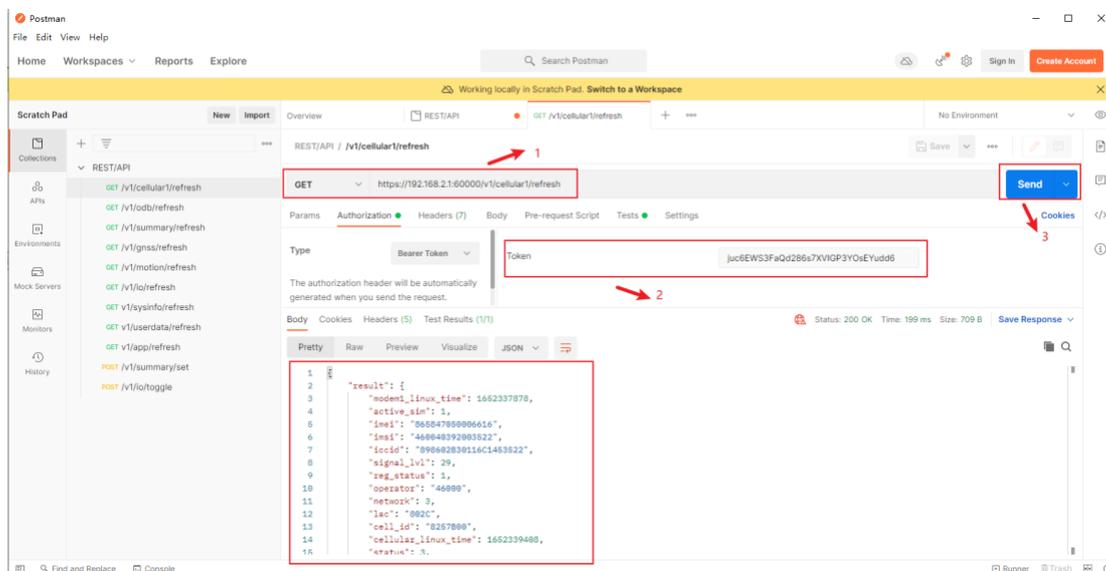
Step 1: click "app>>rest api>> enable", select the address and port of the cloud platform server, click apply and save



Step 2: use tools such as postman according to the interface document to call the interface to obtain data.

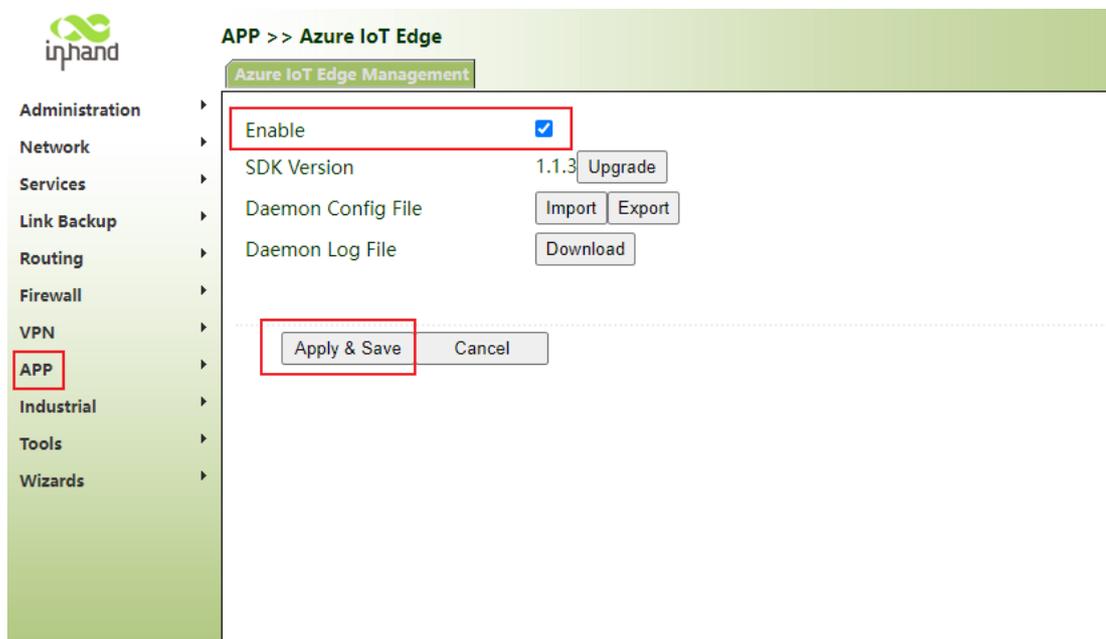
1. Fill in the URL, token, etc. in the interface document, and note whether it is a get or post request;

2. Click send;
3. Finally, the gateway device will return the corresponding data results in JSON format;



6.6 Azure IoT Edge

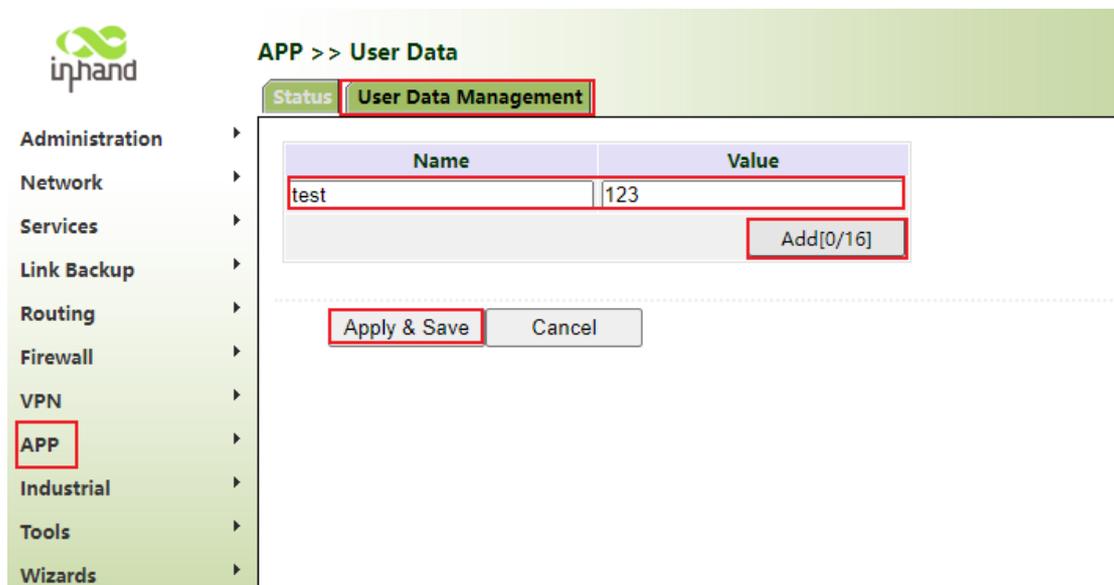
Click "APP>>Azure IOT edge>> enable", click apply and save



Note: this function item depends on docker. The docker function should be opened before opening

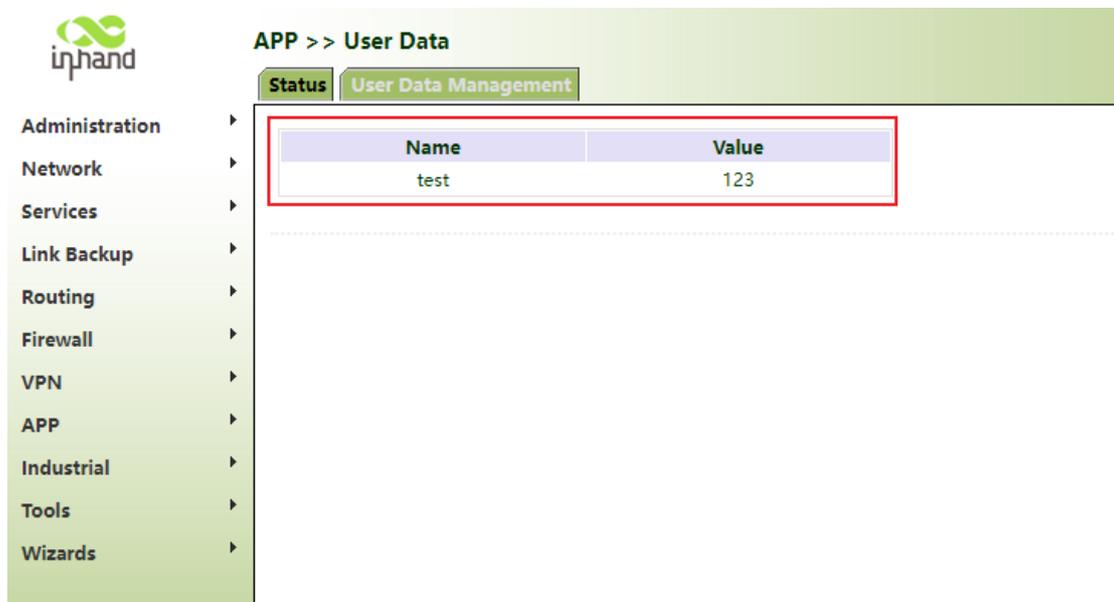
6.7 User Data

Step 1: click "APP>> User Data>> User Data Management", then enter the name and corresponding value, click add, and finally click apply and save.



