



InHand ER605 Edge Router

User Manual

Issue: V1.0.0—December 1 2022

Declaration

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

No part of this document shall be quoted or reproduced in any form or disclosed to any third party without prior written permission of InHand.

The contents of this document are subject to change without prior notice as a result of continuing improvements to the product. InHand cannot promise that the contents are consistent with the actual product information, and assumes no responsibility for any disputes arising out of the discrepancies. InHand reserves the right to update and interpret information in this manual.

Copyright © 2022 Beijing InHand Networks Technology Co., Ltd. and its licensors. All rights reserved.

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

GUI and Symbol Conventions

Format/Symbol	Description
【 】	Represents a function module or menu, such as: in the 【 Status 】 menu.
>	Multi-level menus are separated by the ">" signs. For example, choose File > Create > Folder .
Cautions	Please be careful of the contents under Cautions, improper action may result in loss of data or device damage.
Note	Note contains detailed descriptions and helpful suggestions.

Technical Support

Email: support@inhandnetworks.com

URL: www.inhandnetworks.com

Contents

1 Overview	1
2 Hardware	2
2.1 Indicator Description	2
2.2 Using the Reset Button to Restore Factory Settings	3
3 Default Settings	4
4 Quick Network Connection	5
4.1 Environment Setup	5
4.2 Internet Connection	6
4.2.1 Wired Connection Via a WAN Interface	6
4.2.2 Wireless Connection via the Cellular Interface	8
4.2.3 Wireless Connection via Wi-Fi(STA)	10
5 Dashboard	12
5.1 Device Information	12
5.2 Interface Status	12
5.3 Traffic Statistics	13
5.4 Number of Wi-Fi Connections	13
5.5 Top 5 Clients by Traffic	14
6 Status	15
6.1 Link Monitor	15
6.2 Cellular Signals	15
6.3 Clients	16
6.4 VPN	16
6.5 Events	16

6.6 Logs	17
7 Internet	18
7.1 Uplink Table	18
7.2 Uplink Settings	19
8 Local Network	20
8.1 Passthrough Settings	20
8.2 Local Network List	20
9 Wi-Fi	22
10 VPN	23
10.1 IPSec VPN	23
10.2 L2TP VPN	24
10.2.1 Client	24
10.2.2 Server	25
11 Security	27
11.1 Firewall	27
11.1.1 Inbound and Outbound Rules	27
11.1.2 Port Forwarding	28
11.2 Policy-based Routing	29
11.3 Traffic Shaping	30
12 Services	31
12.1 Interface Management	31
12.2 DHCP Server	31
12.3 Fixed Address List	32
12.4 Static Routes	33

13 System	34
13.1 Adm Management	34
13.2 Cloud Management	34
13.3 Remote Access Control	35
13.4 System Clock	36
13.5 Device Options	36
13.6 Configuration Management	37
13.7 Alarms	37
13.8 Tools	38
13.8.1 Ping	38
13.8.2 Traceroute	38
13.8.3 Packet Capture	39

1 Overview

Edge Router 605 (ER605 for short) is a next-generation edge router developed by InHand to provide fast and secure network connections for business applications. Leveraging 4G cellular networks and various broadband services, ER605 provides ubiquitous, uninterrupted access to the Internet for a variety of business devices. With comprehensive security and wireless features, it establishes real high-speed channels for data transfer between devices.

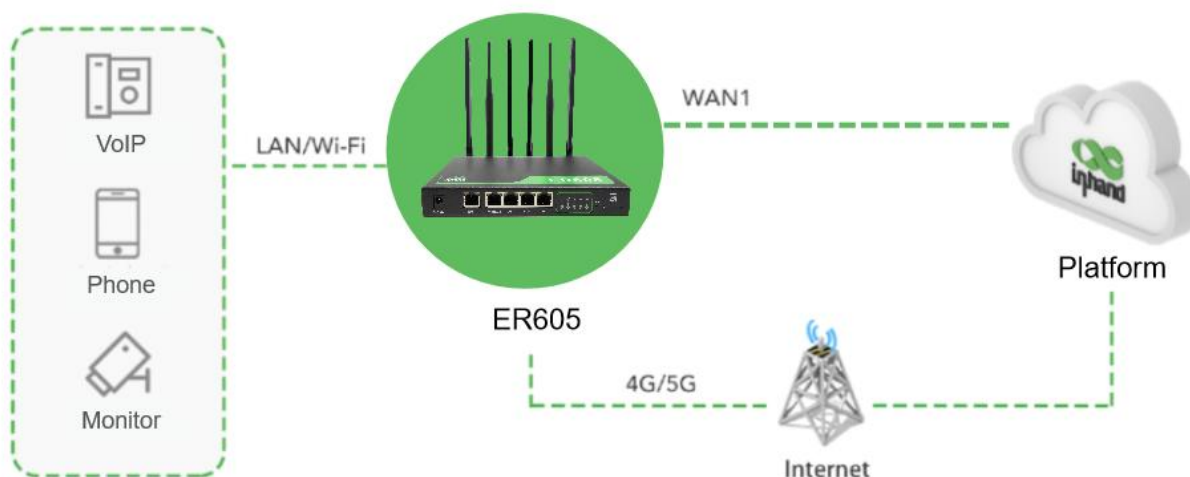


Figure 1 ER605 application

2 Hardware

2.1 Indicator Description

LED Indicator	Status and Description
System status indicator	Off — The router is off. Solid red — The system is starting. Blinking green — The system is running properly. Blinking red — The system does not work properly. Blinking yellow — The system is upgrading.
Connectivity status indicator	Off — The router is not connected to network. Blinking red — The router is connecting to the cellular network. Solid green — The router has connected to the cellular network successfully. Blinking blue — The router is connecting to the wired network. Solid blue — The router has connected to the wired network successfully.
Cellular signal indicator	Off — No signal. Solid red — Signal strength is poor. Solid yellow — Signal strength is good. Solid green — Signal strength is excellent.
Wi-Fi 2.4G	Off: The Wi-Fi 2.4 GHz band is off. Solid yellow — The Wi-Fi 2.4 GHz does not work properly. Blinking yellow — The Wi-Fi 2.4 GHz band is working properly.
Wi-Fi 5G	Off: The Wi-Fi 5 GHz band is off. Solid green — The Wi-Fi 5 GHz does not work properly. Blinking green — The Wi-Fi 5 GHz band is working properly.

Note: If both the cellular and wired networks are connected, the connectivity status indicator shows yellow (wired network). If one of networks is not connected, the indicator shows the color corresponding to the connected network. If neither network is connected, the indicator shows red.

2.2 Using the Reset Button to Restore Factory Settings



Procedure:

Step 1: Power on the device (10 seconds), press and hold the reset button until the SYS indicator is steady yellow

Step 2: Release the button, wait for the SYS LED to flash yellow.

Step 3: Press the reset button again until the SYS indicator is steady yellow

3 Default Settings

No.	Function	Default Settings
1	Cellular network dial-up	Both SIM cards are enabled, and SIM1 is used preferentially.
2	Wi-Fi	- The Wi-Fi 2.4 GHz access point (AP) is enabled, and its SSID is ER605– followed by the last six digits of the wireless MAC address. - The Wi-Fi 5 GHz AP is enabled, and its SSID is ER605-5G– followed by the last six digits of the wireless MAC address. - The authentication method is WPA2-PSK. - The two access points have the same password: last eight digits of the router's SN.
3	Ethernet	- Four LAN interfaces are enabled. - The IP address is 192.168.2.1. - The subnet mask is 255.255.255.0. - The DHCP server is enabled to allocate IP addresses to connected devices from the address pool 192.168.2.2–192.168.2.100.
4	Network access control	- Local HTTP and HTTPS services are enabled, using ports 443 - Access from the cellular network is disabled.
5	User name and password	The user name is adm (super administrator), and the password is 123456.

4 Quick Network Connection

4.1 Environment Setup

Step 1: Install the 4G and Wi-Fi antennas, and insert SIM cards into the router.

Step 2: Connect the power cable and Ethernet cable, and connect any of LAN interfaces to a PC.

Step 3: Assign an IP address to the PC, which must be in the same network segment as the router.

As the dhcp server function is enabled by default on the LAN interface, the PC must be in the same network segment as the router. On the PC, set **IP address** to any value in the range of 192.168.2.2–192.168.2.254, **Default gateway** to 192.168.2.1, **Subnet mask** to 255.255.255.0, **Preferred dns server** to 8.8.8.8, and **Alternate dns server** to the IP address of the carrier's dns server.

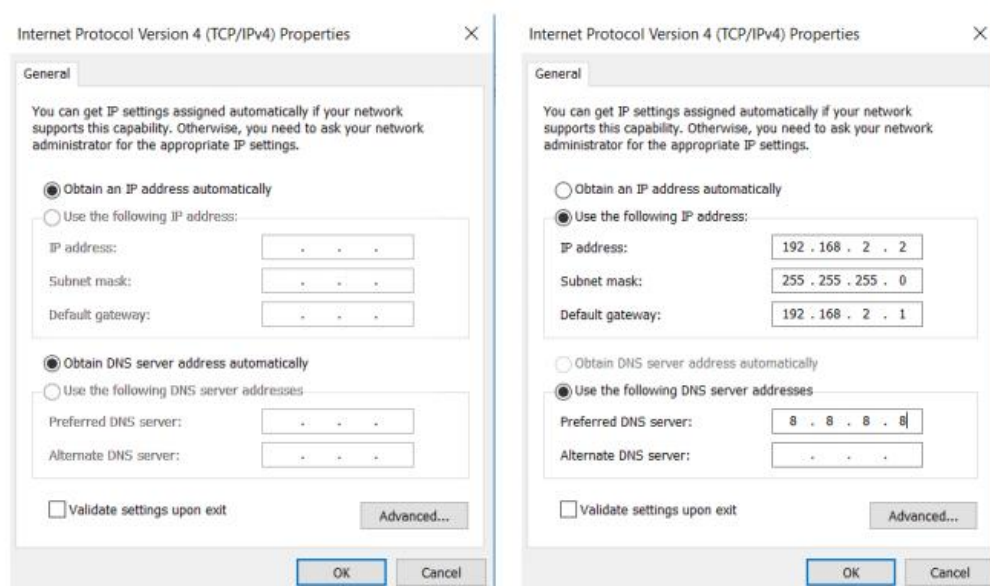


Figure 4-1-1 Dynamic/Manual IP address configuration on the PC

Step 4: Start the web browser and enter the router's default IP address 192.168.2.1 in the address box. On the login page that appears, enter the user name and password (**adm/123456** by default) to log in to the web-based management system of the router. If the web browser displays a message, indicating that the website is not secure, unfold the hidden or advanced settings and choose to continue.

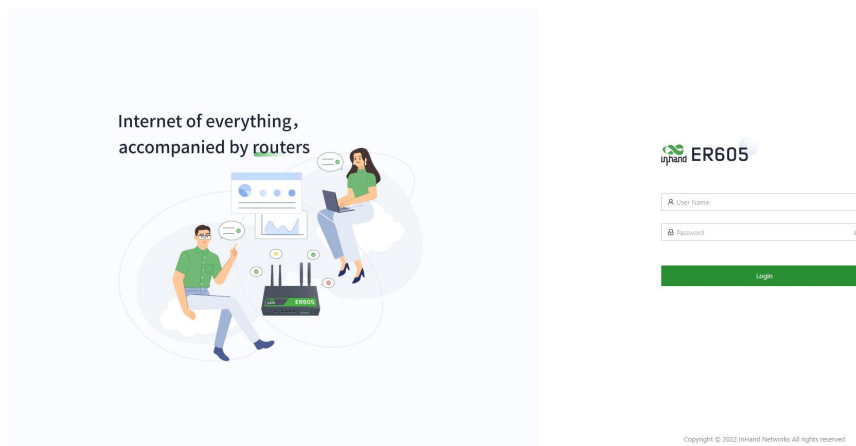


Figure 4-1-2 Login to the web-based management system

4.2 Internet Connection

The ER605 can connect to the Internet via three types of interfaces, each allowing for multiple connection methods. The router has two default uplink interfaces WAN1 and Cellular, which cannot be removed. It supports a maximum of four uplink interfaces, namely, WAN1, WAN2, Cellular, and Wi-Fi(STA). WAN2 and Wi-Fi(STA) need to be added manually and can be removed.

4.2.1 Wired Connection Via a WAN Interface

The ER605 can establish a wired connection through DHCP, a static IP address, or PPPoE. To select a connection method, click **Internet** on the left pane, and then click **Edit** in the row of WAN1

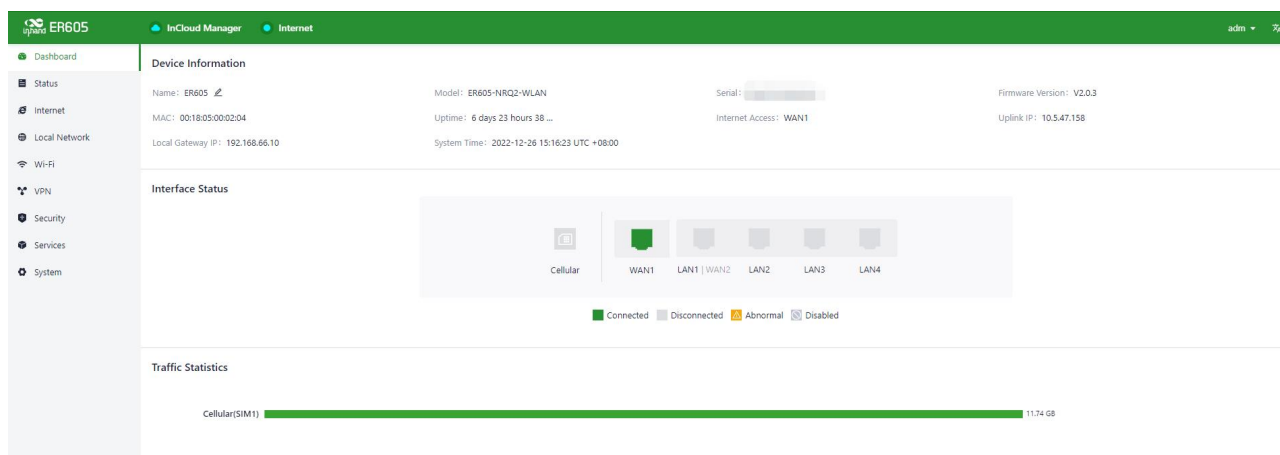


Figure 4-2-1-a Editing interface WAN1

- **DHCP:** The DHCP service is enabled on the WAN interface by default. Therefore, the router can connect to the Internet immediately when the WAN interface is connected to the Internet with an Ethernet cable.
- **Static IP address:** Manually assign an IP address obtained from the carrier or upstream network device. Then, the router can connect to the Internet using this static IP address.

