Edge Router 805 Product User Manual

Table of contents

Declaration

Thank you for choosing our company's product! Before use, please carefully read this user manual. By complying with the following statements, you will help maintain intellectual property rights and legal compliance, ensuring that your user experience aligns with the latest product information. If you have any questions or need written permission, please feel free to contact our technical support team.

Copyright Statement

This user manual contains copyrighted content, and the copyright belongs to InHand Networks and its licensors. Without written permission, no organization or individual may excerpt, copy any part of the content of this manual, or distribute it in any form.

Disclaimer

Due to ongoing updates in product technology and specifications, the company cannot guarantee that the information in the user manual is entirely consistent with the actual product. Therefore, no disputes arising from any discrepancies between the actual technical parameters and the user manual are accepted. Any changes to the product will not be notified in advance, and the company reserves the right to make the final changes and interpretations.

Copyright Information

Conventions

Symbol	Indication
[ ]	Referring to function modules or menus, such as in the [Status] menu."
“ ”	Referring to a button name, such as Clicking the “Add” button.
〉	Multiple levels of menus are separated by "〉 ". For example, "File〉 New〉 Folder" represents the "Folder" menu item under the "New" submenu, which is under the "File" menu.
Cautions	Please be mindful of the following points during the operation, as improper actions may result in data loss or device damage.
Note	Supplement and provide necessary explanations for the description of the operation.

Technical Support

E-mail：support@inhandnetworks.com

URL: www.inhandnetworks.com

1. Overview

The Edge Router 805 is a next-generation 5G edge router product introduced by InHand Networks for the commercial networking sector. It seamlessly integrates 4G/5G wireless networks with a variety of broadband services, offering high-speed and secure network access to various industries. Users can enjoy uninterrupted internet connectivity anytime and anywhere, while benefiting from comprehensive security features and exceptional wireless services. The ER805 transforms device interconnectivity into a reality, providing a high-speed gateway for device informatization.

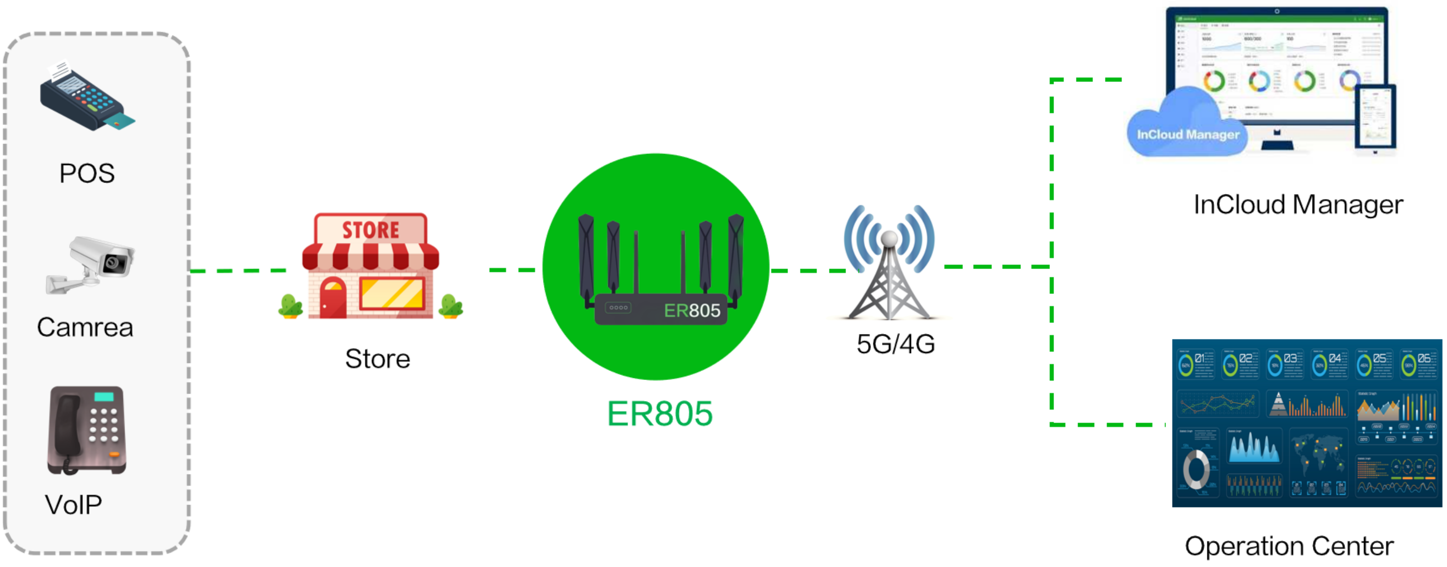


Fig. 1 ER805’s Application

2. Hardware

2.1 LED Indicators

Indicators	Status and Description
System	Off --- Power Off Blink in blue --- System booting in progress. Steady in blue --- The system is running smoothly. Blink in red --- System malfunction detected. Blink in green --- System upgrading in progress.
Network	Blink in red --- Network disconnected. Blink in green --- Cellular network connecting. Steady in green --- Cellular network connected. Blink in blue --- Wired network connecting. Steady in blue --- Wired network connected.
Wi-Fi 2.4G	Off --- 2.4G Wi-Fi disabled. Steady in blue --- Starting up. Blink in blue --- On working

Wi-Fi 5G	Off --- 5 G Wi-Fi disabled. Steady in green --- Starting up. Blink in green --- On working.

For the network status indicator:

- If both cellular and wired connections are normal, it displays a blue wired indicator.
- If only one type of connection is active and noal, it shows the indicator for the active network.
- If there is no network connection, it displays red.

2.2 Restore to Factory Defaults

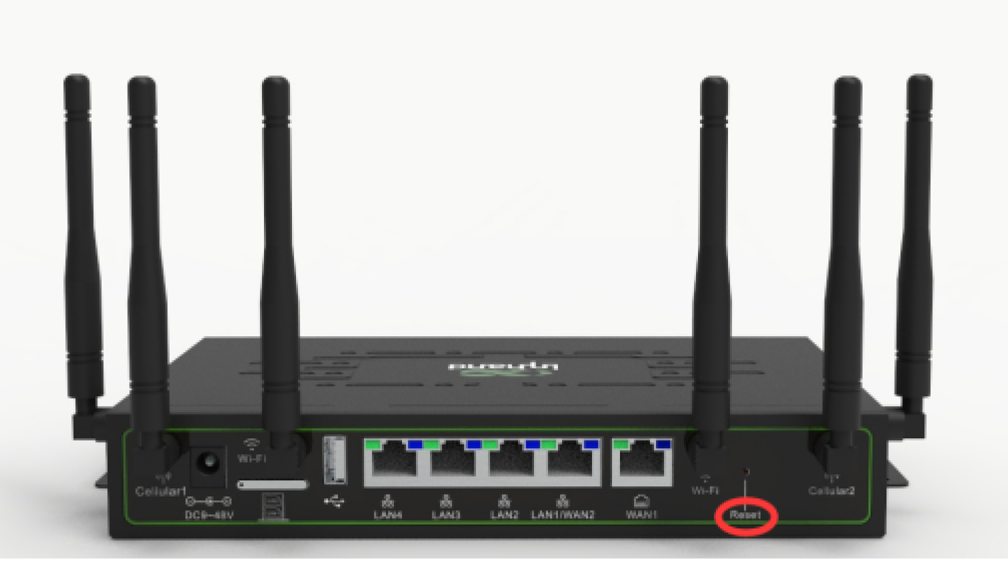


Fig. 2.2 Factory Reset

To reset to factory default settings using the Reset button:

Step 1: After powering on the device, immediately press and hold the Reset button.

Step 2: After holding it for a while, the power indicator light will start flashing. Approximately half a minute later, the power indicator light will stay on steadily.

Step 3: Release the Reset button, and the power indicator light will flash again. Then, press and hold the Reset button once more.

Step 4: The power indicator light will flash slowly. Release the Reset button, and the factory reset will be successful. The device will restart normally.

3. Default Settings

No.	Function	Default Settings
1	**Cellular Dialing**	Default dialing is set to "SIM1"

2	**Wi-Fi**	1. Wi-Fi 2.4G access point enabled, SSID: Prefixed with "ER805-", followed by the last 6 digits of the wireless MAC address. 2. Wi-Fi 5G access point enabled, SSID: Prefixed with "ER805-5G-", followed by the last 6 digits of the wireless MAC address. 3. The authentication method is WPA2-PSK. 4. The password for both is the last 8 digits of the serial number.
3	**Ethernet**	1. Enable all 4 LAN ports. 2. IP Address: 192.168.2.1 Subnet Mask: 255.255.255.0 3. DHCP server enabled, with an address pool from 192.168.2.2 to 192.168.2.100 for automatic IP address assignment to connected devices.
4	**Network Access Control**	Local HTTP and HTTPS are enabled with port numbers 80 and 443 respectively. Disable access from the cellular network.
5	**Username/Password**	adm/123456

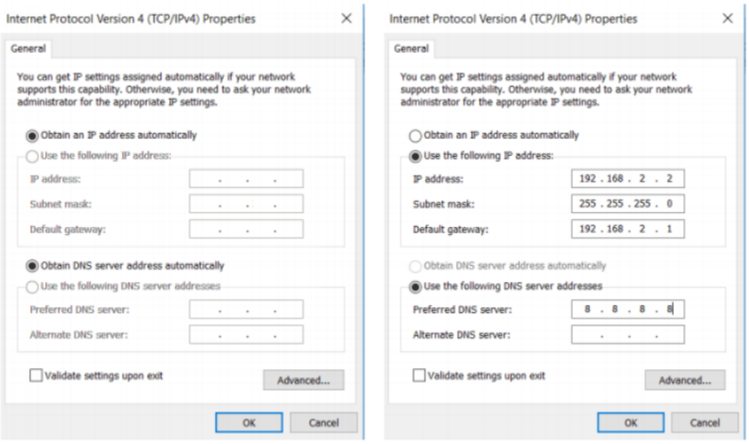
4. Quick Guide

4.1 Environment Setup

Step 1: Install the 4G/5G and Wi-Fi antennas and insert the SIM card.

Step 2: Connect the power cable and an Ethernet cable; connect any LAN port to your PC.

Step 3: Set your PC's IP address to be on the same subnet as the edge router.



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

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

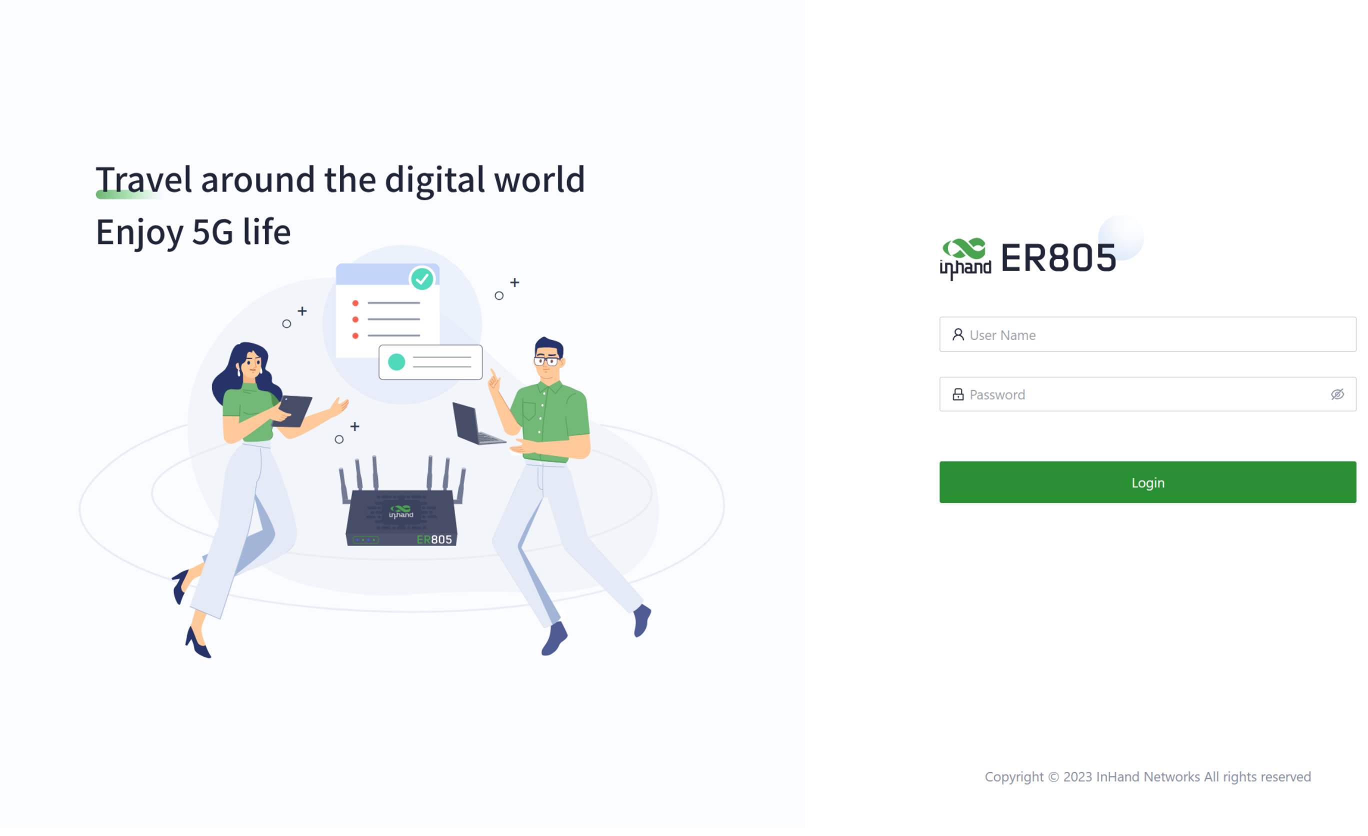
○ Obtain DNS server address automatically
● Use the following DNS server addresses
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: . . .

□ Validate settings upon exit

Fig. 4.1 Configure PC IP Address

The device's LAN port has DHCP Server functionality enabled by default. Once the PC has automatically obtained an IP address, please ensure that your PC and router are in the same address range.If your PC fails to obtain an IP address automatically, please configure it with a static IP address and the following parameters: IP Address: 192.168.2.x (Choose an available address within the range of 192.168.2.2 to 192.168.2.254). Subnet Mask: 255.255.255.0. Default Gateway: 192.168.2.1. DNS Servers: 8.8.8.8 (or your ISP's DNS server address)

Step 4: Enter the default device address 192.168.2.1, in the browser's address bar. After entering the username and password (adm/123456), access the device's web management interface. If the page shows a security warning, click on the "Hide" or "Advanced" button and select "Proceed" to continue.



Travel around the digital world
Enjoy 5G life
inhand
ER805
inhand ER805
User Name
Password
Login
Copyright © 2023 InHand Networks All rights reserved

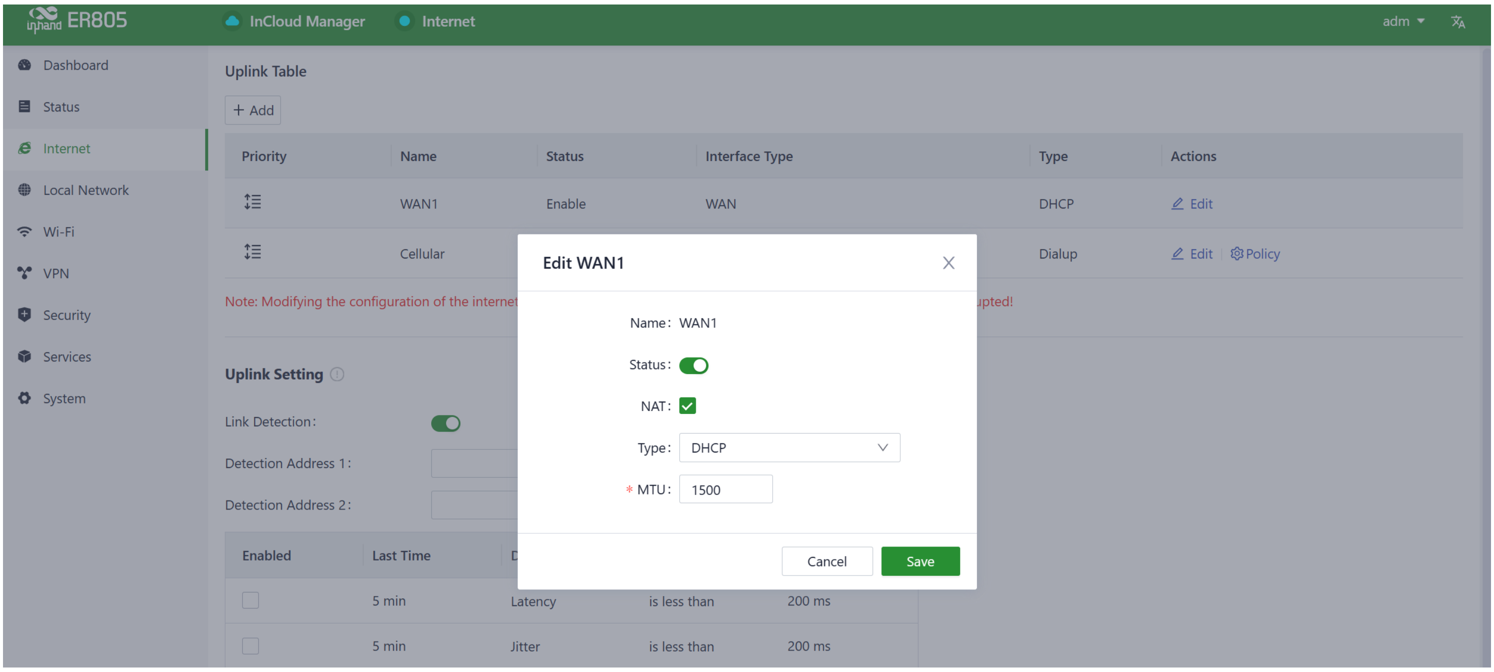
Fig.4-1 Device Web Login Page

4.2 Quickly connect to the Internet

The ER805 supports three access network modes, including wired, cellular, and Wi-Fi. The device's WAN interface has DHCP service enabled by default. Simply connect the WAN interface to the internet using an Ethernet cable, and it will automatically establish an internet connection.

4.2.1 Wired Connection

The ER805 supports three wired internet connection methods: DHCP, Static IP, and PPPoE. The device's WAN interface has DHCP service enabled by default. Simply connect the WAN interface to the internet using an Ethernet cable, and it will automatically establish an internet connection.



Uplink Table

Priority	Name	Status	Interface Type	Type	Actions
☰	WAN1	Enable	WAN	DHCP	Edit
☰	Cellular			Dialup	Edit | Policy

Note: Modifying the configuration of the internet … upted!

Edit WAN1

Name: WAN1

Status: ●

NAT: ☑

Type: DHCP

* MTU: 1500

Uplink Setting

Link Detection: ●

Detection Address 1:

Detection Address 2:

Enabled	Last Time	D		
□	5 min	Latency	is less than	200 ms
□	5 min	Jitter	is less than	200 ms

Fig. 4-2-1-a Edit the WAN1 Interface

4.2.2 5G/4G Connection

In the usual scenario, as per the instructions, upon inserting the SIM card and connecting the Wi-Fi antennas, the ER805 router will automatically establish a dial-up connection and connect to the network when powered on.

4.3 Connect to InCloud Manager

ER805 is a cloud-managed router, and with InCloud Manager, you can achieve batch configuration deployment and software upgrades. The cloud platform offers rich visual charts and advanced features such as SD-WAN and Connector for remote maintenance, enabling small and medium-sized enterprise branches to complete their digital network infrastructure. To use InCloud Manager to manage your ER805, please follow the steps below:

4.3.1 Registration

In your web browser (we recommend using Google Chrome), enter the following URL: https://star.inhandcloud.com. You will be automatically redirected to the portal page, where you can select

"InCloud Manager" to access the SaaS platform for enterprise branch networking.Click 'Create now' to create a new platform account.

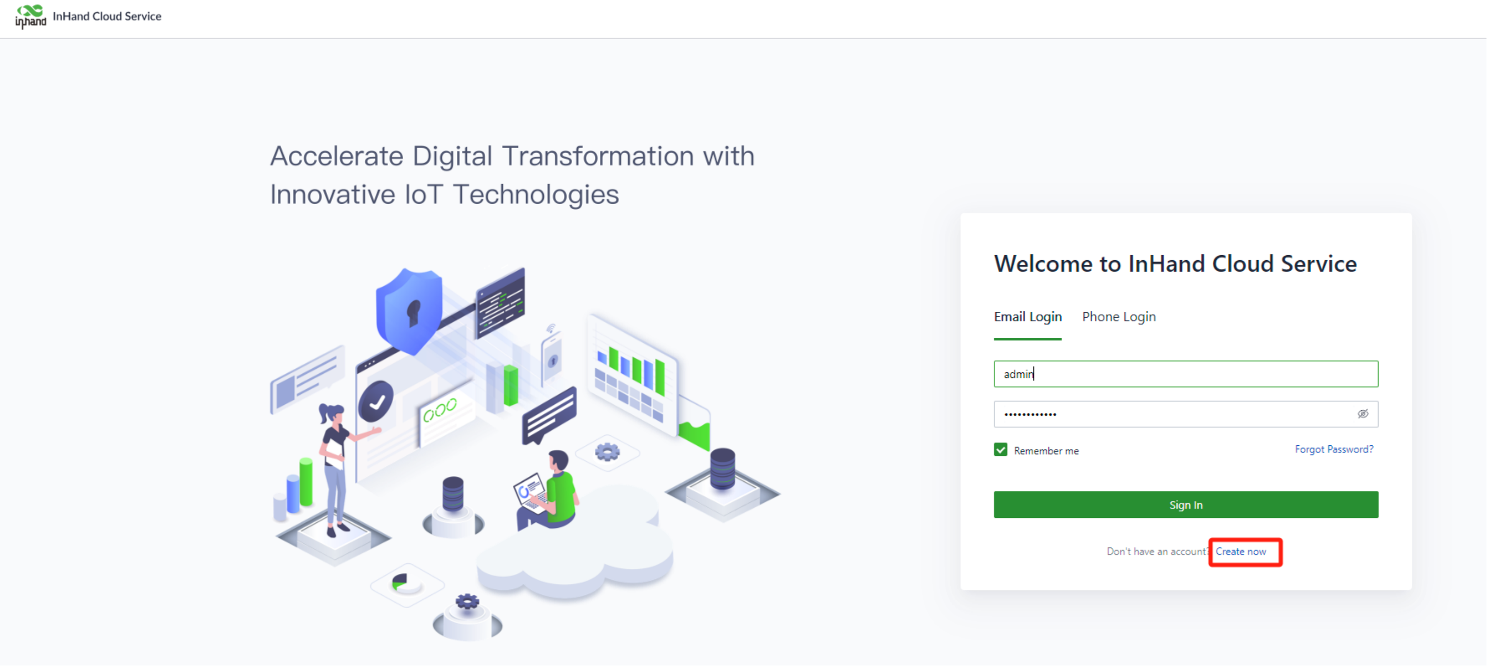
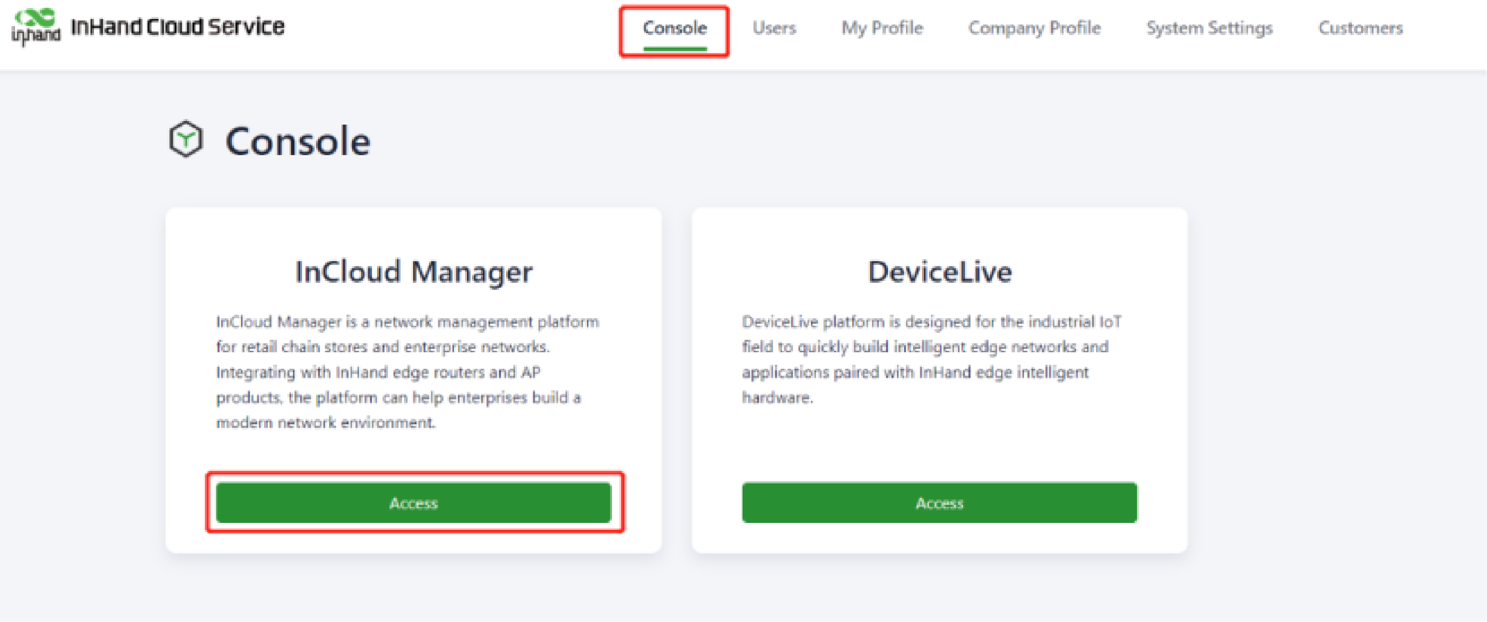


Fig. 4-3-1 Choose SaaS Services

4.3.2 Login

After completing the email registration, you can log in to InCloud Manager using the username and password you used during the registration.



InCloud Manager is a network management platform for retail chain stores and enterprise networks. Integrating with InHand edge routers and AP products, the platform can help enterprises build a modern network environment.

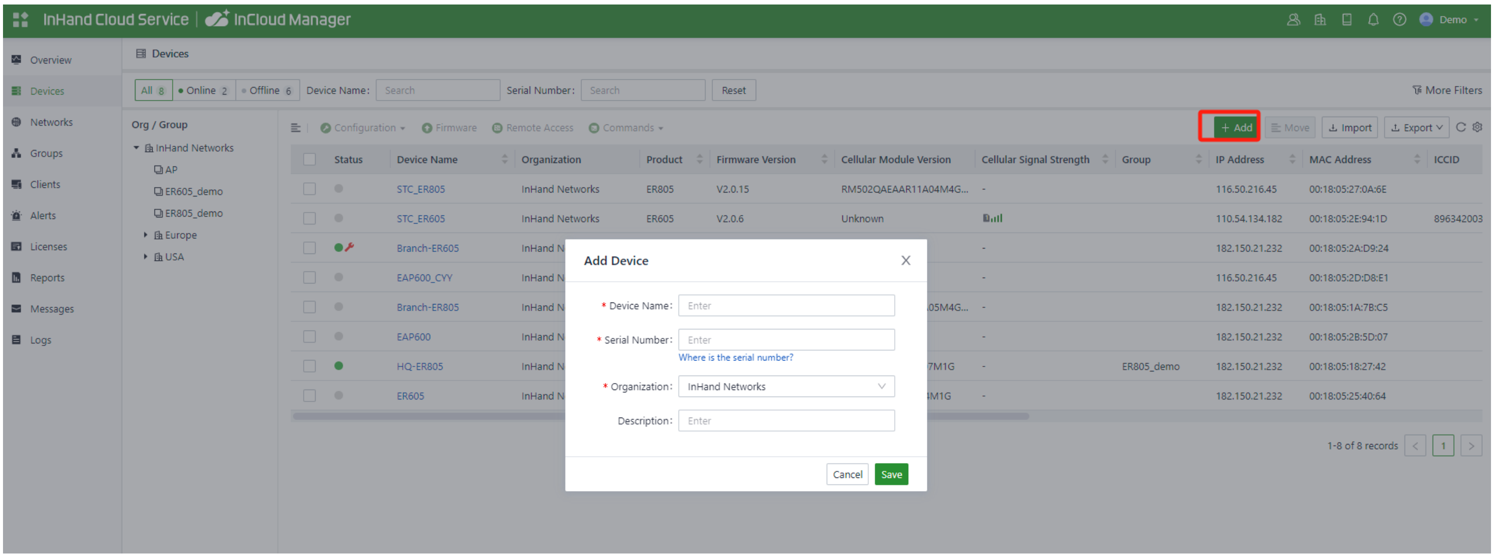
DeviceLive platform is designed for the industrial IoT field to quickly build intelligent edge networks and applications paired with InHand edge intelligent hardware.

Fig. 4-3-1 Choose SaaS Services

Note: When a device is initially added to the platform account, it will automatically receive a 1-year Essential license. Users can renew the license through the "License" menu.

4.3.3 Add device

After logging in, go to the "Devices" menu, click the "Add" button, fill in the device's name, serial number, and MAC address, and then click "Finish" to complete the addition.



Device Name: Search   Serial Number: Search

□	Status	Device Name	Organization	Product	Firmware Version	Cellular Module Version	Cellular Signal Strength	Group	IP Address	MAC Address	ICCID
□	○	STC_ER805	InHand Networks	ER805	V2.0.15	RM502QAEAAR11A04M4G...	-		116.50.216.45	00:18:05:27:0A:6E	
□	○	STC_ER605	InHand Networks	ER605	V2.0.6	Unknown	▮.ıl		110.54.134.182	00:18:05:2E:94:1D	896342003
□	●	Branch-ER605	InHand N				-		182.150.21.232	00:18:05:2A:D9:24	
□	○	EAP600_CYY	InHand N				-		116.50.216.45	00:18:05:2D:D8:E1	
□	○	Branch-ER805	InHand N			05M4G...	-		182.150.21.232	00:18:05:1A:7B:C5	
□	○	EAP600	InHand N				-		182.150.21.232	00:18:05:2B:5D:07	
□	●	HQ-ER805	InHand N			7M1G	-	ER805_demo	182.150.21.232	00:18:05:18:27:42	
□	○	ER605	InHand N			M1G	-		182.150.21.232	00:18:05:25:40:64	

1-8 of 8 records < 1 >

Add Device

* Device Name: Enter

* Serial Number: Enter

Where is the serial number?

* Organization: InHand Networks

Description: Enter

Cancel Save

Fig. 4-3-3 Add Device

5. Monitoring

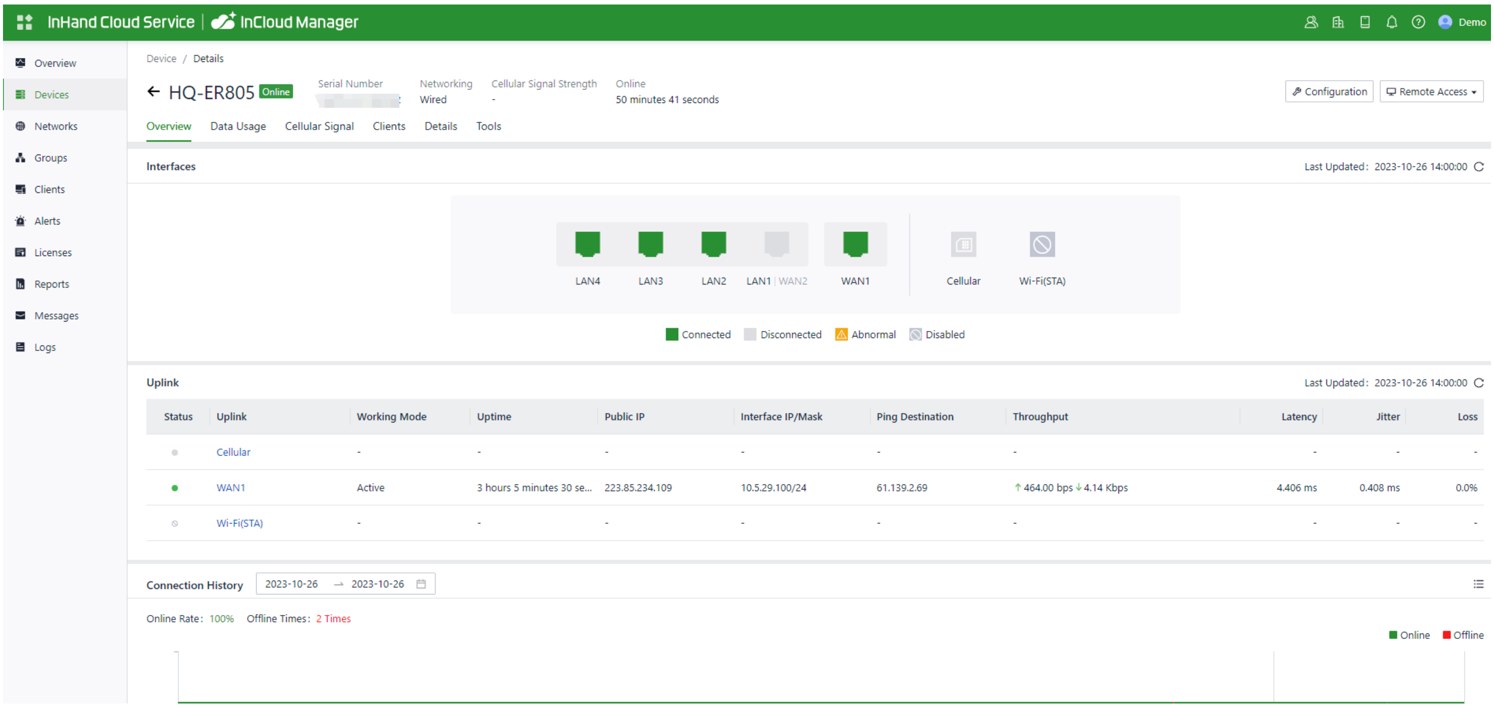
Once the device is added to the platform, you can manage and monitor the network from the platform while also supporting users in remotely viewing real-time status information on the device's local interface.

5.1 Overview Devices

In the "Devices" section, you can click on the "Device Name" to access the device's details page.

5.1.1 Overview

Click on [Dashboard] in the left menu to access the dashboard interface. Here, you can view essential device information, interface status, traffic statistics, cellular signal strength, and the number of connected Wi-Fi devices.



HQ-ER805 Online

Serial Number: [redacted]
Networking: Wired
Cellular Signal Strength: -
Online: 50 minutes 41 seconds

Interfaces
Last Updated: 2023-10-26 14:00:00

Uplink
Last Updated: 2023-10-26 14:00:00

Status	Uplink	Working Mode	Uptime	Public IP	Interface IP/Mask	Ping Destination	Throughput	Latency	Jitter	Loss
●	Cellular	-	-	-	-	-	-	-	-	-
●	WAN1	Active	3 hours 5 minutes 30 se...	223.85.234.109	10.5.29.100/24	61.139.2.69	↑464.00 bps ↓4.14 Kbps	4.406 ms	0.408 ms	0.0%
⦸	Wi-Fi(STA)	-	-	-	-	-	-	-	-	-

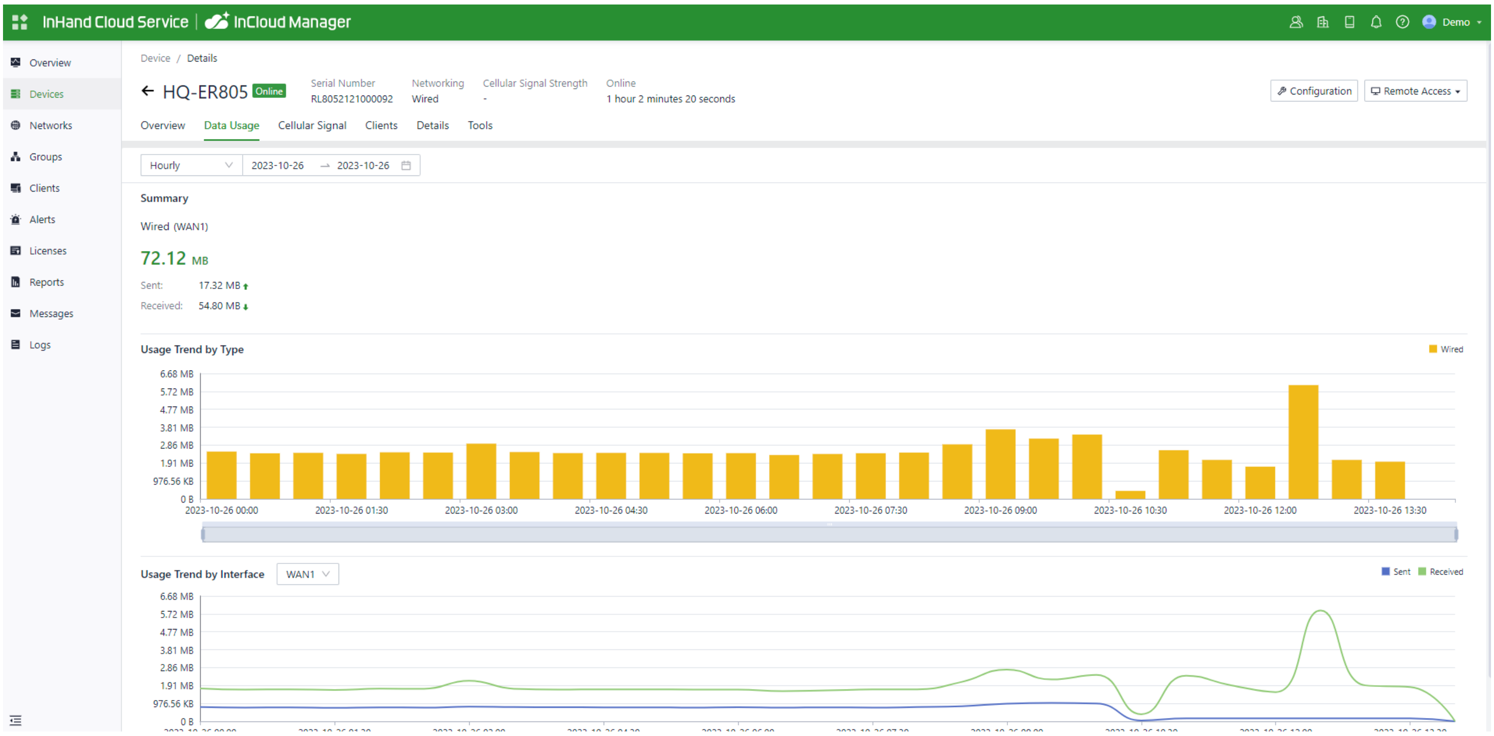
Connection History 2023-10-26 → 2023-10-26

Online Rate: 100% Offline Times: 2 Times

Fig. 5-1-1 Overview Devices

5.1.2 Data Usage

In this function, you can view the traffic usage and historical data of various upstream links.



HQ-ER805 Online

Serial Number: RL8052121000092
Networking: Wired
Cellular Signal Strength: -
Online: 1 hour 2 minutes 20 seconds

Hourly 2023-10-26 → 2023-10-26

Summary

Wired (WAN1)

72.12 MB

Sent: 17.32 MB ↑
Received: 54.80 MB ↓

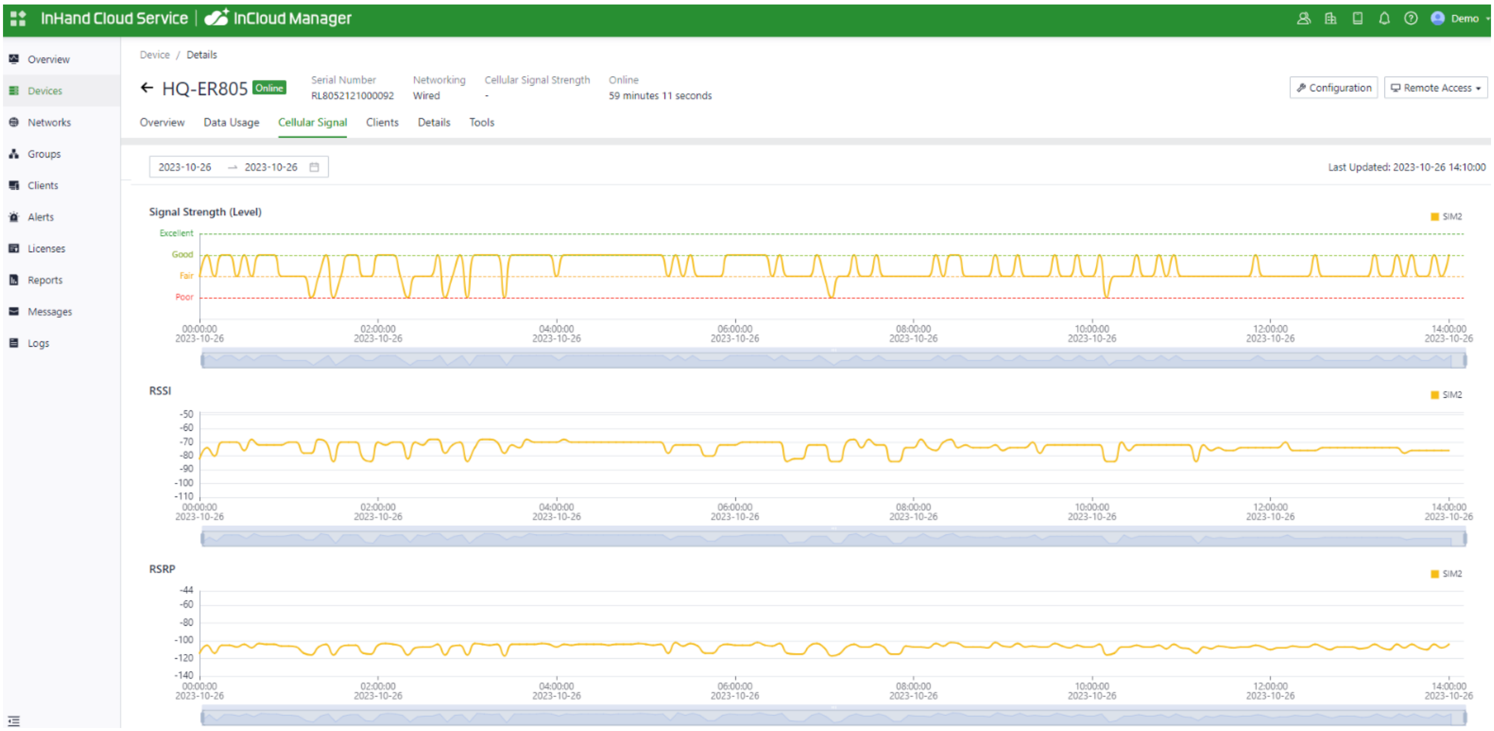
Usage Trend by Type

Usage Trend by Interface WAN1

Fig. 5-1-2 Data Usage

5.1.3 Cellular Signal

In this function, you can view cellular signal curves such as RSSI, RSRP, RSRQ, and SINR.