The screenshot shows the inhand web interface. On the left is a navigation sidebar with categories: Administration, Network, Services, Link Backup, Routing, Firewall, VPN, APP (highlighted with a red box), Industrial, Tools, and Wizards. The main content area is titled "APP >> User Data" and has a "Status" tab and a "User Data Management" sub-tab. Below the tabs is a table with two columns: "Name" and "Value". The "Name" column contains the text "test" and the "Value" column contains the number "123". To the right of the table is a button labeled "Add[0/16]". Below the table are two buttons: "Apply & Save" (highlighted with a red box) and "Cancel".

Step 2: click "status". If the data exists in the status bar, it means that the addition is successful.



The screenshot shows the inhand web interface. On the left is a navigation sidebar with categories: Administration, Network, Services, Link Backup, Routing, Firewall, VPN, APP, Industrial, Tools, and Wizards. The main content area is titled "APP >> User Data" and has a "Status" tab (highlighted with a red box) and a "User Data Management" sub-tab. Below the tabs is a table with two columns: "Name" and "Value". The "Name" column contains the text "test" and the "Value" column contains the number "123".

7. Connecting the Gateway to a Cloud Platform

1. Click "Administration >> Device Manager >> Device Manager", check "Device Manager Enable", select the server address of the cloud platform, enter the registered account and license plate number of the cloud platform, and click Apply & Save.

Administration >> Device Manager

Status **Device Manager**

Device Manager Enable	<input checked="" type="checkbox"/>
Service Type	InVehicle Service ▾
Server Address	che.inhandiot.com ▾
Secure Channel	<input checked="" type="checkbox"/>
Registered Account	test@inhand.com.cn Sign up/Sign in
License Plate Number	川A11111
Asset Number	
Show Advanced Options	<input type="checkbox"/>

2. Click "Status". "Connected" indicates that the gateway is successfully connected to the cloud platform.

8 Industrial Ports (Serial Ports)

The industrial ports of VG710 include RS232 serial ports, RS485 serial ports, and IO ports.

8.1 DTU

RS232 provides full-serial communication, enabling hardware-based traffic control.

RS485 provides half-duplex communication, enabling remote transmission of serial communication data.

Method for setting web pages when the gateway is used as a DTU:

1. Enable DTU 1 (RS232) or DTU 2 (RS-485).
2. Set the connection parameters of the gateway interface and industrial device. Communication is available only when the parameters at both ends of the network link are consistent.

Industrial >> DTU

Serial Port

DTU 1

DTU 2

Serial Port 1

Serial Type	RS232 ▾
Baudrate	9600 ▾
Data Bits	8 bits ▾
Parity	None ▾
Stop Bit	1 bit ▾
Software Flow Control	<input type="checkbox"/>
Hardware Flow Control	<input type="checkbox"/>
Description	<input type="text"/>

Serial Port 2

Serial Type	RS485 ▾
Baudrate	9600 ▾
Data Bits	8 bits ▾
Parity	None ▾
Stop Bit	1 bit ▾
Software Flow Control	<input type="checkbox"/>
Description	<input type="text"/>

Apply & Save

Cancel

- Set the IP address and transmit protocol (TCP or UDP) of the server.

Industrial >> DTU

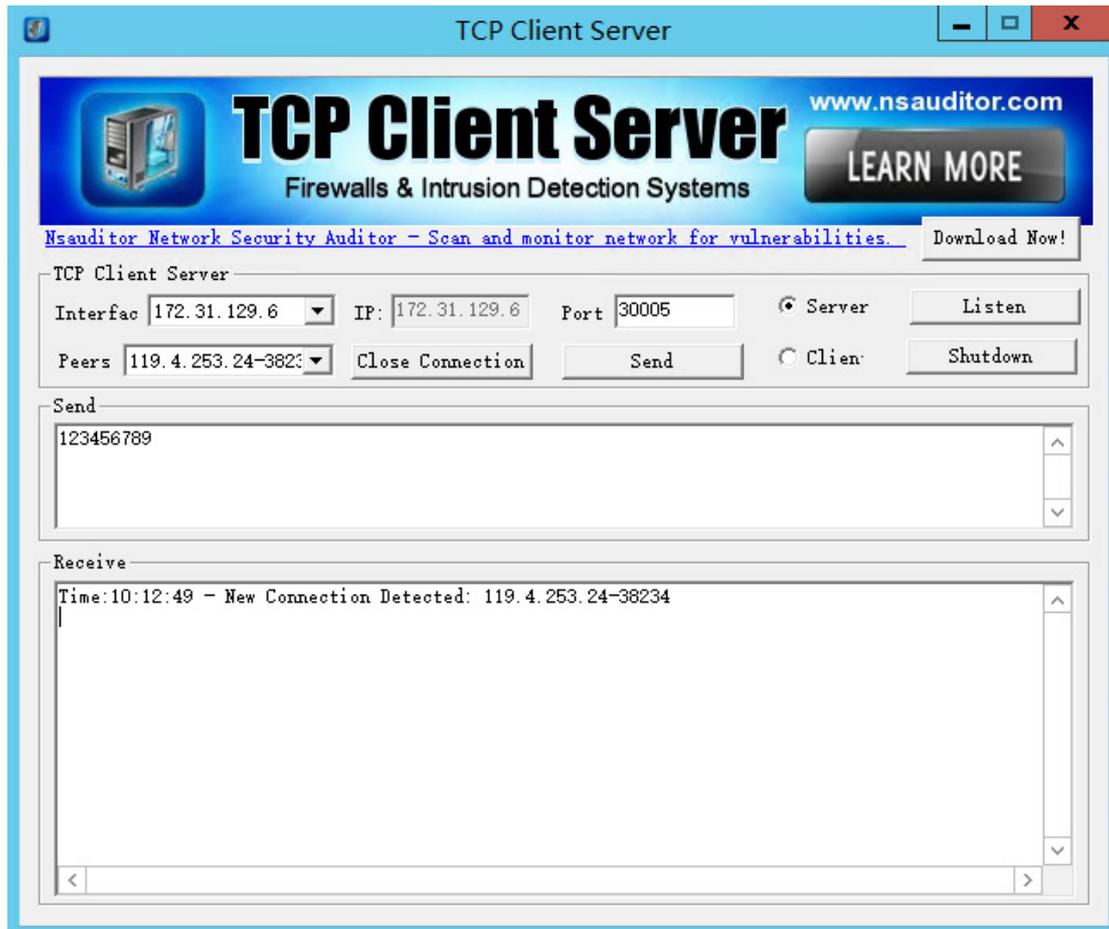
Serial Port DTU 1 DTU 2

Enable	<input checked="" type="checkbox"/>
DTU Protocol	Transparent
Transmit Protocol	TCP Protocol
Connection Type	Long-lived
Keepalive Interval	60 s
Keepalive Retry	5
Serial Buffer Frame	4
Packet Size	1024 Bytes
Force Transmit Timer	100 ms
Min Reconnect Interval	15 s
Max Reconnect Interval	15 s
Multi-server policy	parallel
Source Interface	IP
Local IP Address	
DTU ID	
Enable Debug	<input type="checkbox"/>
Enable Report ID	<input type="checkbox"/>

Destination IP Address

Server Address	Server Port

4. Check that the gateway-connected PC and the server exchange data through DTU.



8.2 IO Ports

IO ports provide six analog inputs, six digital inputs, and four digital outputs. The analog and digital inputs share the ports. The digital parameters correspond to two states: HIGH (1) and LOW (0).

Dry Connect: determines the I/O interface status based on whether the input is on or off.

Wet Connect: determines the I/O interface status based on the input voltage.

No.	Function	
-----	----------	--

1	DI	<p>When the digital input mode is wet contact, the voltage of +2.7 V to +36 V maps to state 1.</p> <p>When the digital input mode is wet contact, the voltage of +0 V to +1 V maps to state 0.</p>
2	AI	<p>The analog input status is determined based on the current or voltage obtained from the analog input interface. Voltage range: +0.5 V ~ +36 V</p> <p>Analog input current detection is not support</p>
3	DO	<p>Default: Low state, not pull-up</p> <p>Set Low pull-up or not pull-up, no voltage</p> <p>Set Hight state and pull-up, output power supply voltage</p> <p>Set Hight state and not pull-up, high resistance state</p>



Industrial >> IO

Status

Administration ▶

Network ▶

Services ▶

Link Backup ▶

Routing ▶

Firewall ▶

VPN ▶

APP ▶

Industrial ▶

Tools ▶

Wizards ▶

Digital Input

Digital Input 1	LOW (0)
Digital Input 2	LOW (0)
Digital Input 3	LOW (0)
Digital Input 4	LOW (0)
Digital Input 5	LOW (0)
Digital Input 6	LOW (0)

Analog Input

Analog Input 1	0.000 V
Analog Input 2	0.000 V
Analog Input 3	0.002 V
Analog Input 4	0.007 V
Analog Input 5	0.000 V
Analog Input 6	0.000 V
Power Input	11.800 V

Digital Output

Digital Output 1	LOW (0)
Digital Output 2	LOW (0)
Digital Output 3	LOW (0)
Digital Output 4	LOW (0)

DO: the power supply voltage limit is the maximum voltage; the maximum input voltage is DC 36V; Typical input current can reach 300mA.

