InHand Networks

Edge Computing Gateway IG902

User Manual

Issue: V2.0—2019.04

InHand Networks
Global Leader in Industrial IoT
www.inhandnetworks.com

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.

Conventions

Symbol	Indication
< >	Content in angle brackets “<>” indicates a button name. For example, the <OK> button.
""	"" indicates a window name or menu name. For example, the pop-up window "New User."
>	A multi-level menu is separated by the double brackets ">". 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].
Cautions	Means reader be careful. Improper action may result in loss of data or device damage.
Note	Notes contain detailed descriptions and helpful suggestions.

Contact Us

Add: 3900 Jermantown Rd., Suite 150, Fairfax, VA 22030 USA
E-mail: support@inhandneworks.com
T: +1 (703) 348-2988
URL: www.inhandnetworks.com

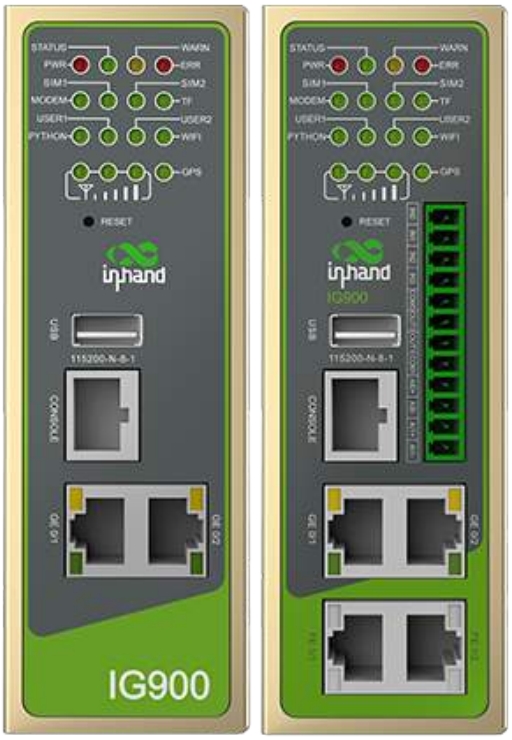
Contents

1 Introduction

IG902 Edge Computing Gateway is a new-generation 4G edge computing gateway that is launched by InHand specifically for the Industrial Internet of Things (IIoT). It provides omnipresent and continuous Internet access through global 3G/4G wireless networks and multiple broadband services. It features a robust edge computing capability, comprehensive security, and wireless services, capable of connecting tens of thousands of devices to networks and providing high-speed data channels for device informatization.

With a robust edge computing capability, IG902 implements data optimization, real-time response, agile connection, and intelligent analysis on IoT edge nodes. This greatly reduces the data traffic between sites and centers, and prevents bottlenecks of cloud-based computing. IG902 can optimize network architectures, deliver more secure and faster responses, and implement onsite services in a more intelligent manner.

Gateway models:



IG902-B IG902-H

2 Network Connection, Web Login, and Communication Parameter Setting

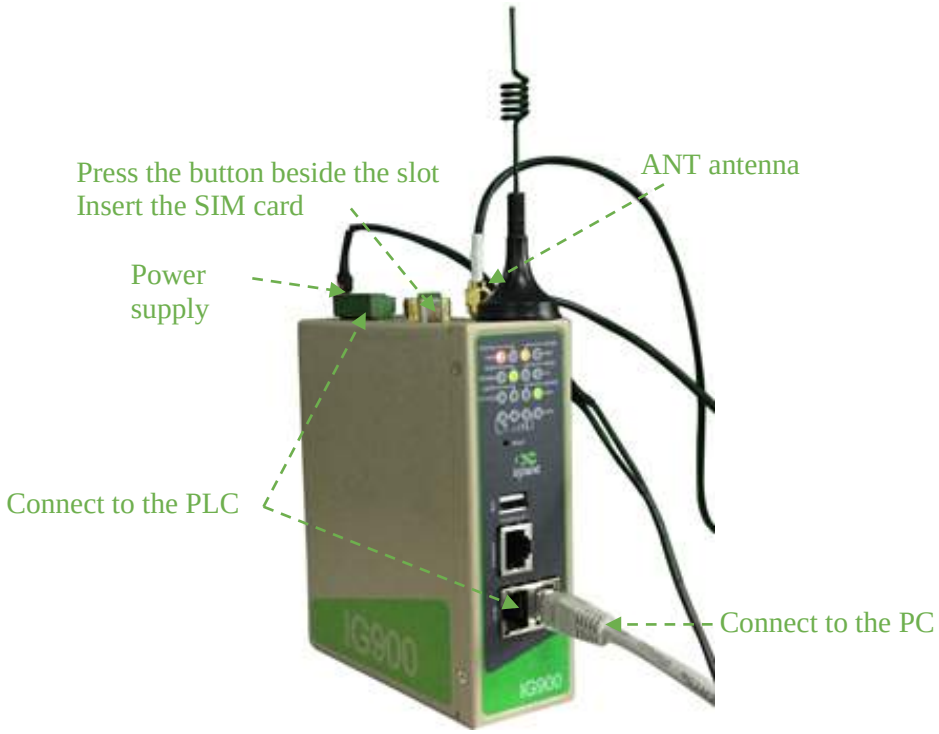
This chapter describes how to establish a network connection for the gateway, log in to the gateway's web-based management page, and set communication parameters based on the selected network connection mode. If the communication parameters described in this chapter do not meet your application requirements, see chapter 3 "Communication Parameter Setting (Supplementary)."

2.1 Network Connection

2.1.1 Cellular Network Connection

1) Wireless dial-up (with a SIM card)

1. Insert the SIM card in slot 1, connect the 4G LTE antenna to the ANT port, and connect the gateway to a power supply. Connect the gateway to the programmable logic controller (PLC) through the serial port or LAN port.

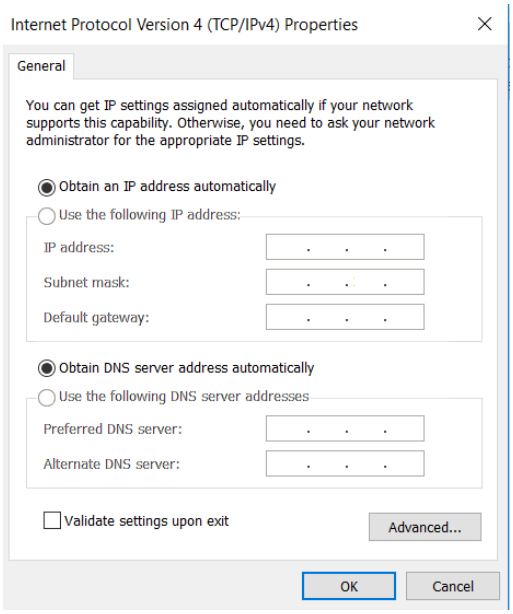


Note:

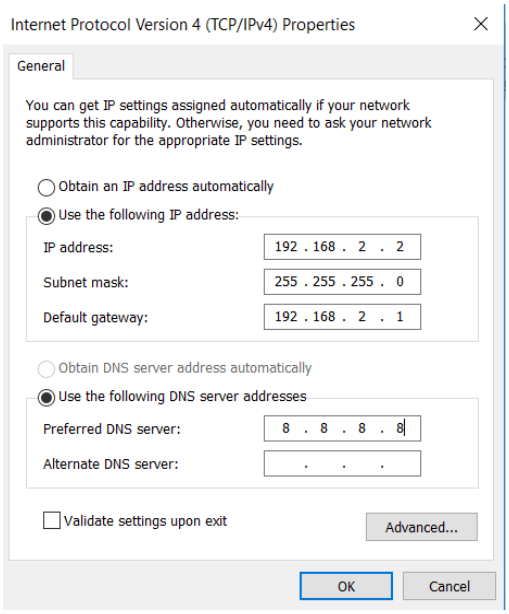
Before inserting or removing the SIM card, power off the gateway; otherwise, data may be lost or the gateway may be damaged.

2. Set the IP addresses of the PC and gateway to be in the same network segment.

(Recommended) Mode 1: Automatic IP address allocation.
Mode 2: Fixed IP address. Set the IP addresses of the PC and the gateway's GF ports to be in the same network segment. The initial IP address of the gateway is 192.168.2.1, and its subnet mask is 255.255.255.0. Select **Use the following IP address**, enter an IP address (any from 192.168.2.2 to 192.168.2.254), subnet mask (255.255.255.0), and default gateway IP address (192.168.2.1), and click **OK**.

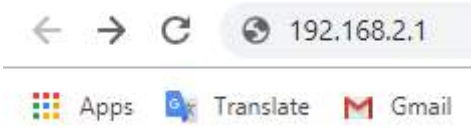


Obtain an IP address automatically

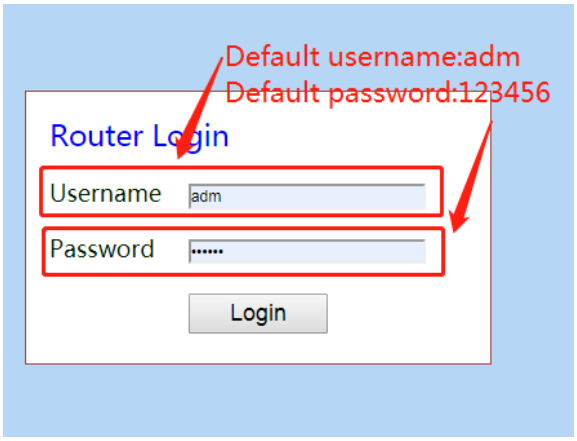


Use the following IP address

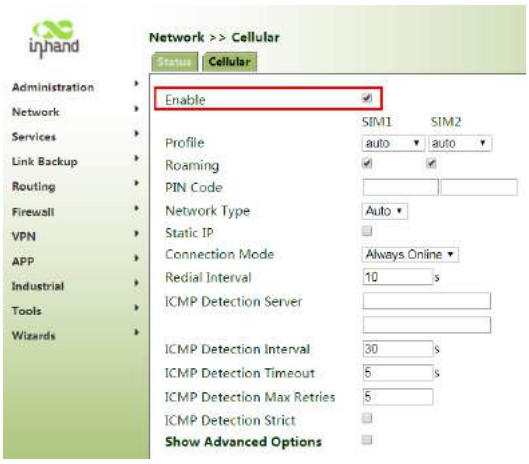
3. Open the web browser and enter 192.168.2.1 (default IP address of the gateway) to access the gateway's web-based management page.



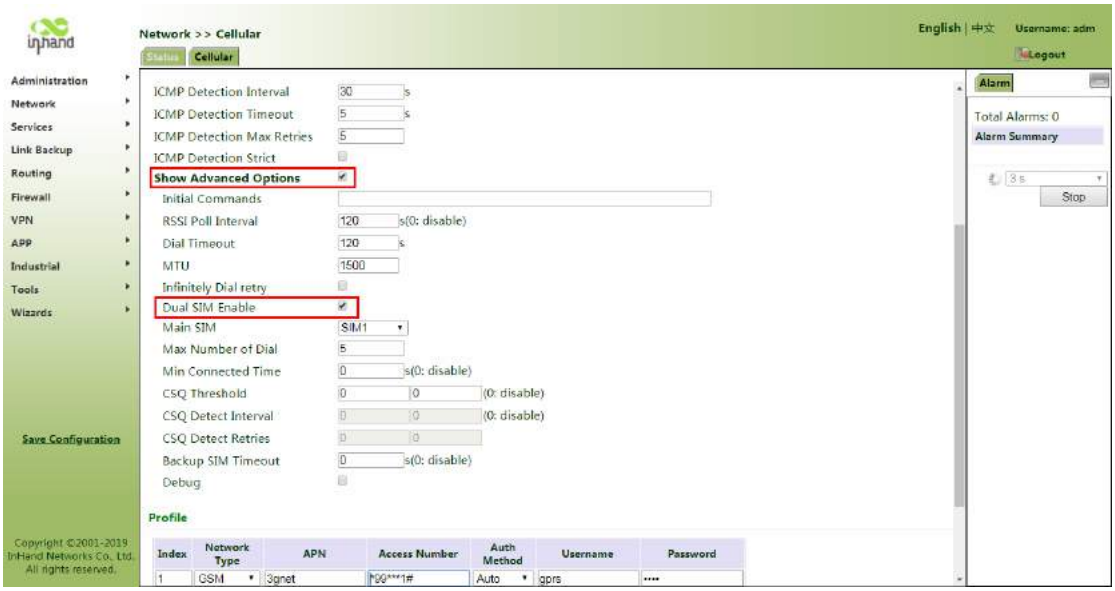
4. Log in to the gateway.



5. Choose **Network** > **Cellular**, and select **Enable**. The SIM card is successfully connected to the network if the network connection status is Connected and an IP address is allocated.



6. The dual SIM card feature is supported. Enable this feature if another SIM card is inserted in slot 2.

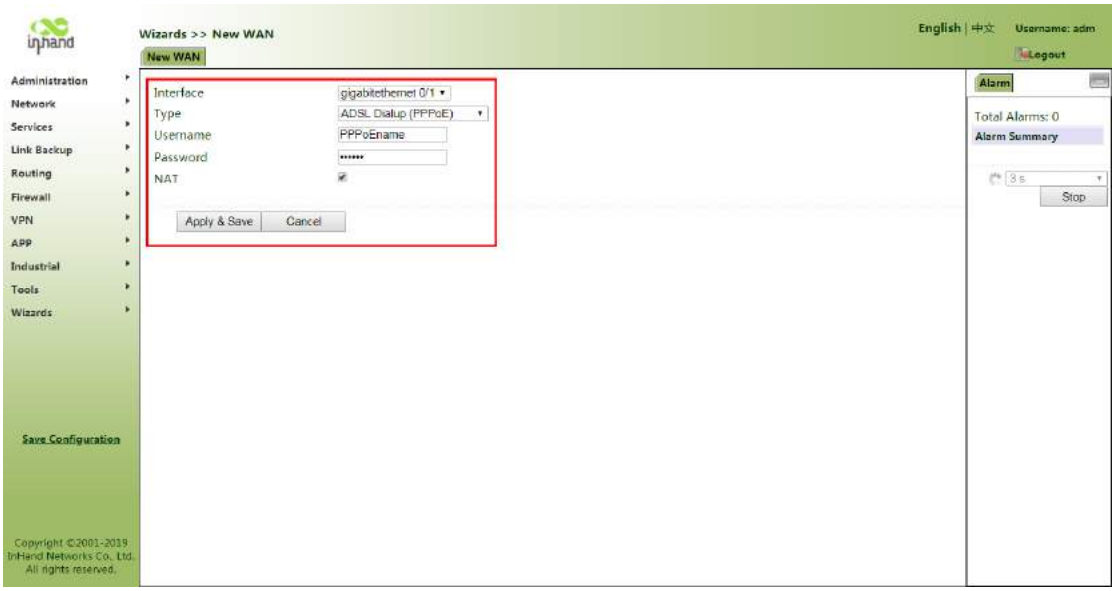


2) Wired dial-up (PPPoE server)

1. Connect cables based on the following figure if a PPPoE server is used for dial-up.

2. Set the IP addresses of the PC and gateway to be in the same network segment. Log in to the gateway's web-based management page. For details, see "Wireless dial-up."

3. Choose **Wizards** > **New WAN**. Select **gigabitethernet 0/1** for **Interface** and **ADSL Dialup (PPPoE)** for **Type**. Enter the name and password of the PPPoE server. Enable **NAT**. Click **Apply & Save**.



2.1.2 Ethernet Connection

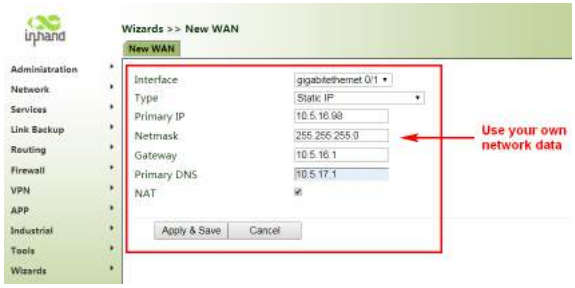
1. Connect the power supply and network cable to the gateway. Connect the LAN port (GE1/1) to the PC and connect the WAN port to the Internet. Connect the gateway to the PLC through the serial port or LAN port.

2. Set the IP addresses of the PC and gateway to be in the same network segment. Log in to the gateway's web-based management page. For details, see section 2.1.1 "Cellular Network Connection."

3. Choose **Wizards** > **New WAN**. Set an IP address for the WAN port so that the gateway can connect to the Internet.

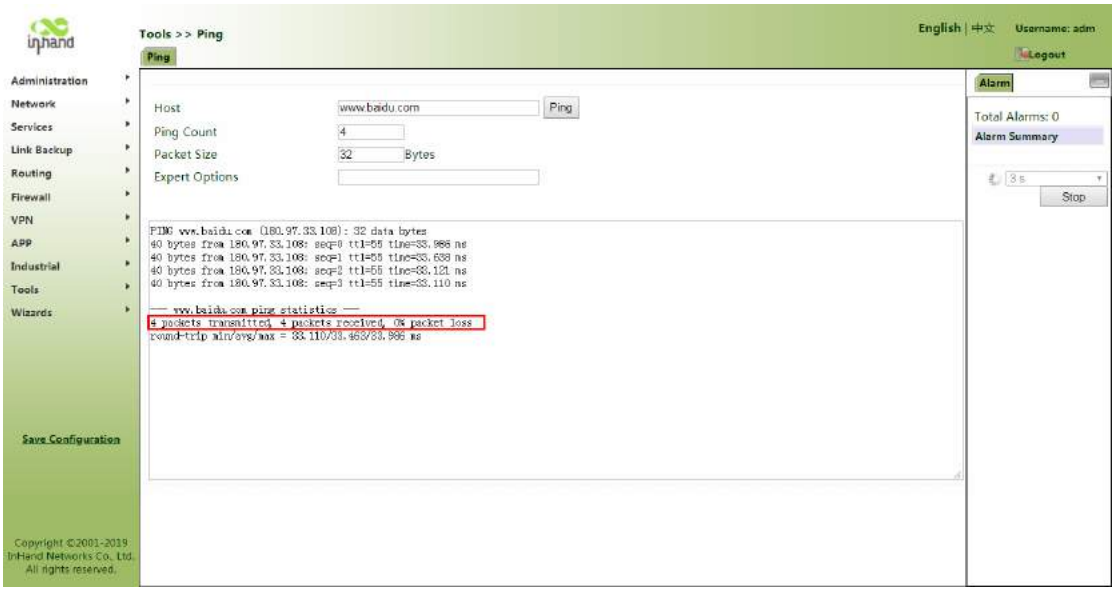
4. DHCP is recommended. If you choose to set a static IP address, set the network parameters and save them based on the actual network connection.

Dynamic IP address allocation



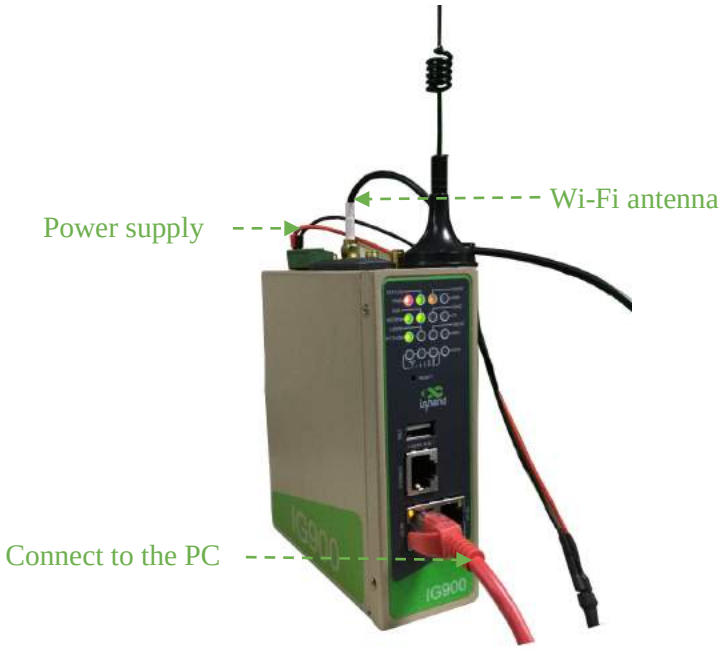
Static IP address setting

5. Choose **Tools** > **Ping** to check whether the gateway is connected to the Internet. Enter the URL of a common website in **Host** for testing. If the following message appears, the gateway is connected to the Internet.



2.1.3 Wi-Fi Connection

1. Connect the power supply and network cable to the gateway, and connect the Wi-Fi antenna to WLAN 1 or 2. Connect the gateway to the PLC through the serial port or LAN port.



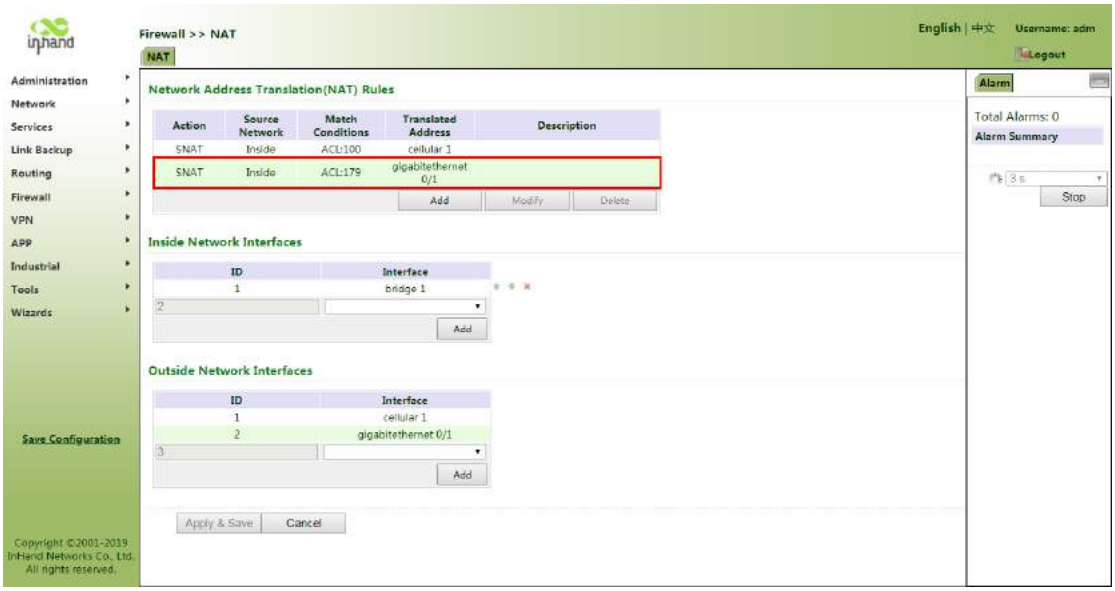
2. Set the IP addresses of the PC and gateway to be in the same network segment. Log in to the gateway's web-based management page. For details, see section 2.1.1 "Cellular Network Connection."