Serial Number: RL8052121000092
Networking: Wired
Cellular Signal Strength: -
Online: 59 minutes 11 seconds

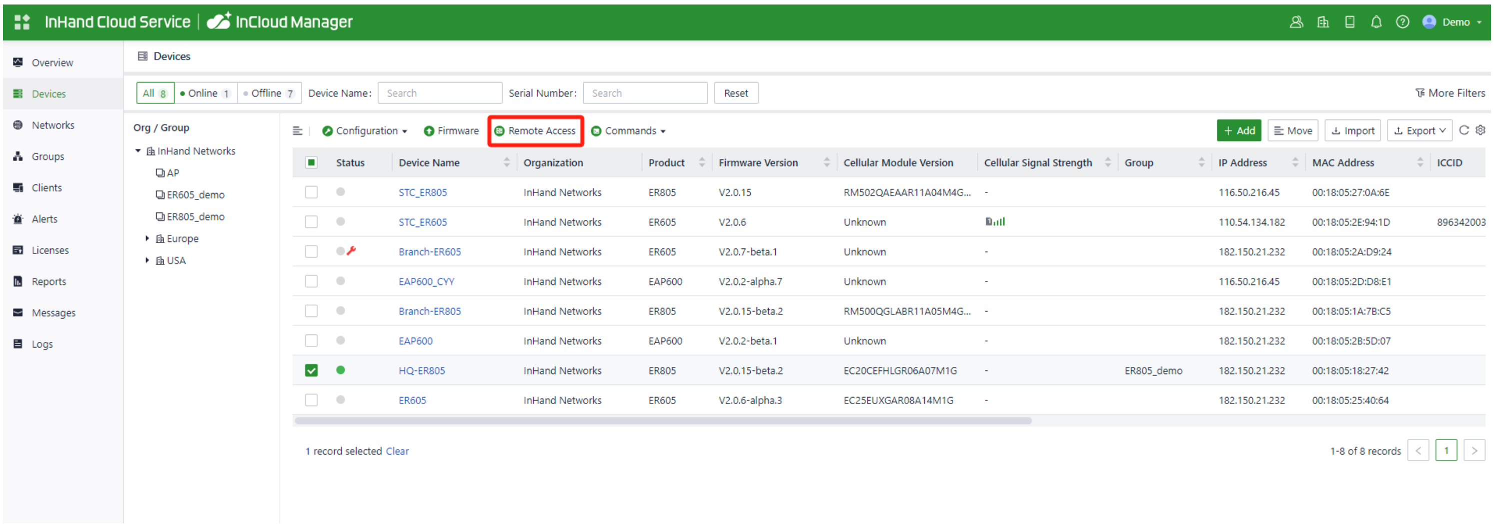
2023-10-26 → 2023-10-26

Last Updated: 2023-10-26 14:10:00

Fig. 5-1-3 Cellular Signal

5.2 Local Device Information

Through the platform's "Remote Access" feature, you can assist in real-time viewing and configuring of devices. Select the target device, click "Remote Access," and it will open the device's local login interface.



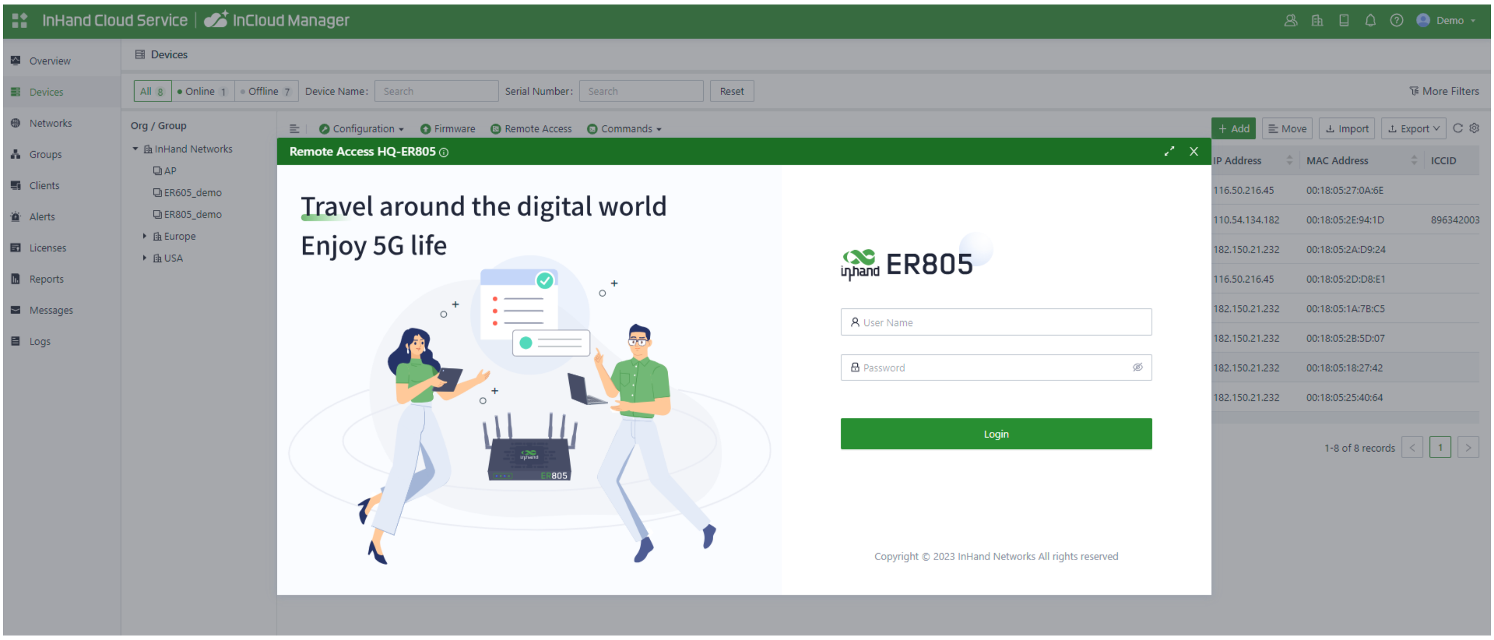
Device Name: Search
Serial Number: Search

■	Status	Device Name	Organization	Product	Firmware Version	Cellular Module Version	Cellular Signal Strength	Group	IP Address	MAC Address	ICCID
□	●	STC_ER805	InHand Networks	ER805	V2.0.15	RM502QAEAAR11A04M4G...	-		116.50.216.45	00:18:05:27:0A:6E	
□	●	STC_ER605	InHand Networks	ER605	V2.0.6	Unknown	▮ıll		110.54.134.182	00:18:05:2E:94:1D	896342003
□	●	Branch-ER605	InHand Networks	ER605	V2.0.7-beta.1	Unknown	-		182.150.21.232	00:18:05:2A:D9:24	
□	●	EAP600_CYY	InHand Networks	EAP600	V2.0.2-alpha.7	Unknown	-		116.50.216.45	00:18:05:2D:D8:E1	
□	●	Branch-ER805	InHand Networks	ER805	V2.0.15-beta.2	RM500QGLABR11A05M4G...	-		182.150.21.232	00:18:05:1A:7B:C5	
□	●	EAP600	InHand Networks	EAP600	V2.0.2-beta.1	Unknown	-		182.150.21.232	00:18:05:2B:5D:07	
☑	●	HQ-ER805	InHand Networks	ER805	V2.0.15-beta.2	EC20CEFHLGR06A07M1G	-	ER805_demo	182.150.21.232	00:18:05:18:27:42	
□	●	ER605	InHand Networks	ER605	V2.0.6-alpha.3	EC25EUXGAR08A14M1G	-		182.150.21.232	00:18:05:25:40:64	

1 record selected Clear

1-8 of 8 records < 1 >

Fig. 5-2-a Remote Access Entry

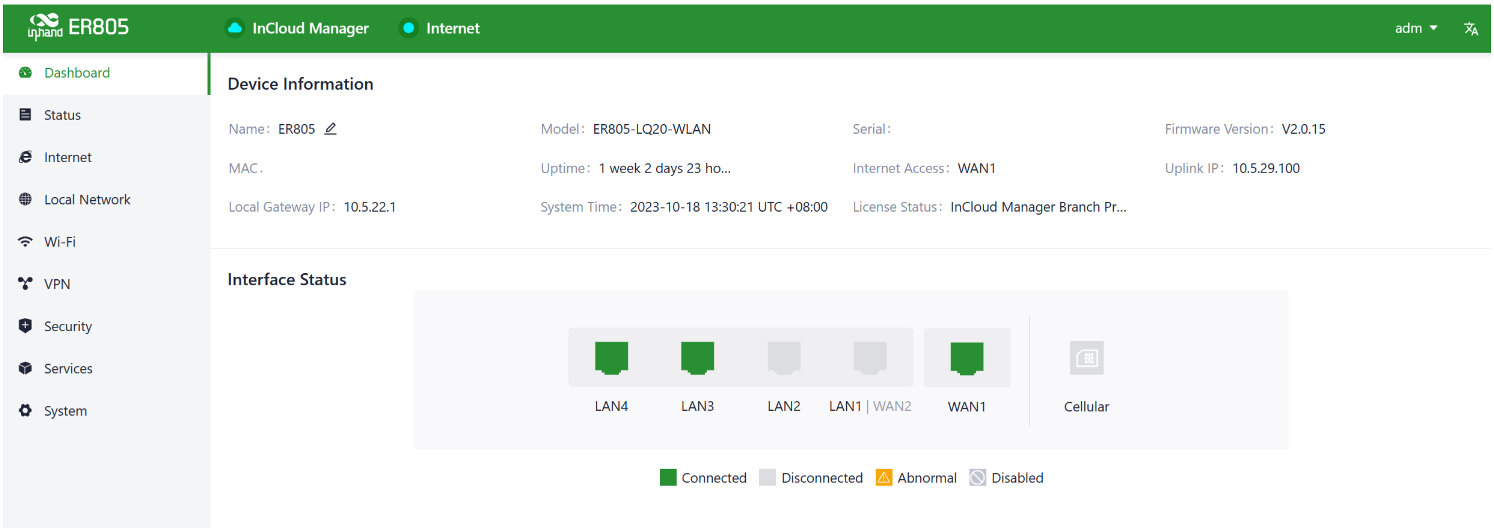


IP Address	MAC Address	ICCID
116.50.216.45	00:18:05:27:0A:6E	
110.54.134.182	00:18:05:2E:94:1D	896342003
182.150.21.232	00:18:05:2A:D9:24	
116.50.216.45	00:18:05:2D:D8:E1	
182.150.21.232	00:18:05:1A:7B:C5	
182.150.21.232	00:18:05:2B:5D:07	
182.150.21.232	00:18:05:18:27:42	
182.150.21.232	00:18:05:25:40:64	

Fig. 5-2-b Remote Access to Local Page

5.2.1 Device Information

In the [Dashboard] interface, users can find basic device information at the top, including the device name, device model, device serial number, MAC address, online duration, and upstream interface address.



Device Information

Name: ER805
Model: ER805-LQ20-WLAN
Serial:
Firmware Version: V2.0.15
MAC:
Uptime: 1 week 2 days 23 ho...
Internet Access: WAN1
Uplink IP: 10.5.29.100
Local Gateway IP: 10.5.22.1
System Time: 2023-10-18 13:30:21 UTC +08:00
License Status: InCloud Manager Branch Pr...

🟩 Connected ▢ Disconnected ⚠ Abnormal ⊘ Disabled

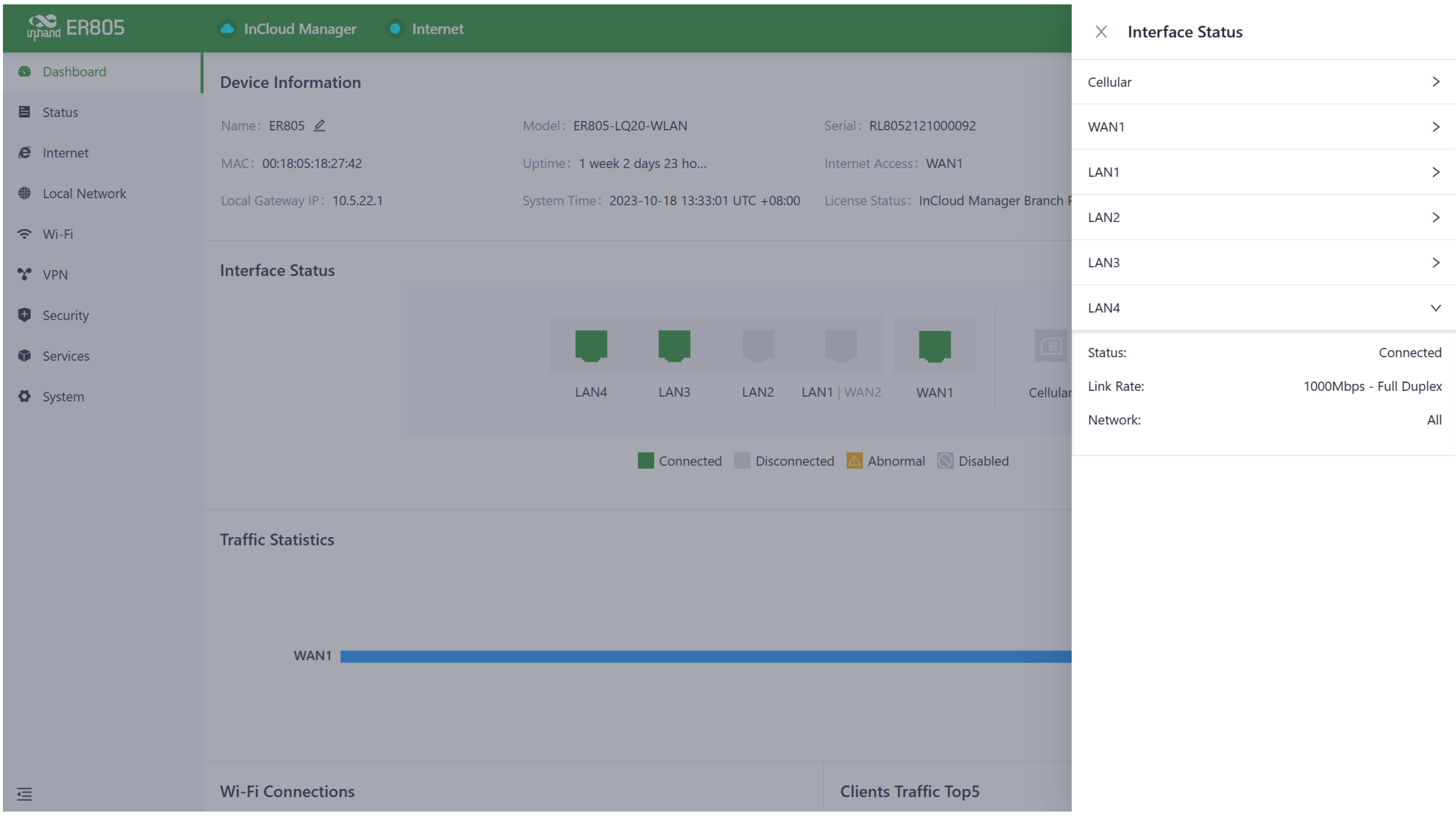
Fig. 5-2-1 Device Information

- **Name: I**dentifies the device's name, which is initially set to "ER805" but can be customized.
- **MAC Address:** Identifies the device's physical MAC address.
- **Local Gateway Address:** The default gateway address of the device's subnet.
- **Model:** Specifies the device's specific model, which can help determine if it supports cellular and WLAN features.
- **Uptime:** Reflects the device's running time since it was powered on.
- **System Time:** Displays the device's time zone and system time.
- **Serial:** A unique code that serves as an identifier for the device and can be used for indexing or adding the device to a platform account.
- **Internet Access:** The upstream interface used by the device for internet connectivity.

- **License Status:** Information about the applied license on the device, distinguishing between Small Star Cloud Manager Basic and Small Star Cloud Manager Professional.
- **Firmware Version:** Shows the device's current software version.
- **Uplin IP:** The IP address of the upstream interface used for device internet connectivity.

5.2.2 Interface Status

In the "Dashboard > Interface Status" feature, you can visually inspect the operational status of each interface. By clicking on the "Interface Icon," you can access detailed information for each interface in a pop-up box on the right-hand side of the interface.



Name: ER805
Model: ER805-LQ20-WLAN
Serial: RL8052121000092
MAC: 00:18:05:18:27:42
Uptime: 1 week 2 days 23 ho...
Internet Access: WAN1
Local Gateway IP: 10.5.22.1
System Time: 2023-10-18 13:33:01 UTC +08:00
License Status: InCloud Manager Branch F

Status: Connected
Link Rate: 1000Mbps - Full Duplex
Network: All

Fig. 5-2-2 Interface Status

5.2.3 Traffic Statistics

Users can monitor the usage of traffic on each upstream interface since the router was powered on through the "Dashboard > Traffic Statistics" feature. The data in traffic statistics will reset after the device is rebooted. If you need to review historical traffic records, you can access this information on the device's details page within InCloud Manager.

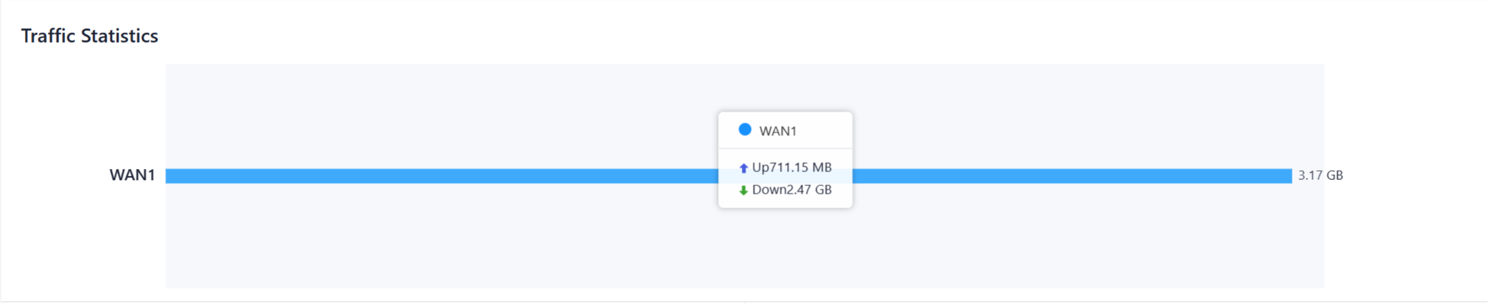


Fig. 5-2-3 Traffic Statistics

5.2.4 Wi-Fi Connections

In the "Dashboard > Wi-Fi Client Count" feature, users can check the number of active SSIDs on the ER805 and the number of connected clients under each SSID.

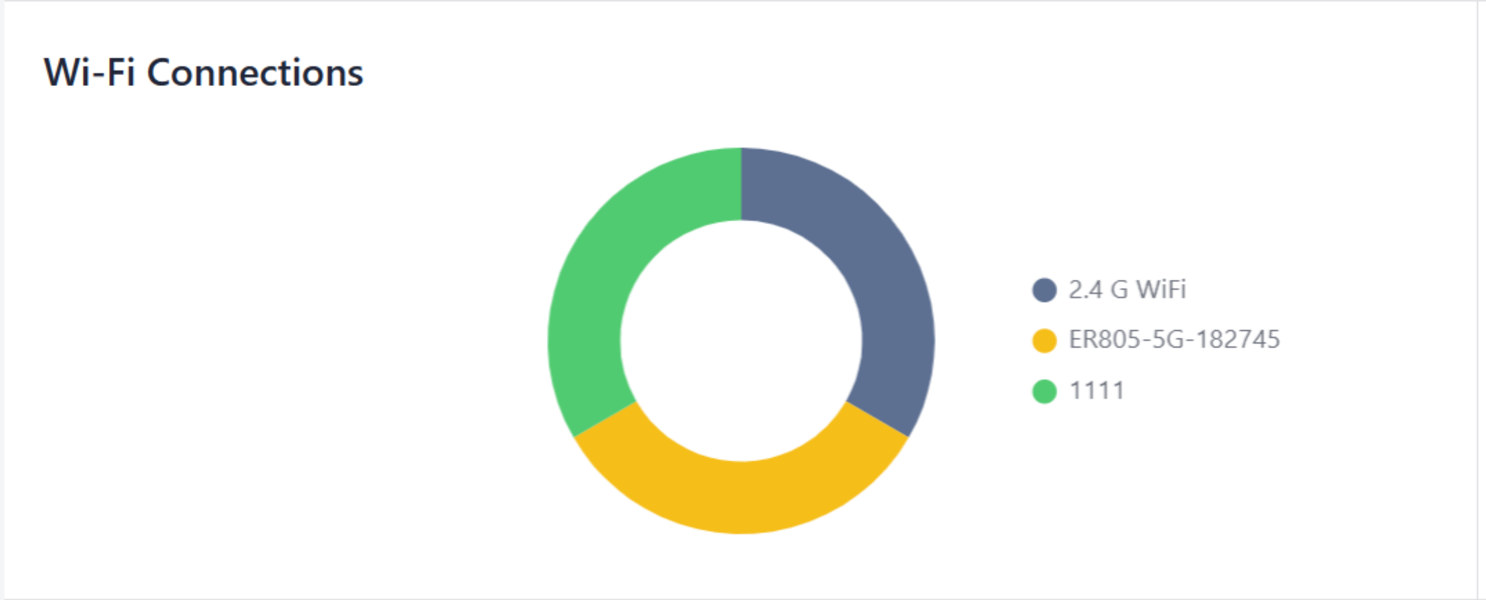


Fig. 5-2-4 The number of clients connected per SSID

5.2.5 Clients Traffic Top 5

In the "Dashboard > Top 5 Client Traffic" feature, users can view the current ranking of client traffic usage for devices connected to the router. It displays up to 5 records, and when a client disconnects, its statistical data will be cleared.

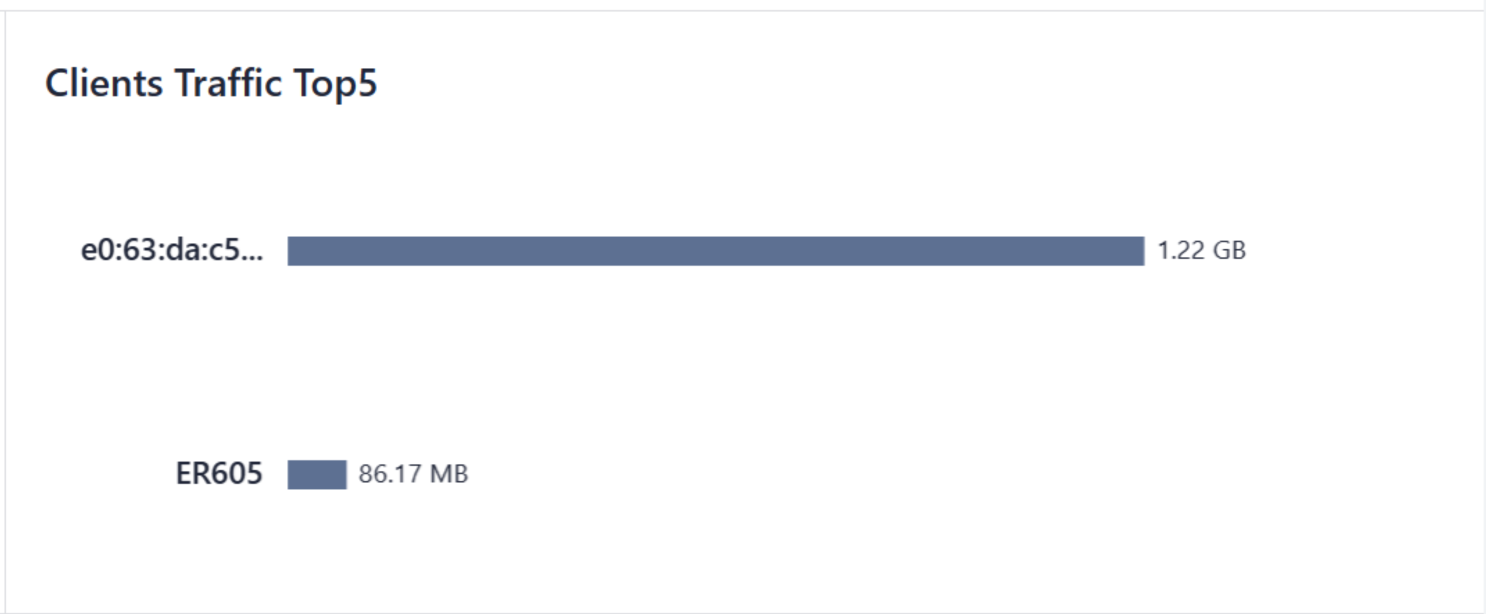
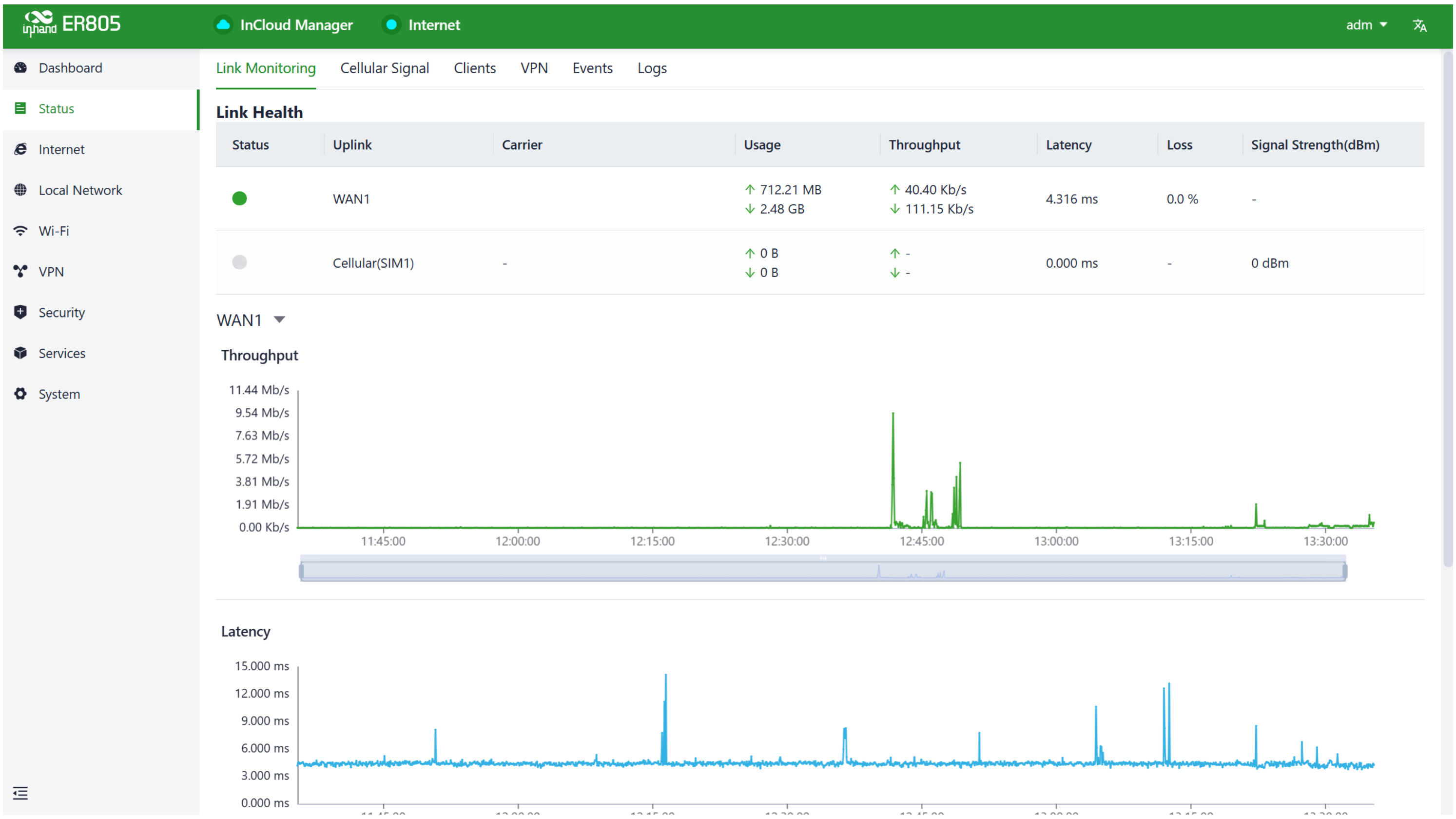


Fig 5-2-5 Top 5 clients by traffic

5.2.6 Link Monitor

You can utilize the "Status > Link Monitoring" feature to check the health status of each upstream link and access information about throughput, latency, packet loss, signal strength, and more for each interface.



Link Health

Status	Uplink	Carrier	Usage	Throughput	Latency	Loss	Signal Strength(dBm)
●	WAN1		↑ 712.21 MB ↓ 2.48 GB	↑ 40.40 Kb/s ↓ 111.15 Kb/s	4.316 ms	0.0 %	-
○	Cellular(SIM1)	-	↑ 0 B ↓ 0 B	↑ - ↓ -	0.000 ms	-	0 dBm

Fig. 5-2-6 Link Monitor interface

5.2.7 Cellular Signals

You can access the "Status > Cellular Signal" feature to check the signal strength of SIM cards under the cellular interface, along with parameters such as RSSI, SINR, RSRP, and more.

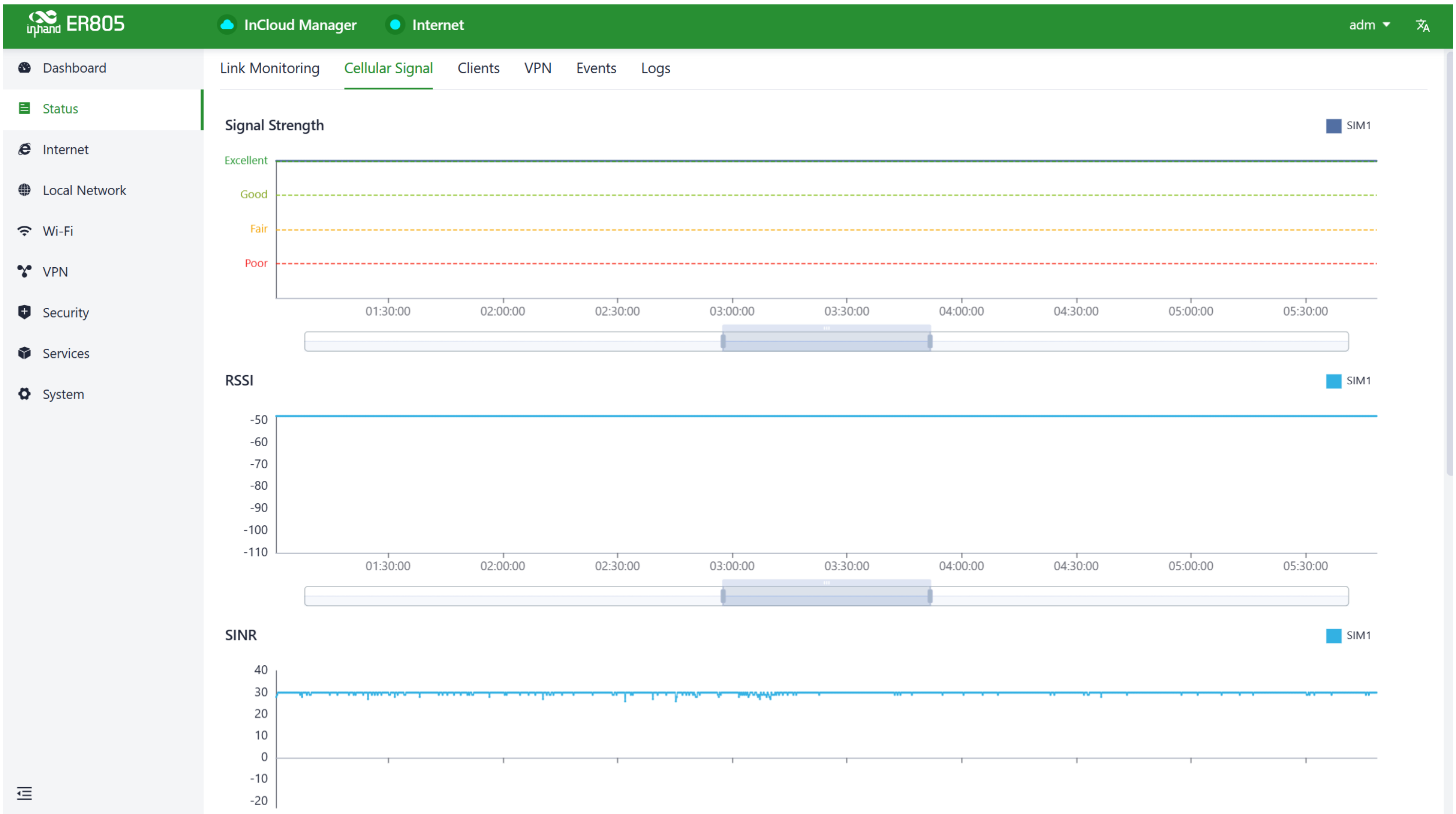
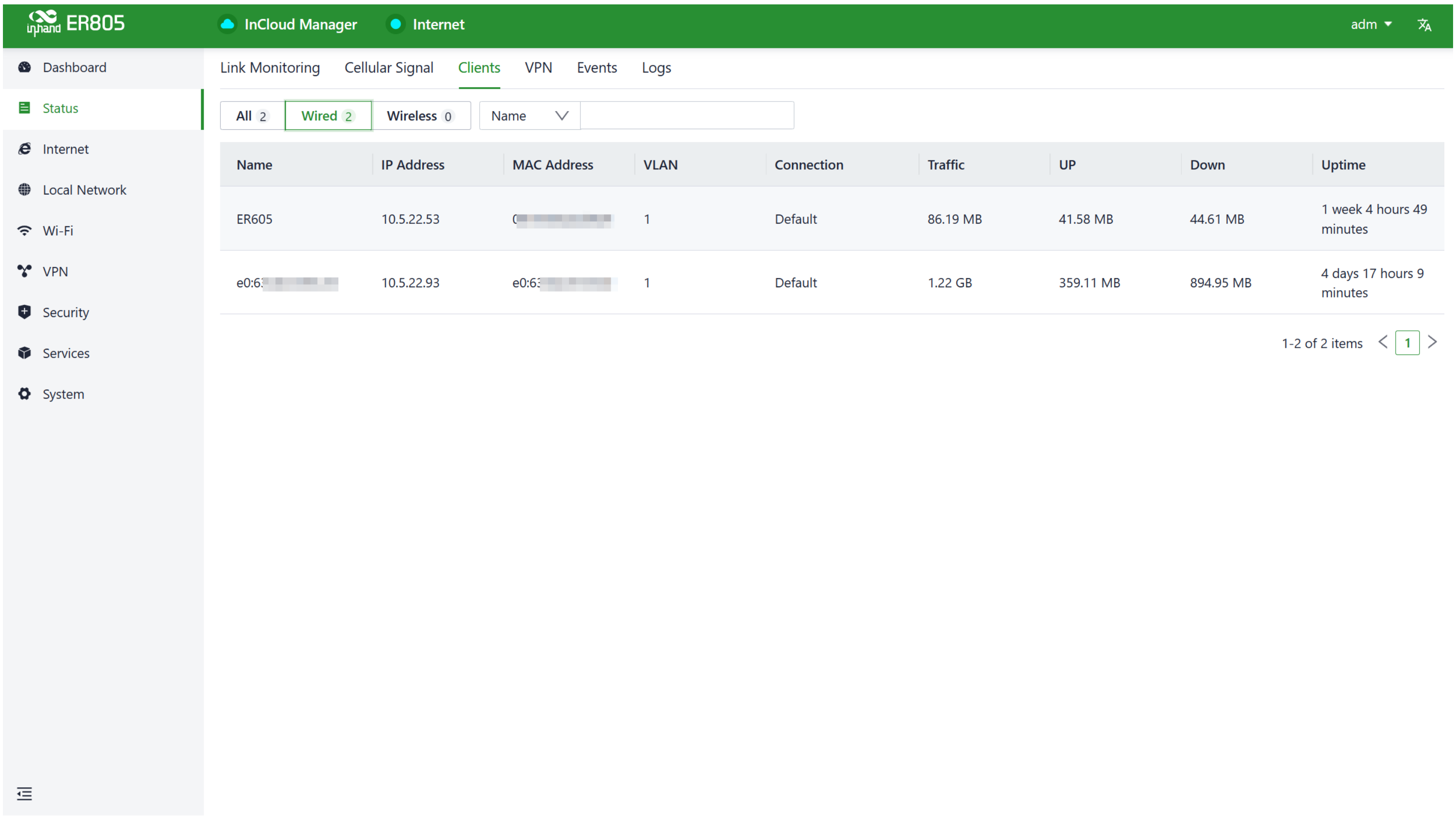


Fig. 5-2-7 Signal Strength

5.2.8 Clients

Through the "Status > Clients" feature, users can view detailed information about both wired and wireless clients connected to the router. This includes details such as names, addresses, MAC addresses, VLANs, connected subnets, traffic usage, online duration, and more.



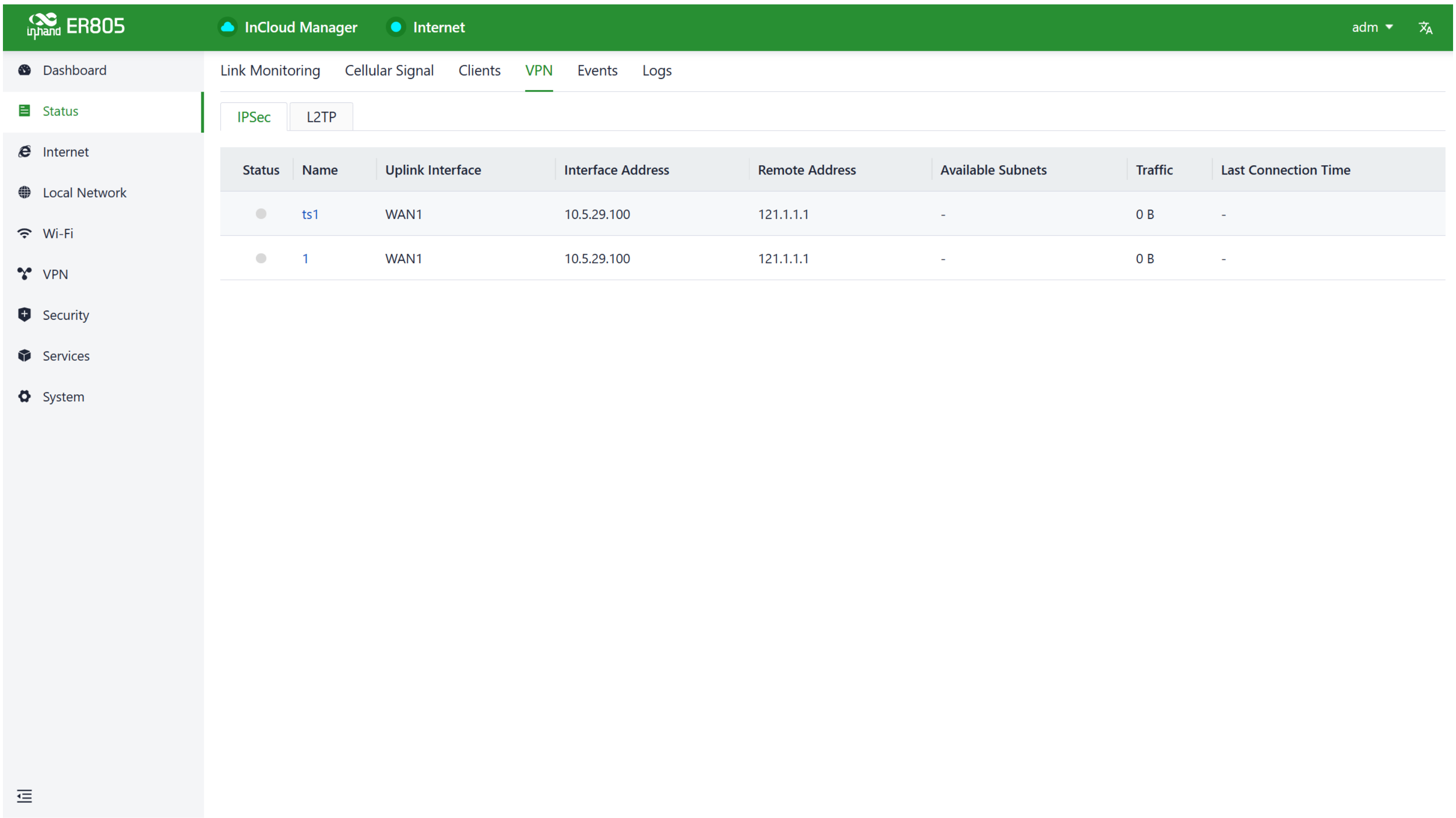
Name	IP Address	MAC Address	VLAN	Connection	Traffic	UP	Down	Uptime
ER605	10.5.22.53	[redacted]	1	Default	86.19 MB	41.58 MB	44.61 MB	1 week 4 hours 49 minutes
e0:6[redacted]	10.5.22.93	e0:6[redacted]	1	Default	1.22 GB	359.11 MB	894.95 MB	4 days 17 hours 9 minutes

1-2 of 2 items < 1 >

Fig. 5-2-8 Clients connected to ER805

5.2.9 VPN

You can access the "Status > VPN" feature to view information about IPSec VPN and L2TP VPN, including their status, traffic, and the duration of the most recent connection.