DO: When do is used as open drain output, the typical perfusion current can reach 300mA.

When do pull-up is used as output, it can output high-level signal. The open circuit test voltage is the same as the power supply voltage. The pull-up resistance is 20K Ω and has no load capacity.

9 System Management

9.1 System

Click "Administration >> System >> Status" and view the current system and network status of the device.

Administration >> System

Status Basic Setup

System Status

Name	VG710
Model	VG710
Serial Number	VF7101937000006
MAC Address	0018.0510.302f
Firmware Version	1.0.0.r11989
Bootloader Version	2012.07.r238
Device Time	2020-01-16 17:01:34
PC Time	2020-01-16 17:01:36 Sync Time
Up time	0 day, 02:01:19
CPU Load (1 / 5 / 15 mins)	0.28 / 0.51 / 0.69
Memory consumption Total/Free	483.67MB / 202.72MB (41.91%)

Network Status

Cellular 1 [Settings]

Status	Connected
Signal Level	📶(27 asu -59 dBm)
Register Status	registered
IP Address	10.175.168.221

Click "Basic Setup" and modify the system language and device name.

Administration >> System

Status	Basic Setup
Language	English ▼
Device Name	VG710
<hr/>	
<input type="button" value="Apply & Save"/> <input type="button" value="Cancel"/>	

9.2 System Time

To ensure the coordination between the device and other devices, set the system time accurately.

Manual time synchronization: Click "Administration >> System Time >> System Time >> Sync Time" to ensure consistency between the gateway time and host time.

Administration >> System Time		
System Time	SNTP Client	NTP Server
Device Time	2020-01-16 17:02:48	
PC Time	2020-01-16 17:02:50	
	<input type="button" value="Sync Time"/>	
Year/Month/Date	2020 ▼ / 01 ▼ / 16 ▼	
Hour:Min:Sec	17 ▼ : 02 ▼ : 38 ▼	
	<input type="button" value="Apply"/>	
Timezone	UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan, Russia ▼	
	<input type="button" value="Apply & Save"/>	

Alternatively, click "Administration >> System >> Status" to synchronize the time.

Administration >> System

Status

Basic Setup

System Status

Name	VG710
Model	VG710
Serial Number	VF7101937000006
MAC Address	0018.0510.302f
Firmware Version	1.0.0.r11989
Bootloader Version	2012.07.r238
Device Time	2020-01-16 17:03:09
PC Time	2020-01-16 17:03:11 <input type="button" value="Sync Time"/>
Up time	0 day, 02:02:54
CPU Load (1 / 5 / 15 mins)	1.07 / 0.69 / 0.73
Memory consumption Total/Free	483.67MB / 202.64MB (41.90%)

Automatic time synchronization: Click "Administration >> System Time >> SNTP Client or NTP Server" and check "Enable" to synchronize the time between the gateway and the SNTP or NTP server. After NTP is enabled, the gateway can synchronize time for all devices on the network.

Administration >> System Time

System Time

SNTP Client

NTP Server

Enable

Update Interval s(60-2592000)

Source Interface

Source IP

SNTP Servers List

Server Address	Port
0.pool.ntp.org	123
1.pool.ntp.org	123
2.pool.ntp.org	123
3.pool.ntp.org	123
<input type="text"/>	<input type="text" value="123"/>
<input type="button" value="Add[4/10]"/>	

9.3 Management Services

When the gateway requires the HTTP, HTTPS, TELNET, and SSH functions, click "Administration >> Management Services", enable the services, and click Apply & Save.

Administration >> Management Services

Management Services

HTTP

Enable	<input checked="" type="checkbox"/>
Listen IP address	<input type="text" value="any"/>
Port	<input type="text" value="80"/>
Remote Access	<input type="checkbox"/>

HTTPS

Enable	<input checked="" type="checkbox"/>
Listen IP address	<input type="text" value="any"/>
Port	<input type="text" value="443"/>
Remote Access	<input checked="" type="checkbox"/>

Source Range	IP Wildcard
<input type="text"/>	<input type="text"/>
<input type="button" value="Add[0/5]"/>	

TELNET

Enable	<input type="checkbox"/>
Listen IP address	<input type="text" value="any"/>
Port	<input type="text" value="23"/>

PORT	23
Remote Access	<input type="checkbox"/>
SSH	
Enable	<input type="checkbox"/>
Listen IP address	any
Port	22
Timeout	120 s(0-120)
Key Mode	RSA
Key Length	1024
Remote Access	<input type="checkbox"/>

9.4 User Management

Click "Administration >> User Management" and create users, modify passwords, or delete users on the user management page.

Superuser and common user:

- Superuser: By default, only one superuser is automatically created by the system, with the user name of **adm** and the default password of **123456**. It has full access rights for the gateway.
- Common user: A common user is created by the superuser. It can view or modify gateway configurations.



说明

Note: You cannot delete the superuser (**adm**) or modify its user name, but can modify its password.

9.5 AAA

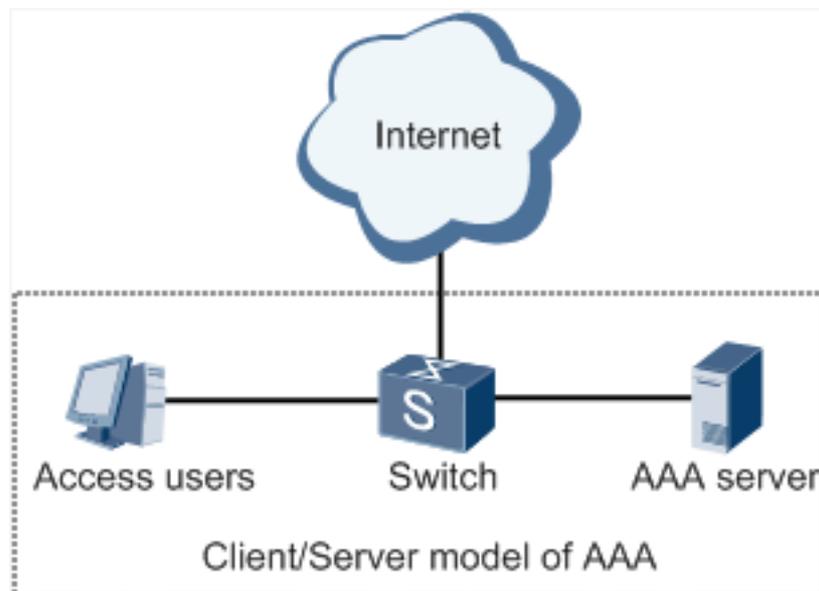
Authentication, authorization, and accounting (AAA) is a security management mechanism for access control in network security, which provides three security services: authentication, authorization, and accounting.

It provides modular methods for the following services:

- Authentication: Verify whether a user has the right for network access.
- Authorization: Authorize a user to use specific services.
- Accounting: Record network resource usage of a user.

You can use only one or two of the security services provided by AAA. For example, if a company only expects to authenticate employees when they access specific resources, the network administrator only needs to configure the authentication server. However, if the company expects to record the network usage of employees, the accounting server must be configured.

AAA usually works in the client/server structure, which is highly scalable and is convenient for centralized management of user information, as shown in the figure below.





说明

Note: **Radius**, **Tacacs+**, and **LDAP** indicate authentication and authorization servers. **Local** indicates the local user name and password of the gateway.

9.5.1 Radius

The Remote Authentication Dial In User Service (Radius) is a distributed information exchange protocol based on the client/server structure. It protects the network from unauthorized access, and is usually used in various network environments that require high security and allow remote user access.

Method for enabling the Radius server for the gateway:

Click "Administration >> AAA >> Radius". In "Server List", enter the server address (domain name/IP address), port ID, and authentication key, click Add, and then click Apply & Save.

Administration >> AAA

Radius **Tacacs+** **LDAP** **AAA Settings**

Server List

Server	Port	Key	Source Interface
<input type="text"/>	1812	<input type="text"/>	<input type="text"/>

9.5.2 Tacacs+

The Terminal Access Controller Access Control System + (Tacacs+) protocol is similar to the Radius protocol. It uses the client/server mode for communication between the network access server (NAS) and the Tacacs+ server. However, Tacacs+ works based on TCP, and Radius works based on UDP.

