FLYINGVOICE

User Guide

SR3000 & SR3000-lite

Copyright

Copyright © 2020 Flyingvoice Network Technology CO., LTD.

Copyright © 2020 Flyingvoice Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Flyingvoice Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

When this publication is made available on media, Flyingvoice Network Technology CO., LTD. gives its consent to downloading and printing copies of the content provided in this file only for private use but not for redistribution. No parts of this publication may be subject to alteration, modification or commercial use. Flyingvoice Network Technology CO., LTD. will not be liable for any damages arising from use of an illegally modified or altered publication.

Trademark

Flyingvoice®, the logo and the name and marks are trademark of Flyingvoice Network Technology CO., LTD, which are registered legally in China, the United States, EU (European Union) and other countries.

All other trademarks belong to their respective owners. Without Flyingvoice's express written permission, the recipient shall not reproduce or transmit any portion thereof in any form or by any means, with any purpose other than personal use.

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", Flyingvoice Network Technology Co., Ltd. III/V 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

FCC compliance 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.

(2) (2)This device must accept any interference received, including interference that may cause undesired operation.

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

Note: 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, 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.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

RF warning for Mobile device:

This equipment complies with FCC 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.

ISED Canada compliance statement

This device complies with ISED 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.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

This equipment complies with IC RSS-102 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.

Le présentappareilestconforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitationestautorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareildoit accepter tout brouillageradioélectriquesubi, mêmesi le brouillageest susceptible d'encompromettre le fonctionnement.

La bande 5150-5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

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.

CE compliance statement

"Flyingvoice Network Technology Co., Ltd." declares that this product is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

For the full RED DoC file, Please download it as follow web: https://www.flyingvoice.com

The wireless operation frequency:

WIFI:24012-2472MHz, Max output power ≤ 20dBm(E.I.R.P)

5150-5350MHz, Max output power ≤ 23dBm(E.I.R.P)

5470-5725MHz, Max output power ≤ 30dBm(E.I.R.P)

5725-5895MHz, Max output power ≤ 13.98dBm(E.I.R.P)

Restrictions in the 5 GHz band:

According to Article 10 (10) of Directive 2014/53/EU, the packaging shows that this radio equipment will be subject to some restrictions when placed on the market in Belgium (BE), Bulgaria (BG), the Czech Republic (CZ), Denmark (DK), Germany (DE), Estonia (EE), Ireland (IE), Greece (EL), Spain (ES), France (FR), Croatia (HR), Italy (IT), Cyprus (CY), Latvia (LV), Lithuania (LT), Luxembourg (LU), Hungary (HU), Malta (MT), Netherlands (NL), Austria (AT), Poland (PL), Portugal (PT), Romania (RO), Slovenia (SI), Slovakia (SK), Finland (FI), Sweden (SE), the United Kingdom (UK), Turkey (TR), Norway (NO), Switzerland (CH), Iceland (IS), and Liechtenstein (LI).

The WLAN function for this device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

AT	BE	BG	HR	CY	CZ	DK
EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL
PT	RO	SK	SI	ES	SE	UK(NI)

Catalogue

Chapter 1 Product Introduction ---- 1

Product Specifications ---- 2

Hardware Installation ---- 4

Preparation for Installation ---- 4

Installation Steps ---- 5

Chapter 2 Boot Configuration ---- 6

Boot ---- 7

1. LCD Display ---- 7

2.Web Access ---- 9

(1) User Role Classification ---- 9

Basic Configuration ---- 12

1. Modify the Account/Password ---- 12

4. Upload/Download Configuration File ---- 14

5. Upgrade Firmware ---- 14

6. Restore Factory ---- 15

7. Reboot ---- 16

Chapter3 Network Configuration ---- 18

WAN Port Configuration ---- 19

1. Set IPv4 Address ---- 19

2. View IP Information ---- 22

3. VLAN Configuration ---- 23

LAN Port Configuration ---- 24

Wireless Network Configuration ---- 26

1. Configure 2.4G band Wi-Fi ---- 26

2. Configure 5G band Wi-Fi ---- 27

Mesh Network Configuration ---- 29

Chapter 4 Function Configuration ---- 34

FXS Port Configuration ---- 35

1. SIP Account Registration ---- 35

2. View the Registration Information ---- 36

Log Setting and View ---- 38

Management Configuration ---- 41

1. Telnet Setting ---- 41

2. SSH Setting ---- 42

3. TR069 Configuration ---- 43

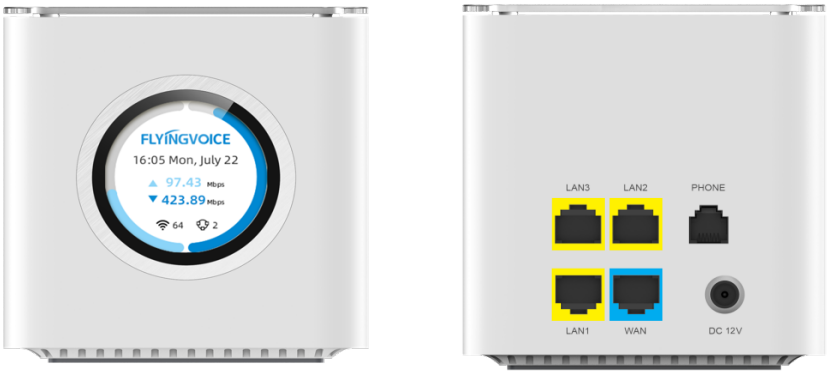
4. Provision Configuration ---- 44

Chapter 1 Product Introduction

This chapter contains the following:

- **Product Specifications**
- **Hardware Installation**

Product Specifications

Specification/ Model	SR3000
Photos	
Power	• 12V / 2A
LCD Screen	• 1.7-inch round touch color screen • Visually display time, up/downlink network speed, number of wireless terminals, Mesh agent status, etc.
Ethernet port	• 1*WAN, 10/100/1000Mbps, uplink to the Internet • 3*LAN, 10/100/1000Mbps, downlink to local network terminals, such as PC, IP phone, etc.
FXS Port	• 1*RJ11 FXS port, support access to analog phone or fire alarm panel.
WPS Button	• External to the bottom of the device, one-button mesh networking.
Reset Button	• External to the bottom of the device. • Long press for more than 5 seconds to support restoring factory settings. • Short press for 1 second to reboot the device.
WiFi6 Antenna	• 802.11 a/n/ac/ax, 2*2 MIMO, 1024-QAM@160MHz 2402Mbps, eFEM. • 802.11 b/g/n/ax, 2*2 MIMO, 1024-QAM@40MHz 573Mbps, eFEM.

EasyMesh	• Support "1+2" mesh networking of the controller and agent, extending network coverage area. • Support LCD one-touch connection and WPS one-button connection.
Network	• Support 2.4GHz & 5GHz Wi-Fi. • Support WPA-PSK/WPA2-PSK. • Support TKIP/AES.
Management	• Support Telnet, TR069, SSH.

Specification/ Model	**SR3000-lite**
Photos	
Power	• 12V / 2A
Network	• 1*WAN/LAN, 10/100/1000Mbps. • Support uplink to the Internet or downlink to the PC to access the web for configuration.
WiFi6 Antenna	• 802.11 a/n/ac/ax, 2*2 MIMO, 1024-QAM@160MHz 2402Mbps, eFEM. • 802.11 b/g/n/ax, 2*2 MIMO, 1024-QAM@40MHz 573Mbps, eFEM.
LED Indicator	• Red/green colors indicate device power-up, mesh connection status. • Red steady -- Booting/Rebooting/Resetting/Upgrading/Device disorder/Mesh failed. • Green steady -- Successful boot up/Mesh successful. • Red flashing slowly -- Network disconnected.

	• Green flashing slowly -- Network connected. • Red flashing fast -- Mesh connecting. • Off - Not power on.
WPS button	• External to the bottom of the device, one-button mesh networking.
Reset button	• External to the bottom of the device. • Long press for more than 5 seconds to support restoring factory settings. • Short press for 1 second to reboot the device.
EasyMesh	• Support "1+2" mesh networking of the controller and agent, expanding network coverage area. • Support WPS one-click connection.
Network	• Support 2.4GHz & 5GHz Wi-Fi. • Support WPA-PSK/WPA2-PSK. • Support TKIP/AES.
Management	• Support Telnet, TR069, SSH.

Hardware Installation

Preparation for Installation

Before installing the equipment, please check whether the items are complete and whether the installation conditions are available. Open the packing box of the equipment and check whether the items in the box are complete against the list of items. If you find that the items in the box do not match the list, please contact us directly.

Attention

- The installation location should be equipped with conditions for connecting the equipment to the outside (e.g., power cord, network cable, PC, etc.), and the AC power outlet should be a single-phase, three-pronged power outlet, and ensure that the ground wire is reliably grounded.
- The environment of the installation location should ensure sufficient air flow to facilitate the heat dissipation of the equipment (the appropriate operating temperature of the equipment is 0℃ ~ 50℃).
- The installation location should be waterproof, moisture-proof, lightning and other conditions (equipment suitable for environmental humidity of 10% to 90%).

Installation Steps

Before setting up your router, you must properly connect your device:

- Connect the WAN port of the device to the modem with an Ethernet cable.

- Connect your computer to the LAN port of the device with an Ethernet cable.

- Connect one end of the power cable to the device's power connector and the other end to a power outlet.

- Start the router.

- Check that the power supply, LCD and LED are working properly.

Warning

- Do not attempt to use a power adapter that does not come standard and do not unplug the power supply while configuring or changing the device.
- Using another power adapter may damage the device and will void the manufacturer's warranty.

Chapter 2 Boot Configuration

This chapter contains the following:

- **Boot**
- **Basic Configuration**

Boot

After the device is powered up and networked successfully, users can confirm the device initialization status and obtain the network configuration by viewing the device's LCD display (SR3000 only), LED indicators (SR3000-lite only), or by accessing the device's web.

1. LCD Display

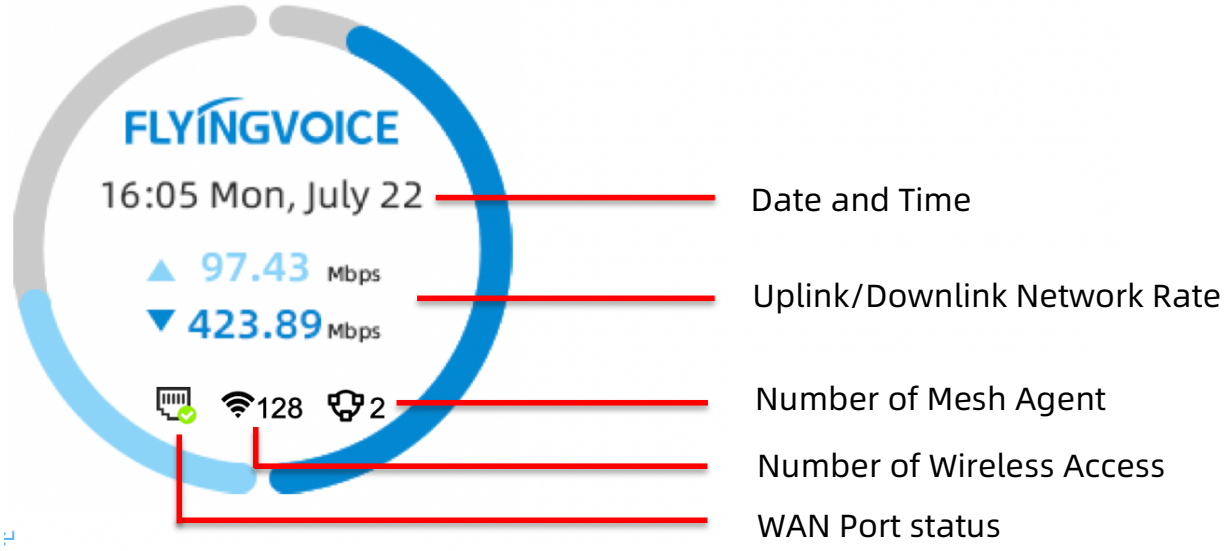
When the SR3000 is powered on, the boot loading progress bar is automatically displayed, and then analyze the current Wi-Fi environment. as shown in the following figure:

After the progress is loaded, it will automatically jump to the language selection interface, which currently supports only 2 languages: English (default), Simplified Chinese.

As shown in the figure below:

After the language selection is completed, it automatically jumps to the standby interface,

as shown in the following figure:



Parameters	Description
Date and Time	Real-time display of the current local date and time.
Uplink/Downlink Network Rate	Display the data transfer rate of uplink and downlink of the device in real time. The half circles on the left and right sides also dynamically display the corresponding network speed percentage.
Number of Mesh Agent Routes	Display the number of agent routes in the Mesh network.
Number of Wireless Access Terminals	Display the number of wireless access terminals through the Wi-Fi in real time.

WAN Port Status	Display the WAN port link status and network status of the device: : Linked with Internet access. : Linked without Internet access. : Dislinked.

2.Web Access

SR3000 and SR3000-lite support Web Login access.