Edit WAN1

Name: WAN1

Status: ☒

NAT: ☒

Type: Static IP

* IP Address:

* Mask:

* Gateway Address:

* Main DNS:

Secondary DNS:

* MTU: 1500

Cancel Save

Figure 4-2-1-b Assigning a static IP address to the router

- PPPoE: Configure the PPPoE service on WAN1. Then, the router can dial up to the Internet through the broadband service.

Edit WAN1

Name: WAN1

Status: ☒

NAT: ☒

Type: PPPoE

* User Name:

* Password:

Local IP Address:

Remote IP Address:

Cancel Save

Figure 4-2-1-c Configuring PPPoE

To use the second WAN interface, click **Add** on the **Internet** page to add WAN2. This interface provides the same functions as WAN1.

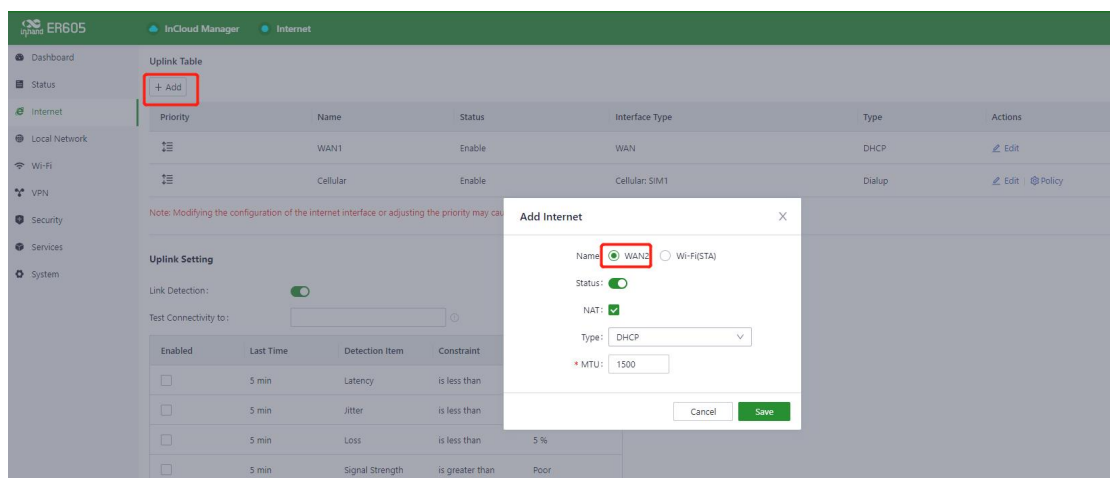


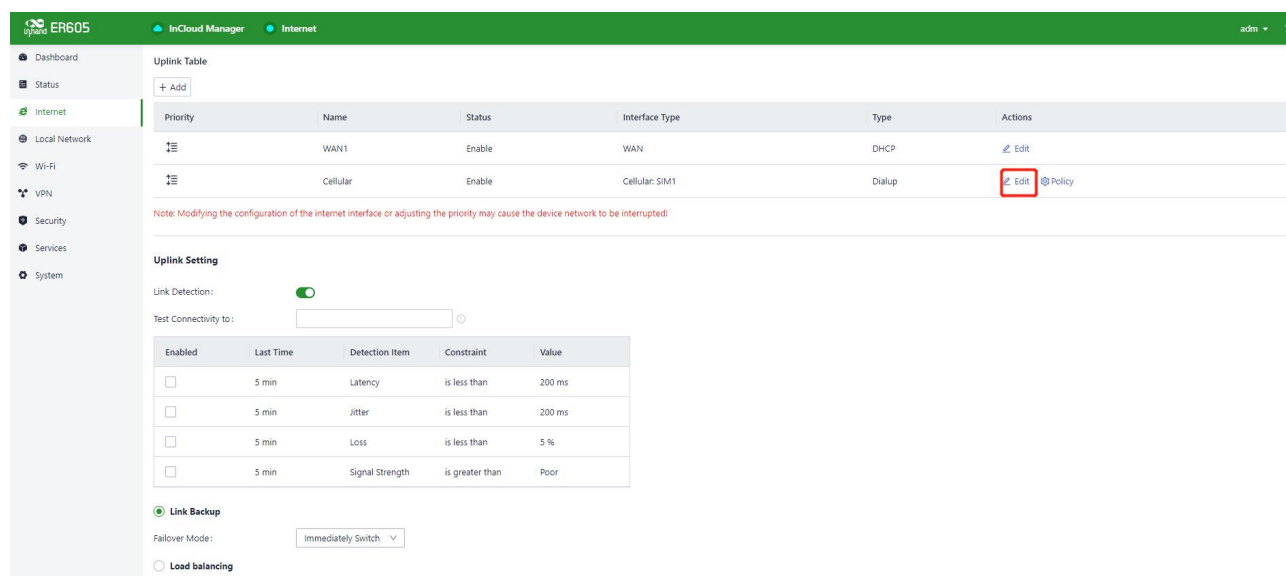
Figure 4-2-1-d Adding WAN2

Notes:

- After you add WAN2, interface LAN1 changes to WAN2.
- After you remove WAN2, the interface changes back to LAN1.
- When WAN2 is removed, all configuration on this interface, including the static routes, inbound and outbound rules, port forwarding, policy-based routing, VPN, and traffic shaping, is deleted.

4.2.2 Wireless Connection via the Cellular Interface

Generally, the ER605 dials up to the cellular network automatically after you install the SIM cards and antennas according to the installation guide, and power on the router. To set the access point name (APN), click **Internet** on the left pane, and then click **Edit** in the row of **Cellular**.



Edit Cellular
✕

Status: ☒

NAT: ☒

Work Mode: Only SIM1 ▼

Dialing Parameters: Auto ▼

Service Type: Auto ▼

5G Type: SA/NSA ▼

PIN Code:

* MTU:

Mask:

Cancel
Save

Figure 4-2-2-a/b Editing the cellular interface

The ER605 allows you to set traffic policies for cellular network access. After a traffic policy is enabled, the working SIM card will take the specified action when the traffic usage reaches the set threshold.

Edit SIM Card Policy
✕

SIM1 Threshold: ☒

* Threshold: GB ▼

Monthly Reset Day: 1 ▼

Action: Notification ▼

Usage of the month: 0 KB [Modify](#)

SIM2 Threshold: ☐

* Threshold: GB ▼

Monthly Reset Day: 1 ▼

Action: Notification ▼

Usage of the month: 0 KB [Modify](#)

Cancel
OK

Figure 4-2-2-c Configuring a traffic policy for cellular network access

Actions:

- Notification: record the generated traffic reaching the threshold event, and the traffic transmission is not restricted.

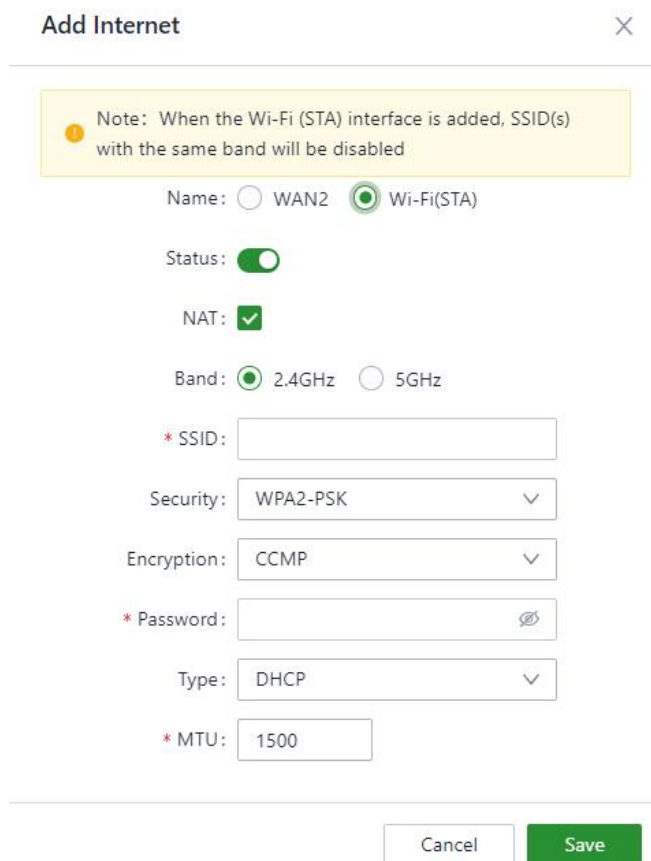
- Only Cloud Management:record the generated traffic reaching the threshold event, only keep the traffic of the cloud management device, and the access to the Internet traffic will be restricted.
- Switch SIM:record the generated traffic reaching the threshold event and trigger SIM card switching.

Notes:

- When the router is used on a private network, disable link detection on the **【 Internet 】** page. Otherwise, the cellular interface cannot work properly, because the cellular link cannot be detected.
- In some cases, you need to enter the subnet mask of the cellular interface to ensure proper functioning of ARP.
- Before removing or installing a SIM card, unplug the power cable of the router to prevent data loss or damage to the router.

4.2.3 Wireless Connection via Wi-Fi(STA)

The ER605 can connect to an AP as a wireless client (STA). To use this connection method, click **Add** on the **【 Internet 】** page, select **Wi-Fi(STA)** in the dialog box that appears, and enter the SSID and password.



The screenshot shows the 'Add Internet' dialog box with a close button (X) in the top right corner. A yellow note box at the top states: 'Note: When the Wi-Fi (STA) interface is added, SSID(s) with the same band will be disabled'. Below the note, the 'Name' field has two radio buttons: 'WAN2' (unselected) and 'Wi-Fi(STA)' (selected). The 'Status' is a toggle switch that is turned on. The 'NAT' checkbox is checked. The 'Band' has two radio buttons: '2.4GHz' (selected) and '5GHz' (unselected). The 'SSID' field is marked with a red asterisk and is empty. The 'Security' dropdown menu is set to 'WPA2-PSK'. The 'Encryption' dropdown menu is set to 'CCMP'. The 'Password' field is marked with a red asterisk and is empty, with an eye icon to its right. The 'Type' dropdown menu is set to 'DHCP'. The 'MTU' field is marked with a red asterisk and contains the value '1500'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 4-2-3 Adding the Wi-Fi(STA) interface

Notes:

- After you add the Wi-Fi(STA) interface, the SSIDs of the router on the same frequency band are disabled and cannot be enabled manually.
- After you delete the Wi-Fi(STA) interface, the SSIDs on the same frequency band can be enabled or disabled manually.

- When the Wi-Fi(STA) interface is deleted, all configuration on this interface, including the static routes, inbound and outbound rules, port forwarding, policy-based routing, and traffic shaping, is deleted.

5 Dashboard

Click **[Dashboard]** on the left pane to display the dashboard of the router, on which you can view basic device information, interface status, traffic statistics, cellular signals, and number of Wi-Fi connections.

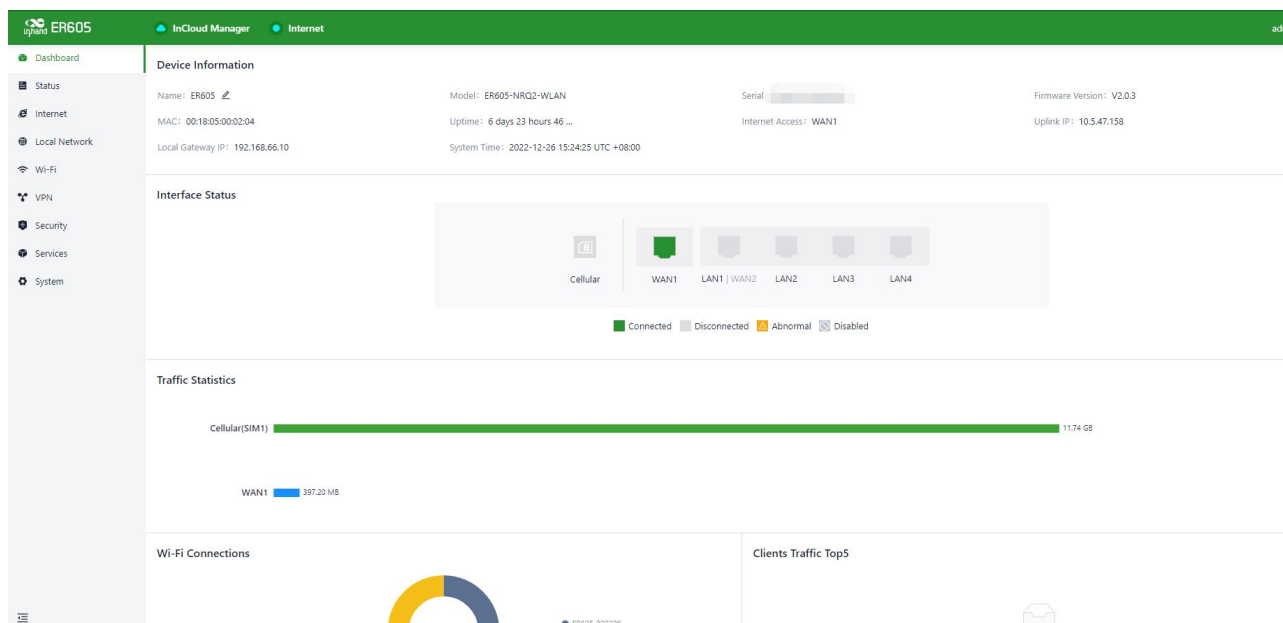


Figure 5 Dashboard

5.1 Device Information

Basic information about the router is displayed on the top of the dashboard. The network connection method and uplink interface address vary depending on the working uplink.