The Tacacs+ protocol is mainly used for AAA of end users and Point-to-Point Protocol (PPP) and virtual private dial-up network (VPDN) access users. Its typical application is to authenticate, authorize, and perform accounting for an end user who needs to log in to the device for operations. As a Tacacs+ client, the device sends the user name and password to the Tacacs+ server for verification. After authentication and authorization, the user can log in to the device for operations.

Method for enabling the Tacacs+ server for the gateway:

Click "Administration >> AAA >> Tacacs+". In "Server List", enter the server address (domain name/IP address), port ID, and authentication key, click Add, and then click Apply & Save.

Administration >> AAA

Radius Tacacs+ LDAP AAA Settings

Server List

Server	Port	Key
<input type="text"/>	49	<input type="text"/>

Add[0/10]

Apply & Save Cancel

9.5.3 LDAP

The main advantage of the Lightweight Directory Access Protocol (LDAP) lies in its quick response to users' search operations. For example, massive user authentication operations may be performed concurrently. If a database is used, because the database is divided into various tables, to meet this simple authentication requirement, the database must be searched each time, along with synthesis and filtering. This results in low efficiency. LDAP is equivalent to one table, and requires only the user name and password, with some other parameters, which is quite simple. It can meet the authentication requirement regarding the efficiency and structure.

Method for enabling the LDAP server for the gateway:

Click "Administration >> AAA >> LDAP". In "Server List", enter any name for "Name", enter the server address (domain name/IP address) and port ID, and enter the base DN obtained from the server. Set the user name and password for accessing the server. Select "None", "SSL", or "StartTLS" for "Security". Click Add, and then click Apply & Save.

Administration >> AAA

Radius Tacacs+ **LDAP** AAA Settings

Server List

Name	Server	Port	Base DN	Username	Password	Security	Verify Peer
						None ▾	<input type="checkbox"/>

Add[0/10]

Apply & Save Cancel

9.5.4 AAA Authentication

AAA authentication methods:

- No authentication (**none**): No validity check is performed. Generally, this method is not used.
- Local authentication (**local**): User information is configured on the NAS. Local authentication is fast, which can reduce the operational costs, but the information storage amount is limited by hardware.
- Remote authentication: User information is configured on the authentication server. Remote authentication is supported over Radius, Tacacs+, and LDAP.

AAA authorization methods:

- No authorization (**none**): No authorization is performed for users.
- Local authorization (**local**): Authorization is performed based on the properties configured by the NAS for the local account.
- Tacacs+ authorization: Users are authorized by the Tacacs+ server.
- Authorization after successful Radius authentication: Authorization is bound to authentication, and cannot be performed independently over Radius.
- LDAP authorization

Method for enabling authentication and authorization for the gateway:

Click "Administration >> AAA >> AAA Settings". 1, 2, and 3 are corresponding to Radius, Tacacs, and LDAP respectively. Authentication entries 1, 2, and 3 must be corresponding to authorization entries 1, 2, and 3 respectively. When all of radius, tacacs+, and local are set, the priority sequence is as follows: 1 > 2 > 3.

Administration >> AAA

Radius Tacacs+ LDAP **AAA Settings**

Service	Authentication			Authorization		
	1	2	3	1	2	3
telnet	none	none	none	none	none	none
ssh	none	none	none	none	none	none
web	none	none	none	none	none	none

Apply & Save Cancel

9.6 Configuration Management

Method for importing configurations: Click "Administration >> Config Management >> Config Management >> Browse", select a configuration file, and click Import to import the configuration file to the gateway.

Method for backing up current running configurations to the PC (common): Click Backup running-config.

Method for backing up the startup file to the PC: Click Backup startup-config.

Method for restoring default configurations: Click Restore default configuration and then click OK.



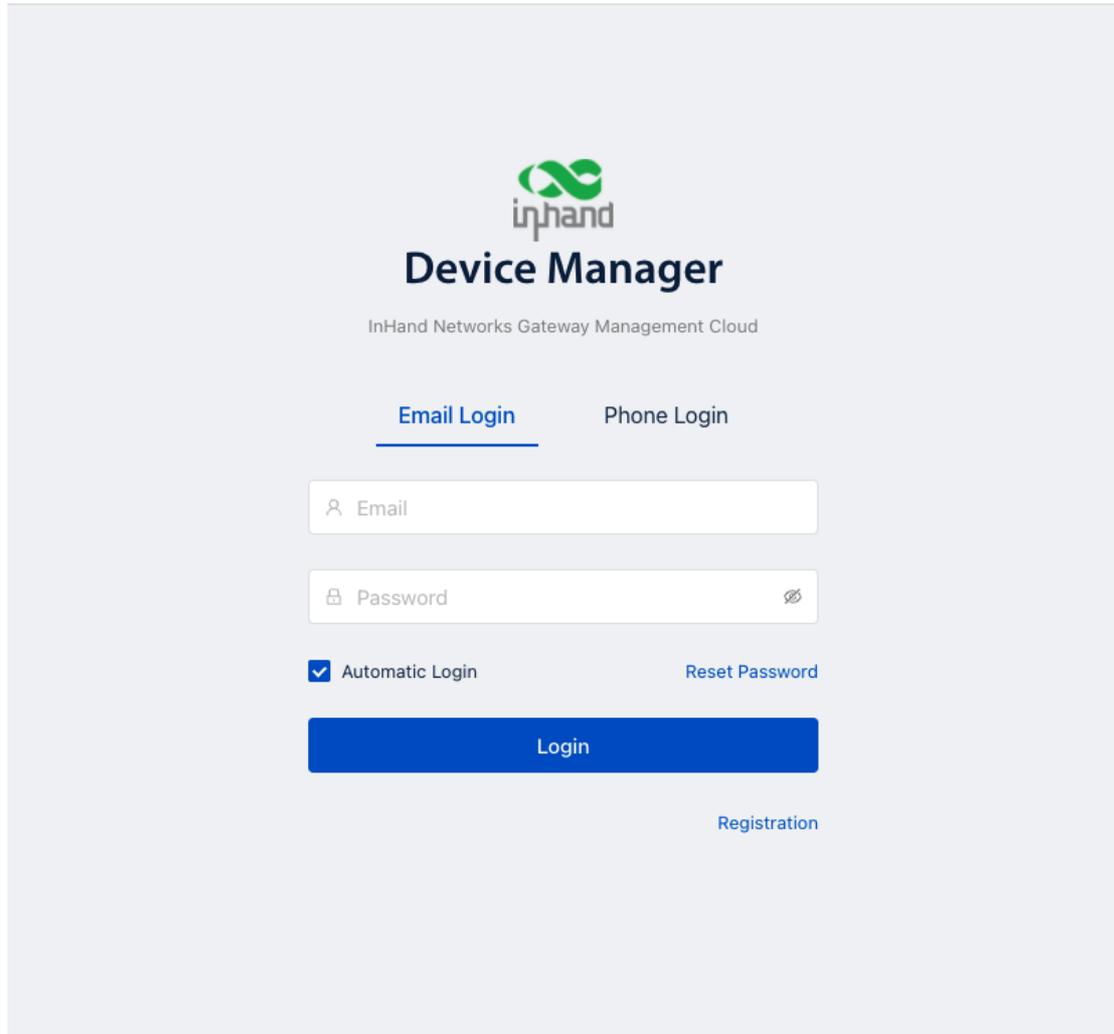
9.7 Device Manager of InHand Cloud

Click "Administration >>Device Manger>>Device Manger" config InHand Cloud service.

9.7.1 Config DeviceManger

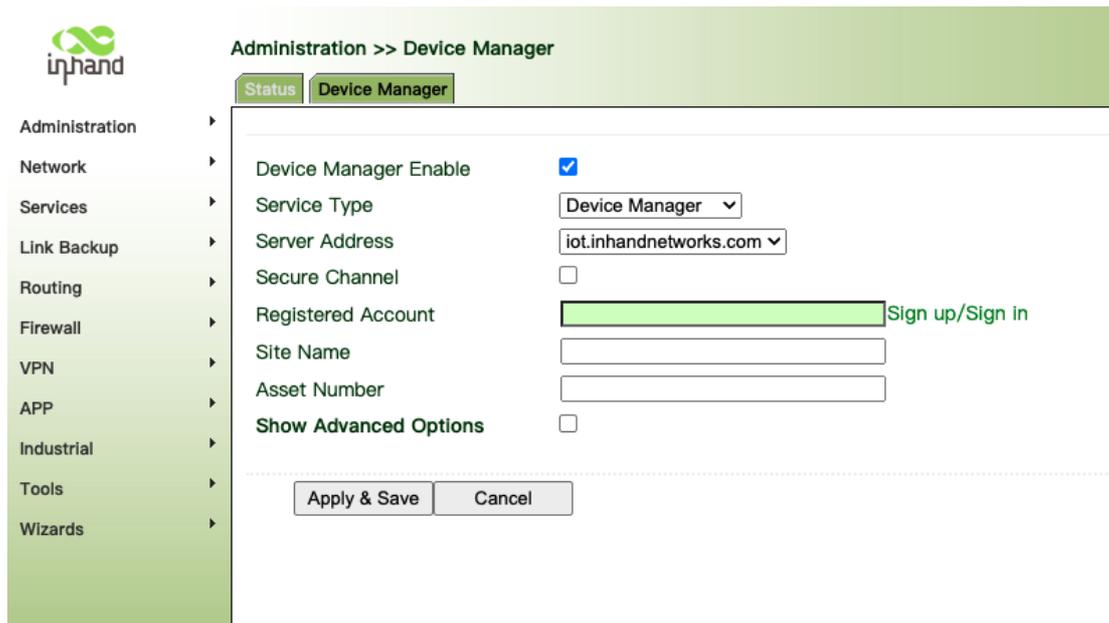
Device ManagerWith a visualization user interface and simple operation steps, the Device Manager platform enables you to manage and monitor InHand' s hardware devices, such as routers and gateways with convenience. It can quickly integrate devices and manage them with just a few clicks. The cloud deployment delivers easy-to-use experience, allowing you to focus on your core business and empowering your growth.