3. Choose **Network** > **WLAN**. Enable the WLAN port and set parameters, as shown in the following figure.

4. Click the **Status** tab. The network connection status is Connected.

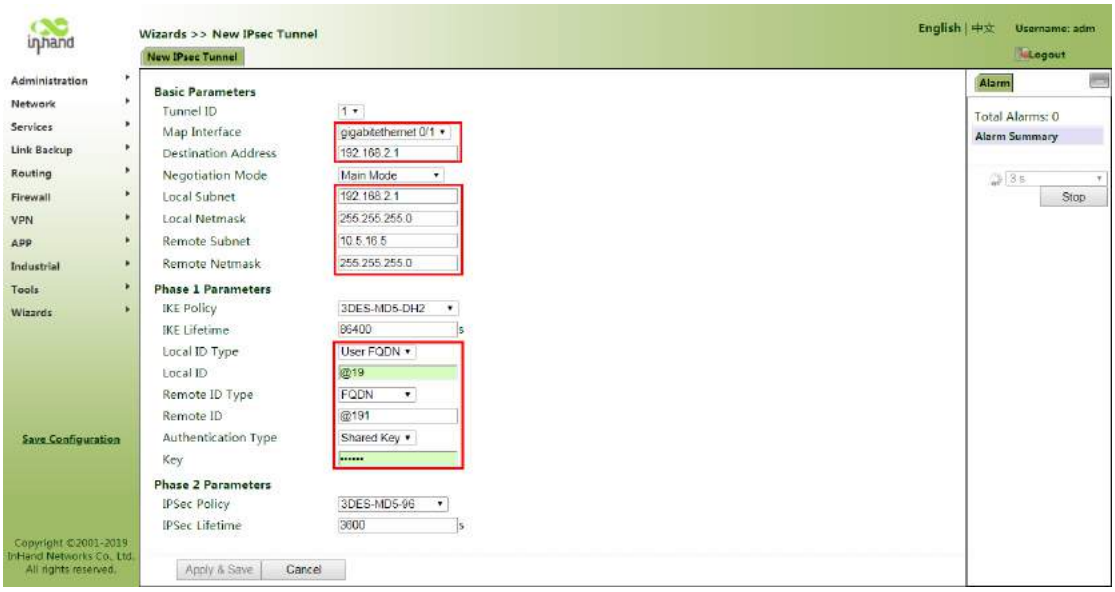
5. Choose **Wizard** > **New WLAN** and set the parameters.

6. Choose **Firewall** > **NAT**. The Wi-Fi connection is successful if the dot11radio 1 connection is displayed.



2.2 Creating an IPsec Tunnel

You can create a dedicated virtual tunnel between the gateway and another device in the network or a cloud platform after a network connection is established. This section shows how to create an IPsec tunnel. Choose **Wizards** > **New IPsec Tunnel**, select the interface for which you want to create an IPsec tunnel, and enter the peer IP address and the subnet addresses and masks at both ends of the tunnel. During the first phase, enter the identifiers and connection keys at both ends of the tunnel, and click **Apply & Save**.

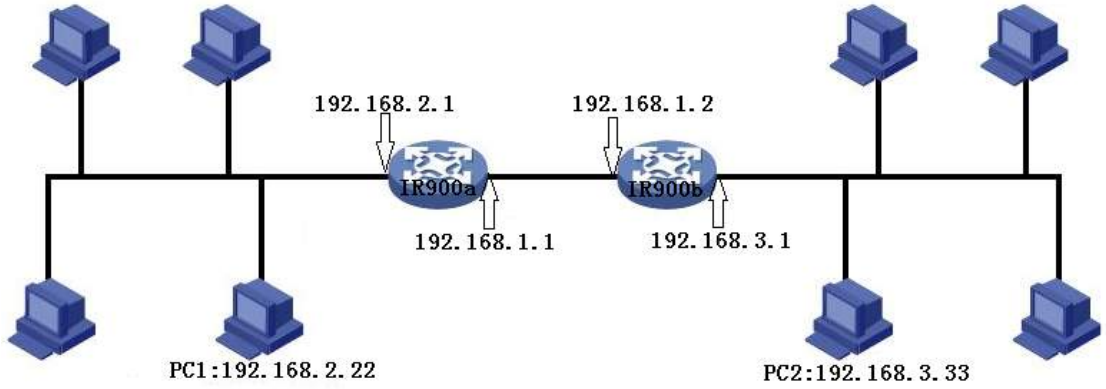


3 Communication Parameter Setting (Supplementary)

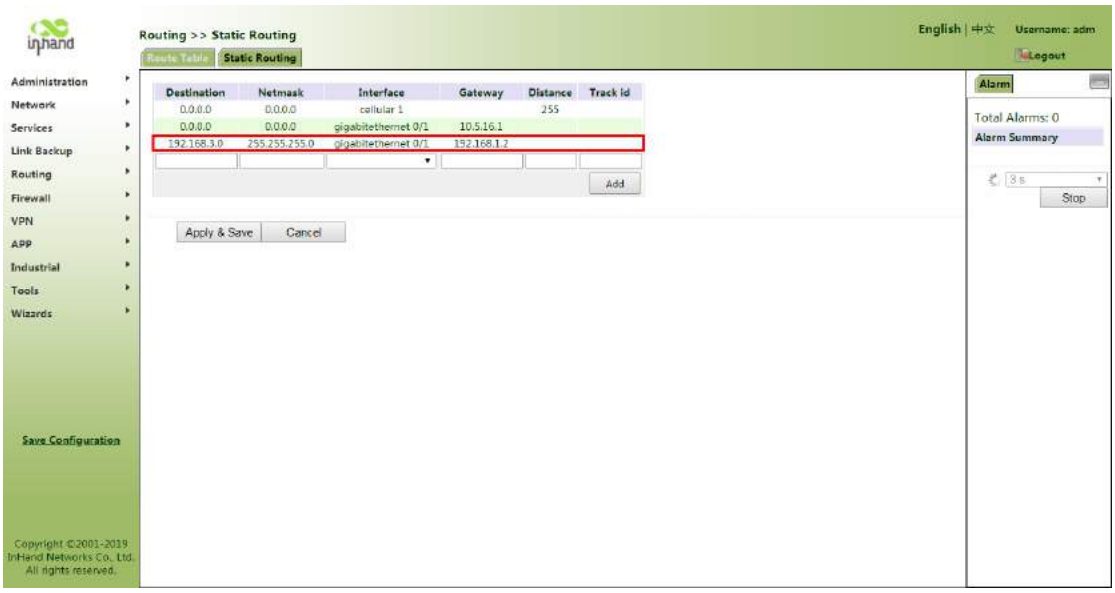
This chapter supplements chapter 2. If the communication parameter setting described in chapter 2 does not meet your requirements, set the parameters based on this chapter.

3.1 Static Route

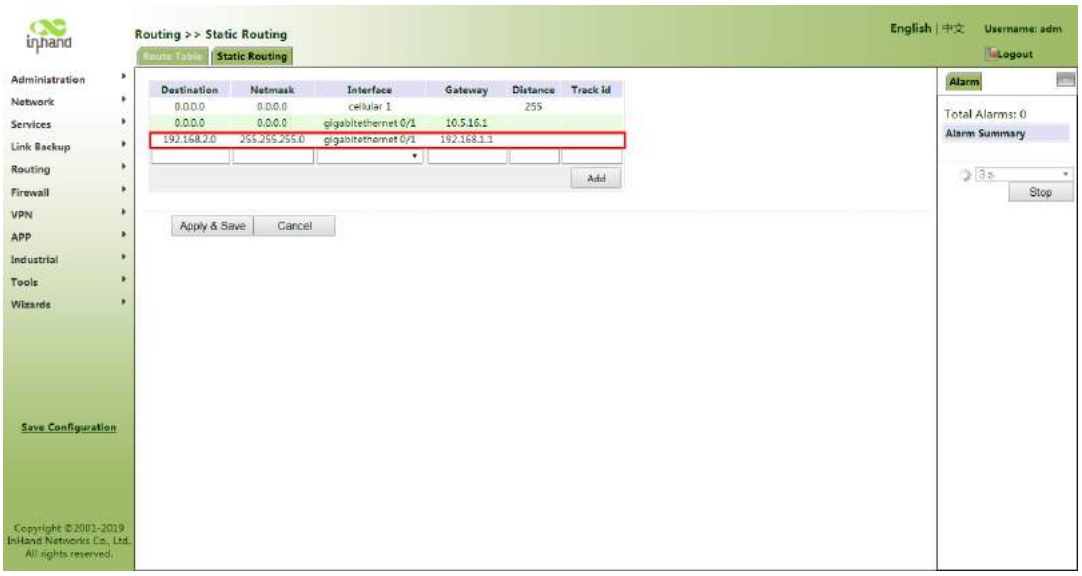
PC 1 and PC 2 located in two separate subnets cannot communicate with each other when no static route is configured. To enable communication between PC 1 and PC 2, you need to configure a static gateway between the two LANs, as shown in the following topology.



Configure the gateway as follows:
Step 1: Choose **Routing** > **Static Routing** to configure edge computing gateway A. Set **Destination** to the gateway address of PC 2 in the format xxx.xxx.xxx.0. The default value of **Netmask** is 255.255.255.0, whereas 0.0.0.0 indicates all subnet masks. Set either **Interface** (interface connected to gateway B) or **Gateway** (which must be configured on gateway B in advance).



Step 2: Configure edge computing gateway B. Set the parameters based on the following figure.

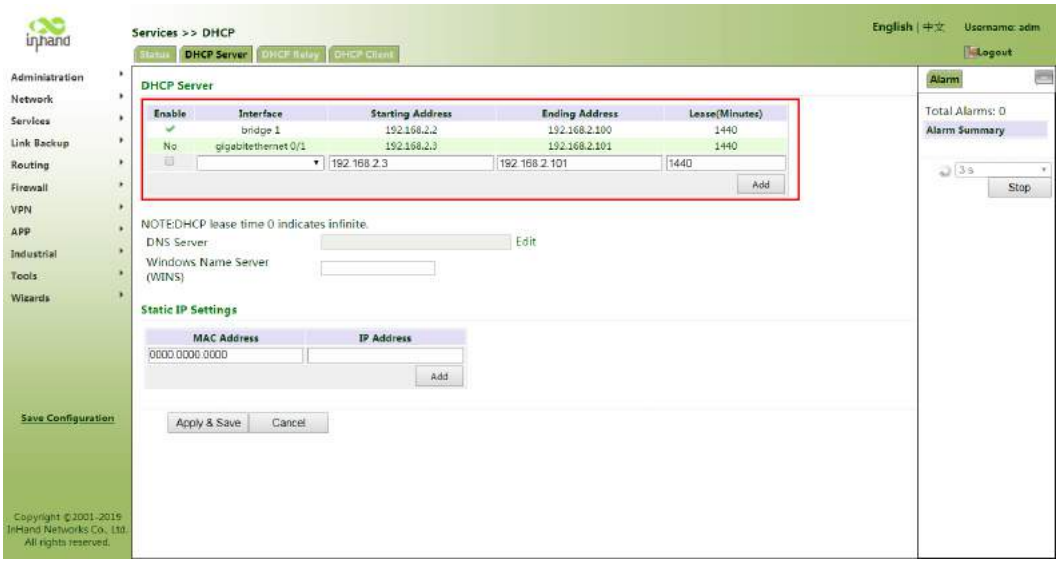


Step 3: Check whether PC 1 and PC 2 can communicate with each other. If yes, the static gateway is added successfully.

3.2 Automatic IP Address Allocation (DHCP)

DHCP adopts the client/server communication mode. The client sends a configuration request to the server, which then returns corresponding configuration, such as the IP address allocated to the client. This implements dynamic configuration of the IP address and other information.

- The gateway can work as the DHCP server to allocate a different IP address to each login workstation. The DHCP server greatly simplifies network management tasks that are otherwise completed manually.

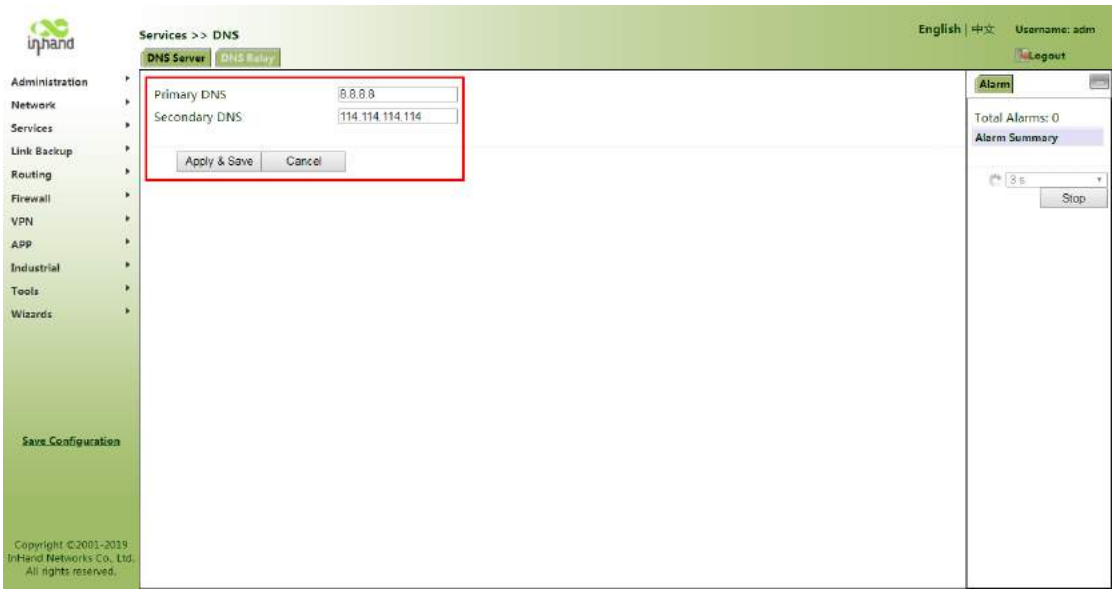


- The gateway can also work as the DHCP client to receive the IP address allocated by the DHCP server after login. This requires that the gateway's Ethernet interface be set to automatic mode.

3.3 DNS

A domain name server (DNS) converts domain names to corresponding IP addresses that can be identified by PCs. Users only need to remember domain names. DNS is typically set only when the WAN port uses a static IP address:

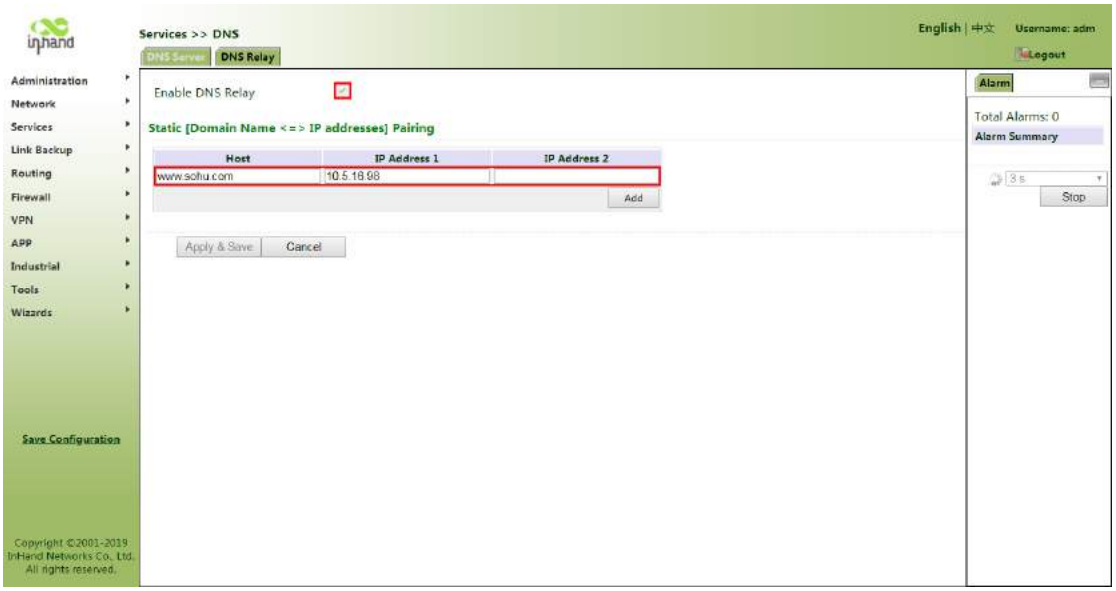
DNS Server: On this tab page, you can configure the gateway to resolve dynamic domain names through the DNS.



DNS Relay: On this tab page, you can configure the gateway as a DNS proxy to forward DNS request and response packets between the DNS client and server and resolve domain names on behalf of the DNS client.

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

You can set **Static [Domain Name <=> IP addresses] Pairing** to map IP addresses to domain names so that IP addresses can be accessed by using domain names.

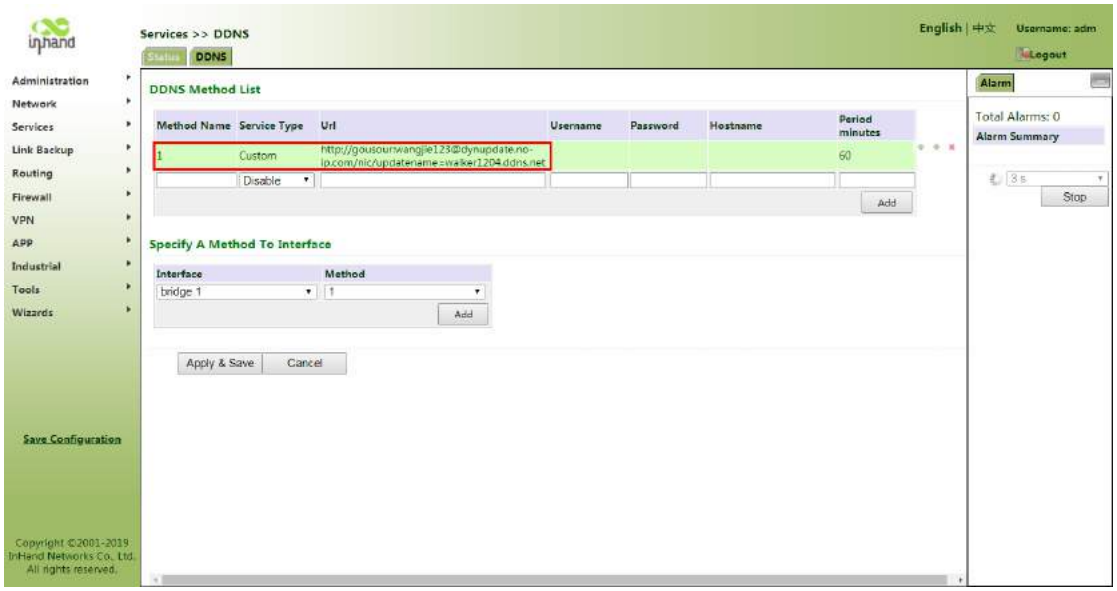


3.4 DDNS

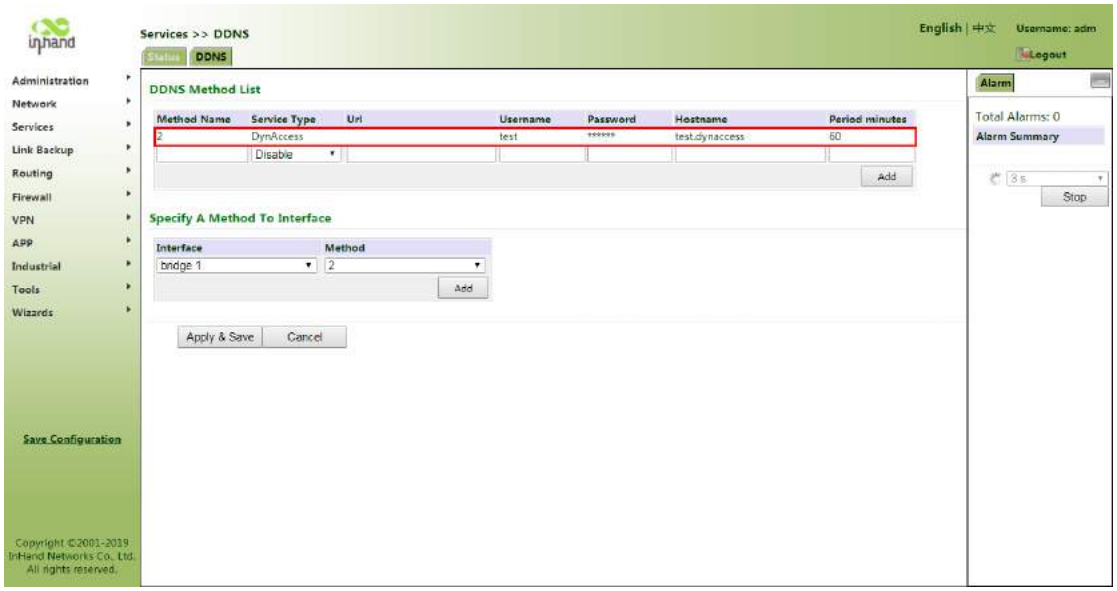
The edge computing gateway obtains public IP addresses through dial-up. You can configure Dynamic Domain Name Server (DDNS) to map users' dynamic IP addresses to a fixed DNS.

