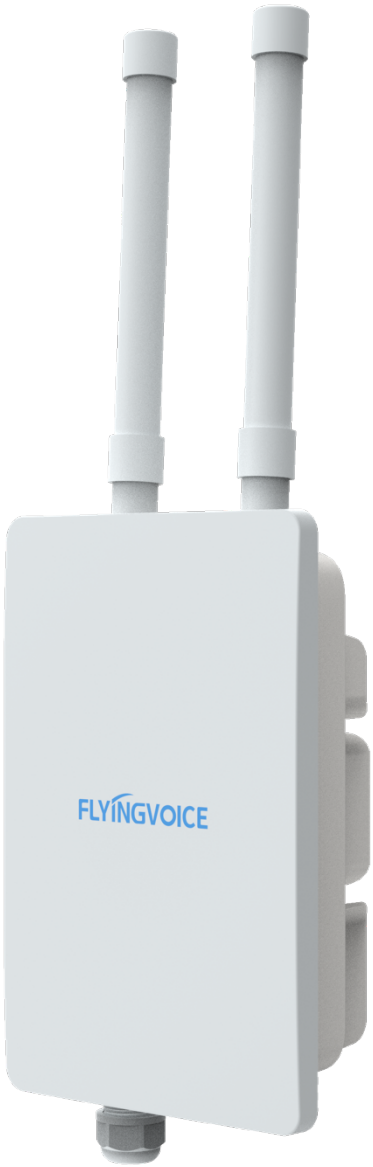
FLYINGVOICE



T5X Series CPE User Guide

T5100/T5300

Copyright

Trademark

Warranty

1. Warranty

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS GUIDE ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS GUIDE ARE BELIEVED TO BE ACCURATE AND PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF PRODUCTS.

2. Disclaimer

FLYINGVOICE NETWORK TECHNOLOGY CO., LTD. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS GUIDE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE. FLYINGVOICE Network Technology CO., LTD. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance, or use of this guide.

3. Limitation of Liability

Flyingvoice and/or its respective suppliers are not responsible for the suitability of the information contained in this document for any reason. The information is provided "as is", and Flyingvoice does not provide any warranty and is subject to change without notice. All risks other than risks caused by use of the information are borne by the recipient. In no event, even if Flyingvoice has been suggested the occurrence of damages that are direct, consequential, incidental, special, punitive or whatsoever (Including but not limited to loss of business profit, business interruption or loss of business information), shall not be liable for these damages.

End User License Agreement

This End User License Agreement ("EULA") is a legal agreement between you and Flyingvoice. By installing, copying or otherwise using the Products, you: (1) agree to be bounded by the terms of this EULA, (2) you are the owner or an authorized user of the device, and (3) you represent and warrant that you have the right, authority and capacity to enter into this agreement and to abide by all its terms and conditions, just as if you had signed it. The EULA for this product is available on the Flyingvoice Support page for the product.

Patent Information

China, the United States, EU (European Union) and other countries are protecting one or more patents of accompanying products and/or patents being applied by Flyingvoice.

Technical Support

Visit www.flyingvoice.com for product documents and FAQ, or contact Flyingvoice by email at support@flyingvoice.com. We’ ll get you the help you need.

Declaration of Conformity

1. **Part 15 FCC Rules**

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

• This device may not cause harmful interference

• This device must accept any interference received, including interference that may

cause undesired operation.

• The distance between user and products should be no less than 20cm。

Note: This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio 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: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user’ s authority to operate this equipment.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’ s authority to operate the equipment.

GNU GPL INFORMATION

Flyingvoice products firmware contains third-party software under the GNU General Public License (GPL). Flyingvoice uses software under the specific terms of the GPL. Please refer to the GPL for the exact terms and conditions of the license.

The original GPL license, source code of components licensed under GPL and used in Flyingvoice products can be downloaded online:

https://www.flyingvoice.com/soft_GPL.aspx

Content

About This Guide

Thank you for choosing Flyingvoice T5X series CPE, the main models are T5100/T5300, different models have different protection level and installation environment.

The T5100 is introduced as an example, which is a 5G CPE designed for outdoor use, with simple and rugged design, IP67 dustproof and waterproof rating and 6KV lightning protection design and can be flexibly mounted on walls and poles. The T5100 also integrates a 2.5GE port with PoE, a SIM card slot, and a USB-C interface for external PC debugging, providing integrated versatility. The T5100 offers all-in-one versatility. It eliminates the time and cost of laying fiber optic and other wired networks, providing users with fast and convenient broadband Internet access.

Related Documentation

The following types of related documents are available on each page:

1. Datasheet
2. Quick Installation Guide

If you have any questions about the documentation, please email us at support@flyingvoice.com.

We would appreciate your feedback, including but not limited to feedback on the structure, content, accuracy or completeness of the document, thanks!

Chapter 1 Product Introduction

This section describes the hardware components and installation methods, such as interfaces, LED lights, device power-on, and networking status.

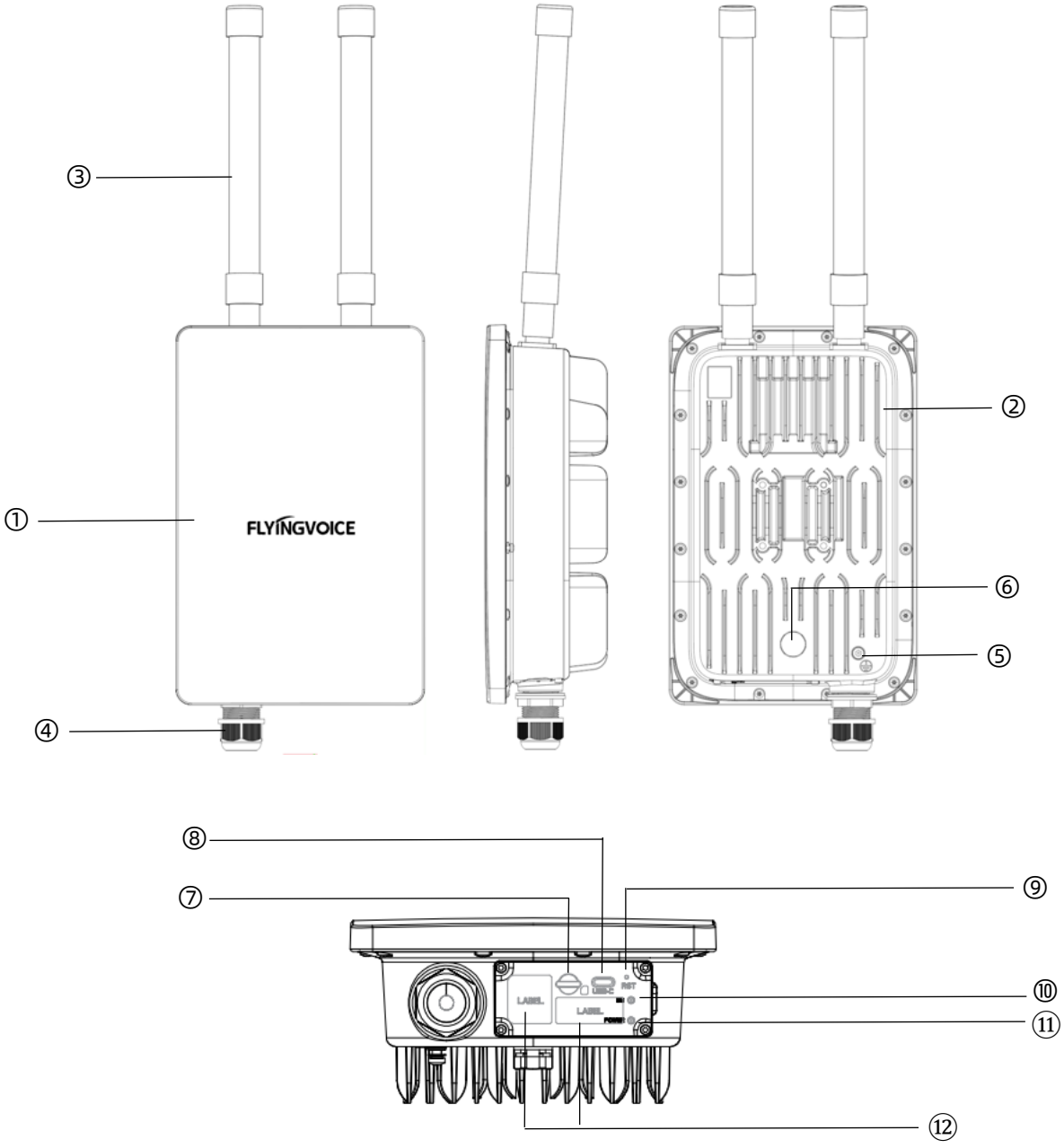
Topics contained as the following:

1.1 Hardware Introduction

This section describes the appearance and hardware structure of each model.

The T5X series CPE includes 2 models: T5100 and T5300.

T5100

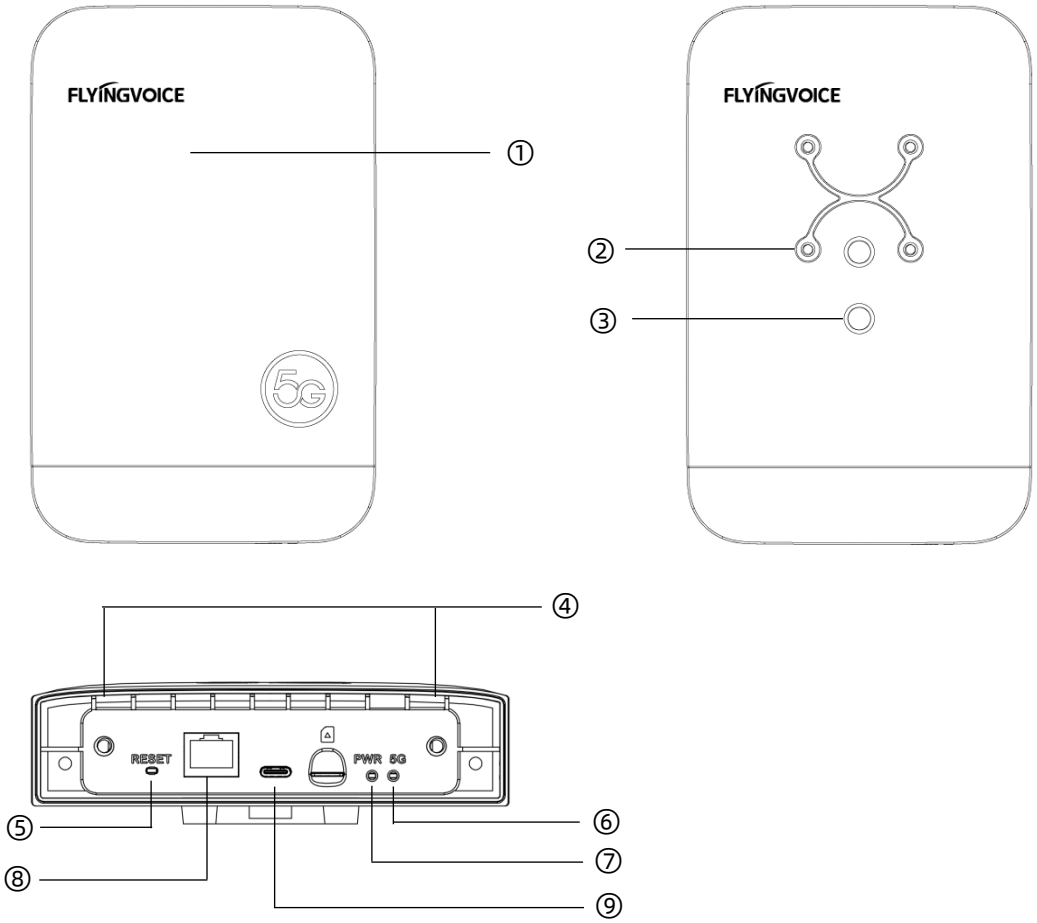


T5100 components are described below:

No.	Item	Description
1	Outer shell	Display FLYINGVOICE Logo. Made of UV-resistant and weatherable PC945-701C material.
2	Bottom shell	Made of cast aluminum, sand blasting process.
3	External antennas	Two 5G Sub-6GHz omni-directional antennas are connected externally through the SMA interfaces, which can be flexibly removed and replaced. The material is waterproof and sunscreen, which is convenient for outdoor installation.
4	Waterproof Screw Port	Internal LAN port for external PoE adapter power via network cable. The cable outlet can be used with the waterproof cable gland to secure the cable and prevent water from entering the device.
5	GND interface	Grounded against lightning strikes, protects equipment for normal operation outdoors.
6	Pneumatic Valve Hole	Balance the internal air pressure due to inner heat generated by device's operation.
7	SIM card slot	Remove the cover before using, this is use for inserting Nano-SIM card to get networked.
8	USB-C interface	USB3.0 Type-C

		Can be connected to PC for device debugging.
9	RST button	Short press 1s~5s: Restart the device. Long press more than 5s: Restore factory settings.
10	5G indicator	Steady Green: strong signal. Steady Blue: medium signal. Steady Red: weak signal. Slow Blinking Red: No Internet (such as the SIM card blocked/overdue/network failure). Light Off: No power/No SIM card or the SIM card can't be recognized correctly.
11	Power indicator	Steady Red: Device is starting or the device is abnormal. Steady Green: Device is powered on. Off: No power.
12	Label	Displays device model, IMEI code, MAC address, serial number, etc.

T5300



T5300 components are described below:

No.	Item	Description
1	Outer shell	Display FLYINGVOICE Logo and 5G icon. Made of UV-resistant and weatherable PC945-701C material.
2	Wall Screw Holes	For wall bracket mounting
3	Heat sink screw holes	For internal heat sink mounting
4	Bottom screw holes	For use with bottom shell attachment

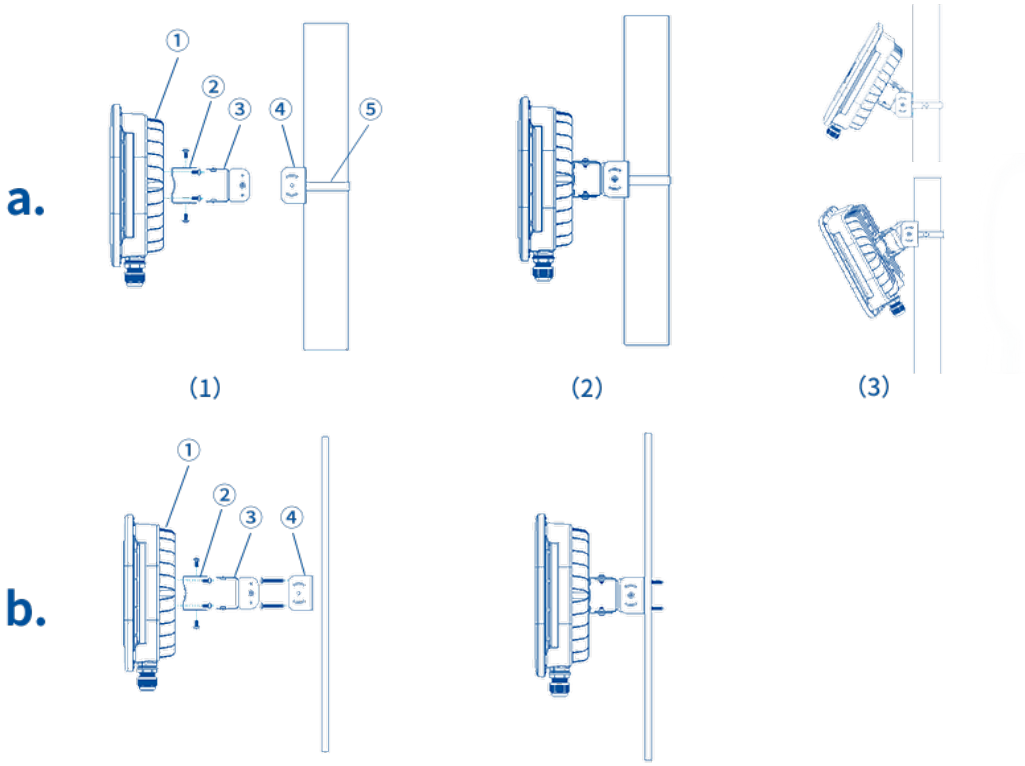
5	RST button	Short press 1s~5s: Restart the device. Long press more than 5s: Restore factory settings.
6	5G indicator	Steady Green: strong signal. Steady Blue: medium signal. Steady Red: weak signal. Slow Blinking Red: No Internet (such as the SIM card blocked/overdue/network failure). Light Off: No power/No SIM card or the SIM card can't be recognized correctly.
7	Power indicator	Steady Red: Device is starting or the device is abnormal. Steady Green: Device is powered on. Off: No power.
8	Waterproof Screw Port	Internal LAN port for external PoE adapter power via network cable. The cable outlet can be used with the waterproof cable gland to secure the cable and prevent water from entering the device.
9	USB-C interface	USB3.0 Type-C Can be connected to PC for device debugging.

The differences between T5 series models:

Model	T5100	T5300
Chipset	Qualcomm x65	Qualcomm x62
Bands	Sub-6GHz & mmWave	Sub-6GHz
PoE Protocol	IEEEE802.3bt	IEEEE802.3af
Power Consumption	30W	13W
IPXX Protection Level	IP67	IP65
Installation	Outdoor（Wall/Pole）	Indoor/Outdoor （Desktop/Wall/Window/Pole）

1.2 Installation Guide

This section describes the 2 basic installation methods of CPE: pole and wall, as shown in the following figure:



You can find the quick installation guide and standard components in the product box. Please Install with metal brackets and screw packs.

a. Pole-Fixed

1. Put ⑤ around the mounting pole and through the hole of 4, tighten ⑤ and then tighten the screws to fix it.

2. Attach ② to the back of ① with the screws included in the package.

3. Attach ③ to ④ and fix them with the screws.

4. Attach ① ② to ③ and fix them with the screws.

5. Adjust the angle of the device to get best effect and tighten all screws.

b. Wall-mounted

1. Attach ④ to the wall with the screws included in the package.

2. Attach ② to the back of ① with the screws included in the package.

3. Attach ③ to ④ and fix it with the screws.

4. Attach ① ② to ③ and fix them with the screws.

5. Adjust the angle of the device to get best effect and tighten all screws.

Chapter 2 Web Configuration

This section describes how to log in, view device status information, IP configuration.

Topics contained as the following:

2.1 Log in

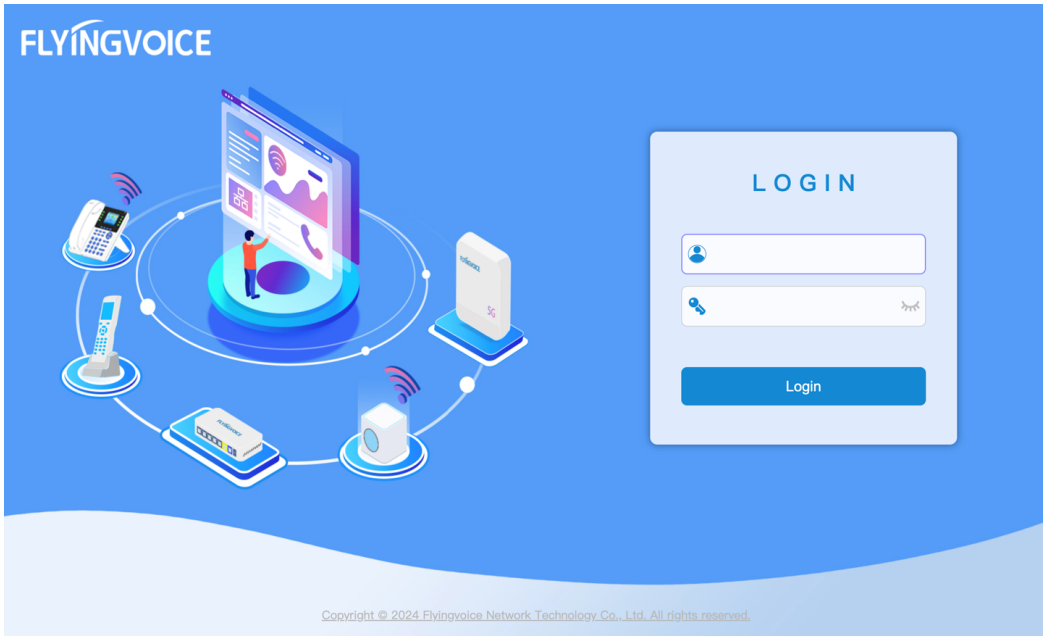
The T5X Series CPE provides a web browser-based interface for configuring and managing the device.

Before configuring, make sure your PC is properly connected to the LAN port of the device.

Log in to the device Web page:

1. The URL format of the login page is: http://IP address (LAN port), and the default LAN port IP address is: 192.168.225.1

2. Please enter the corresponding address in the address input box: http://192.168.225.1, and then the page will navigate to the login page of the device, as shown in the following figure:



3. The login account: administrator.

The initial account/password is: admin/the last six digits of SN number;

for the highest permissions, can view and configure all pages.

Enter the usename and password, click the login button to enter.

2.2 Status & Log

You can view device system information, network and system logs through the web interface.