Figure 5-1 Device information

5.2 Interface Status

The status of each interface is displayed clearly on the dashboard. You can click any interface icon to view detailed information about the interface.

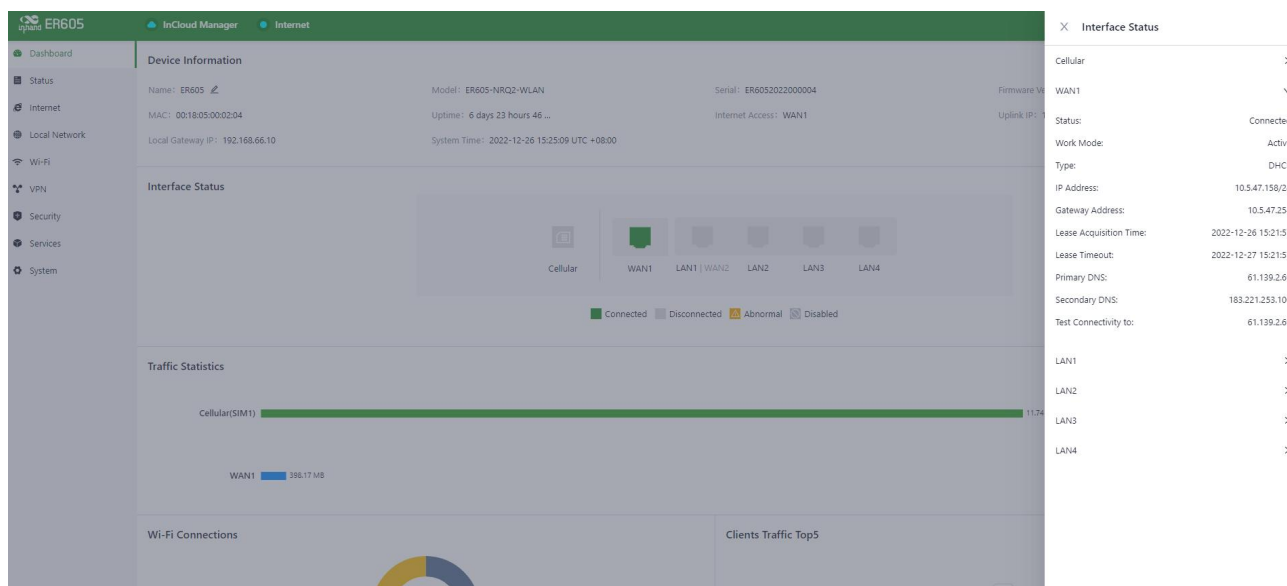


Figure 5-2 Interface status

5.3 Traffic Statistics

You can check traffic statistics collected on each uplink interface since the router is powered on. Traffic statistics are reset after a reboot of the router. To view historical traffic statistics, log in to InCloud Manager and enter the details page of the router.



Figure 5-3 Traffic statistics

5.4 Number of Wi-Fi Connections

You can view the number of SSIDs enabled on the ER605 and number of clients connected to each SSID.



Figure 5-4 Number of Wi-Fi connections

5.5 Top 5 Clients by Traffic

You can view the rankings of clients connected to the router by their traffic statistics. A maximum of five records can be displayed. When a client is disconnected from the router, its traffic statistics are cleared.

Clients Traffic Top5



Figure 5-5 Top 5 clients by traffic

6 Status

Click **Status** on the left pane to display the **【Status】** page, where you can view information about uplinks, cellular signals, clients, VPNs, events, and logs of the router.

6.1 Link Monitor

The **【Link Monitor】** module displays the health of each uplink, as well as the throughput, delay, packet loss rate, and signal strength on each uplink interface.

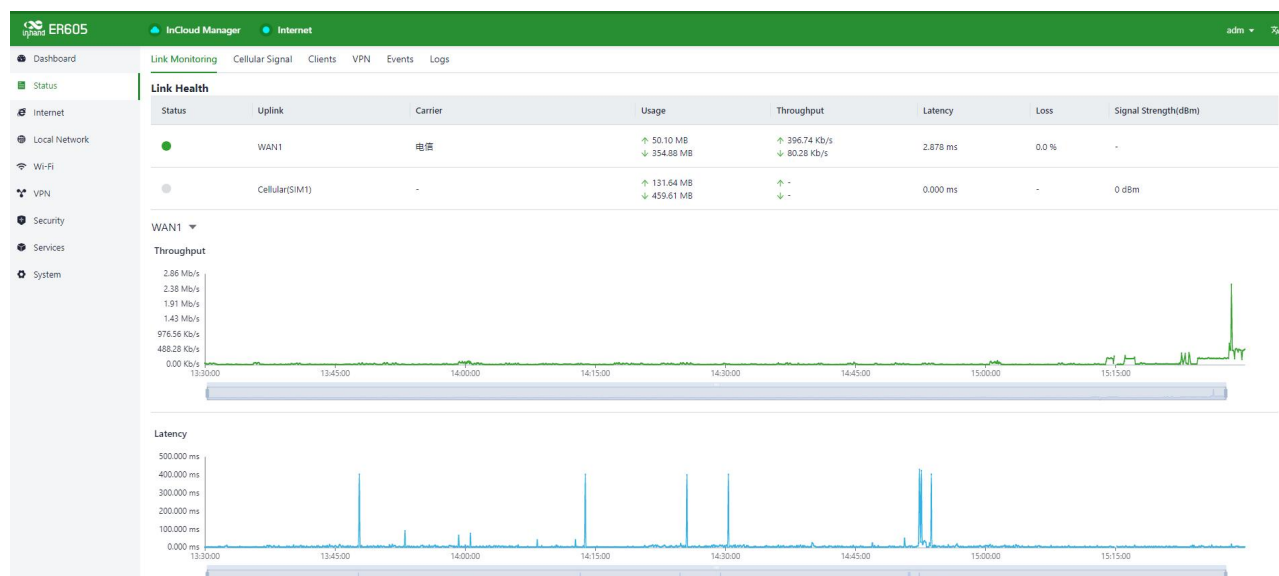


Figure 6-1 Link Monitor

6.2 Cellular Signals

The **【Cellular Signals】** module displays the SIM card signal strength on the cellular interface, as well as other parameters such as the received signal strength indication (RSSI), signal to interference plus noise ratio (SINR), and reference signal receiving power (RSRP).



Figure 6-2 Signal strength

6.3 Clients

The **【 Clients 】** module displays details about each client connected to the router, such as its name, IP address, MAC address, VLAN ID, connected subnet, traffic statistics, and online duration.

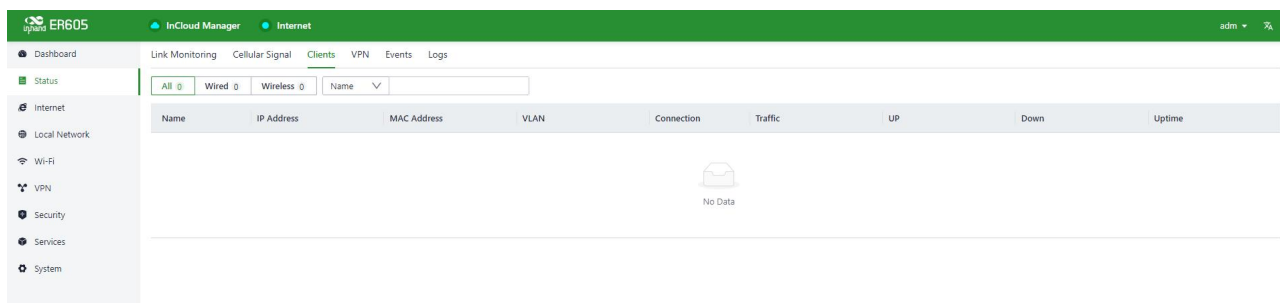


Figure 6-3 Clients

6.4 VPN

The **【 VPN 】** module displays information about IPsec VPN and L2TP VPN, such as their status, name, traffic statistics, and duration of the latest connection.

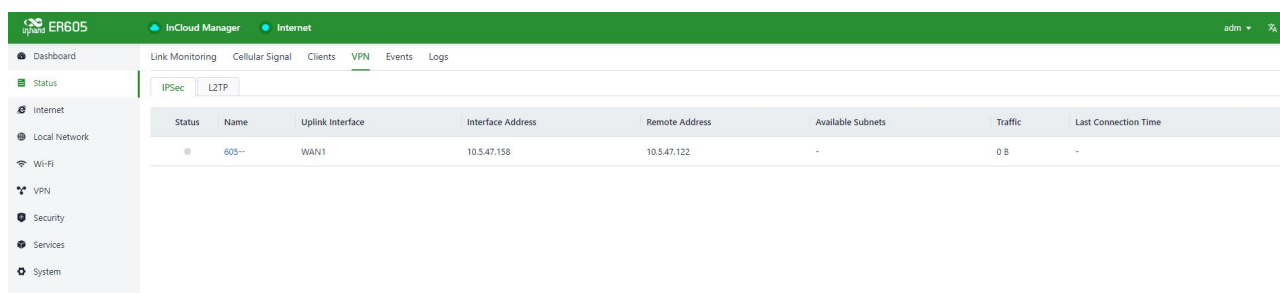


Figure 6-4 VPN

6.5 Events

The **【 Events 】** module displays the events that have occurred during operation of the router, helping you understand its running status.

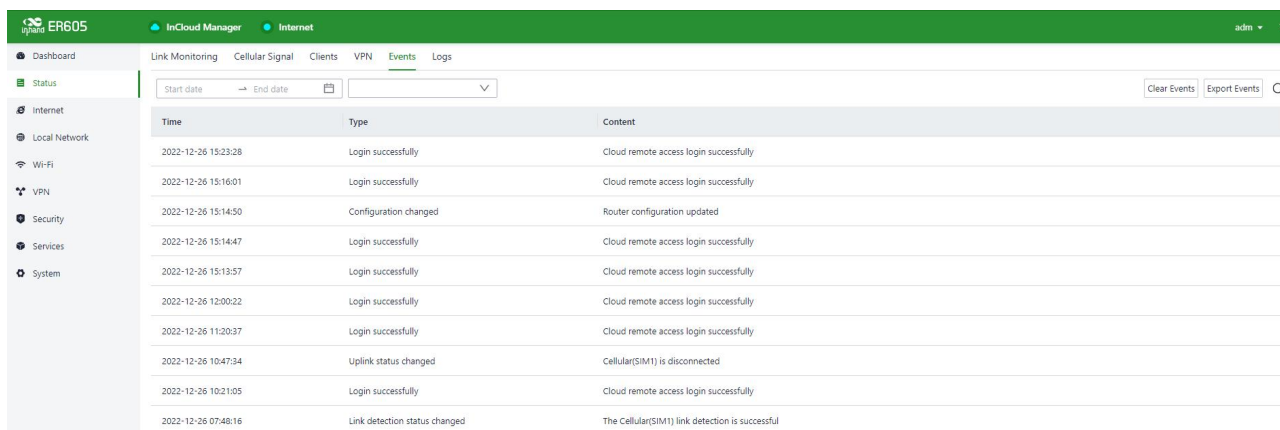


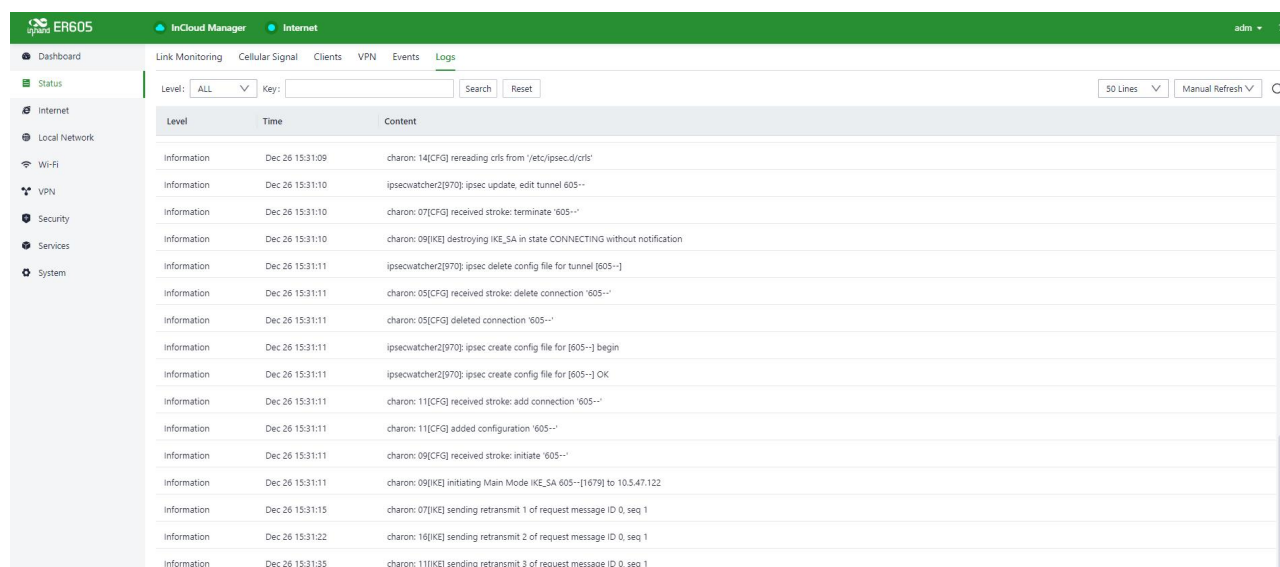
Figure 6-5 Events

The router supports the following types of events:

- Login successfully/failed
- Configuration changed
- CPU utilization is too high
- Memory utilization is too high
- VPN status changed
- Uplink status changed
- Uplink switched
- WAN2/LAN1 switched
- Detection status changed
- Cellular traffic reaches the threshold
- Reboot
- Upgrade

6.6 Logs

The **logs** module displays logs recorded during operation of the router, which can be used for troubleshooting when the router does not work properly. You can download and delete logs.