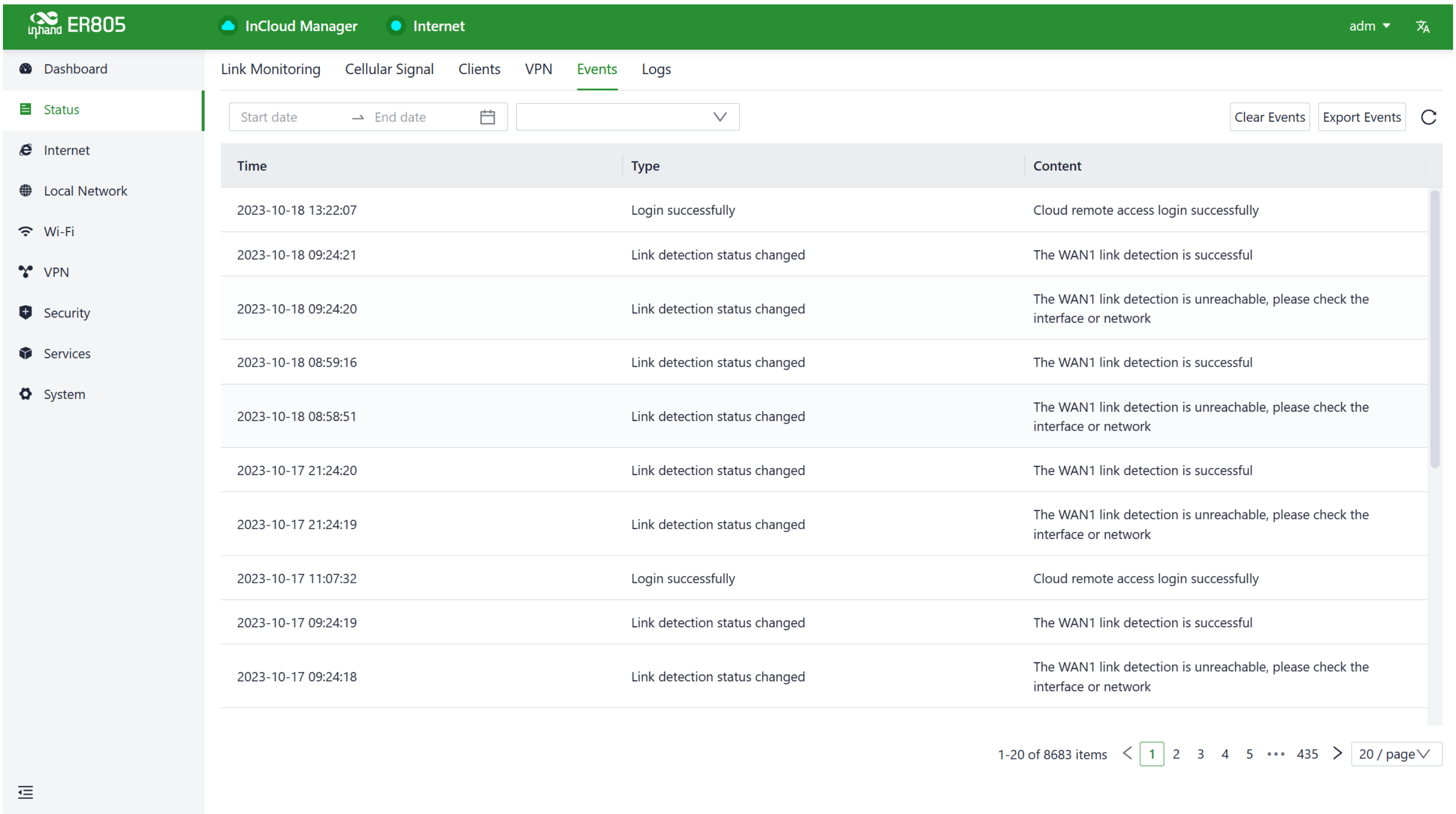


Status	Name	Uplink Interface	Interface Address	Remote Address	Available Subnets	Traffic	Last Connection Time
●	ts1	WAN1	10.5.29.100	121.1.1.1	-	0 B	-
●	1	WAN1	10.5.29.100	121.1.1.1	-	0 B	-

Fig. 5-2-9 VPN Information

5.2.10 Events

You can use the "Status > Events" feature to check event information related to the device's operation, helping users understand the device's operational status.



Time	Type	Content
2023-10-18 13:22:07	Login successfully	Cloud remote access login successfully
2023-10-18 09:24:21	Link detection status changed	The WAN1 link detection is successful
2023-10-18 09:24:20	Link detection status changed	The WAN1 link detection is unreachable, please check the interface or network
2023-10-18 08:59:16	Link detection status changed	The WAN1 link detection is successful
2023-10-18 08:58:51	Link detection status changed	The WAN1 link detection is unreachable, please check the interface or network
2023-10-17 21:24:20	Link detection status changed	The WAN1 link detection is successful
2023-10-17 21:24:19	Link detection status changed	The WAN1 link detection is unreachable, please check the interface or network
2023-10-17 11:07:32	Login successfully	Cloud remote access login successfully
2023-10-17 09:24:19	Link detection status changed	The WAN1 link detection is successful
2023-10-17 09:24:18	Link detection status changed	The WAN1 link detection is unreachable, please check the interface or network

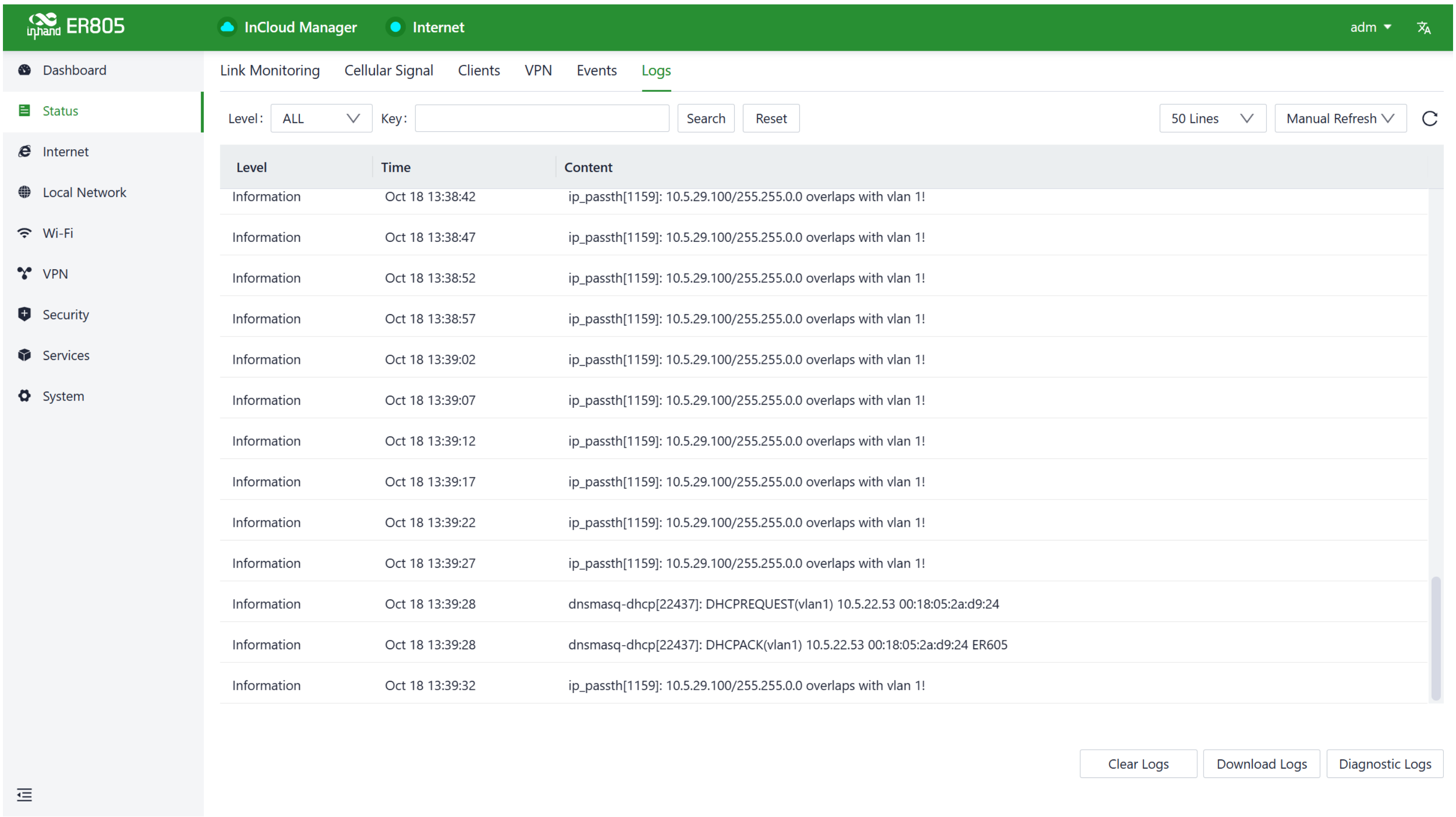
Fig. 5-2-10 Event Types

Currently supported event types:

- Successful/Failed User Logins.
- High CPU Utilization in the Last 5 Minutes.
- High Memory Utilization in the Last 5 Minutes.
- Cellular Traffic Reaches Threshold.
- VPN Status Changes.
- Uplink Status Changes.
- Uplink Switching.
- WAN2/LAN1 Switching.
- Reboot.
- Upgrade.

5.2.11 Logs

Through the "Status > Logs" feature, users can examine the system logs, which contain information about the device's operational history. When the device encounters issues, technical personnel can use these logs for troubleshooting and diagnosis.



Level: ALL Key:

50 Lines Manual Refresh

Level	Time	Content
Information	Oct 18 13:38:42	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:38:47	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:38:52	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:38:57	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:39:02	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:39:07	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:39:12	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:39:17	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:39:22	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:39:27	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!
Information	Oct 18 13:39:28	dnsmasq-dhcp[22437]: DHCPREQUEST(vlan1) 10.5.22.53 00:18:05:2a:d9:24
Information	Oct 18 13:39:28	dnsmasq-dhcp[22437]: DHCPACK(vlan1) 10.5.22.53 00:18:05:2a:d9:24 ER605
Information	Oct 18 13:39:32	ip_passth[1159]: 10.5.29.100/255.255.0.0 overlaps with vlan 1!

Fig. 5-2-11 Logs information

- **Download Logs:** Download the device's operational logs.
- **Download Diagnostic Logs:** Download the device's diagnostic logs, which include system operation logs, device information, and device configurations.
- **Clear Logs:** Clear the device's operational logs; this does not clear the device's diagnostic logs.

6. Configuration

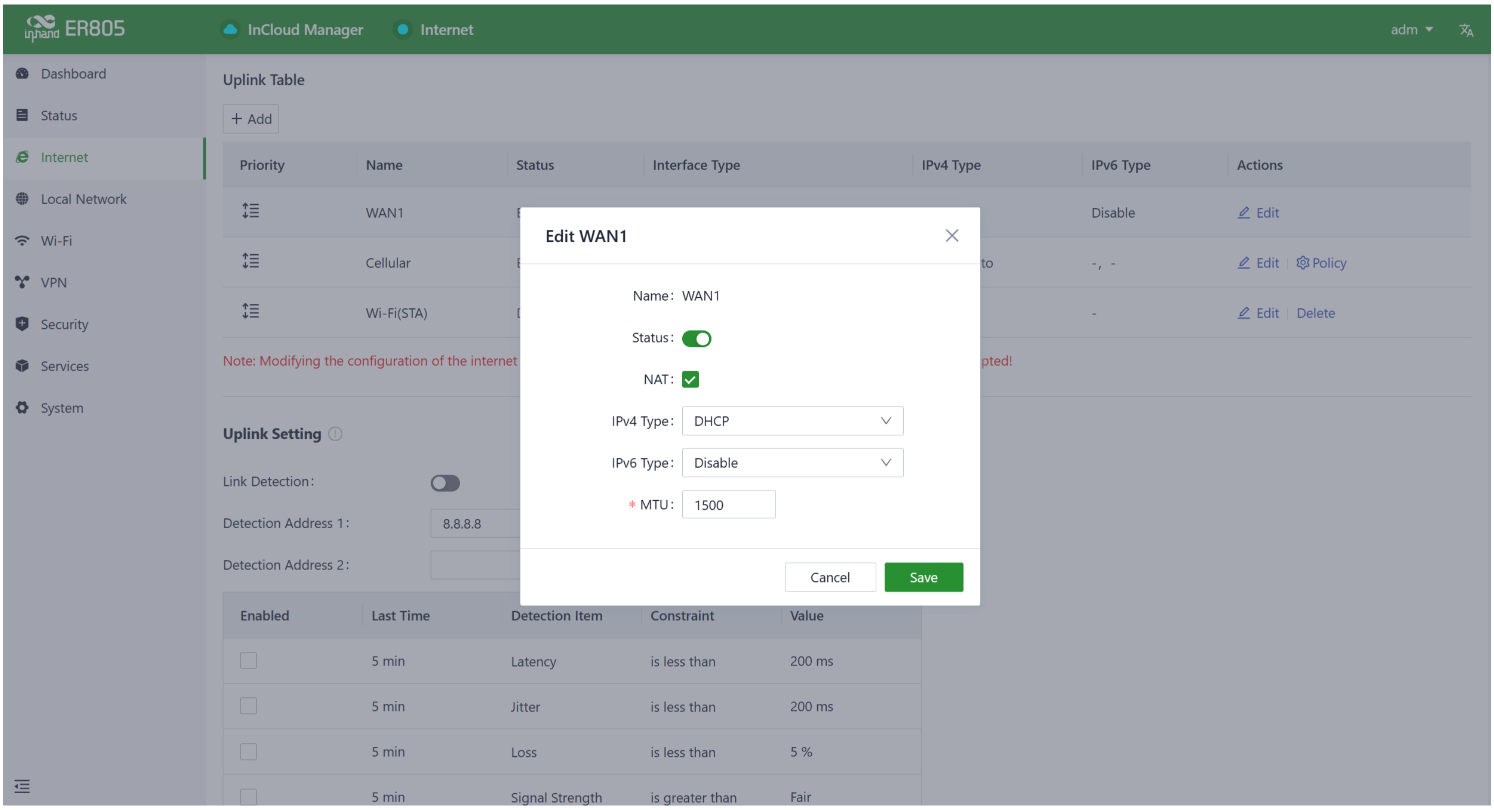
You can achieve batch configuration of devices through the platform's remote configuration. Select the target device, click "Edit" in the remote configuration section, and complete the configuration for the device. Below is an introduction to the configuration for a single device:

6.1 Internet

You can configure the parameters and operational modes of each upstream interface under the "Internet" feature. The ER805 supports three access network modes, including wired, cellular, and Wi-Fi. The device comes with two non-removable upstream links by default, WAN1, and Cellular. It can support up to four upstream links, including WAN1, WAN2, Cellular, and Wi-Fi (STA). WAN2 and Wi-Fi (STA) interfaces need to be manually added and can be removed as needed.

6.1.1 Wired Connection

The ER805 supports three wired internet connection methods: DHCP, Static IP, and PPPoE. You can modify the connection method by clicking on the "Edit" button as shown in the illustration. The default method is "DHCP."



Uplink Table

Priority	Name	Status	Interface Type	IPv4 Type	IPv6 Type	Actions
	WAN1	E			Disable	Edit
	Cellular	E		to	-, -	Edit Policy
	Wi-Fi(STA)	D			-	Edit Delete

Note: Modifying the configuration of the internet … pted!

Edit WAN1

Name: WAN1

Status: ●

NAT: ☑

IPv4 Type: DHCP

IPv6 Type: Disable

* MTU: 1500

Uplink Setting

Link Detection:

Detection Address 1: 8.8.8.8

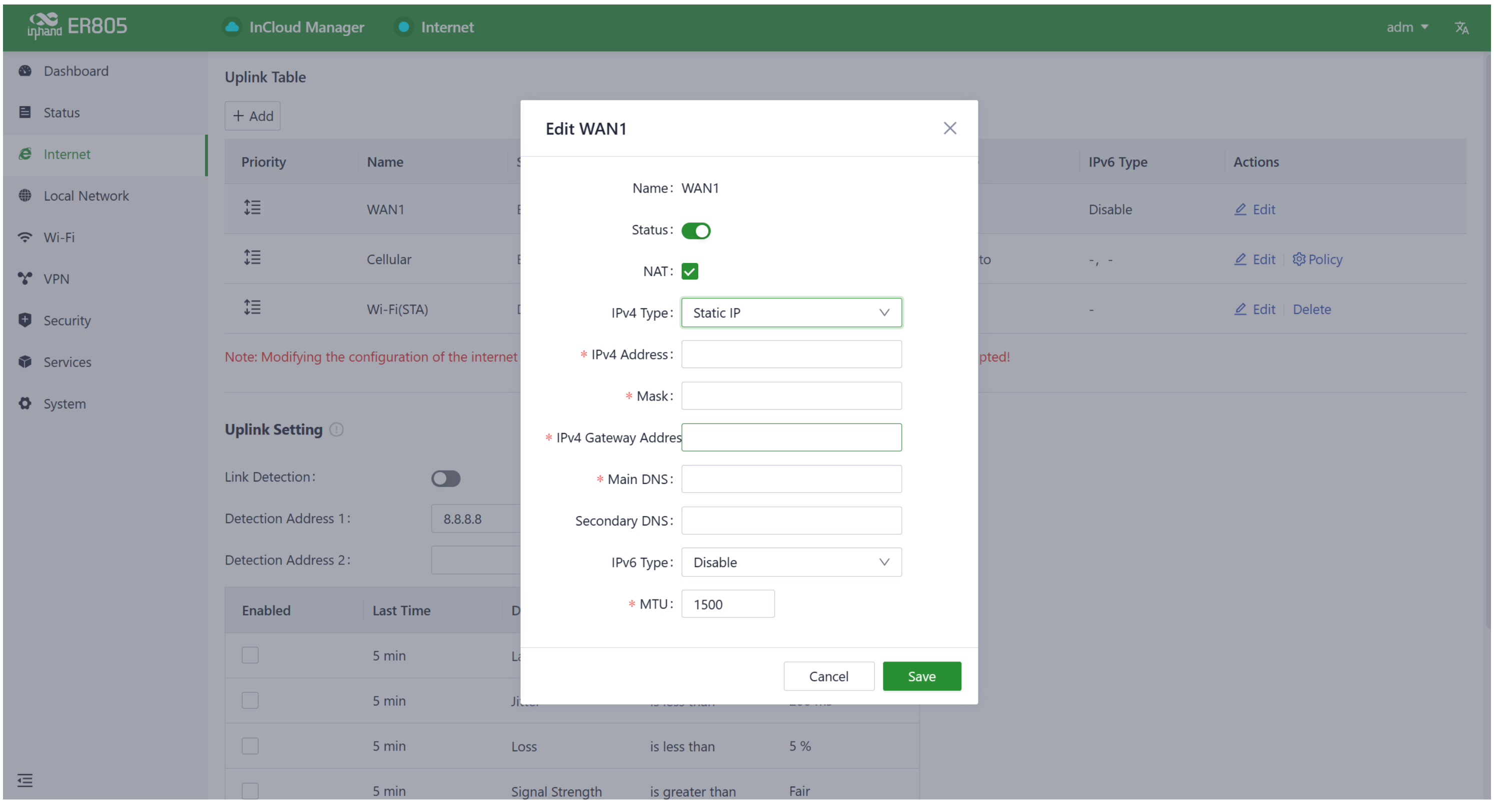
Detection Address 2:

Enabled	Last Time	Detection Item	Constraint	Value
□	5 min	Latency	is less than	200 ms
□	5 min	Jitter	is less than	200 ms
□	5 min	Loss	is less than	5 %
□	5 min	Signal Strength	is greater than	Fair

Fig. 6-1-1-a Edit the WAN1 Interface

- **DHCP**: The device's WAN interface has DHCP service enabled by default. Simply connect the WAN interface to the internet using an Ethernet cable, and it will automatically establish an internet connection.

- **Static IP:** Users have the option to manually configure an address either obtained from their internet service provider or one that is within the same network segment as their upstream device. Once the configuration is complete, the router will access the network via the specified static IP address.



Priority	Name	IPv6 Type	Actions
	WAN1	Disable	Edit
	Cellular	-, -	Edit Policy
	Wi-Fi(STA)	-	Edit Delete

Note: Modifying the configuration of the internet … pted!

Uplink Setting

Link Detection:

Detection Address 1: 8.8.8.8

Detection Address 2:

Enabled	Last Time	D		
□	5 min	La		
□	5 min	Jitter	is less than	200 ms
□	5 min	Loss	is less than	5 %
□	5 min	Signal Strength	is greater than	Fair

Edit WAN1

Name: WAN1

Status: ●

NAT: ☑

IPv4 Type: Static IP

* IPv4 Address:

* Mask:

* IPv4 Gateway Addres

* Main DNS:

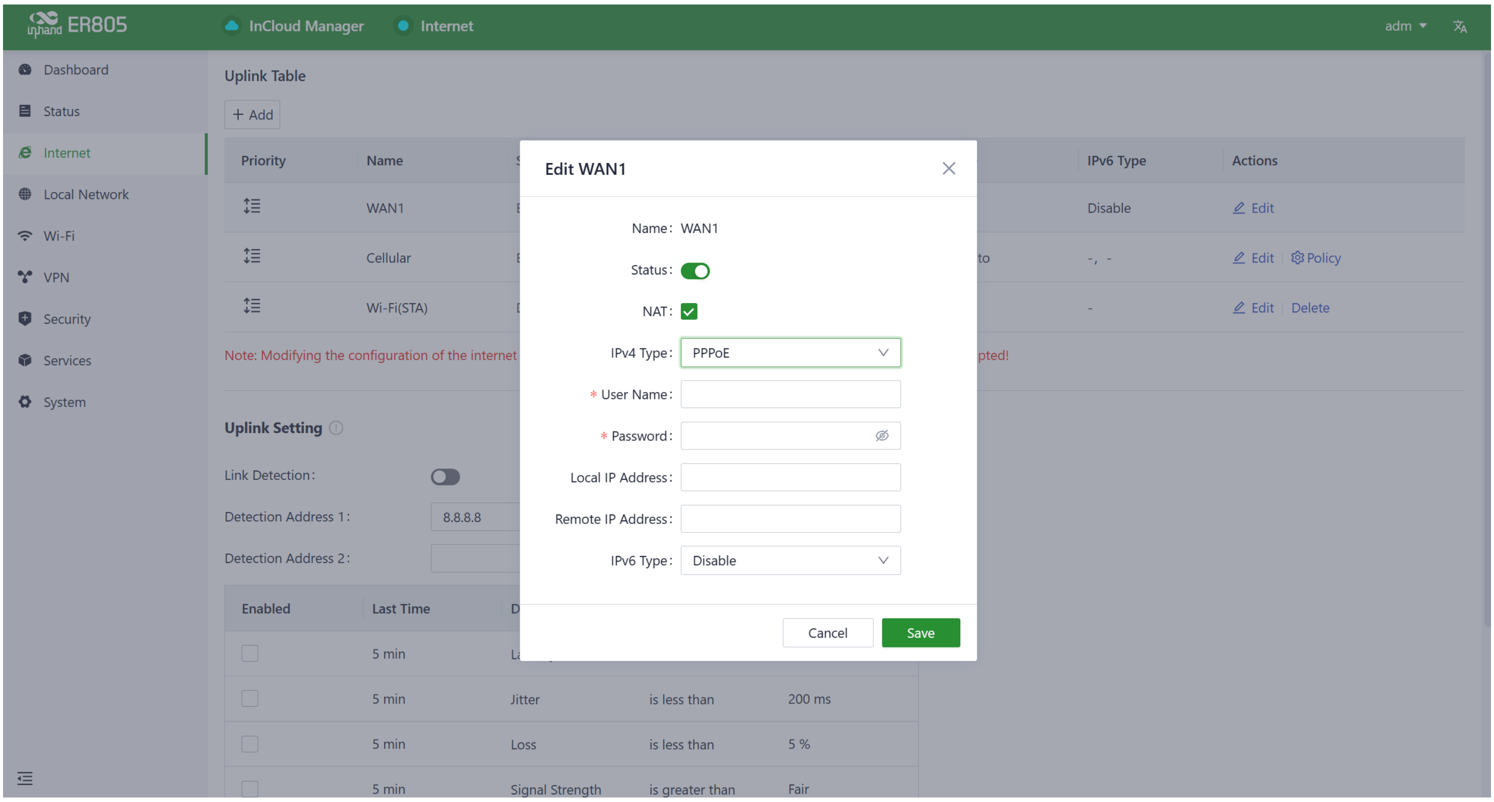
Secondary DNS:

IPv6 Type: Disable

* MTU: 1500

Fig. 6-1-1-b Assigning a static IP to the Router

- **PPPoE:** Users have the option to configure broadband dial-up. Once the configuration is complete, the router will establish an internet connection through the broadband dial-up.



Priority	Name	IPv6 Type	Actions
	WAN1	Disable	Edit
	Cellular	-, -	Edit Policy
	Wi-Fi(STA)	-	Edit Delete

Note: Modifying the configuration of the internet … pted!

Uplink Setting

Link Detection:

Detection Address 1: 8.8.8.8

Detection Address 2:

Enabled	Last Time	D		
□	5 min	La		
□	5 min	Jitter	is less than	200 ms
□	5 min	Loss	is less than	5 %
□	5 min	Signal Strength	is greater than	Fair

Edit WAN1

Name: WAN1

Status: ●

NAT: ☑

IPv4 Type: PPPoE

* User Name:

* Password:

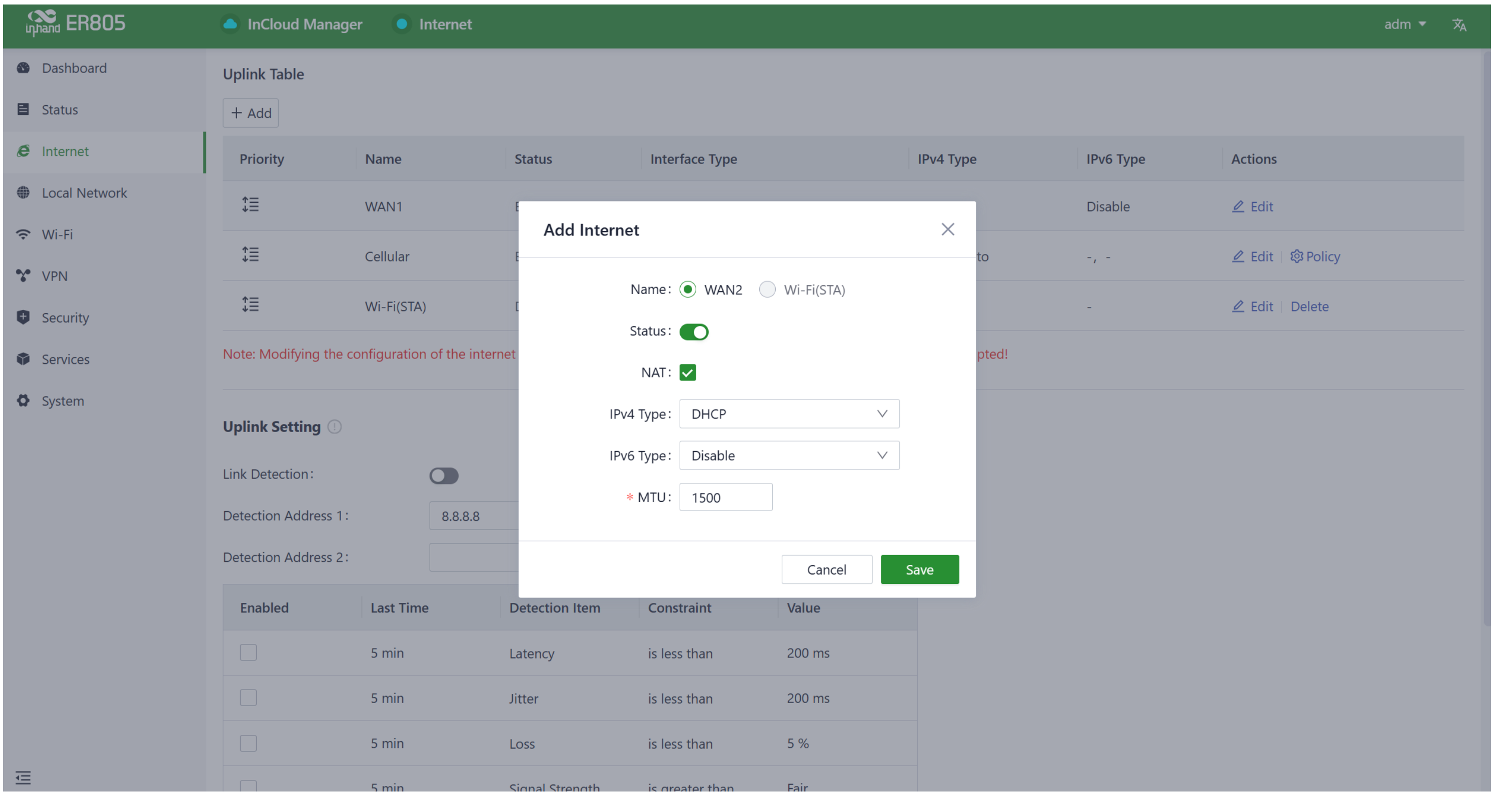
Local IP Address:

Remote IP Address:

IPv6 Type: Disable

Fig. 6-1-1-c Set up Dial-up Internet Access

When you require dual WAN connections, they can click the "Add" button in the [Internet] menu to add the WAN2 interface. The WAN2 interface supports the same configuration options as the WAN1 interface.



Uplink Table

+ Add

Priority	Name	Status	Interface Type	IPv4 Type	IPv6 Type	Actions
	WAN1				Disable	Edit
	Cellular				-, -	Edit Policy
	Wi-Fi(STA)				-	Edit Delete

Note: Modifying the configuration of the internet ... pted!

Uplink Setting

Link Detection:

Detection Address 1: 8.8.8.8

Detection Address 2:

Enabled	Last Time	Detection Item	Constraint	Value
□	5 min	Latency	is less than	200 ms
□	5 min	Jitter	is less than	200 ms
□	5 min	Loss	is less than	5 %
□	5 min	Signal Strength	is greater than	Fair

Add Internet

Name: ● WAN2 ○ Wi-Fi(STA)

Status: on

NAT: ☑

IPv4 Type: DHCP

IPv6 Type: Disable

* MTU: 1500

Cancel | Save

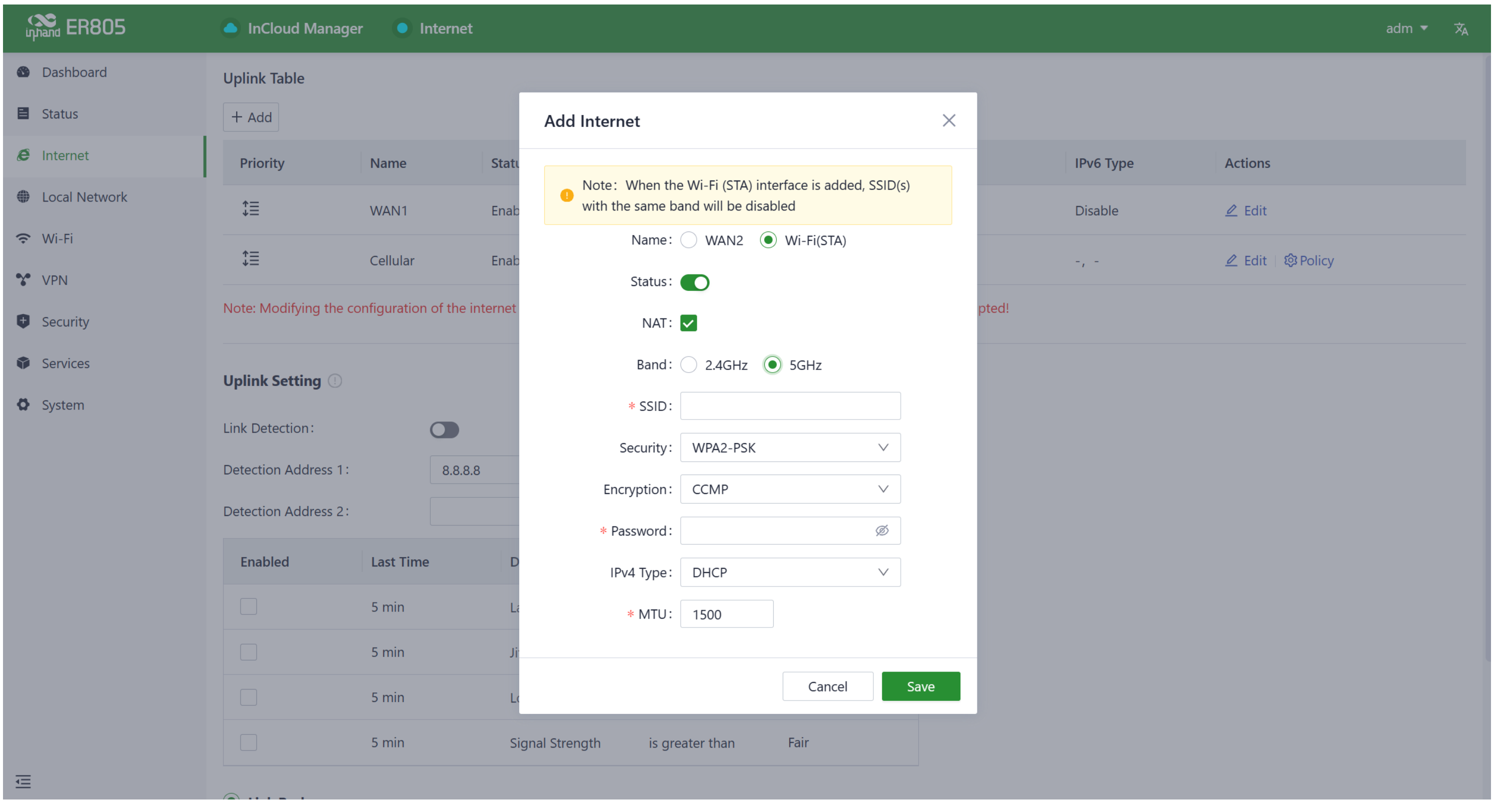
Fig. 6-1-1-d Add WAN2 Interface

Note:

- After adding the WAN2 interface, the original LAN1 interface role will switch to WAN2.
- After deleting the WAN2 interface, the WAN2 interface role will switch back to LAN1.
- After deleting WAN2, all configuration related to the WAN2 interface, including static routes, inbound/outbound rules, port forwarding, policy routing, and traffic shaping settings will be removed.

6.1.2 Wireless Connection

The ER805 supports connecting as a client to an on-site AP's network. To do this, click on the "Add" button as shown in the illustration, select "Wi-Fi (STA)," and fill in the required parameters, including the SSID name and password.



Add Internet

Note: When the Wi-Fi (STA) interface is added, SSID(s) with the same band will be disabled

Name: ○ WAN2 ● Wi-Fi(STA)

Status: on

NAT: ☑

Band: ○ 2.4GHz ● 5GHz

* SSID:

Security: WPA2-PSK

Encryption: CCMP

* Password:

IPv4 Type: DHCP

* MTU: 1500

Cancel Save

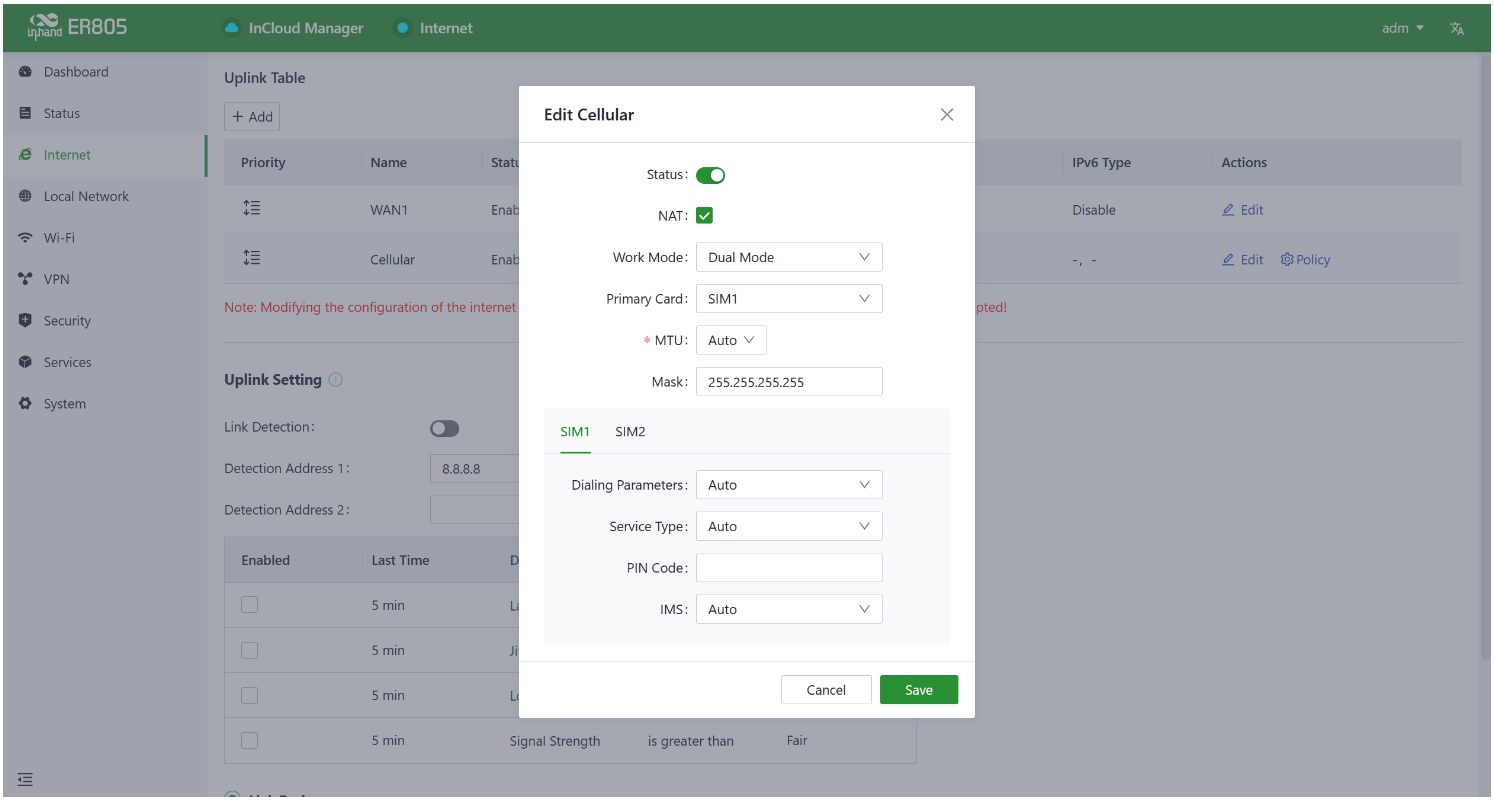
Fig. 6-1-2 Add Wi-Fi(STA) Interface

Cautions:

- Upon adding Wi-Fi (STA), ER805 will automatically disable SSIDs in the same frequency band within the Wi-Fi settings, and the status field for those SSIDs cannot be modified.
- After removing Wi-Fi (STA), the “Status” field and SSIDs in the same frequency band within the Wi-Fi settings can be modified.
- When Wi-Fi (STA) is deleted, all configuration associated with the Wi-Fi (STA) interface, including static routes, inbound/outbound rules, port forwarding, policy routing, and traffic shaping settings, will be removed

6.1.3 5G/4G Connection

In the usual scenario, as per the instructions, upon inserting the SIM card and connecting the Wi-Fi antennas, the ER805 router will automatically establish a dial-up connection and connect to the network when powered on. To configure APN (Access Point Name) parameters, users can select the "Cellular" interface in the [Internet] menu and click the "Edit" button to access the APN parameter configuration interface.



Edit Cellular

Status: ●

NAT: ☑

Work Mode: Dual Mode

Primary Card: SIM1

* MTU: Auto

Mask: 255.255.255.255

SIM1 | SIM2

Dialing Parameters: Auto

Service Type: Auto

PIN Code:

IMS: Auto

Priority	Name	Statu	IPv6 Type	Actions
	WAN1	Enab	Disable	Edit
	Cellular	Enab	-, -	Edit Policy

Note: Modifying the configuration of the internet ... pted!