Configure the gateway as follows:

Step 1: Set the DDNS parameters of the gateway. If a custom domain name is used, find the DDNS expression on the server's official website, and enter a URL in the format http://*user name*:password@ddns.oray.com/ph/update?hostname=*host name*, as shown in the figure "DNS parameter setting 1." If a common domain name is used, enter the registered account, password, and host name, as shown in figure "DNS parameter setting 2." DDNS is not used if **Disable** is selected.



DNS parameter setting 1



DNS parameter setting 2

Step 2: Wait for several minutes after you configure DDNS and save and apply the settings. Then, ping the host name (domain name) to check that DDNS is configured successfully.

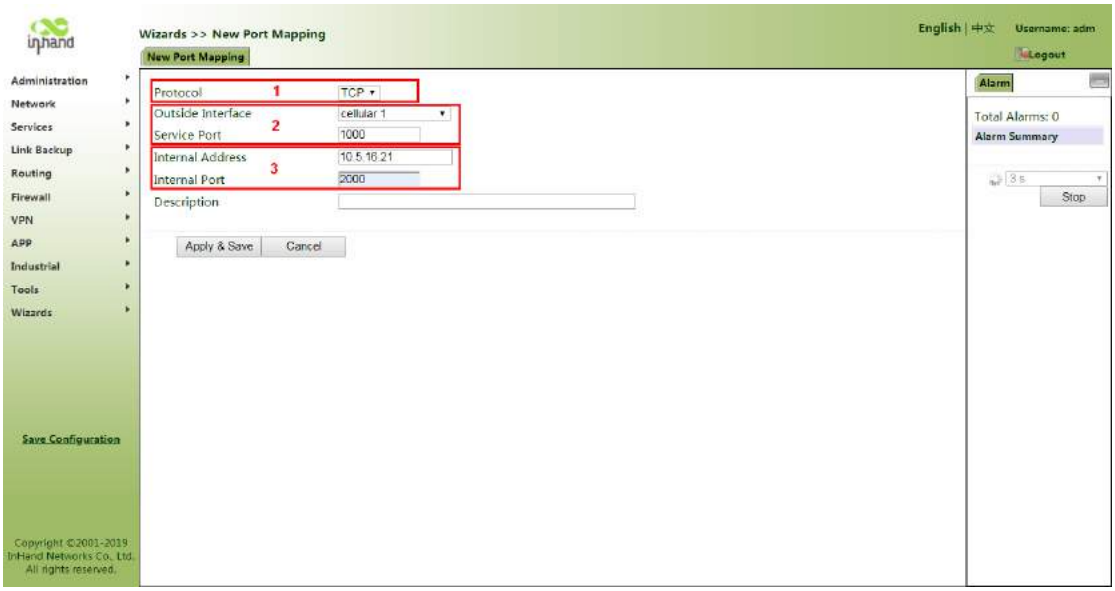
3.5 Port Mapping (NAT)

Port mapping can be configured on the **Wizards** and **Firewall** pages.

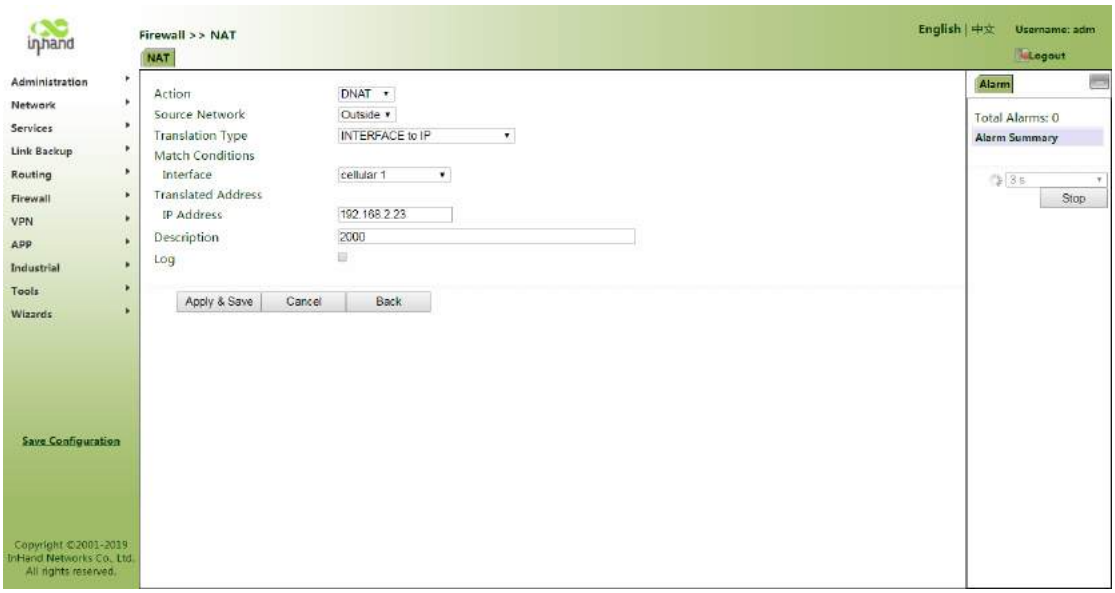
Choose **Wizards** > **New Port Mapping** to configure the gateway to access the Internet.

bridge1: bridge interface; **Cellular 1**: SIM dial-up interface; **Gigabitethernet0/1**: WAN port.

As shown in the following figure, port 1000 of Cellular 1 is mapped to port 2000 with the IP address 10.5.16.21. The public server with the IP address 10.5.16.21 can be accessed through the gateway's Cellular 1 port.



Choose **Firewall** > **NAT**. Configure Internet access through dial-up. Port GE 0/2 is connected to the server with the IP address 192.168.2.23. Configure the gateway to access the server through the public network.

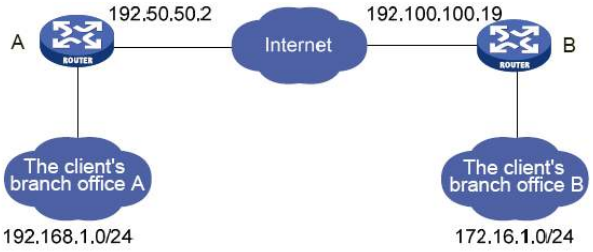


3.6 VPN Application

3.6.1 Point-to-Point IPsec VPN Configuration

Establish a security tunnel between gateways A and B to protect the data flows between the subnet (192.168.1.0/24) for customer branch A and the subnet (172.16.1.0/24) for customer branch B. Configure the use of the Encapsulation Security Protocol (ESP), 3DES encryption algorithm, and SHA authentication algorithm.

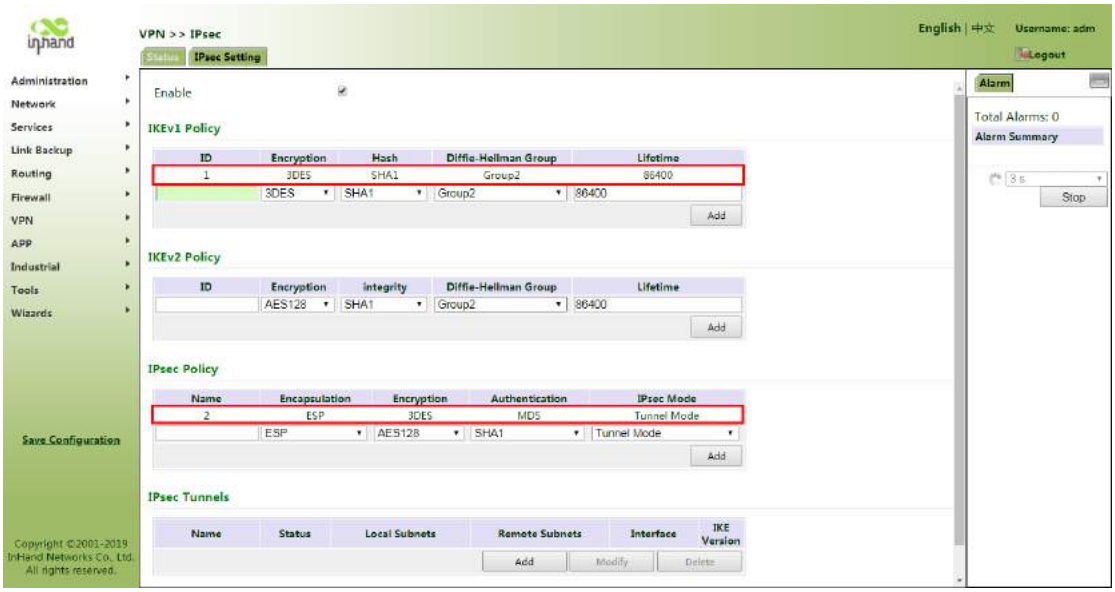
The following figure shows the IPsec VPN topology.



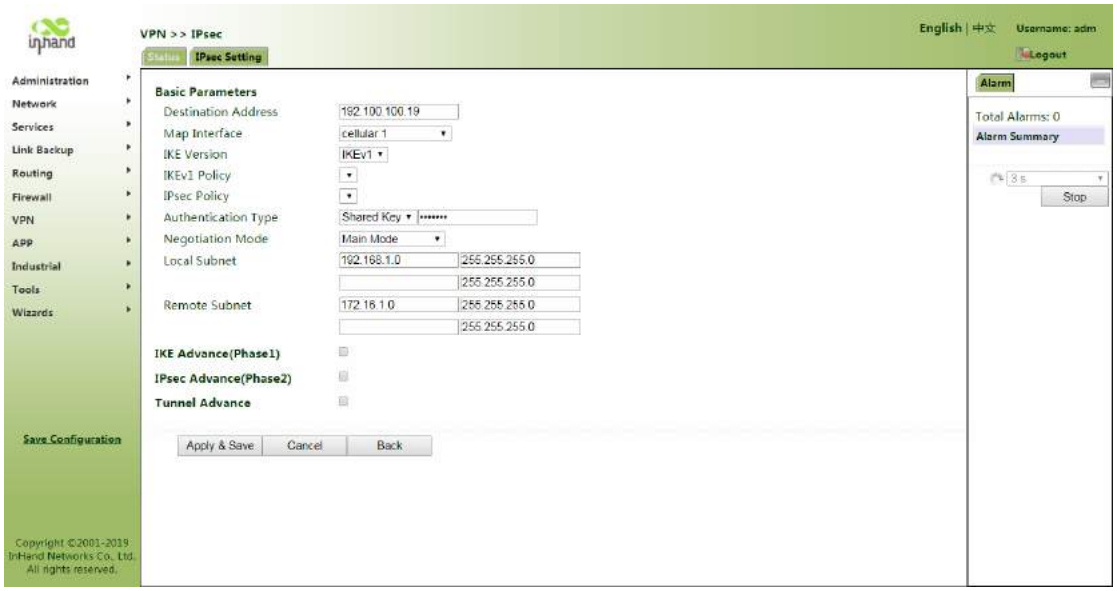
Networking configuration procedure:

(1) Configure gateway A

Step 1: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Set the parameters.



Step 2: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Click **Add** next to **IPsec Tunnel Setting**. Set the parameters on the displayed page, as shown in the following figure.



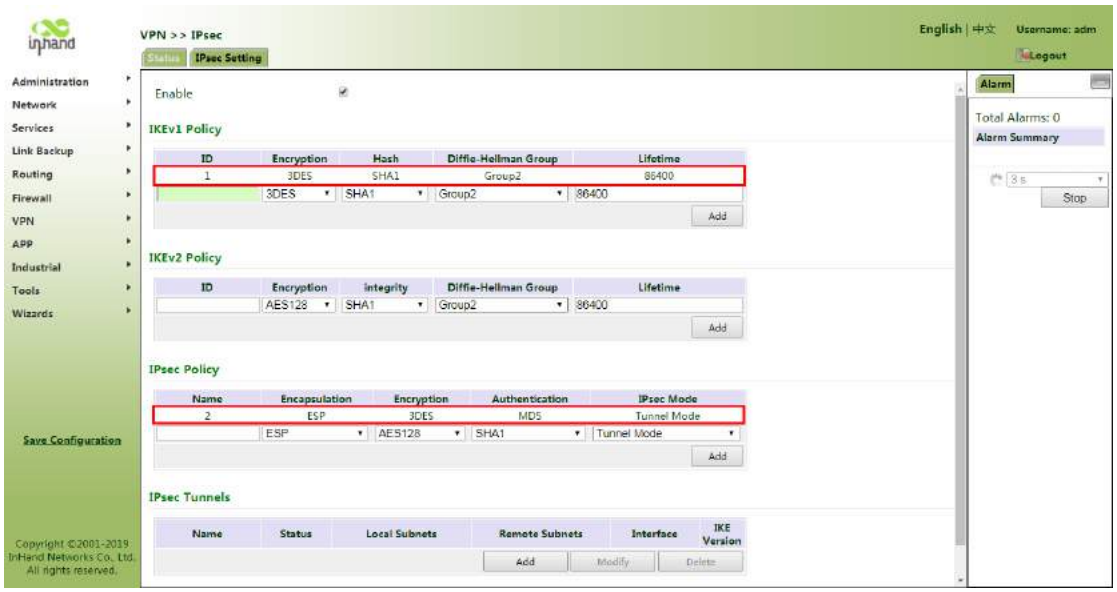
Note:

The local and peer identifier addresses do not need to be set, unless otherwise specified.

IPsec Profile is set only when DMVPN is configured. It does not need to be set when IPsec VPN is created.

(2) Configure gateway B

Step 1: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Set the parameters.

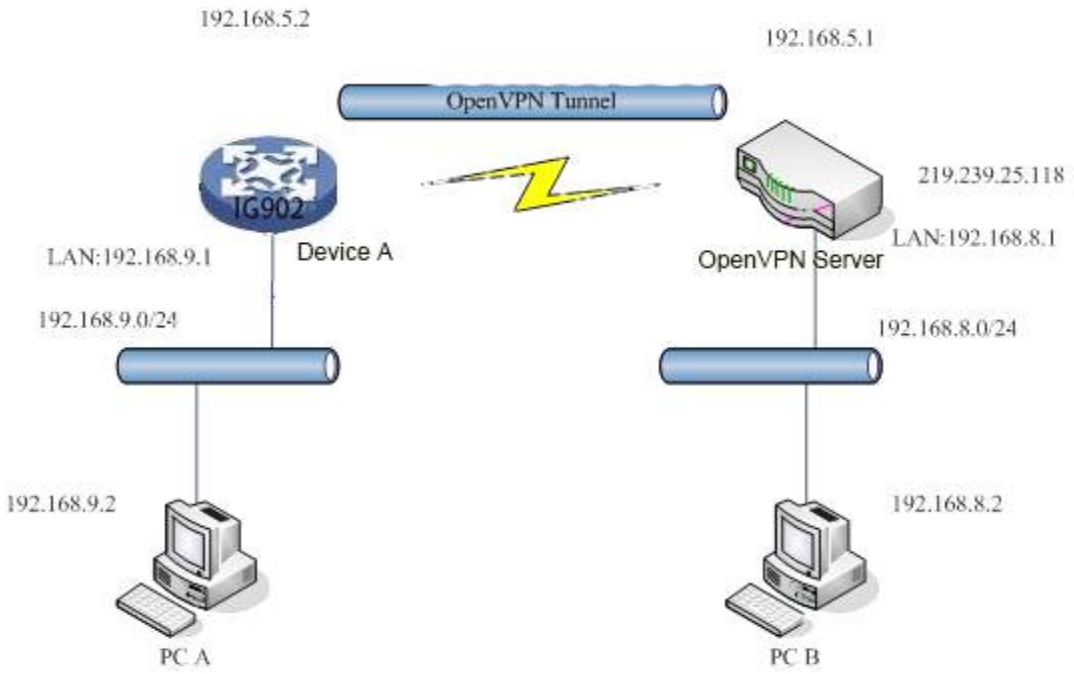


Step 2: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Click **Add** next to **IPsec Tunnel Setting**. Set the parameters on the displayed page.

(3) Check the VPN status
Go to the **Status** page and check that the VPN status is Connected.

3.6.2 OpenVPN

OpenVPN is based on TCP/UDP and applicable to any ports. The following figure shows an example of OpenVPN topology.



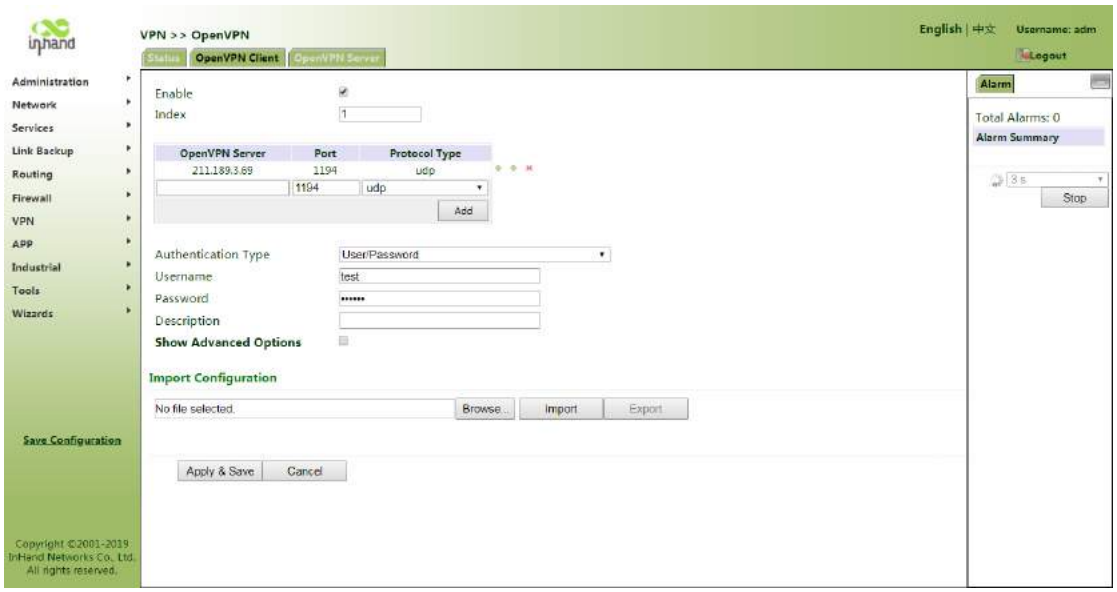
In the preceding figure, an OpenVPN tunnel is established between device A and the OpenVPN server. The virtual IP addresses at both ends of the tunnel are 192.168.5.2 and 192.168.5.1.

A. If OpenVPN of device A is configured as the gateway mode, the packets destined for the 192.168.8.0/24 subnet are forwarded to the OpenVPN tunnel through the gateway and reach the OpenVPN server. Correspondingly, a static gateway must be added on the OpenVPN server so that the packets destined for the 192.168.9.0/24 subnet are forwarded to the OpenVPN tunnel through the gateway. In this way, PC A and PC B are connected through the OpenVPN tunnel and can communicate with each other.

B. If OpenVPN of device A is configured as the NAT mode, the static gateway 192.168.9.0/24 does not need to be added on the OpenVPN server. With this configuration, PC A can access PC B, but PC B cannot access PC A directly. This configuration is applicable to active uploading.

Configure the gateway as follows:

Step 1: Set the OpenVPN parameters of the device.



Step 2: Complete certificate configuration based on the specific authentication type after a tunnel is established. The mapping between authentication types and certificates is as follows:

None: No certificates are required.

Pre-shared Key: No certificates are required.

User/Password: Only the CA certificate is required, such as **ca.crt**.

X.509 Cert (multi-client), X.509 Cert: The CA certificate and the device's public and private key certificates are required, such as **ca.crt**, **my.crt**, and **my.key**.

Note:

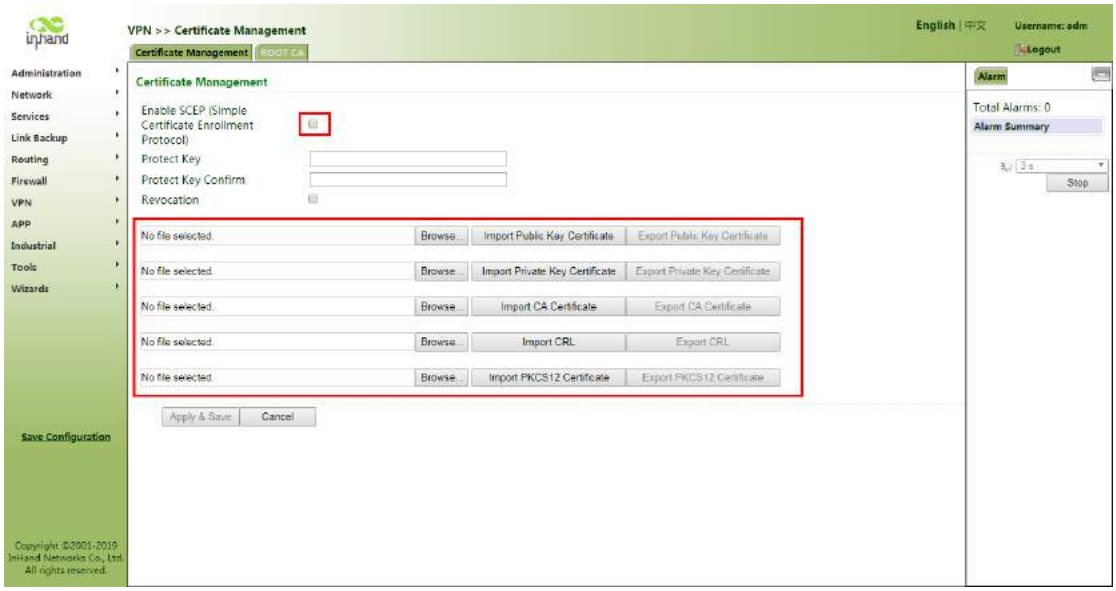
1. The file names of the CA certificate and public key certificate are suffixed with **.crt**, and the file name of the private key certificate is suffixed with **.key**.