After the device is powered on, user can connect to a PC through the LAN port and can access the IP address (192.168.1.1) to log in to the web interface for viewing or configuration.

(1) User Role Classification

Access to the web interface is only one user level of management: Administrator.

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

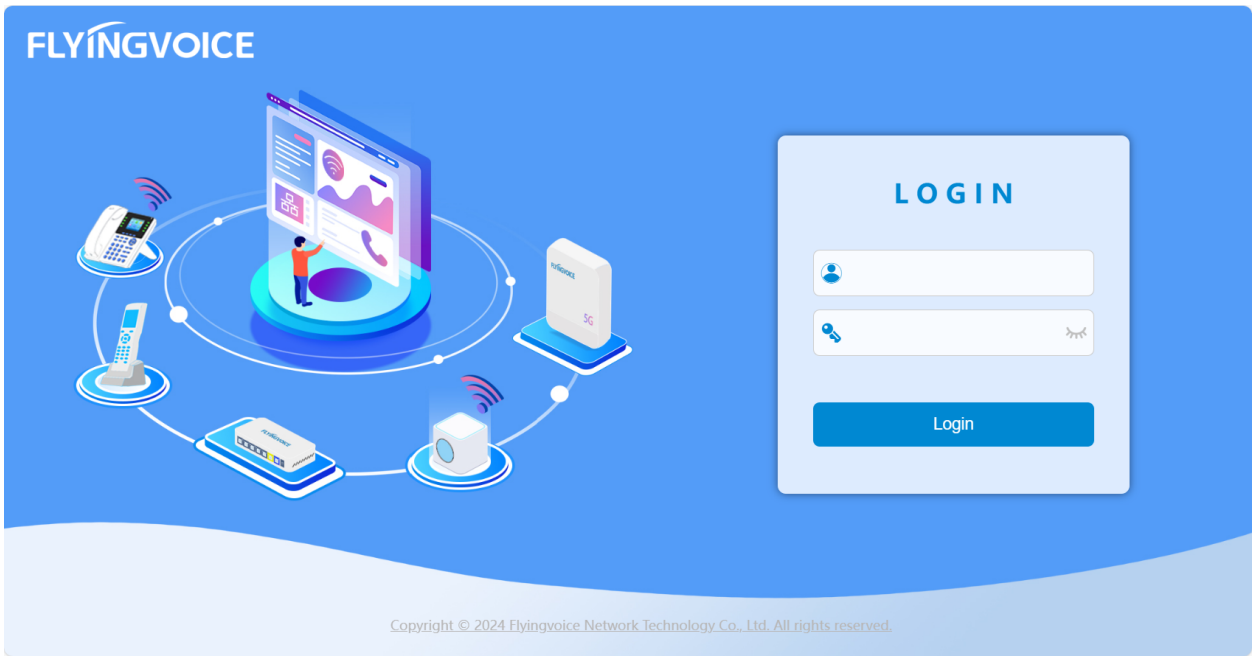
for the highest permissions, can view and configure all pages.

(2) Web Login

Ensure that the PC is properly connected to the LAN port of the device. The device has a built-in web server to respond to HTTP get/post requests, and users can access the web through the browser.

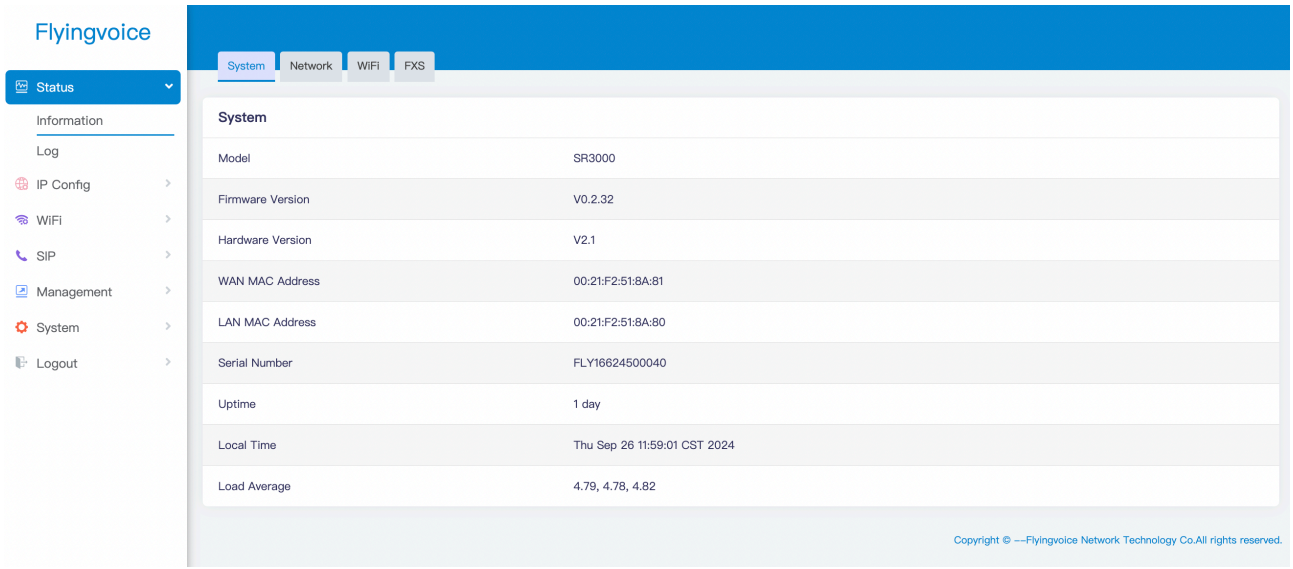
Enter the IP address (default 192.168.1.1) in the address bar of the browser on the PC, and the system will jump to the web login page,

as shown in the following figure:



User enters the account and password according to the role level, and the system automatically jumps to the status information page that indicates after successful login,

as shown in the following figure:



Parameter	Description
Model	Display the product model of the current device, which cannot be modified.
Firmware Version	Display the firmware version of the device, which can be upgraded on demand.
Hardware Version	Display the hardware version of the device's current internal hardware PCBA.

WAN MAC Address	Display the MAC address of the WAN port of the device, which is fixed by factory default.
LAN MAC Address	Display the MAC address of the LAN port of the device, which is fixed by factory default.
Serial Number	Display the factory serial number of the device.
Uptime	Display the time since the device first start.
Local Time	Display the current local time and date.
Average Load	Display the average load of the device over 3 time periods: Within the last 1 minute, within the last 5 minutes, and within the last 15 minutes.

Basic Configuration

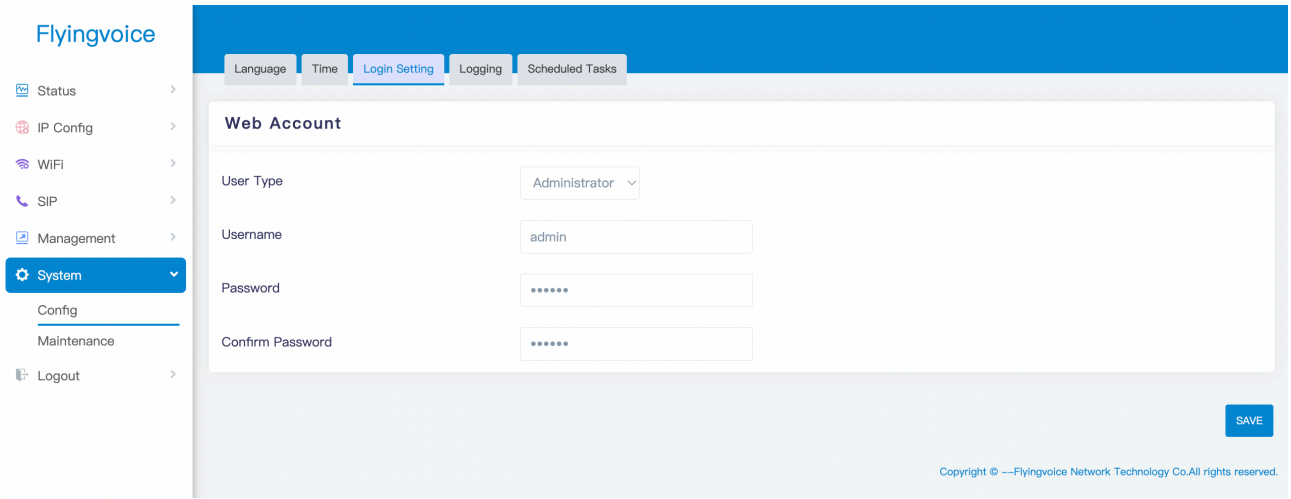
After the device boots up successfully, it supports logging into the Web to configure basic functions, including account/password modification, language modification, local time synchronization, upload/download configuration file, upgrade firmware, rebooting or restore factory setting.

1. Modify the Account/Password

This function privilege only applies to the administrator role. After logging in to the web, users can change the account and password of administrator and user.

Path: **System** -> **Config** -> **Login Setting** -> **Web Account**,

as shown in the following figure:



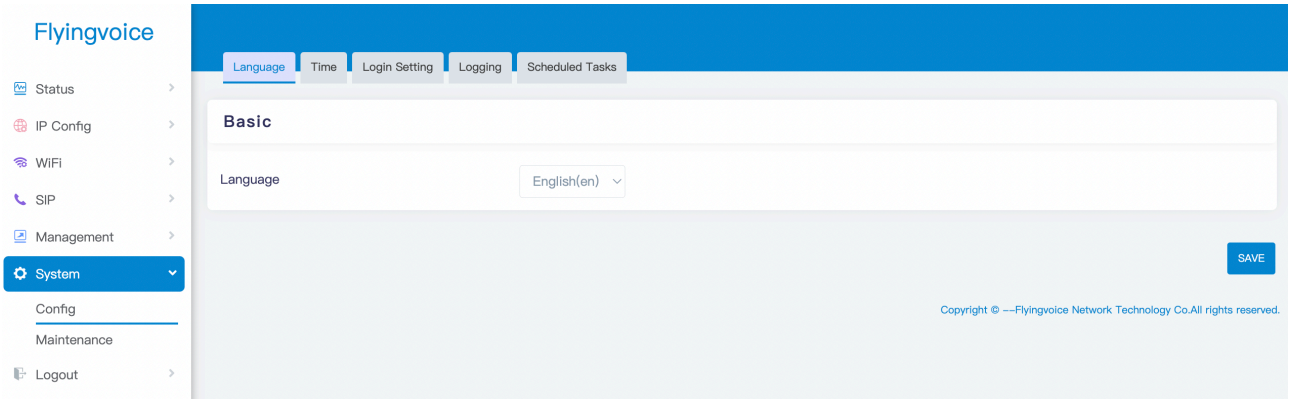
Parameter	Description
User Type	You can choose to the user level of the account: Administrator.
Username	Fill in the modified new username.
Password	Fill in the new modified password.
Confirm Password	Fill in the new modified password again to ensure consistency.

2. Modify the Language

User can modify the display language of the web page after logging in to the Web.

Path: **System** -> **Config** -> **Language**,

as shown in the following figure:



Parameters	Description
Language	You can modify the language of the system web display: Simplified Chinese, English.

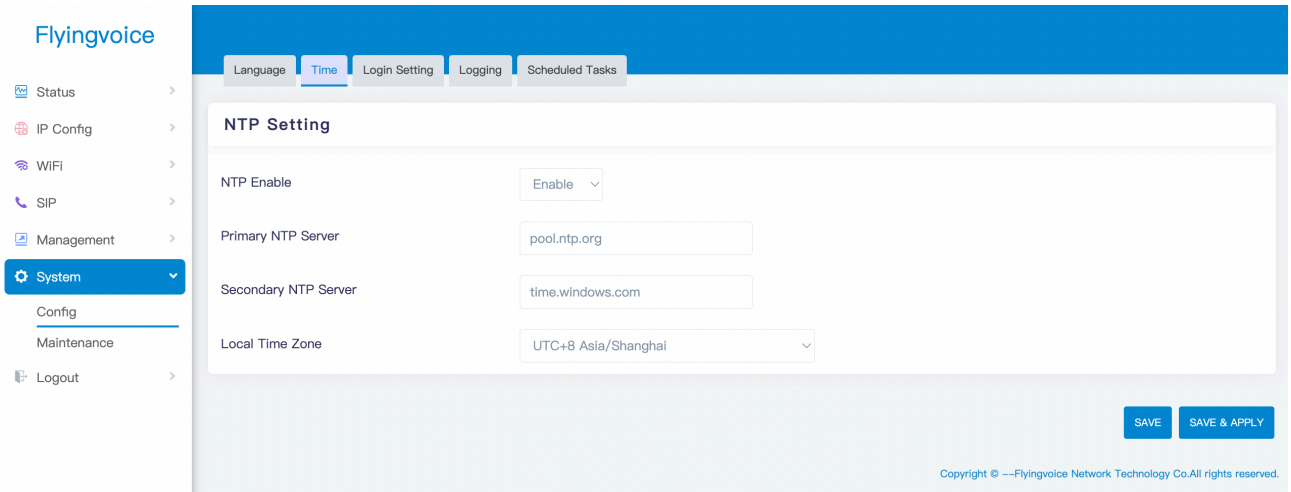
Note: The SR3000's LCD display will also change the language setting synchronously.