Step1: Register a user Global site <https://iot.inhandnetworks.com>



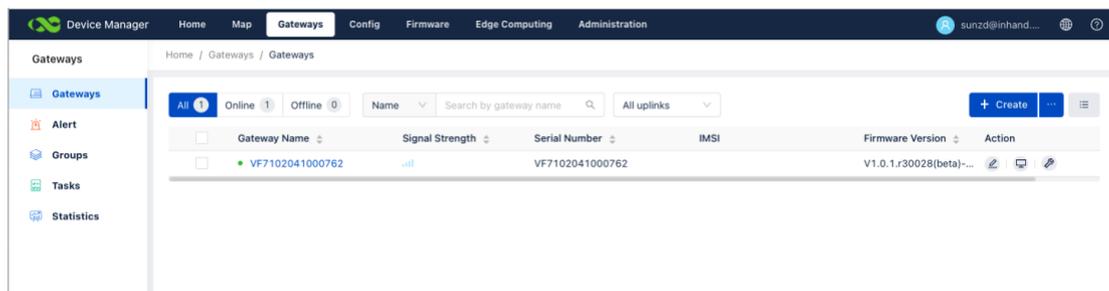
Step2:

- Config Service Type "Device Manager"
- Server Address "iot.inhandnetworks.com" If you have already privatized the deployed Device Manager Cloud, fill in the private deployment server IP or domain name. Server Typy select "Coustomer".
- Secure Channel, After checking, it will be transmitted with SSL encryption.
- Registered Account: Use step 1 registered account email address.
- Site name and Asset Number customer defined.
- Make sure the VG710 is connected to the Internet.

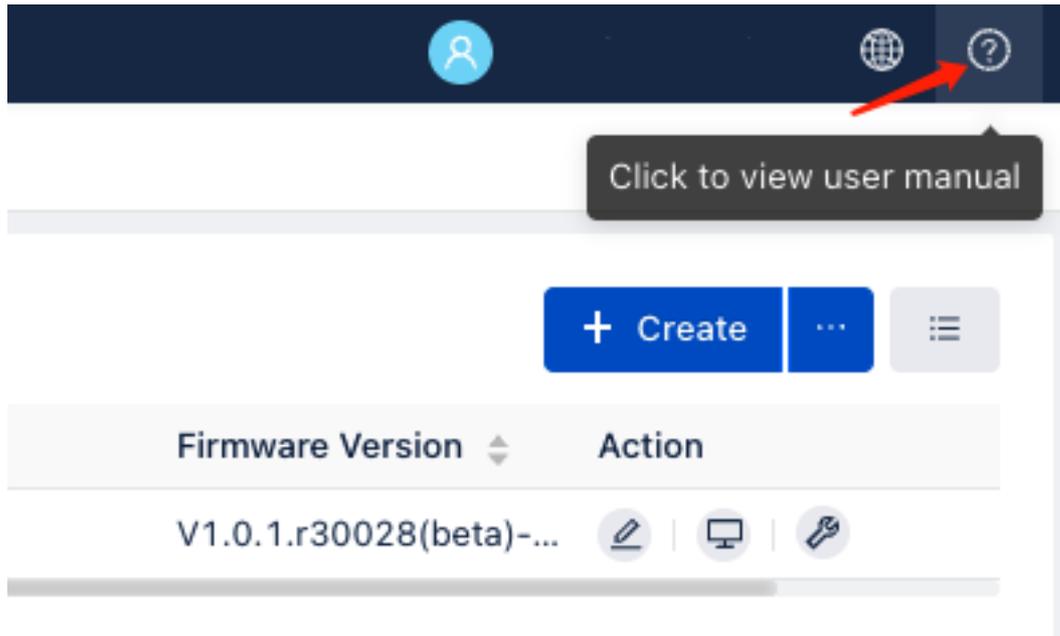


Step3:

- Login Device Manager cloud.
- Check Gateways, VG710 will auto login server.
- For more usage reference manuals:



- For more usage reference manual.



9.7.1 InConnect Service

The InConnect is a simple “plug & play” service which builds secure remote networks for your machines (IPCs, servers, IP cameras, PLCs, HMIs, RTUs, controllers, etc.). Featuring user-friendly interfaces and simple operation, the SaaS (Software as a Service) based solution enables you to access your devices anytime from anywhere, and stay connected with your business and with the world - especially in these challenging times when normal working routines have been disrupted. Support VPN networking in the way of subnet to subnet.

Step1: Register a user Global site <https://ics.inhandnetworks.com>

Step2:

- Config Service Type “InConnect Service”

- Server Address "ics.inhandnetworks.com" If you have already privatized the deployed Device Manager Cloud, fill in the private deployment server IP or domain name. Server Typy select "Coustomer".
- Secure Channel , After checking, it will be transmitted with SSL encryption.
- Registered Account : Use step 1 registered account email address.
- Site name and Asset Number customer defined.
- Make sure the VG710 is connected to the Internet.

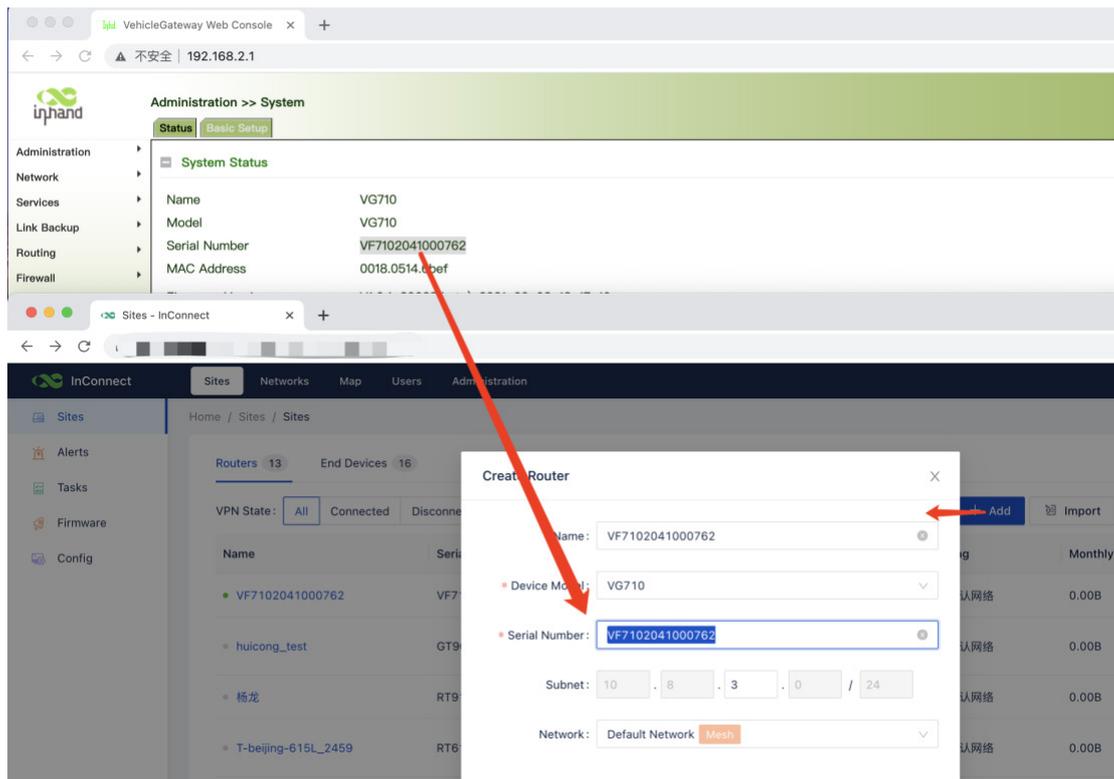
The screenshot displays the 'Administration >> Device Manager' configuration page. On the left is a sidebar with a tree view containing: Administration, Network, Services, Link Backup, Routing, Firewall, VPN, APP, Industrial, Tools, and Wizards. The main panel has a breadcrumb 'Administration >> Device Manager' and two tabs: 'Status' and 'Device Manager'. The configuration form includes the following fields:

- Device Manager Enable:**
- Service Type:** InConnect Service (dropdown)
- Server Address:** ics.inhandnetworks.com (dropdown)
- Secure Channel:**
- Registered Account:** xxxxx@inhand.com.cn (text input) with a [Sign up/Sign in](#) link.
- Site Name:** (text input)
- Asset Number:** (text input)
- Show Advanced Options:**

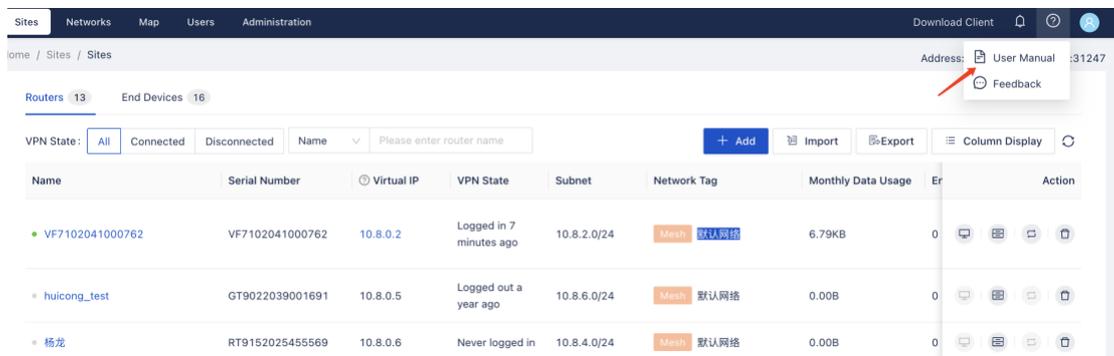
At the bottom of the form are two buttons: 'Apply & Save' and 'Cancel'.

Step3:

- Login InConnect service.
- Check Gateways, VG710 will auto login server.
- Add VG710 SN to Server:



- For more usage reference manuals:



9.7.1 Smart Fleet Service

InHand Smart Fleet Cloud Platform, referred to as Smart Fleet, is a business platform that provides enterprise-level vehicle monitoring and management services for enterprise customers. Smart Fleet can help you manage vehicles intelligently and efficiently, break down

vehicle data barriers, and realize multi-data joint analysis, vehicle Full life cycle management and control, intelligent vehicle operation and maintenance, help the informatization construction and digital transformation of engineering vehicles.

Smart Fleet can connect multiple vehicles to the same network. You can centrally monitor and manage vehicles, issue configurations, and upgrade firmware in a unified manner.

Smart Fleet helps users to quickly build an IoT network and master vehicle operation data in real time, allowing you to easily implement centralized monitoring and management of vehicles and gateways through the cloud platform. Effectively solve the problems of data isolation, collaboration bottlenecks, and lack of management.

Step1: Register a user Global site <https://smartfleet.cloud>

Step2:

- Config Service Type "InVehicle Service"
- Server Address "smartfleet.cloud" If you have already privatized the deployed Device Manager Cloud, fill in the private deployment server IP or domain name. Server Typy select "Coustomer".
- Secure Channel , After checking, it will be transmitted with SSL encryption.
- Registered Account : Use step 1 registed account email address
- License Plate Number is required.
- Asset Number Group ID is customer defined.
- Other interface information of the gateway can be reported to the platform in seconds.
- Make sure the VG710 is connected to the Internet.



Administration >> Device Manager

Status Device Manager

- Administration
- Network
- Services
- Link Backup
- Routing
- Firewall
- VPN
- APP
- Industrial
- Tools
- Wizards

Device Manager Enable

Service Type InVehicle Service

Server Address smartfleet.cloud

Secure Channel

Registered Account Sign up/Sign in

License Plate Number

Asset Number

Group ID

GNSS report interval s

MOTION report interval s

IO report interval s

OBD-II report interval s

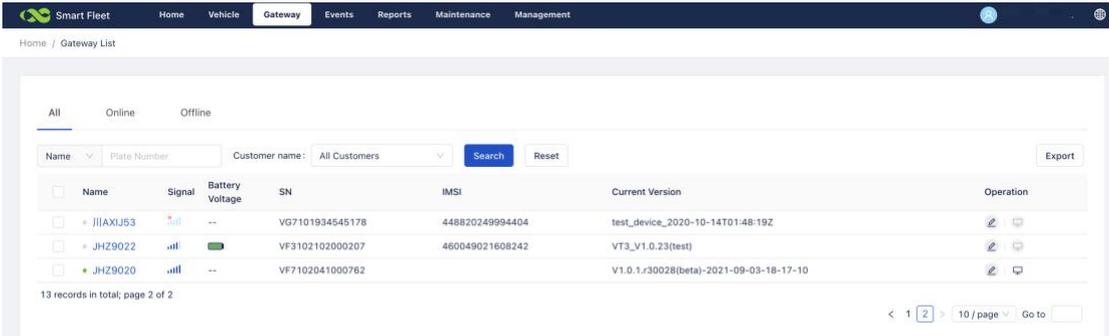
SENSOR report interval s

Show Advanced Options

Apply & Save Cancel

Step3:

- Login InConnect service.
- Check Gateways, VG710 will auto login server.



Smart Fleet Home Vehicle Gateway Events Reports Maintenance Management

Home / Gateway List

All Online Offline

Name Plate Number Customer name: All Customers Search Reset Export

Name	Signal	Battery Voltage	SN	IMSI	Current Version	Operation
JJAXIJ53		--	VG7101934545178	448820249994404	test_device_2020-10-14T01:48:19Z	
JHZ9022			VF3102102000207	460049021608242	VT3_V1.0.23(test)	
JHZ9020		--	VF7102041000762		V1.0.1:30028(beta)-2021-09-03-18-17-10	

13 records in total; page 2 of 2

< 1 2 > 10 / page Go to

9.8 SNMP

9.8.1 SNMP

Currently, the SNMP Agent of VG710 supports SNMPv1, SNMPv2c, and SNMPv3.

- SNMPv1 and SNMPv2c use community names for authentication.
- SNMPv3 uses user names and passwords for authentication.

Method for enabling SNMP for VG710:

Click "Administration >> SNMP >> SNMP", check "Enable", select "v1c" for "v2c" for "SNMP Version", and click Apply & Save.

Administration >> SNMP

SNMP SnmpTrap SnmpMibs

Enable

Listen IP address any

SNMP Version v2c

Contact Information Beijing_Inhand_Networks

Location Information Beijing_China

Community Management

Community Name	Access Limit	MIB View
public	Read-Only	DefaultView
private	Read-Write	DefaultView
<input type="text"/>	Read-Only	DefaultView

If v3c is selected, the corresponding user and user group need to be configured. Enter any name for "Groupname", select a security level, and click Add. Enter any name for "Username", select the new group name for "Groupname", set "Authentication" and "Authentication password", click Add, and then click Apply & Save.

Administration >> SNMP

SNMP SnmpTrap SnmpMibs

Enable	<input checked="" type="checkbox"/>
Listen IP address	any
SNMP Version	v3
Contact Information	Beijing_Inhand_Networks
Location Information	Beijing_China

User Group Management(v3)

Groupname	Security Level	Read-only View	Read-write View	Inform View
	NoAuth/NoPriv	DefaultView	DefaultView	DefaultView
Add[0/4]				

User Management(v3)

Username	Groupname	Authentication	Authentication password	Encryption	Encryption password
		None		None	
Add[0/16]					

Apply & Save Cancel

9.8.2 SnmpTrap (Alarm)

The SNMP trap is a type of entrance. When this entrance is reached, the SNMP managed devices actively notify the NMS, instead of waiting for the polling of NMS. On an SNMP-enabled network, the agents on managed devices can report errors to the NMS anytime, without the need of waiting for the polling of NMS. The errors are reported to the NMS through traps.

Method for enabling SnmpTrap for the gateway:

Click "Administration >> NMP >> SnmpTrap". Enter the IP address of the NMS. Enter the corresponding group name when v1c or v2c is selected, or the corresponding user name when v3c is selected, ensuring that the name consists of 1 - 32 characters. By default, the UDP port ID ranges from 1 to 65535.