Topics contained as the following:

- System Information
- Network Information
- System Log

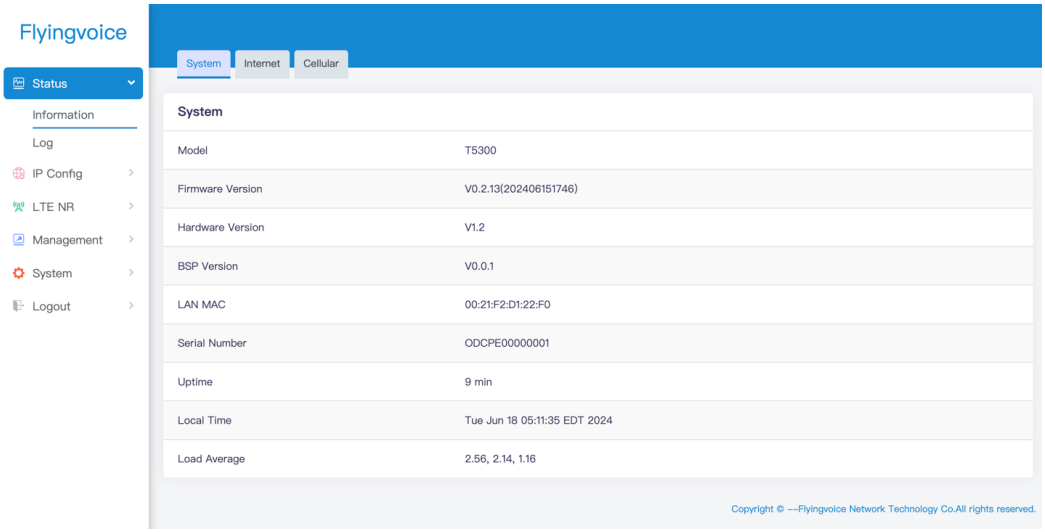
System Information

You can view device information such as device model, software version, etc. through this interface.

View System Information through the web page:

1. Navigate to **Status**-> **Information** -> **System.**

2. View the device system information.



Parameter Name	Description
Model	Display the product model.
Firmware Version	Display the firmware version number of the device's software, which can be upgraded according to your requirements.
Hardware Version	Display the hardware PCBA version of the device.
BSP Version	Display the version of the changed files in the 5G module.
LAN MAC	Display the MAC address of the LAN port of the device. It is fixed by factory default.
Serial Number	Display the factory serial number of the device.
Uptime	Display how long the device runs after being turned on.
Local Time	Display the UTC time of the area where the device is located.
Load Average	Displays the average load of the device for 3 time periods: In the last minute, in the last 5 minutes, in the last 15 minutes.

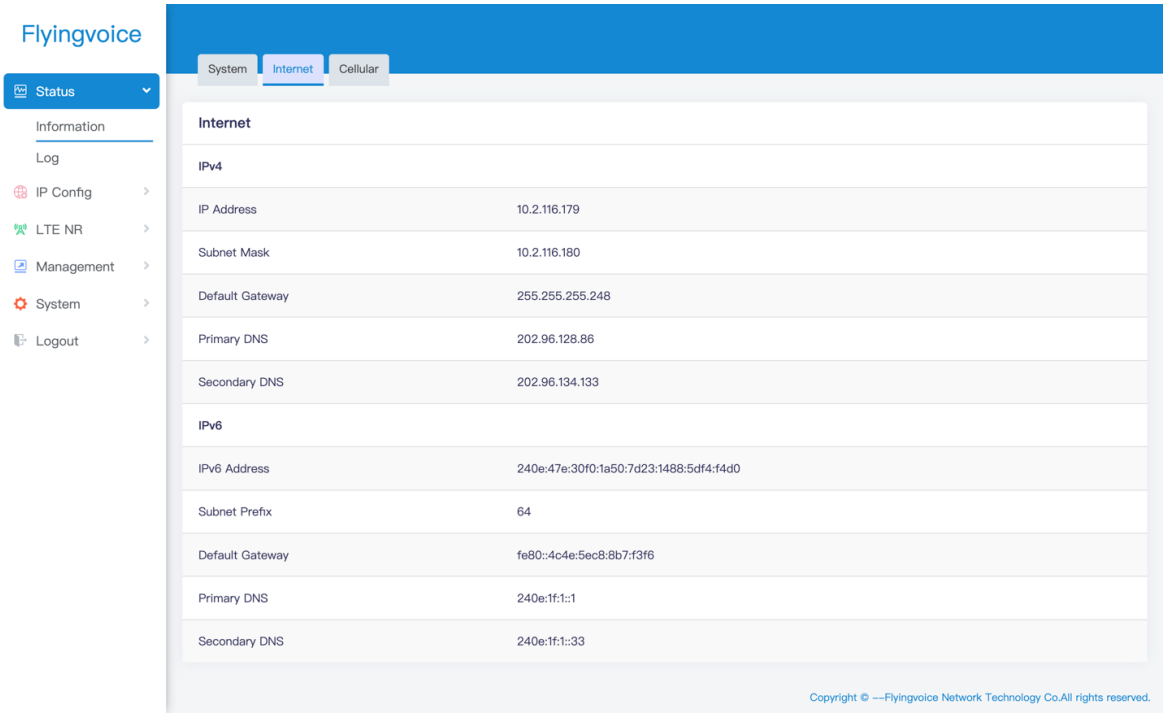
Network Information

On these web pages, you can view the network connection status of the device, including the current IPv4 and IPv6 address, SIM card status, and 4G / 5G cellular network signal parameters, etc.

View Network Information through the web page:

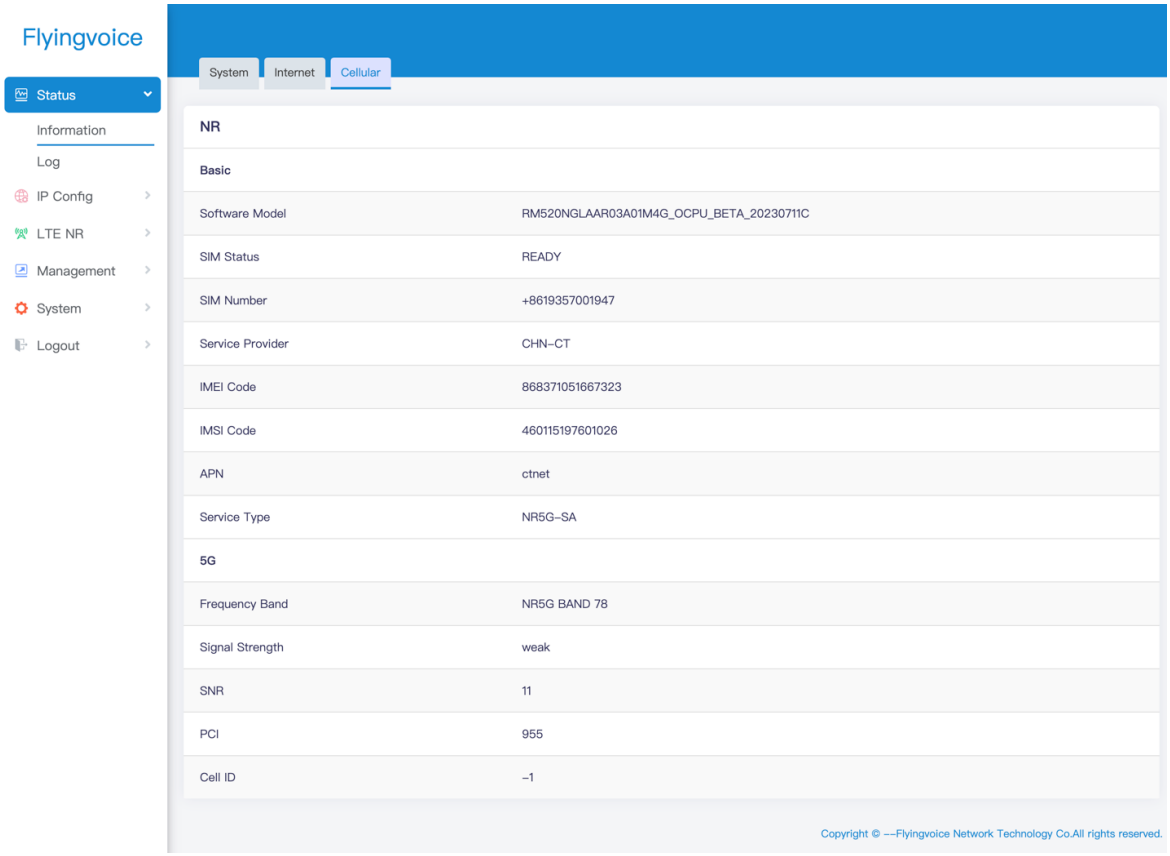
1. Navigate to **Status**-> **Information** -> **Internet.**

2. View IP information of the device, including IPv4 and IPv6.



3. Navigate to **Status**-> **Information** -> **Cellular.**

4. View the SIM card information and 5G NR radio parameters.



Parameter Name	Description
Basic	
Software Model	Display the software version of the 5G module of the device, which cannot be modified after delivery.
SIM Status	Display whether the SIM card is currently inserted or recognized by the device.
SIM Number	If the SIM card is inserted and the device recognizes it, the SIM card number is displayed.
Service Provider	If the SIM card is inserted and the device recognizes it, the carrier to which the current SIM card belongs is displayed.
IMEI Code	Display the unique identification code of the device, which is fixed after delivery and can also be viewed on the label of the
IMSI Code	Display the unique identification code of the device SIM card, which is fixed by the carrier.

APN	Displays the APN (Access Point Name) of the device, which can be modified manually.
Service Type	Display the 5G networking mode of the device, which is generally SA or NSA.
5G	
Frequency Band	Display the currently accessed 5G frequency bands.
Signal Strength	Display the current 5G signal strength: weak, medium, strong.
SNR	Display the ratio of the current 5G signal to noise, indicating the quality of the current network.
PCI	Displays the current PCI for identifying individual physical cells in the cellular network.
Cell ID	Display the unique cell ID of the current access.

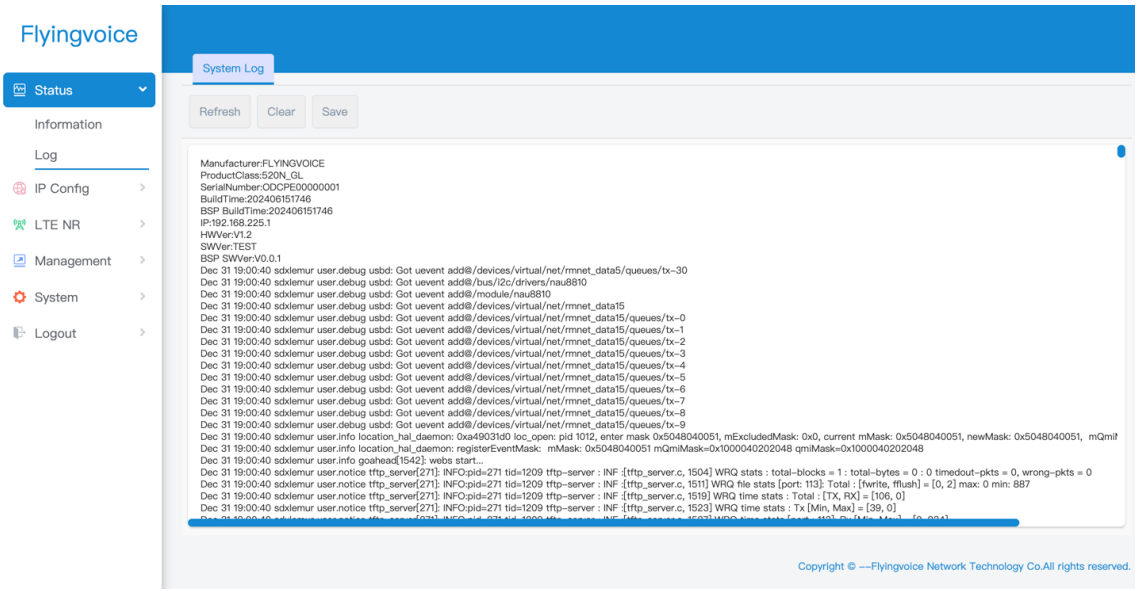
System Log

System logs are usually part of the system status and are used to record device operation, events, and error messages. Administrators can view the system logs to obtain information about the operating status of the device.