3. Setting Time and Date

User can modify the time and date after logging in to the web.

Path: **System** -> **Config** -> **Time** -> **NTP Setting**,

as shown in the following figure:



Parameters	Description

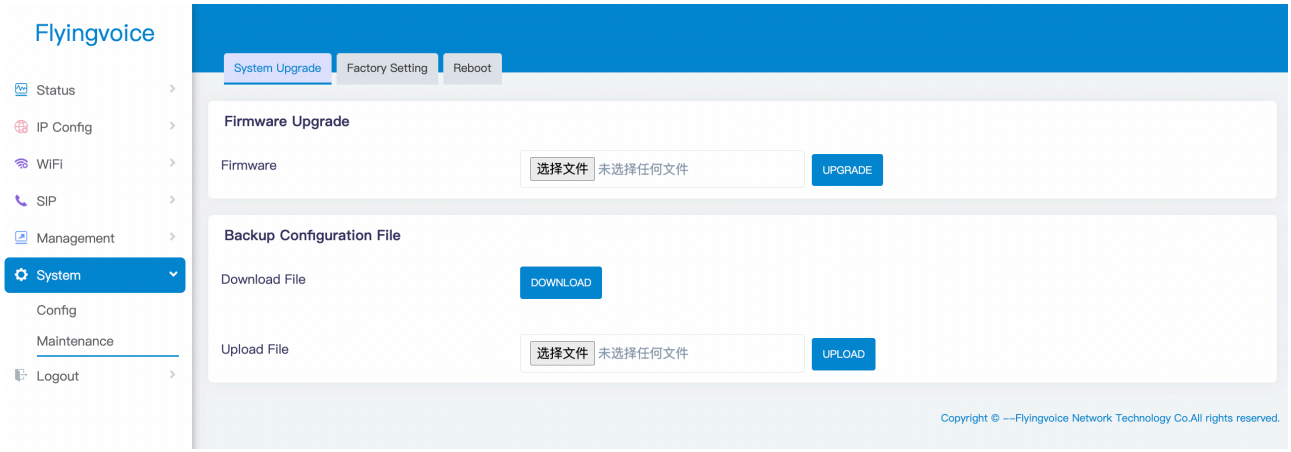
NTP Enable	Optional enable or disable NTP settings to synchronize the current network time.
Primary NTP server	Fill in the modified primary NTP server address for time synchronization.
Secondary NTP server	Fill in the modified Secondary NTP server address for backup.
Local Time Zone	UTC time zone, optional the corresponding country and region, default is UTC-5 American New York.

4. Upload/Download Configuration File

After logging in to the web, user can download the configuration file of the current device, set the function parameters in batch and then upload to the device.

Path: **System** -> **Maintenance** -> **System Upgrade** -> **Backup**,

as shown in the following figure:



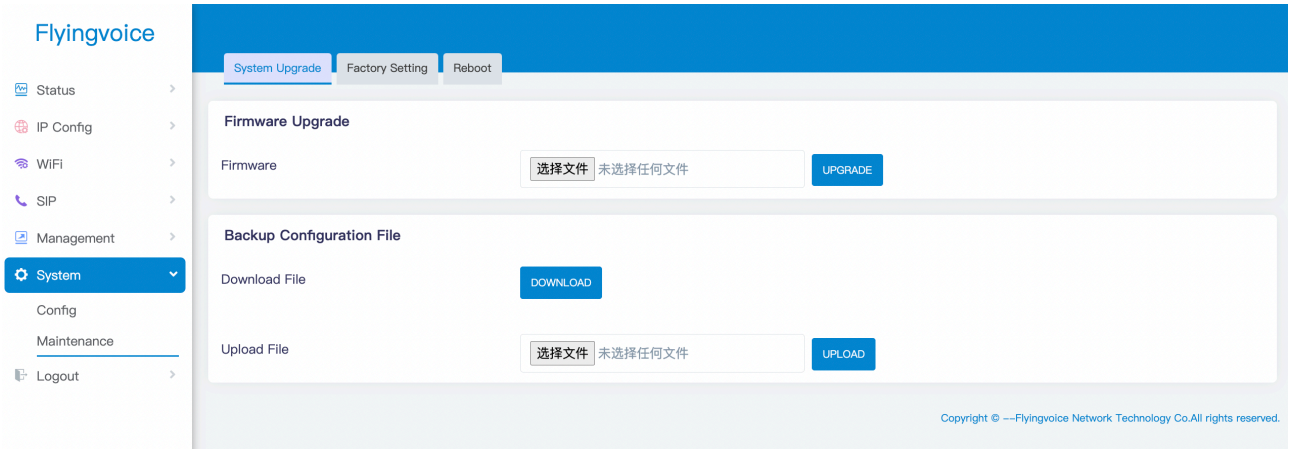
Parameters	Description
Download File	Download the current configuration file of the device with one click. User can view the configuration parameters and corresponding values or use it as a configuration file template to modify and upload again.
Upload File	One-click to select a local file and then upload it.

5. Upgrade Firmware

After logging in to the web, user can choose to manually upgrade or downgrade the firmware version of the device.

Path: **System** -> **Maintenance** -> **System Upgrade** -> **Firmware Upgrade**,

as shown in the following figure:



Parameters	Description
Firmware	One-click to select a local firmware file and then upload it.

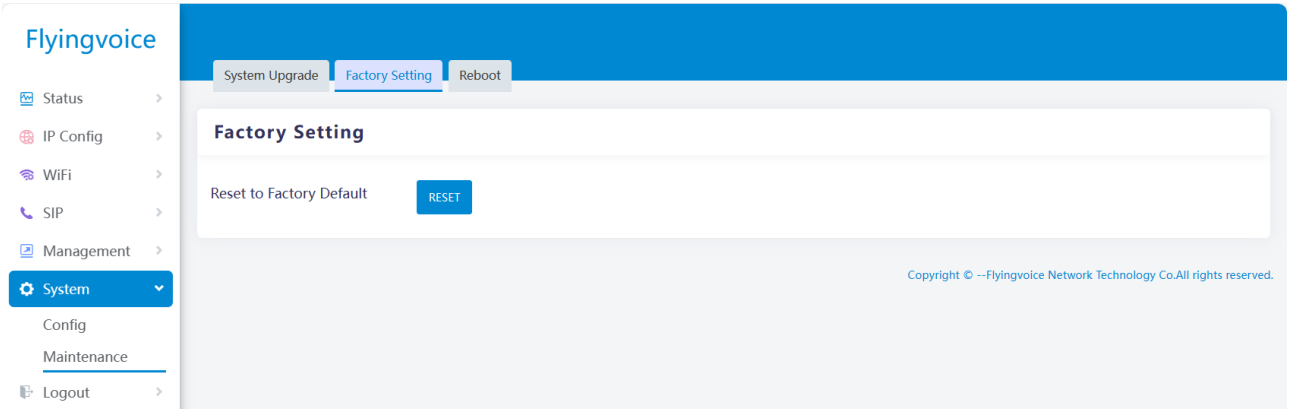
Note: User is generally not supported to upgrade or downgrade the firmware version at will, which may result in the device not being able to boot up. If you need to refresh the version, please contact us to get the firmware file. Please do not disconnect the device from power and network during the upgrade process.

6. Restore Factory

User can set the device to factory status with one click after logging in to the web, or by long pressing the reset button at the bottom of the device for more than 5 seconds.

Path: **System**-> **Maintenance**-> **Factory Setting**,

as shown in the following figure:



Parameters	Description
Factory Setting	Set the device to factory status with one click.

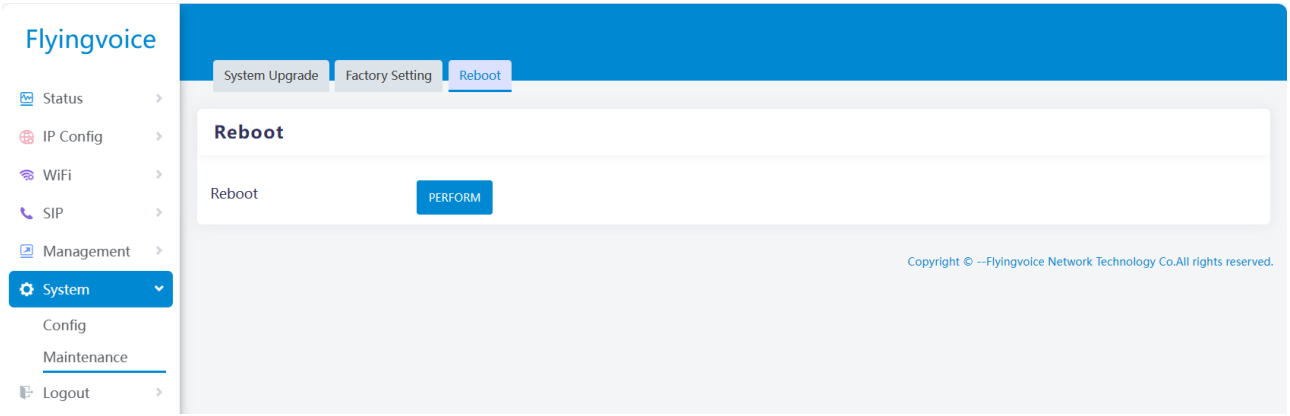
Note: Do not disconnect the device from power and Internet during the process of restoring the device to the factory.

7. Reboot

User can reboot the device with one click after logging in to the web, or by short pressing the reset button at the bottom of the device for 1 second. And it also supports schedule reboot by once / every day / every week.

(1) Path: **System** -> **Maintenance** -> **Reboot**,

as shown in the following figure:

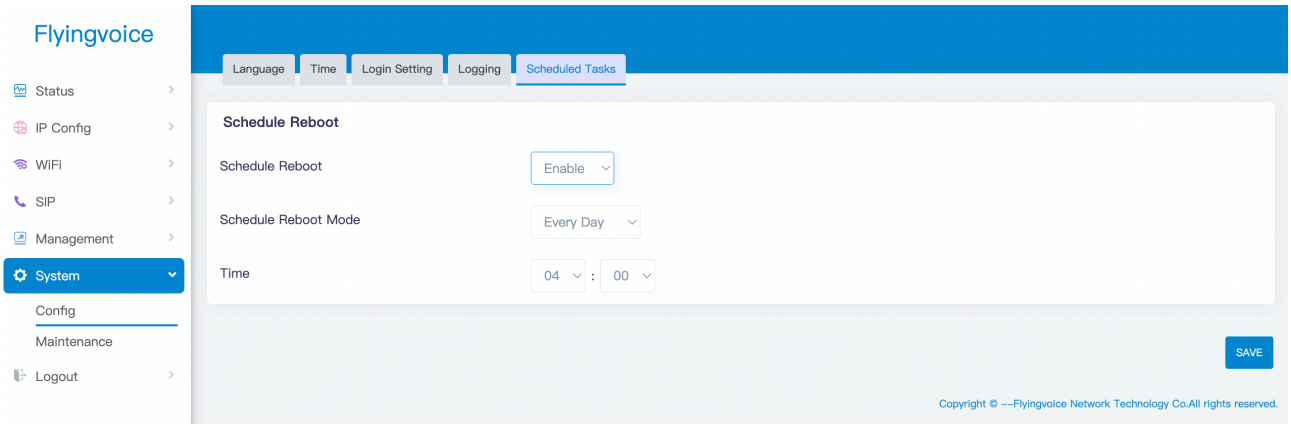


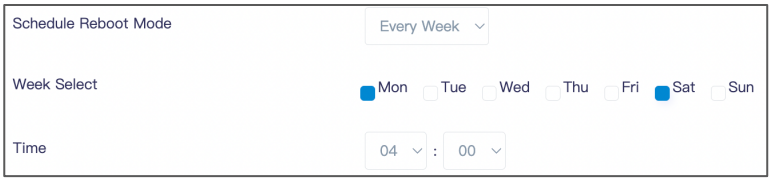
Parameters	Description
Reboot	Reboot the device with one click.

Note: Do not disconnect the device from power and Internet during the process of rebooting.

(2) Path: **System** -> **Config** -> **Schedule Tasks**:

as shown in the following figure:



Parameters	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.