Administration >> SNMP

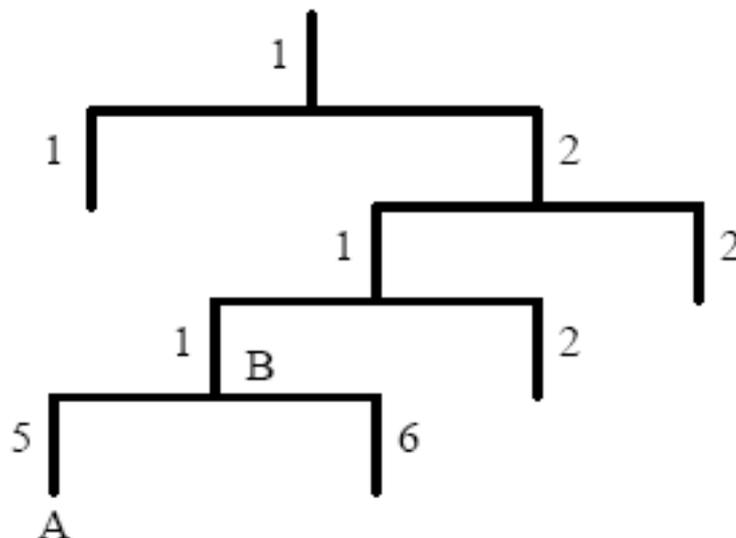
SNMP SnmpTrap SnmpMibs

Configure SnmpTrap

Host address	Security Name	UDP Port
<input type="text"/>	<input type="text"/>	162
		<input type="button" value="Add[0/4]"/>

9.8.3 SnmpMibs

In SNMP messages, management variables are used to describe the managed objects on the device. To uniquely identify the managed objects on the device, SNMP uses a hierarchical naming scheme to identify the managed objects. The entire hierarchical structure is like a tree. The nodes of the tree represent the managed objects, as shown in the figure below. Each node can be uniquely identified by a path starting from the root.

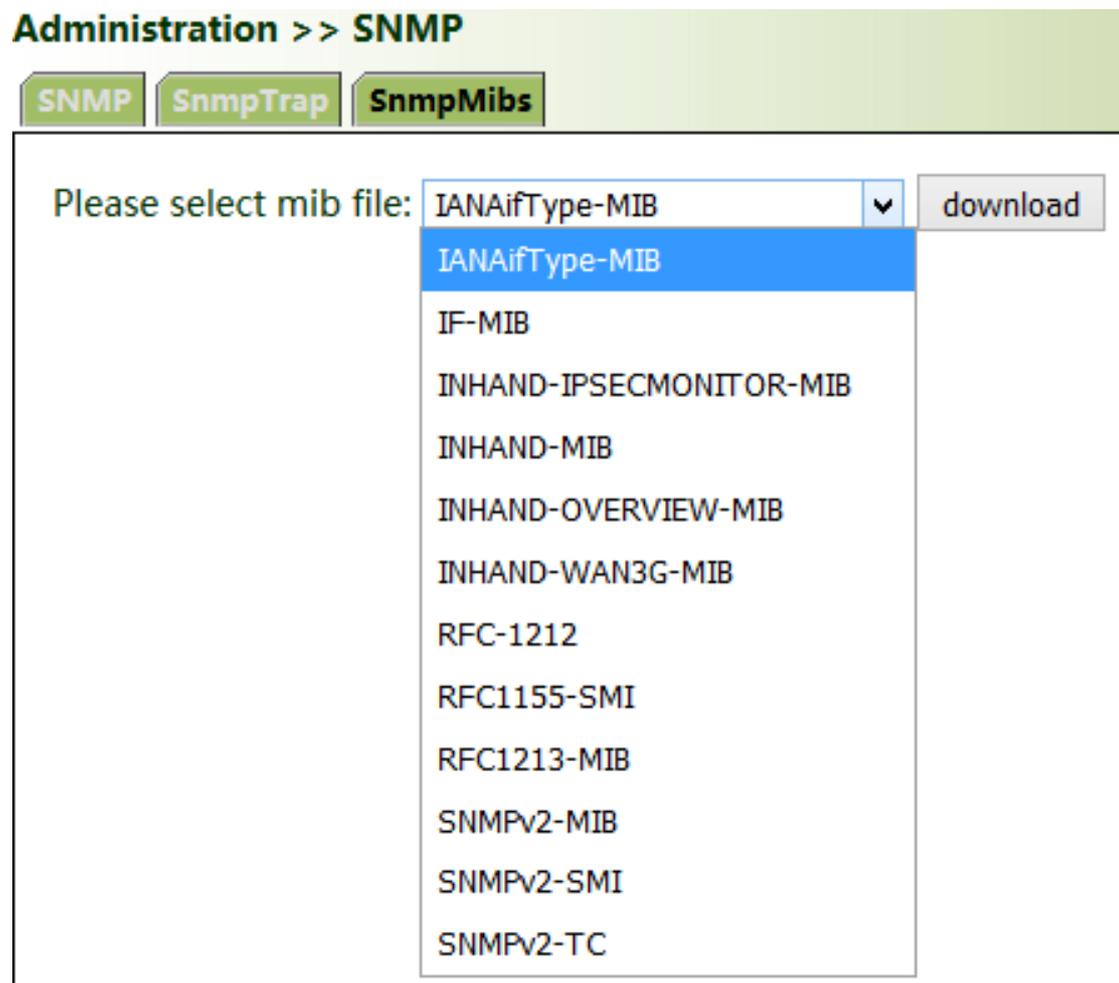


The management information base (MIB) is used to describe the hierarchical structure of the tree. It is a set of standard variable

definitions for the monitored network device. In the above figure, managed object B can be uniquely determined based on a string of numbers {1.2.1.1}, which form the object identifier (OID) of the managed object.

Method for downloading a SnmpMibs file to the PC via the gateway:

Click "Administration >> SNMP >> SnmpMibs", select a folder, and click download to download it to the PC. Find the folder on the PC and import it to the NMS.



9.8 Alarm

The alarm function enables users to identify gateway abnormalities in time. When an abnormality occurs, the gateway reports an alarm. You can select system-defined abnormalities and choose an appropriate notification way to obtain the abnormality information. All alarms

are recorded in alarm logs so that users can identify abnormalities and perform troubleshooting in time.

Alarm states:

- **Raise:** indicates that the alarm has been generated but not been confirmed.
- **Confirm:** indicates that the alarm cannot be solved currently.
- **All:** indicates all generated alarms.

Alarm levels:

- **EMERG:** The device undergoes a serious error that causes a system reboot.
- **CRIT:** The device undergoes an unrecoverable error.
- **WARN:** The device undergoes an error that affects system functions.
- **NOTICE:** The device undergoes an error that affects system performance.
- **INFO:** A normal event occurs.

(1) **Status:** Click "Administration >> Alarm >> Status" and view all alarms generated in the system since power-on.



(2) **Alarm Input:** Select an alarm type as required. When this item is abnormal, an alarm is generated.

(3) **Alarm Output:** When an alarm is generated, the system automatically sends the alarm content to the destination email address via an email. This function is not available for common users. Set the sender mail address in "Email Alarm" and the receiver mail address in "Mail Address". "Mail Server IP/Name" can be found on the browser (for example, enter "smtp.exmail.qq.com" if you use a Tencent Enterprise mailbox.)

Administration >> Alarm

Status **Alarm Input** **Alarm Output** **Alarm Map**

Email Alarm

Enable Email Alarm:	<input type="checkbox"/>
Mail Server IP/Name:	<input type="text"/>
Mail Server Port:	<input type="text" value="25"/>
Account Name:	<input type="text"/>
Account Password:	<input type="text"/>
Crypto:	<input type="text" value="NO"/>

(4) **Alarm Map**: Alarms can be received in two ways: command line interface (CLI) (console interface) and Email. Some devices support SMS alarms. To enable email-based mapping, enable and set the email address on the "Alarm Output" page.

9.9 System Logs

Method for viewing system logs:

Click "Administration >> System Log" to view system logs.

This page also provides the following operations: "Clear Log", "Download Log File", "Download Diagnose Data", "Clear History Log", and "Download History Log". History logs are those stored for extended time as specified on the "System Log" page.

The diagnose data file is encrypted, because the gateway configuration information is downloaded together with the diagnose data. You need to decrypt the file with the decryption tool provided by InHand.

Administration >> Log ENGIS

Log System Log

Too many logs, old logs are not displayed. Please download log file to check more logs!

Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x0a, response ID: 0x05)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x0b, response ID: 0x0a)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(3) and expected length(4)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(4) and expected length(3)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x0f, response ID: 0x0d)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x11, response ID: 0x0f)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x1c, response ID: 0x11)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(3) and expected length(4)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x21, response ID: 0x1f)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x23, response ID: 0x21)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(4) and expected length(3)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(3) and expected length(4)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(4) and expected length(3)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(3) and expected length(4)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(4) and expected length(3)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(3) and expected length(4)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x4e, response ID: 0x4d)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(4) and expected length(3)
Warning	Jan 16 17:12:31	obd[1456]: PID or MID or infoTypeID mismatch(request ID: 0x5c, response ID: 0x51)
Warning	Jan 16 17:12:31	obd[1456]: mismatch between response length(3) and expected length(4)

Clear Log Download Log File Download Diagnose Data
Clear History Log Download History Log

The storage capacity of the gateway is limited (512 KB by default). To save all the logs, you need to use a remote log server (for example, [Kiwi Syslog Daemon](#)). Set the address and port of the log server on the web page. The gateway uploads all the system logs to the remote log server.