Level	Time	Content
Information	Dec 26 15:31:09	charon: 14[CFG] rereading crls from '/etc/ipsec.d/crls'
Information	Dec 26 15:31:10	ipsecwatcher2[970]: ipsec update, edit tunnel 605--
Information	Dec 26 15:31:10	charon: 07[CFG] received stroke: terminate '605--'
Information	Dec 26 15:31:10	charon: 09[IKE] destroying IKE_SA in state CONNECTING without notification
Information	Dec 26 15:31:11	ipsecwatcher2[970]: ipsec delete config file for tunnel [605--]
Information	Dec 26 15:31:11	charon: 05[CFG] received stroke: delete connection '605--'
Information	Dec 26 15:31:11	charon: 05[CFG] deleted connection '605--'
Information	Dec 26 15:31:11	ipsecwatcher2[970]: ipsec create config file for [605--] begin
Information	Dec 26 15:31:11	ipsecwatcher2[970]: ipsec create config file for [605--] OK
Information	Dec 26 15:31:11	charon: 11[CFG] received stroke: add connection '605--'
Information	Dec 26 15:31:11	charon: 11[CFG] added configuration '605--'
Information	Dec 26 15:31:11	charon: 09[CFG] received stroke: initiate '605--'
Information	Dec 26 15:31:11	charon: 09[IKE] initiating Main Mode IKE_SA 605--[1679] to 10.5.47.122
Information	Dec 26 15:31:15	charon: 07[IKE] sending retransmit 1 of request message ID 0, seq 1
Information	Dec 26 15:31:22	charon: 16[IKE] sending retransmit 2 of request message ID 0, seq 1
Information	Dec 26 15:31:35	charon: 11[IKE] sending retransmit 3 of request message ID 0, seq 1

Figure 6-6 Logs

- **Clear Logs:** clear running logs of the router.
- **Download Logs:** download running logs of the router.
- **Download Diagnostic Logs:** download log information for troubleshooting, it contains system running logs, device information, and device configuration.

7 Internet

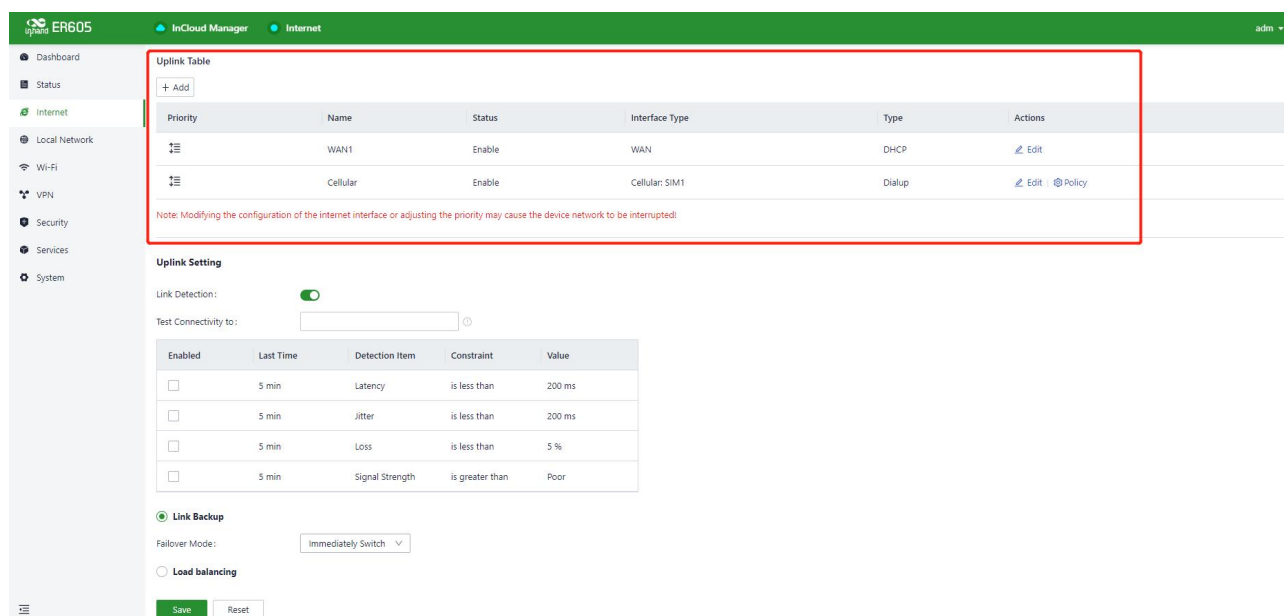
On the **Internet** page, you can set parameters for the uplink interfaces and specify a multi-link work mode.

Notes:

- Exercise caution when changing settings on the **Internet** page, as doing so may cause an interruption of the network connection.

7.1 Uplink Table

On the uplink table, you can edit WAN1 and Cellular, and add, edit, or delete WAN2 and Wi-Fi(STA). For details, see section 4.2 [Internet Connection](#). You can drag icons in the **Priority** column to reprioritize the interfaces.



The screenshot shows the InHand ER605 Internet configuration page. The left sidebar contains navigation options: Dashboard, Status, Internet (selected), Local Network, Wi-Fi, VPN, Security, Services, and System. The main content area is titled 'Internet' and contains two sections: 'Uplink Table' and 'Uplink Setting'.

The 'Uplink Table' section is highlighted with a red box. It contains a table with the following data:

Priority	Name	Status	Interface Type	Type	Actions
1	WAN1	Enable	WAN	DHCP	Edit
2	Cellular	Enable	Cellular: SIM1	Dialup	Edit Policy

Below the table, a note states: 'Note: Modifying the configuration of the internet interface or adjusting the priority may cause the device network to be interrupted!'

The 'Uplink Setting' section is located below the table. It includes a 'Link Detection' toggle switch (currently on), a 'Test Connectivity to:' dropdown menu, and a table with the following data:

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	Poor

Below this table, there is a 'Link Backup' section with a 'Failover Mode' dropdown menu (currently set to 'Immediately Switch') and a 'Load balancing' radio button. At the bottom of the 'Uplink Setting' section are 'Save' and 'Reset' buttons.

Figure 7-1 Uplink list

7.2 Uplink Settings

On the **【Internet】** page, you can configure link detection and set parameters for the uplink interfaces.

Uplink Setting

Link Detection:



Test Connectivity to:

 ⓘ

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	Poor

☒ Link Backup

Failover Mode:

Immediately Switch ▾

☐ Load balancing

Figure 7-2 Uplink settings

- By default, link detection is enabled. In the private network environment, please manually configure the address that can be detected or disable the link detection function to prevent the cellular interface from working normally. When this function is disabled, the **Status** page does not display the transmission latency, jitter, packet loss rate, or signal strength on each uplink interface.
- If the link detection address is left empty, the system detects the primary dns server address obtained by each interface. When the IP address of the link detection is filled in, all uplink use this address as the detection address
- When the router works in link backup mode, you can enable the items to be detected. The router then monitors these items and triggers a link switch when any item exceeds the threshold. If no item is enabled, link switch is only triggered based on priority and connectivity of the links.
- When the router works in load balancing mode, all the links forward traffic on a per packet basis.

8 Local Network

On the [**Local Network**] page, you can add local subnets and assign them to clients connected to the router through the LAN interfaces or SSIDs.

8.1 Passthrough Settings

Through this function, the router's uplink interface address can be transparently transmitted to the client device for use.

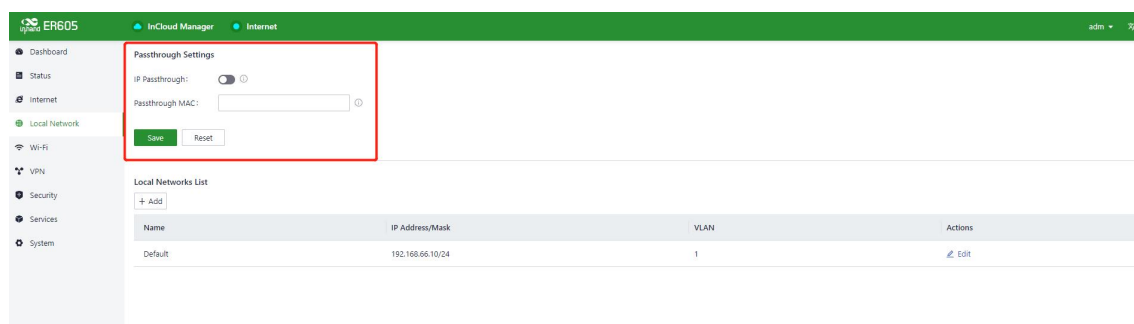


Figure 8-1 Passthrough Settings

Note:

- After the IP Passthrough mode is enabled, only one client can access the Internet. The following functions will not work:

Static routing, VPN, Port Forwarding, Policy-Based Routing, SD-WAN Overlay, Connecor.

- You can still access the router via the IP address of the default subnet.

8.2 Local Network List

Click **Add** or **Edit** to add a local network or edit an existing local network.

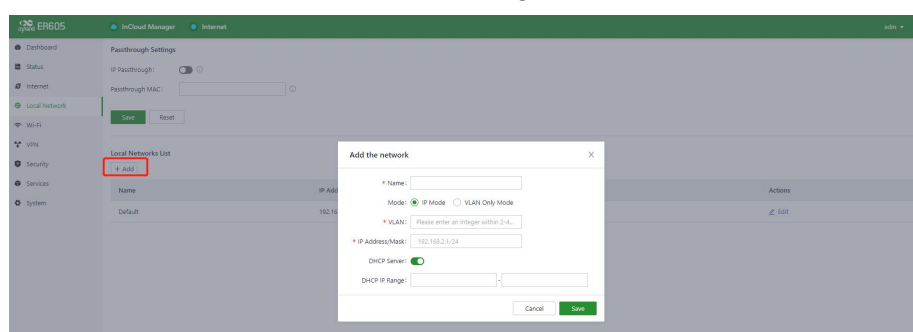


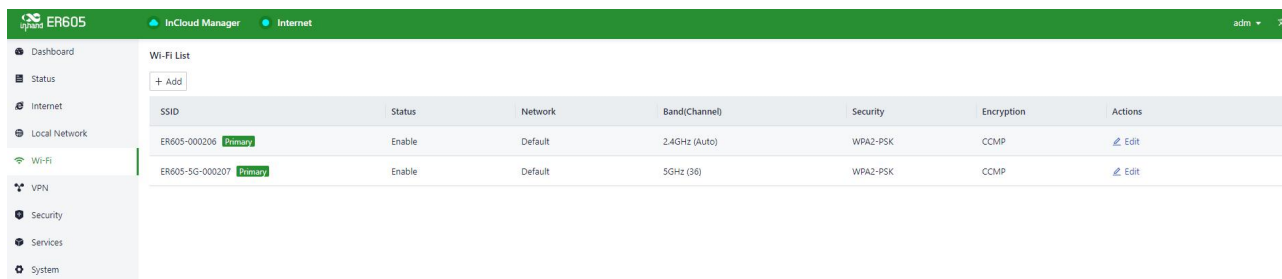
Figure 8-2 Adding a local network

Notes:

- The default local network cannot be removed. You can only change its IP address/mask, and DHCP server configuration.
- After a local network is added, its mode cannot be changed.
- The VLAN Only mode is used for transparent transmission of Layer 2 protocol packets. Therefore, you do not need to set the IP address/mask and DHCP Server for this mode.

9 Wi-Fi

The ER605 can serve as an AP to provide multiple SSIDs for wireless network access. You can define SSIDs for different purposes and set parameters for these SSIDs.



SSID	Status	Network	Band(Channel)	Security	Encryption	Actions
ER605-000206 Primary	Enable	Default	2.4GHz (Auto)	WPA2-PSK	CCMP	Edit
ER605-5G-000207 Primary	Enable	Default	5GHz (36)	WPA2-PSK	CCMP	Edit

Figure 9-1 Wi-Fi list

Click **Add** or **Edit** to add an SSID or edit an existing SSID.

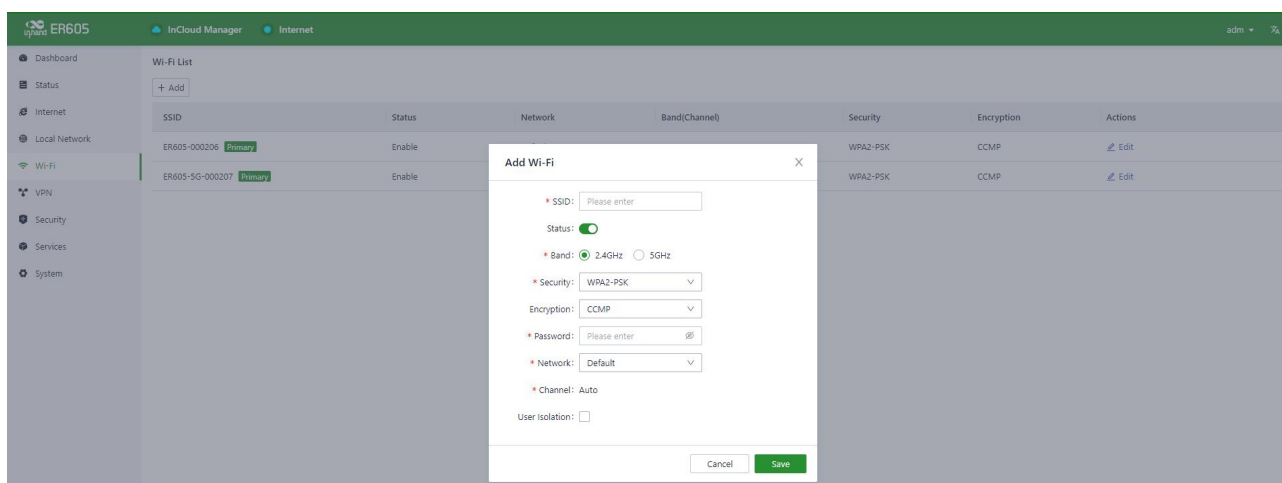


Figure 9-2 Editing an SSID

- The router has two default primary SSIDs, one for the 2.4 GHz band and one for the 5 GHz band. You cannot change the bands of the two SSIDs or delete the SSIDs.
- After an SSID is added, its band cannot be changed, and its channels are automatically synchronized with channels of the corresponding primary SSID.
- If you have added the Wi-Fi(STA) interface on the **Internet** page, none of SSIDs on the same band as the Wi-Fi (STA) interface can be enabled, until this interface is removed.