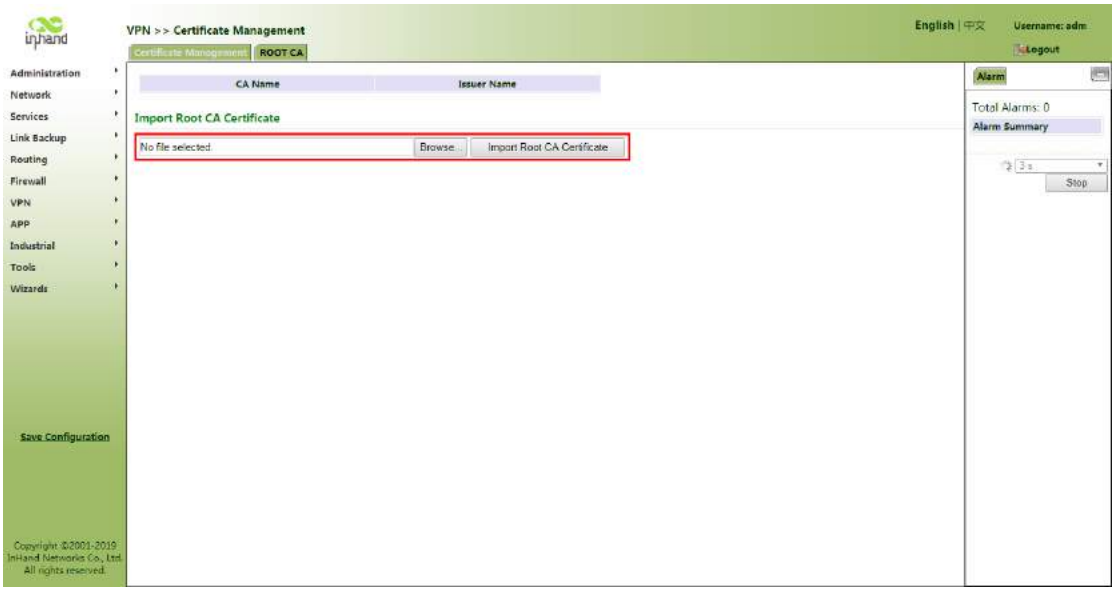
2. The system time of the device must be accurate when the certificate feature is used.

Step 3: Configure the OpenVPN server. Add a static gateway with a route destined for 192.168.2.0/24 by running **route add -net 192.168.2.0 netmask 255.255.255.0 dev tun0**. Assume that the network port of the OpenVPN server is tun0.

3.6.3 Certificate Management

On the **Certificate Management** page, you can import VPN certificates. If no local certificates are available, select **Enable SCEP (Simple Certificate Enrollment Protocol)** to apply for a certificate online.

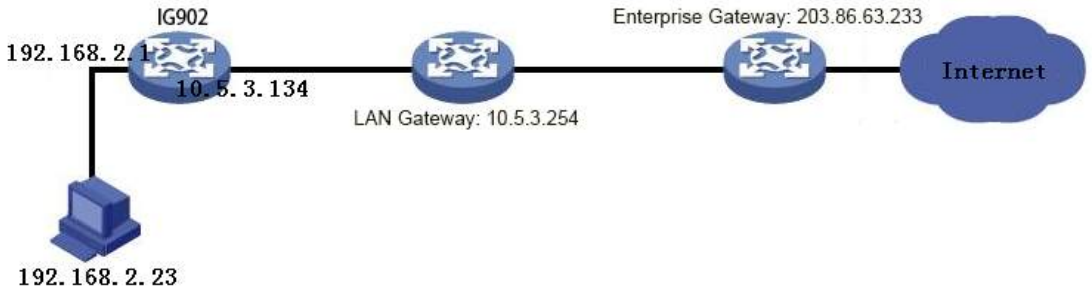




3.7 Link Backup

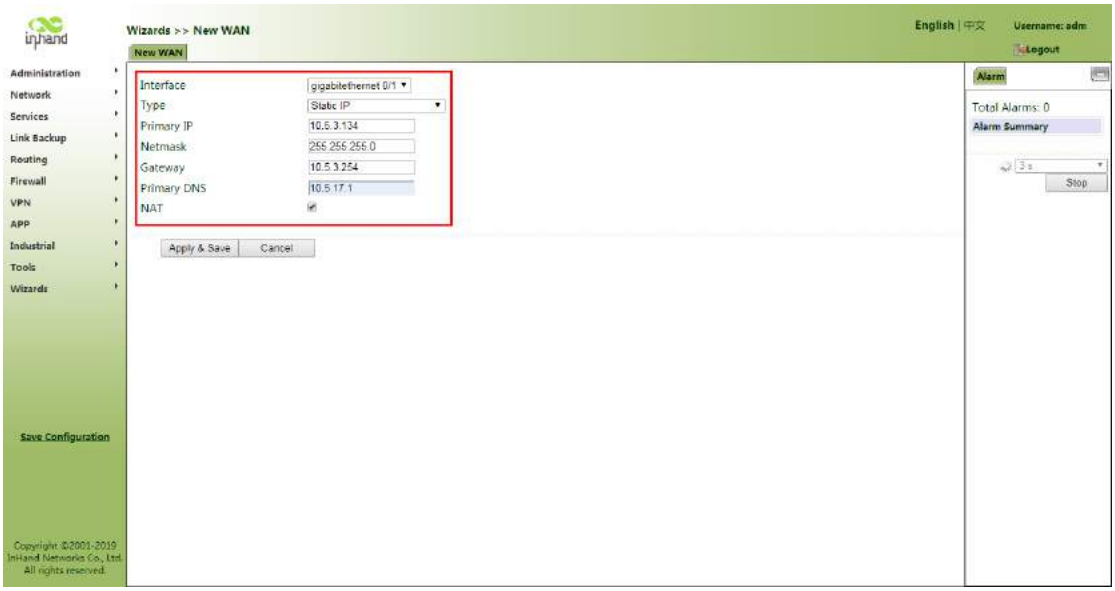
3.7.1 Interface Backup

You can configure interface backup to enable the gateway to access the Internet through dial-up even when the wired network is faulty. The following figure shows the topology of interface backup.

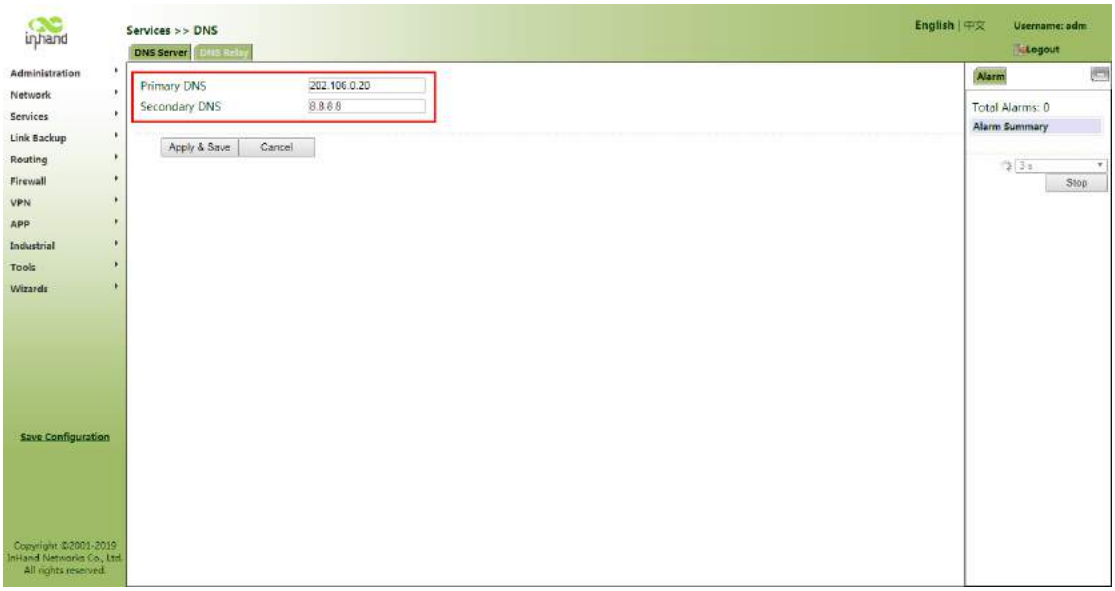


Configure the gateway as follows:

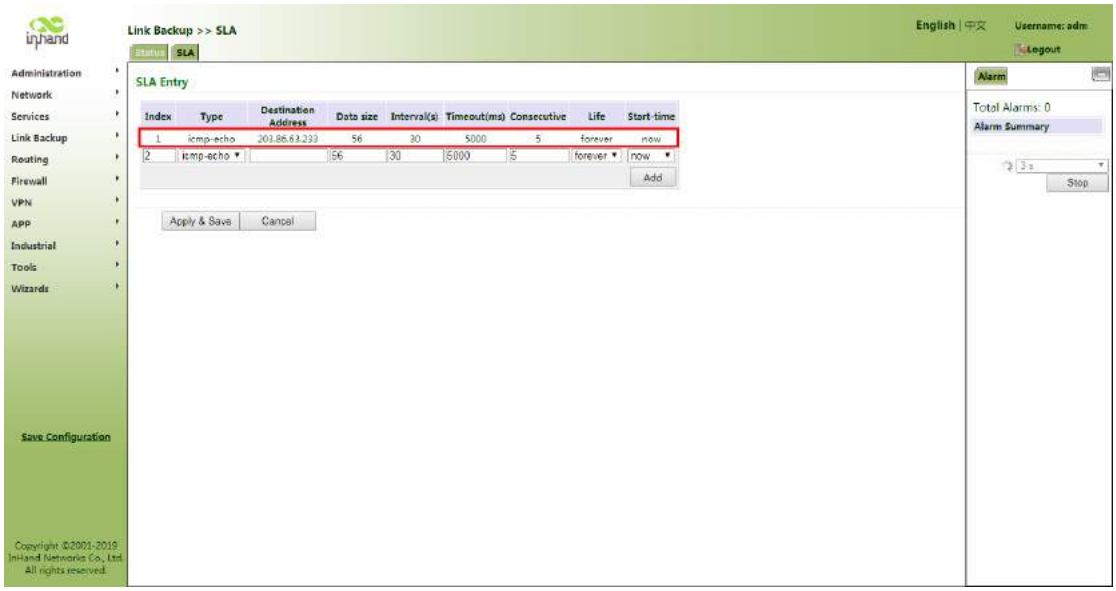
Step 1: Choose **Wizards** > **New WAN** to set the parameters of Internet access in wired mode.



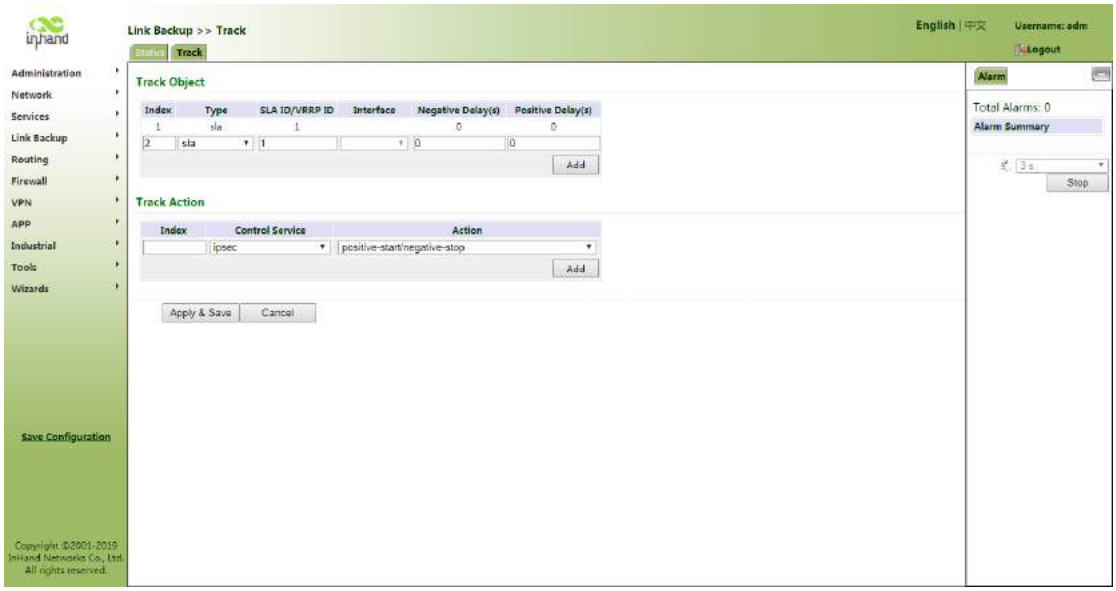
Step 2: Choose **Services** > **DNS** > **DNS Server** to set corresponding parameters. Check that the PC can access the Internet after configuration.



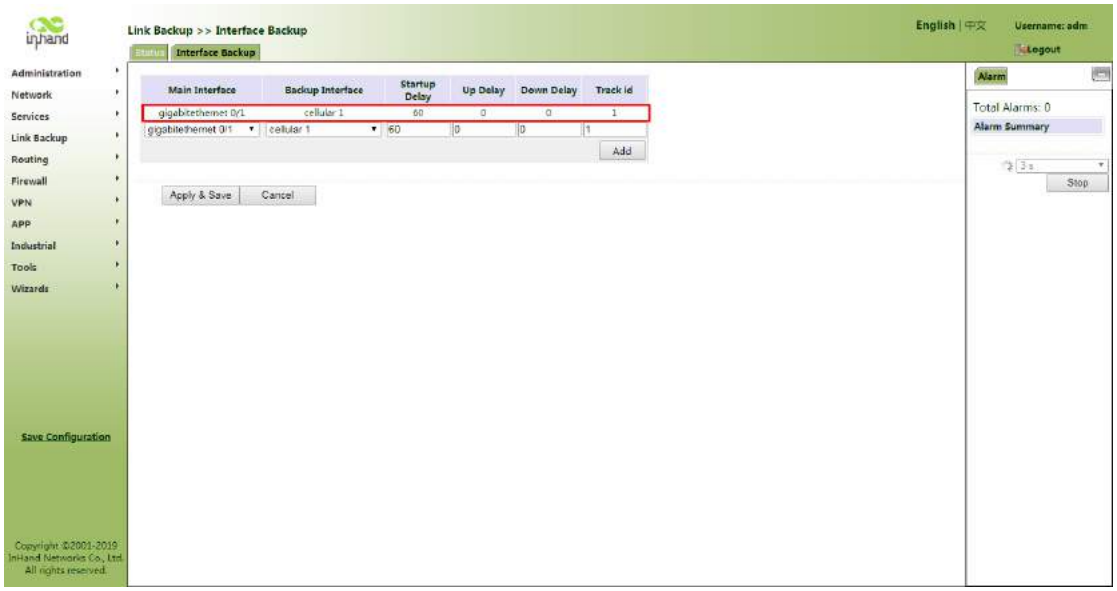
Step 3: Choose **Link Backup** > **SLA** to set corresponding parameters. Set the IP address to a public or private IP address that supports ICMP detection. For example, 203.86.63.233 is the IP address of the enterprise gateway for the PC.



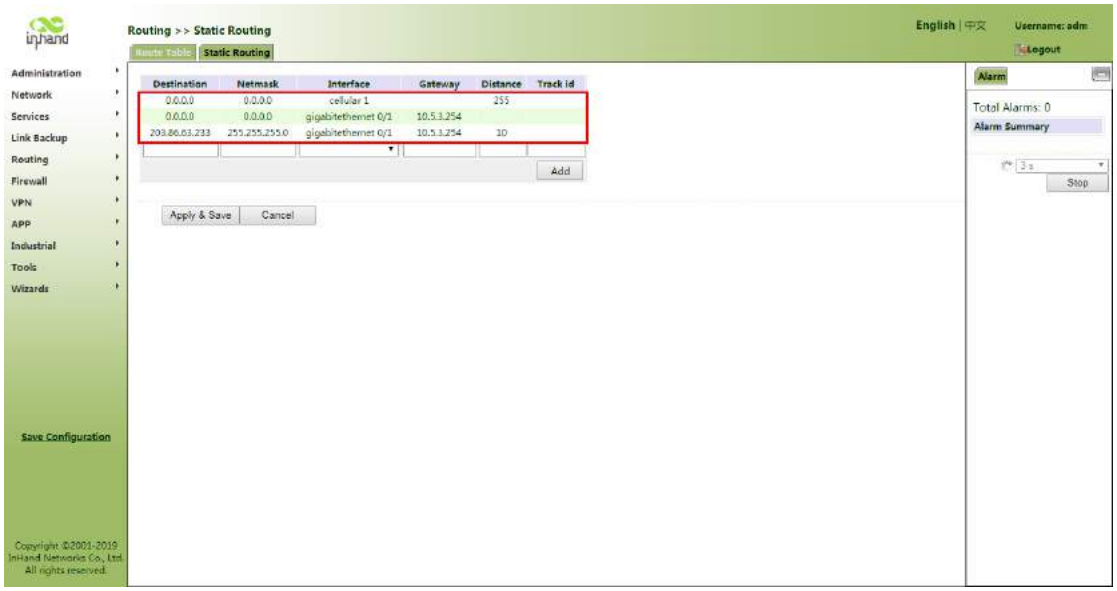
Step 4: Choose **Link Backup** > **Track** to set corresponding parameters.



Step 5: Choose **Link Backup** > **Interface Backup** to set corresponding parameters.



Step 6: Choose **Routing** > **Static Routing** to set corresponding parameters. Add three routes. 10.5.3.234 is the IP address of the LAN route for the PC. The distance parameter indicates the priority. The smaller the parameter value, the higher the priority.



Step 7: Disconnect the network cable to simulate a wired network fault. In this case, the gateway accesses the Internet through dial-up on the cellular port. Then, reconnect the network cable so that the gateway accesses the Internet through the wired network.

3.7.2 VRRP Hot backup

Several gateways are connected to the same network. Host A backs up gateway A. When gateway A is faulty, gateway B takes over the services on the faulty gateway to work as the host temporarily.

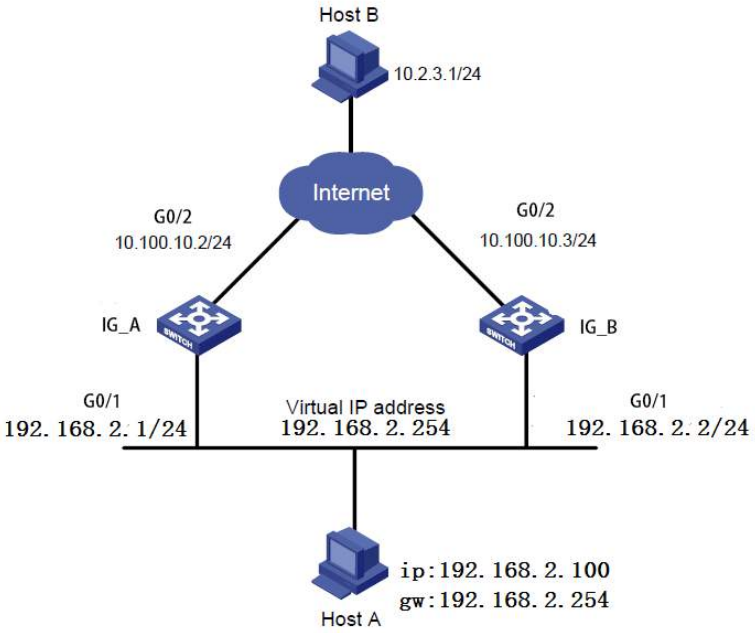
1. Networking requirements

Gateways A and B form a VRRP backup group, which is the default gateway used by host A to access host B on the Internet.

Structure of the VRRP backup group:

- The group number is 1.
- The IP address of the virtual gateway in the backup group is 192.168.2.254/24.
- Switch A is the master switch.
- Switch B is the backup switch and supports preemption.