Administration >> Log

Log System Log

Log to Remote System

Syslogd server address	Port Number
192.168.2.100	514

Add[0/4]

Log to Console

History log size KBytes(64-2048)

History log severity and above

Apply & Save Cancel

9.12 System Upgrade

Click "Administration >> Upgrade >> Browse", select an upgrade file, and click Upgrade. Restart the system after the upgrade is completed.

Administration >> Upgrade

Select the file to use:

No file selected.

Browse...

Upgrade

Firmware Version : 1.0.0.r11989



注意

Note:

During the software upgrade, do not perform any operation on the web page; otherwise, the software upgrade may be interrupted.

9.12 System Reboot

Click "Administration >> Reboot >> OK to reboot the system.



Administration >> Reboot

- Administration
- Network
- Services
- Link Backup
- Routing
- Firewall
- VPN
- APP
- Industrial
- Tools
- Wizards

- System
- System Time
- Management Services
- User Management
- AAA
- Config Management
- Device Manager
- SNMP
- Alarm
- Log
- Upgrade
- Reboot

VG710
VG710
VF7101937000006
0018.0510.302f
1.0.0.r11989
2012.07.r238
2020-01-16 17:14:55
2020-01-16 17:14:56
0 day, 02:14:39

CPU Load (1 / 5 / 15 mins) 0.07 / 0.25 / 0.48
Memory consumption 483.67MB / 198.97MB (41.14%)
Total/Free

Confirm Reboot ?

Sync Time

10 Diagnostic Tools

Diagnostic tools are used to detect the network connection of the gateway: Ping, Traceroute, Tcpdump, and Link Speed Test.

Ping: It is used to detect the external network connection of the device. Enter any common website in China for "Host" and click "Ping". If data transmission occurs, the network is connected properly.

Tools >> Ping

Ping

Host	<input type="text" value="g.cn"/>	<input type="button" value="Ping"/>
Ping Count	<input type="text" value="4"/>	
Packet Size	<input type="text" value="32"/> Bytes	
Expert Options	<input type="text"/>	

```
PING g.cn (203.208.43.79): 32 data bytes
40 bytes from 203.208.43.79: seq=0 ttl=118 time=35.083 ms
40 bytes from 203.208.43.79: seq=1 ttl=118 time=32.003 ms
40 bytes from 203.208.43.79: seq=2 ttl=118 time=31.548 ms
40 bytes from 203.208.43.79: seq=3 ttl=118 time=31.676 ms

--- g.cn ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 31.548/32.577/35.083 ms
```

Traceroute: Enter the IP address of the peer host and click "Trace" to detect the route connection.

Tools >> Traceroute english

Traceroute

Host:

Maximum Hops:

Timeout: s

Transmit Protocol:

Expert Options:

```

traceroute to g.cn (203.208.43.87), 20 hops max, 38 byte packets
 1 192.168.100.1 (192.168.100.1)  3.195 ms  4.402 ms  3.325 ms
 2 * * *
 3 182.150.21.1 (182.150.21.1)  9.764 ms  6.654 ms  7.288 ms
 4 118.112.213.21 (118.112.213.21)  5.588 ms  10.628 ms  4.966 ms
 5 61.139.121.37 (61.139.121.37)  11.402 ms  171.208.199.205 (171.208.199.205)  8.987 ms  171.208.199.185 (171.208.199.185)
 24.459 ms
 6 202.97.78.177 (202.97.78.177)  32.139 ms  30.755 ms  202.97.78.189 (202.97.78.189)  31.062 ms
 7 * * *
 8 219.142.18.222 (219.142.18.222)  34.296 ms  44.998 ms  bj141-142-174.bjtelecom.net (219.141.142.174)  53.204 ms
 9 203.208.62.16 (203.208.62.16)  30.968 ms  32.616 ms  219.142.18.222 (219.142.18.222)  36.003 ms
10 203.208.43.87 (203.208.43.87)  32.372 ms  203.208.62.49 (203.208.62.49)  36.248 ms  203.208.62.16 (203.208.62.16)  33.870
ms

```

Tcpdump:

Select an interface ("any" or "bridgel"), set "Capture Number", and click Start Capture >> Stop Capture >> Download Capture File.

Tools >> Tcpdump

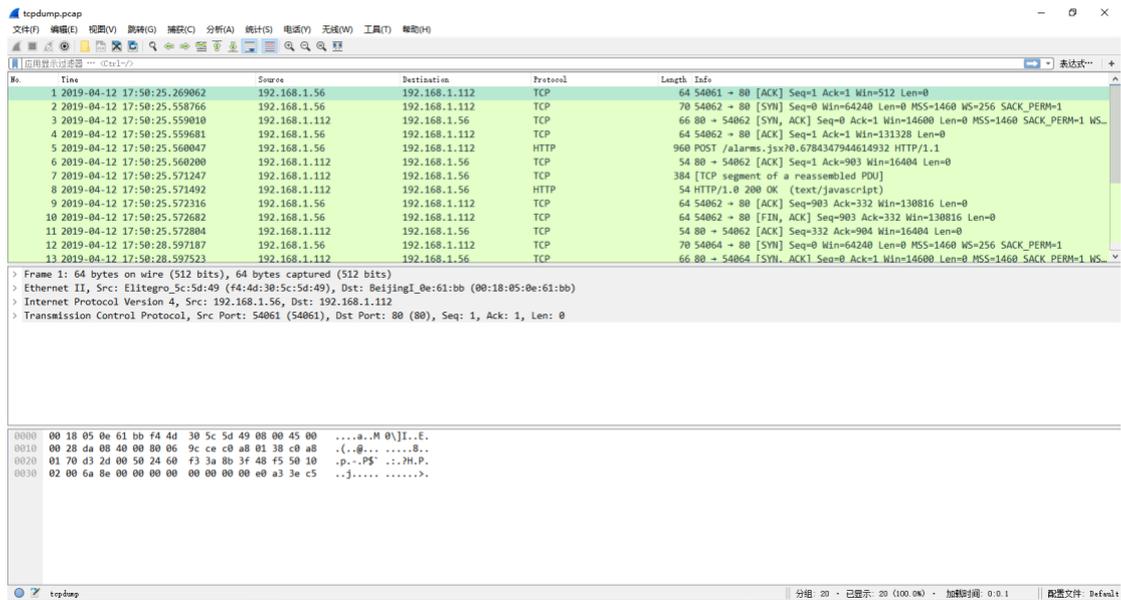
Tcpdump

Interface:

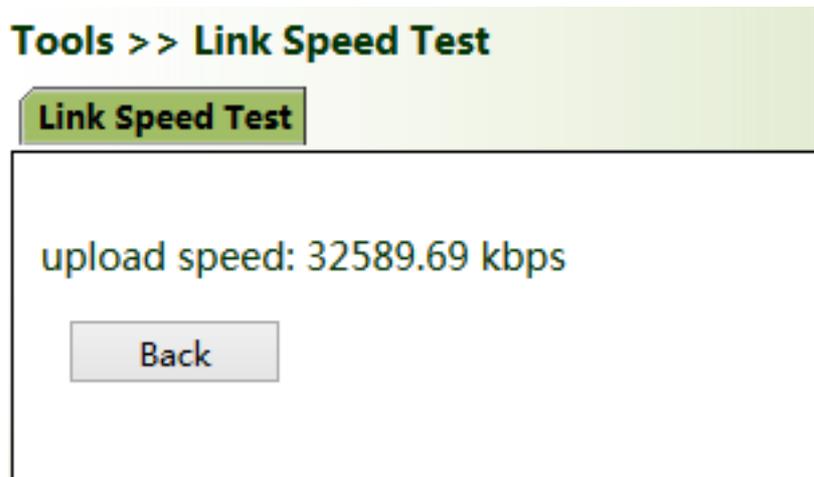
Capture Number: (10-1000)

Expert Options:

Download wireshark from the browser to open the downloaded file and analyze the messages to understand the network connection of the interface.



Link Speed Test: Upload and download files to test the link speed.



Chapter II Edge calculation

Powerful edge computing capabilities facilitate the development of custom applications. The remote fleet management platform is easy for secondary development by third-party software developers. With an open cloud ecosystem that supports Microsoft Azure and AWS, the VG710 offers more options for application developers. It supports Node-RED docker image low code edge computing solutions.



APP

Status APP Management

Administration ▶

Network ▶

Services ▶

Link Backup ▶

Routing ▶

Firewall ▶

VPN ▶

APP ▶

Industrial ▶

Tools ▶

Wizards ▶

Your password

APP Manager Status	Stopped	
Python Version	Python3	
SDK Version	2.3.15 Upgrade	
Debug Server Status	Stopped	
APP Filesystem Use%	10% of 6537 MB	
Data/Log Filesystem Use%	10% of 6537 MB	
APP	Card	Unrecognized

- APP
- Docker
- Third-Party Platform
- Local MQTT Broker
- REST API
- Azure IoT Edge
- User Data