10 VPN

A virtual private network (VPN) is a private network established on a public network for encrypted communication. A VPN gateway encrypts data packets and translates destination IP addresses of data packets to implement remote access. The VPN service can be provided through a server, hardware client, or software client.

10.1 IPSec VPN

IPSec VPN is an open network security protocol suite developed by IETF to ensure secure data transmission over the Internet through source authentication, data encryption, data integrity check, and anti-replay at the IP layer. This protocol suite lowers the risks of data leakage and interception, and ensures the data integrity and privacy, thus protecting the security of communication.

Choose **VPN > IPSec VPN**, and click **Add** to add an **[IPSec VPN.]**

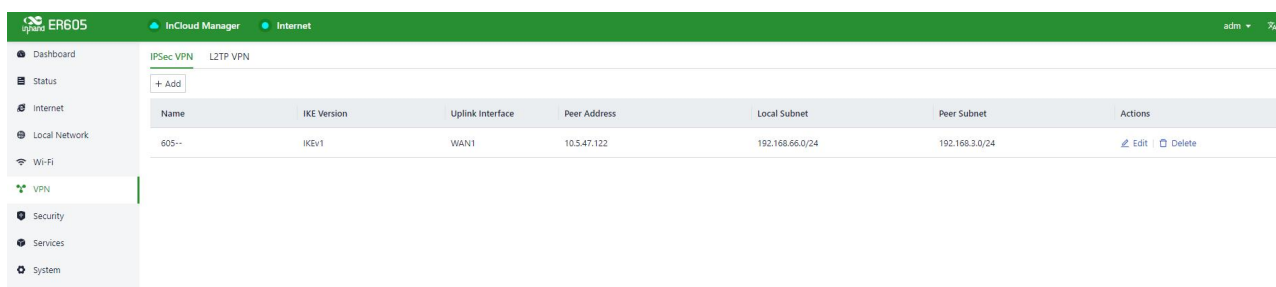


Figure 10-1-1 Adding an IPSec VPN

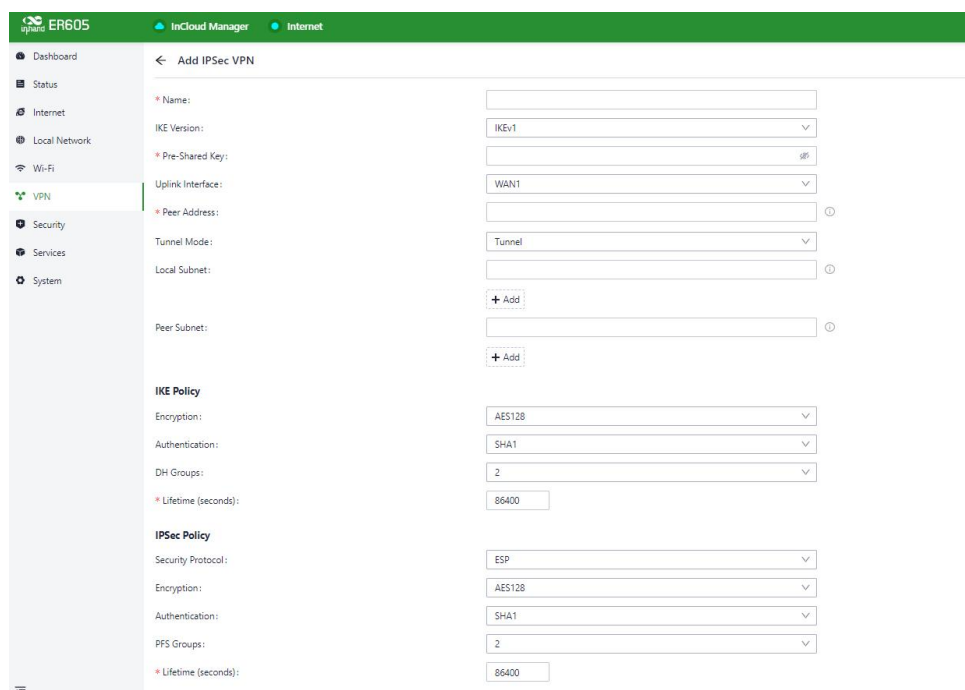


Figure 10-1-2 Setting the new IPSec VPN

After the IPSec VPN configuration is completed on both sides, an IPSec VPN tunnel is established. To check the status of this tunnel, click **Status** on the left pane, and then click the **VPN** tab. The following parameters must be set:

- Name:** specifies the name of the IPSec VPN created on the router, which is used for local VPN management.

- **IKE Version:** specifies the version of the Internet Key Exchange (IKE) protocol used on the router, which can be IKEv1 or IKEv2.
- **Pre-Shared Key:** specifies the authentication key for IKE negotiation, which must be consistent on both sides.
- **Internet Interface:** specifies the local uplink interface used to establish the IPsec VPN tunnel.
- **Tunnel Mode:** specifies the IP packet encapsulation mode on the IPsec VPN tunnel, which can be tunnel mode or transfer mode.
- **Peer Address:** specifies the IP address of the peer device that will establish a tunnel with the ER605.

Notes:

When two ER series routers establish an IPsec VPN tunnel, the one using a public IP address acts as the server by default. On the IPsec server, the peer IP address must be set to 0.0.0.0. On the IPsec client, the peer IP address must be set to the public IP address of the server's interface used to establish the tunnel.

- **Local Subnet:** specifies the IP address segment of the traffic to be sent out by the ER605 through the IPsec VPN tunnel.
- **Peer Subnet:** specifies the IP address segment used for communication on the other end of the IPsec VPN tunnel.
- **IKE Policy:** allows you to set IKE parameters.
 - **Encryption:** specifies the encryption algorithm for IKE.
 - **Authentication:** specifies the authentication algorithm for IKE.
 - **DH Groups:** specifies the DH key exchange mode.
 - **Lifetime:** specifies the lifetime of the IKE security association (SA). The default value is 86400 seconds.
- **IPsec Policy:** allows you to set IPsec parameters.
 - **Security Protocol:** specifies the security protocol used for the External Router Protocol (ERP).
 - **Encryption:** specifies the encryption algorithm for the Encapsulating Security Payload (ESP) protocol.
 - **Authentication:** specifies the authentication algorithm for ESP.
 - **PFS Groups:** specifies the Perfect Forward Secrecy (PFS) mode, which improves the communication security through an additional key exchange in Phase 2 of negotiation.
 - **Lifetime:** specifies the lifetime of the IPsec SA. The default value is 86400 seconds.

10.2 L2TP VPN

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol for virtual private dial networks (VPDNs). This protocol establishes a tunnel from a remote site to the headquarters of an enterprise over a public switched telephone network (PSTN) or integrated services digital network (ISDN) through Point-to-Point Protocol (PPP) negotiation. This tunnel allows remote users to connect to the intranet of the enterprise in a secure way.

10.2.1 Client

The ER605 can serve as an L2TP client to establish a tunnel to a remote L2TP server. Choose **L2TP VPN > Client** on the **【VPN】** page, and click **Add** to add an L2TP client.

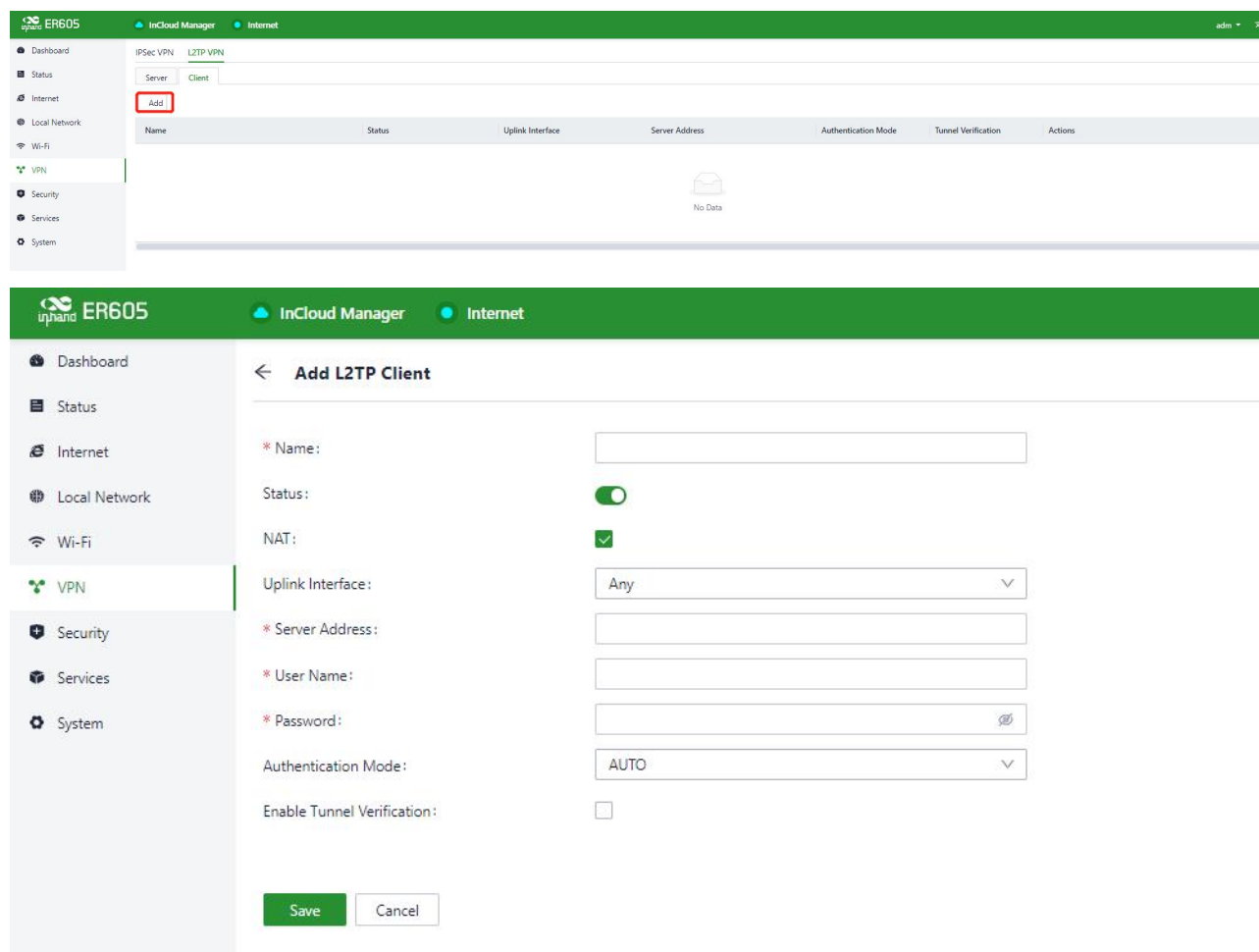


Figure 10-2-1-a/b Adding an L2TP client

- **Name:** specifies the local identifier of the L2TP client.
- **Status:** enables or disables L2TP tunneling on the client.
- **NAT:** enables or disables network address translation (NAT) for packets forwarded by the router for the clients connected to it.
- **Uplink Interface:** specifies the uplink interface used to establish a tunnel from the L2TP client to the server.
- **Server Address:** specifies the IP address used by the remote L2TP server to communicate with the L2TP client.
- **User Name/Password:** specifies the user name and password for L2TP negotiation, which must be consistent on both ends of the tunnel.
- **Authentication:** specifies the authentication mode for the L2TP tunnel.
- **Enable Tunnel Authentication:** When this option is selected, make sure both ends of the tunnel are configured with the same server name and verification key.

10.2.2 Server

Generally, an L2TP server is deployed at the headquarters of an enterprise to provide remote access for employees on the move or in branches. On the **VPN** page, choose **L2TP VPN > Server** to display the L2TP server configuration page.

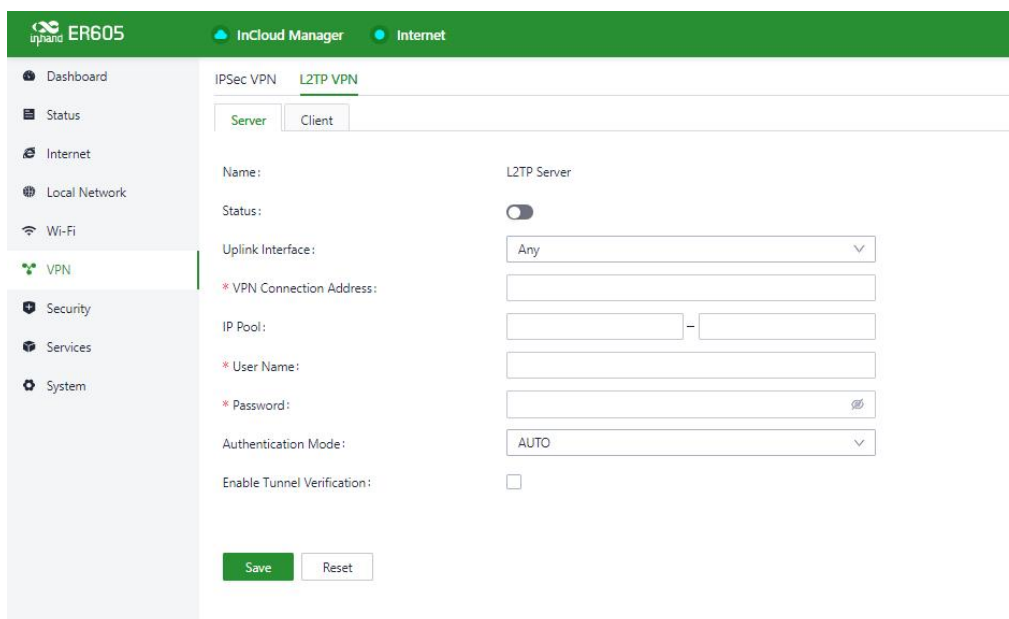


Figure 10-2-2 L2TP server configuration

- **Name:** displays the name of the L2TP server, which cannot be changed.
- **Status:** enables or disables the L2TP server function. This function is disabled by default.
- **Uplink Interface:** specifies the uplink interface used to establish a tunnel from the L2TP server.
- **VPN Address:** specifies the gateway address for the L2TP client. The gateway assigns an IP address to the L2TP client from the specified IP address pool.
- **Address Pool:** specifies the IP address range for the L2TP client.
- **User Name/Password:** specifies the user name and password for L2TP negotiation, which must be consistent on both ends of the tunnel.
- **Authentication:** specifies the authentication mode for the L2TP tunnel.
- **Enable Tunnel Authentication:** when this option is selected, make sure both ends of the tunnel are configured with the same user name and password.