2. Networking diagram

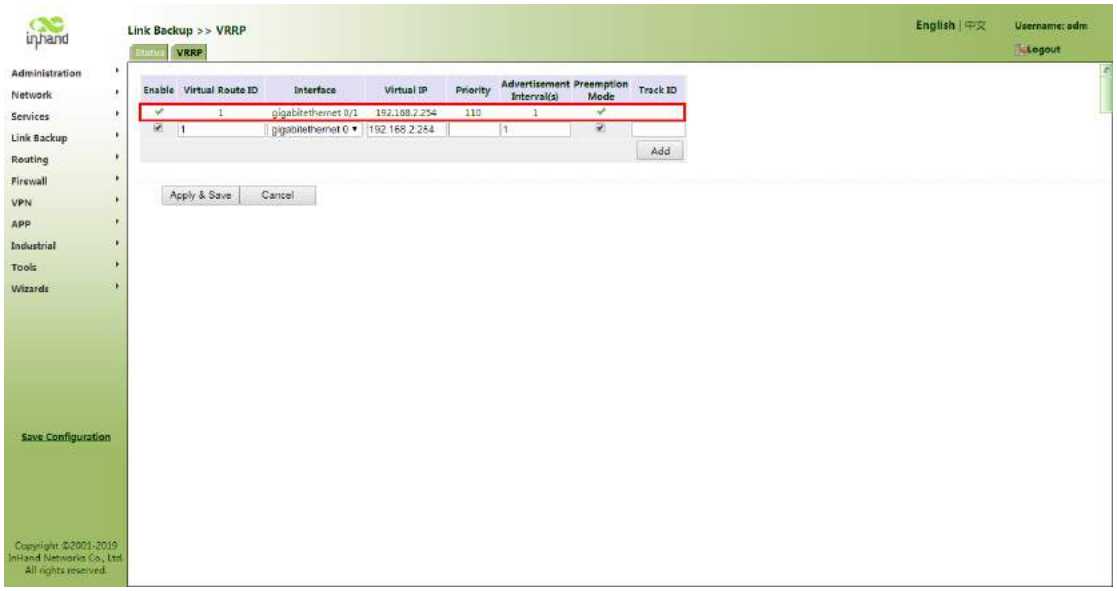


3. Configuration procedure

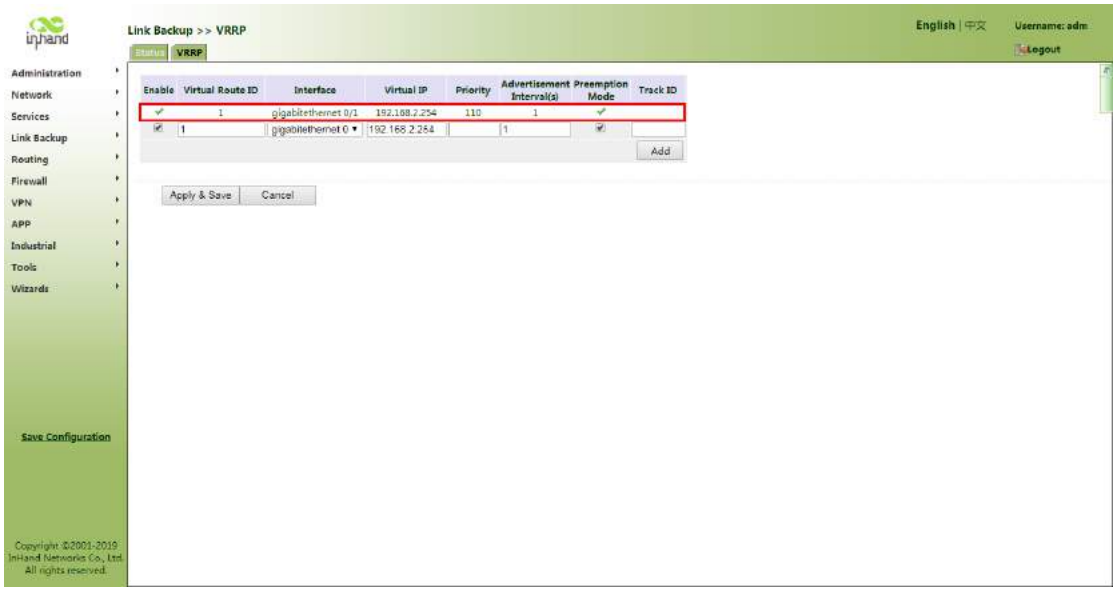
(1) Configure gateway A

Step 1: Configure G0/1.

Choose **Link Backup** > **VRRP** from the navigation tree and click the **VRRP** tab to configure VRRP.

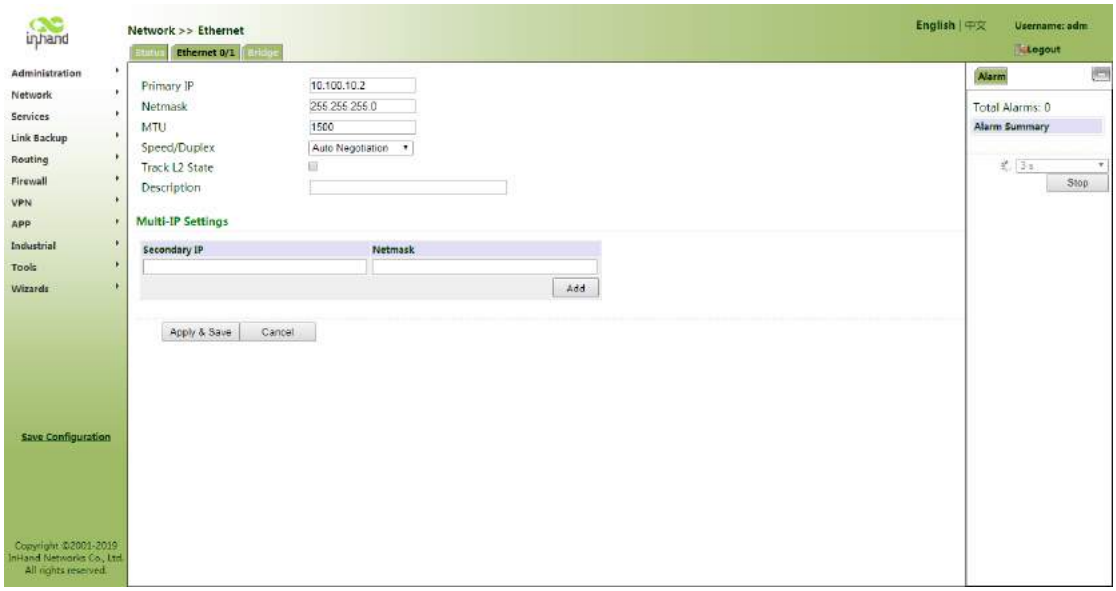


Choose **Link Backup** > **VRRP** from the navigation tree and click the **Status** tab to check the VRRP status.



Step 2: Configure G0/2.

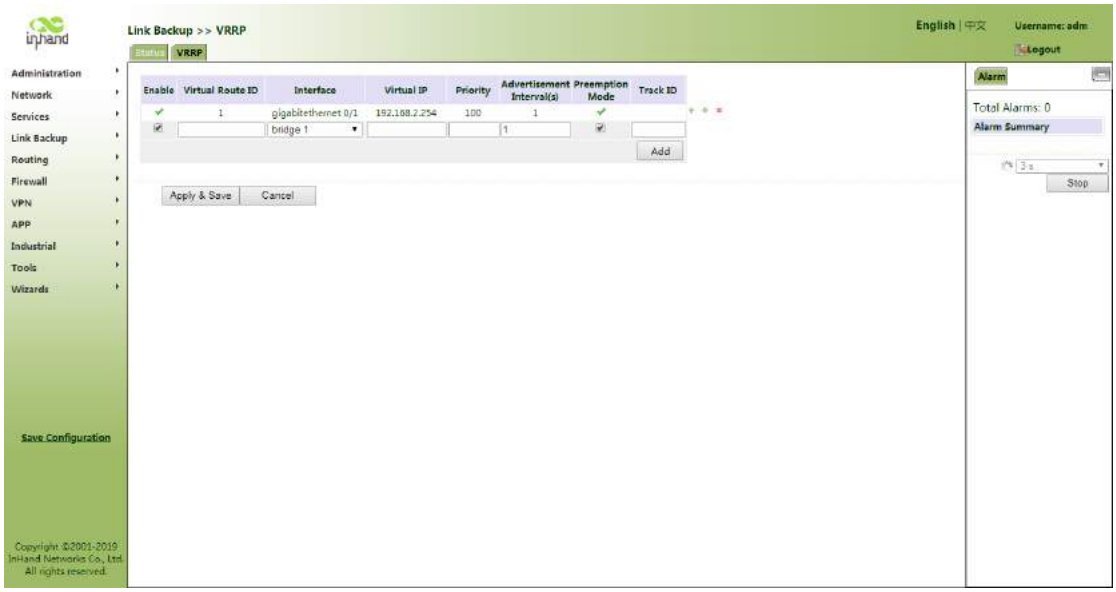
Choose **Network** > **Ethernet** from the navigation tree and click the **Ethernet 0/2** tab to configure the Ethernet port 0/2.



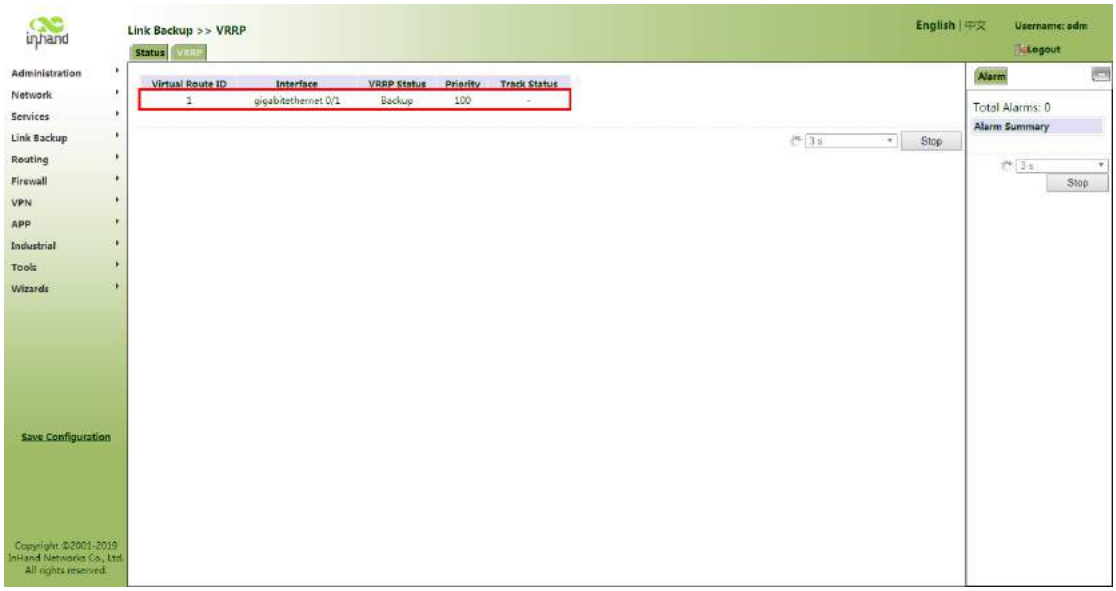
(2) Configure gateway B

Step 1: Configure G0/1.

Choose **Link Backup** > **VRRP** from the navigation tree and click the **VRRP** tab to configure VRRP.

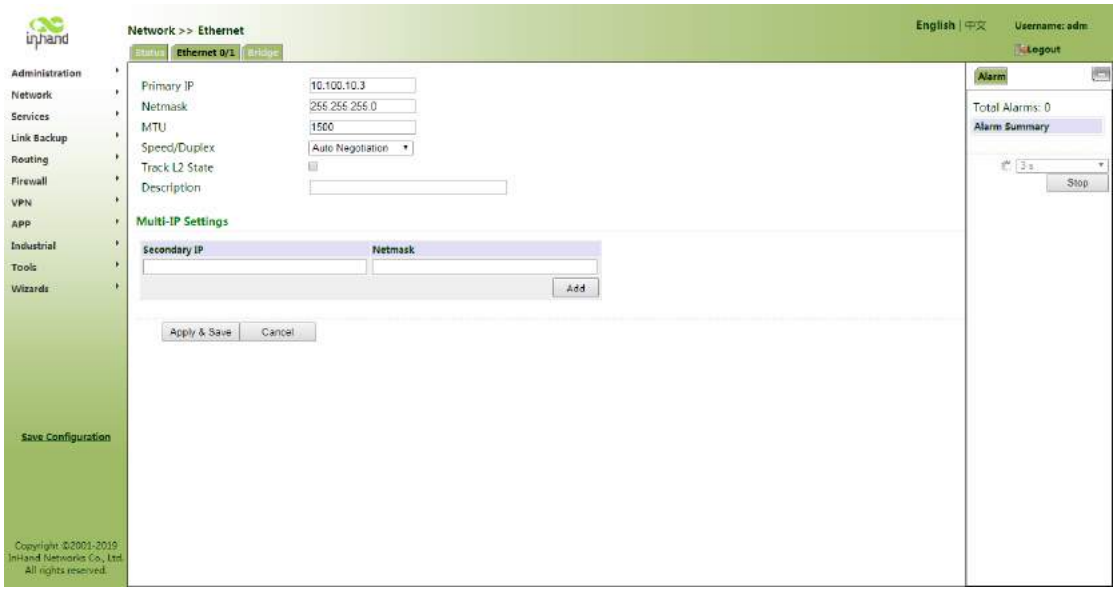


Choose **Link Backup** > **VRRP** from the navigation tree and click the **Status** tab to check the VRRP status.



Step 2: Configure G0/2.

Choose **Network** > **Ethernet** from the navigation tree and click the **Ethernet 0/2** tab to configure the Ethernet port 0/2.



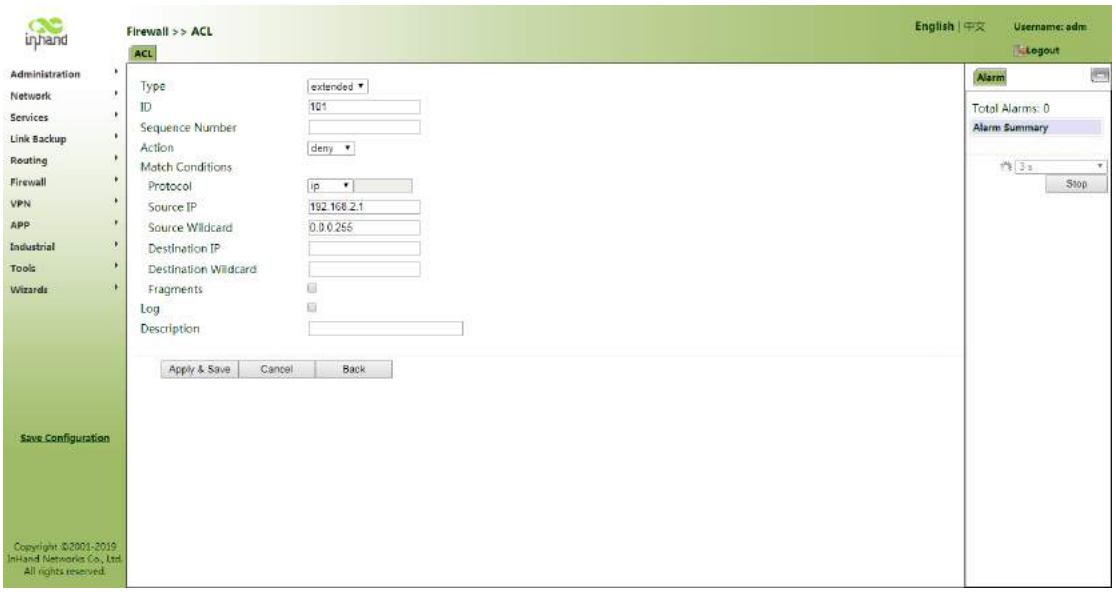
Set the IP address of the default gateway for host A to 192.168.2.254, In normal cases, gateway A is in the running state. When it is powered off or faulty, gateway B takes over the services on gateway A. The preemption mode allows gateway A to assume the master role when it is restored.

3.8 Access Control List (ACL)

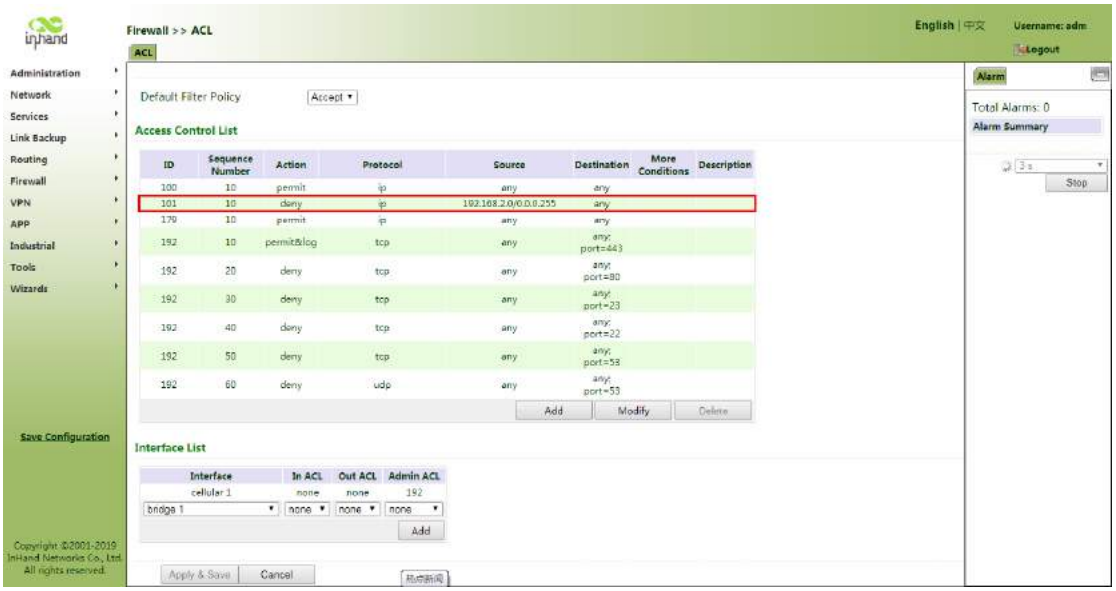
You can control the gateway to allow or prohibit access to network ports.

Configure the gateway as follows:

Step 1: Open the **ACL** page and click **Add** to add an access control list (ACL) and set parameters.



Step 2: Click **Apply & Save**. The information about the new ACL with the ID 101 is displayed on the page.



Step 3: In **Interface List**, select **cellular1** for **Interface** and **101** for **Out ACL**. Click **Add** and save the settings.


Firewall >> ACL
English | 中文
Username: adm
Logout
ACL
Administration
Network
Services
Link Backup
Routing
Firewall
VPN
APP
Industrial
Tools
Wizards
Save Configuration
Default Filter Policy
Accept
Access Control List
ID
Sequence Number
Action
Protocol
Source
Destination
More Conditions
Description
100 10 permit ip any any
101 10 deny ip 192.168.2.0/0.0.0.255 any
179 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
Add
Modify
Delete
Interface List
Interface
In ACL
Out ACL
Admin ACL
cellular 1 none 101 none
bridge 1 none none none
Add
Apply & Save
Cancel
Alarm
Total Alarms: 0
Alarm Summary
3 s
Stop
Copyright ©2001-2019 InHand Networks Co., Ltd. All rights reserved.

4 Basic System Settings

4.1 User Management

Choose **Administration** > **User Administration** and click the **User Administration** tab. You can create and delete users and change your password.

Two user types are provided: superuser and common user.

- Only one superuser is provided and automatically created by the system. It has all the access permissions on the gateway. The superuser name is **adm**, and its default password is **123456**.
- Common users are created by the superuser and have the permission to view the gateway configuration, but cannot modify it.

User permissions are classified into three levels:

- Users of permission levels 1 to 11 can only view parameters but cannot set parameters.
- Users of permission levels 12 to 14 can configure the Ethernet interface LAN address, system time, static routes, basic firewall settings, virtual IP address mapping, system logs, and access control, apply for certificates, and upgrade the system.
- Users of permission level 15 can view and set all parameters.

Note:

The user name of the superuser (**adm**) cannot be modified, and the superuser cannot be deleted. However, its password can be changed.

4.2 System Time

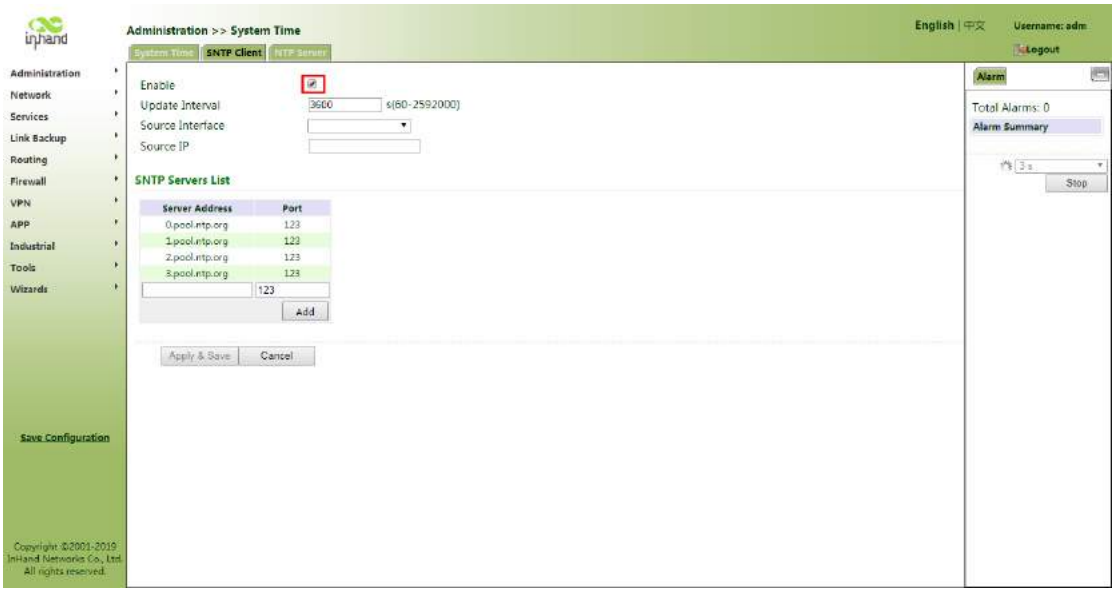
You need to set the system time of the gateway accurately so that the gateway can coordinate with other devices.

Manual time synchronization: Choose **Administration** > **System Time** and click the **System Time** tab. Set time synchronization between the gateway and the connected host. Alternatively, set the system time of the gateway and select the time zone where the gateway is located. You only need to click **Sync Time** for manual time synchronization.

Automatic time synchronization: Choose **Administration** > **System Time**, select **SNTP** or **NTP**, and select **Enable** to configure clock synchronization for all the devices in the network so that the gateway can provide multiple applications based on unified time.