Chapter3 Network Configuration

This chapter contains the following:

- WAN Port Configuration
- LAN Port Configuration
- Wireless Network Configuration
- Mesh Network Configuration

WAN Port Configuration

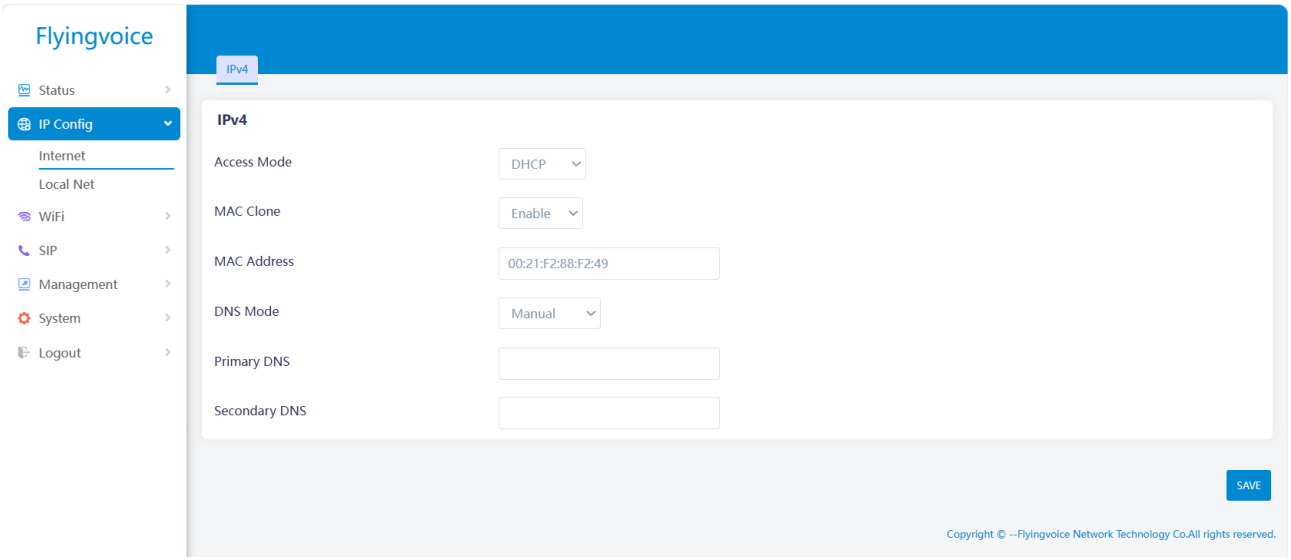
The device supports setting IPv4 address of WAN port, and user can set IP-related information manually or automatically by setting the network access method. Currently, it supports DHCP, static IP, and PPPoE.

1. Set IPv4 Address

Path: **IP Config**-> **Internet**-> **IPv4**

（1）DHCP mode

By default, the SR3000 accesses the Internet in DHCP mode and automatically obtains the IPv4 address of the WAN port.

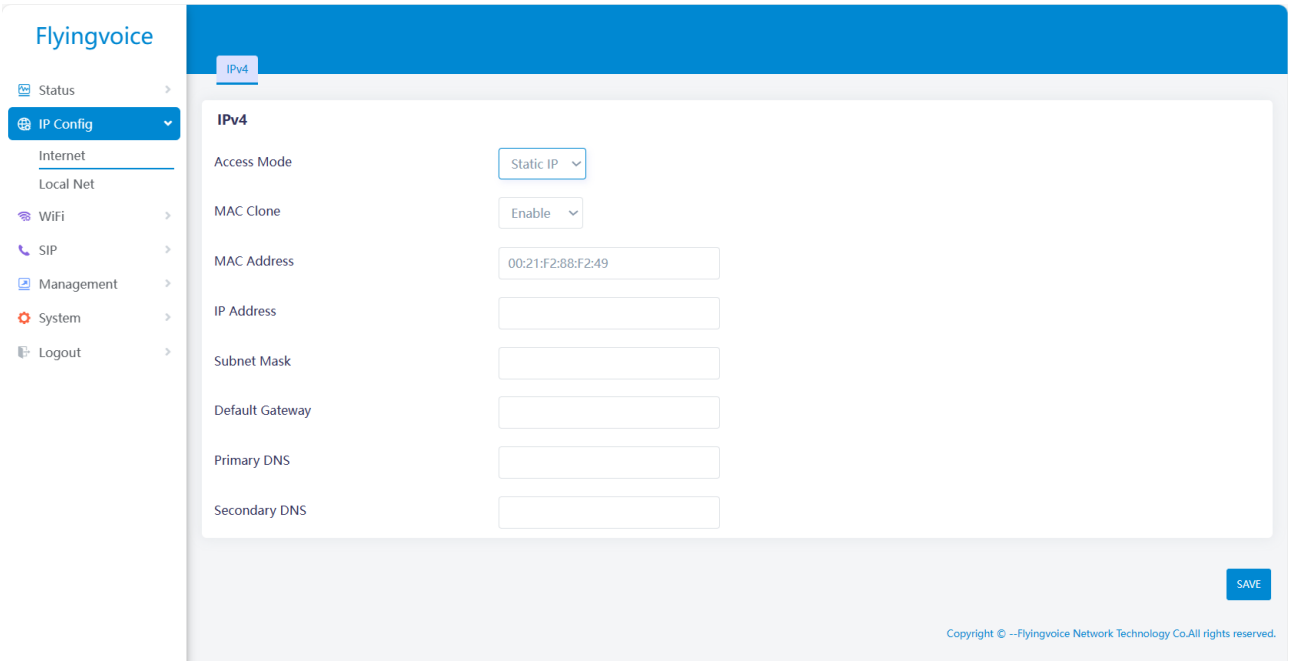


Parameters	Description
Access Mode	The default mode is DHCP.
MAC Clone	Optional enable or disable MAC Clone. After enable the function, you need to fill in the MAC Address.
MAC Address	Fill in the modified MAC address as the MAC address of the WAN port.
DNS Mode	Optional a mode: Auto, Manual.

	After choosing the Manual mode, you need to fill in the Primary DNS & Secondary DNS.
Primary DNS	Fill in the Primary DNS.
Secondary DNS	Fill in the Secondary DNS for backup.

（2）Static IP mode

You can use this configuration when you receive a fixed public IP address or a public subnet from your Internet provider. In most cases, a cable service provider will provide a fixed public IP, while a DSL service provider will provide a public subnet. If you have a public subnet, you can assign an IP address to the WAN port.

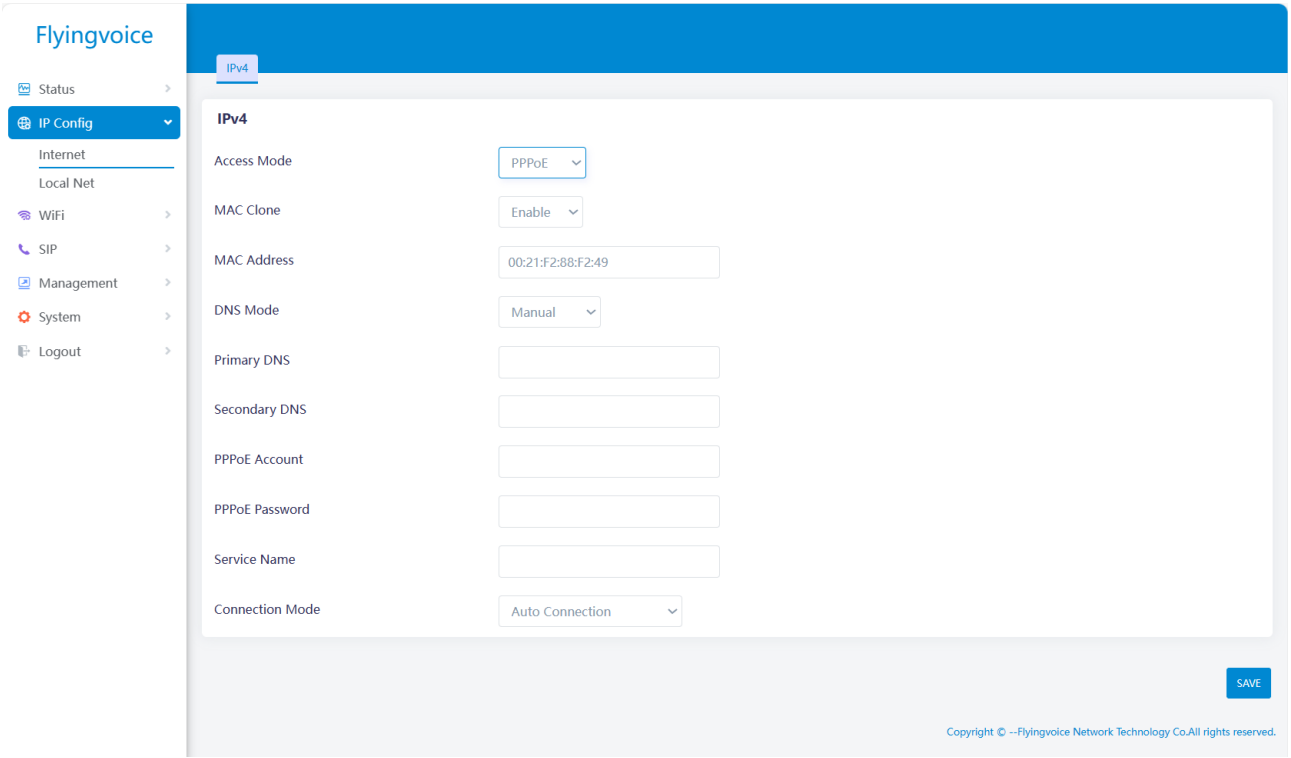


Parameters	Description
Access Mode	The default mode is DHCP. Select the Static IP mode.
MAC Clone	Optional enable or disable MAC Clone. After enable the function, you need to fill in the MAC Address.
MAC Address	Fill in the modified MAC address as the MAC address of the WAN port.
IP Address	Fill in the IPv4 address specified by the user. Supports IP conflict detection. If the static IP address is on the same network segment as the LAN interface or DHCP address pool, the system prompts you to automatically avoid using another private IP address.

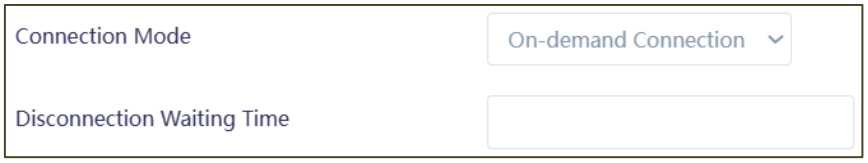
Subnet Mask	Fill in the subnet mask of the IPv4 address.
Default Gateway	Fill in the local gateway address.
Primary DNS	Fill in the Primary DNS.
Secondary DNS	Fill in the Secondary DNS for backup.

（3）PPPoE mode

PPPoE is mostly used for DSL modem users, ISP provide information about usernames, passwords, and authentication modes, and all local users can share a PPPoE public connection to access the Internet.



Parameters	Description
Access Mode	The default mode is DHCP. Select the PPPoE mode.
MAC Clone	Optional enable or disable MAC Clone. After enable the function, you need to fill in the MAC Address.
MAC Address	Fill in the modified MAC address as the MAC address of the WAN port.
DNS Mode	Optional a mode: Auto, Manual. After choosing the Manual mode, you need to fill in the Primary DNS & Secondary DNS.

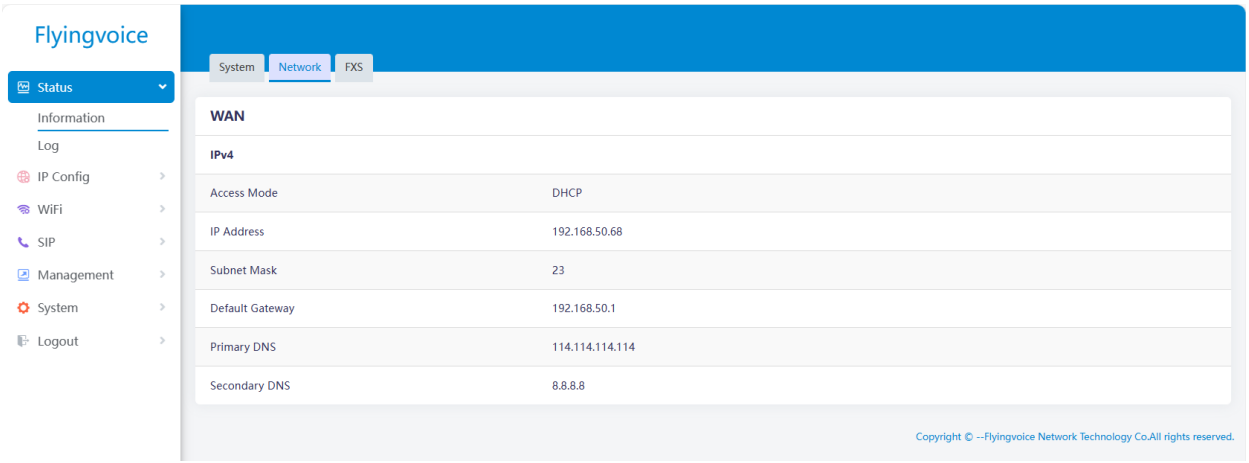
Primary DNS	Fill in the Primary DNS.
Secondary DNS	Fill in the Secondary DNS for backup.
PPPoE Account	Fill in the PPPoE account obtained from the ISP.
PPPoE Password	Fill in the PPPoE password obtained from the ISP.
Service Name	Fill in the PPPoE authentication service name. If it is empty, the service name is automatically detected.
Connection Mode	Optional a mode: Auto Connection, On-demand Connection, Timed Connection. After choosing On-demand Connection mode, you need to fill in the Disconnection Waiting Time, and the device will dial the connection automatically when there is access data, and if there is no data, the network connection will be automatically disconnected within the set time.  After choosing Timed Connection mode, you need to set the Time Period, and the device will dial the connection automatically within the set time only.