View System Logs through the web page:

1. Navigate to **Status**-> **Log** -> **System Log.**

2. View system logs information of the device.



3. Support one-click refresh of the current log, clear all log information, save the current log file to local.

2.3 IP Configuration

The IP configuration is usually part of the network configuration, where you can configure IPv4 networks.

Topics contained as the following:

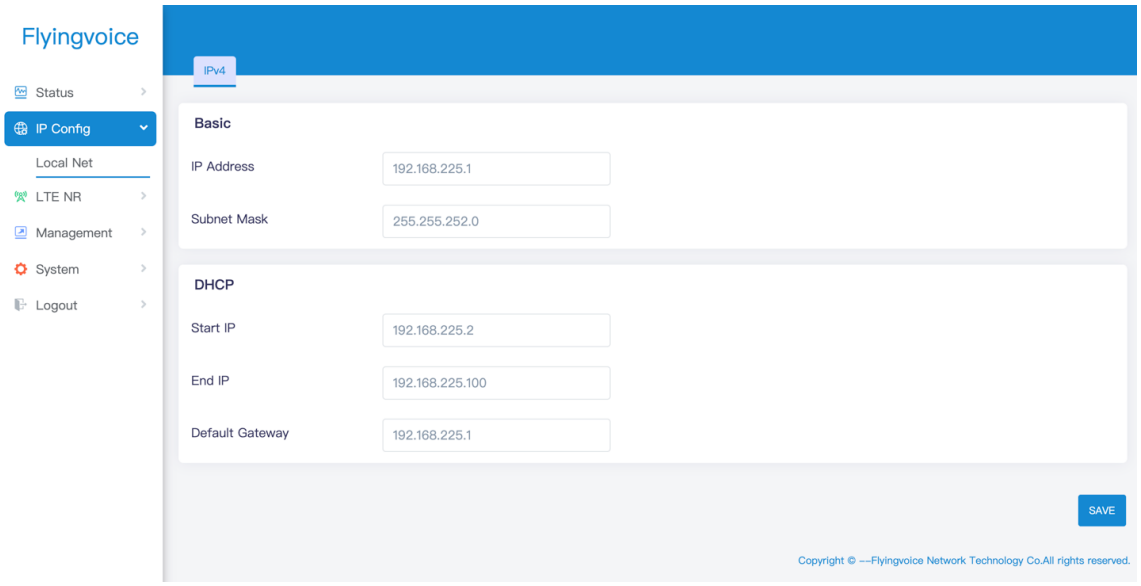
- IPv4

IPv4

Config IPv4 Address through the web page:

1. Navigate to **IP Config**-> **Local Net** -> **IPv4.**

2. Set the IPv4 address, subnet mask, and DHCP address pool, and click Save.



Parameter Name	Description
Basic	
IP Address	Enter the IPv4 address of the device's LAN port, default is 192.168.225.1.

Subnet Mask	Enter the IPv4 subnet mask of the LAN port, default is 255.255.255.0.
DHCP	
Start IP	By default, the device supports creating DHCP address pools for terminals as a DHCP server. Enter the start IP address of the DHCP address pool. Default is 192.168.225.2.
End IP	Enter the end IP address of the DHCP address pool, default is 192.168.225.100.
Default Gateway	Enter the gateway address of the DHCP server, default is 192.168.225.1.

Chapter 3 5G Configuration

This section describes 5G settings, including network protocol settings, frequency band settings, APN settings, and PIN settings, etc.

Topics contained as the following:

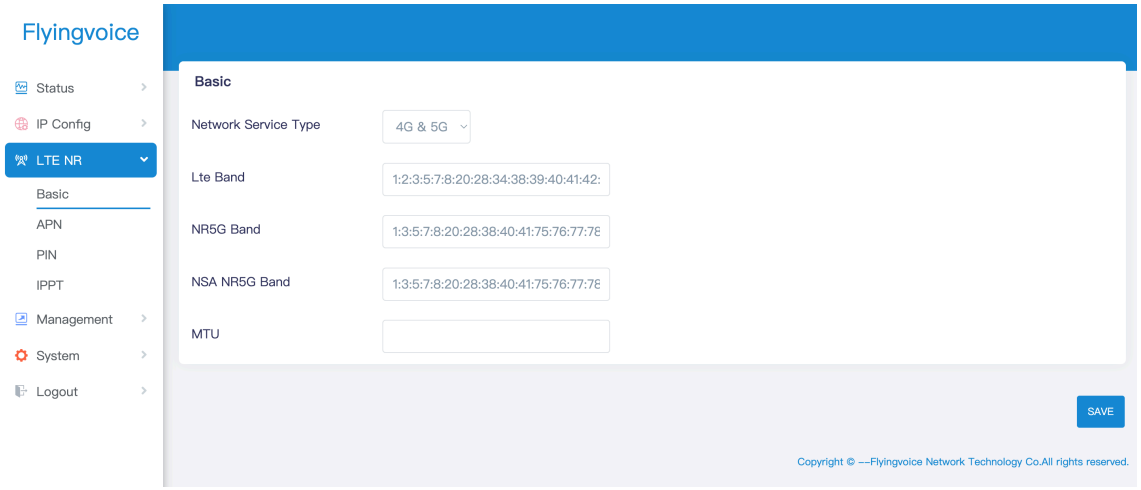
3.1 Basic Settings

You can enter to the Basic Settings page to set the network connection type and band configuration.

Config 5G network through the web page:

1. Navigate to **LTE NR**-> **Basic.**

2. Config basic settings (network service type, LTE or NR5G bands, etc.), click save.



Parameter Name	Description
Network Service Type	User can select the network type that the device connects to. Optional Auto / Only 4G / Only 5G, default is Auto.
LTE Band	User can enter the specified 4G frequency bands. The default is all supported 4G bands by the module.
NR5G Band	User can enter the specified 5G SA frequency bands. The default is all supported 5G bands by the module.
NSA NR5G Band	User can enter the specified 5G NSA frequency bands. The default is all supported 5G bands by the module.
MTU	Maximum Transmission Unit (MTU), which specifies the

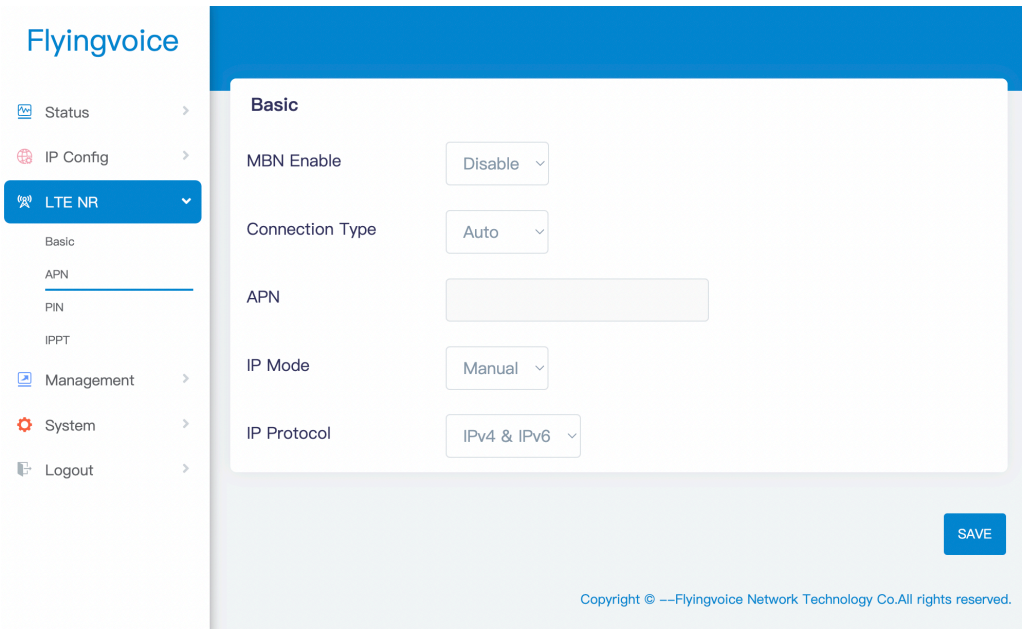
3.2 APN Settings

APN (Access Point Name) configuration is used in mobile networks to specify the parameters needed for a device to connect to the network of a mobile operator. Each mobile operator has its own APN, which includes the network parameters required to connect to the data network.

Config APN through the web page:

1. Navigate to **LTE NR**-> **APN.**

2. Config APN settings, click save.



Parameter Name	Description
MBN Enable	Supports activation of MBN files to meet the configuration requirements of the operator network. Disabled by default, MBN will activate the general ROW by default; When set to automatic, the corresponding MBN file will be automatically identified and activated according to the SIM card operator used by the user. This operation may cause risks and network abnormalities.

Connection Type	User can select a mode of the device how to access an APN. Optional Auto / Manual, default is Auto.
APN	Access Point Name, specifies the network identifier used to connect to the mobile network. If you select the manual connection mode, need to enter this parameter.
IP Protocol	The version of the IP protocol used by the device to establish a connection on the mobile network, Optional IPv4 / IPv6 / IPv4 & IPv6, default is IPv4 & IPv6.

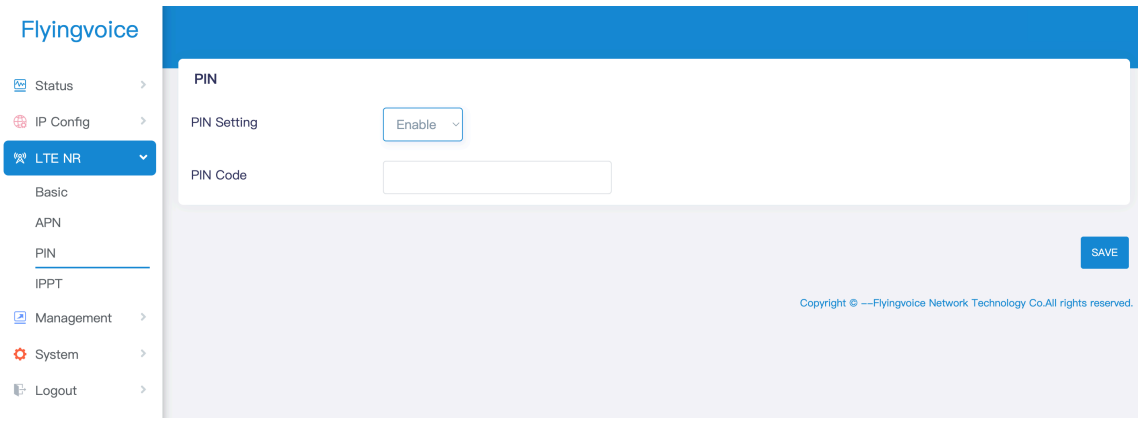
3.3 PIN Code Settings

PIN (Personal Identification Number) is a common security feature used to protect the SIM card in mobile devices such as phones and CPE (Customer Premises Equipment). Each SIM card comes with a unique PIN code, which is a numeric code typically consisting of 4 to 8 digits.