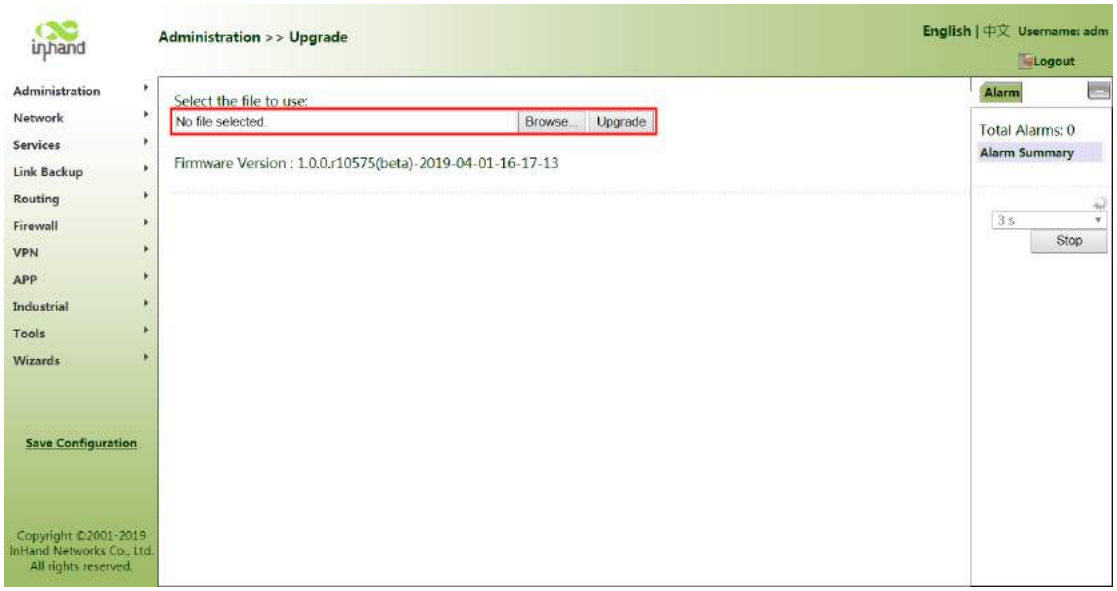
SNTP is the simplified version of NTP. After SNTP is enabled, the gateway synchronizes the local time with the downstream device. SNTP is typically enabled for automatic time synchronization for InHand devices.

After NTP is enabled, the gateway assumes the client or server function to synchronize the time of all the other devices in the network.



4.3 System Upgrade

Choose **Administration** > **Upgrade**, click **Browse**, select an upgrade file, and click **Upgrade**.

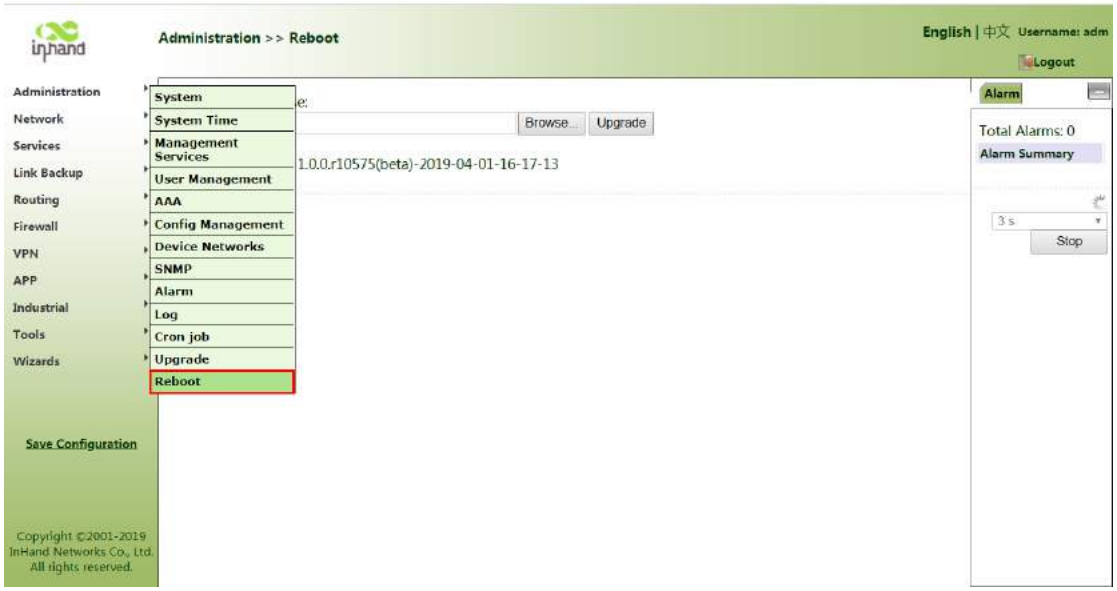


Note:

Do not perform any operations on the web interface during software upgrade; otherwise, the upgrade may be interrupted.

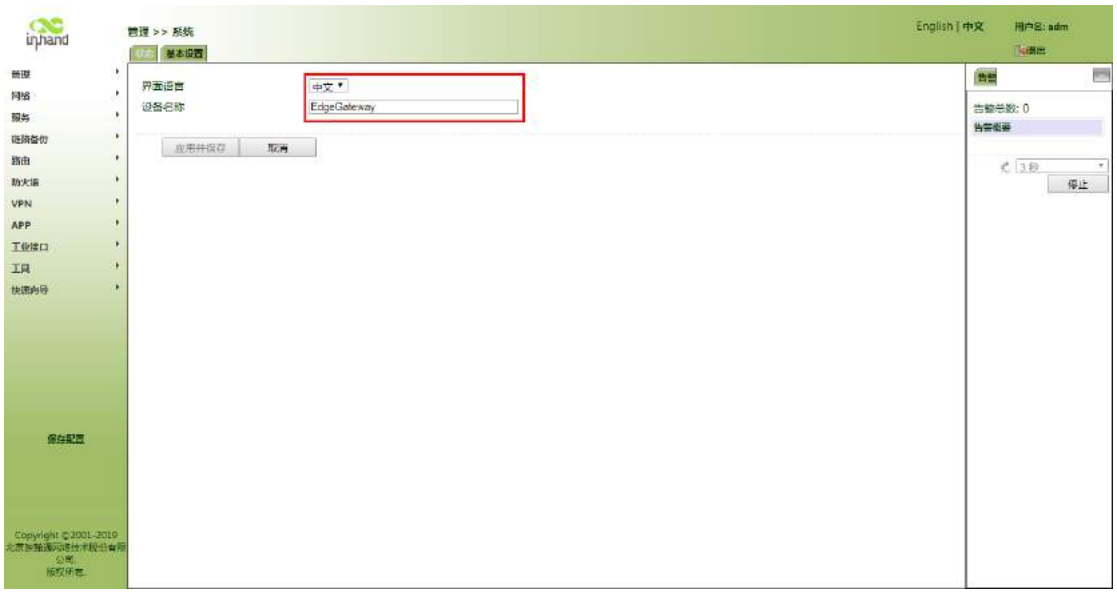
4.4 System Restart

Choose **Administration** > **Reboot** and click **OK**. You can restart the system when the gateway module is not found on the web interface.



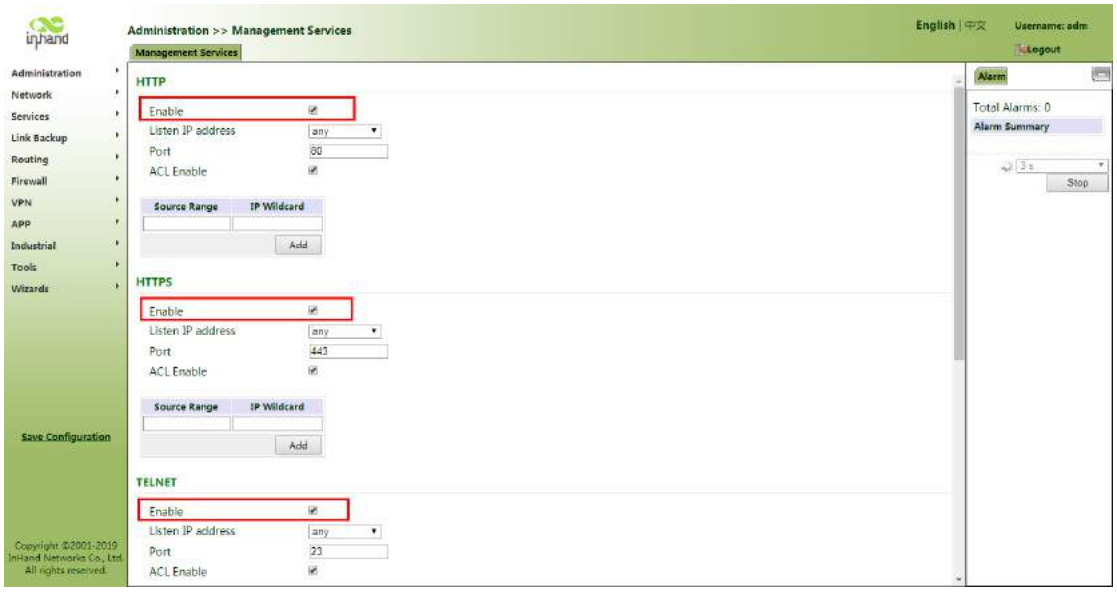
4.5 Changing the Language and Gateway Name

Choose **Administration** > **System** > **Basic Settings** to change the system language and gateway name.



4.6 Management Services

When the gateway requires the HTTP, HTTPS, Telnet, and SSH functions, you need to enable the functions on the **Administration** > **Management Services** page of the web interface.

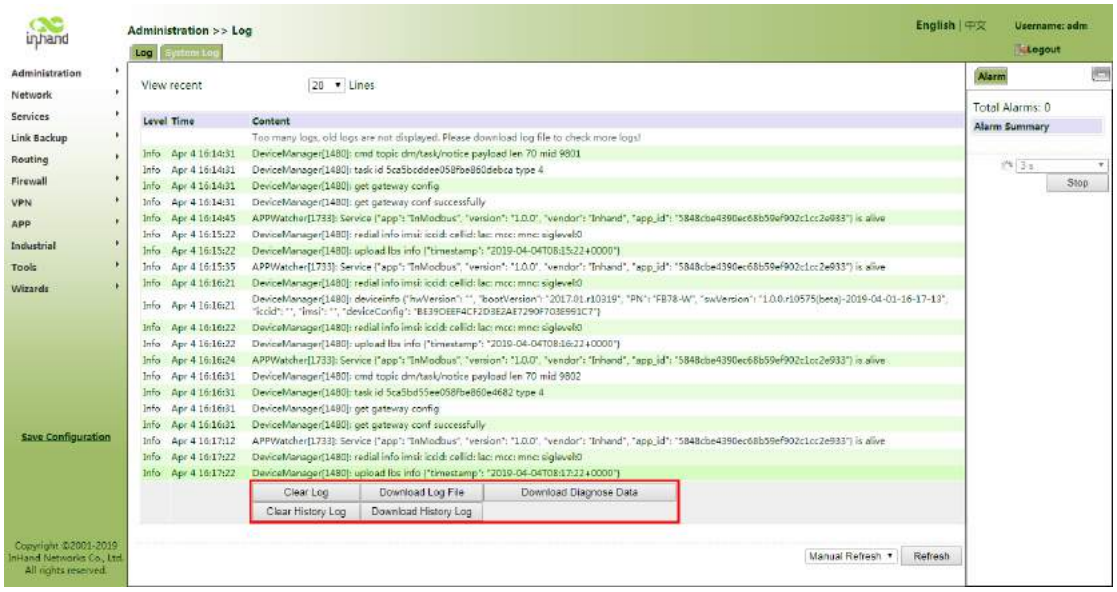


4.7 Checking System Logs

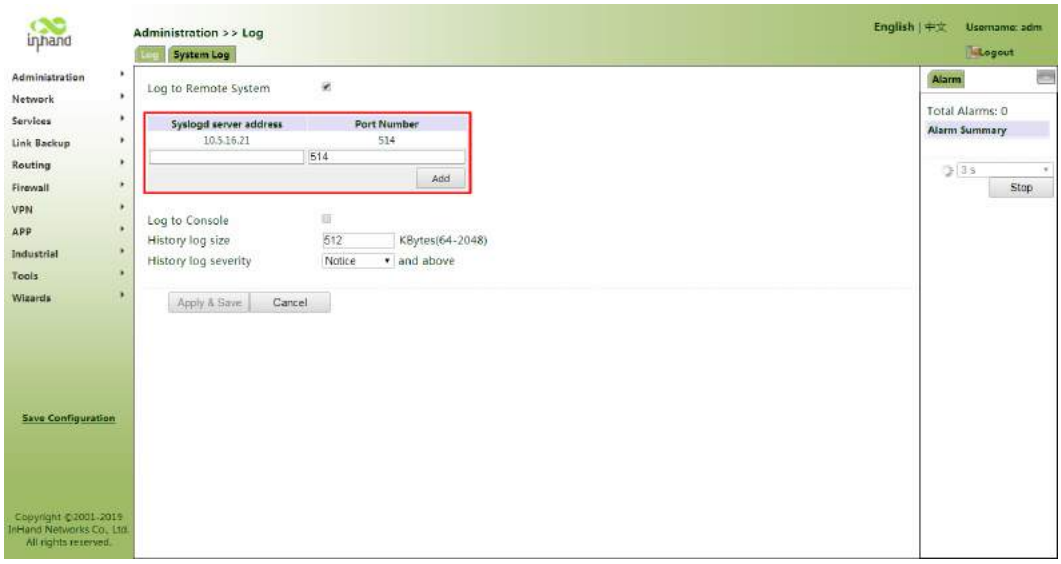
Choose **Administration** > **Log** to check system logs.

On this page, you can also clear and download logs, including historical logs. Historical logs are those logs with a long storage period specified on the **System Log** page.

The system diagnosis record file is encrypted and can be viewed only after being decrypted using the decryption tool provided by InHand. The gateway configuration is downloaded along with the system diagnosis record.



The gateway provides a limited storage capacity, which is 512 KB by default. You need to use a remote log service, such as Kiwi Syslog Daemon, to save all log information. To obtain the software, you can contact InHand Sales Support or download it from the Internet. After you set the address and port of the log server on the web interface, the gateway uploads all system logs to the remote log server.



4.8 Alarm

The alarm function notifies you of any gateway errors promptly. The gateway reports an alarm when an error occurs. You can select predefined error types and a proper notification method to obtain error information. All alarms are recorded in alarm logs, allowing you to locate and fix errors as soon as possible.

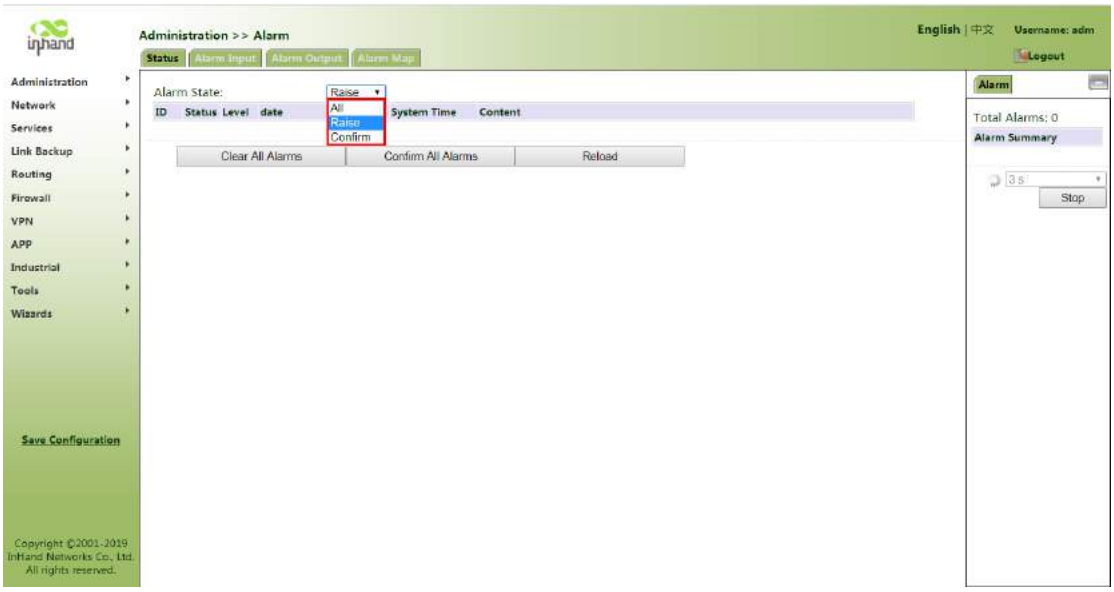
(1) Choose **Administration** > **Alarm** > **Status** to view all alarms generated in the system since power-on.

Alarms have the following states:

- Raise: indicates that the alarm is generated but not confirmed.
- Confirm: indicates that the alarm cannot be cleared currently.
- All: indicates all generated alarms.

Alarms are classified into the following levels:

- EMERG: The gateway encounters a serious error that may cause a system reboot.
- CRIT: The gateway encounters an unrecoverable error.
- WARN: The gateway encounters an error that affects system functions.
- NOTICE: The gateway encounters an error that affects system performance.
- INFO: A normal event occurs.

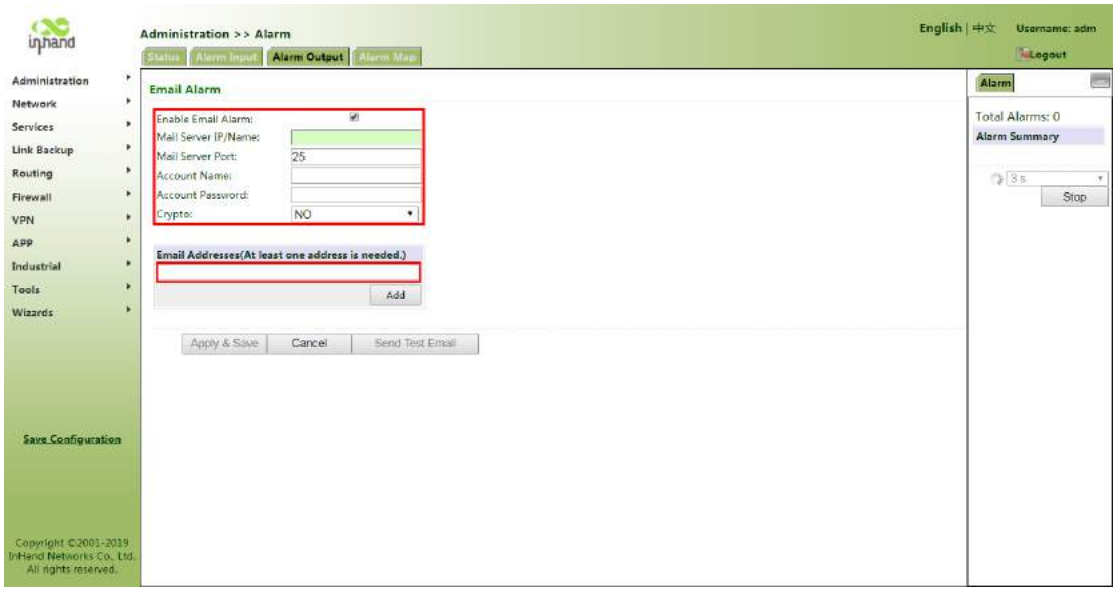


(2) **Alarm Input**: Select the desired alarm type. An alarm is generated when an error of the selected type occurs.

(3) **Alarm Output**: When an alarm is generated, the system automatically sends the alarm content to the target email address. This function is unavailable for common users.

Enter information about the sender's email address in **Email Alarm**, and enter information about the receiver's email address in **Email Addresses**.

Mail Server IP/Name can be determined by searching the Internet. For example, if Tencent Exmail is used, enter **smtp.exmail.qq.com**.



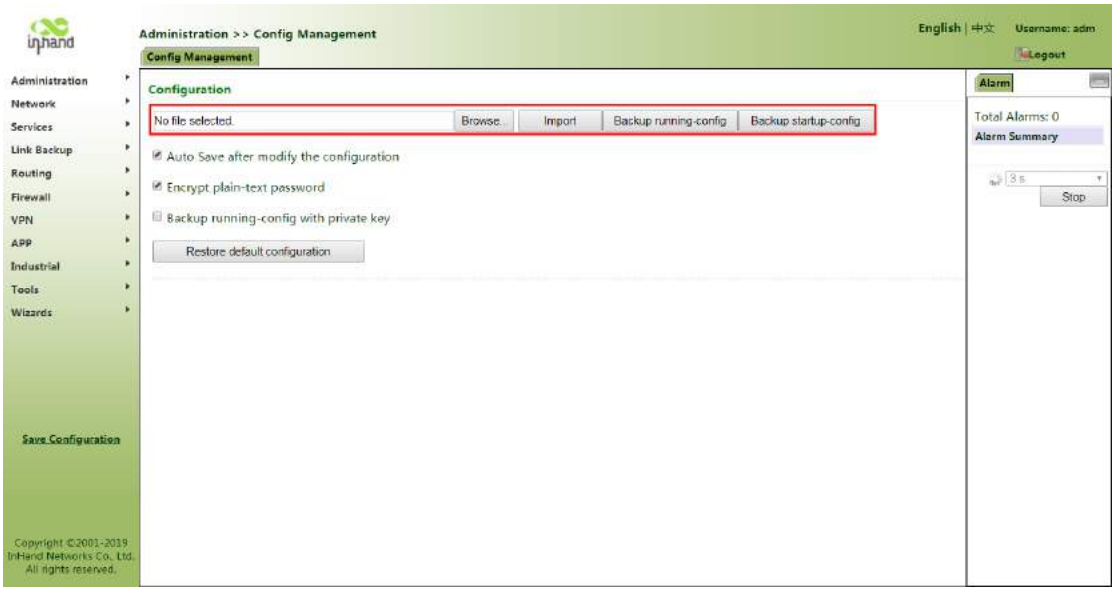
(4) **Alarm Mapping**: You can select CLI (console port) or email for receiving alarms. To enable email mapping, you need to enable it on the **Alarm Output** tab page and set an email address.