11 Security

On the **Security** page, you can configure advanced security features, including firewall, policy-based routing, and traffic shaping.

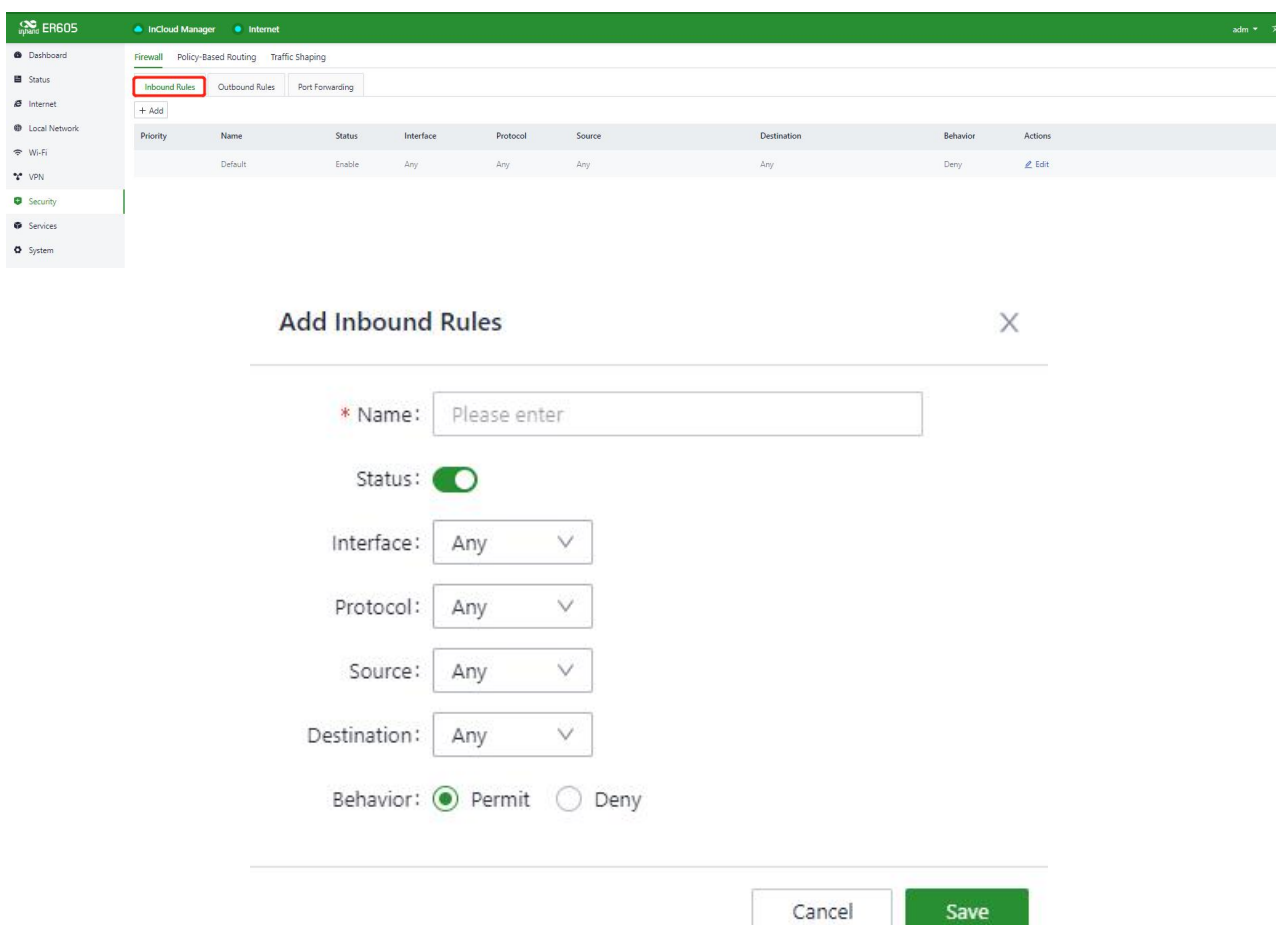
11.1 Firewall

You can set inbound and outbound rules and port forwarding for the firewall.

11.1.1 Inbound and Outbound Rules

You can set inbound and outbound rules to control inbound and outbound traffic on an interface. For example, if a large number of attacks are initiated from an IP address, you can set an inbound rule on the firewall to restrict traffic sent from this IP address.

If you want to prevent some internal users from accessing the Internet, set an outbound rule to restrict outbound traffic sent from these users. Inbound and outbound rules contain the same parameters and differ only in default settings. The following figure shows an example of adding an inbound rule.



Priority	Name	Status	Interface	Protocol	Source	Destination	Behavior	Actions
	Default	Enable	Any	Any	Any	Any	Deny	Edit

Figure 11-1-1-a/b Adding an inbound rule

- **Name:** specifies the local identifier of the inbound rule.
- **Status:** enables or disables the rule.
- **Interface:** specifies the traffic forwarding interface. For an outbound rule, select the interface from which traffic is sent out. For an inbound rule, select the interface on which traffic is received.

- **Protocol:** specifies the protocol type of packets to be matched. Options are **Any**, **TCP**, **UDP**, **ICMP**, and **Custom**.
 - **Source:** specifies the source IP address of packets to be matched. You can enter an IP address or retain the default option **Any**.
 - **Destination:** specifies the destination IP address of packets to be matched. You can enter an IP address or retain the default option **Any**.
 - **Behavior:** specifies the action taken for packets matching the rule. Options are **Permit** and **Deny**.
 - Inbound rule: controls external traffic received by the router. By default, all external traffic is denied.
 - Outbound rule: controls traffic sent out through the router. By default, all outbound traffic is permitted.
- You can reprioritize inbound and outbound rules on the rule list.

11.1.2 Port Forwarding

After a port forwarding rule is configured on an interface of the router, the router forwards data traffic arriving at this interface to the specified port on the target internal client. In this way, services deployed on the intranet are available for external users. The port forwarding feature allows the router to forward packets of different ports to different private IP addresses and ports, so that the same public IP address can be used to access multiple servers. For example, if external users need to access the service with port 1024 on the client with the IP address 192.168.2.10, you can map this port to port 1024 on WAN1. Then, external users can access data of this service on the client by entering https://IP address of WAN1:1024 in the address box of their web browser.

The screenshot displays the InHand ER605 web management interface. The left sidebar contains navigation links: Dashboard, Status, Internet, Local Network, Wi-Fi, VPN, Security, Services, and System. The 'Internet' section is active, showing sub-tabs for Firewall, Policy-Based Routing, and Traffic Shaping. Under 'Firewall', there are links for Inbound Rules, Outbound Rules, and Port Forwarding. The 'Port Forwarding' link is highlighted, and a '+ Add' button is visible. Below this is a table with columns: Name, Status, Interface, Public Port, Protocol, Local Address, Local Port, and Actions. The table currently shows 'No Data'. A modal window titled 'Add Port Forwarding' is open, featuring the following fields:

- Name:** A text input field.
- Status:** A toggle switch, currently turned on.
- Interface:** A dropdown menu with 'Any' selected.
- Protocol:** A dropdown menu with 'TCP&UDP' selected.
- Public Port:** A text input field with an information icon.
- Local Address:** A text input field with an information icon.
- Local Port:** A text input field with an information icon.

 At the bottom of the modal are 'Cancel' and 'Save' buttons.

Figure 11-1-2-a/b Adding a port forwarding rule

- **Name:** specifies the local identifier of the port forwarding rule.
- **Status:** enables or disables the port forwarding rule.
- **Interface:** specifies the uplink interface that provides port mapping for internal clients. This interface must have a public IP address.
- **Protocol:** specifies the protocol type to which port mapping is applied. Options are **TCP**, **UDP**, and **TCP&UDP**.
- **Public Port:** specifies the protocol port on the uplink interface to be mapped to the protocol port on the internal client. The value range is the same as that of **Local Port**.
- **Local Address:** specifies the IP address of the target client that external users need to access.
- **Local Port:** specifies the protocol port that external users need to access on the target client. The value range is the same as that of **Public Port**.

11.2 Policy-based Routing

Policy-based routing (PBR) allows the router to forward different data flows through different links based on the configured policies. This feature enables flexible route selection and control, thus improving the link utilization and reducing operational cost of the enterprise. Choose **Security > Policy-based Routing** and click **Add** to add a PBR rule.

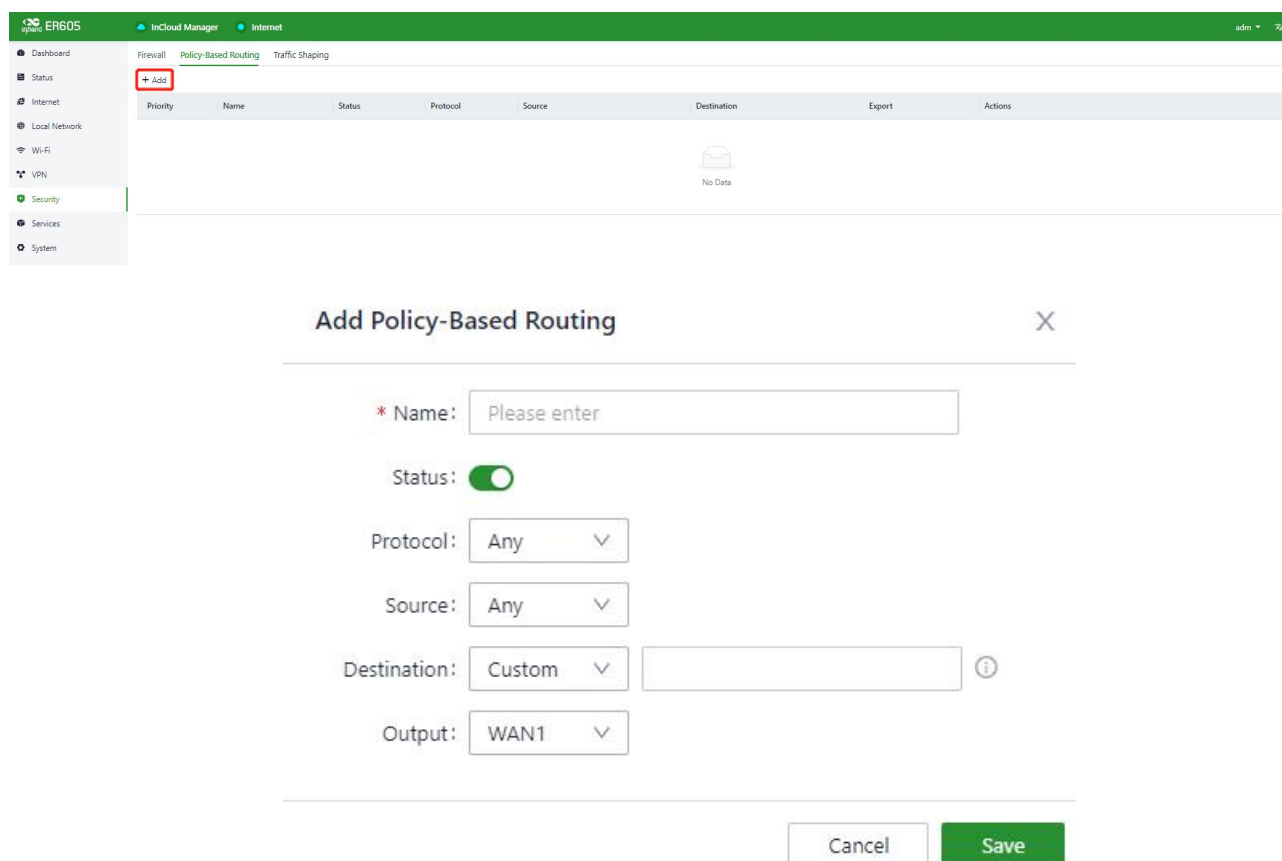


Figure 11-2-a/b Adding a PBR entry

Notes:

- The source and destination addresses of the PBR entry cannot be set to **Any** at the same time.

11.3 Traffic Shaping

To optimize your network, you can create shaping policies to apply per-user controls on a per-protocol basis. This allows you to reduce bandwidth for recreational traffic, and to prioritize bandwidth for your business-critical enterprise traffics. Choose **Security > Traffic Shaping** and click **Edit** to modify the bandwidth of the uplink.

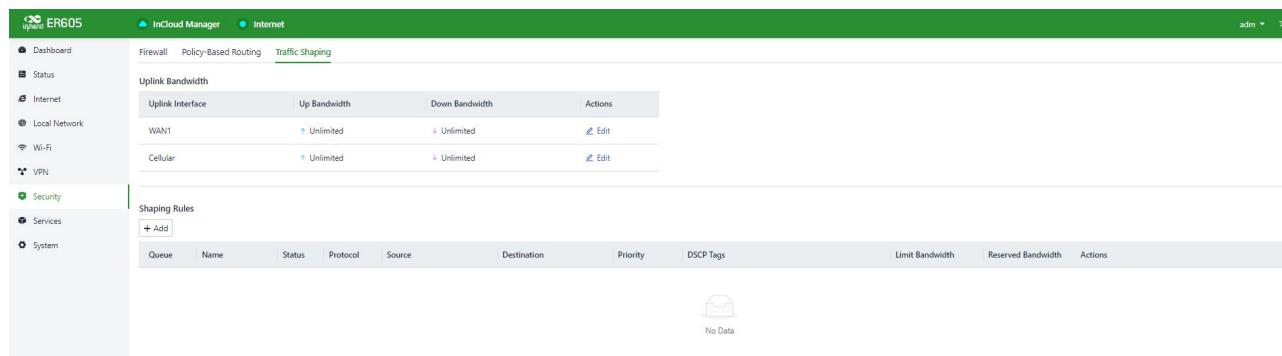


Figure 11-3-a Editing uplink bandwidth

Click **Add** to create a new rule to add a traffic shaping rule. Traffic shaping policies consist of a series of rules that are performed in the order in which they appear in the policy, similar to custom firewall rules. There are two main components to each rule: the type of traffic to be limited or shaped (rule definition), and how that traffic should be limited or shaped (rule actions).