2. View IP Information

After configuring the IP information of the WAN port, user can view it on the web status page.

Path: **Status**-> **Information**-> **Network**-> **WAN**,

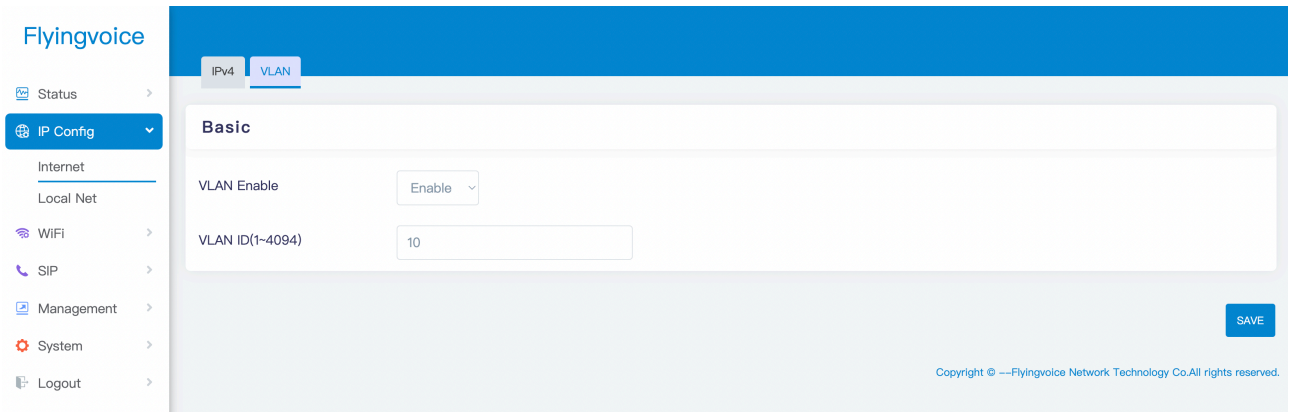
as shown in the following figure:



3. VLAN Configuration

Supports VLAN configuration based on WAN port and it achieves access to VLAN in office.

Path: **IP Config**->**Internet**->**VLAN**, as shown in the figure below:



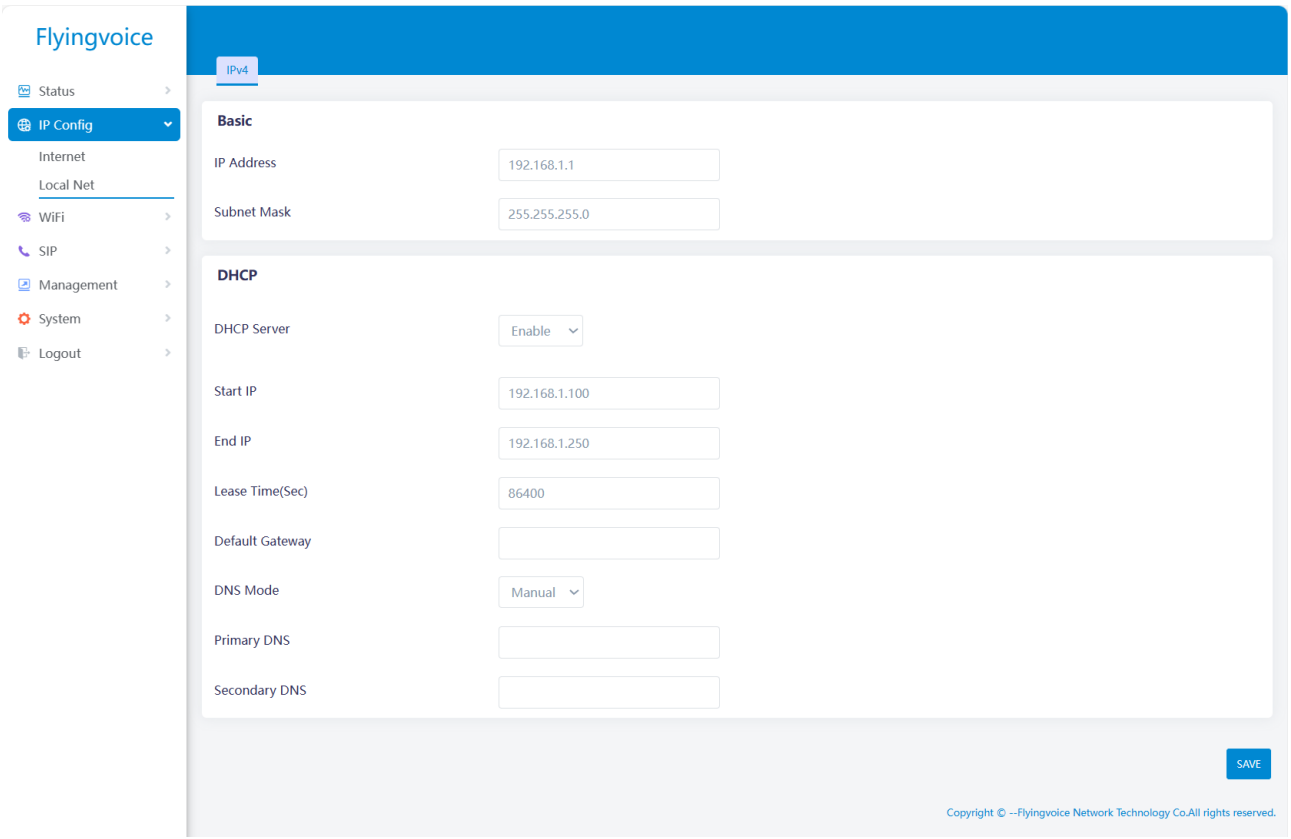
Parameters	Description
VLAN Enable	Optional enable or disable the VLAN function, the default is disable.
VLAN ID	Fill in the VLAN ID in the network environment that the user wants to join, with a limit range of 1 to 4094. After the setting is completed, you can join the network segment of the VLAN and can access the IP address.

LAN Port Configuration

SR3000 supports acting as a DHCP server to set the IPv4 address of the LAN port and can assign IP addresses to the terminal devices connected to the LAN ports.

1. Set IPv4 Address

Path: **IP Config**-> **Local Network**-> **IPv4**



Parameters	Description
IP Address	Fill in the local IPv4 address of the device on the LAN. The default IP is 192.168.1.1. Supports IP conflict detection. If the static IP address is on the same network segment as the WAN interface, the system prompts you to automatically avoid using another private IP address.
Subnet Mask	Fill in the subnet mask to determine the network size, the default is 255.255.255.0.

DHCP Server	Optional enable or disable the DHCP Server. After the DHCP server is enabled, you need to create a DHCP address pool.
Start IP	Fill in the DHCP start IP of the address pool. Fill in a valid IP address as the start IP address sent by the DHCP server to the DHCP client. If the IP address of the LAN port is 192.168.1.1, the start IP address must be greater than or equal to 192.168.1.2 but smaller than the end IP address.
End IP	Fill in the DHCP end IP. Fill in a valid IP address as the end IP address sent by the DHCP server to the DHCP client.
Lease Time	Fill in the validity period of the IP address assigned by the DHCP server to the device. During this time, the server will not assign the IP address to other devices.
Default Gateway	Fill in the Default Gateway.
DNS Mode	Optional a mode: Auto, Manual. After choosing the Manual mode, you need to fill in the Primary DNS & Secondary DNS.
Primary DNS	Fill in the Primary DNS.
Secondary DNS	Fill in the Secondary DNS for backup.

Wireless Network Configuration

After the device is powered on and started, the wireless network (dual-band 2.4GHz & 5GHz) is enabled by default and is supported wireless access by the terminal devices.

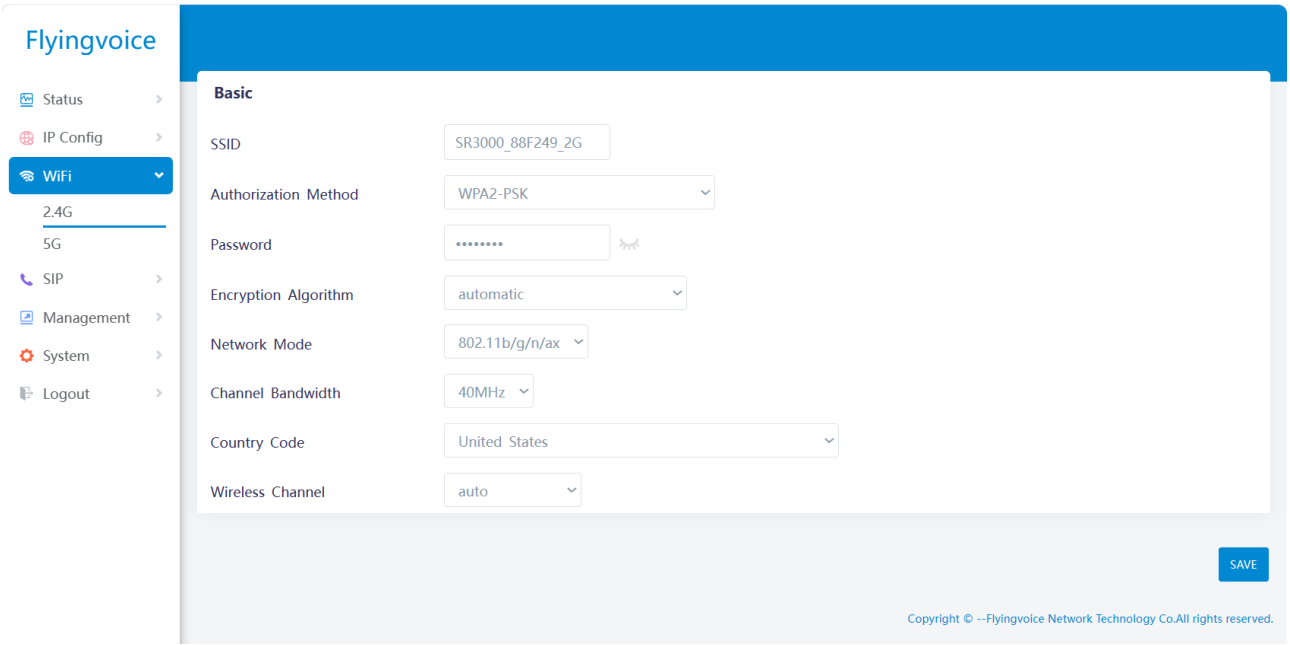
After logging in to the web, user can modify the SSID, password, encryption algorithm of Wi-Fi, etc.

Note: The initial SSID and password are posted on the bottom of the device, user can check them.

1. Configure 2.4G band Wi-Fi

Path: **Wi-Fi**-> **2.4G**,

as shown in the following figure:



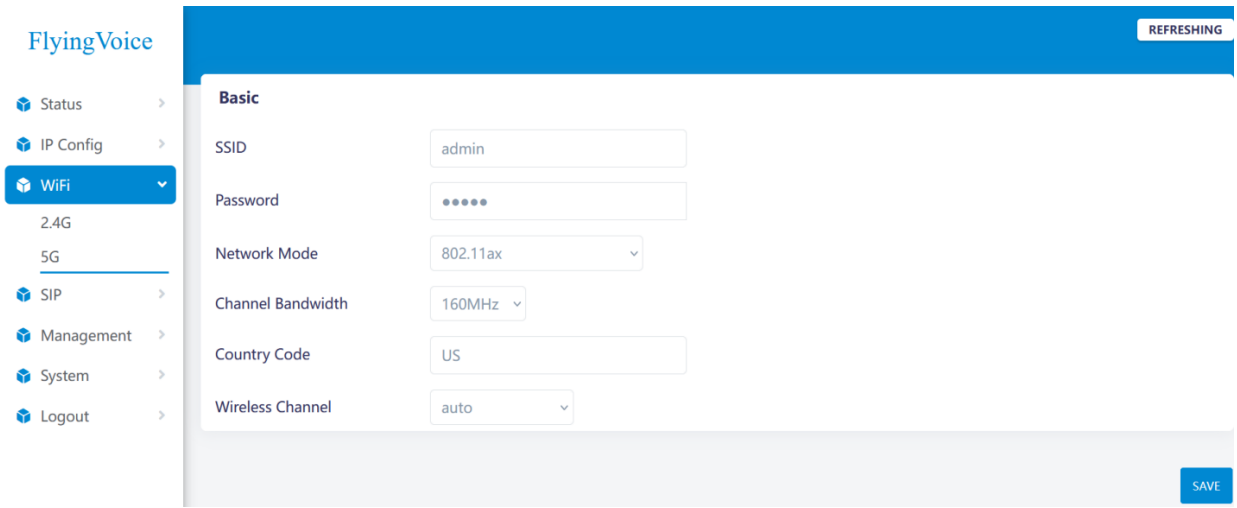
Parameters	Description
SSID	Fill in the name of 2.4G band Wi-Fi, the default is SR3000_MAC after six digits_2G.