Config PIN code through the web page:

1. Navigate to **LTE NR-> PIN.**

2. Check PIN code, click save.



Parameter Name	Description

PIN Setting	User can select the current enabled status of the PIN code. Optional Enable or Disable, default is Disable.
PIN Code	Enter the PIN code and verify to unlock the SIM card.

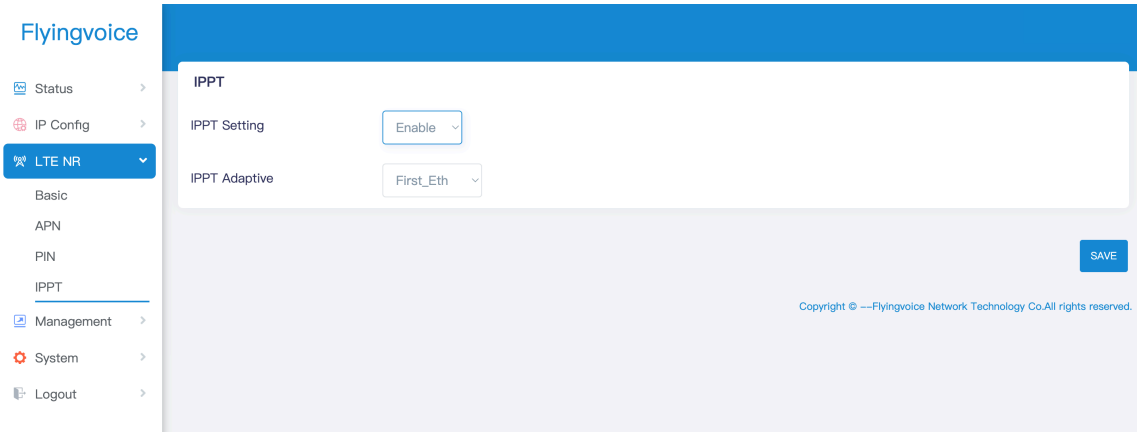
3.4 IPPT Settings

IPPT（IP Passthrough），the public IP address obtained by the CPE device can be assigned to the terminal under the LAN port. However, only a single terminal connected to the CPE can be obtained. The terminal can be confirmed by specifying a fixed MAC address. The CPE device supports 2 modes to specify the configuration terminal to obtain the IP address of the CPE.

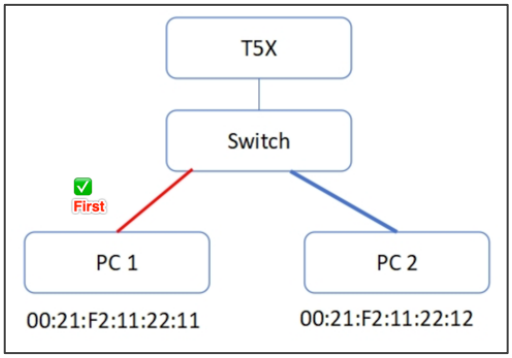
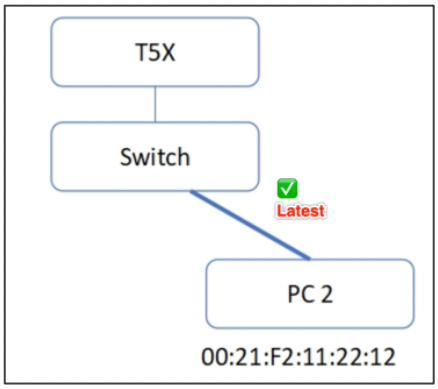
Config IPPT through the web page:

1. Navigate to **LTE NR**-> **IPPT.**

2. Config IPPT enable and select a mode, click save.



Parameter Name	Description
IPPT Setting	User can select the current enabled status of the IPPT. Optional Enable or Disable, default is Disable.

IPPT Adaptive	Two modes are supported: First_Eth, Latest_Eth; First_Eth: For the first connection allocation, multiple terminals access CPE in turn. The first terminal will be assigned a fixed MAC address and obtain the IP address of CPE as the IPPT Host. When this first terminal is disconnected, other terminals will also not obtain it.  Latest_Eth: The latest connection allocation, multiple terminals access CPE in turn, and the first terminal will also be assigned a fixed MAC address and obtain the IP address of CPE as IPPT Host, but it is allowed to release the MAC address and change to other terminals as IPPT Host. User can change the IPPT Host in two ways. One is to reboot the CPE and disconnect the original IPPT Host terminal, only another terminal is retained to access, then this terminal will be changed as the IPPT Host and obtain the IP address of CPE. Another is not to reboot the CPE, also need to disconnect the original IPPT Host terminal, and re-connect another terminal to CPE, then then this terminal will be changed as the IPPT Host and obtain the IP address of CPE. 

Chapter 4 Management Configuration

This section describes how to modify system and management configurations of the device, including language Settings, time Settings, login account Settings, Telnet Settings and Provision Settings, etc.

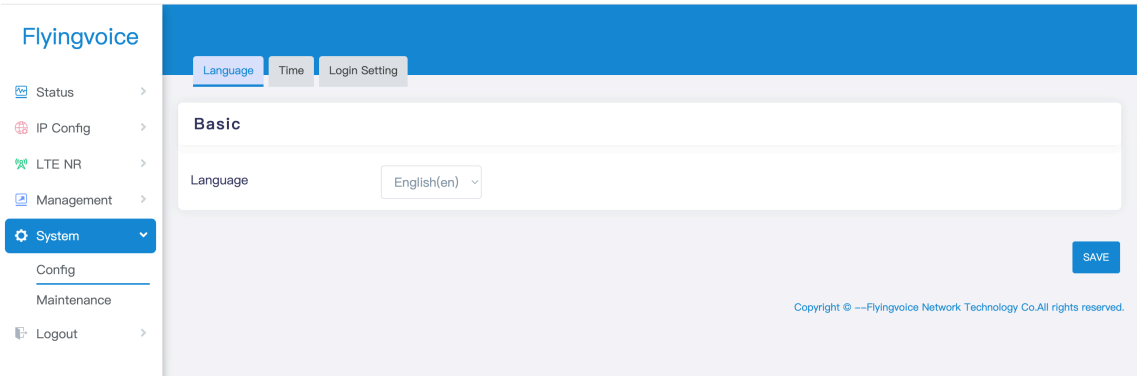
Topics contained as the following:

4.1 Language Setting

Config system language through the web page:

1. Navigate to **System**-> **Config**-> **Language.**

2. Select a language, click save.



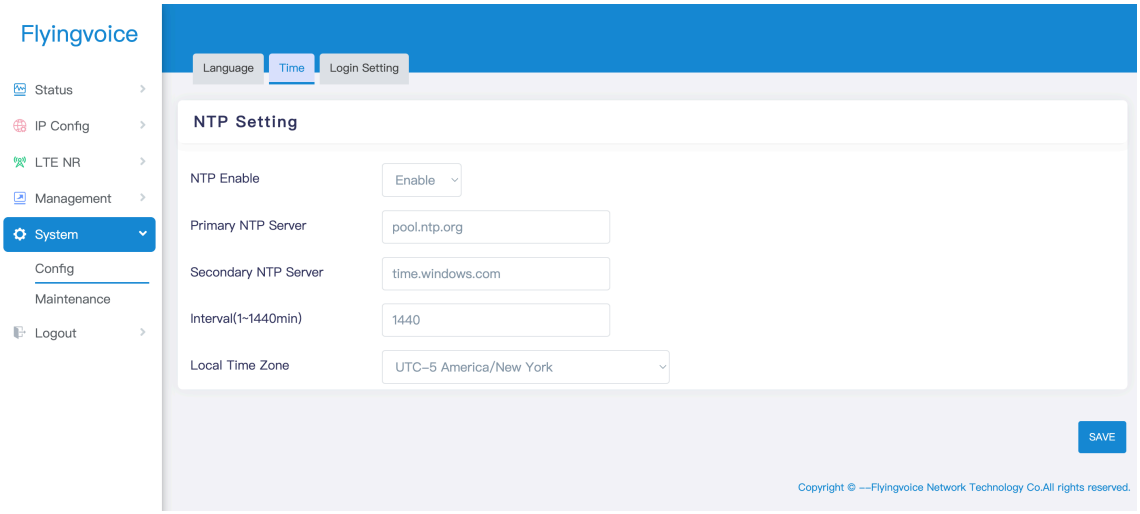
Parameter Name	Description
Language	User can select the language displayed on the web page of the device. Optional Chinese or English. The default is English.

4.2 Time Settings

Config system time through the web page:

1. Navigate to **System**-> **Config**-> **Time.**

2. Config NTP enable, set the NTP server and time zone, click save.



Parameter Name	Description
NTP Enable	User can choose to enable NTP to set synchronization server time or time zone time.
Primary NTP Server	Enter the IP address or domain name of the primary NTP server for time synchronization.
Secondary NTP Server	Enter the IP address or domain name of the secondary NTP, which is used for backup when the active NTP server fails.
Interval	Enter the refresh period of the NTP server. The default value is 1440 minutes.
Local Time Zone	The value is in the UTC time format. User can select the time zone where the device is located. The default time zone is UTC-5 New York.

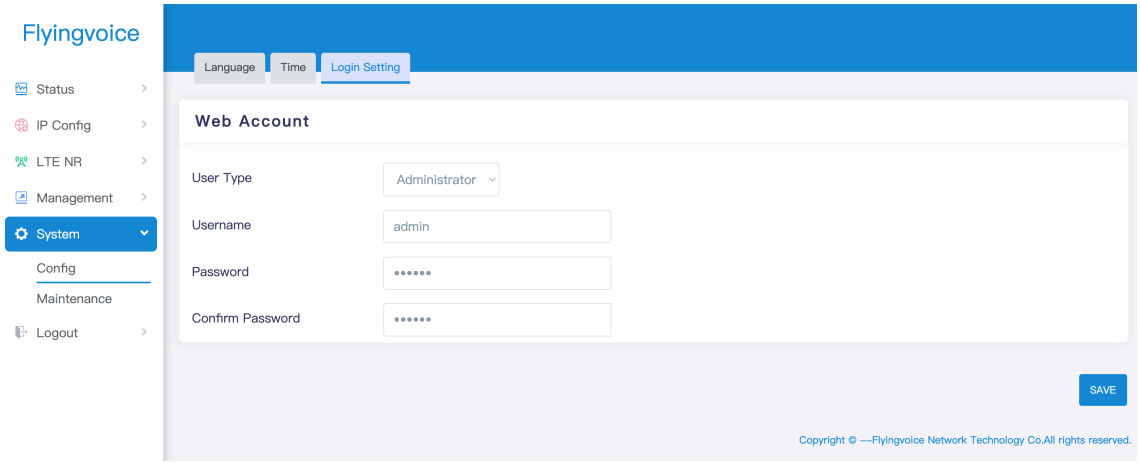
4.3 Login Account Settings

The username and password used to log in to the web page of the device. It is recommended that the administrator customize the password after the initial login.