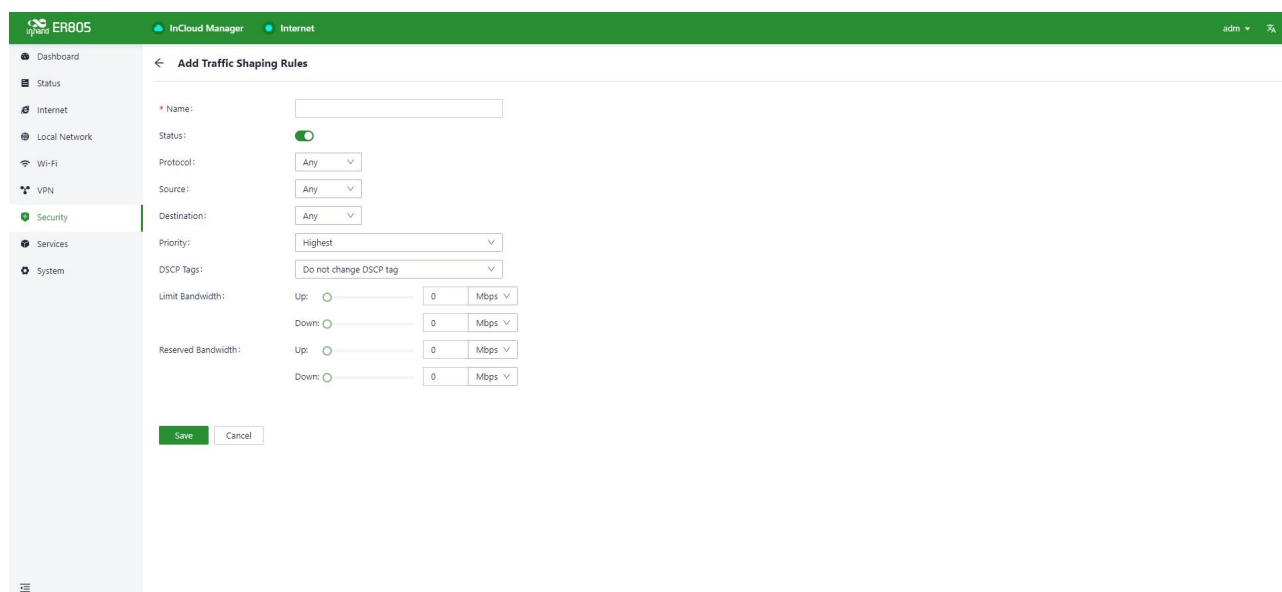


Figure 11-3-b Adding traffic shaping rule

Note:

- Traffic forwarding priority for unmatched rules is medium.
- When the bandwidth is set to 0, the rate of traffic is not limited.
- The value of guaranteed bandwidth should not be greater than the limit bandwidth.

12 Services

12.1 Interface Management

In the **【Interface Management】** module, you can specify the local subnets allowed to communicate with external networks, and set a rate limit for the interface.

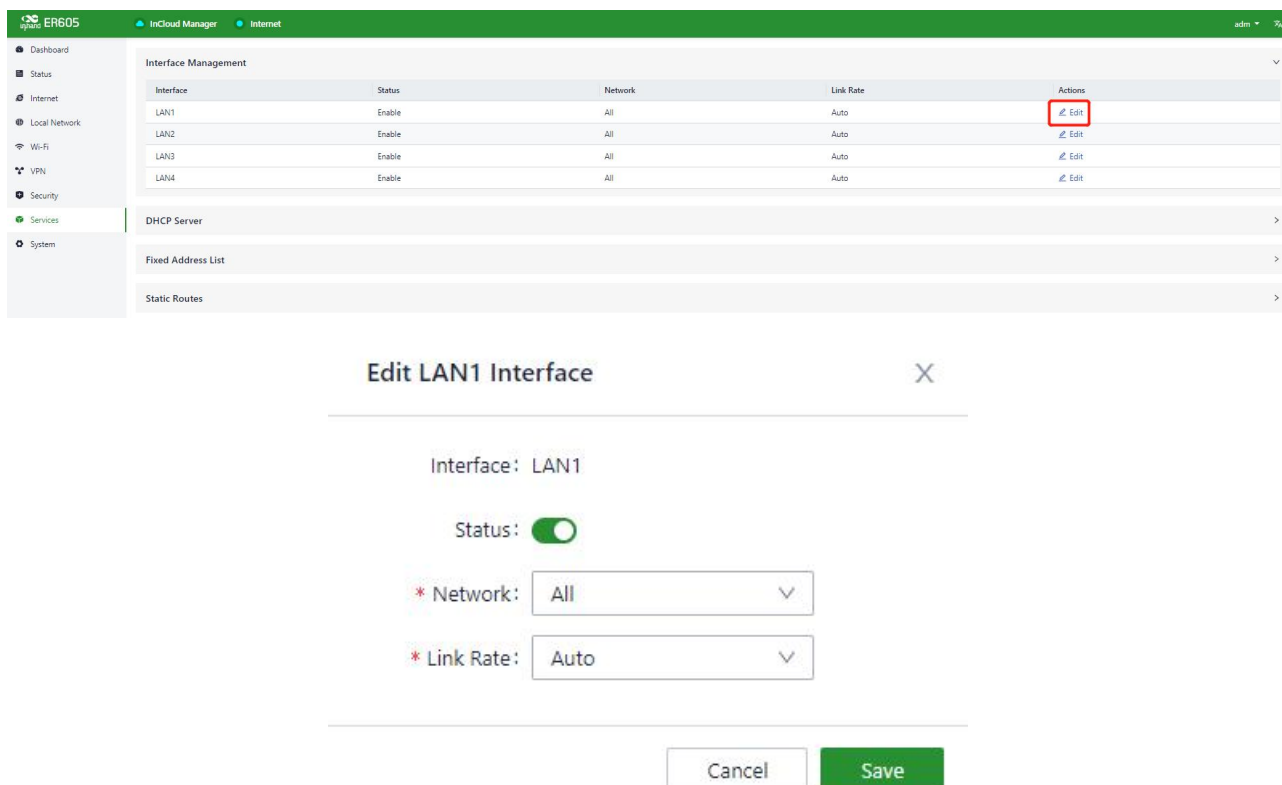
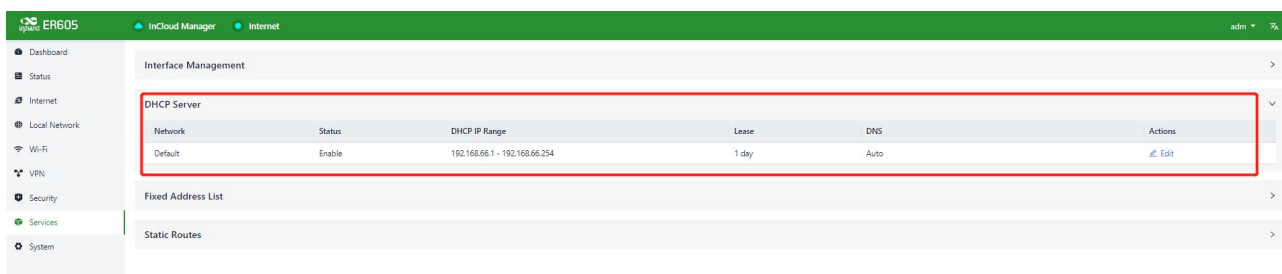


Figure 12-1-a/b Editing a LAN interface

12.2 DHCP Server

DHCP implements dynamic IP address allocation in a client/server model. The client sends a configuration request to the server, and the server replies with an IP address assigned to the client.



Edit DHCP Server
✕

Network: Default
10.5.22.1/24

Status: ☒

* DHCP IP Range: -

* Lease:

* DNS:

Cancel
Save

Figure 12-2-a/b Editing a DHCP server

- DHCP servers are created on the router based on local networks connected to the router. When a local network is removed, the DHCP server for this network is also removed.
- The DHCP server function is available only for local networks in IP mode. It does not take effect for networks in VLAN Only mode.

12.3 Fixed Address List

You can assign fixed IP addresses to clients connected to the router based on their MAC addresses.

Figure 12-3 Adding a fixed IP-MAC address mapping

- The IP address assigned must be in the IP address range of the local network in IP mode.
- When a local network is removed, all the address mapping entries in the IP address range of the network are deleted.

12.4 Static Routes

You can configure static routes to direct data traffic to specified routes and interfaces. The static route list displays only manually created routes and does not include the routes generated automatically on uplink interfaces.

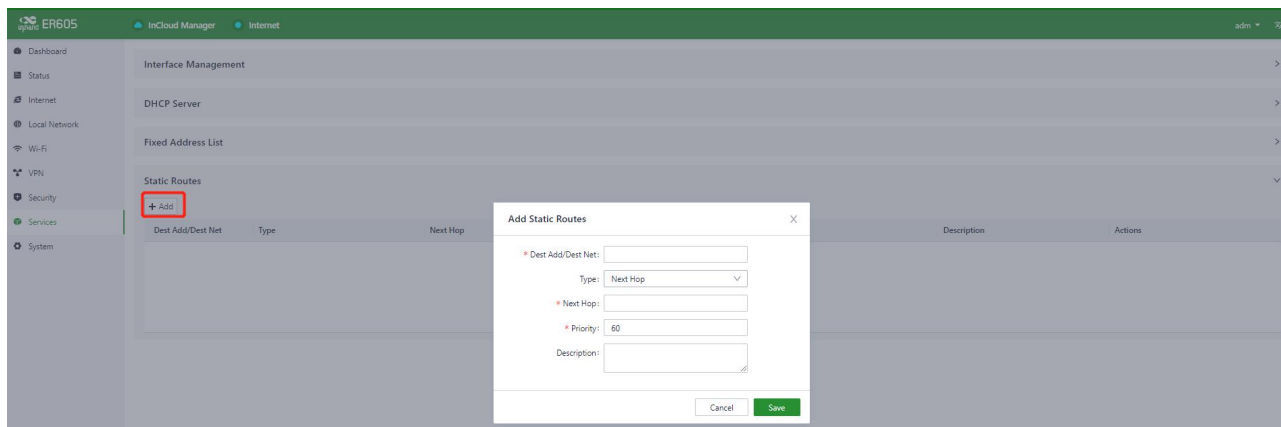


Figure 12-4 Adding a static route

- Static routes to the same destination IP address or network cannot have the same next-hop address, outbound interface, or preference.
- When WAN2, Wi-Fi(STA), or the interface serving as an L2TP VPN client is removed, static routes using this interface as the outbound interface are also deleted.

13 System

On the **System** page, you can configure various functions, including cloud management, remote access control, clock, device options, configuration management, alarms, tools, and log server.

13.1 Adm Management

The initial user name for the router is **adm** and the initial password is **123456**. Change the password to enhance security. Click **adm** in the upper right corner of the page, and select **Change Password**.

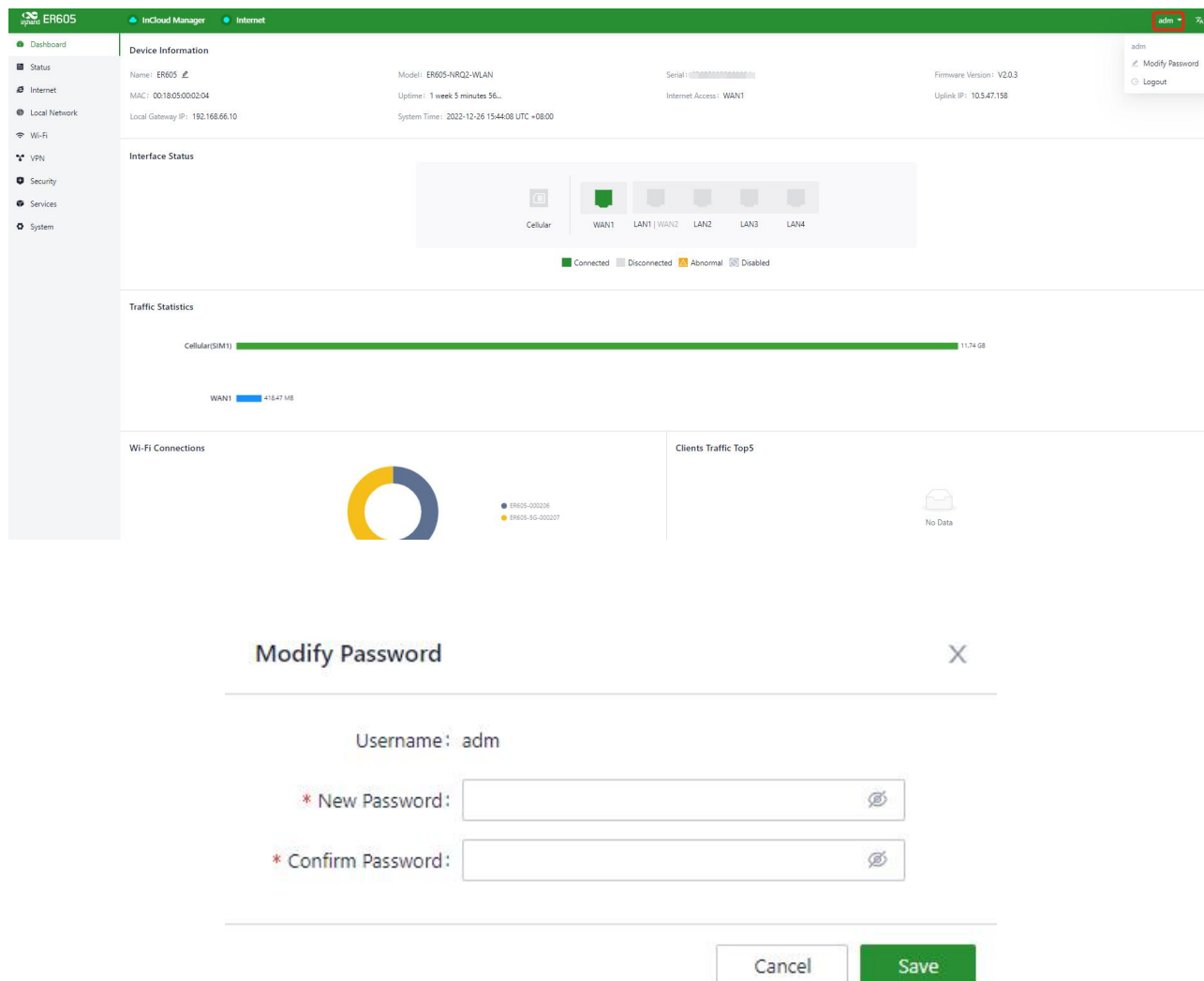


Figure 13-1-a/b Changing the password of adm

13.2 Cloud Management

InCloud Manager (star.inhandcloud.com) is a cloud platform developed by InHand to help enterprises accelerate network deployment, simplify network O&M, and improve service experience. This platform provides zero touch deployment, intelligent O&M, and security features to create good service experience for users. When your devices are connected to the cloud platform, you can log in to the platform to manage the devices remotely, perform batch configuration, and monitor traffic on these devices.