Link Detection: ○

Detection Address 1: 8.8.8.8

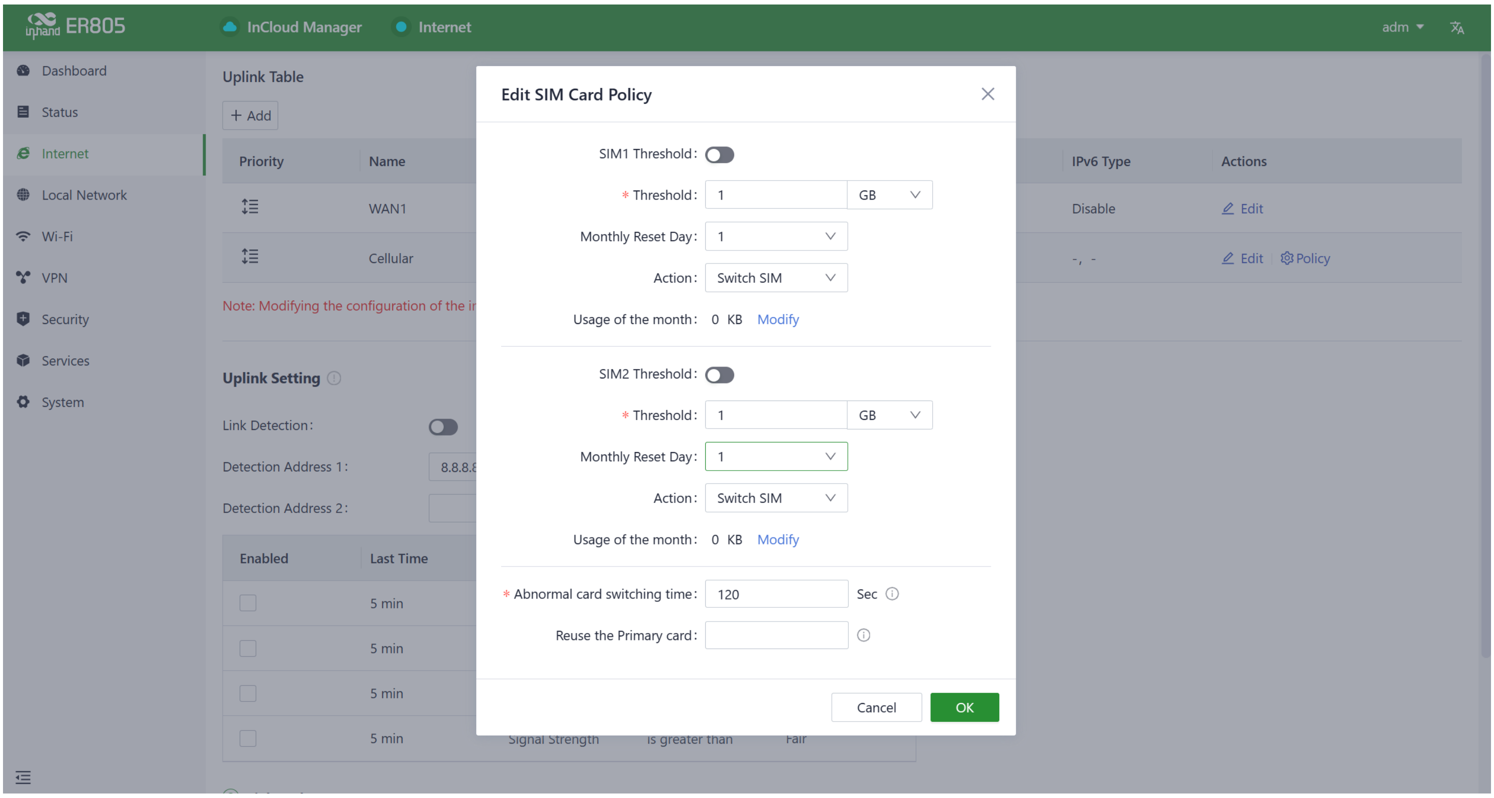
Detection Address 2:

Enabled	Last Time	D		
□	5 min	L		
□	5 min	Ji		
□	5 min	L		
□	5 min	Signal Strength	is greater than	Fair

Fig. 6-1-3-a Edit the cellular Interface

The ER805, in addition to supporting cellular internet access, now includes a traffic policy feature. Once the policy is enabled, the SIM card will take specific actions when the traffic reaches a threshold. Traffic usage statistics will reset at the beginning of the next month.

You can select the "Cellular" interface in the [Internet] menu and click the "Policy" button to access the SIM card’s policy parameter configuration interface.



Edit SIM Card Policy

SIM1 Threshold: ○

* Threshold: 1 GB

Monthly Reset Day: 1

Action: Switch SIM

Usage of the month: 0 KB Modify

SIM2 Threshold: ○

* Threshold: 1 GB

Monthly Reset Day: 1

Action: Switch SIM

Usage of the month: 0 KB Modify

* Abnormal card switching time: 120 Sec

Reuse the Primary card:

Fig. 6-1-3-b Edit the SIM cards' traffice policy

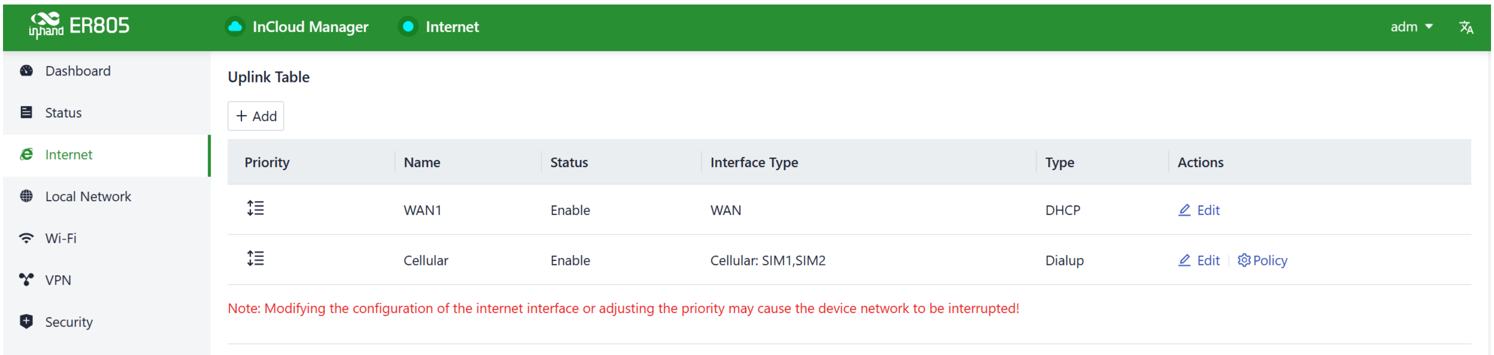
- Actions: These are the actions triggered when SIM card traffic reaches a threshold.
  - Notification: It generates an event when traffic reaches the threshold but does not stop forwarding regular business traffic.
  - Cloud Management Only: It generates an event when traffic reaches the threshold, allowing only the forwarding of cloud-based management traffic while blocking access to the internet for regular business traffic.
  - Switch the SIM card: It generates an event when traffic reaches the threshold and switches to another SIM card for internet access.

Cautions:

- In certain dedicated network scenarios, it may be necessary to manually disable the "Link Detection" function under the [Internet] menu to prevent cellular connectivity issues caused by unsuccessful detection.
- In some cases, manual configuration of the subnet mask for the cellular interface may be required to ensure the proper functioning of the ARP (Address Resolution Protocol) feature.
- When inserting or removing a SIM card, it is essential to disconnect the power to prevent data loss or damage to the device.

6.1.4 Uplink Table

You can edit the WAN1 and Cellular interfaces and add/edit/remove WAN2 and Wi-Fi (STA) interfaces in the "Internet > Upstream Link List." You can also adjust the priority of each interface by dragging the "Priority" icon. Interfaces are arranged from top to bottom based on their priority, with higher priority interfaces taking precedence in determining the current upstream interface for device operation.



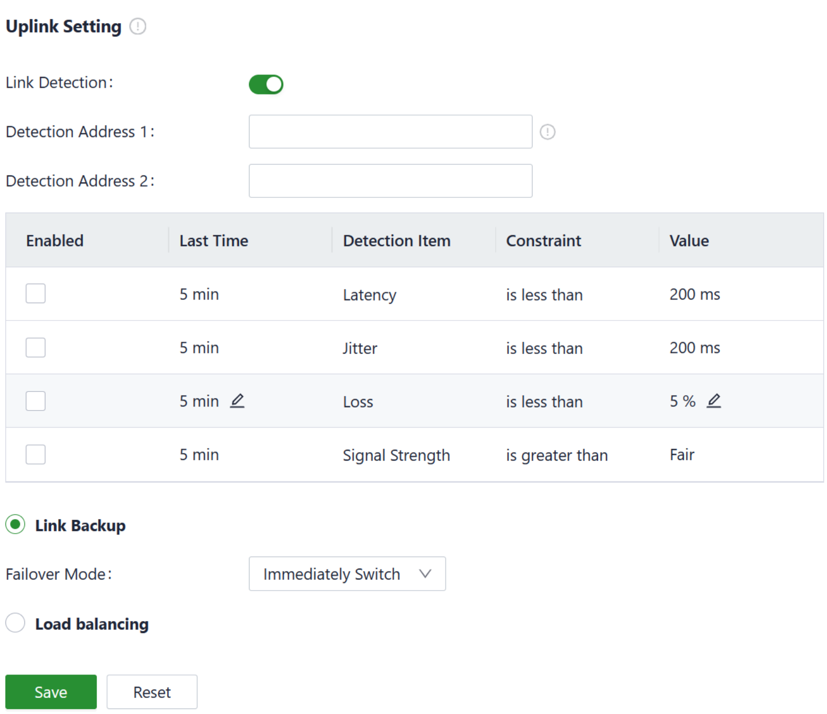
Priority	Name	Status	Interface Type	Type	Actions
⇅	WAN1	Enable	WAN	DHCP	Edit
⇅	Cellular	Enable	Cellular: SIM1,SIM2	Dialup	Edit | Policy

Note: Modifying the configuration of the internet interface or adjusting the priority may cause the device network to be interrupted!

Fig. 6-1-4 Uplink Table Interface

6.1.5 Uplink Settings

You can configure link detection settings and establish collaboration modes between different upstream interfaces through the "Internet > Upstream Link Settings" feature.



Uplink Setting

Link Detection: ●

Detection Address 1:

Detection Address 2:

Enabled	Last Time	Detection Item	Constraint	Value
□	5 min	Latency	is less than	200 ms
□	5 min	Jitter	is less than	200 ms
□	5 min	Loss	is less than	5 %
□	5 min	Signal Strength	is greater than	Fair

● **Link Backup**

Failover Mode: Immediately Switch

○ **Load balancing**

Fig. 6-1-4 Uplink Settings Interface

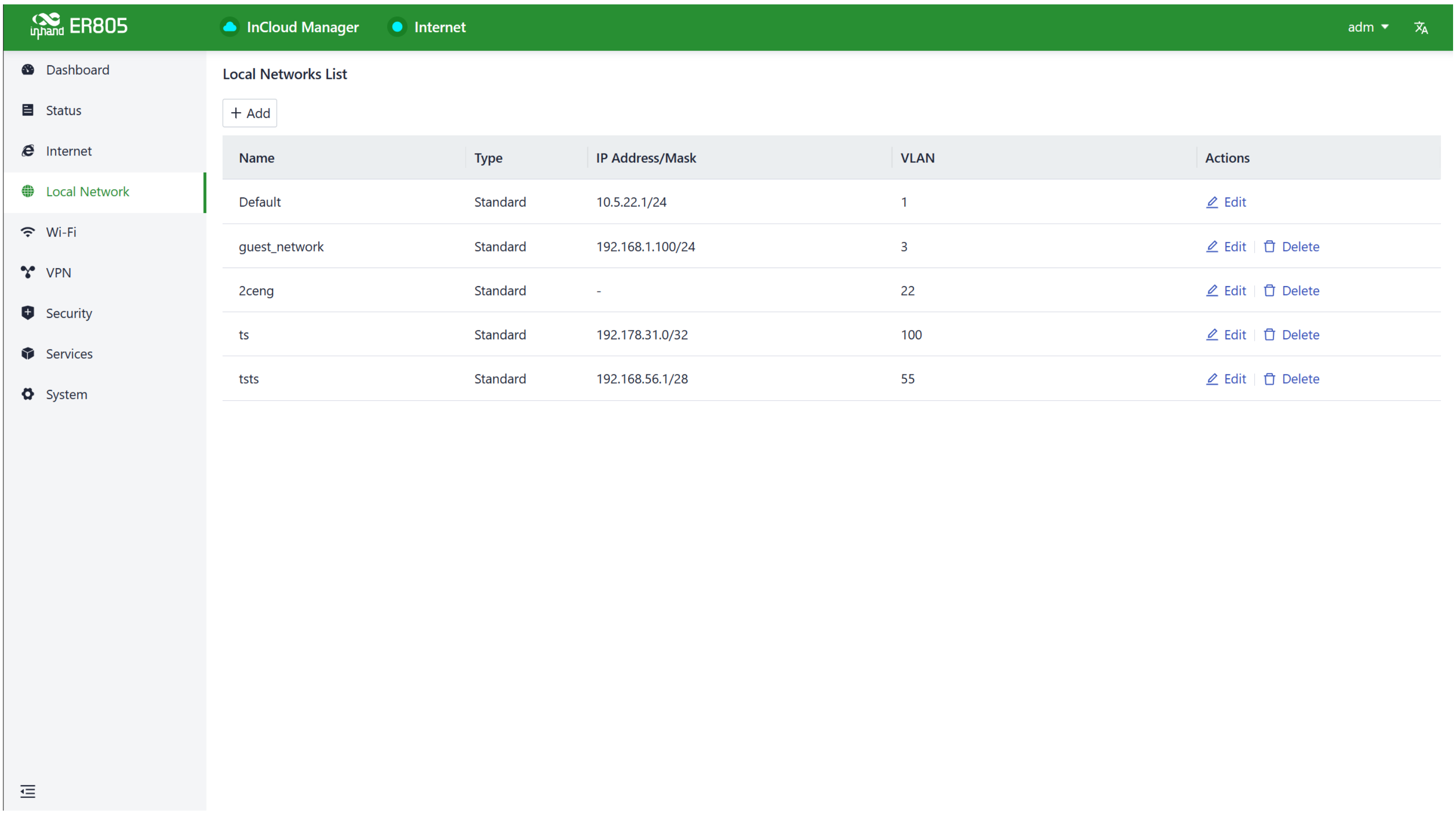
Link Detection Switch: The device has link detection functionality enabled by default. However, in certain specialized network environments where external communication is not possible, users may need to manually disable link detection. When link detection is turned off, users won't be able to view latency, jitter, packet loss, signal strength, and other information for upstream interfaces in the [Status] menu.

Notes:

- Modifying settings in the Internet menu can potentially lead to a disruption in device connectivity. Exercise caution when making changes.
- When the link detection address is left empty, the default behavior is to detect the DNS address via the upstream interface. If you specify a detection address, all upstream interfaces will only detect the address you provided.
- In the router's link backup mode, users can customize detection parameters, and the device will switch links based on the enabled detection items. When detection items are not enabled, upstream link switching will only occur based on priority and link connectivity.
- In the device's load balancing mode, all operational upstream links will forward business traffic, provided they are functioning correctly.

6.2 Local Network

In the [Local Network] feature, users have the flexibility to define their local subnets. This includes configuring the address range, VLAN ID, DHCP services, and other related parameters for the local LAN. Once the configuration is complete, users need to further apply these settings to the device's LAN port through [Interface Management] or apply them to the desired SSID in the Wi-Fi settings. This series of operations is intended to ensure that client devices can smoothly connect to the local network according to the planned network addresses.

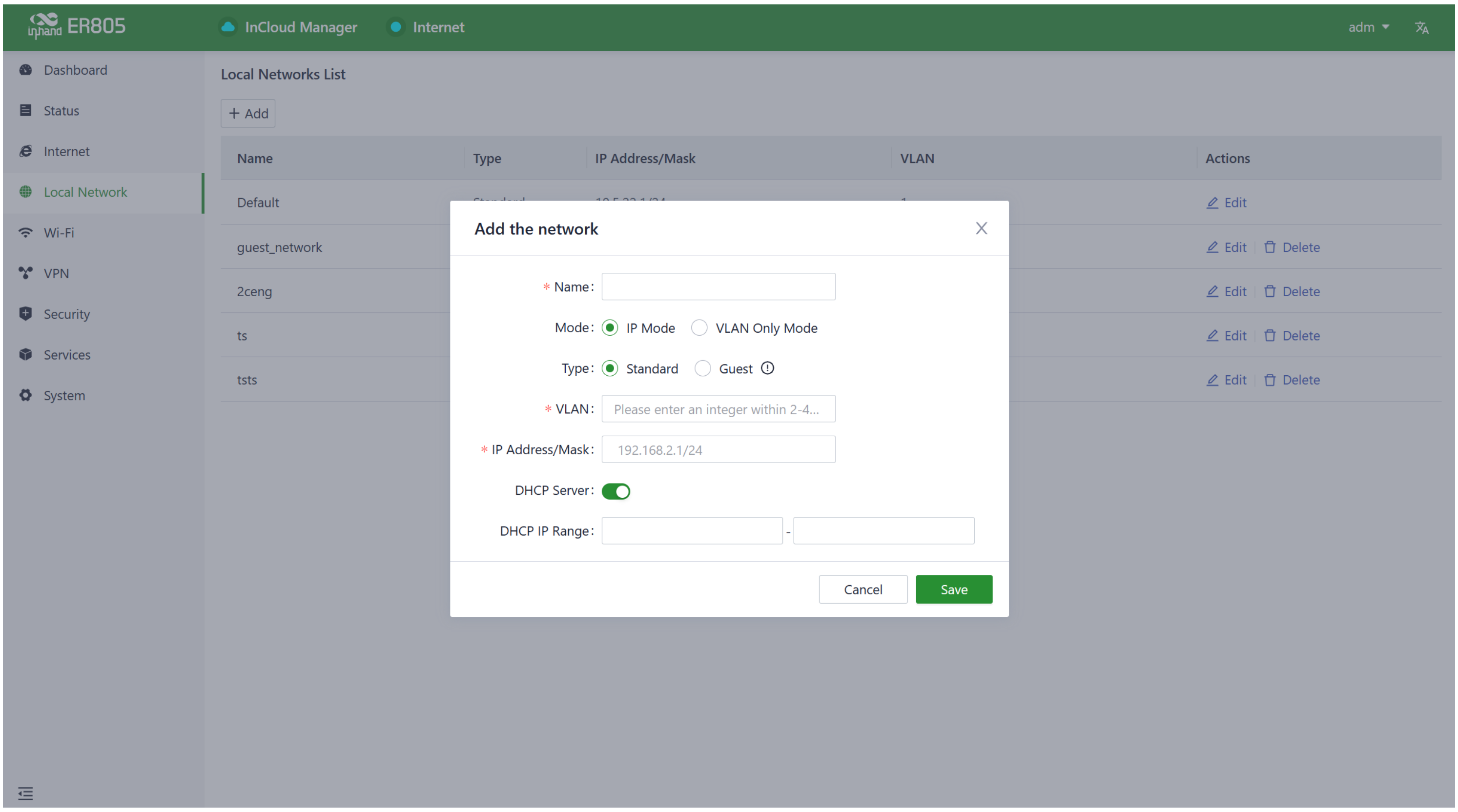


Local Networks List

Name	Type	IP Address/Mask	VLAN	Actions
Default	Standard	10.5.22.1/24	1	Edit
guest_network	Standard	192.168.1.100/24	3	Edit | Delete
2ceng	Standard	-	22	Edit | Delete
ts	Standard	192.178.31.0/32	100	Edit | Delete
tsts	Standard	192.168.56.1/28	55	Edit | Delete

Fig 6-2-a Local Network List

Click the "Add/Edit" button to add a new local network or edit an existing one.



Add the network

* Name:

Mode: ● IP Mode ○ VLAN Only Mode

Type: ● Standard ○ Guest

* VLAN: Please enter an integer within 2-4...

* IP Address/Mask: 192.168.2.1/24

DHCP Server: ●

DHCP IP Range: -

Fig. 6-2-b Add/Edit the local network

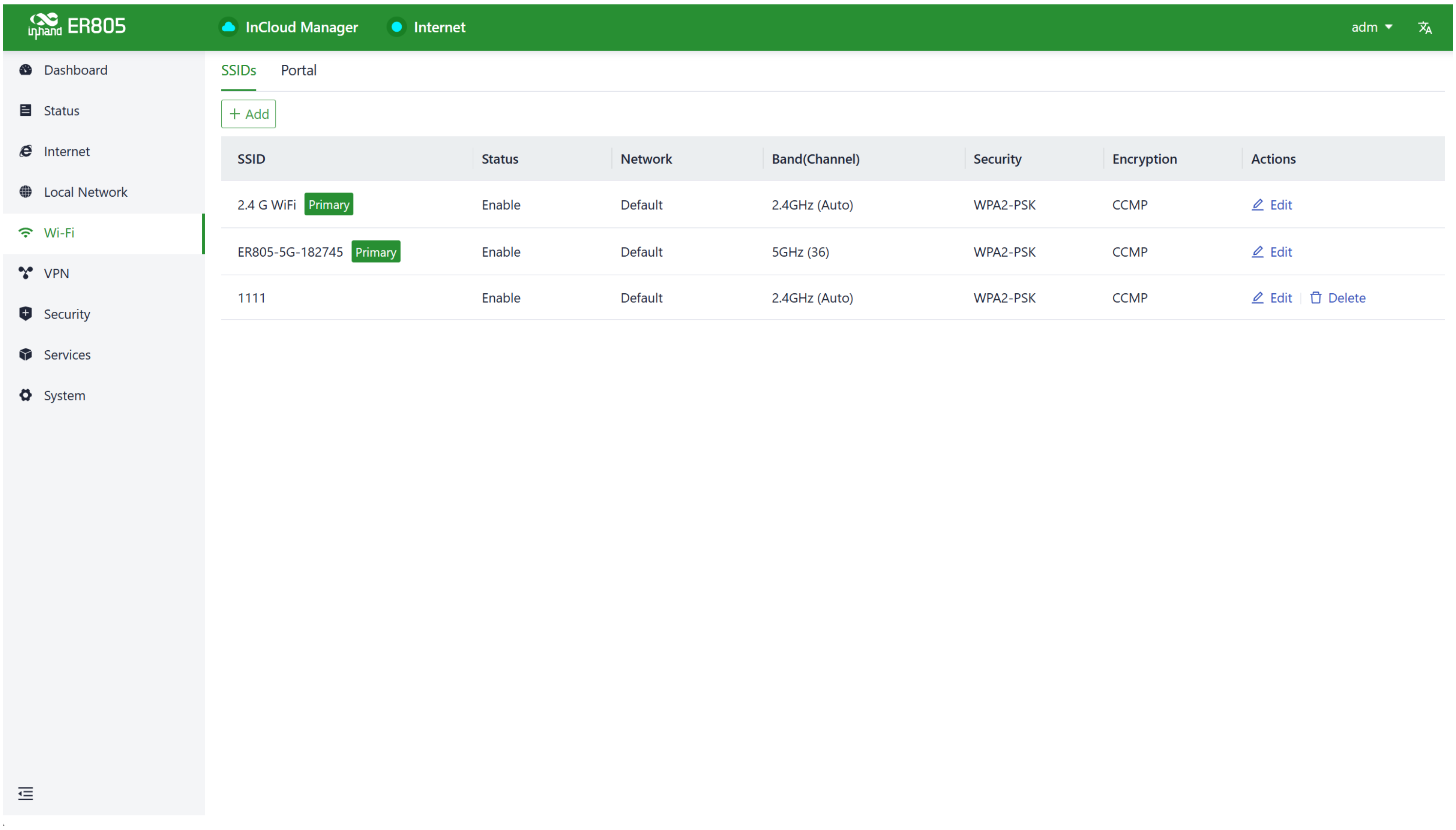
Name: Used to identify the network. Users can select this name to apply the network in both [Wi-Fi] and [Interface Management].
Mode: Choose whether the current subnet operates in 2-layer transparent mode or 3-layer IP mode. The default is "IP mode."
VLAN: This allows for the division of the local network into different virtual logical networks. The default VLAN for all interfaces and Wi-Fi is "default (VLAN1)."
IP Address/Subnet Mask: This is the gateway address for accessing the router through the LAN port or Wi-Fi. The default is "192.168.2.1."
DHCP Server: Clients connecting to the router can obtain IP addresses through this function. It is enabled by default, and the address range is generated based on the "IP Address/Subnet Mask."

Note:

- The default local network cannot be deleted, and you can only modify the IP address/subnet mask and DHCP server settings.
- Once a local network is added, you cannot change its mode.
- The VLAN Only mode is designed for 2-layer transparent operation and doesn't require configuration of IP address/subnet mask or DHCP server settings.

6.3 Wi-Fi

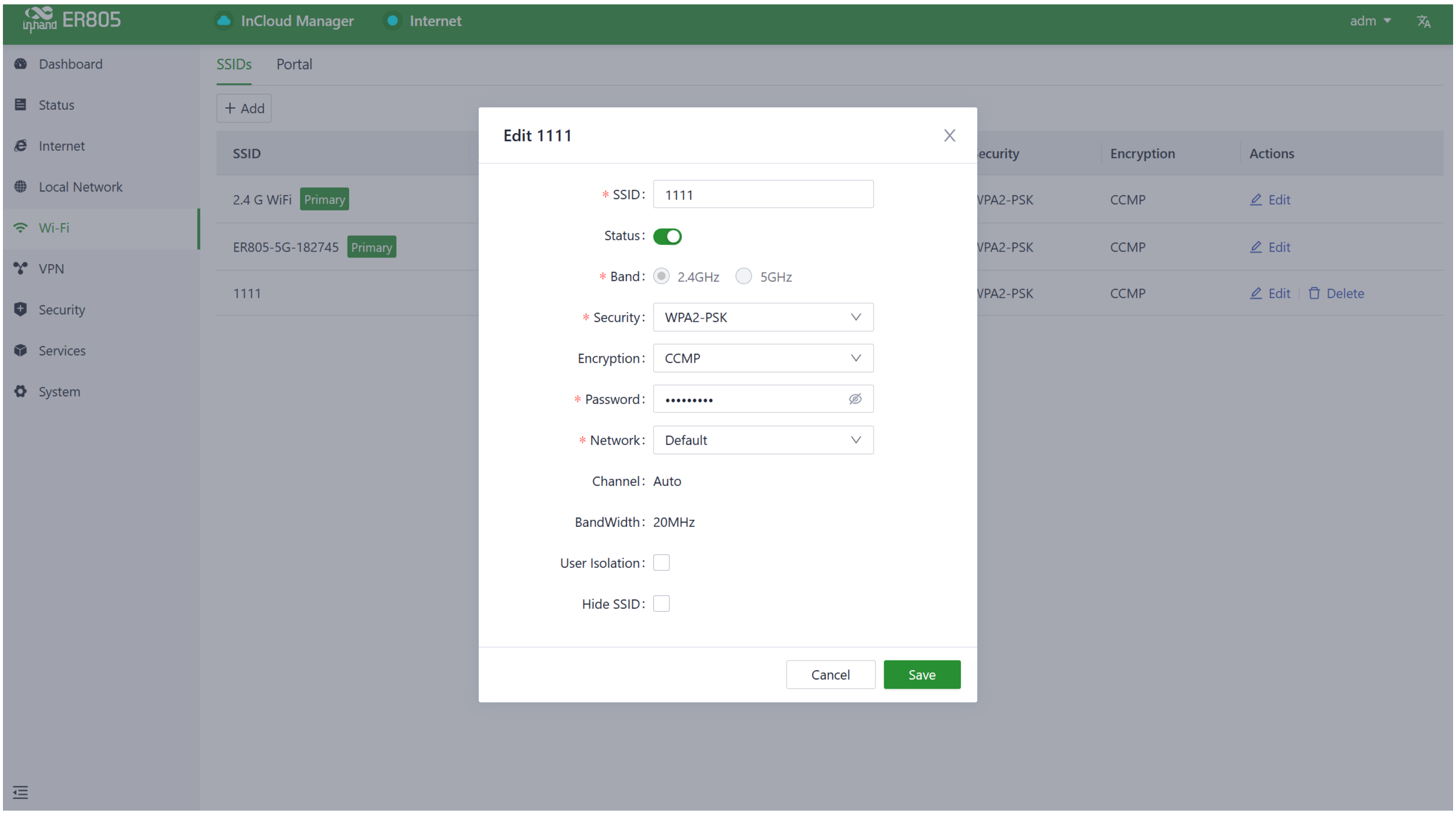
Wi-Fi is a widely used wireless communication technology that enables computers, smartphones, tablets, and other devices to connect to the internet or a local network. Wi-Fi technology allows devices to transmit data over a certain range through wireless signals, providing the convenience of accessing networks without the need for physical connections.
The ER805 can function as an Access Point (AP) to provide multiple SSID wireless network access. Users have the flexibility to customize different SSIDs for various purposes and configurations.



SSID	Status	Network	Band(Channel)	Security	Encryption	Actions
2.4 G WiFi Primary	Enable	Default	2.4GHz (Auto)	WPA2-PSK	CCMP	Edit
ER805-5G-182745 Primary	Enable	Default	5GHz (36)	WPA2-PSK	CCMP	Edit
1111	Enable	Default	2.4GHz (Auto)	WPA2-PSK	CCMP	Edit Delete

Fig. 6-3-a Wi-Fi List

By clicking the "Add/Edit" button under "Wi-Fi > Wi-Fi List," you can add a new SSID or edit an existing one.



Edit 1111

* SSID: 1111

Status: ●

* Band: ○ 2.4GHz ○ 5GHz

* Security: WPA2-PSK

Encryption: CCMP

* Password: •••••••••

* Network: Default

Channel: Auto

BandWidth: 20MHz

User Isolation: □

Hide SSID: □

Fig. 6-3-b Edit the SSID

Notes:

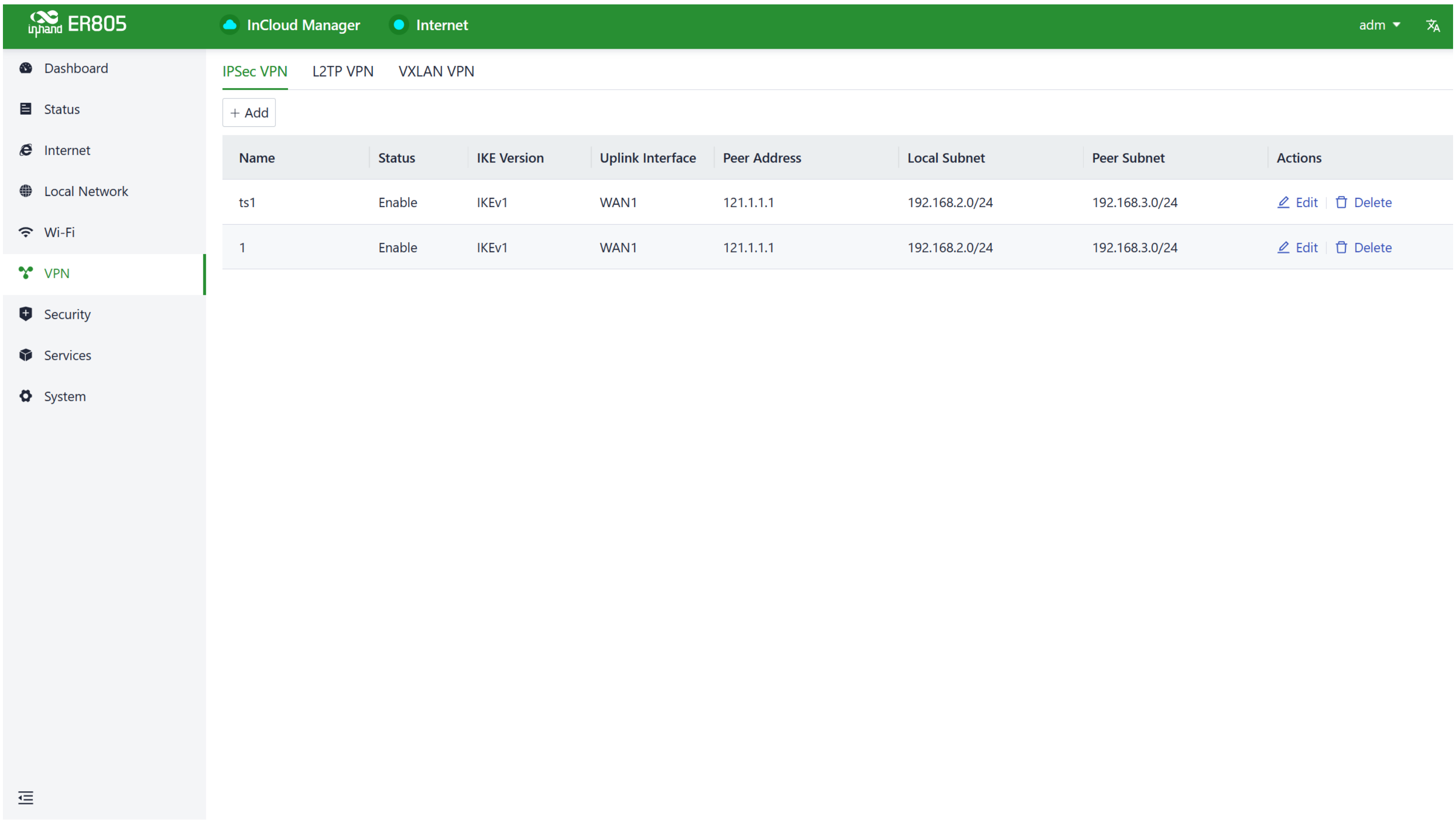
- The device comes with default 2.4GHz and 5GHz main SSIDs. The frequency bands of these main SSIDs cannot be modified and cannot be deleted.
- Once an SSID is added, its frequency band cannot be changed, and it will automatically use the same channel as its corresponding main SSID.
- If a user creates a Wi-Fi (STA) interface in the "Internet" menu with the same frequency band as an existing SSID, that SSID cannot be enabled until the Wi-Fi (STA) interface is deleted.

6.4 VPN

A Virtual Private Network (VPN) is an encryption technology used to establish a secure, private network connection over the public internet. It enables users to securely access private network resources over the internet from anywhere. VPNs achieve this by encrypting communication data, ensuring the confidentiality and security of the communication and preventing unauthorized access. This technology is highly valuable for connecting to corporate networks, maintaining online privacy, and accessing restricted content. VPNs have a wide range of applications, including in the corporate, personal, and mobile device sectors, making them a crucial tool for safeguarding privacy and data security.

6.4.1 IPSec VPN

IPsec (Internet Protocol Security) VPN is a protocol suite designed to enhance network communication security by encrypting and authenticating data transmission. It is widely used for establishing secure remote access, site-to-site connections, and Virtual Private Networks (VPNs). IPsec VPN ensures data protection and security through encryption and authentication methods.
Click the "Add" button under "VPN > IPSec VPN" to add a new IPSec VPN.



Name	Status	IKE Version	Uplink Interface	Peer Address	Local Subnet	Peer Subnet	Actions
ts1	Enable	IKEv1	WAN1	121.1.1.1	192.168.2.0/24	192.168.3.0/24	Edit Delete
1	Enable	IKEv1	WAN1	121.1.1.1	192.168.2.0/24	192.168.3.0/24	Edit Delete

Fig. 6-4-1 Add an IPSec VPN

Once configurations are completed at both ends, the tunnel can be established. Users can check the tunnel establishment status in the "Status > VPN" menu.

- **Name:** This is the user-assigned name for the IPSec VPN to identify it for local management purposes.
- **IKE Version:** You can set the version of the Internet Key Exchange (IKE) protocol to be used. It supports both IKEv1 and IKEv2.
- **Pre-Shared Key:** This is a secret shared key that must be configured the same on both devices for authentication during IKE negotiation.
- **Internet Interface:** Choose the upstream interface used to establish the IPSec VPN locally.
- **Tunnel Mode:** This sets the encapsulation mode for IPSec on IP packets. It supports both tunnel mode and transport mode.
- **Peer Address:** This is the address of the remote endpoint with which ER805 establishes the IPSec tunnel.

Notes:

This setup allows the device with the public IP address to act as the server, and the client devices connect to it using the server's public IP address. If you have more specific questions or need further assistance with IPSec VPN configuration, please let me know.

- **Local Subnet:** Specify the subnet addresses that need to communicate through the ER805 IPSec VPN tunnel.
- **Remote Subnet:** Specify the subnet address on the other end of the tunnel that needs to communicate through the IPSec VPN tunnel.
- **IKE Policy:** Supports configuring the IKE protocol.
- **Encryption Method:** Sets the encryption algorithm used by IKE.
  - **Options:** DES, 3DES, AES128, AES192, AES256 (default: AES128)
- **Authentication Method:** Set the authentication algorithm used by IKE.
  - **Options:** MD5, SHA1, SHA2-256, SHA2-384, SHA2-512 (default: SHA1)
- **DH Group:** Configure the DH exchange parameters used during the IKE phase key negotiation.
  - **Options:** 1, 2, 5, 14, 15, 16, 19, 20
- **Timeout:** Set the IKE SA (Security Association) lifetime, defaulting to 86400 seconds.

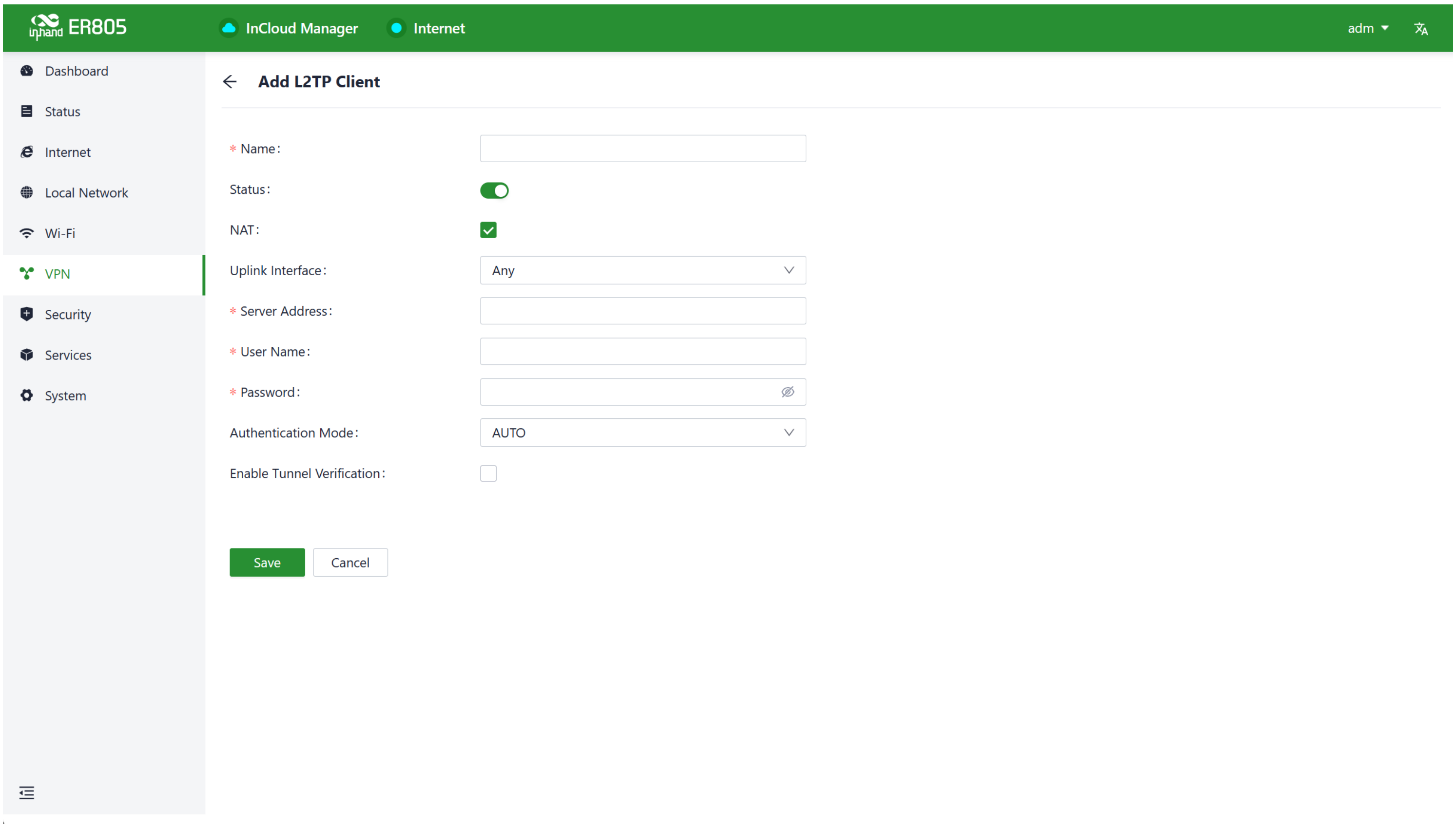
- **IPSec Policy:** This allows you to configure IPSec parameters.
- **Security Protocol:** Sets the security protocol used by the ESP protocol.
  - **Options:** DES, 3DES, AES128, AES192, AES256 (default: AES128)
- **Encryption Method:** Sets the encryption algorithm used by the ESP protocol.
  - **Options:** MD5, SHA1, SHA2-256, SHA2-384, SHA2-512 (default: SHA1)
- **PFS Group:** In IPSec, during the negotiation of a security policy, an additional key exchange is performed in Phase 2 to enhance communication security.
  - **Options:** 1, 2, 5, 14, 15, 16, 19, 20
- **Timeout:** Sets the IPSec SA aging time, default is 86400 seconds.