Authorization Method	Optional a method: WPA-PSK, WPA2-PSK, WPA-PSK/WPAs-PSK mix mode or no encryption. Choose an appropriate authorization method to improve the security and privacy of your wireless data packets.
Password	Fill in the password of 2.4G band Wi-Fi, the default is SN after eight digits.
Encryption Algorithm	Optional an Encryption Algorithm: CCMP(AES), TKIP/CCMP(AES) mixed mode or Auto.
Network Mode	Optional network modes for 2.4G band Wi-Fi: 802.11g、802.11b/g/n、802.11b/g/n/ax; 802.11g: Support 2.4G bands only, with a maximum theoretical rate of 54Mbps. 802.11b/g/n: Compatible with 802.11b, 802.11g and 802.11n, support 2.4G and 5G bands, with a maximum theoretical rate of 600Mbps. 802.11b/g/n/ax: Compatible with 802.11b, 802.11g, 802.11n and 802.11ax, support 2.4G and 5G bands, with a maximum theoretical rate of 9607.8Mbps.
Channel Bandwidth	Bandwidth of optional 2.4G band Wi-Fi: 20MHz, 40MHz.
Country Code	Optional the country area and choose the local supported wireless channel according to the selected country.
Wireless Channel	Optional wireless channel for 2.4G band Wi-Fi, the default is Auto.

2. Configure 5G band Wi-Fi

Path: **Wi-Fi**-> **5G**,

as shown in the following figure:



Parameters	Description
SSID	Fill in the name of 5G band Wi-Fi, the default is SR3000_MAC after six digits_5G.
Authorization Method	Optional a method: WPA-PSK, WPA2-PSK, WPA-PSK/WPAs-PSK mix mode or no encryption. Choose an appropriate authorization method to improve the security and privacy of your wireless data packets.
Password	Fill in the password of 5G band Wi-Fi, the default is SN after eight digits.
Encryption Algorithm	Optional an Encryption Algorithm: CCMP(AES), TKIP/CCMP(AES) mixed mode or Auto.
Network Mode	Optional network modes for 5G band Wi-Fi: 802.11a/n, 802.11a/n/ac, 802.11a/n/ac/ax. 802.11a/n: Compatible with 802.11a and 802.11n, support 2.4G and 5G bands, with a maximum theoretical rate of 600Mbps. 802.11a/n/ac: Compatible with 802.11a, 802.11n and 802.11ac, support 2.4G and 5G bands, with a maximum theoretical rate of 600Mbps. 802.11a/n/ac/ax: Compatible with 802.11a, 802.11n, 802.11ac and 802.11ax, support 2.4G and 5G bands, with a maximum theoretical rate of 9607.8Mbps.
Channel Bandwidth	Bandwidth of optional 5G band Wi-Fi: 20MHz, 40MHz, 80MHz, 160MHz.
Country Code	Optional the country area and choose the local supported wireless channel according to the selected country.
Wireless Channel	Optional wireless channel for 5G band Wi-Fi, the default is Auto.

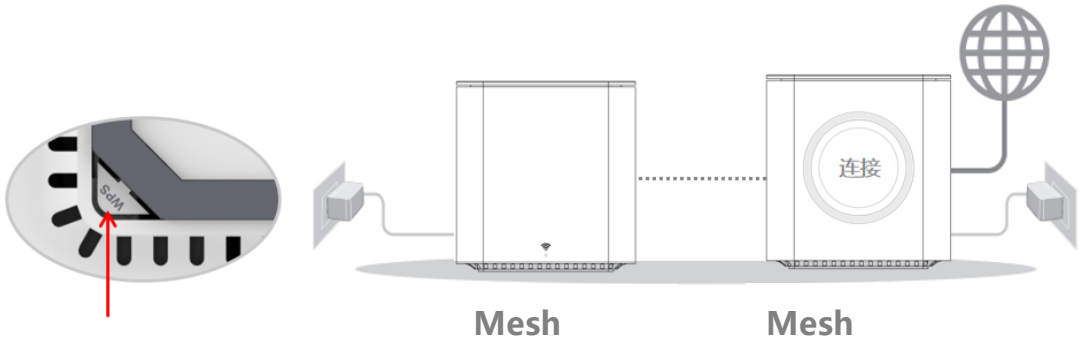
Mesh Network Configuration

The device supports mesh wireless networking with controller and agent router and supports up to "1+2" combination at present. After successful network configuration, user can view the network information of controller and agent routers, and effectively expand network coverage, support roaming switching of terminal devices, applicable to enterprises, homes and other types of households.

Users can configure SR3000 through the LCD, WPS button, and web interface.

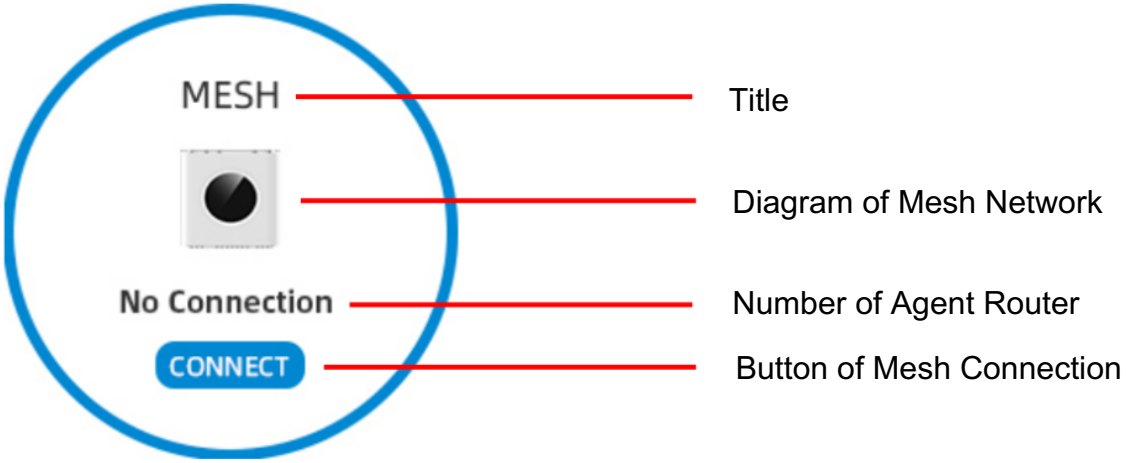
1. Mesh Networking Configuration by LCD

Note: This method is only applicable when SR3000 is used as the controller router, as shown in the following figure:



After SR3000 is normally powered up and networked, user can slide up and down to switch the LCD display content, if it is in the default standby page, just slide down a page,

as shown in the following figure:



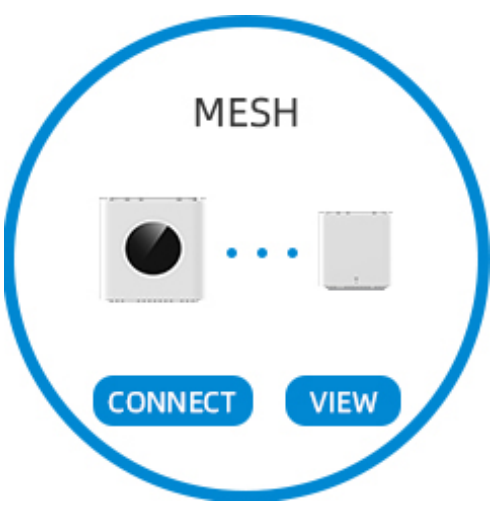
Parameters	Description
Title	Display the current page for the mesh networking setting.
Diagram of Mesh Network	Display the diagram of the mesh networking status, in this figure, there is no mesh networking. If the mesh networking is successful, it will display the diagram of 2 or 3 devices connected.
Number of Agent Router	Display the current number of mesh agent router, in this figure, there is no agent router to access the network.
Button of Mesh Connection	Trigger the mesh scanning with one click, and it will automatically jump to the scanning loading page.

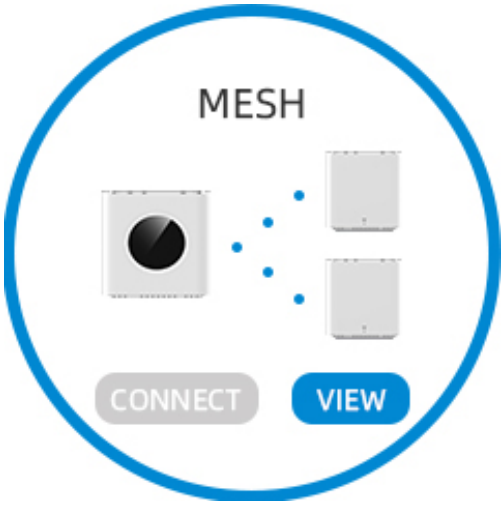
After user clicks Mesh connection button on LCD and presses WPS button at the bottom of agent router, and the controller router will scan and connect automatically, then the connection result will be displayed on LCD synchronously, as shown in the following figure:

Parameters	Description
Connection Successful	After normal connection, LCD will show connection successful and jump to Mesh page automatically after 2 seconds.
Connection Failed	If the connection is abnormal (e.g. the controller and agent routers are temporarily disconnected, or they are too far away to scan, etc.), LCD will display connection failed and need to manually click the Back button, so that user can reconnect again.

When Mesh networking is successful, it jumps to Mesh page,

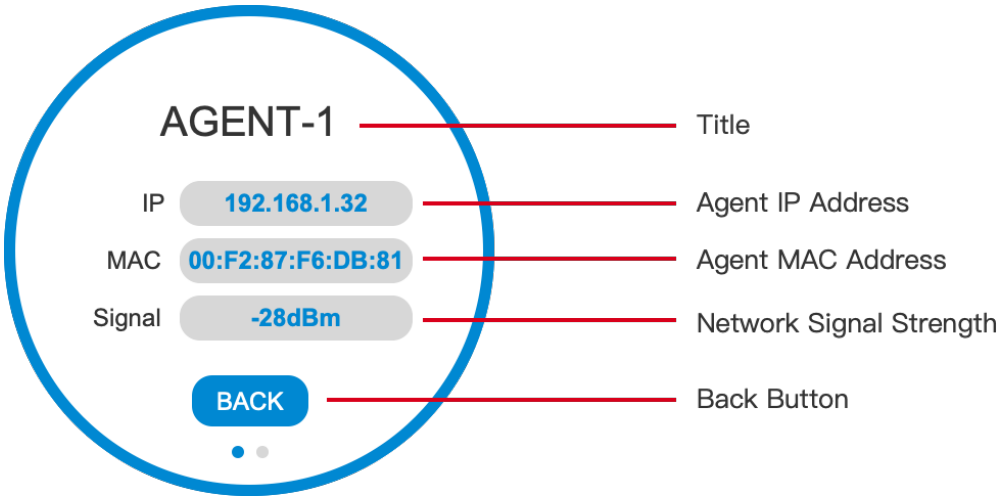
as shown in the following figure:





Parameters	Description
View Button	After successful Mesh connection, user can view the status information of the agent router in the agent router page after clicking the button.

Agent Router Information page, as shown in the following figure:

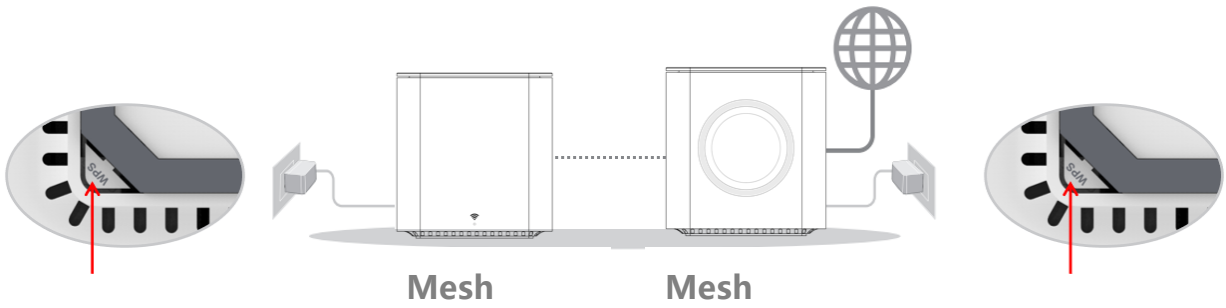


Parameters	Description
Title	The maximum number of agent router in mesh network is 2. This figure shows that the first agent router's information page, and user can swipe left and right to switch to view the information page of the second agent router.
Agent IP Address	Display the IP address of the agent router.
Agent MAC Address	Display the MAC address of the agent router.
Network Signal Strength	Real-time display of the wireless network signal strength of the agent router.
Return Button	One click returns to the previous Mesh page.