Config system login account through the web page:

1. Navigate to **System**-> **Config**-> **Login Setting.**

2. Config username and password, click save.



Parameter Name	Description
User Type	Support to select the user level of the current device web login, optional only administrator.
Username	The user identifier used for authentication. The default administrator is admin.
Password	The authentication password associated with the username, which supports password change but is not visible to the current password.
Confirm Password	Enter the changed password again and confirm the password twice.

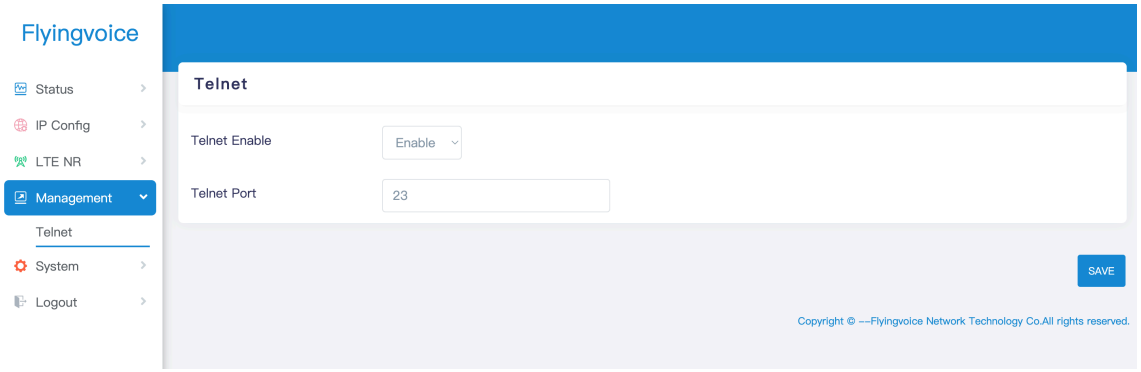
4.4 Telnet Settings

Support remote device through Telnet command, remote login access to the local device.

Config telnet through the web page:

1. Navigate to **System**-> **Management**-> **Telnet.**

2. Config Telnet enable and setting telnet port, click save.



Parameter Name	Description
Telnet Enable	Optional whether to enable remote Telnet, the default is Enable.
Telnet Port	After telnet is enabled, enter the telnet port number for connecting to the device. The default is 23.

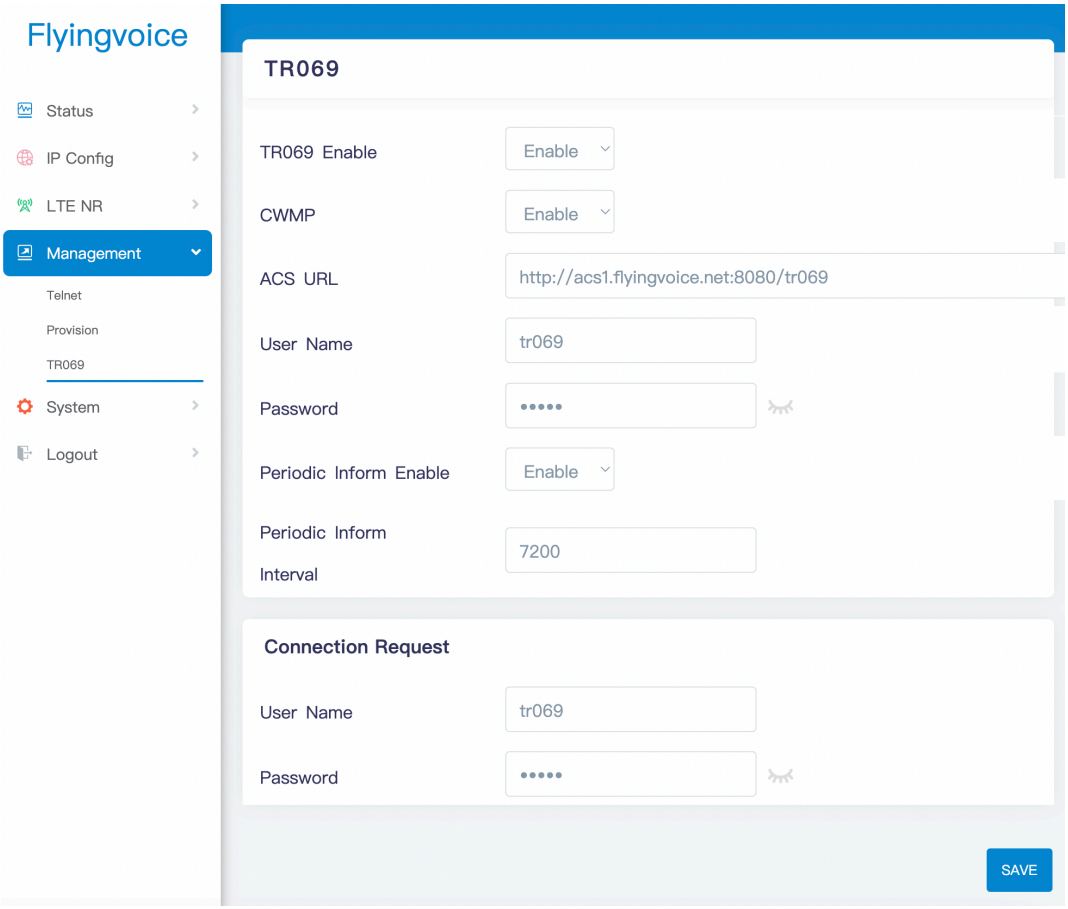
4.5 TR069 Settings

TR069 is used for automatic negotiation and interaction between the device and ACS, which can realize automatic configuration and remote management of the device.

Config telnet through the web page:

1. Navigate to **System-> TR069**

as shown in the following figure:



Parameter Name	Description
TR069 Enable	Enable TR069 protocol for remote management and configuration of the device, optional enable/disable.
CWMP	Enable CPE WAN Management Protocol (CWMP), optional enable/disable.
ACS URL	The URL address of the Auto-Configuration Server (ACS) used for the device connection and communication with the ACS.
User Name	ACS username, used to connect to ACS, the default is none.
Password	ACS password associated with the username the default is none.
Periodic Inform Enable	Enables sending notifications to ACS periodically, optionally enable/disable.
Periodic Inform Interval	The time interval at which scheduled notifications are sent to the ACS to report device status and information.

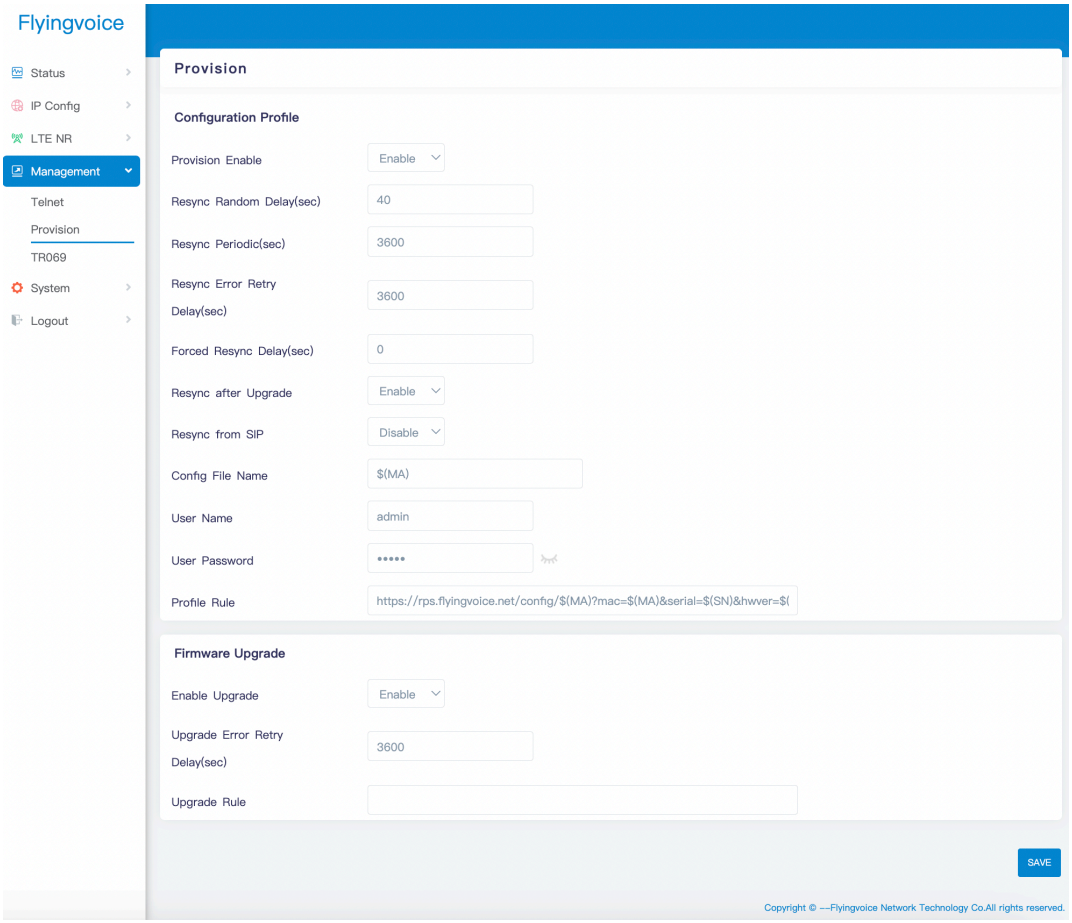
User Name	CPE username, used to verify the username when ACS connects to the device, the default is product model, like SR3000 or SR3000-lite.
Password	CPE password, used to verify the password when ACS connects to the device, the default is product serial number.

4.6 Provision Settings

Provision configuration supports 3 protocols: TFTP (supports option 66), HTTP and HTTPS. It automatically resynchronizes the remote TFTP/HTTP/HTTPS server for remote deployment, such as delivery configuration and upgrade.