6.4.2 L2TP VPN

The Layer 2 Tunneling Protocol (L2TP) is a Layer 2 VPN protocol designed to establish secure point-to-point or site-to-site Virtual Private Network (VPN) connections. It is commonly used for remote access and branch office connectivity, creating secure communication channels for users or networks to protect the privacy and integrity of data transmission.

6.4.2.1 Work as a client

The ER805 can act as an L2TP client and establish a tunnel with a remote L2TP server. Click on the "L2TP VPN" menu, then navigate to "Client," and use the "Add" button to configure an L2TP client.



Add L2TP Client

* Name:

Status: ●

NAT: ☑

Uplink Interface: Any

* Server Address:

* User Name:

* Password:

Authentication Mode: AUTO

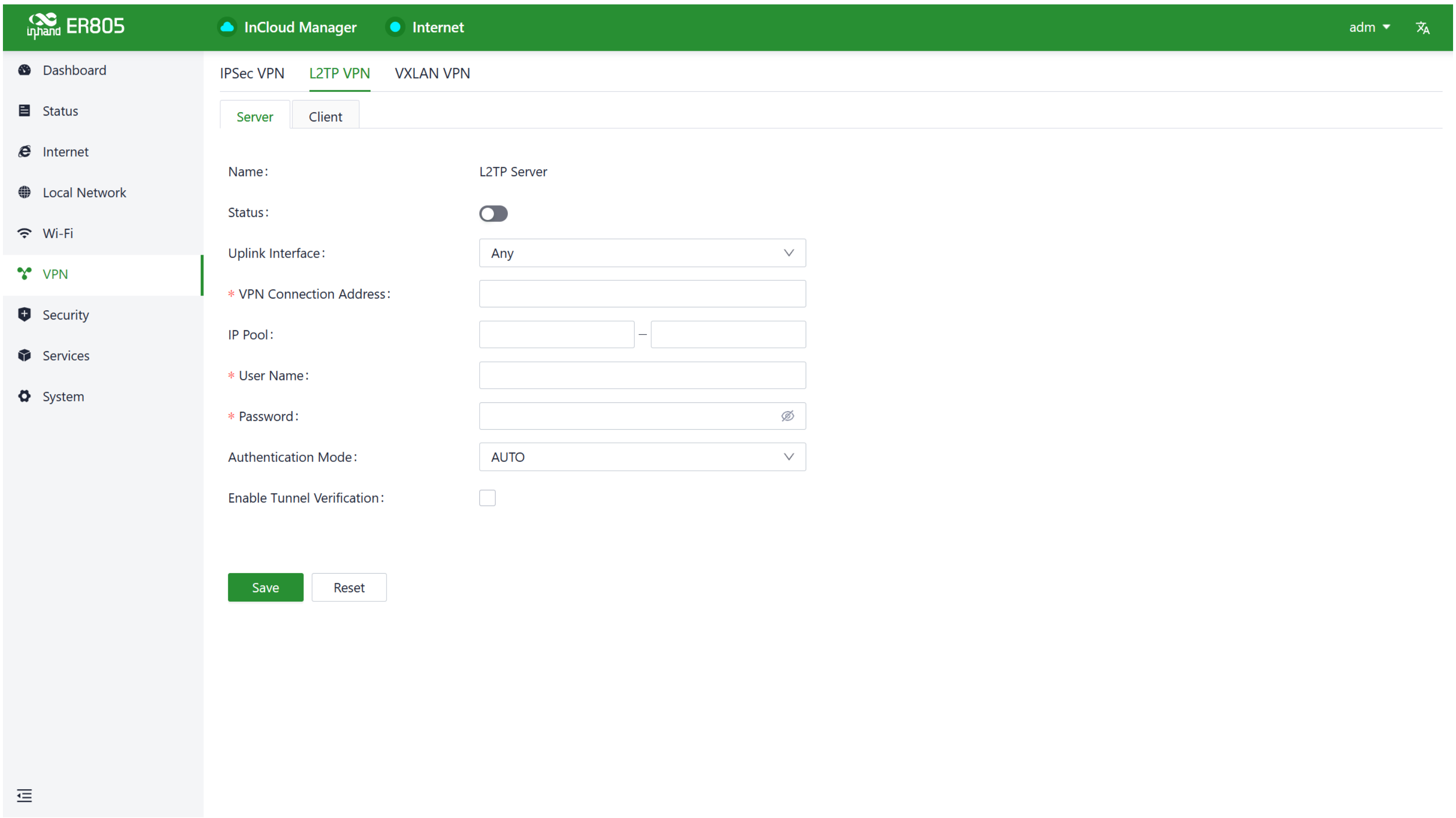
Enable Tunnel Verification: □

Fig. 6-4-2-1 Set the L2TP client parameters

- **Name:** The name of the L2TP client for local identification.
- **Status:** The switch to enable or disable the L2TP client tunnel.
- **NAT:** The switch for NAT functionality when forwarding with the L2TP client.
- **Upstream Interface:** The upstream interface used for communication between the L2TP client and the server.
- **Server Address:** The communication address of the remote L2TP server.
- **Username/Password:** Usernames and passwords that need to be configured the same on both ends during L2TP negotiation.
- **Authentication Mode:** Setting the L2TP authentication mode.
- **Enable Tunnel Authentication:** When enabled, both ends need to configure the same username and password for tunnel authentication.

6.4.2.2 Work as a Server

A typical L2TP server is usually deployed at the headquarters of an enterprise, serving as a remote access server for mobile office or branch offices. To configure the L2TP server settings, please click on "VPN > L2TP VPN > Server" to access the L2TP server editing page.



Name: L2TP Server

Status:

Uplink Interface: Any

* VPN Connection Address:

IP Pool: –

* User Name:

* Password:

Authentication Mode: AUTO

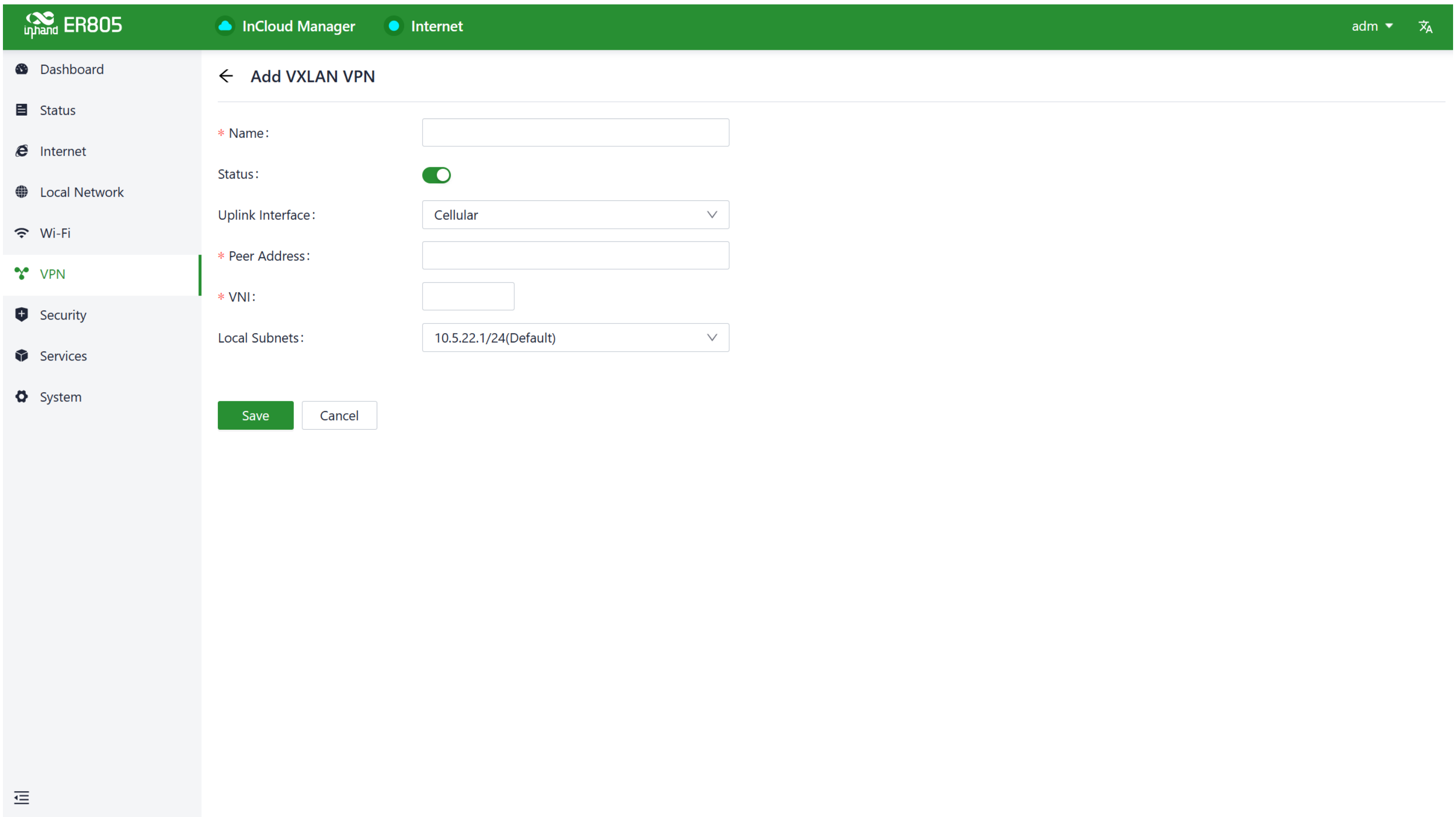
Enable Tunnel Verification: □

Fig. 6-4-2-2 Set the L2TP server parameters

- **Name:** The name of the L2TP server, not editable.
- **Status:** The on/off switch for the L2TP server function, default is off.
- **Upstream Interface:** The upstream interface used by the L2TP server.
- **VPN Communication Address:** The gateway address for L2TP clients, which can be assigned to devices within the IP address pool.
- **Address Pool:** The IP address pool is used for communication when L2TP clients connect.
- **Username/Password:** Usernames and passwords that need to be the same on both ends for L2TP negotiation.
- **Authentication Mode:** Setting the L2TP authentication mode.
- **Enable Tunnel Verification Function:** When enabled, the usernames/passwords for tunnel verification on both ends need to be the same.

6.4.3 VXLAN VPN

VXLAN（Virtual Extensible LAN）is essentially a tunnelling technology that establishes a logical tunnel over an IP network between the source and destination network devices. It achieves data transmission and forwarding by encapsulating user-side packets in a specific manner.
Click the "Add" button under "VPN > VXLAN VPN" to create a new VXLAN VPN.



Add VXLAN VPN

* Name:

Status: ●

Uplink Interface: Cellular

* Peer Address:

* VNI:

Local Subnets: 10.5.22.1/24(Default)

Fig. 6-4-3 Add a VXLAN VPN

- **Name:** Set the name for this VXLAN VPN network.
- **Upstream Interface:** The outbound interface used to establish a VXLAN tunnel with other devices.
- **Peer Address:** Configure the IP address of the peer device with which this device needs to establish a VXLAN VPN network.
- **VNI:** The VXLAN Network Identifier, where each VNI represents a different tenant or network segment.
- **Local Subnet:** Specify the address range assigned to local client devices when they connect.

Note:

- VXLAN cannot be used with other VPN functions and IP Passthrough functions at the same time.

6.5 Security

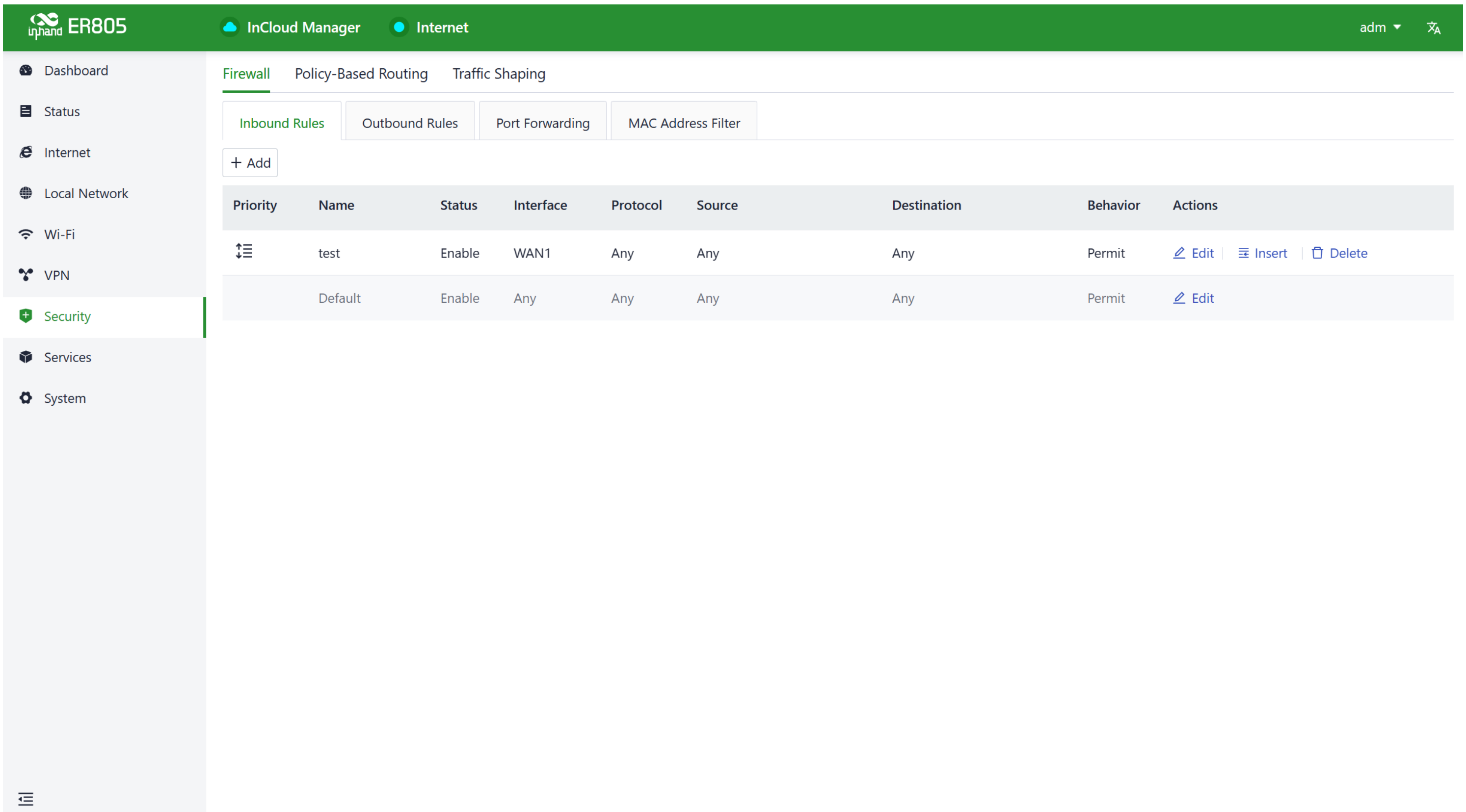
In the [Security] menu, users can configure advanced features related to firewalls, policy routing, and traffic shaping.

6.5.1 Firewall

The firewall currently includes functions such as inbound rules, outbound rules, port forwarding, MAC address filtering, and more.

6.5.1.1 Inbound Rules/Outbound Rules

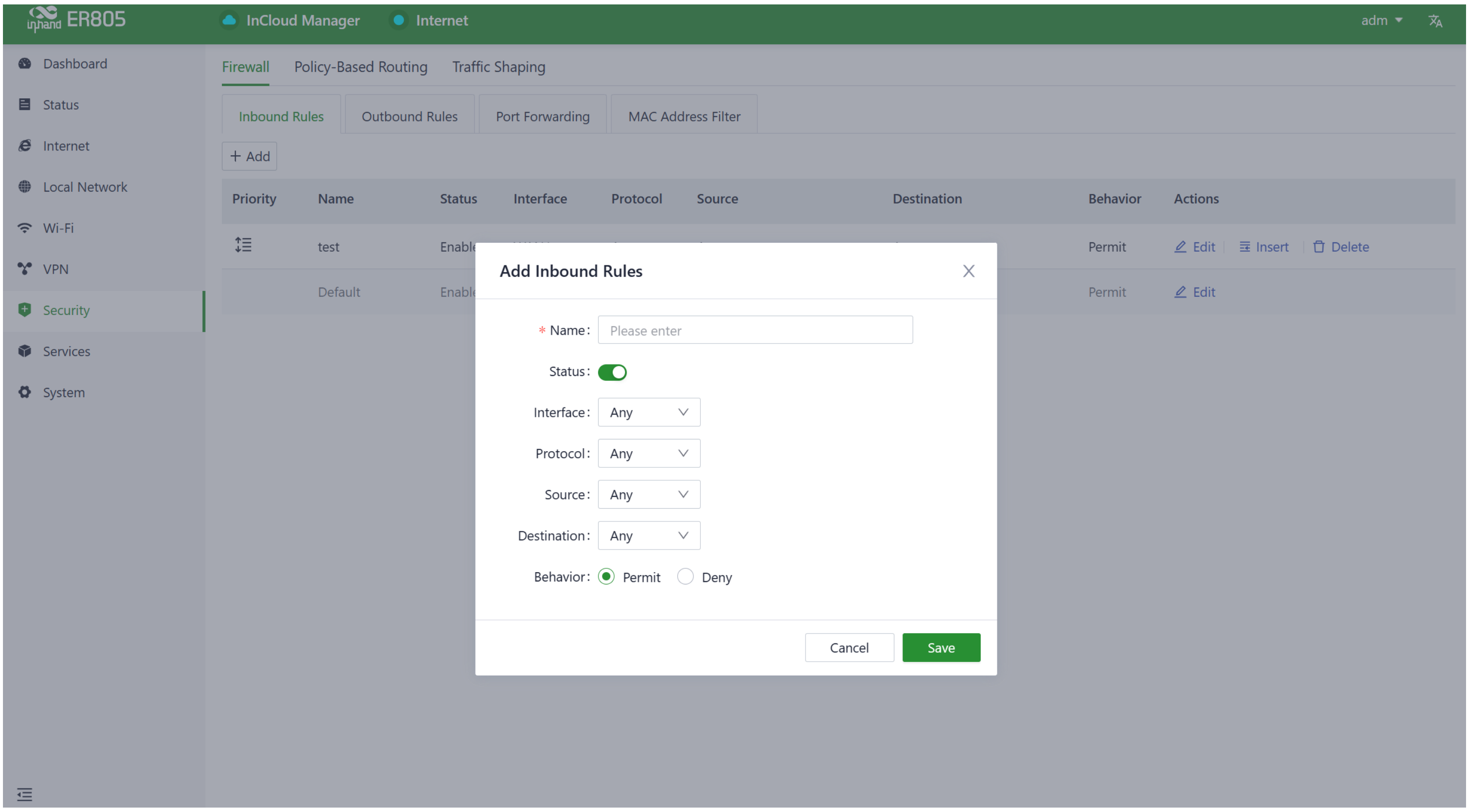
You can implement traffic in/out control based on interfaces through the "Security > Firewall > Outbound Rules/Inbound Rules" feature. For example, if a user is subjected to a significant amount of attacks from a specific source IP address, they can use inbound firewall rules to restrict traffic from that IP address.



Priority	Name	Status	Interface	Protocol	Source	Destination	Behavior	Actions
↕☰	test	Enable	WAN1	Any	Any	Any	Permit	Edit Insert Delete
	Default	Enable	Any	Any	Any	Any	Permit	Edit

Fig. 6-5-1-1-a Firewall Function Entry

Furthermore, IT personnel can utilize outbound firewall rules to restrict certain users' access to external networks. Inbound and outbound rules share the same configurable content, with the only distinction being the default rules.



Add Inbound Rules

* Name: Please enter

Status: ●

Interface: Any

Protocol: Any

Source: Any

Destination: Any

Behavior: ● Permit ○ Deny

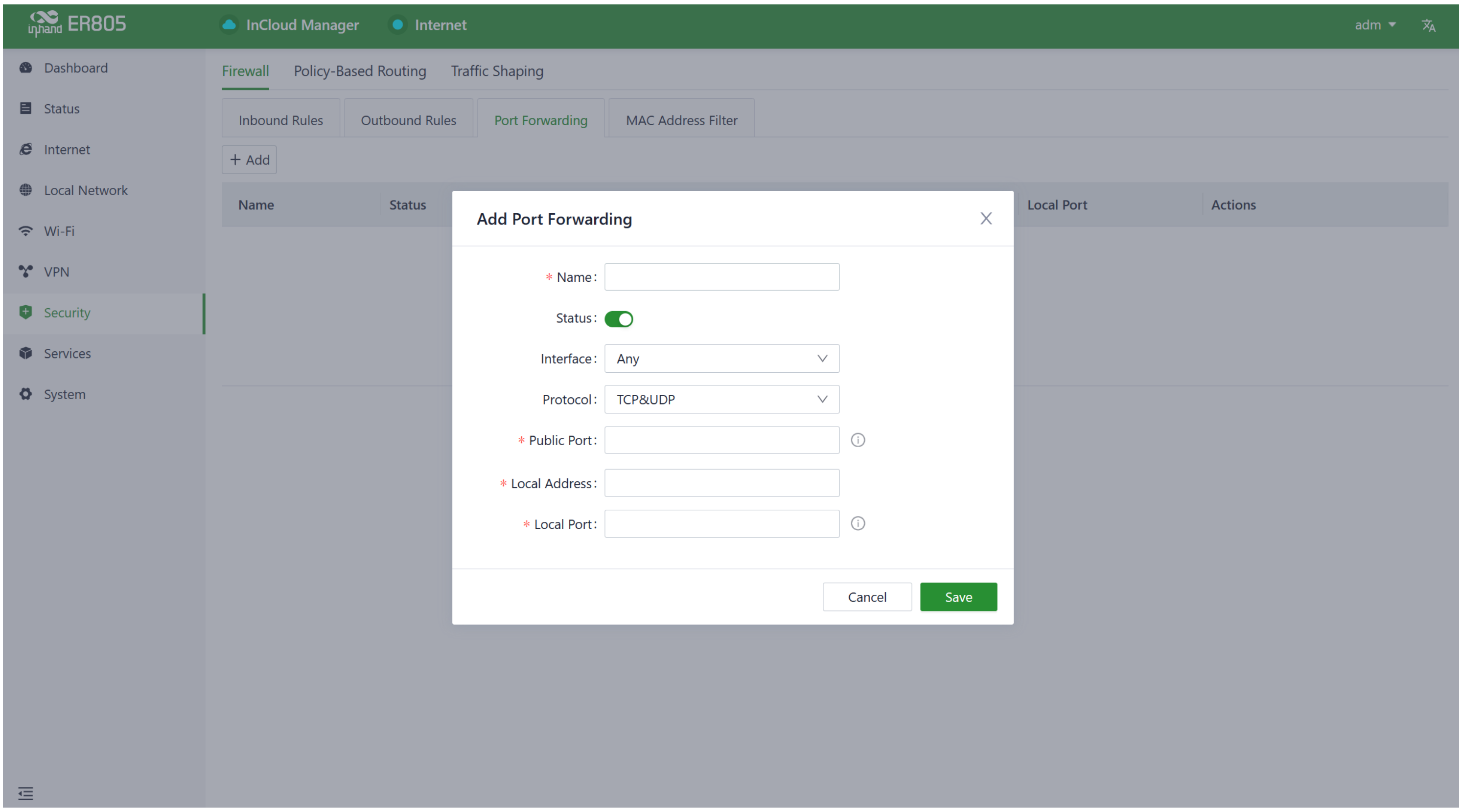
Fig. 6-5-1-1-b Add inbound/outbound rule

- **Name:** Set the name of the inbound/outbound rule for local identification.
- **Status:** Rule function switch.
- **Interface:** For outbound rules, it specifies the upstream interface where traffic leaves the router. For inbound rules, it specifies the upstream interface where traffic enters the router
- **Protocol:** Match traffic based on the protocol type, with options like Any, TCP, UDP, ICMP, or custom.
- **Source:** Match the source address for traffic, supporting custom, with the default as Any.
- **Destination:** Match the destination address for traffic, supporting custom, with the default as Any.
- **Action:** Action taken for matching traffic in inbound/outbound rules, supporting allow and deny.
- **Inbound Rules:** Traffic management rules for external network accessing the router, with the default as deny all.
- **Outbound Rules:** Traffic management rules for traffic going out through the router, with the default allowing all.
- Support for adjusting the priority of inbound and outbound rules.

6.5.1.2 Port Forwarding

Port forwarding, also known as port mapping or port redirection, is used to redirect network packets from one network port (or address) to another network port or address. Users can configure port forwarding rules under "Security > Firewall > Port Forwarding." When external traffic accesses a specific port on the router, the device forwards the data to the corresponding port of an internal client, enabling external access to services inside the router.

For example, when a user needs to access the service on port 1024 of the internal client at 192.168.2.10 from the external network, they can map this client's port to port 1024 under the WAN1 interface. External users only need to enter "https://WAN1 address:1024" in their browser to access the target device's data, where the WAN1 address is the IP address of the WAN1 interface.



Add Port Forwarding

* Name:

Status: ●

Interface: Any

Protocol: TCP&UDP

* Public Port:

* Local Address:

* Local Port:

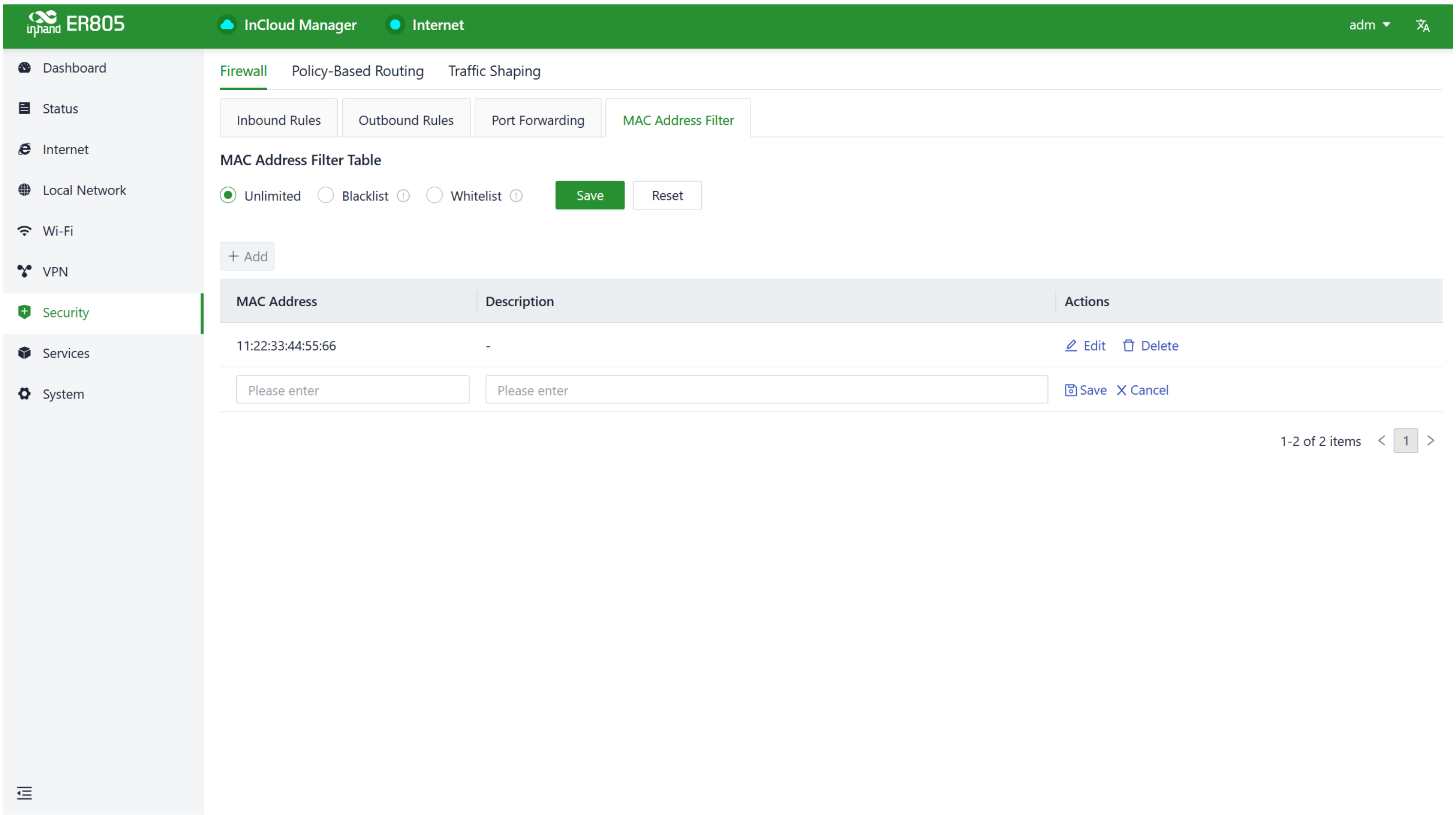
Fig. 6-5-1-2 Add a Port Forwarding Rule

- **Name:** The name of the port forwarding rule, used for local identification.
- **Status:** The on/off switch for the port forwarding rule.
- **Interface:** The upstream interface that provides mapping functionality for internal clients. The upstream interface needs public IP address support.
- **Protocol:** The protocol type of the traffic for port mapping, supports TCP, UDP, and TCP & UDP.
- **Public Port:** The port number on the upstream interface that provides mapping
- **Local Address:** The address of the target device located under the router that the external network needs to access.
- **Local Port:** The port of the target device that the external network needs to access. It needs to be consistent with the public port input range.

6.5.1.3 MAC Address Filter

MAC address filtering involves allowing or disallowing devices in a MAC address list to access the internet, which means controlling LAN devices' internet access requests through MAC address filtering on the router. Users can configure MAC address filtering rules in "Security > Firewall > MAC Address Filtering."

You can create multiple MAC addresses in the list, add address descriptions, and set it to allow only the MAC addresses to access the network (whitelist), or you can block MAC addresses in the list from accessing the network (blacklist).



MAC Address Filter Table

● Unlimited ○ Blacklist ○ Whitelist Save Reset

+ Add

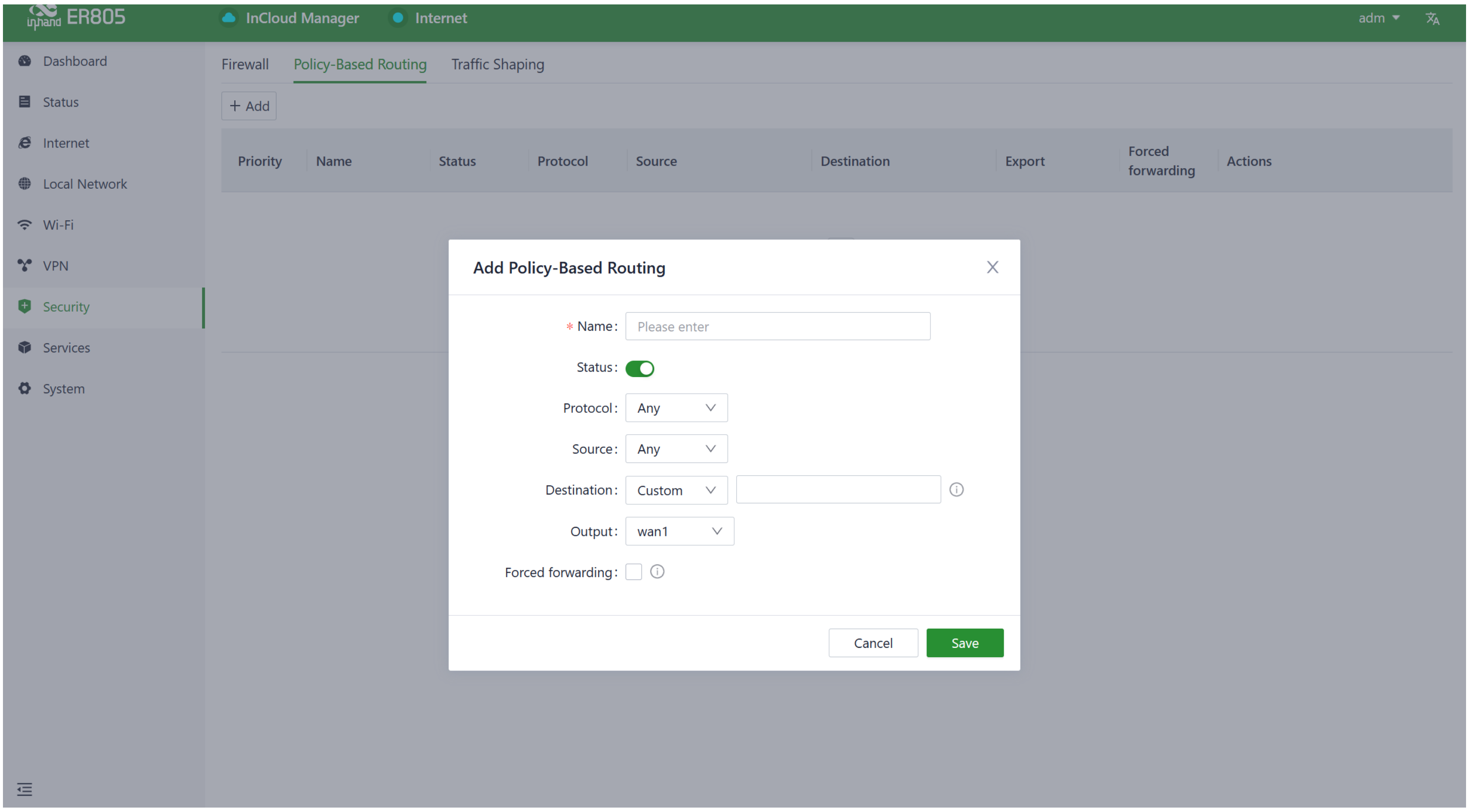
MAC Address	Description	Actions
11:22:33:44:55:66	-	Edit Delete
Please enter	Please enter	Save Cancel

1-2 of 2 items < 1 >

Fig. 6-5-1-3 Add a MAC address filter rule

6.5.2 Policy-Based Routing

Policy routing is a feature that allows users to create policies based on their specific needs, enabling them to route different data flows through different links. This improves the flexibility and control of routing decisions, enhances link utilization efficiency, and reduces enterprise costs. Click the "Add" button under "Security > Policy Routing" to create a new policy routing rule.



Add Policy-Based Routing

* Name:	Please enter
Status:	●
Protocol:	Any
Source:	Any
Destination:	Custom
Output:	wan1
Forced forwarding:	□

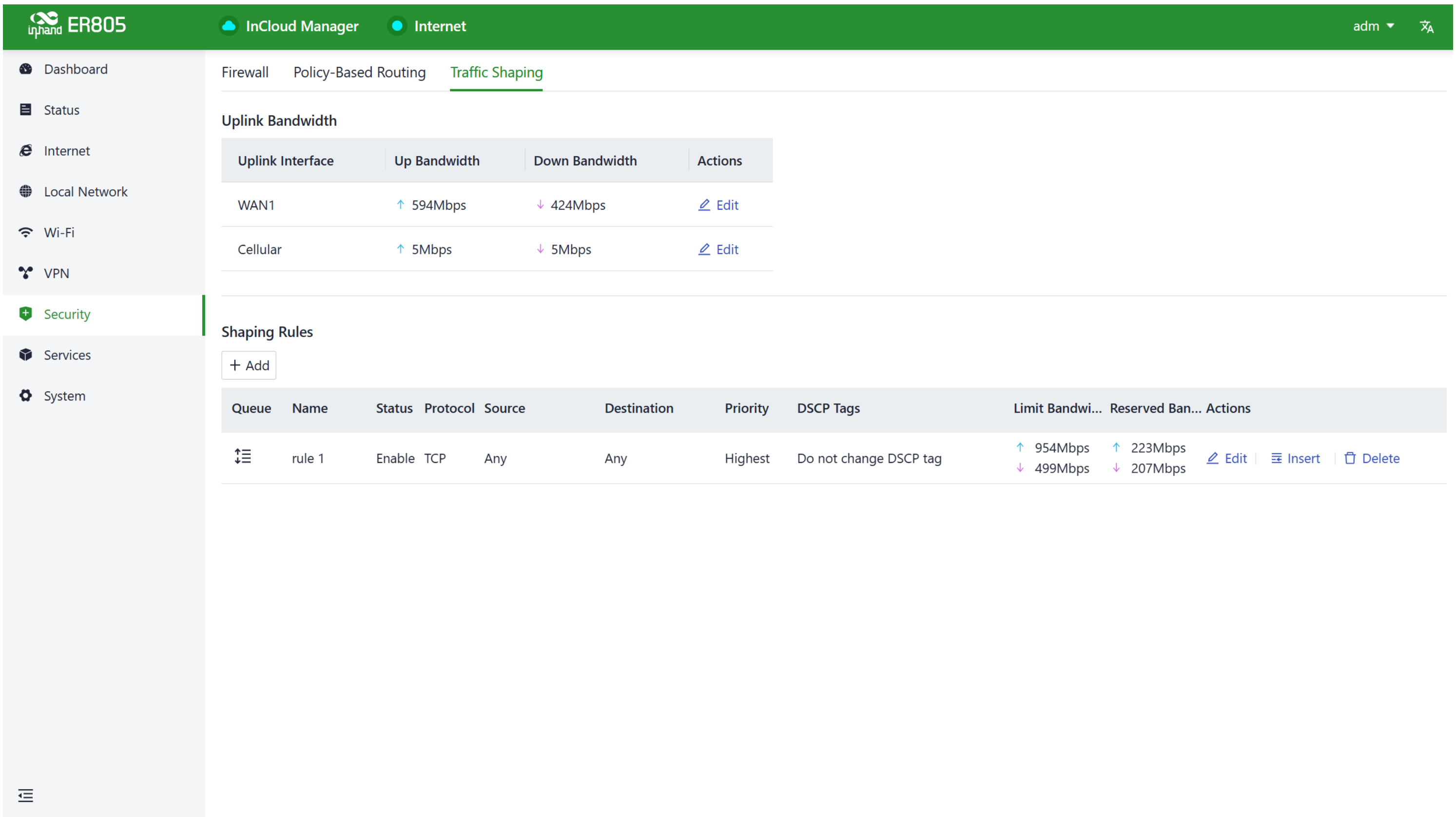
Fig. 6-5-2 Add a router policy

Cations:

- The source address and destination address in a policy routing rule cannot both be set as "Any."

6.5.3 Traffic Shaping

Create a traffic shaping policy to optimize your network based on each protocol, giving users control and prioritizing critical business traffic. This feature can also reduce the bandwidth allocated to entertainment traffic.You can configure traffic shaping rules in "Security > Traffic Shaping > Add/Edit."



Uplink Bandwidth

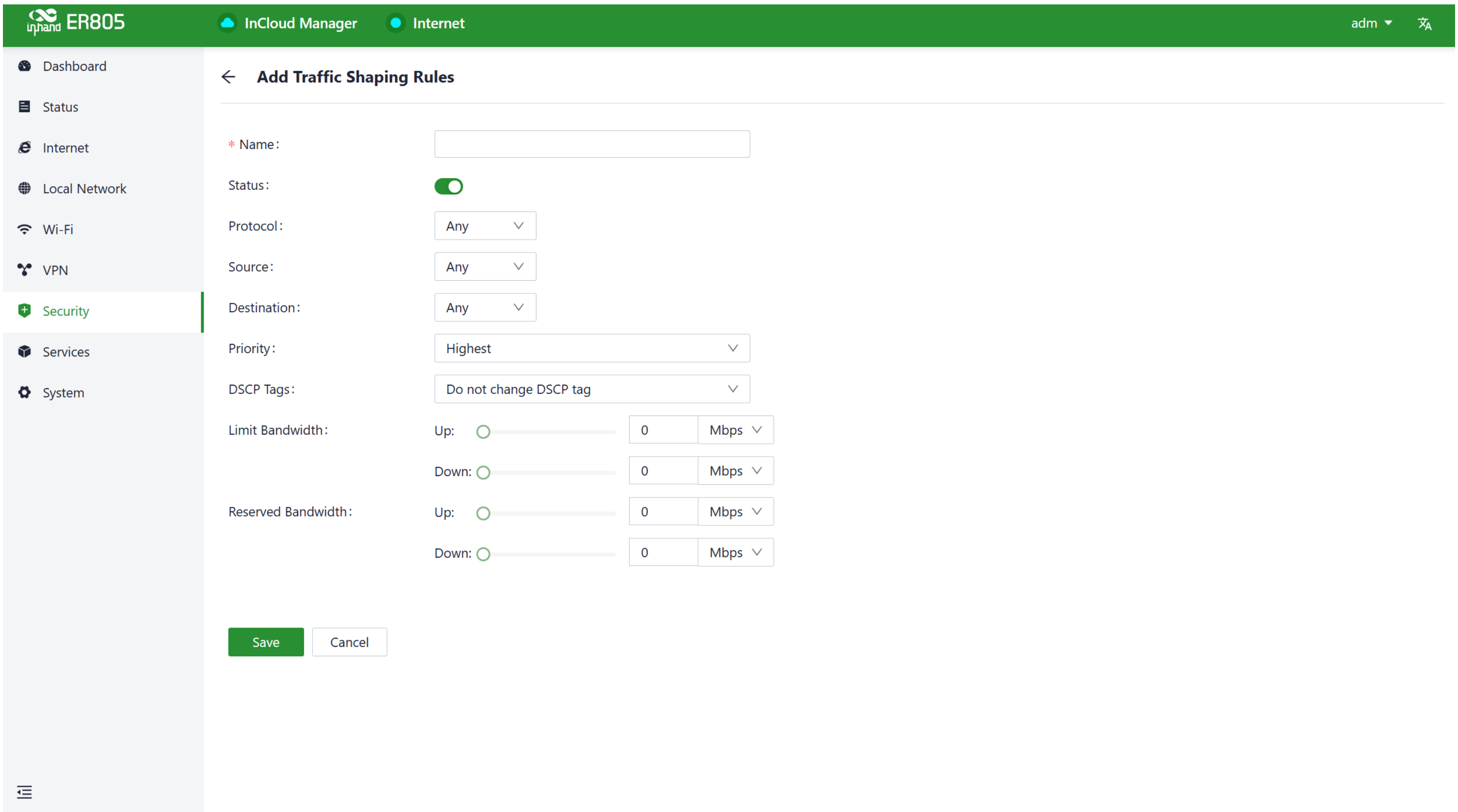
Uplink Interface	Up Bandwidth	Down Bandwidth	Actions
WAN1	↑ 594Mbps	↓ 424Mbps	Edit
Cellular	↑ 5Mbps	↓ 5Mbps	Edit

Shaping Rules

+ Add

Queue	Name	Status	Protocol	Source	Destination	Priority	DSCP Tags	Limit Bandwi...	Reserved Ban...	Actions
	rule 1	Enable	TCP	Any	Any	Highest	Do not change DSCP tag	↑ 954Mbps ↓ 499Mbps	↑ 223Mbps ↓ 207Mbps	Edit | Insert | Delete

Fig. 6-5-3-a Traffic Shaping interface



Add Traffic Shaping Rules

* Name:	
Status:	●
Protocol:	Any
Source:	Any
Destination:	Any
Priority:	Highest
DSCP Tags:	Do not change DSCP tag
Limit Bandwidth:	Up: 0 Mbps
	Down: 0 Mbps
Reserved Bandwidth:	Up: 0 Mbps
	Down: 0 Mbps

Fig. 6-5-3-b Add a traffic-shaping rule

Traffic shaping policies consist of a series of rules executed sequentially, similar to custom firewall rules. Each rule comprises two main components: the type of traffic to restrict or adjust and how to limit or adjust that traffic.