In the **【 Cloud Management 】** module, you can select the cloud platform you want to visit. When the cloud platform and cloud management service are no longer needed, you can disable the cloud service

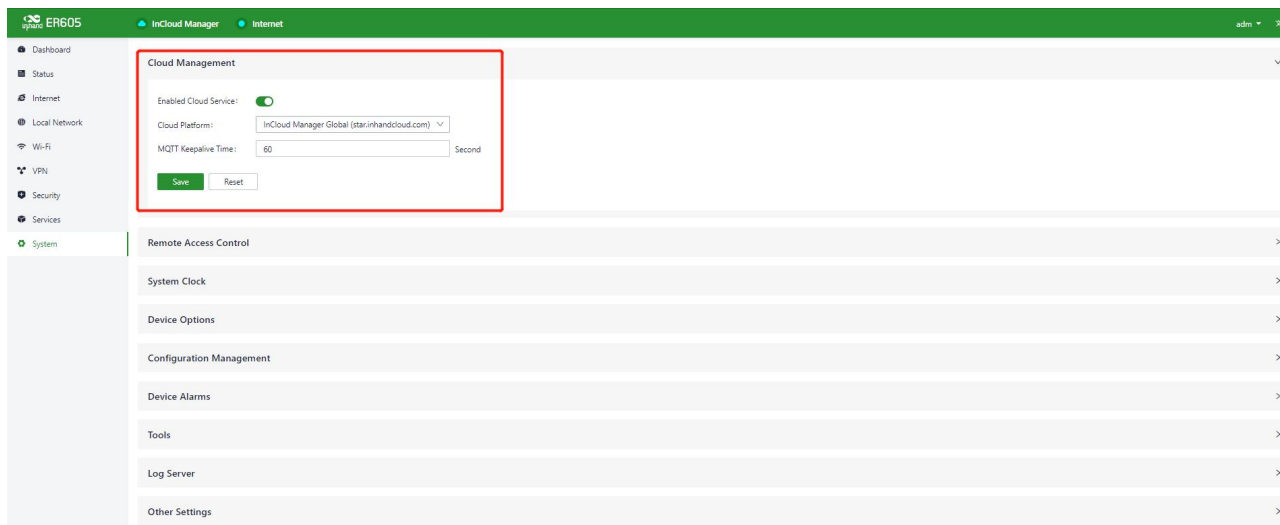


Figure 13-2 Cloud management

Notes:

- The ER605 connects to the InCloud Manager platform automatically. If you do not want to use this platform, disable the cloud service manually.

13.3 Remote Access Control

In the **【 Remote Access Control 】** module, you can determine whether to allow access to the web-based management system of the router from the Internet, and specify the allowed protocol ports.

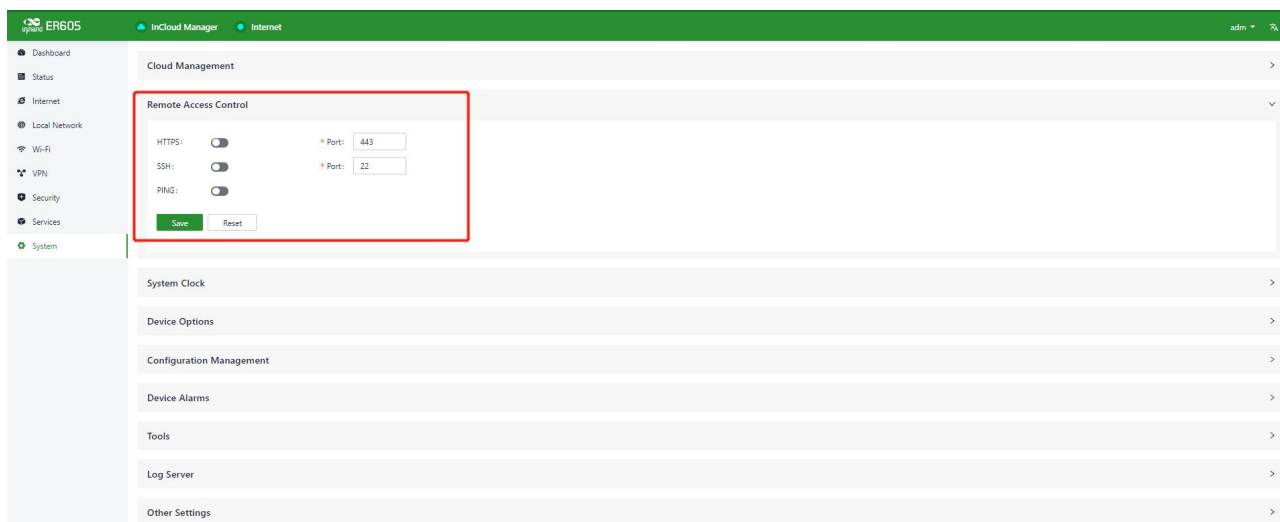


Figure 13-3 Configuring remote access control

- HTTPS:** when this service is enabled, you can access the web-based management system of the router remotely by entering the public IP address and port of its uplink interface in the address box of the web browser.
- SSH:** when this service is enabled, you can use a remote access tool, such as CRT, to log in to the web-based management system of the router by entering the public IP address and port of its uplink interface, as well as the user name and password.

- Ping: when this service is enabled, ping requests can be initiated to the IP address of the uplink interface from external networks.

Notes:

- Remote access control does not apply to LAN interfaces.
- Firewall policies do not restrict remote access.

13.4 System Clock

In the **System Clock** module, you can select a time zone for the system and enable the NTP server to synchronize time with the target NTP server.



Figure 13-4 Setting the system clock

13.5 Device Options

In them **Device Options** module, you can reboot the router, upgrade the firmware, and restore factory settings of the router.

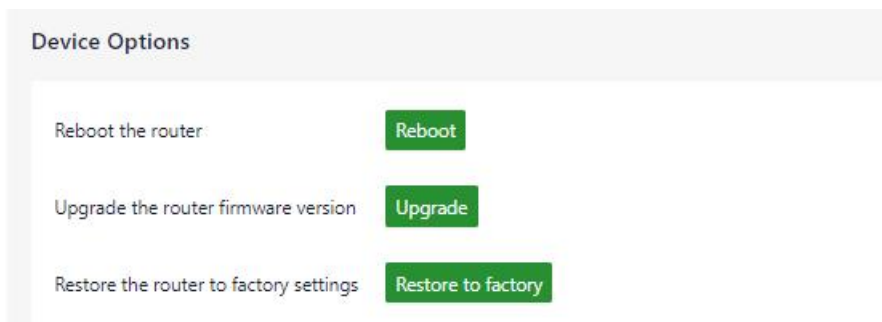


Figure 13-5 Device options

Notes:

- Before upgrading the firmware, make sure the new firmware is obtained from an official source. If a wrong firmware is loaded, the router will be unable to work.
- When the router is connected to the cloud platform, the cloud platform synchronizes the settings configured before you restore the factory settings to the router again. The router only clears historical data.

13.6 Configuration Management

You can export the configuration file of the router to your PC as a backup. Once the configuration is lost on the router, you can import the configuration file to the router to restore the configuration.

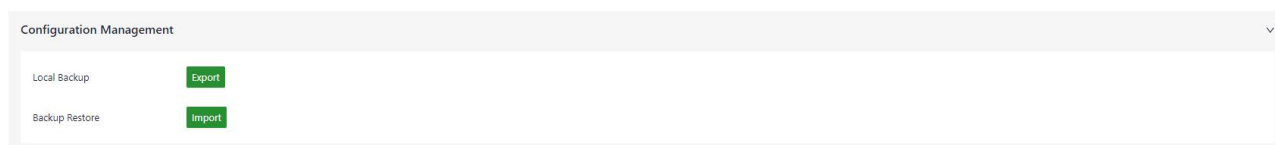


Figure 13-6 Configuration management

13.7 Alarms

If you need to monitor some events that may occur on the router, select the matching alarm events in the **Alarm Settings** module and specify an email address for receiving alarms. When an event of the specified type occurs, the router sends an email to the specified address. The unselected alarm events are recorded in logs on the router.

The router supports the following events:

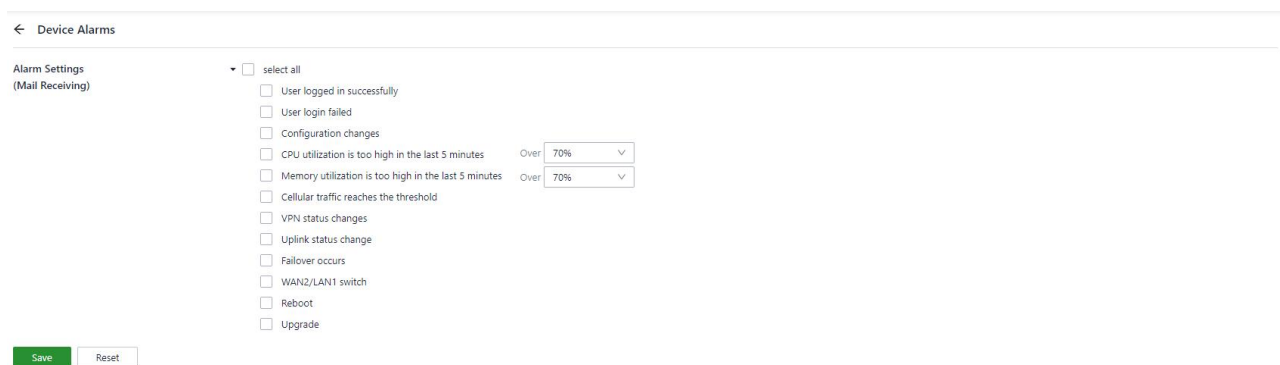


Figure 13-7-a Alarm settings

After you set the mail server address, port, user name, and password, the router uses the specified mailbox to send alarm emails. You can send a test email to check whether the mail server configuration is correct.

Receive Mail Settings

Enable: ☐

* Mail Server Address:

* Mail Server Port:

* Username:

* Password:

TLS: ☐

* Receiving Email Address:

Send a test email to:

Figure 13-7-b Mail server settings

13.8 Tools

13.8.1 Ping

The ping service is used to test the connectivity between the router and external networks through the Internet Control Message Protocol (ICMP). Enter any domain name or IP address in the **Target** field, and then click **Start** to test the connectivity with this target.

Ping

* Target:

Interface:

* Packet Size: Bytes

* Packet numbers:

```

PING 8.8.8.8 (8.8.8.8): 64 data bytes
72 bytes from 8.8.8.8: seq=0 ttl=50 time=91.376 ms
72 bytes from 8.8.8.8: seq=1 ttl=50 time=89.177 ms
72 bytes from 8.8.8.8: seq=2 ttl=50 time=90.676 ms
72 bytes from 8.8.8.8: seq=3 ttl=50 time=90.155 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 89.177/90.346/91.376 ms
  
```

Figure 13-8-1 Ping

13.8.2 Traceroute

Enter the IP address of the target host, select an interface, and then click **Start** to test the route to the destination IP address.

Traceroute

* Target:

Interface:

```

traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1 * * *
 2 * * *
 3 * * *
 4 111.9.130.241 (111.9.130.241) 28.993 ms 34.698 ms 34.048 ms
 5 223.87.26.45 (223.87.26.45) 24.967 ms 37.221 ms 35.848 ms
  
```

Figure 13-8-2 Traceroute

13.8.3 Packet Capture

You can capture data packets on a specified interface. By selecting an option from the **Output** drop-down list, you can view information about the captured data packets or export the information to your PC.

Capture

Interface: Any

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

* Time: 60 Seconds

Output: View output below

Start

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/>

Figure 13-8-3 Packet Capture

FCC STATEMENT

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE 1: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure

The equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The availability of some specific channels and/or operational frequency bands is country dependent and firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

The EUT only works at 5150~5250MHz frequency and 5725~5850MHz frequency.

IC STATEMENT

This device complies with Industry Canada license-exempt RSS standard(s): Operation is subject to the following Two conditions:

- (1) this device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3 (B)

Avis d'Industrie Canada

Le présent appareil est conforme aux CNR d'industrie Canada applicables aux appareils radio exem pts de licence L'exploitation est autorisée aux deux conditions suivantes:

- 1) l'appareil ne doit pas produire de brouillage; et
 - 2) l'utillsateur de l'appareil doit accepter brouillage radioélectrique subi meme si le brouillage est susceptible d'encompromettre le fonctionnement. mauvais fonctionnement de l'appareil.
- Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

CAN NMB-3 (B)

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.

Frequency band 5150-5250 MHz in Canada for indoor use only.