4.9 Configuration Import and Backup

Choose **Administration** > **Config Management**, click **Browse**, select a configuration file, and click **Import** to import the configuration file to the gateway.

Click **Back Up running-config** to back up the current runtime configuration to the PC. This is a common operation.

Click **Back Up startup-config** to back up the boot file to the PC.



4.10 Restoring Default Settings

4.10.1 Webpage Mode

Choose **Administration** > **Config Management** and click **Restore Default**. The default settings are restored after the system restarts.

4.10.2 Hardware Mode

Restore the default settings in hardware mode as follows:

Step 1: Find the **RESET** button on the gateway panel.

Step 2: Press and hold the **RESET** button for 10 seconds after the gateway is powered on.

Step 3: Release the **RESET** button when the ERR indicator is in red.

Step 4: Press and hold the **RESET** button for 1 second when the ERR indicator is off.

Step 5: Check whether the ERR indicator blinks three times and then turns off. If yes, the default settings are restored successfully.

5 Connecting the Gateway to a Cloud Platform

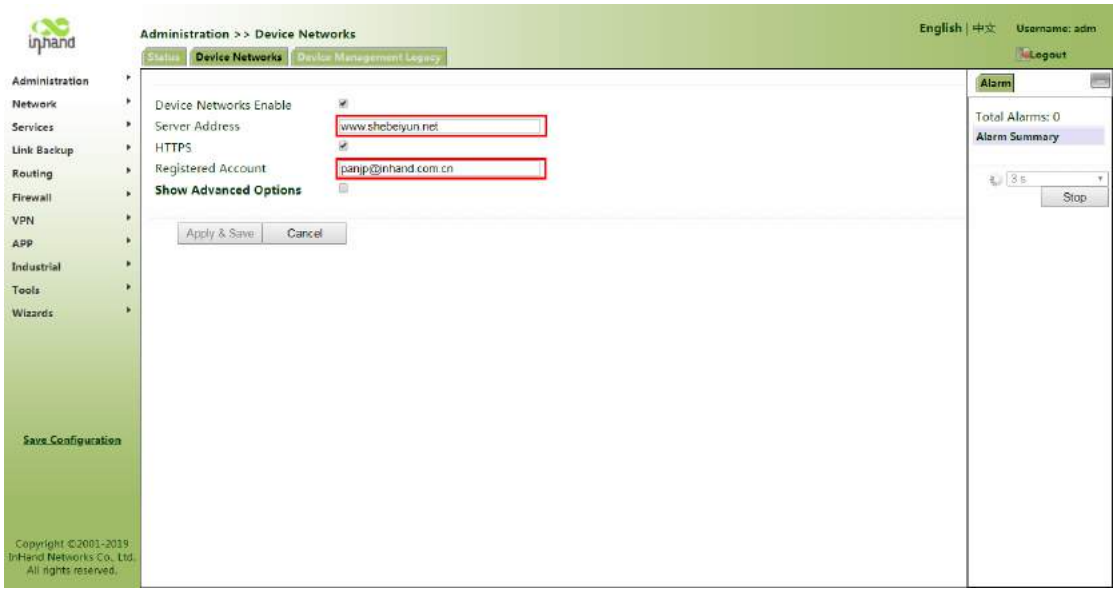
Two connection protocols are supported: Message Queue Telemetry Transport (MQTT, applicable to the **remote device monitoring platform**) and Open Virtual Device Protocol (OVDP, applicable to the **gateway platform**). The remote device monitoring platform is recommended because it allows the gateway to be automatically added on the cloud platform. Either of the two platforms can be selected for connection.

1) Using the remote device monitoring platform

Procedure:

Step 1: Choose **Administration** > **Device Networks**, click the **Device Networks** tab, and select **Device Networks Enable**. Enter the cloud platform address and the account that registers the cloud platform. Click **Apply & Save**.

Step 2: Log in to the cloud platform to add the gateway.

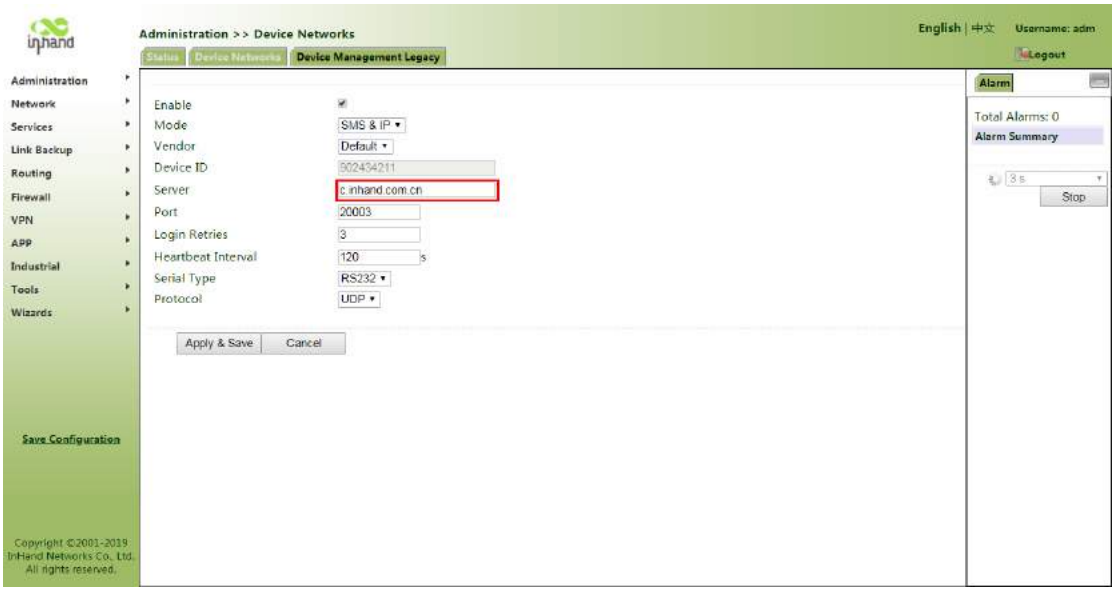


2) Using the gateway platform

Procedure:

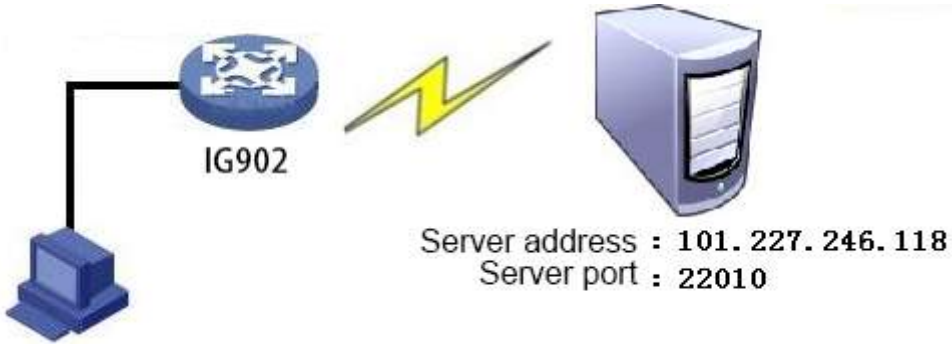
Step 1: Choose **Administration** > **Device Networks**, click the **Device Management Legacy** tab, and select **Enable**. Enter the cloud platform address and click **Apply & Save**.

Step 2: Log in to the cloud platform to add the gateway.


Administration >> Device Networks
English | 中文
Username: adm
Logout
Status
Device Networks
Device Management Legacy
Administration
Network
Services
Link Backup
Routing
Firewall
VPN
APP
Industrial
Tools
Wizards
Save Configuration
Copyright ©2001-2019 InHand Networks Co. Ltd. All rights reserved.
Enable
Mode
SMS & IP
Vendor
Default
Device ID
502434211
Server
c.inhand.com.cn
Port
20003
Login Retries
3
Heartbeat Interval
120
s
Serial Type
RS232
Protocol
UDP
Apply & Save
Cancel
Alarm
Total Alarms: 0
Alarm Summary
3 s
Stop

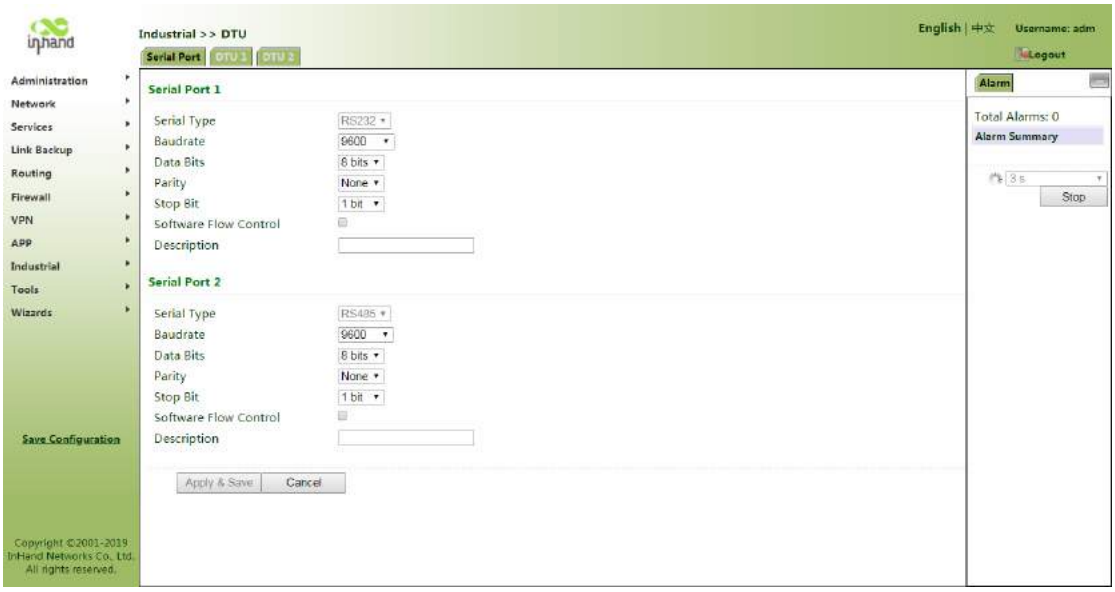
6 Industrial Interface (DTU)

Set the gateway's DTU function to enable the gateway to communicate with the server. The following figure shows the related topology.

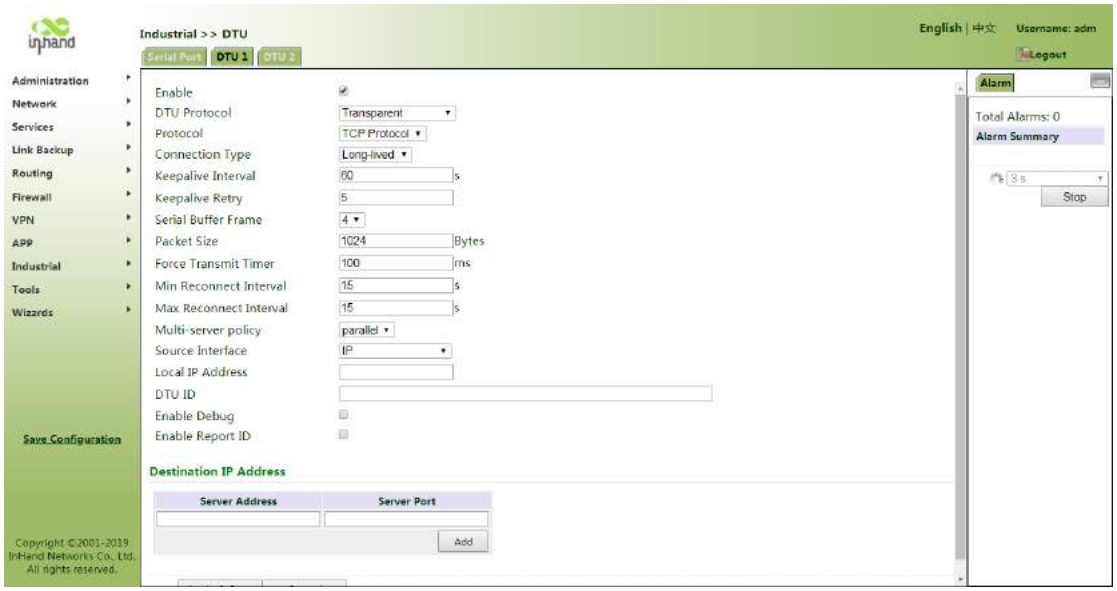


Configure the gateway as follows:

Step 1: Set the DTU serial port parameters. Ensure that the parameter settings are consistent with those of the peer device's serial port.



Step 2: Set the DTU function parameters.



Step 3: Check that the gateway-connected PC and the server exchange data through DTU.

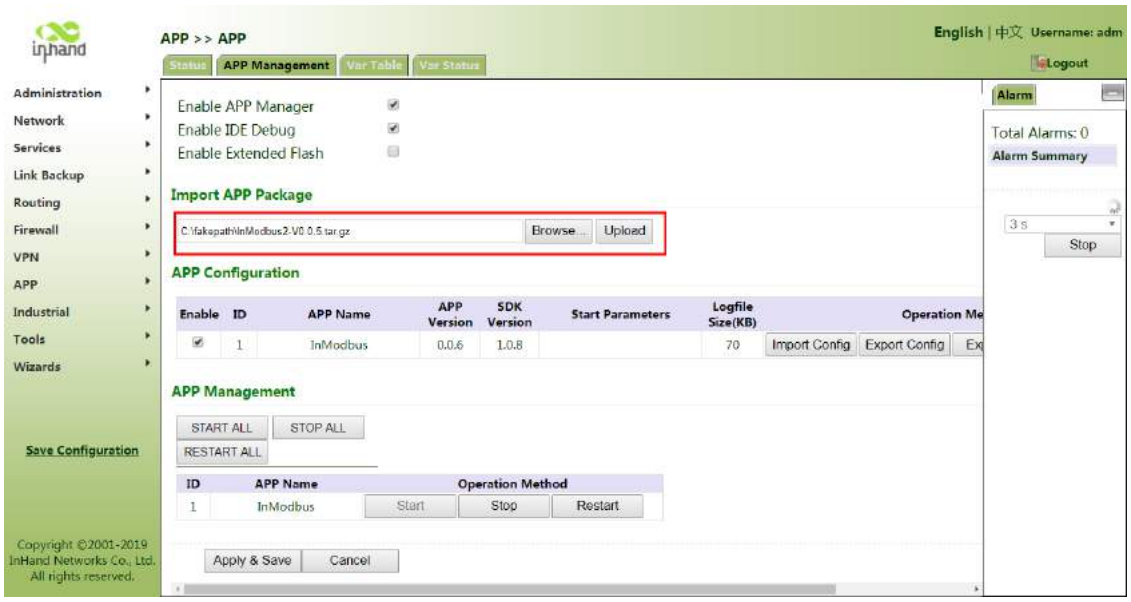
7 App Development

This chapter describes how to quickly develop apps in Python. Development of an InModbus app is used as an example.

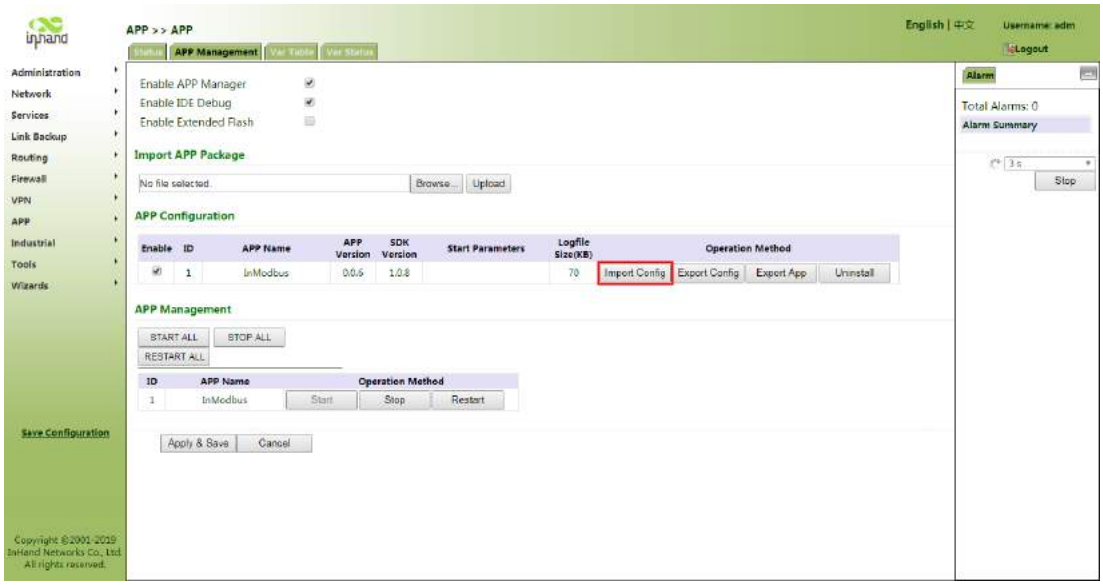
7.1 InModbus App

7.1.1 Installing an InModbus App

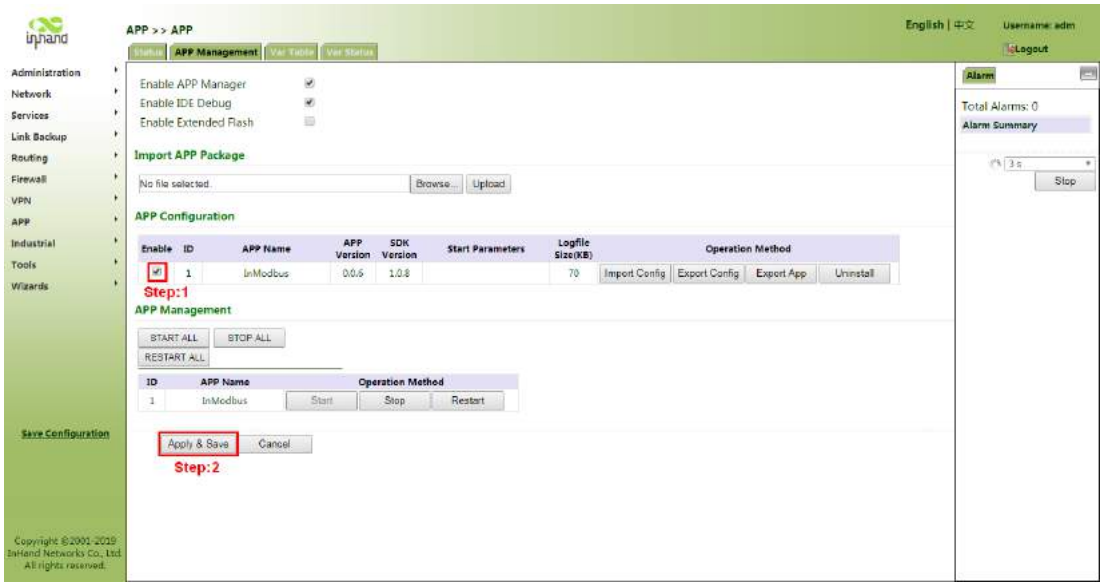
(1) On the gateway's web interface, choose **APP** > **APP** and click the **APP Management** tab. Select **Enable APP Manager** and **Enable IDE Debug**. Click **Browse** and select the InModbus app file package. Click **Upload** to upload the app to the gateway.



(2) Import the custom app configuration file. If the configuration file does not need to be modified, the gateway uses the default configuration file in the app package by default.

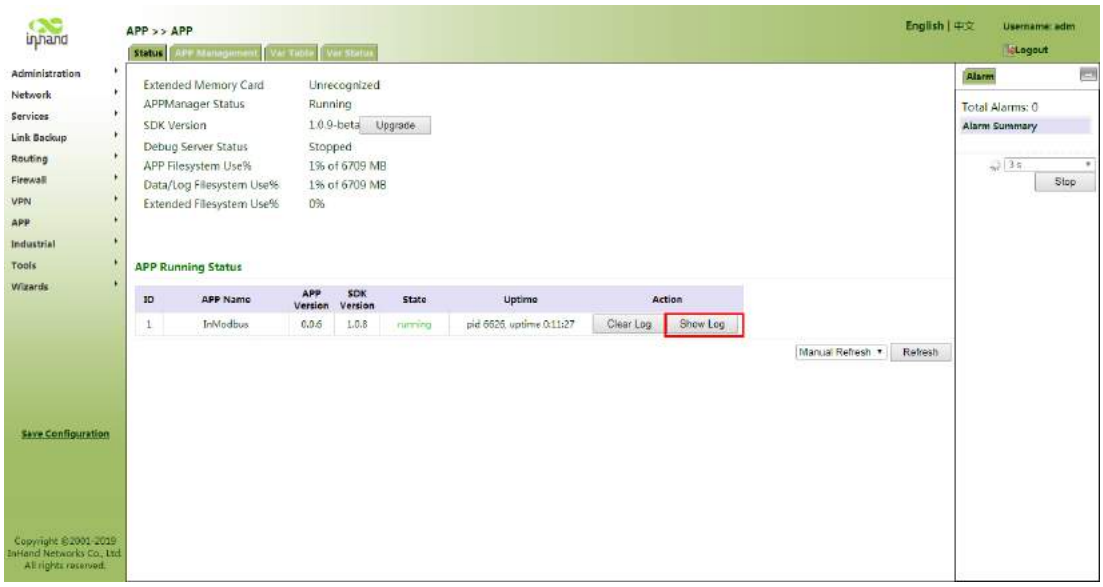


(3) Configure and launch the InModbus app.



(4) Check the InModbus app status.

On the gateway's web interface, choose **APP** > **APP** > **Status** to view details about the Python app, for example, the app name, version, running status, runtime, and action. To view the run log of the app, click **Show Log**. The log is displayed on a new tab page. If InModbus cannot start, check whether the system firmware version matches the Python SDK version.