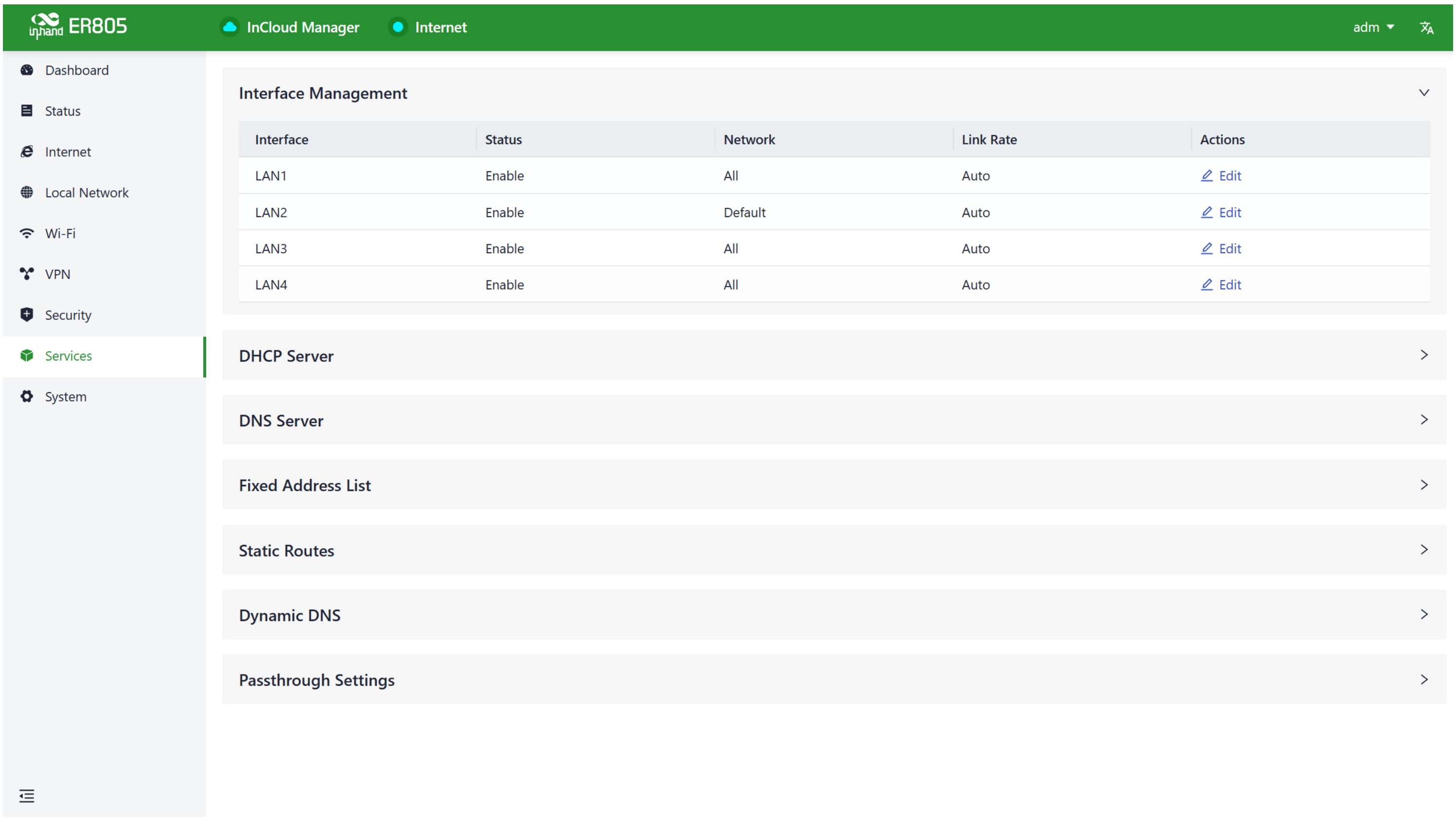
Notes:

- Traffic forwarding priority for unmatched rules is medium.
- When Limit Bandwidth is set to 0, the system will not limit the bandwidth.
- The value of Reserved Bandwidth should not be greater than the Limit Bandwidth.

6.6 Services

6.6.1 Interface Management

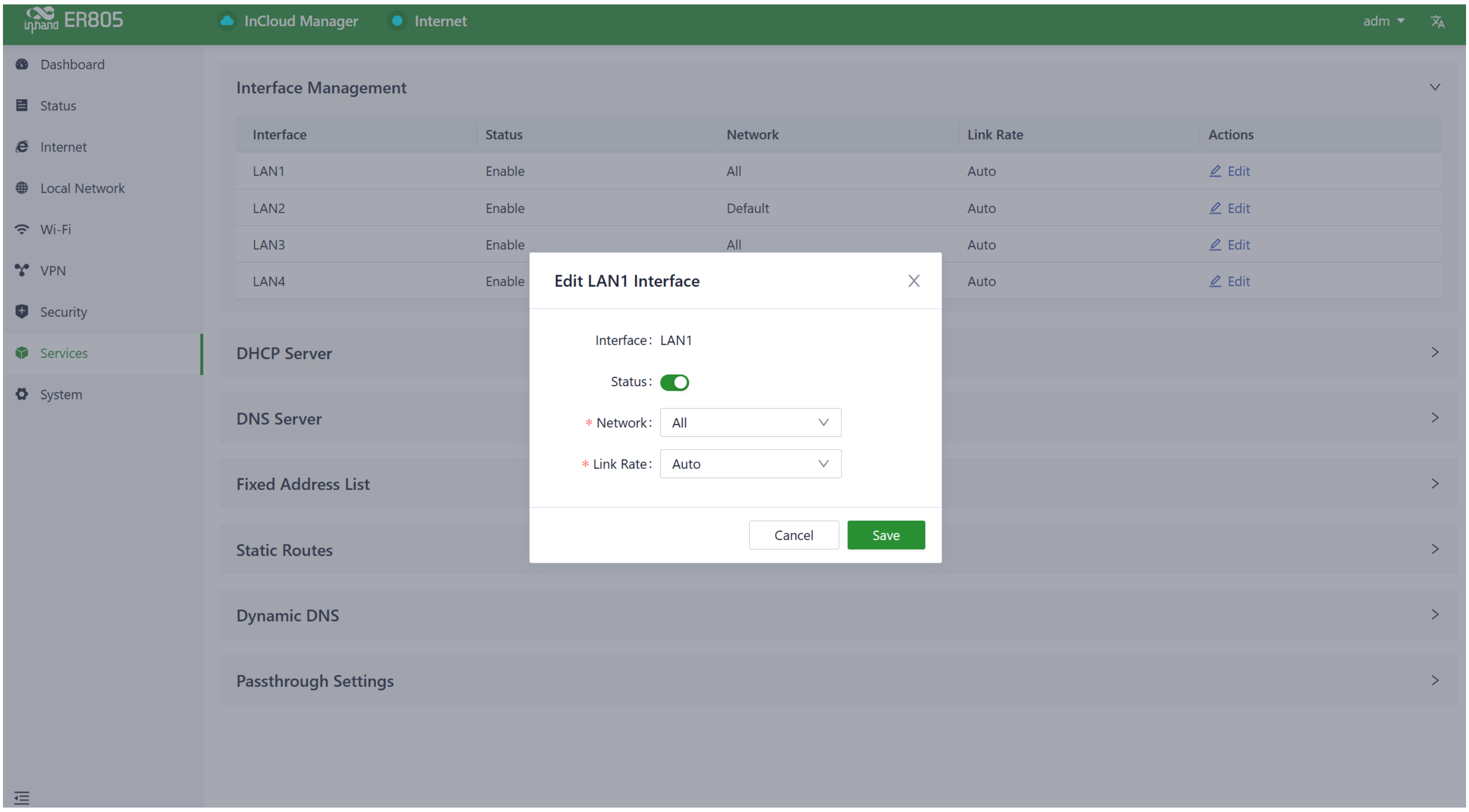
You can configure local networks allowed through a specific interface and set the interface's speed in the "Services > Interface Management" function.



Interface Management

Interface	Status	Network	Link Rate	Actions
LAN1	Enable	All	Auto	Edit
LAN2	Enable	Default	Auto	Edit
LAN3	Enable	All	Auto	Edit
LAN4	Enable	All	Auto	Edit

Fig. 6-6-1-a Interface Management



Interface	Status	Network	Link Rate	Actions
LAN1	Enable	All	Auto	Edit
LAN2	Enable	Default	Auto	Edit
LAN3	Enable	All	Auto	Edit
LAN4	Enable		Auto	Edit

Interface: LAN1

Status: ●

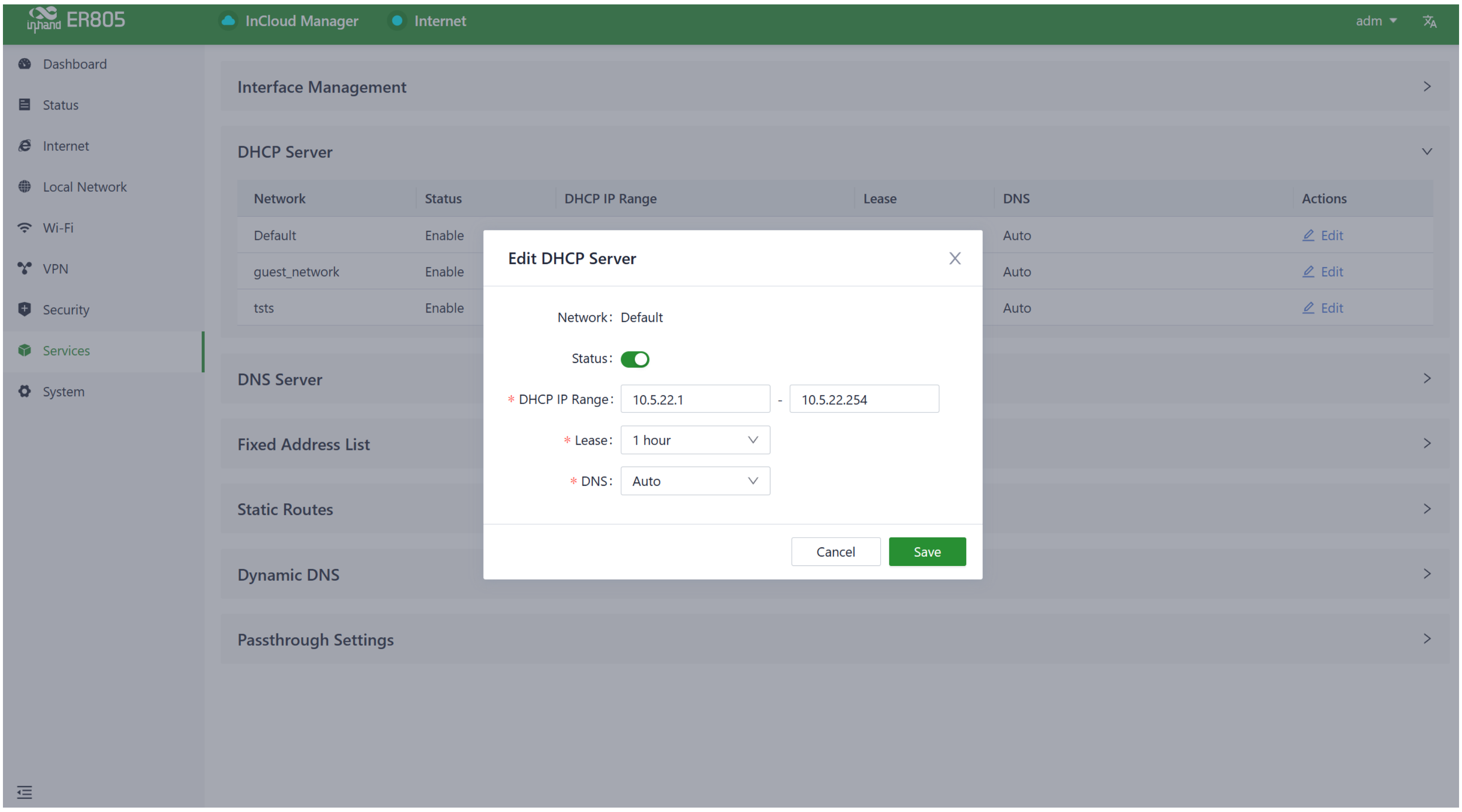
* Network: All

* Link Rate: Auto

Fig. 6-6-1-b Edit the interface

6.6.2 DHCP Server

The DHCP (Dynamic Host Configuration Protocol) service operates in a client/server communication mode, where clients request IP addresses from servers, and servers respond to these requests by assigning IP addresses dynamically to clients.You can configure the DHCP server’s IP address pool using the "Services > DHCP Server" feature.



Network	Status	DHCP IP Range	Lease	DNS	Actions
Default	Enable			Auto	Edit
guest_network	Enable			Auto	Edit
tsts	Enable			Auto	Edit

Edit DHCP Server

Network: Default

Status: ●

* DHCP IP Range: 10.5.22.1 - 10.5.22.254

* Lease: 1 hour

* DNS: Auto

Cancel Save

Fig. 6-6-2 DHCP Server

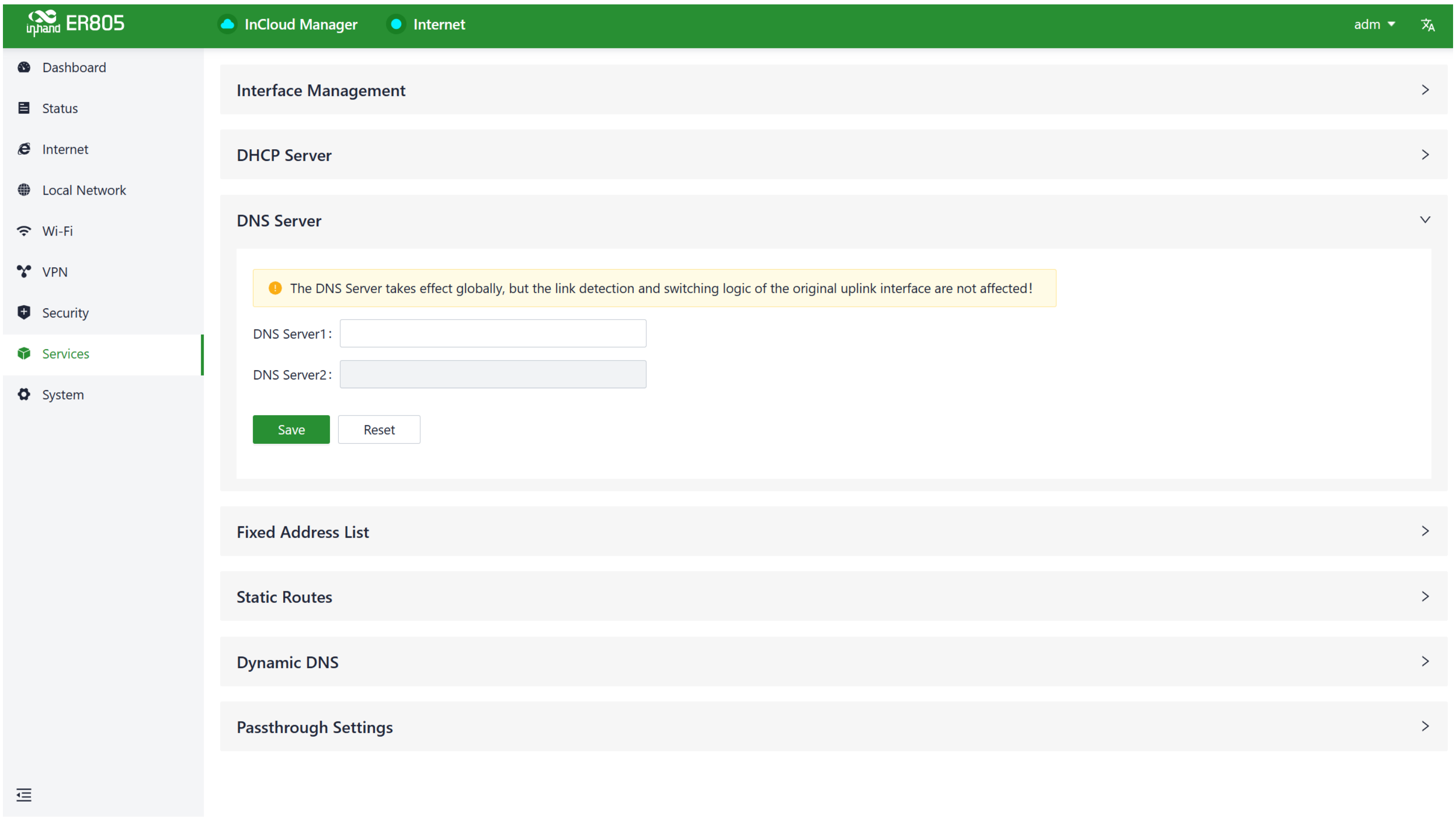
Notes:

- The device's DHCP service is generated based on the network information in the local network. If you remove a local subnet from the "Local Network List," the DHCP Server for that local subnet will also be deleted.
- Local network entries need to be set in “IP” mode for the DHCP server function to take effect. Networks in “VLAN Only” mode are not within the selectable range.

6.6.3 DNS Server

DNS (Domain Name System) servers are a crucial network component responsible for translating human-readable domain names (e.g., www.example.com) into computer-understandable IP addresses (e.g., 192.168.1.1). DNS servers act as the address book of the internet, helping computers and devices find the locations of other devices and ensuring that information can be correctly delivered across the network.

When users don't set DNS server addresses in "Services > DNS Server," the DNS addresses obtained from the device's upstream interface will be used for domain name resolution. When users configure DNS server addresses, the configured DNS addresses will be used for domain name resolution.



The DNS Server takes effect globally, but the link detection and switching logic of the original uplink interface are not affected!

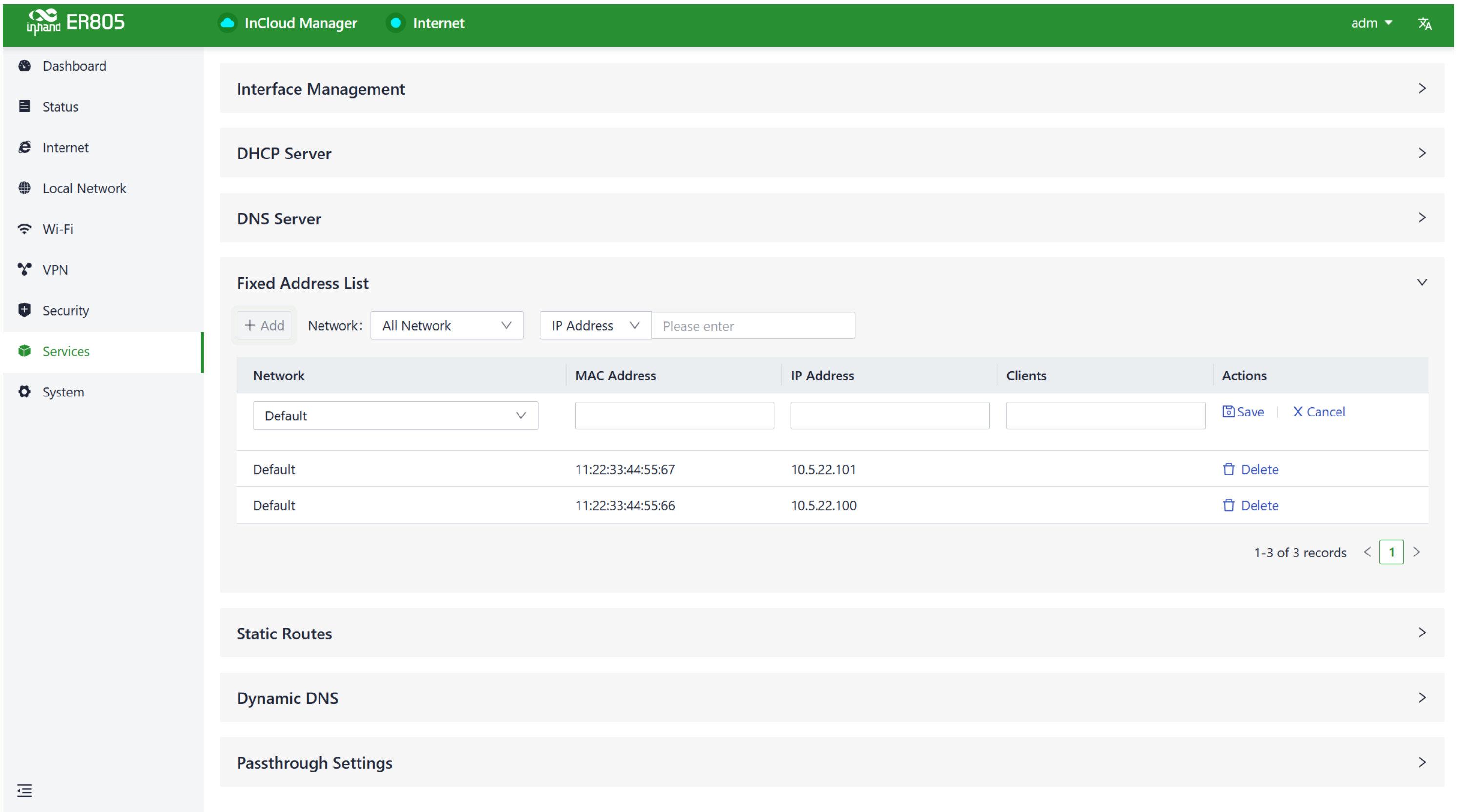
DNS Server1 :

DNS Server2 :

Fig. 6-6-3 Add a DNS server

6.6.4 Fixed Address List

You can use the "Services > Fixed Address List" function to allocate a fixed IP address to a device based on its MAC address. This means that the device will consistently receive the same IP address every time it connects to the ER805.



Network	MAC Address	IP Address	Clients	Actions
Default				Save | Cancel
Default	11:22:33:44:55:67	10.5.22.101		Delete
Default	11:22:33:44:55:66	10.5.22.100		Delete

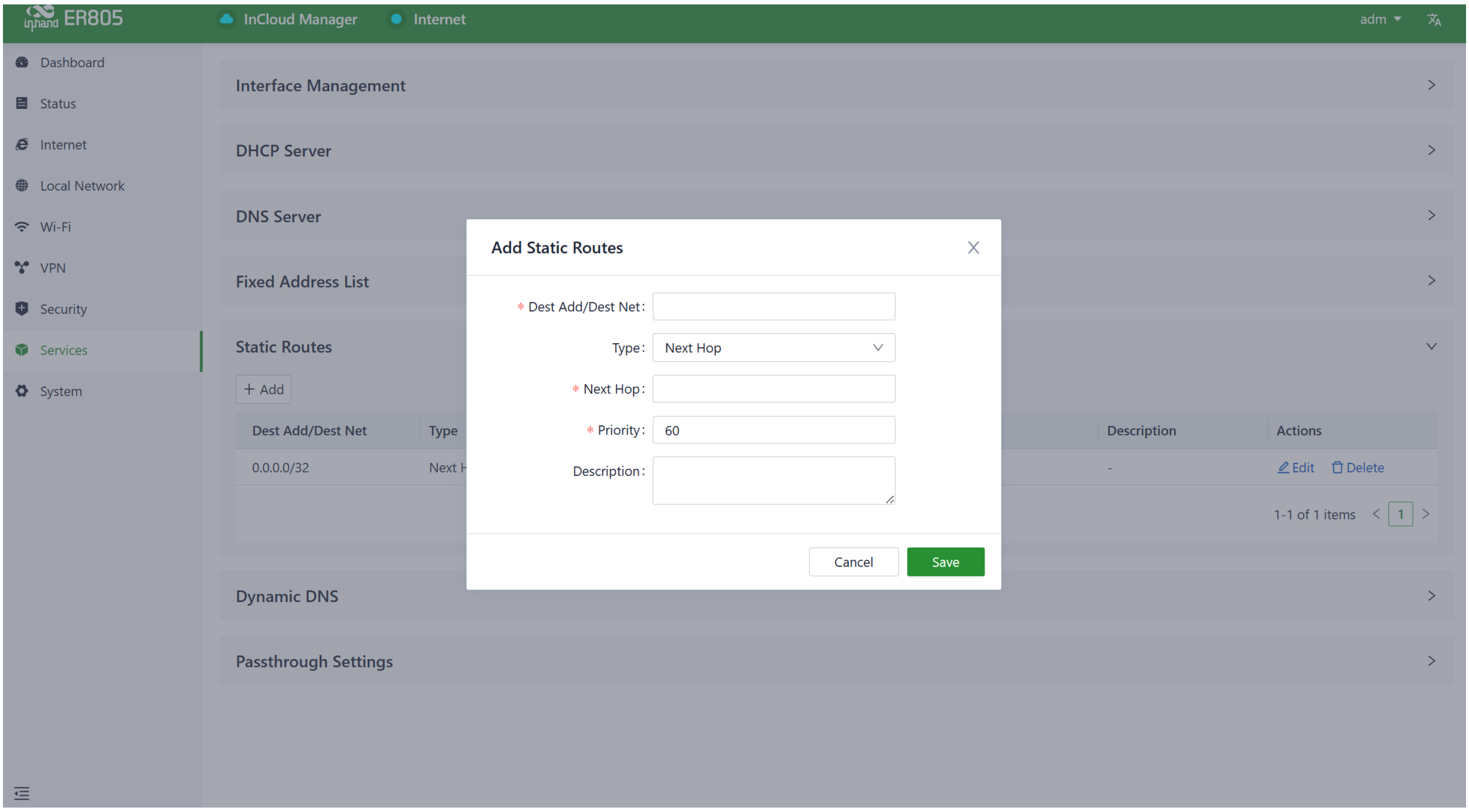
Fig. 6-6-4 Add a fixed IP address

Cautions:

- The available addresses for allocation must fall within the address range of the local network in IP mode, or else the configuration will not take effect
- When the local network is deleted, all fixed address allocation rules within the local network's address range will be removed.

6.6.5 Static Routes

You can configure static routing entries using the "Services > Static Routing" feature to enable data to be forwarded through specified paths and interfaces. The contents of the static routing table are manually created by users, and routing entries generated by other services, such as VPN functionality, will not be displayed in this table.



Add Static Routes

* Dest Add/Dest Net:

Type: Next Hop

* Next Hop:

* Priority: 60

Description:

Dest Add/Dest Net	Type	Description	Actions
0.0.0.0/32	Next H	-	Edit Delete

1-1 of 1 items

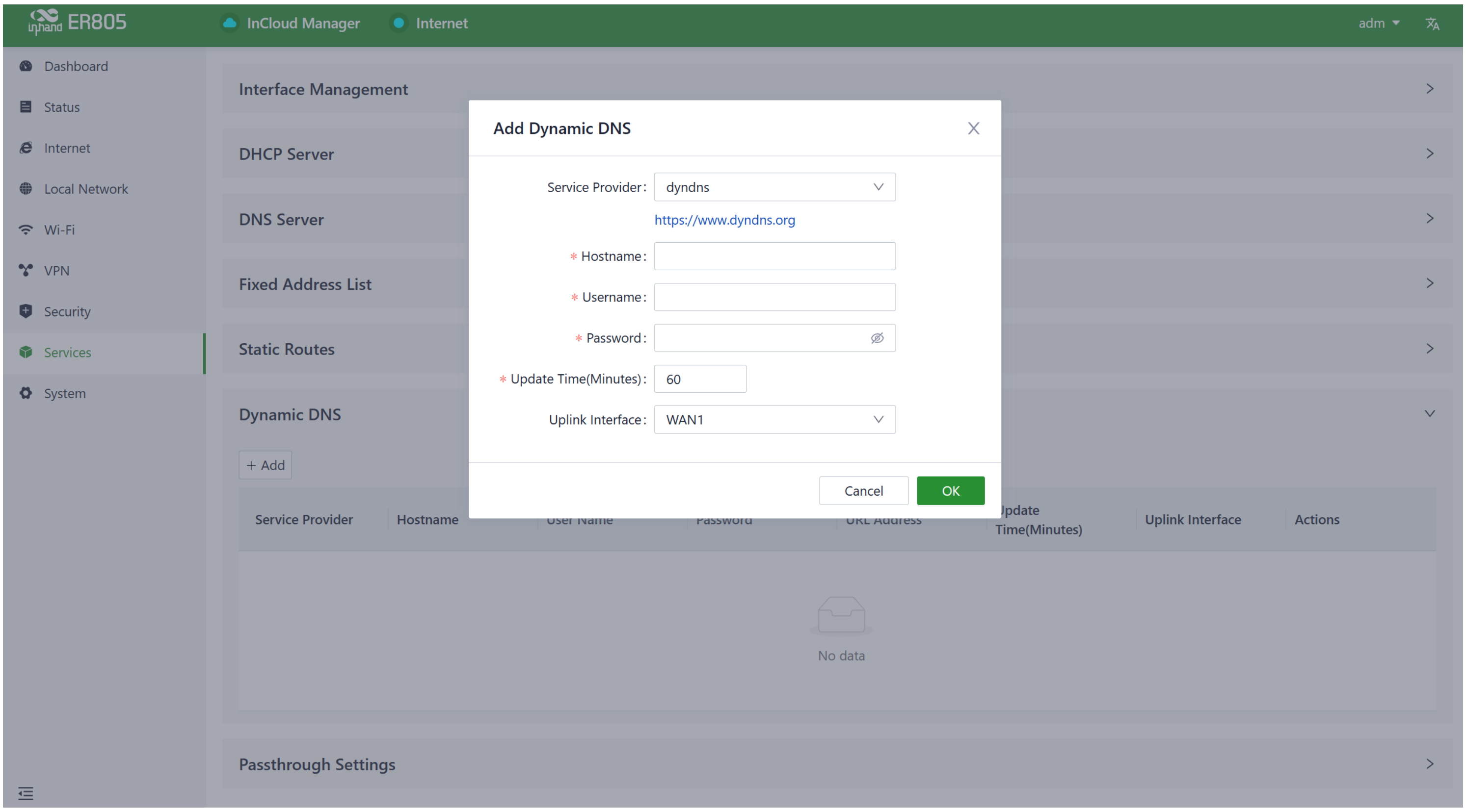
Fig. 6-6-5 Add a static route

Cautions:

- For static routes with the same destination address/network, the next-hop address, interface, or priority cannot be the same; otherwise, it will result in a non-functional route.
- When WAN2, Wi-Fi (STA), or L2TP Client VPN is deleted, the corresponding static routes using those interfaces will also be removed.

6.6.6 Dynamic DNS

Dynamic DNS (Dynamic Domain Name System) is used to automatically update the name server content in the domain system. According to internet domain rules, domain names are typically associated with fixed IP addresses. Dynamic DNS technology allows users with dynamic IP addresses to have a fixed name server. This enables external users to connect to the URL of users with dynamic IP addresses through regular updates.
You can manually configure the Dynamic DNS server address under the "Services > Dynamic DNS" feature.



Add Dynamic DNS

Service Provider: dyndns

https://www.dyndns.org

* Hostname:

* Username:

* Password:

* Update Time(Minutes): 60

Uplink Interface: WAN1

Service Provider	Hostname	User Name	Password	URL Address	Update Time(Minutes)	Uplink Interface	Actions

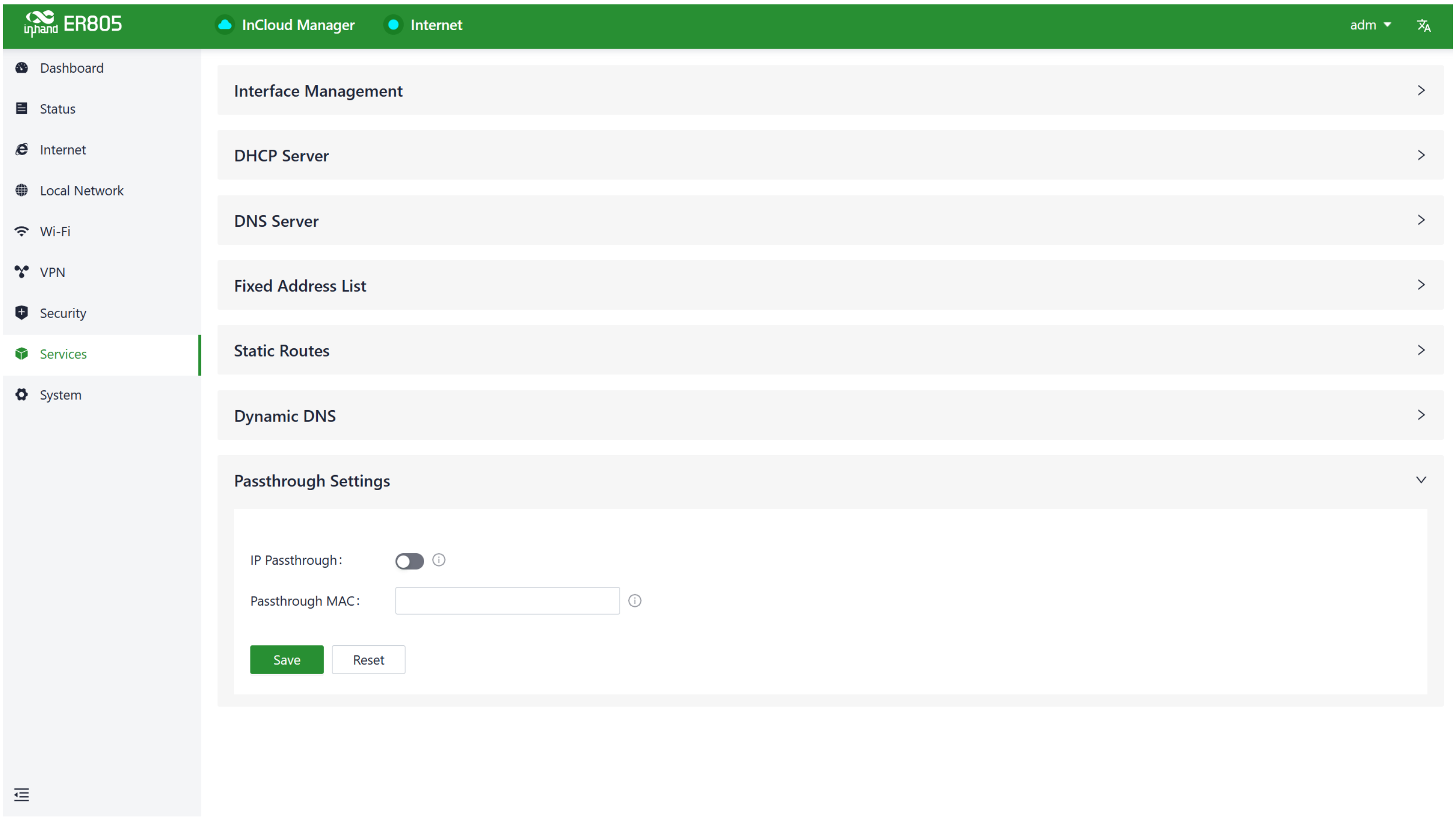
No data

Fig. 6-6-6 Add a Dynamic DNS service

- **Service Provider:** Provided by the Dynamic DNS service operator, you can choose from dyndns, 3322, oray, no-ip, or use a custom option (requires a URL).
- **Hostname:** Register for a hostname by clicking on the URL below the service provider.
- **Username:** Register for a username by clicking on the URL below the service provider.
- **Password:** The password set by the user during registration.

6.6.7 Passthrough Settings

You can enable the IP Passthrough feature through "Service > Passthrough Settings." Once enabled, client devices can obtain the upstream interface address of the ER805.



IP Passthrough:

Passthrough MAC:

Fig. 6-6-7 Enable the IP Passthrough

- **Passthrough MAC:** Only clients bound to this MAC can obtain the upstream interface address of the device.

Cautions:

- When the IP Passthrough mode is enabled, only one client can access the public network. : static routing, VPN, policy-based routing, SD-WAN Overlay, and cloud connectivity.
- When accessing client devices, you need to release inbound rules.
- You can still access the router via the default subnet's IP address.

6.7 System

In the "System" menu, users can configure settings related to cloud management, remote access control, clock settings, device options, configuration management, device alerts, tools, and log servers, among other functions.

6.7.1 adm Management

The initial username and password for the device are "adm" and "123456." To ensure the security of your device, it's recommended that you change the password. You can do this by clicking on "adm" in the top navigation bar and selecting "Change Password" from the dropdown menu.

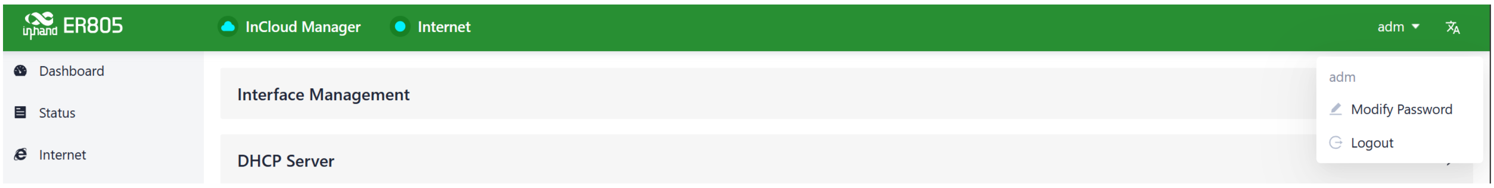
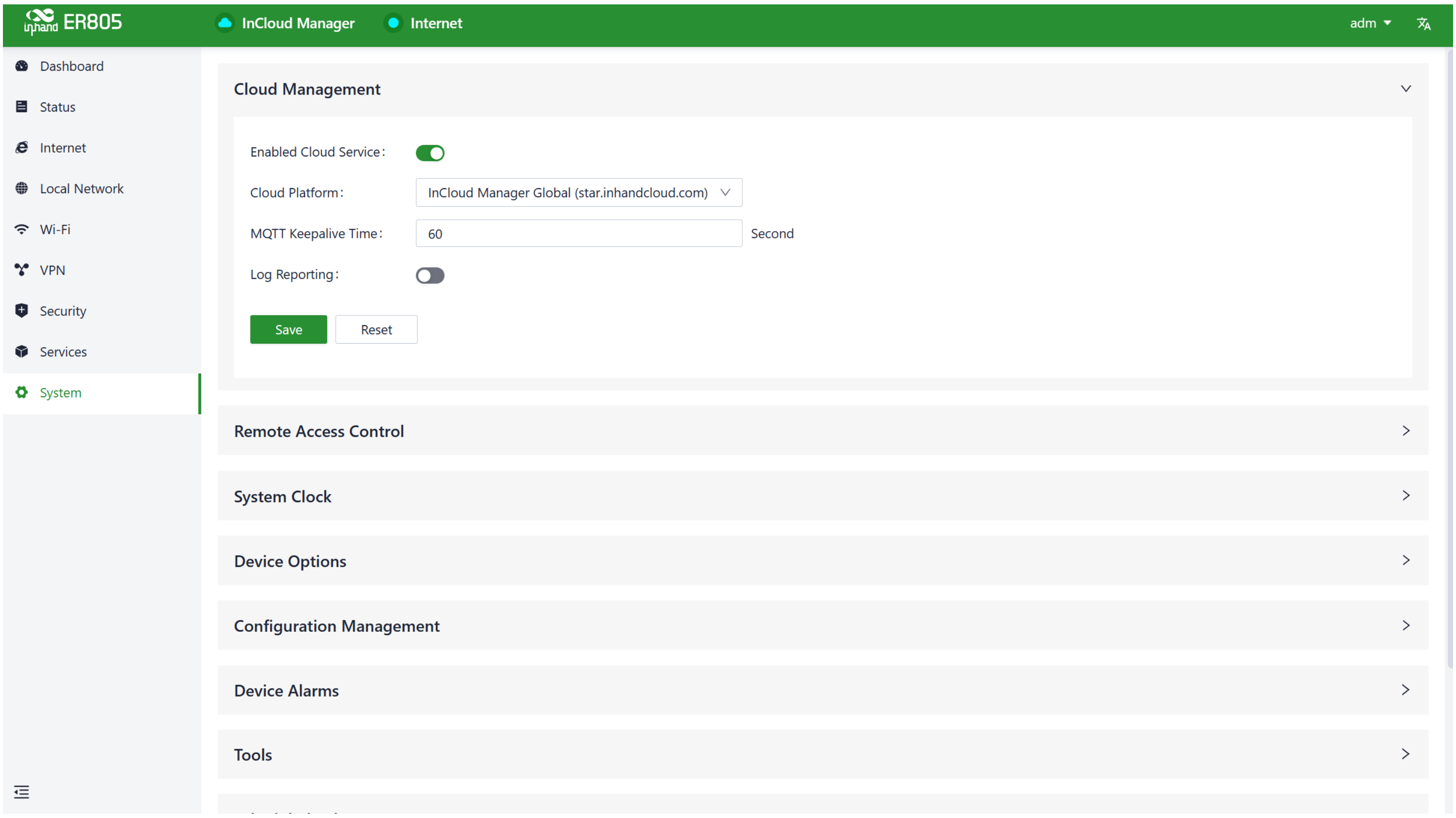


Fig. 6-7-1 Modify the Password

6.7.2 Cloud Management

The InCloud Service (star.inhandcloud.com) is a cloud platform developed by InHand Networks to address the challenges faced by enterprise networks, such as slow deployment, complex operations, and poor user experiences. This platform is designed with a focus on user needs and integrates features like zero-touch deployment, intelligent operations and maintenance, security protection, and excellent user experience capabilities. Once devices are connected to the cloud platform, users can perform remote management, batch configuration, traffic monitoring, and other operations through the platform, making network device management more convenient and efficient.