Navigate to **Management** -> **Provision**,

as shown in the following figure:



Parameter Name	Description
Provision Enable	Optional whether to enable the provision function.
Resync Random Delay(sec)	Fill in the maximum delay time for requesting synchronized files, default 40 seconds. A random value is generated in the interval from 0 to 40 seconds, and the device waits for this value for the interval before requesting the provision server. When 0 is filled in, it means that the feature is disabled to prevent many devices from sending too many server requests at the same time.
Resync Periodic(sec)	Fill in the cycle time for the device to automatically re-synchronize with the server, default 3600 seconds.
Resync Error Retry Delay(sec)	Fill in the interval to re-synchronize again after a synchronization error, default 3600 seconds.
Forced Resync Delay(sec)	Fill in the forced synchronization time, if the device is in a busy state, such as a call at the specified re-synchronization time, server synchronization is not possible, then define this interval to guarantee that the device is forced to re-synchronize after being idle, default 0 seconds.
Resync after Upgrade	Optional whether to trigger the re-synchronization function after each firmware upgrade.
Resync From SIP	Optional whether to enable re-synchronization from SIP.
Config File Name	Fill in the configuration file name.
User Agent	Fill in the name of the user agent.
User Name	Fill in the username required for HTTP authentication, default is admin.
User Password	Fill in the password required for HTTP authentication, default is admin.
Profile Rule	Fill in the path URL of the configuration file to complete the synchronization command, the command is a TCP/IP operation and an associated URL, the TCP/IP operation can be TFTP, HTTP or HTTPS.

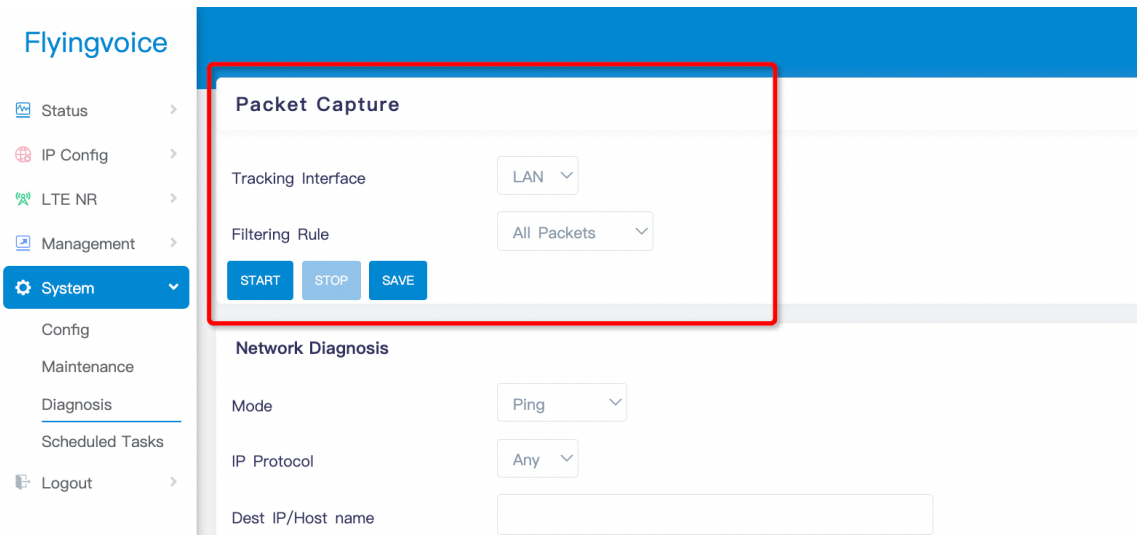
Enable Upgrade	Optional whether to upgrade the firmware on re-synchronization.
Upgrade Error Retry Delay(sec)	Fill in the retry interval after upgrade failure, when the upgrade fails, the system starts timing from the set value, and automatically re-upgrades after decreasing to 0. The default is 3600 seconds.
Upgrade Rule	Fill in the path where the upgrade firmware file is located under the server.

4.7 Diagnosis

Supports packet capture and network diagnostics, including Ping, Traceroute, and TWAMP.

Capture packets through the web page:

Packet capture is a commonly used tool to obtain the corresponding complete packet, analyze the process from packet sending to building connection, and analyze network failures.



1. Navigate to **System** -> **Diagnosis** -> **Capture Packet**

2. Select the port for packets tracking, the default is LAN port

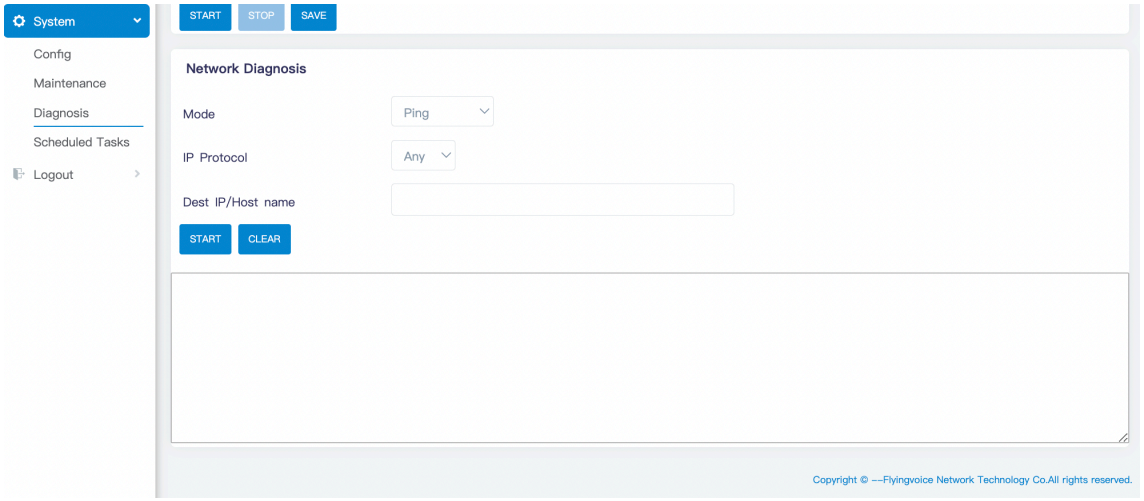
3. Select the packets format to capture, the default is all packets

4. Click Start, and after finishing, you can save the file to the local for analysis

as shown in the following figure:

Ping diagnosis through the web page:

Ping is the most common debugging tool for detecting the accessibility of network devices. It uses ICMP message information to detect whether the specified IPv4 address is reachable and output corresponding statistical information.



1. Navigate to **System** -> **Diagnosis** -> **Network Diagnosis**

2. Select Mode: Ping

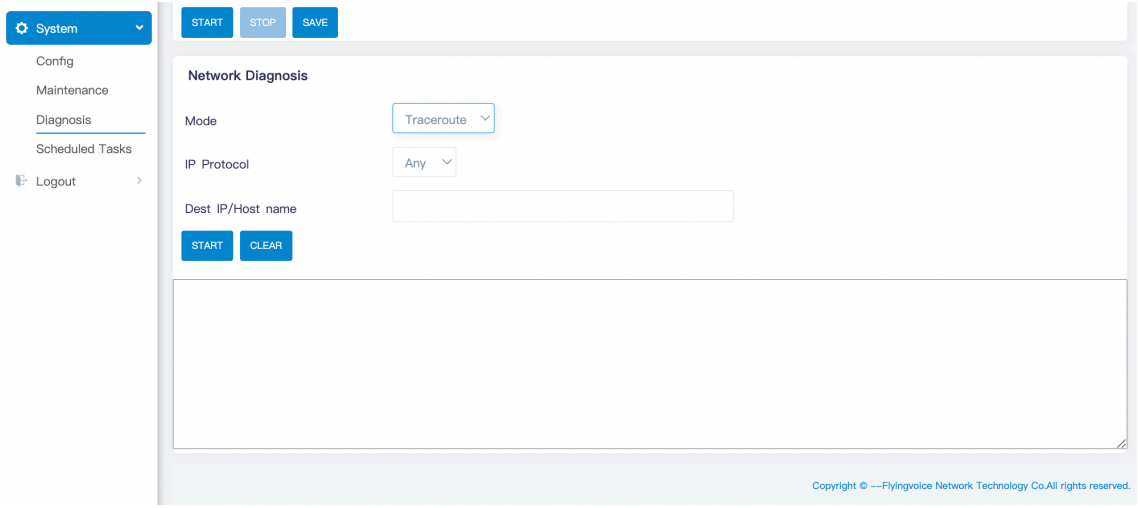
3. Select IP Mode, the default is IPv4 & IPv6

4. Enter the destination IP address or domain name to be accessed

5. Click Start, and the access information (whether communication with the remote host is reachable, delay, and packet loss) will be displayed in the text box.

Traceroute diagnosis through the web page:

Traceroute is mainly used to view the path information of the data packet from the source to the destination, so as to check whether the network connection is available. When the network fails, the user can use this method to locate the fault point.



1. Navigate to **System** -> **Diagnosis** -> **Network Diagnosis**

2. Select Mode: Traceroute

3. Select IP mode, the default is IPv4 & IPv6

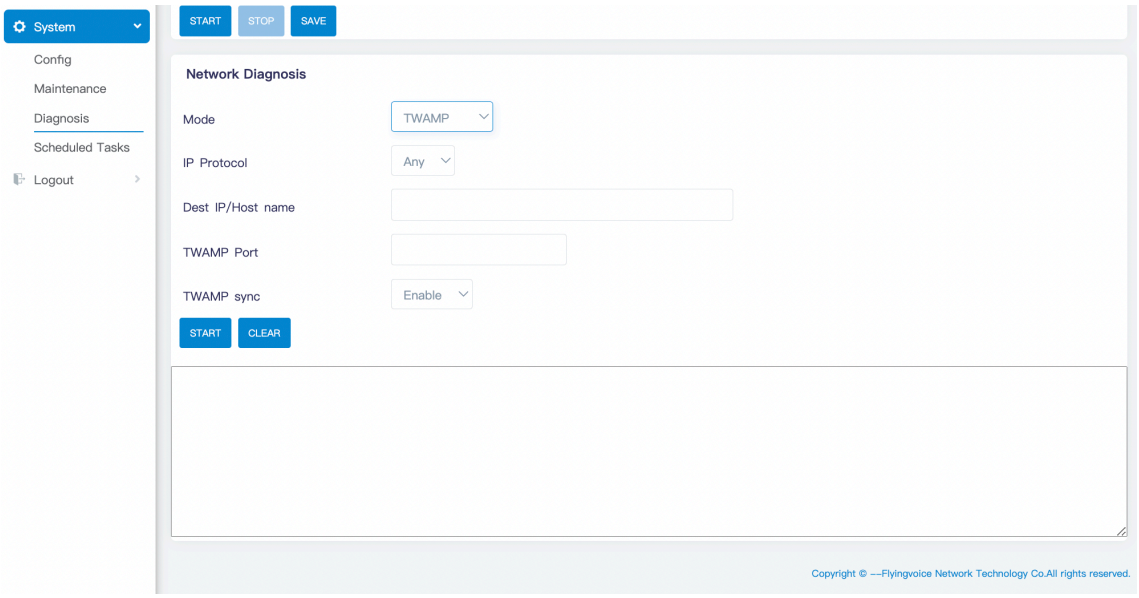
4. Enter the destination IP address or domain name to be accessed

5. Click Start, and the obtained information will be displayed in the text box (the gateway address of each hop communicating with the remote host, and the time difference between the sent 3 UDP packets and the corresponding received ICMP timeout packets or ICMP port unreachable packets)

TWAMP diagnosis through the web page:

TWAMP is a performance measurement technology for IP links. It can perform bidirectional performance statistics in both the forward and reverse directions, and

detect bidirectional delay, jitter, and packet loss rate.