2. Mesh Networking Configuration by WPS Button

Note: This method is applicable to any networking method of SR3000 and SR3000-lite,

as shown in the following figure:



Any model of controller and agent router, while pressing the WPS button on the bottom of the device, the device will automatically scan and connect.

The connection result can be viewed via LCD (SR3000 only) and LED indicator (SR3000-lite only).

3. Mesh Networking Configuration by Web Interface

After logging in to the web, user can configure the mesh networking and view the network topology and network status information of the controller and agent routers in the web page.

It is not currently supported, please look forward to it.

Chapter 4 Function Configuration

This chapter contains the following:

- FXS Port Configuration
- Log Setting and View
- Management Configuration

FXS Port Configuration

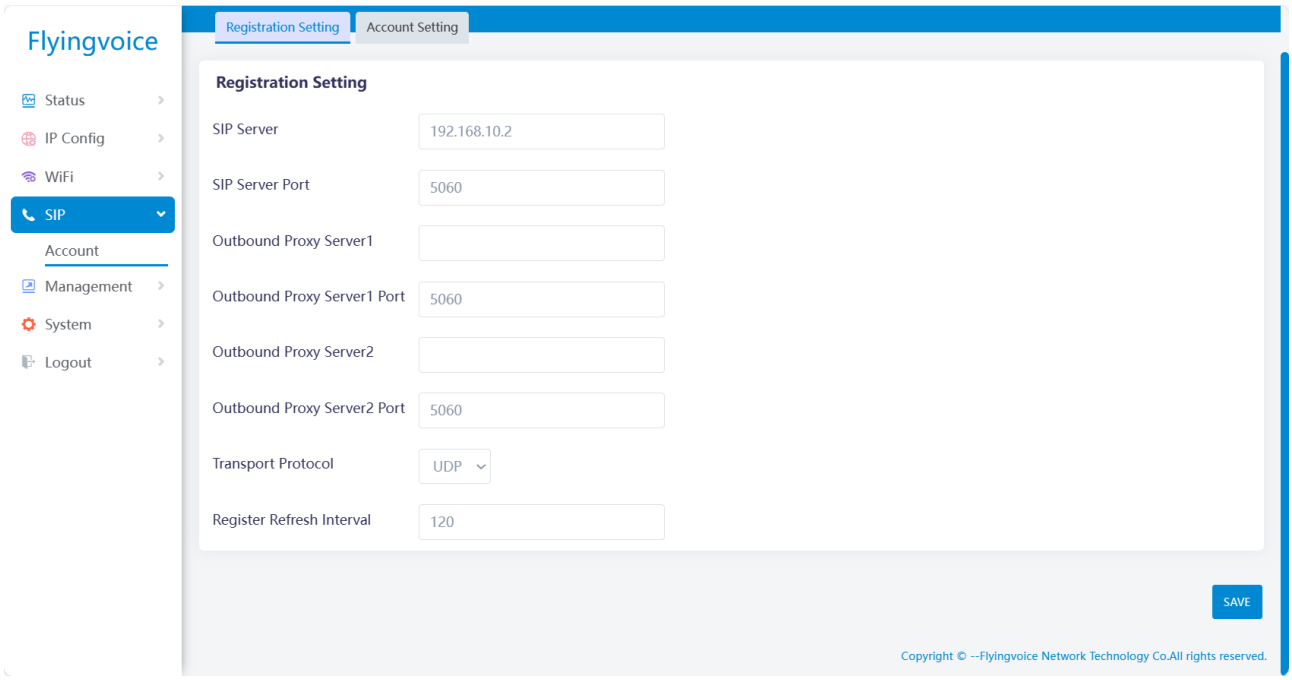
The device integrates 1 FXS port and supports registration of 1 SIP account, which can be externally connected to the analog phone, fax machine, fire/burglar alarm panel to send down the account to realize analog line to IP call.

Note: This feature is only supported by SR3000.

1. SIP Account Registration

Path: **SIP->Registration Setting**,

as shown in the following figure:

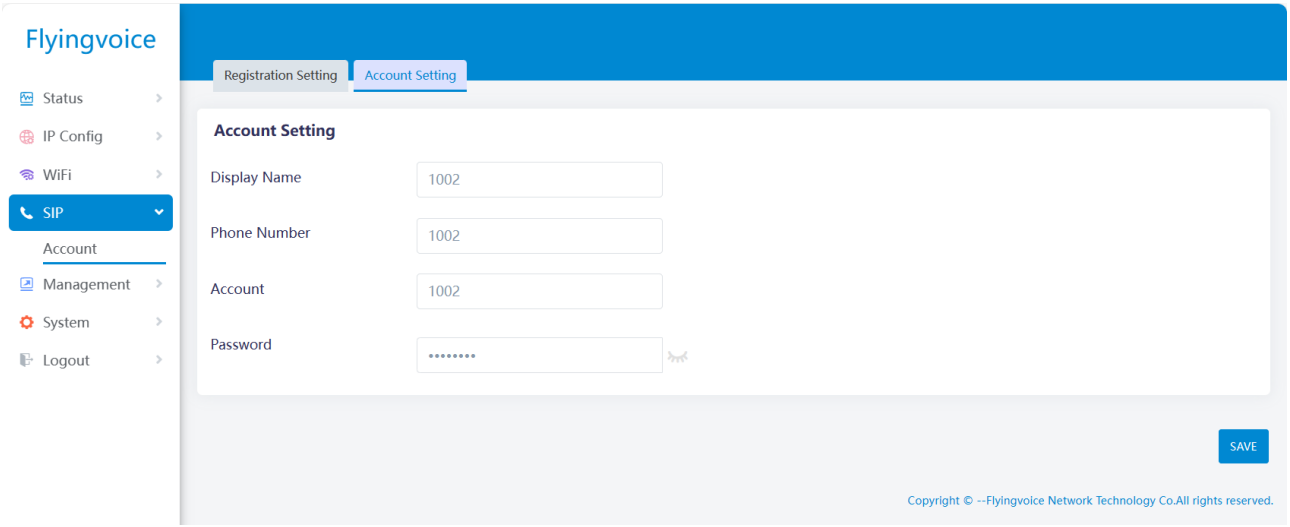


Parameters	Description
SIP Server	Fill in the domain name or IP address of the SIP server where the account is registered.
SIP Server Port	Fill in the port number of the VoIP service supported by the SIP server; the default is 5060.
Outbound Proxy Server1	Fill in the domain name or IP address of the outbound server.

Outbound Proxy Server1 Port	Fill in the port number of the outbound server, , the default is 5060.
Outbound Proxy Server2	Fill in the domain name or IP address of the backup outbound server.
Outbound Proxy Server2 Port	Fill in the port number of the backup outbound server, , the default is 5060.
Transport Protocol	Optional SIP message transmission type: UDP, TCP.
Register Refresh Interval	Fill in the refresh interval time of account registration, the default is 120 seconds.

Path: **SIP->Account Setting**,

as shown in the following figure:



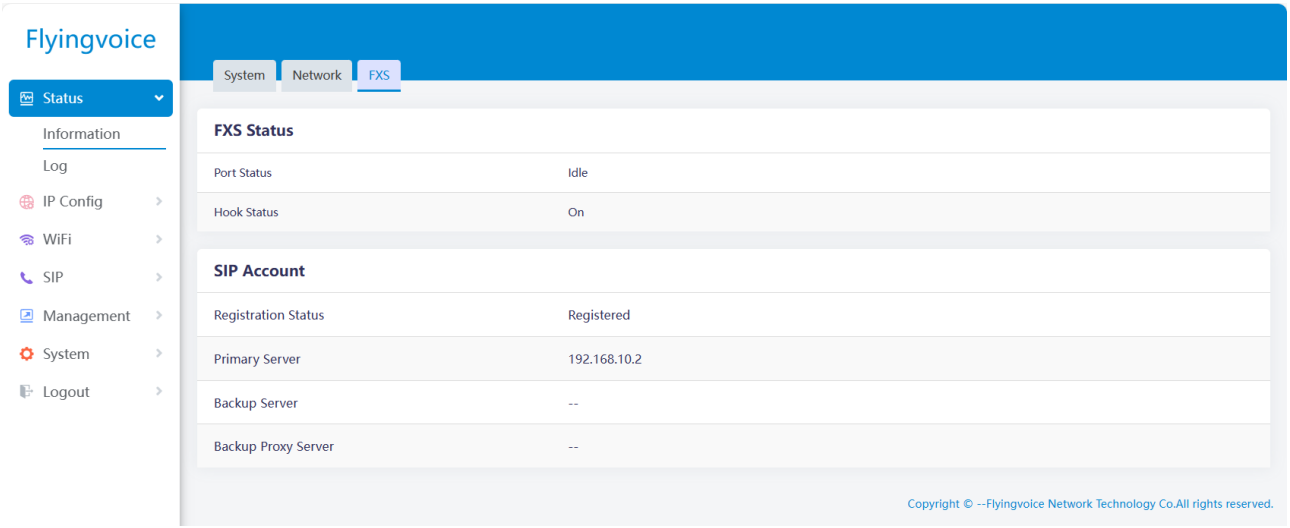
Parameters	Description
Display Name	Fill in the customized account name displayed on the LCD of analog phone.
Phone Number	Fill in the extension number provided by the SIP server.
Account	Fill in the SIP account name provided by the SIP server.
Password	Fill in the SIP account password provided by the SIP server.

2. View the Registration Information

After the account is registered, user can view the registration information on the web page.

Path: **Status**-> **Information**-> **FXS**,

as shown in the following figure:



Parameters	Description
Port Status	Display whether the FXS port is in Connected or Idle.
Hook Status	Display whether the call status of FXS port is in the off hook or hang up state.
Registration Status	Display whether the SIP account is successfully registered.
Primary Server	If the SIP account is successfully registered, the domain name or IP address of the registration SIP server is displayed.
Backup Server	If the SIP account is successfully registered, the domain name or IP address of the Outbound Proxy Server1 is displayed.
Backup Proxy Server	If the SIP account is successfully registered, the domain name or IP address of the Outbound Proxy Server2 is displayed.

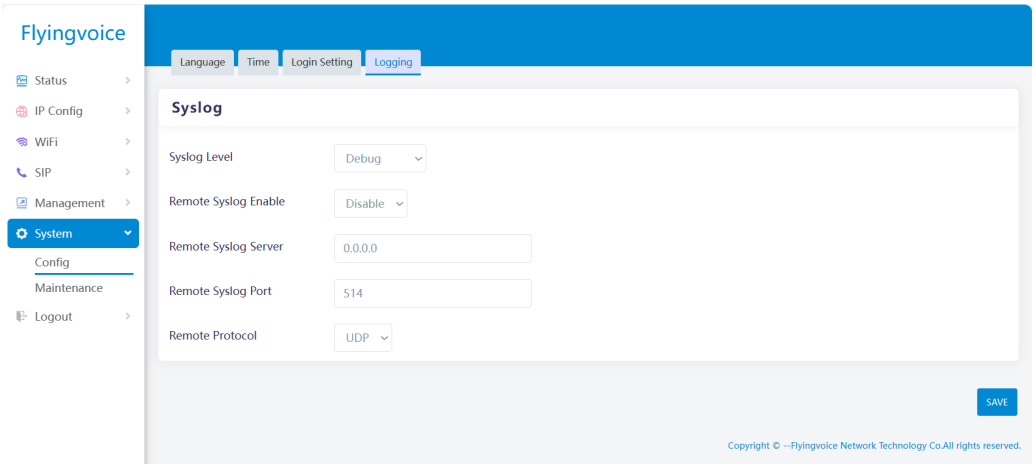
Log Setting and View

The device supports setting and viewing local and remote system logs.

1. Log Setting

Path: **System**-> **Config**-> **Log Setting**,

as shown in the following figure:



Parameters	Description
Syslog Level	Optional different levels of syslog output: Debug, INFO, Notice, Warning, Error, Critical, Alert, Emergency. Debug: Record all diagnostic debugging information. INFO: Record all normal operation information. Notice: Record the normal operation of the information, more important information than INFO. Warning: Record warning information, indicating the existence of some abnormalities or potential problems. Error: Record the error information in the program, indicating that there has been an unrecoverable error in the execution of the program. Critical: Record urgent information that a program component is unavailable, indicating that it needs to be fixed immediately. Alert: The degree of urgency is lower than Emergency, the current system is still available, but also need to be dealt with immediately. Emergency: The most serious level of logging, may lead to system unavailability.

Remote Syslog Enable	Optional whether to enable the remote syslog function.
Remote Syslog Server	After the remote syslog is enable, fill in the remote logging server domain name or IP address.
Remote Syslog Port	After the remote syslog is enable, fill in the remote logging server port number.
Remote Protocol	Optional remote data transmission type: UDP, TCP.

Note: After log Settings are modified, restart the system to take effect.