ER805 automatically connects to the InCloud Service after establishing an internet connection by default. If you do not wish to use the cloud management function, you can disable it manually in the "System > Cloud Management" function.



Cloud Management

Enabled Cloud Service: ●

Cloud Platform: InCloud Manager Global (star.inhandcloud.com)

MQTT Keepalive Time: 60 Second

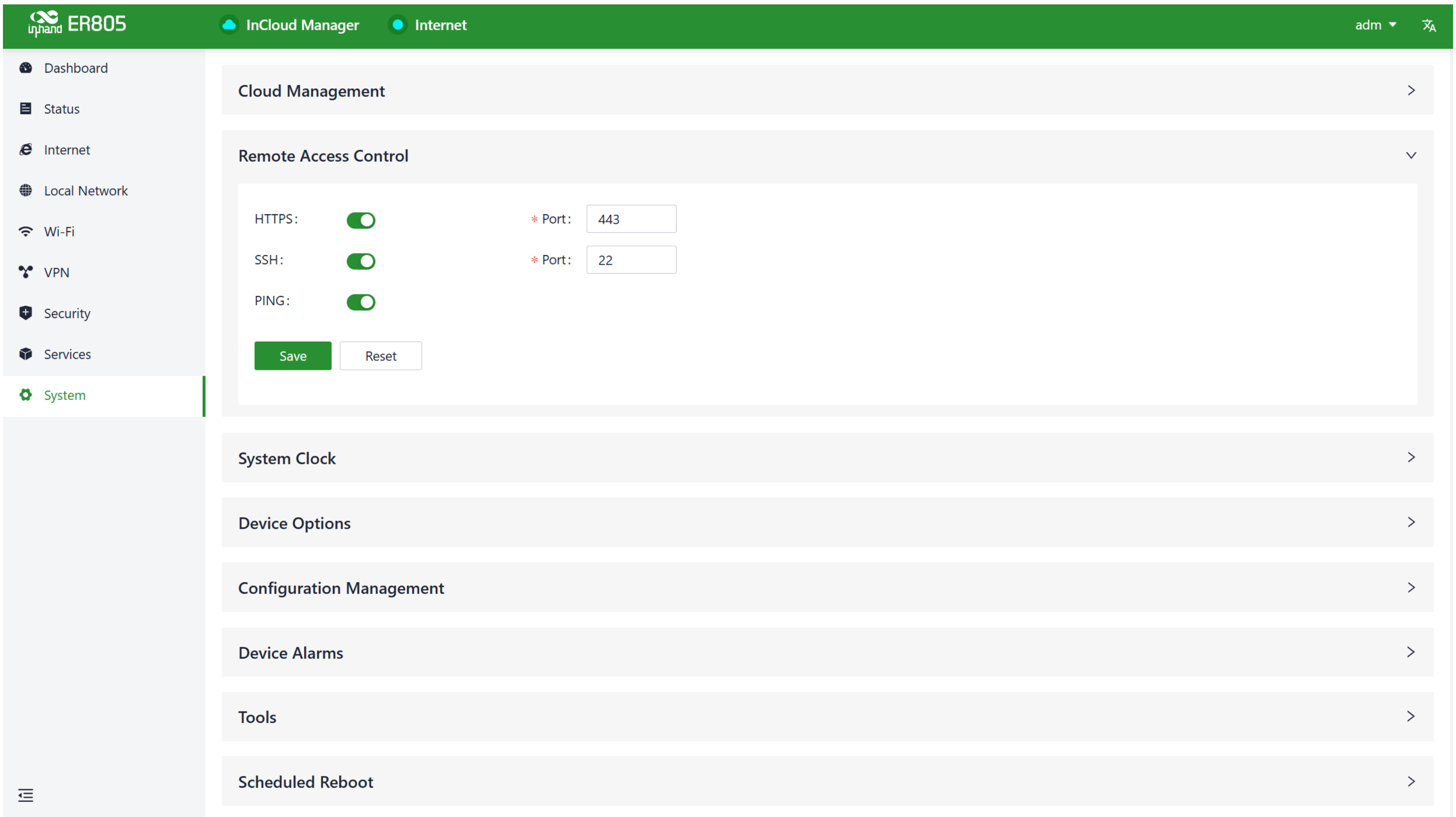
Log Reporting: ○

Save Reset

Fig. 6-7-2 Enable the InCloud Service

6.7.3 Remote Access Control

You can configure whether to allow external access to the router's web configuration interface from the Internet through the "System > Remote Access Control" function. You can also set the service port for this purpose.



HTTPS: ● * Port: 443

SSH: ● * Port: 22

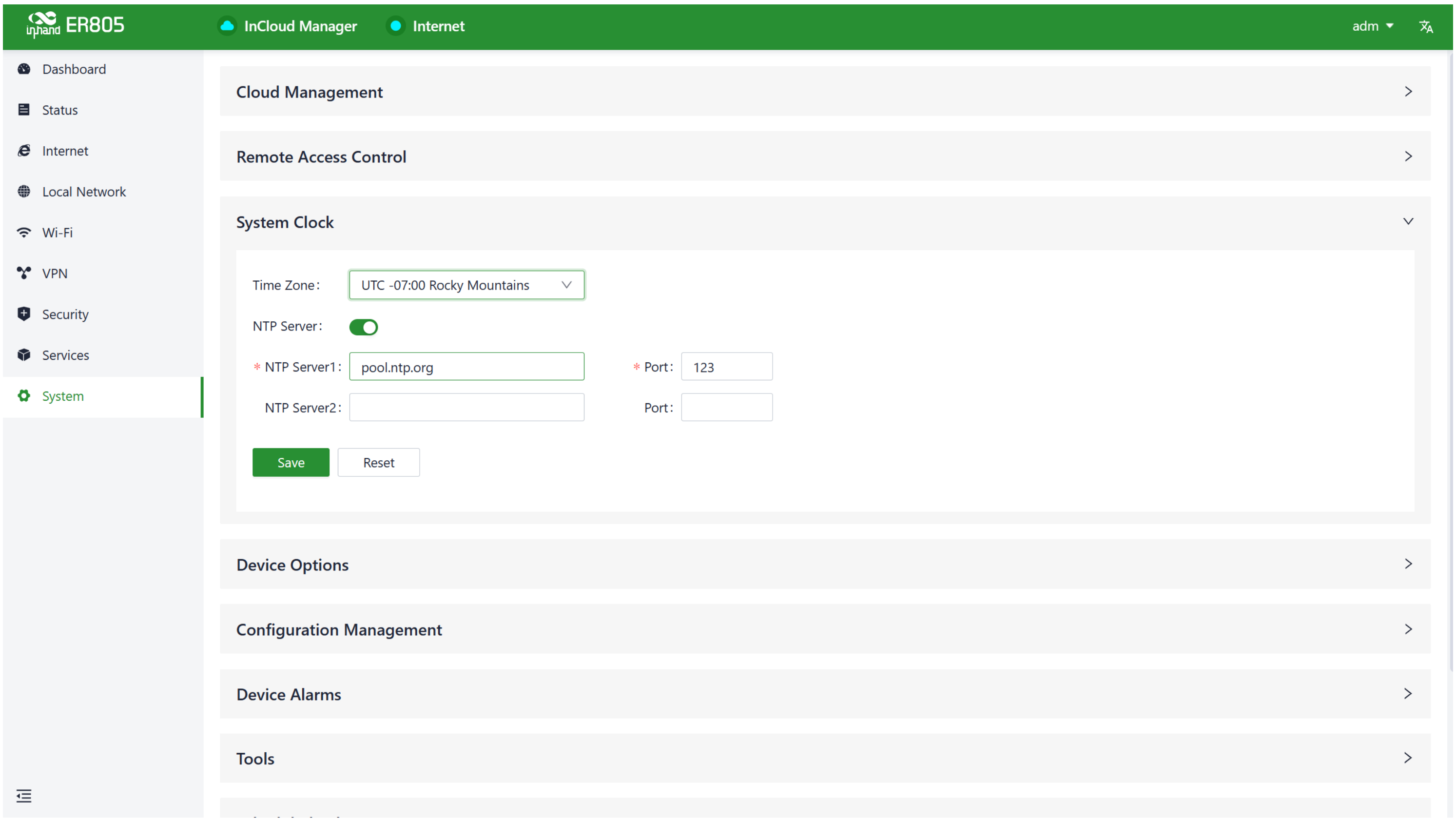
PING: ●

Fig. 6-7-3 Set the parameters of remote access

- **HTTPS:** When enabled, users can access the router's web interface remotely by entering the public IP address and port number of the upstream interface in a web browser.
- **SSH:** When enabled, users can remotely log in to the router's backend using remote tools (such as CRT) by providing the public IP address, port number, username, and password.
- **Ping:** When enabled, the upstream interface allows external networks to initiate Ping requests.

6.7.4 System Clock

In network functionality, the clock function refers to the capability used to coordinate and synchronize the time between network devices. Clock functionality within a network is crucial for data transmission, log recording, security, coordination, and troubleshooting. It ensures that various devices in the network are operating with synchronized times, which is essential for efficient and secure network operations.
You can use the "System > Clock" function to select their current time zone and configure NTP (Network Time Protocol) server addresses to synchronize the device's system time with an NTP server.



Time Zone: UTC -07:00 Rocky Mountains

NTP Server: ●

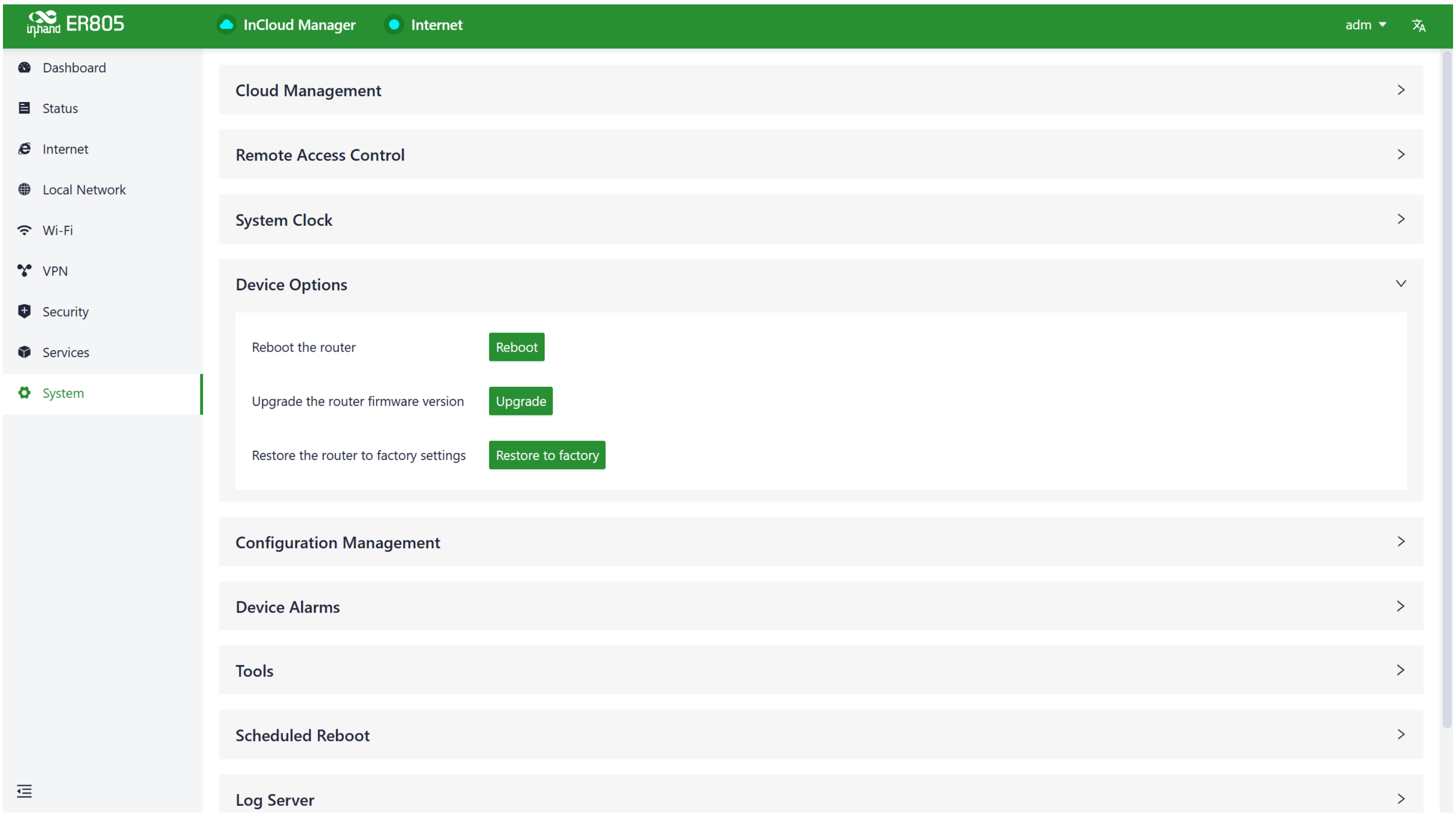
* NTP Server1: pool.ntp.org * Port: 123

NTP Server2: Port:

Fig. 6-7-4 Set the time zone and NTP server

6.7.5 Device Options

In the "System > Device Options" section, users can perform various device operations such as rebooting, upgrading firmware, and restoring factory settings.



Reboot the router Reboot

Upgrade the router firmware version Upgrade

Restore the router to factory settings Restore to factory

Fig. 6-7-5 Device Options

Cautions:

- When performing a local firmware upgrade, it is essential to ensure that the firmware is obtained from a legitimate source to avoid rendering the device inoperable due to incorrect firmware imports.
- When a device is connected to the cloud platform, the platform will synchronize the previous configuration to the device again due to cloud-based configuration synchronization. The device will only clear historical data during the factory reset.

6.7.6 Configuration Management

Configuring backups and backup recovery are critical tasks in network management and maintenance. They involve saving the configuration information of network devices so that it can be quickly restored or transferred when needed.

Users can export device configurations to local storage in the "System > Configuration Management" menu. This backup can be imported into the device in case of configuration loss or when you need to overwrite the existing configuration.

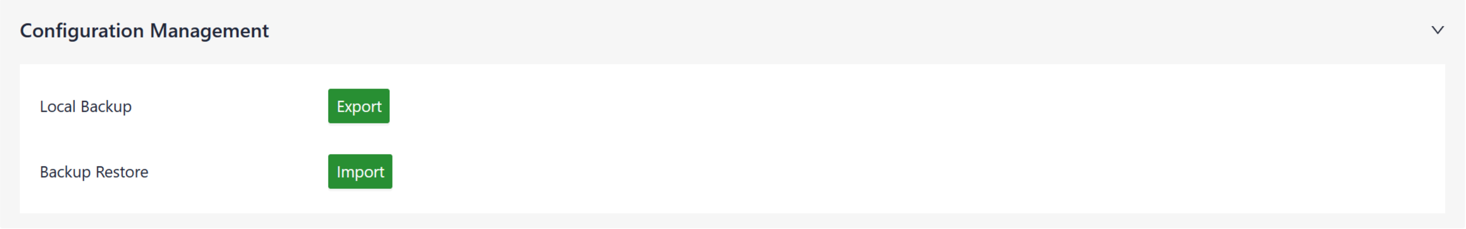
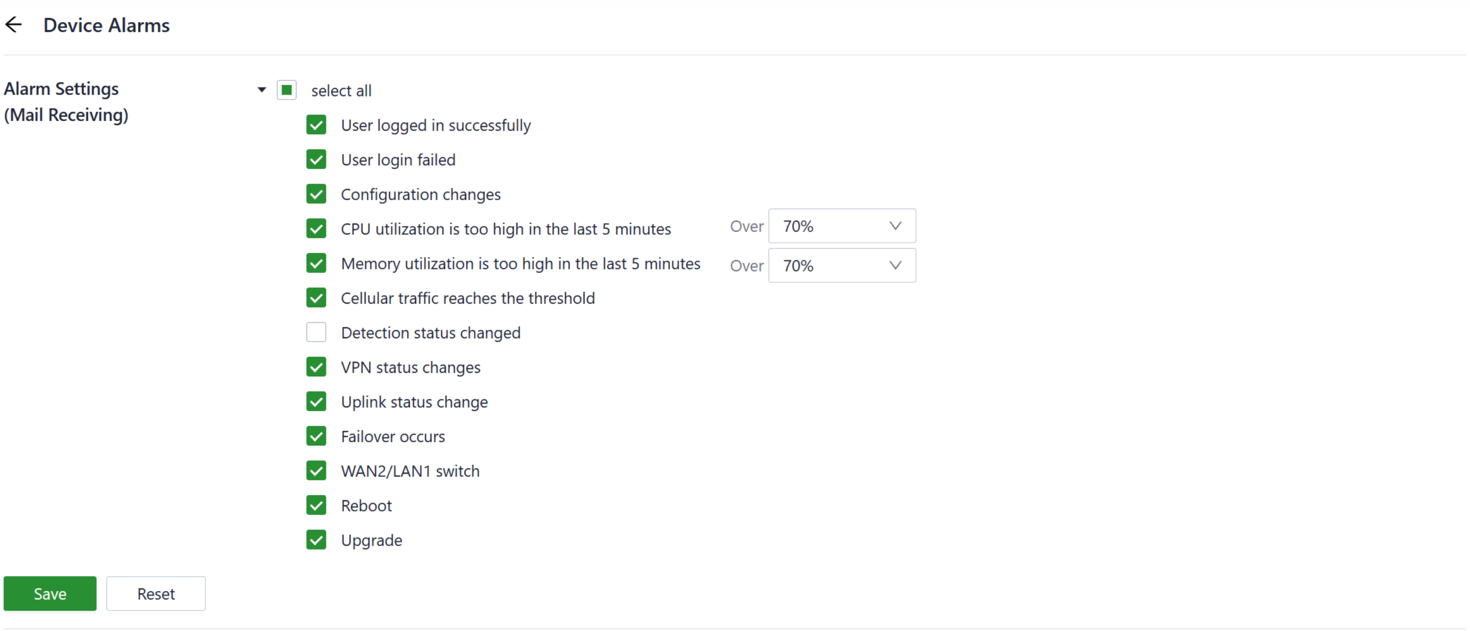


Fig. 6-7-6 Configuration Management interface

6.7.7 Device Alarms

You can choose to focus on specific events that may occur on the device by selecting the corresponding alarm events and configuring the email address for receiving alerts. When an alarm event occurs, the device will automatically send an email notification. It's important to note that even if a user doesn't select certain alarm options, related alarm events will still be recorded in the device's local logs.

You can configure alarm event types and email addresses for alarm notifications in the "System > Device Alarms" menu.

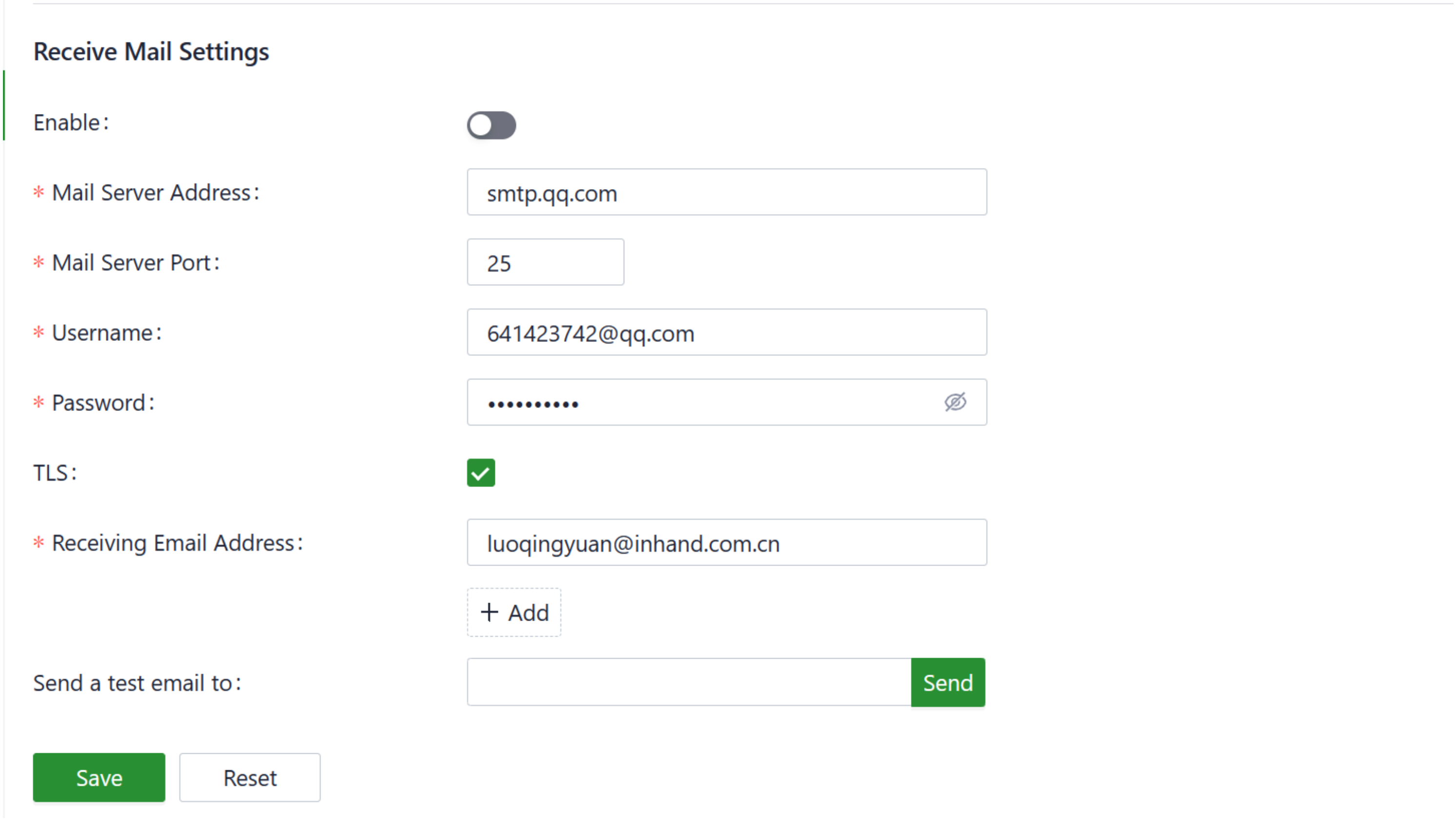

← Device Alarms

Alarm Settings (Mail Receiving)

▪ select all
- ☑ User logged in successfully
- ☑ User login failed
- ☑ Configuration changes
- ☑ CPU utilization is too high in the last 5 minutes Over 70%
- ☑ Memory utilization is too high in the last 5 minutes Over 70%
- ☑ Cellular traffic reaches the threshold
- □ Detection status changed
- ☑ VPN status changes
- ☑ Uplink status change
- ☑ Failover occurs
- ☑ WAN2/LAN1 switch
- ☑ Reboot
- ☑ Upgrade

Fig. 6-7-7-a Alarm event types

After configuring the outgoing email server address, port, username, and password, the device will use this email account to send alarm notifications. You can use the "Send Test Email" option to verify whether the outgoing email configuration is correct. This test email will help you ensure that the device can successfully send alarm notifications to the specified email address.


Receive Mail Settings

Enable: ○

* Mail Server Address: smtp.qq.com

* Mail Server Port: 25

* Username: 641423742@qq.com

* Password: ••••••••••

TLS: ☑

* Receiving Email Address: luoqingyuan@inhand.com.cn

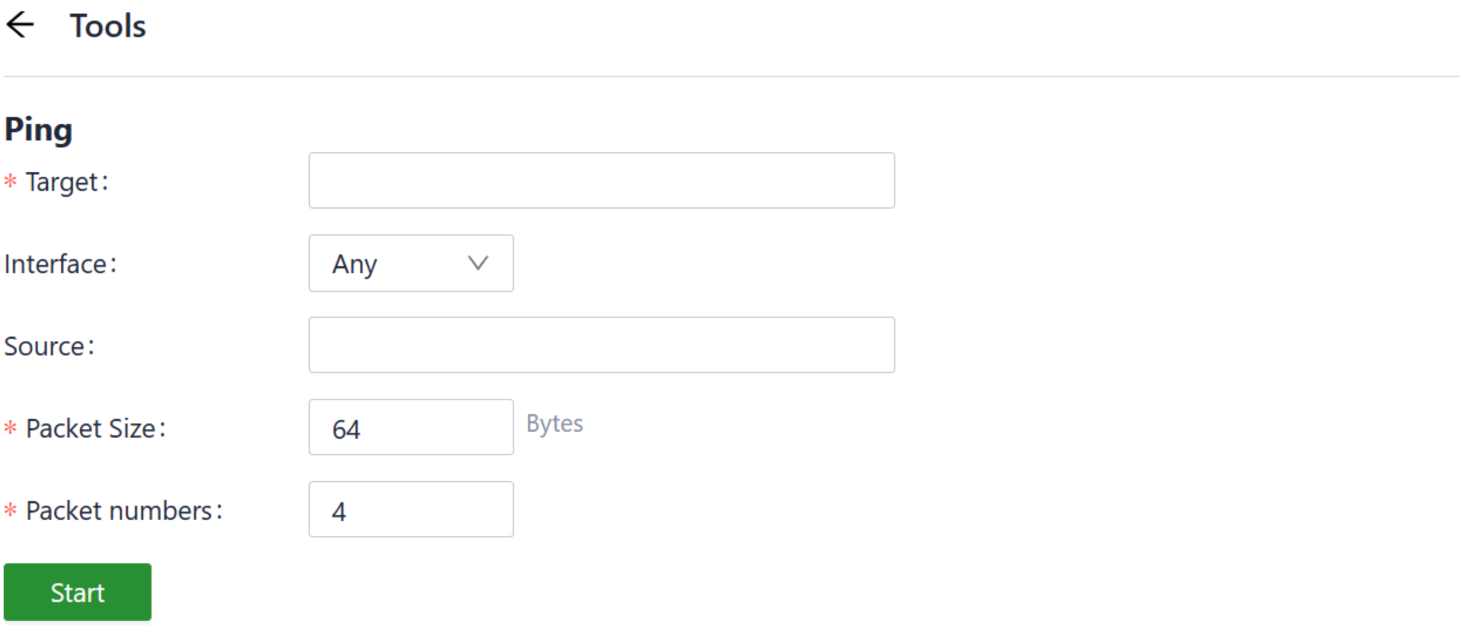
Send a test email to:

Fig. 6-7-7-b Mail receiving settings

6.7.8 Tools

6.7.8.1 Ping

You can use ICMP (Internet Control Message Protocol) to check the device's external network connectivity. In the "Target" field, enter any domain name or IP address you want to test the device's connectivity to, and then click "Start" to check the connectivity status between the device and the specified target. This can help you determine whether the device can reach the target over the internet.
You can perform a network ping test on a target by going to "System > Tools > Ping." This allows to send ICMP echo requests to the specified target IP address or domain name and receive ICMP echo replies to check network connectivity and latency to that target.



← Tools

Ping

* Target:

Interface: Any

Source:

* Packet Size: 64 Bytes

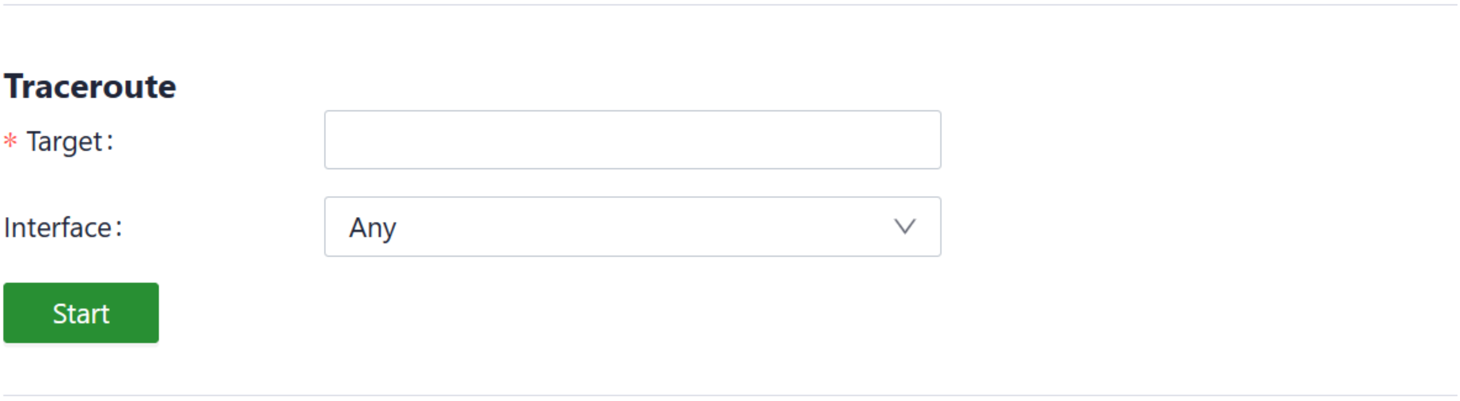
* Packet numbers: 4

Start

Fig. 6-7-8-1 Ping

6.7.8.2 Traceroute

Traceroute is a network diagnostic tool used to determine the network path that data packets take from the source to the destination, as well as the intermediate routers or hops along that path.You can enter the target host's IP address in "System > Tools > Traceroute," choose the outgoing interface for the traffic, click "Start," and check the device's connectivity to the target IP by tracing the route.



Traceroute

* Target:

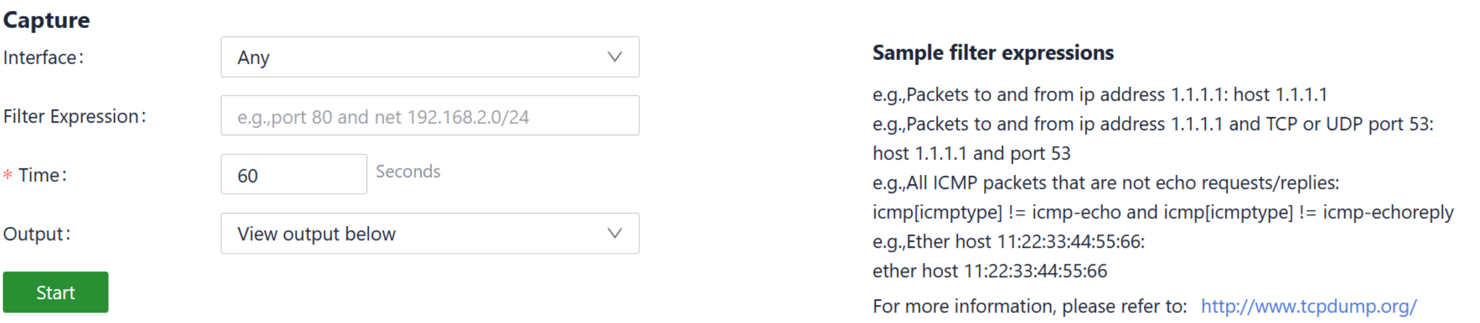
Interface: Any

Start

Fig. 6-7-8-2 Traceroute

6.7.8.3 Capture

Packet capturing is a network monitoring and analysis technique used to capture and record data packets transmitted over a computer network. Packet capture tools are typically used for network troubleshooting, network performance analysis, security auditing, and protocol analysis, among other purposes.
Users can capture packets passing through a specific interface in "System > Tools > Packet Capture." By selecting the "Output" option, users can choose to display the captured data within the interface or export it locally for further analysis.



Capture

Interface: Any

Filter Expression: e.g.,port 80 and net 192.168.2.0/24

* Time: 60 Seconds

Output: View output below

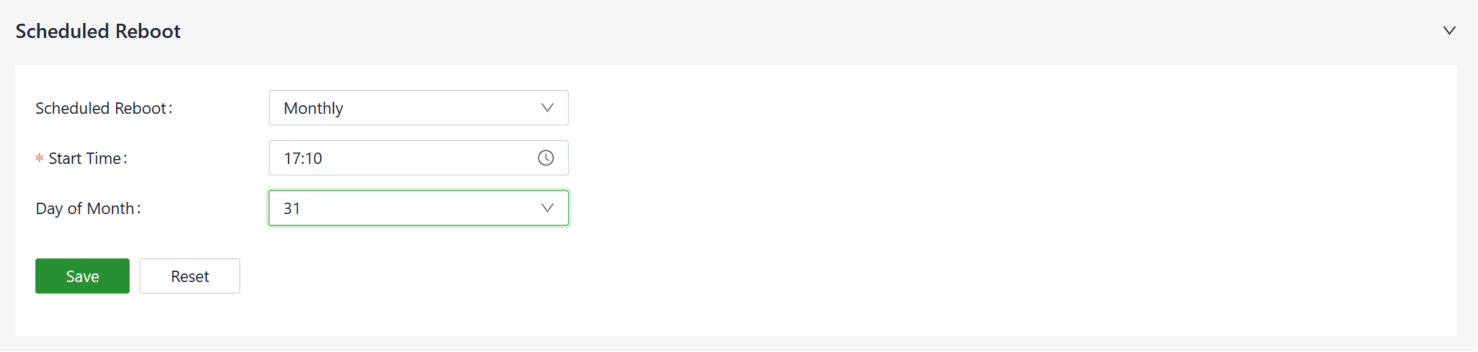
Sample filter expressions

e.g.,Packets to and from ip address 1.1.1.1: host 1.1.1.1
e.g.,Packets to and from ip address 1.1.1.1 and TCP or UDP port 53: host 1.1.1.1 and port 53
e.g.,All ICMP packets that are not echo requests/replies: icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echoreply
e.g.,Ether host 11:22:33:44:55:66: ether host 11:22:33:44:55:66
For more information, please refer to: http://www.tcpdump.org/

Fig. 6-7-8-3 Capture

6.7.9 Scheduled Reboot

Scheduled reboot is a network device management strategy that allows administrators to automatically restart a device at a specific time or under certain conditions to ensure the device's normal operation and performance.
In practice, users can set up scheduled reboots in the "System > Scheduled Reboot" function based on their business requirements. The device supports scheduled reboots at fixed times daily, weekly, or monthly.
In the case of monthly reboots, if the selected reboot day exceeds the actual number of days in the month, the device will reboot on the last day of the month. For example, if you choose to reboot on the 31st of every month, it will reboot on the 30th in a month with only 30 days.



Scheduled Reboot

Scheduled Reboot: Monthly

* Start Time: 17:10

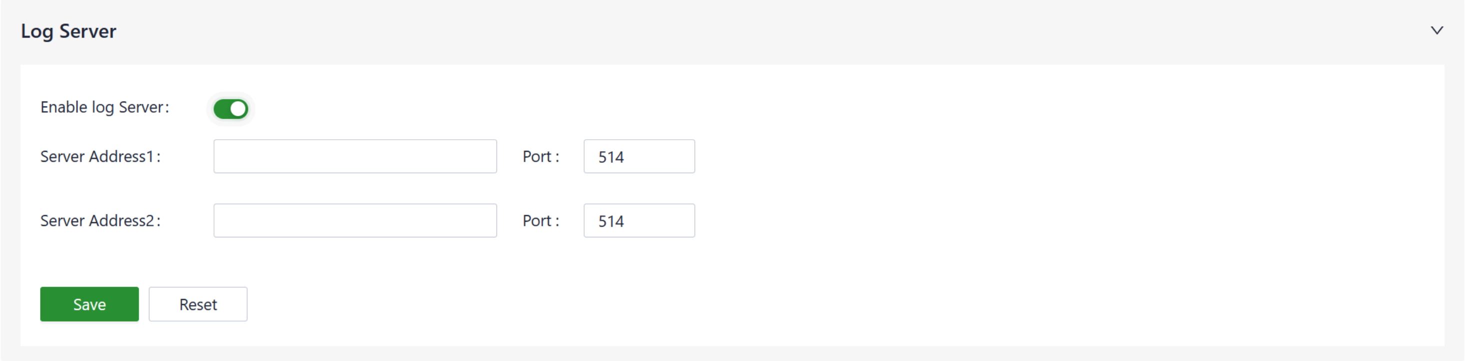
Day of Month: 31

Fig. 6-7-9 Set the scheduled reboot time

6.7.10 Log Server

A log server is a dedicated server or software application used to collect, store, and manage log information generated by network devices, applications, and operating systems. These log records include events, warnings, errors, activities, and other relevant information and are crucial for monitoring, troubleshooting, and performance optimization.

When users enable the log file server function in the "System > Log Server" feature, the device will periodically upload log files to the specified log server.



Log Server

Enable log Server: ●

Server Address1: Port: 514

Server Address2: Port: 514

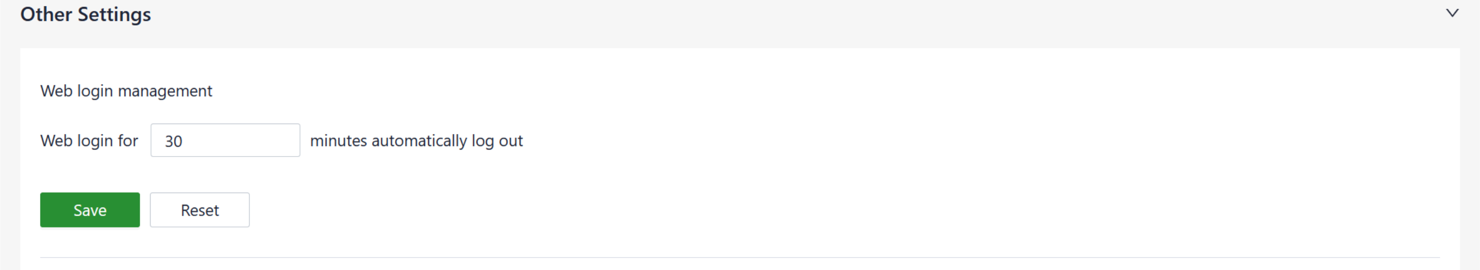
Fig. 6-7-10 Set the log server address

6.7.11 Other Settings

6.7.11.1 Web Login Management

When a user logs in to the local interface of the device through the web and the session remains active for a certain period, it will automatically log out or disconnect to protect the user's privacy and security.

You can configure the logout time in "System > Other Settings > Web Login Management." If the online time during a single login session on the device's web page exceeds the configured time, the system will automatically log the user out, and they will need to log in again to continue their operations.



Other Settings

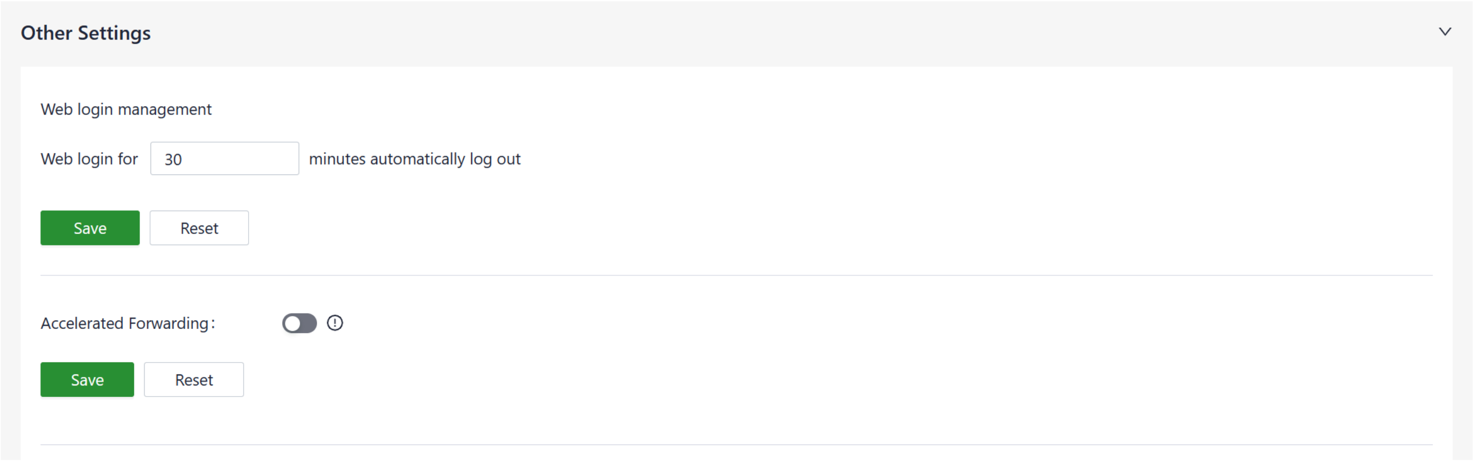
Web login management

Web login for 30 minutes automatically log out

Fig. 6-7-11-1 Set the web page logout time

6.7.11.2 Accelerated Forwarding

This feature can be used to accelerate packet forwarding and enhance network performance. It is turned off by default.After enabling this feature in "System > Other Settings > Accelerated Forwarding," the device's cellular speed will significantly improve.