1. Navigate to **System** -> **Diagnosis** -> **Network Diagnosis**

2. Select Mode: TWAMP

3. Select IP mode, the default is IPv4 & IPv6

4. Enter the destination IP address to be accessed

5. Enter the service port of TWAMP

6. Enter the synchronization time of TWAMP. Only when both parties use TWAMP can time synchronization be set

7. Click Start, and the information of both parties will be displayed in the text box (bidirectional delay and packet loss of communication with the remote host)

Chapter 5 Maintenance Configuration

This section describes how to maintain and upgrade device, restore factory state, backup, and reboot.

Topics contained as the following:

5.1 Backup

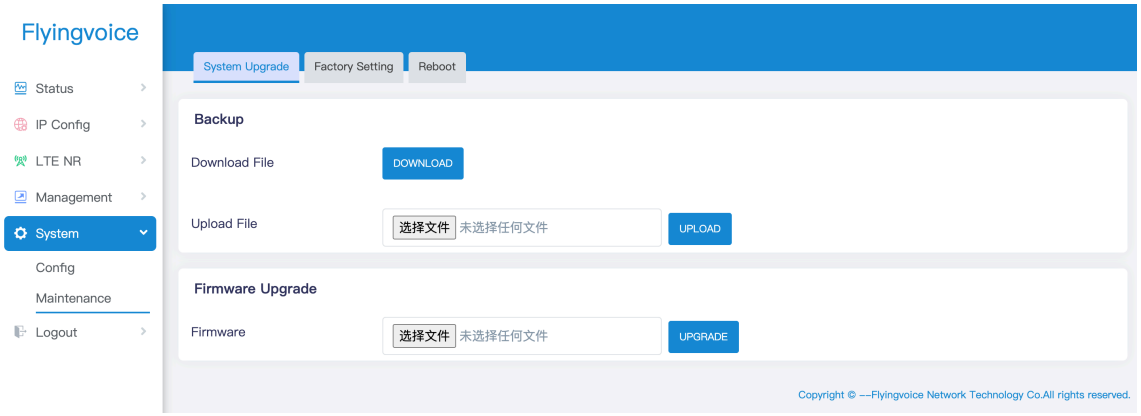
User can download system files to back up the current configuration information of the device. Or upload the configuration file to copy the configuration of other devices.

Config backup configuration the web page:

1. Navigate to **System**-> **Maintenance**-> **System Upgrade**-> **Backup.**

2. If you want to back up the current configuration, you can click the download button to save the current configuration file to the local.

If you want to quickly configure your device or copy the configuration of another device, you can click Upload and select local file.



5.2 Firmware Upgrade

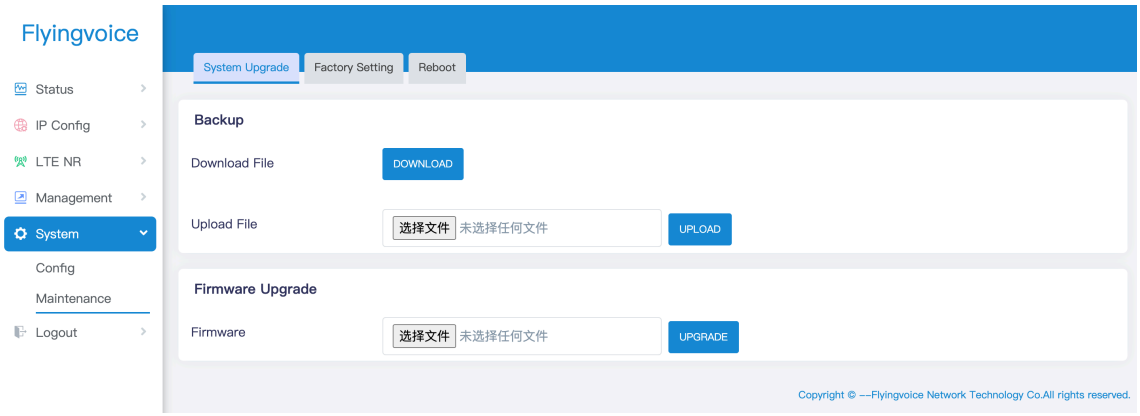
Users can upgrade or downgrade the firmware version as required.

Config firmware configuration the web page:

1. Navigate to **System**-> **Maintenance**-> **System Upgrade**-> **Firmware Upgrade.**

2. Select the local file and click the Upgrade button.

Note: Do not power off or restart during the upgrade process.

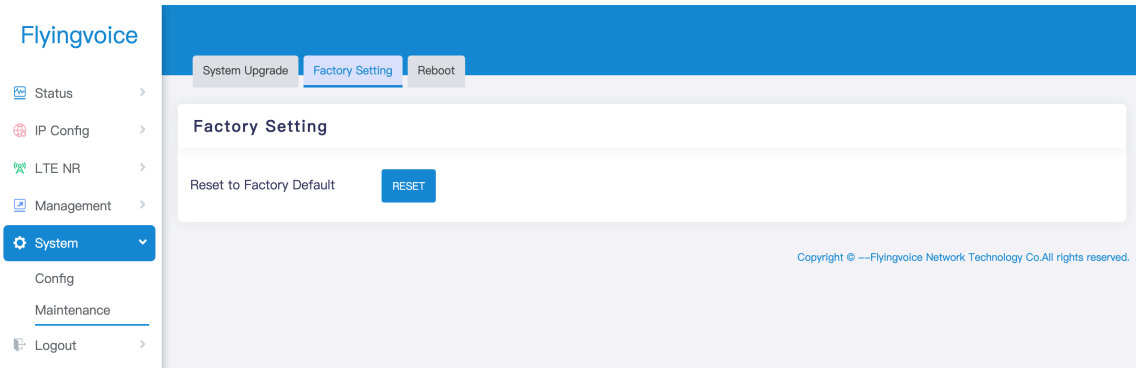


5.3 Factory Setting

Config factory setting the web page:

1. Navigate to **System**-> **Maintenance**-> **Factory Setting.**

2. Click Reset button.

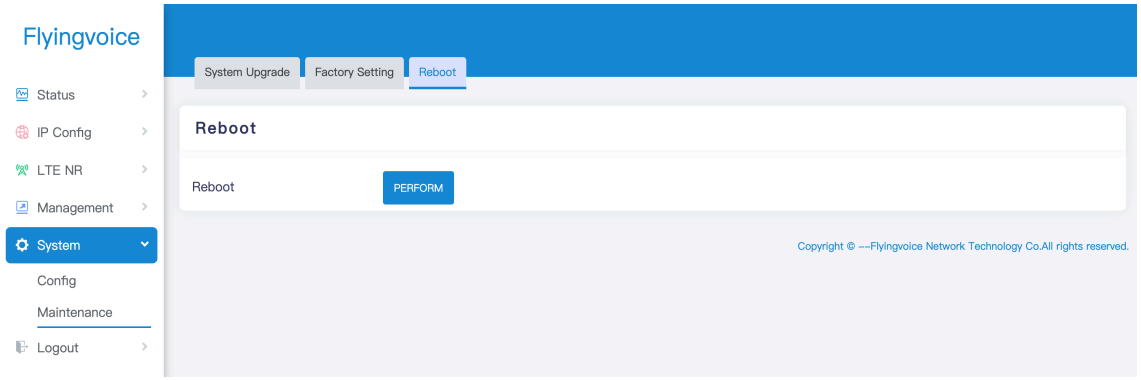


5.4 Reboot

Config reboot setting the web page:

1. Navigate to **System**-> **Maintenance**-> **Reboot.**

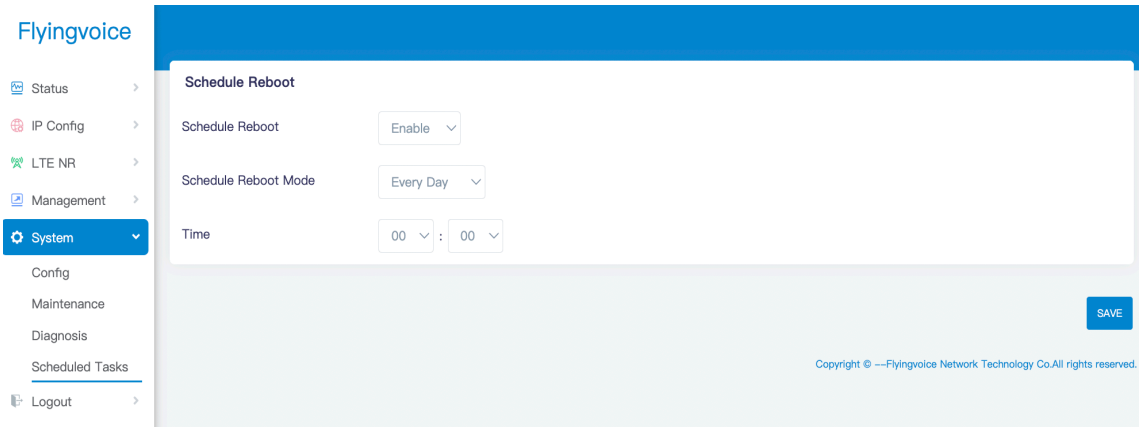
2. Click Perform button.



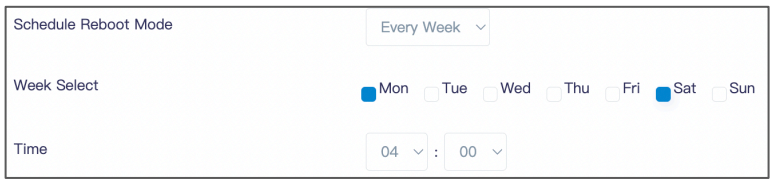
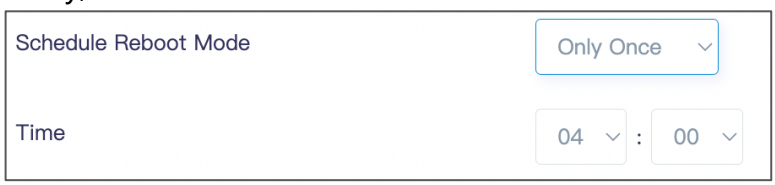
It also supports schedule reboot by once / every day / every week.

Navigate to **System** -> **Config** -> **Schedule Tasks**.

as shown in the following figure:



Parameter Name	Description
Schedule Reboot	Optional whether to enable the schedule reboot. Default is disabled.

Schedule Reboot Mode	If you enable the schedule reboot, you can choose the mode: every day, every week or just once. Every day: Cycle by day, automatically reboots at a certain point each day.  Every Week: Multiple options, cycle according to the day of the week, automatically reboots at a certain point on the day of the week.  Only Once: Automatically reboots only at a certain point in today; 
Time	If you enable the schedule reboot and choose a mode, you should choose time of the reboot.