7.1.2 Enabling the Remote Device Monitoring Platform

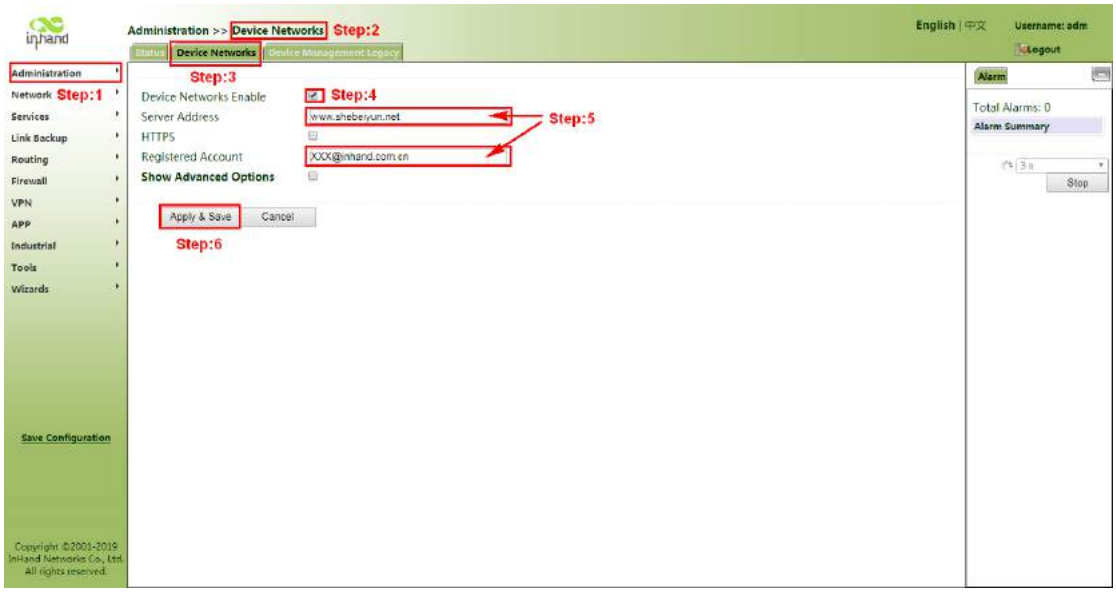
The remote device monitoring platform is the software that provides the monitoring service for onsite devices and implements the maintenance management, energy monitoring, asset management, and variable monitoring and management functions. The data collected by the InModbus app is uploaded to the platform through a built-in application of the remote device monitoring platform.

To use the remote device monitoring platform, register an account at **http://www.shebeiyun.net** and log in to the platform by using the registered email address. After login, bind the gateway to your account.

Note:

Skip this section if you need to upload data to other platforms than www.shebeiyun.net. Ensure that the platform that you use is supported by InModbus 2 and that the connection parameters are set in the configuration file.

On the gateway's web interface, choose **Administration** > **Device Networks** and click the **Device Networks** tab to enable the remote device monitoring platform. Enter the server address **www.shebeiyun.net** and register an account with your email address, such as xxx@inhand.com.cn. Retain the default settings for other options if you do not have special requirements. Click **Apply**. To check the connection status, click the **Status** tab. **Connected** indicates that the connection is normal.



7.1.3 Enabling the Variable Editing Service

Choose **APP** > **Var Table**, select **Enable**, and click **Apply & Save** to enable the variable editing service. After the service is enabled, the hidden options on this page are displayed.

Note:

After the configuration is complete, restart the app manually to make the new configuration effective.

7.1.4 Modifying Configuration

7.1.4.1. Adding and Modifying Devices

This operation corresponds to the **Controller** part of configuration file editing. To add a device, click **Add** on the **Var Table** tab page and click **Apply & Save**.

Note:

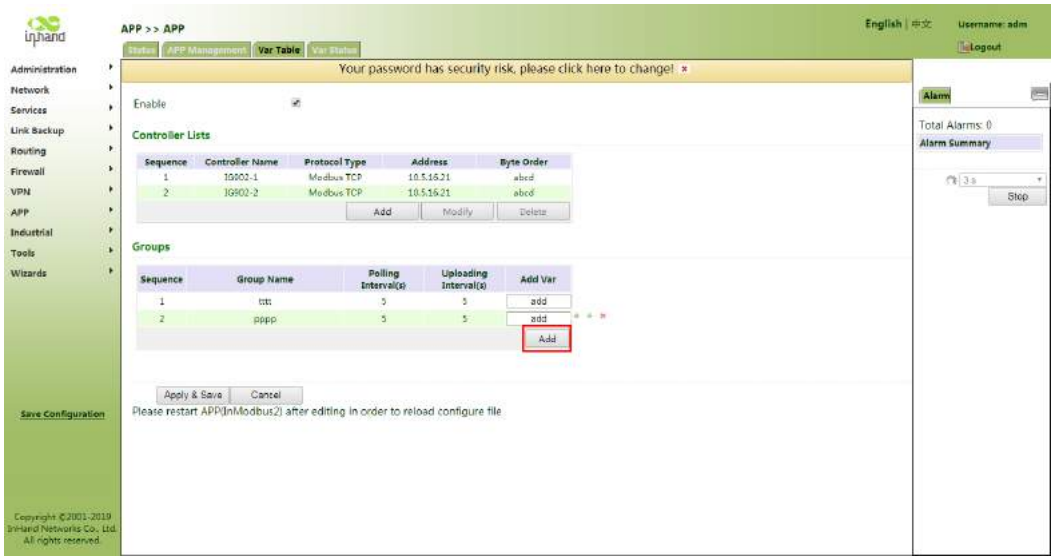
Device information, such as the device name, cannot be modified after being saved.

Such device information includes:

1. Device name (special characters and numeric strings are not allowed)

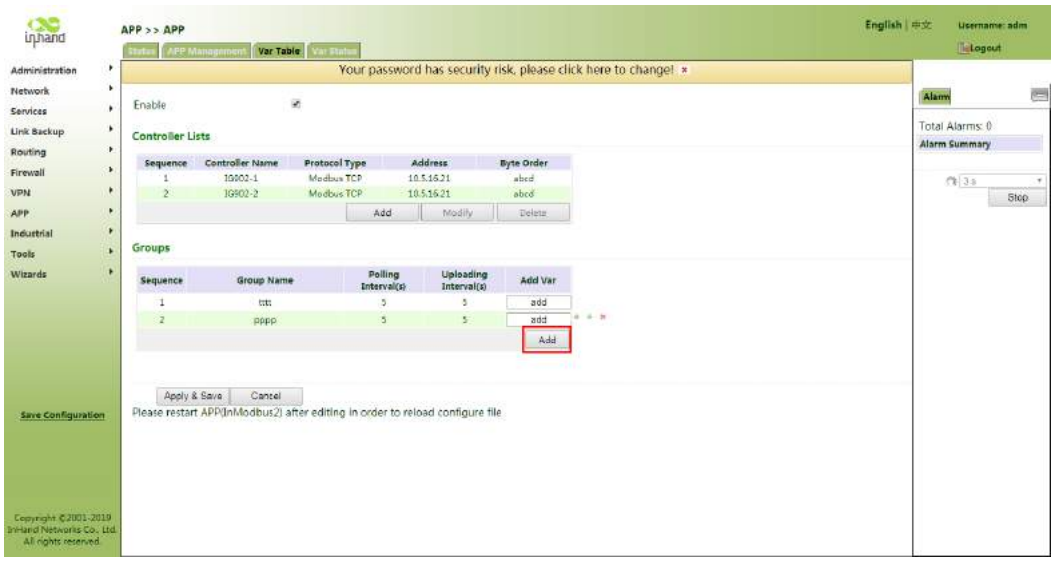
2. Variable address order (which can be empty after being created and are system-defined by default)

3. Register address (which cannot be modified or deleted when being used by the collection group)



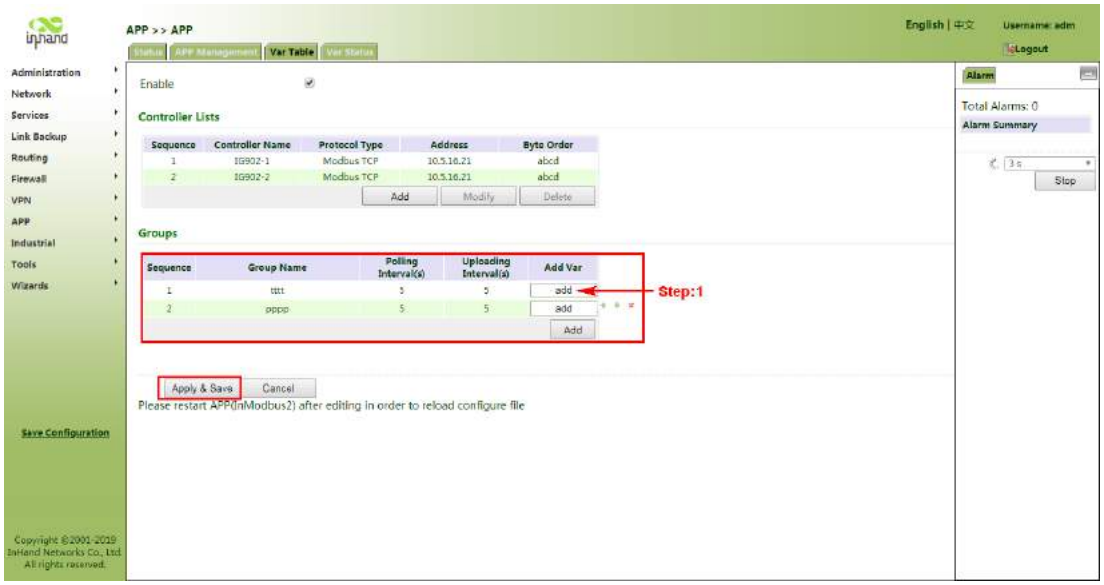
7.1.4.2. Adding and Modifying Collection Groups

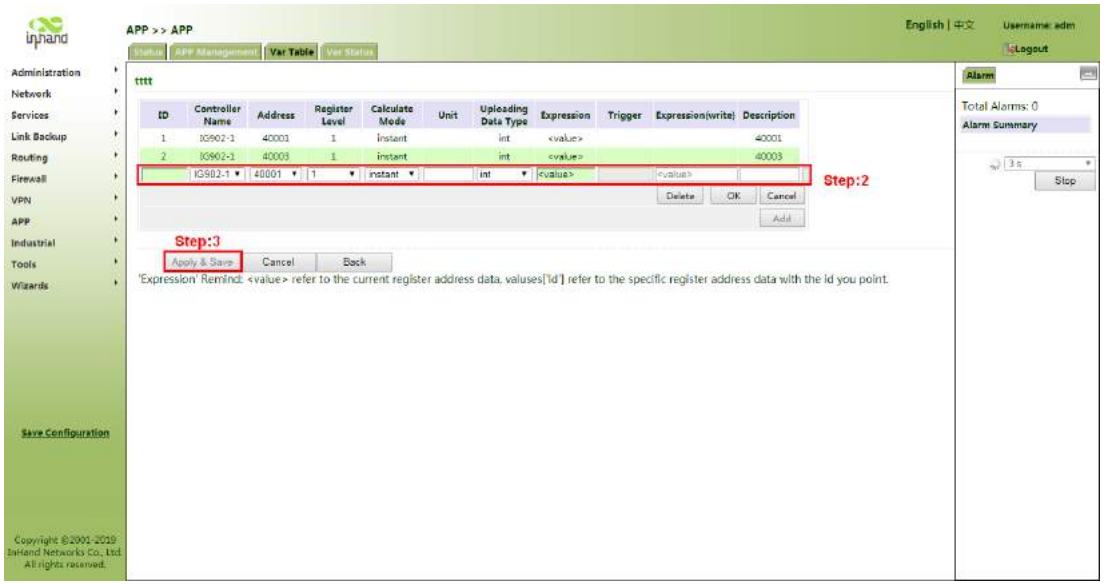
This operation corresponds to the **Collection Policy Group** configuration, in which the collected I/O values are calculated based on policies. To meet different requirements, the configuration file uses micro expressions. In the format of micro expressions, <value> indicates the value collected by the current register address, and values['id'] indicates the value calculated by the register address with the specified ID.



Note:

Collection group information, such as the group name, cannot be modified after being saved.


APP >> APP
Enable
Controller Lists
Sequence
Controller Name
Protocol Type
Address
Byte Order
Add
Modify
Delete
Groups
Sequence
Group Name
Polling Interval(s)
Uploading Interval(s)
Add Var
Step:1
Apply & Save
Cancel
Please restart APP(InModbus2) after editing in order to reload configure file
Save Configuration
Alarm
Total Alarms: 0
Alarm Summary
Stop


APP >> APP
tttt
ID
Controller Name
Address
Register Level
Calculate Mode
Unit
Uploading Data Type
Expression
Trigger
Expression(write)
Description
Delete
OK
Cancel
Add
Step:2
Step:3
Apply & Save
Cancel
Back
'Expression' Remind: <value> refer to the current register address data, values['Id'] refer to the specific register address data with the id you point.
Save Configuration
Alarm
Total Alarms: 0
Alarm Summary
Stop

8 Appendix CLI Commands

1 Help Command

You can enter **help** or **?** on the console to obtain command assistance. When entering a command, you can enter **?** to obtain help information about the current command or command parameters. When the entered command or command parameters are unique, they can be complemented automatically.

1.1 help

Command: help [<cmd>]
Function: obtains command assistance.
View: all views
Parameter: <cmd> indicates a command name.
Example:

- ✧ Enter **help**.
  The command output lists all available commands.
- ✧ Enter **help show**.
  The command output lists all the parameters of the **show** command and related instructions.

2 View Switching Commands

2.1 enable

Command: enable [15 [<*password*>]]
Function: enters privileged EXEC mode.
View: common user view
Parameter: 15 indicates a user permission level. Currently, only permission level 15 (superuser) is supported.
<*password*> indicates the password corresponding to the privileged EXEC mode. If it is not entered, a password input prompt appears.
Example: Enter **enable adm** in the common user view.
The system switches to the superuser. The password is **123456**.

2.2 disable

Command: disable
Function: exits privileged EXEC mode.
View: superuser view and configuration view
Parameter: none
Example: Enter **disable** in the superuser view.
The system returns to the common user view.

2.3 end and !

Command: end or !
Function: exits the current view and returns to the previous view.
View: configuration view
Parameter: none
Example: Enter **end** in the configuration view.
The system returns to the superuser view.

2.4 exit

Command: exit
Function: exits the current view and returns to the previous view. If the current view is the common user view, entering this command will log you out of the console.
View: all views
Parameter: none
Example:

- ✧ Enter **exit** in the configuration view.
  The system returns to the superuser view.
- ✧ Enter **exit** in the common user view.
  The system exits the console.

3 Commands for Checking the System Status

3.1 show version

Command: show version
Function: shows the model, software version, and other information about the gateway.
View: all views
Parameter: none
Example: Enter **show version**.
The following information is displayed:
Model: model of the gateway
SN: SN of the gateway
Description: www.inhand.com.cn
Current version: current version of the gateway
Current bootloader version: current bootloader version of the gateway

3.2 show system

Command: show system
Function: shows information about the gateway system.
View: all views
Parameter: none
Example: Enter **show system**.
The following information is displayed:
For example, 00:00:38 up 0 min, load average: 0.00, 0.00, 0.00

3.3 show clock

Command: show clock
Function: shows the system time of the gateway.
View: all views
Parameter: none
Example: Enter **show clock**.
The following information is displayed:
For example, Sat Jan 1 00:01:28 UTC 2000

3.4 show modem

Command: show modem
Function: shows the modem status of the gateway.
View: all views
Parameter: none
Example: Enter **show modem**.
The following information is displayed:
Modem type
Status
Vendor

Product name
Information level
Registration status
IMSI
Network type

3.5 show log

Command: show log [lines <n>]
Function: displays the system logs of the gateway. By default, the latest 100 logs are displayed.
View: all views
Parameter: **lines** <*n*> indicates the number of logs that can be displayed. When *n* is set to a positive integer, the *n* latest logs are displayed. When *n* is set to a negative integer, the *n* earliest logs are displayed. When *n* is set to 0, all logs are displayed.
Example: Enter **show log**.
The 100 latest logs are displayed.

3.6 show users

Command: show users
Function: shows the user list of the gateway.
View: all views
Parameter: none
Example: Enter **show users**.
The following system user list is displayed:
User:
---
* adm

The user marked with an asterisk (*) is the superuser.

3.7 show startup-config

Command: show startup-config
Function: shows the startup configuration of the gateway.
View: superuser view and configuration view
Parameter: none
Example: Enter **show startup-config**.
The startup configuration of the system is displayed.

3.8 show running-config

Command: show running-config
Function: shows the runtime configuration of the gateway.
View: superuser view and configuration view
Parameter: none
Example: Enter **show running-config**.
The runtime configuration of the system is displayed.

4 Commands for Checking the Network Status

4.1 show interface

Command: show interface
Function: shows the interface status information about the gateway.
View: all views
Parameter: none
Example: Enter **show interface**.

The status of each interface is displayed.

4.2 show route

Command: Show ip route
Function: shows the routing table of the gateway.
View: all views
Parameter: none
Example: Enter **Show ip route**.
The routing table of the system is displayed.

4.3 show arp

Command: show arp
Function: shows the ARP table of the gateway.
View: all views
Parameter: none
Example: Enter **show arp**.
The ARP table of the system is displayed.

5 Network Test Commands

The gateway provides network test tools, such as ping, Telnet, and traceroute.

5.1 ping

Command: ping <*hostname*> [count <*n*>] [size <*n*>] [source <*ip*>]
Function: performs ICMP detection on the specified host.
View: all views
Parameter: <*hostname*> indicates the IP address or domain name of the host to be detected.
count <*n*> indicates the detection times.
size <*n*> indicates the size of a detection packet, in bytes.
source <*ip*> indicates the IP address used during detection.
Example: Enter **ping www.g.cn**.
The system detects www.g.cn and displays the detection results.

5.2 telnet

Command: telnet <*hostname*> [<*port*>] [source <*ip*>]
Function: logs in to the specified host through telnet.
View: all views
Parameter: <*hostname*> indicates the IP address or domain name of the host for Telnet login.
<*port*> indicates the Telnet port.
source <*ip*> indicates the IP address used during Telnet login.
Example: Enter **telnet 192.168.2.2**.
Login is initiated to 192.168.2.2 through Telnet.

5.3 traceroute

Command: traceroute <*hostname*> [maxhops <*n*>] [timeout <*n*>]
Function: performs gateway detection on the specified host.
View: all views
Parameter: <*hostname*> indicates the IP address or domain name of the host to be detected.
maxhops <*n*> indicates the maximum number of hops during gateway detection.
timeout <*n*> indicates the timeout period of each hop, in seconds.
Example: Enter **traceroute www.g.cn**.
The system performs gateway detection on www.g.cn and displays the detection results.

6 Configuration Commands

You can run the **configure** command in the superuser view to switch to the configuration view for gateway management. Some configuration commands support the **no** and **default** forms. The **no** form cancels the setting of a parameter, and the **default** form restores the default setting of a parameter.

6.1 configure

Command: configure terminal
Function: switches to the configuration view and enters configuration from a terminal.
View: superuser view
Parameter: none
Example: Enter **configure terminal** in the superuser view.
The system switches to the configuration view.

6.2 hostname

Command: hostname [<*hostname*>]
default hostname
Function: shows or sets the host name of the gateway.
View: configuration view
Parameter: <*hostname*> indicates a new host name.
Example:

- ✧ Enter **hostname** in the configuration view.
  The host name of the gateway is displayed.
- ✧ Enter **hostname MyRouter** in the configuration view.
  The host name of the gateway is set to **MyRouter**.
- ✧ Enter **default hostname** in the configuration view.
  The host name of the gateway is restored to the default one.

6.3 clock timezone

Command: clock timezone <*timezone*> <*n*>
default clock timezone
Function: sets the time zone information about the gateway.
View: configuration view
Parameter: <*timezone*> indicates the name of a time zone, consisting of three uppercase letters.
<*n*> indicates the time zone offset, in the range from –12 to +12.
Example:

- ✧ Enter **clock timezone CST -8** in the configuration view.
  The gateway is set to the UTC+8 time zone named CST (short for China Standard Time).
- ✧ Enter **default clock timezone** in the configuration view.
  The gateway is restored to the default time zone.

6.4 clock set

Command: clock set <*YEAR/MONTH/DAY*> [<*HH:MM:SS*>]
Function: sets the date and time of the gateway.
View: configuration view
Parameter: <*YEAR/MONTH/DAY* > indicates a date, in the format *year-month-day*.
<*HH:MM:SS* > indicates the time, in the format *hours-minutes-seconds*.
Example: Enter **clock set 2009-10-5 10:01:02** in the configuration view.
The time of the gateway is set to 10:01:02, October 5, 2009.

6.5 ntp server

Command: ntp server <*hostname*>
no ntp server
default ntp server
Function: sets a client for the NTP server.
View: configuration view
Parameter: <*hostname*> indicates the IP address or domain name of the NTP server host.
Example: Enter **sntp-client server pool.ntp.org** in the configuration view.
The address of the NTP server is set to pool.ntp.org.

7 System Management Commands

7.1 reboot

Command: reboot
Function: restarts the system
View: superuser view and configuration view
Parameter: none
Example: Enter **reboot** in the superuser view.
The system is restarted.

7.2 enable password

Command: enable password [<*password*>]
Function: changes the password of the superuser.
View: configuration view
Parameter: <*password*> indicates a new password of the superuser.
Example: Enter **enable password** in the configuration view.
Enter a password as prompted.

7.3 username

Command: username <*name*> [password [<*password*>]]
no username <*name*>
default username
Function: sets the user name and password.
View: configuration view
Parameter: none
Example:

- Enter **username abc password 123** in the configuration view.
  A common user is added, with the user name **abc** and password **123**.
- Enter **no username abc** in the configuration view.
  The common user **abc** is deleted.
- Enter **default username** in the configuration view.
  All common users are deleted.