Other Settings

Web login management

Web login for 30 minutes automatically log out

Accelerated Forwarding:

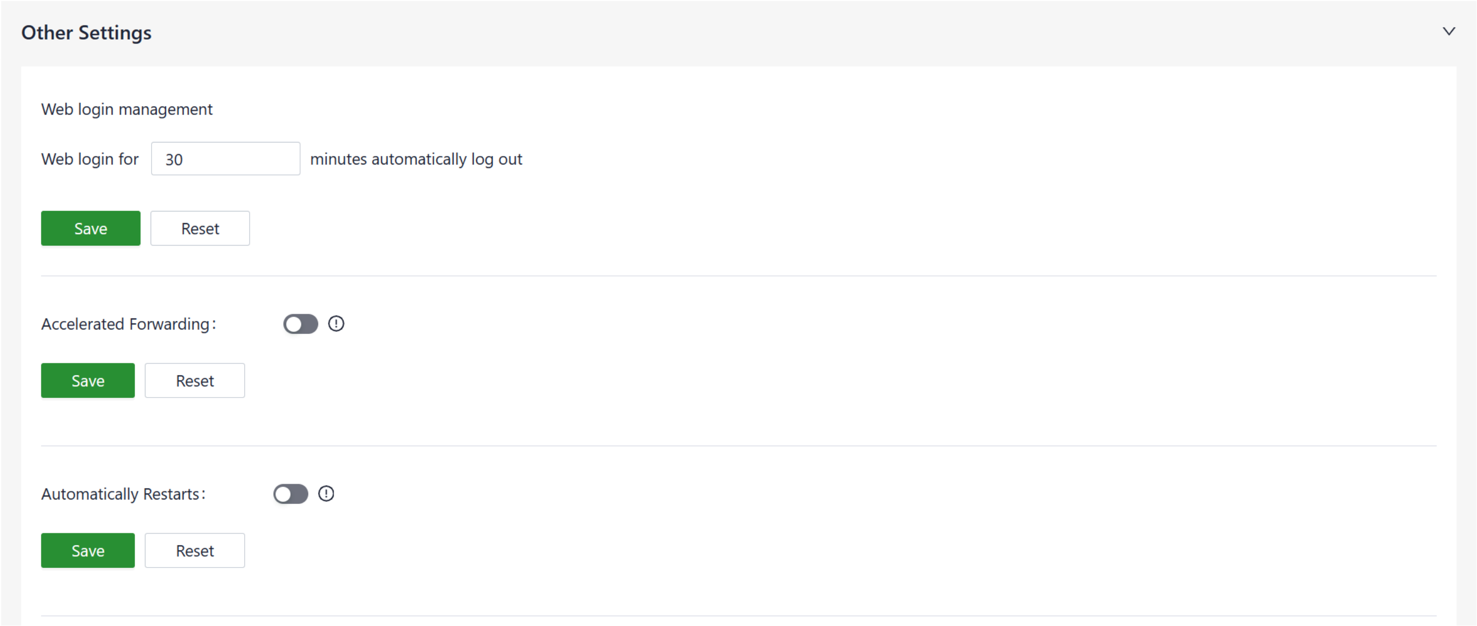
Fig. 6-7-11-2 Enable the accelerated forwarding

Cautions:

- Enabling this feature will disable the normal functioning of IPSec VPN, traffic shaping, and other related features.

6.7.11.3 Automatically Restarts

This feature can be used to quickly forward packets, improving network performance. By default, it is turned off. When users enable this feature in "System > Other Settings > Fast Forward," the device's data forwarding rate will significantly increase.



Other Settings

Web login management

Web login for 30 minutes automatically log out

Accelerated Forwarding:

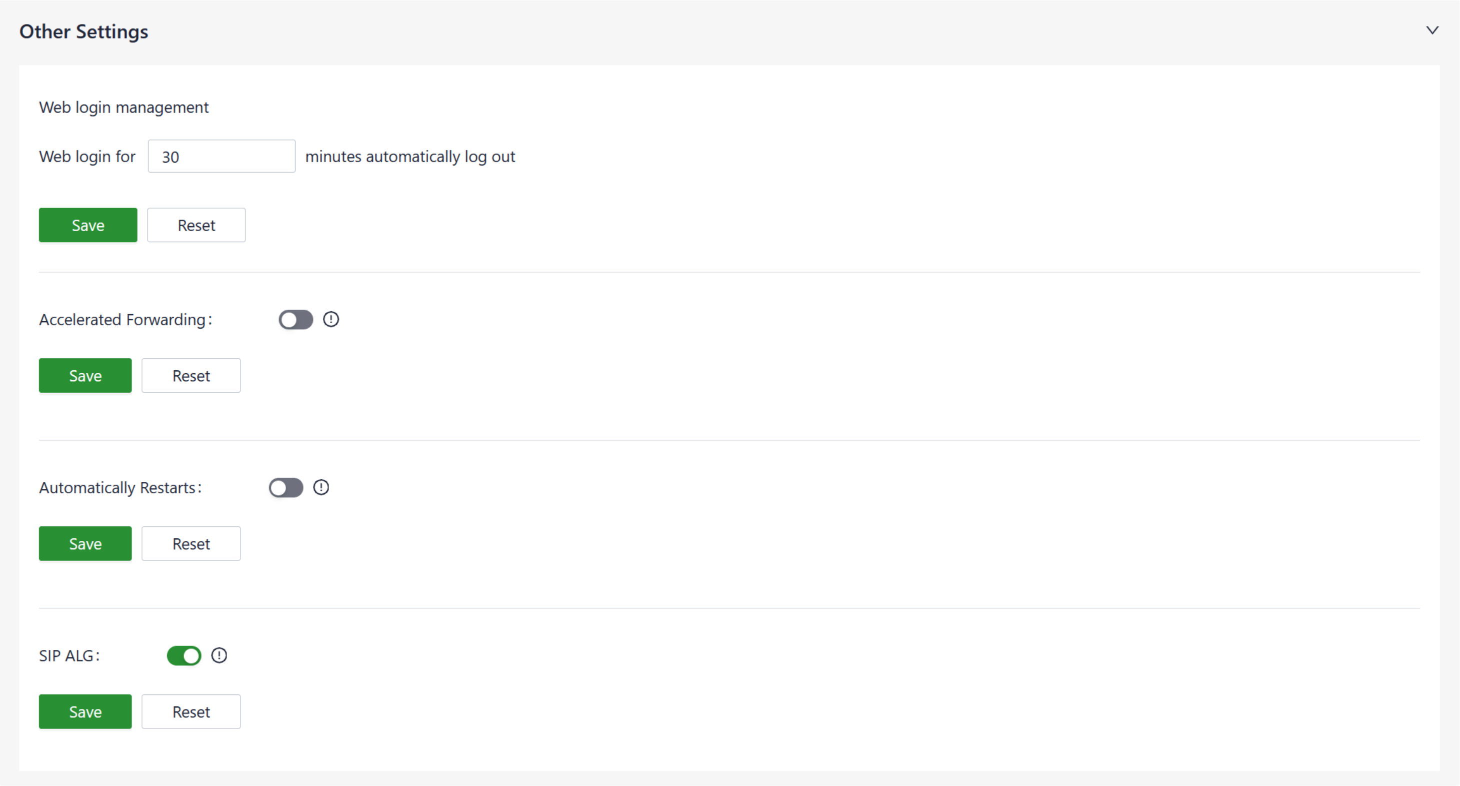
Automatically Restarts:

Fig. 6-7-11-3 Enable the Automatically

6.7.11.4 SIP ALG

SIP ALG consists of two technologies: Session Initiation Protocol (SIP) and Application Layer Gateway (ALG). This protocol is typically used to assist in managing and handling SIP communications (Session Initiation Protocol for establishing and managing real-time communication sessions, such as voice and video calls).

Users can enable this feature in "System > Other Settings > SIP ALG."



Other Settings

Web login management

Web login for 30 minutes automatically log out

Accelerated Forwarding: ○

Automatically Restarts: ○

SIP ALG: ●

Fig. 6-7-11-4 Enable the SIP ALG

Note：

- If the connected device needs to engage in VoIP (Voice over Internet Protocol) phone communication, it is recommended to disable this function.

6.7.12 SD-WAN

Backgroud:
Between enterprise branches, there is often a need for mutual access to facilitate business data transfer, video conferencing, and other requirements. Traditional VPN configurations can be complex and troubleshooting can be challenging. InHand Networks introduces SD-WAN network functionality, which, through a user-friendly interface, assists users in rapidly establishing connections between branches. This not only enhances link flexibility but also significantly reduces operational and management complexity, ultimately providing enterprise users with a better network experience.

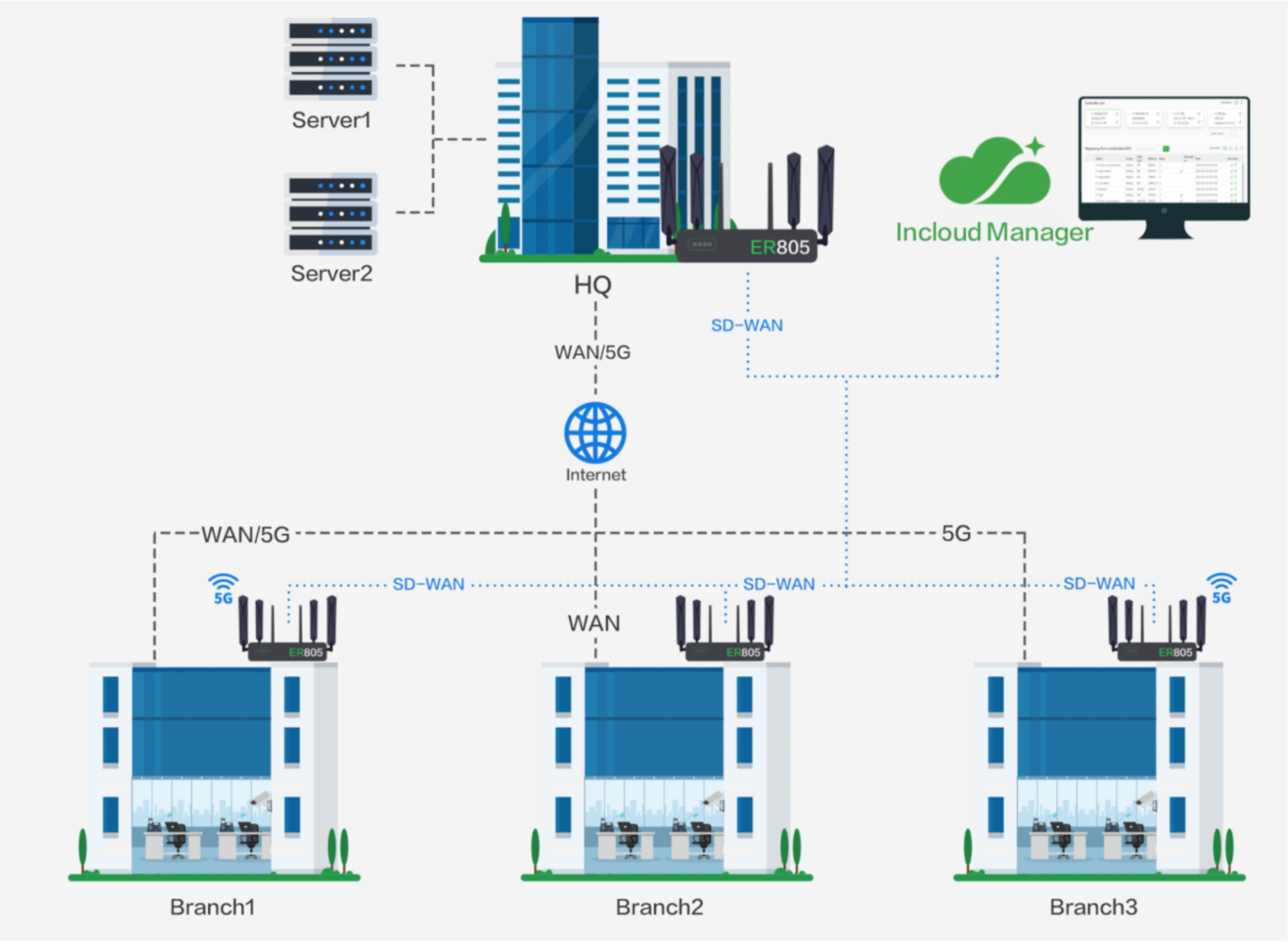


Fig. 6-7-12-a Application Scenarios

Process：

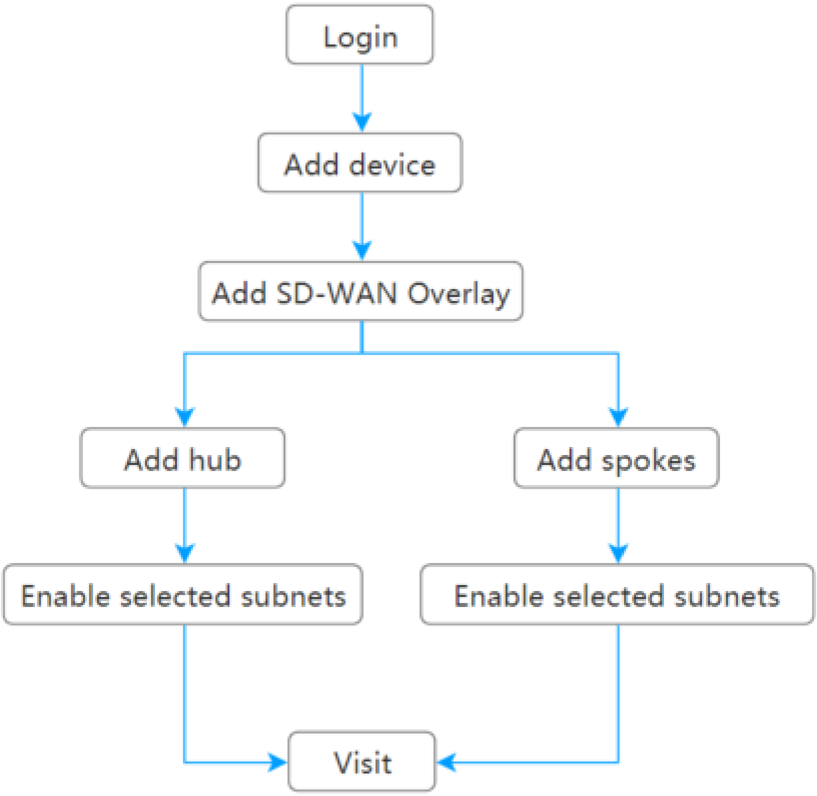
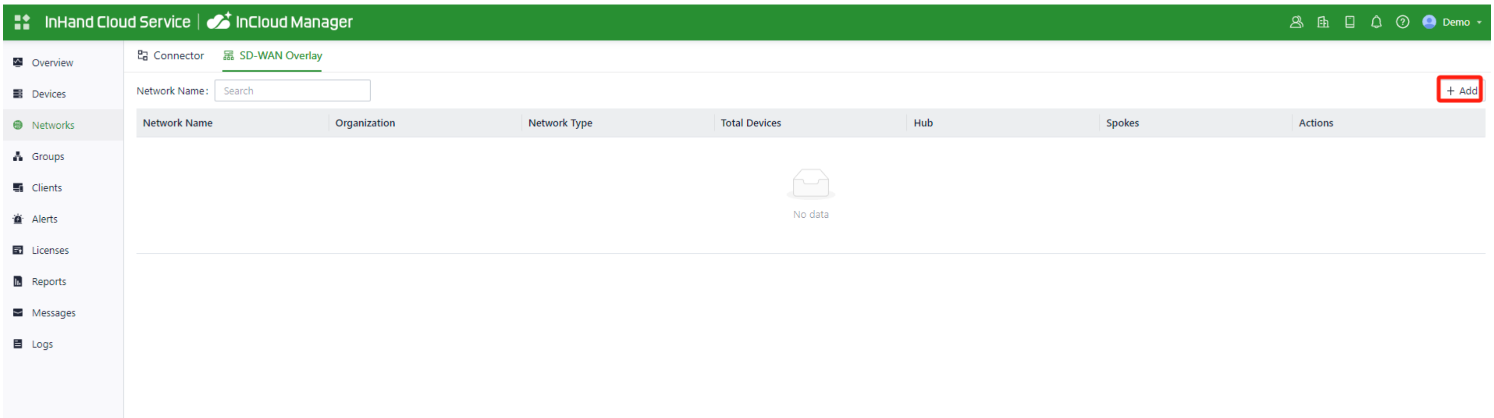


Fig. 6-7-12-b Application Scenarios

6.7.12.1 Create Network

In the platform's "Network" function, select "SD-WAN," click on "Add," and you will be redirected to the SD-WAN network addition page.

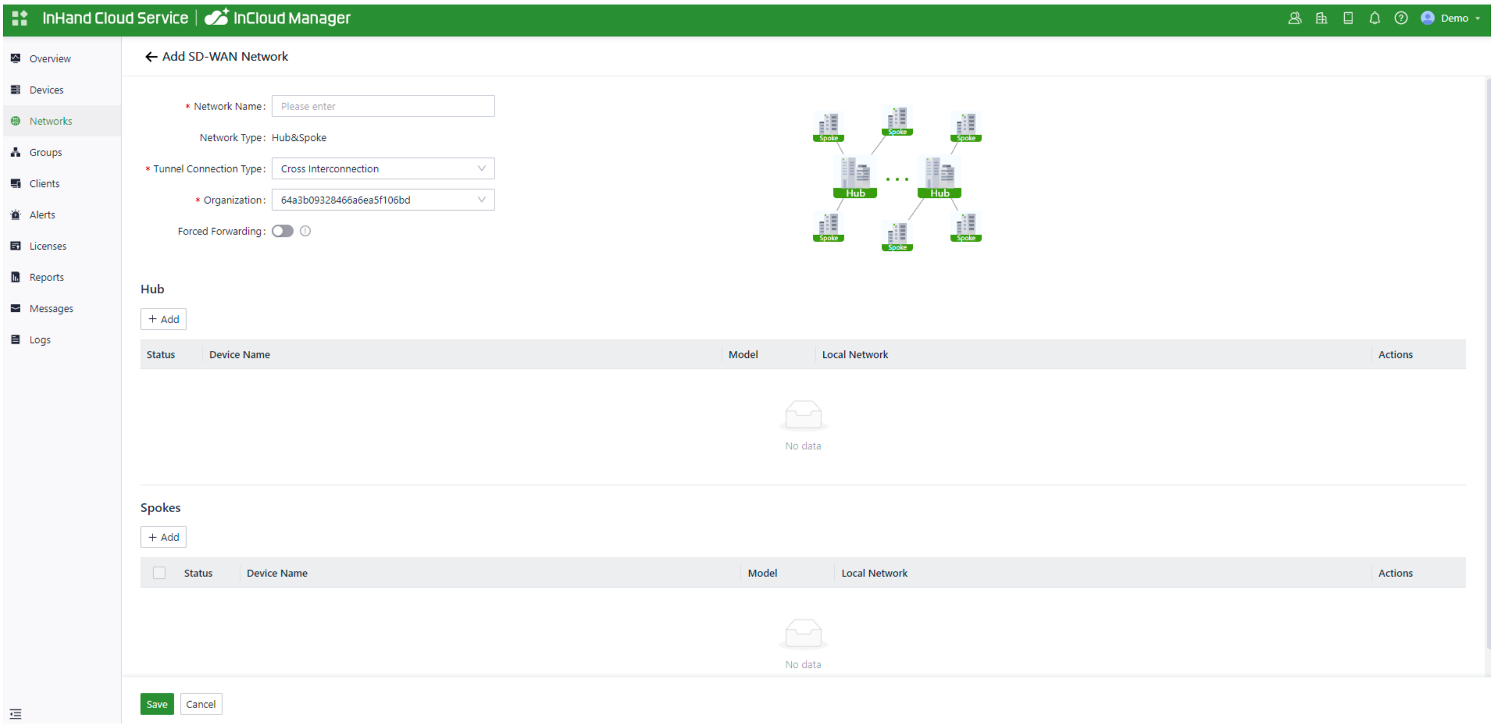


Network Name: Search

Network Name	Organization	Network Type	Total Devices	Hub	Spokes	Actions

No data

Fig. 6-7-12-1-a SD-WAN Entry



Add SD-WAN Network

* Network Name: Please enter

Network Type: Hub&Spoke

* Tunnel Connection Type: Cross Interconnection

* Organization: 64a3b09328466a6ea5f106bd

Forced Forwarding: ○

Hub

+ Add

Status	Device Name	Model	Local Network	Actions

No data

Spokes

+ Add

□	Status	Device Name	Model	Local Network	Actions

No data

Fig. 6-7-12-1-b Create SD-WAN Network

The current SD-WAN network supports the Hub & Spoke topology, with device roles divided into central and branch devices. All branch devices establish tunnels through the central device, and traffic between branch devices passes through the central device.

Hub:

- Central devices require a public IP address to ensure the operation of the SD-WAN network. Users can also address the issue of insufficient public IPs through IP mapping.

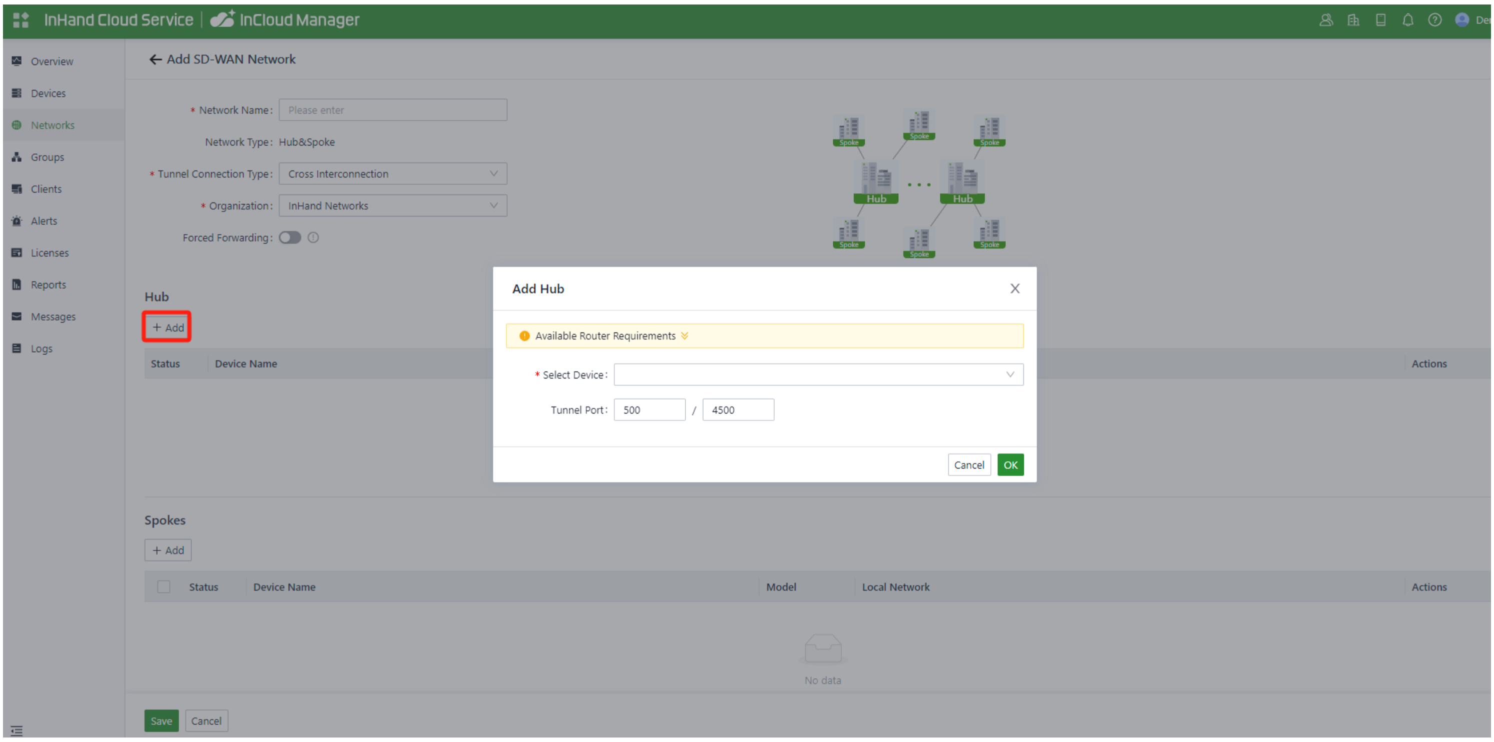
- Tunnels are established between the central device's upstream interface with public IP addresses and all upstream interfaces of the branch devices.
- In the firewall rules, the central device's upstream device needs to allow two port numbers and map them to the upstream interface of the ER series router. The port range is 1-65535.
- Supported device models: ER805, ER605, ER2000
- A maximum of 5 devices can be added.

Spoke:

- Branch devices have no specific requirements for public IP addresses.
- Multiple branch devices can be added, with the final number determined by the performance of the central device.
- Supported device models: ER805, ER605.

6.7.12.2 Add device

On the "Add Network" page, click the "Add" button for either the central device or branch device, depending on the type of device you want to add to the network.After selecting the device, provide the public IP mapping information for the device. If you need to modify the device's network configuration, you can click the "Edit" button for the local network to perform remote configuration.



← Add SD-WAN Network

* Network Name: Please enter

Network Type: Hub&Spoke

* Tunnel Connection Type: Cross Interconnection

* Organization: InHand Networks

Forced Forwarding:

Hub

Status	Device Name	Actions

Add Hub

Available Router Requirements

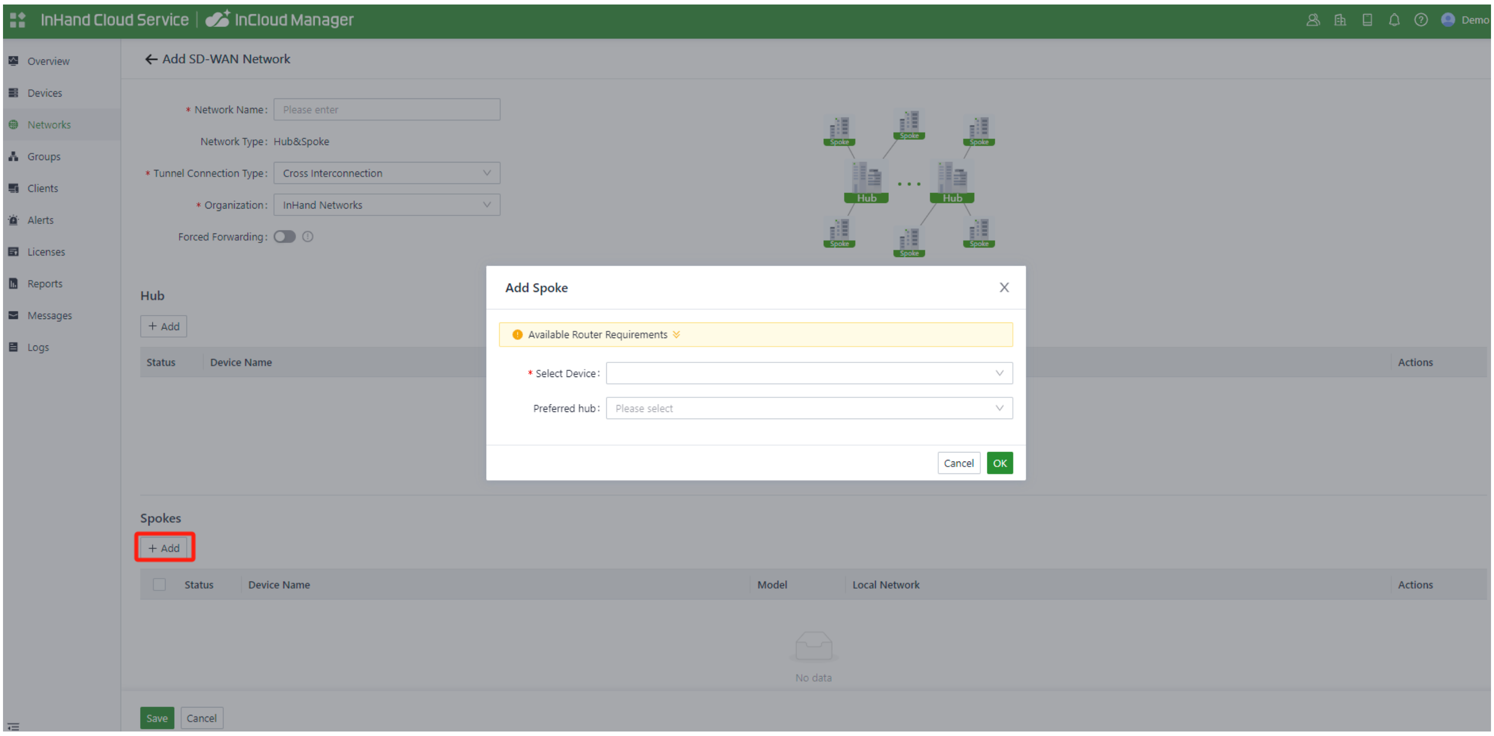
* Select Device:

Tunnel Port: 500 / 4500

Spokes

Status	Device Name	Model	Local Network	Actions

Fig. 6-7-12-2-a Add Hub



Add SD-WAN Network

* Network Name: Please enter

Network Type: Hub&Spoke

* Tunnel Connection Type: Cross Interconnection

* Organization: InHand Networks

Forced Forwarding:

Hub

Add Spoke

Available Router Requirements

* Select Device:

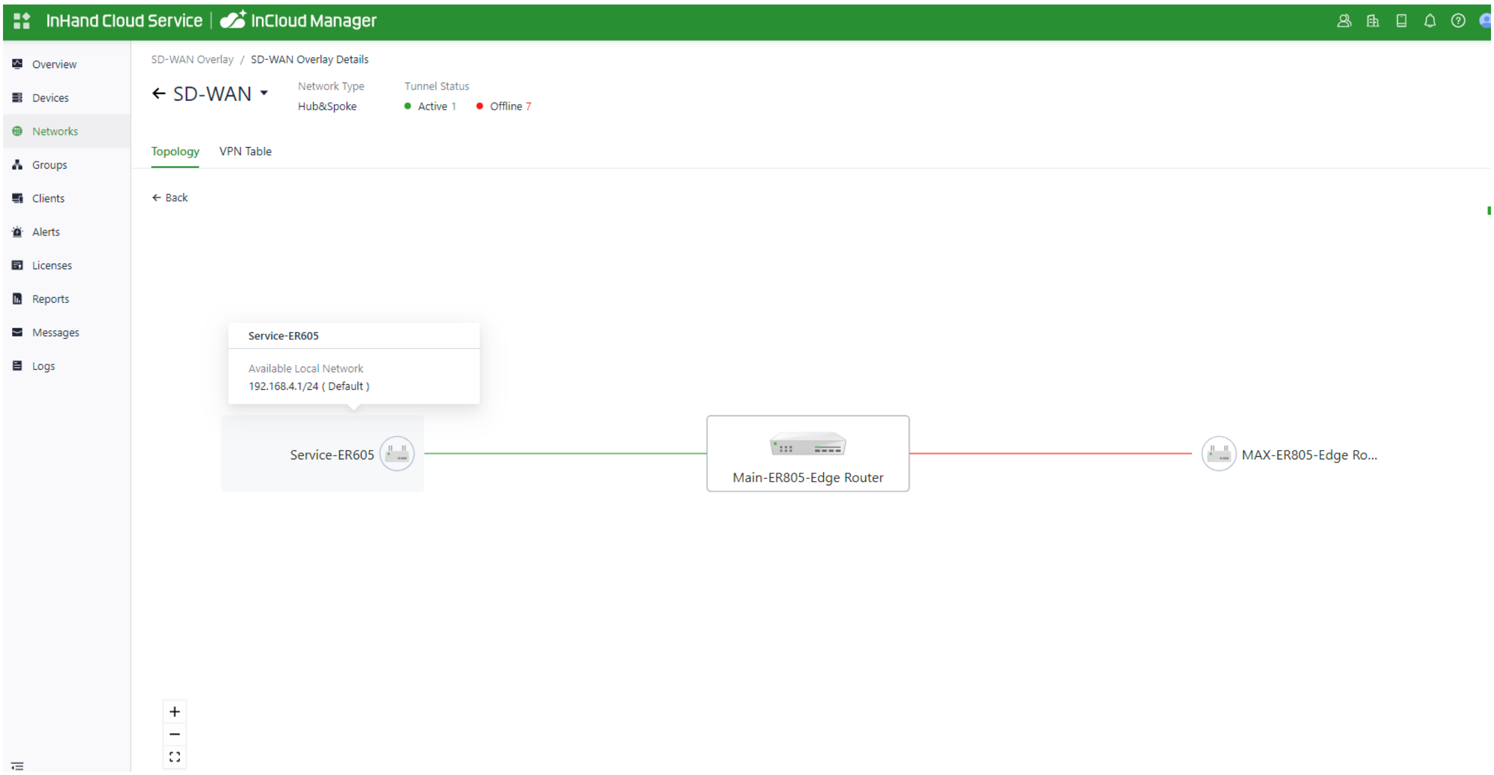
Preferred hub: Please select

Fig. 6-7-12-2-b Add Spoke

After you've completed the addition, click the "Save" button at the bottom left corner of the page, and the network will be successfully created. All the devices and selected subnets will now be interconnected. In a single network, the local networks of central devices and branch devices cannot be the same, as it could impact communication.

6.7.12.3 Check Status

After the network is added, you will be automatically directed to the topology page. Alternatively, you can go to the "SD-WAN Network" list and click on the network name to access the topology details page. Within the network, all branch devices establish connections with the central device.



SD-WAN

Network Type: Hub&Spoke

Tunnel Status: Active 1 Offline 7

Service-ER605

Available Local Network

192.168.4.1/24 (Default)

Fig. 6-7-12-3-a Topology

When hovering the mouse over a link, it displays the status of the tunnels established with the interfaces of the central device.

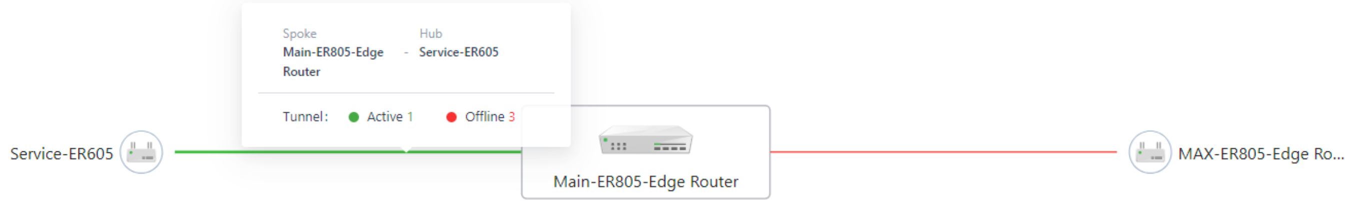
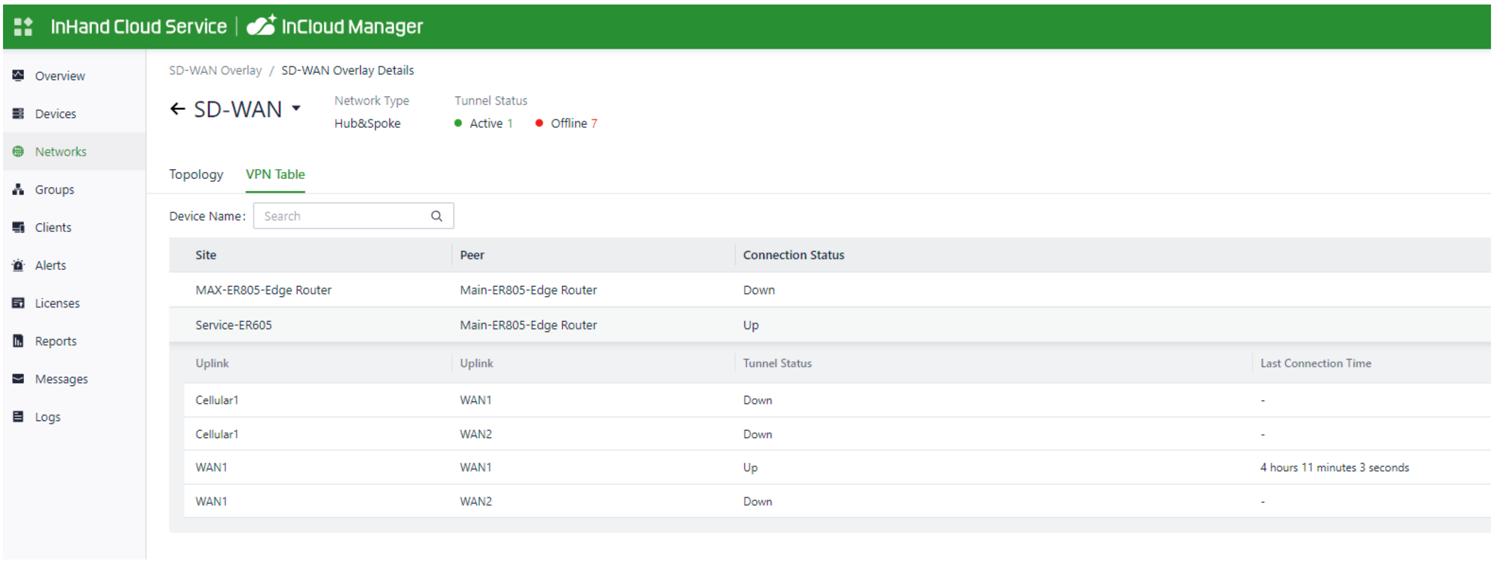


Fig. 6-7-12-3-b Link Status

Click on the "VPN Table" at the top-right corner of the "SD-WAN Network Details" page to switch to a tabular view, displaying information about all devices within the network that have established VPN connections with the central device.



Network Type: Hub&Spoke

Tunnel Status: ● Active 1 ● Offline 7

Device Name:

Site	Peer	Connection Status
MAX-ER805-Edge Router	Main-ER805-Edge Router	Down
Service-ER605	Main-ER805-Edge Router	Up

Uplink	Uplink	Tunnel Status	Last Connection Time
Cellular1	WAN1	Down	-
Cellular1	WAN2	Down	-
WAN1	WAN1	Up	4 hours 11 minutes 3 seconds
WAN1	WAN2	Down	-

Fig. 6-7-12-3-c VPN List

7. Security Precautions

1. Please use the original power adapter to avoid damaging the device due to mismatched power adapters.
2. When installing the device, avoid placing it in an environment with strong electromagnetic interference, and keep it at a safe distance from high-power equipment. After installation, ensure that the device is stable to prevent accidental drops and potential damage.
3. Ensure that the device's operating environment meets the temperature and humidity requirements specified in the user manual.

4. Regularly inspect the device's cables, including Ethernet cables and power adapter connections. Keep the cables clean, and replace them if any damage is detected.
5. When cleaning the device, avoid spraying chemical agents directly on the device's surface to prevent damage to the housing or internal components. Use a soft cloth for cleaning.
6. Do not attempt to disassemble or modify the device on your own, as this can pose safety risks and may void the device's warranty.

8. FAQ

1.What are the differences between ER routers and regular routers?

1. Edge Router: Supports both wired and cellular mobile data connectivity (4G, 5G) for network access, providing more ways to connect to the network. The edge router is a 5G router that supports SD-WAN and allows for centralized management through a cloud platform.

2. Regular Router: Typically relies on fixed broadband connections, such as DSL or fibre optics, and connects to the network through wired connections. Regular routers lack a unified management platform and advanced features like firewall and SD-WAN.

2.Unable to Connect to 4G/5G Network?

1. Physical Environment: Start by checking if the SIM card is inserted into the correct slot and ensure all cellular antennas are properly installed.

2. APN Settings: Make sure that the APN configuration matches the information provided by your service provider.

3. Check Device Connectivity: Log in to the device's local interface and use the built-in ICMP tool to ping 8.8.8.8 to test connectivity. If it can connect, then check the connectivity between your device (e.g., computer or smartphone) and the router.

4. Check SIM Card: Take out the SIM card and insert it into a phone to see if it can connect to the internet.

5. Restart: Try powering off the router, wait a few seconds, and then reconnect the power to retry the network connection.

6. Factory Reset: Perform a factory reset on the router and then attempt to connect again.

3.Is the cloud platform free of charge?

InHand Networks has been committed to providing high-quality network services for small and medium-sized chain organizations. When users utilize the cloud platform services, they are required to purchase licenses for each device to access the extensive cloud-based features.

4.How to add devices to the cloud platform?

1. Start by registering for InCloud Manager account at https://star.inhandcloud.com/.

2. Log in to the cloud platform using your registered account. Under the device menu, click "Add," and follow the prompts to enter the device's serial number and MAC address. This will complete the device addition process. When a device is added for the first time, it comes with a complimentary 1-year free Basic Edition license. Users can renew their licenses as needed in the future.

5.Is it possible to use the device without the cloud platform?

Yes, it is possible. Users can complete the majority of configuration tasks locally. However, for features like bulk configuration deployment, firmware upgrades, SD-WAN, Connector, and more, you would need to combine local device settings with the cloud platform.

If you are unable to resolve the issue using the above steps or encounter any other problems, please contact InHand Networks for technical support. You can visit www.inhandnetworks.com for more information.