2. View the Log

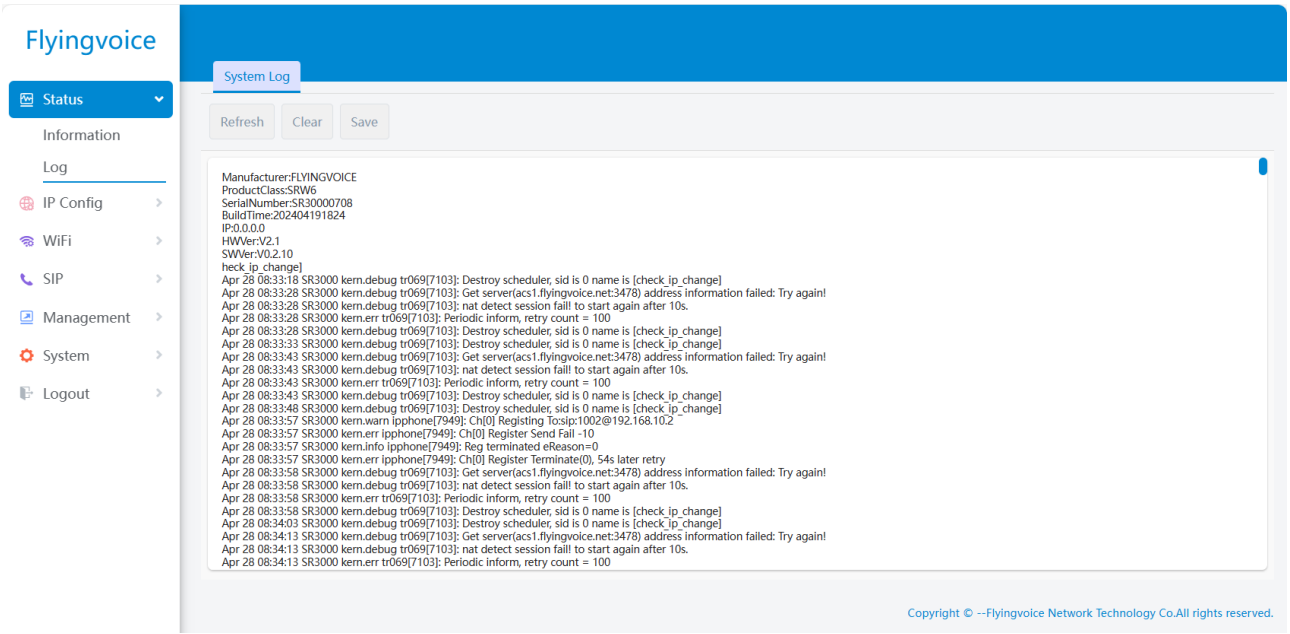
After user enable the log function, it supports to view, refresh, clear and save the system log content, and supports to view the exception log content.

Note: When the system log capacity reaches 64k, the system will automatically clear the log.

(1)View the System Log

Path: **Status**-> **Log**-> **System Log**,

as shown in the following figure:



User can refresh the system log, clear all log contents, and save the log file locally with one click.

Management Configuration

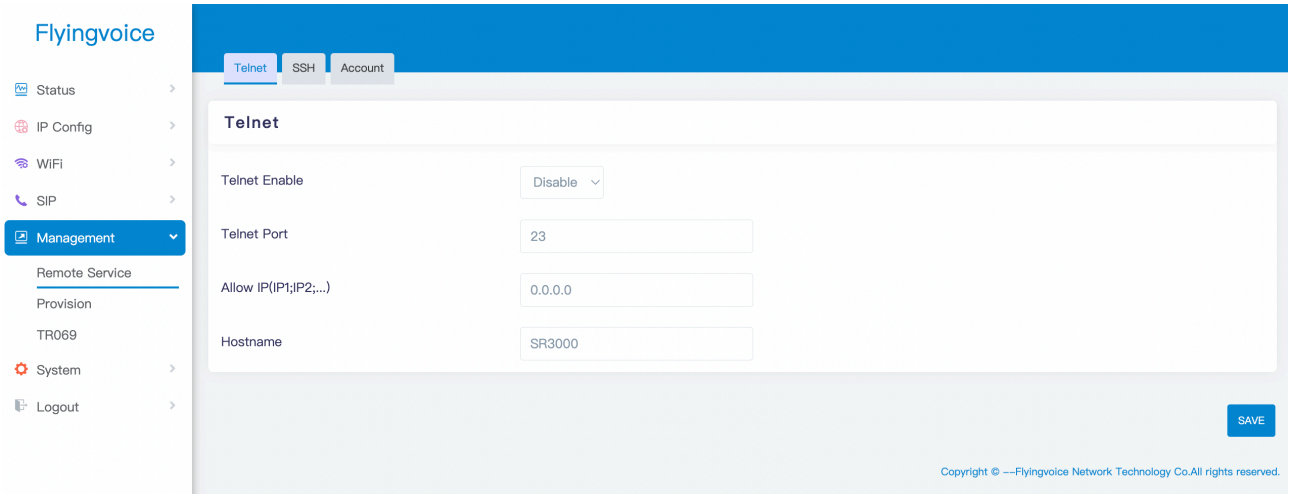
The device supports management configuration, including Telnet, SSH, TR069 and Provision configuration.

1. Telnet Setting

It supports remote devices to access the local device by telnet command.

Path: **Management** -> **Remote Service** -> **Telnet**,

as shown in the following figure:



Parameters	Description
Telnet Enable	Optional whether to enable the remote telnet function.
Telnet Port	After telnet is enable, fill in the port number used for telnet to the device, the default is 23.
Username	Fill in the username for logging in to the Telnet remotely.
Password	Fill in the password for logging in to the Telnet remotely.
Allowed IP	After telnet is enable, fill in the IP address of the remote devices that allow remote telnet access.

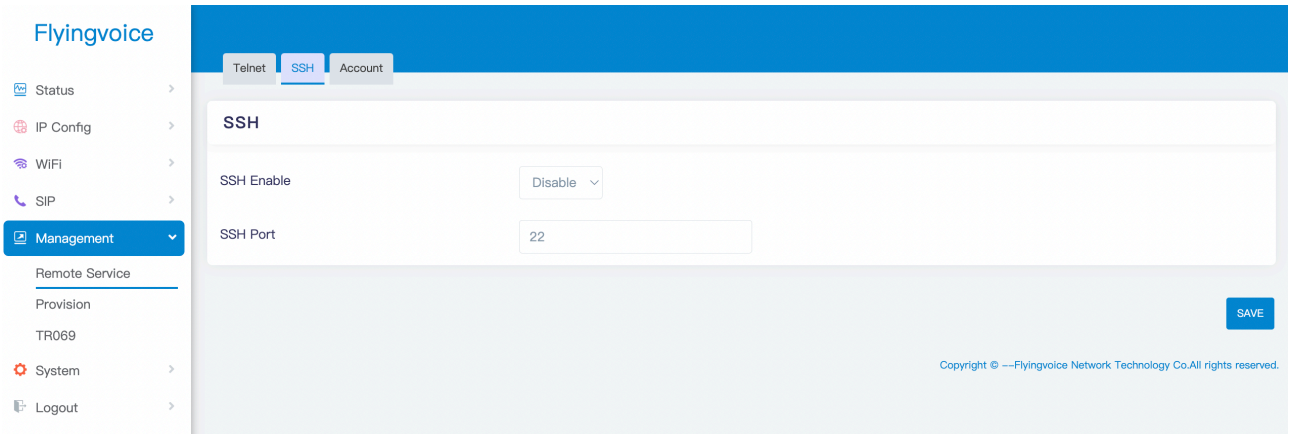
Hostname	After telnet is enable, fill in the host name of the device. The default is model of the device, such as SR3000.

2. SSH Setting

It supports access to the device through SSH (Secure Shell) tool, and supports encrypted remote login and management of the device.

Path: **Management** -> **Remote Service** -> **SSH**,

as shown in the following figure:

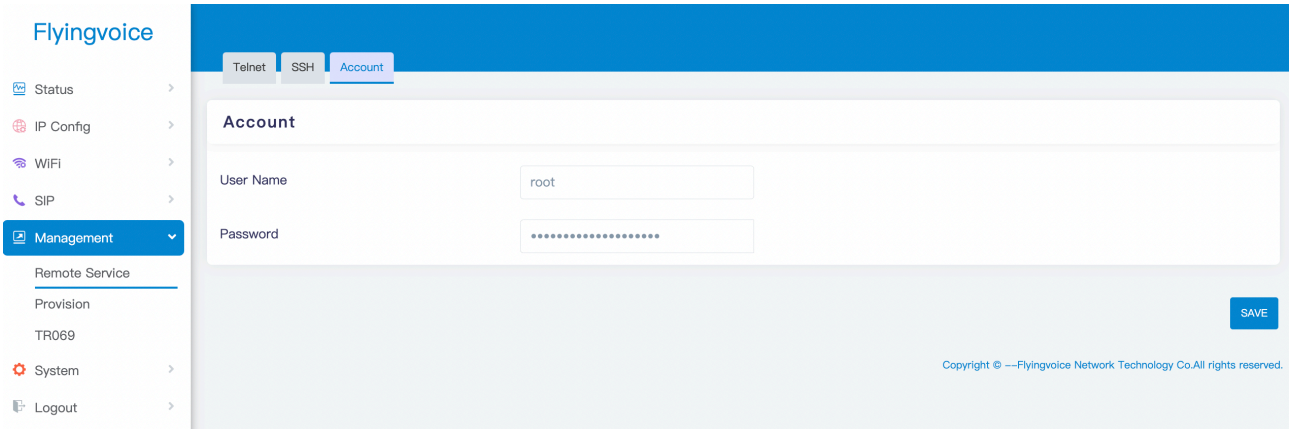


Telnet & SSH Login Configuration

Telnet and SSH use the same remote login account and password mechanism.

Path: **Management** -> **Remote Service** -> **Account**,

as shown in the following figure:

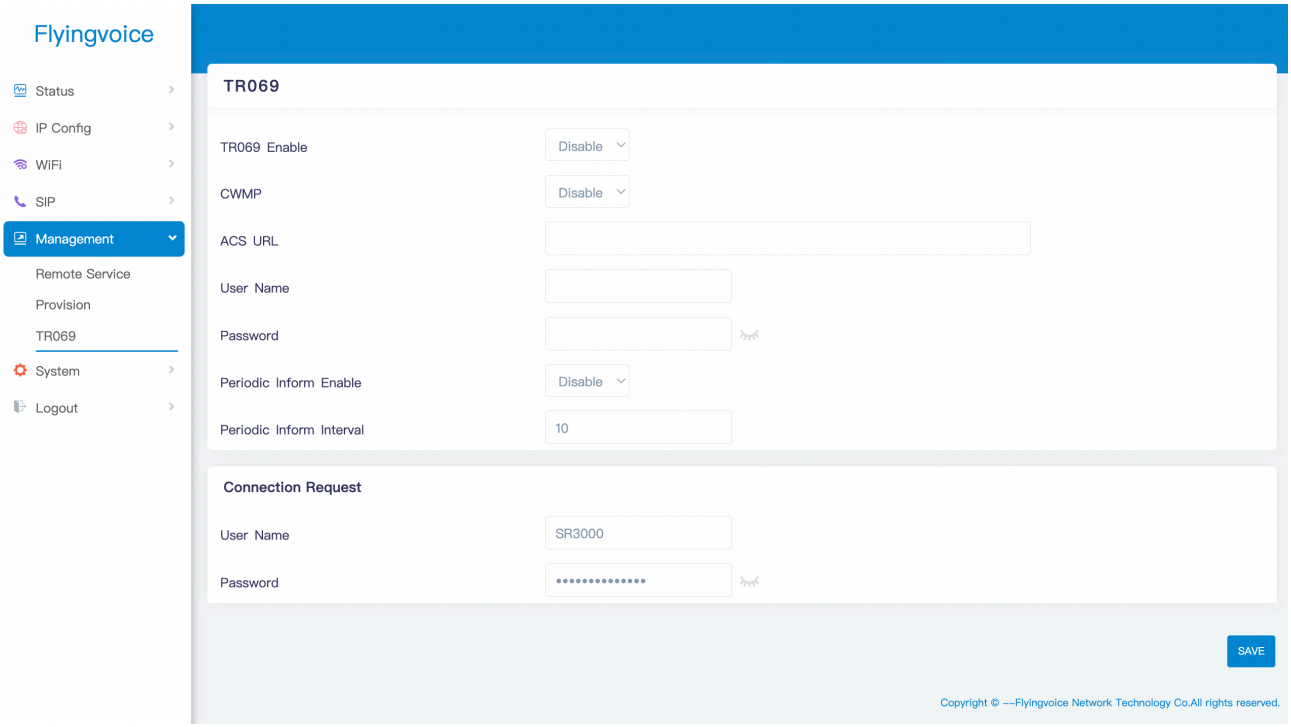


3. TR069 Configuration

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

Path: **Management** -> **TR069**,

as shown in the following figure:



Parameters	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 lnform Enable	Enables sending notifications to ACS periodically, optionally enable/disable.

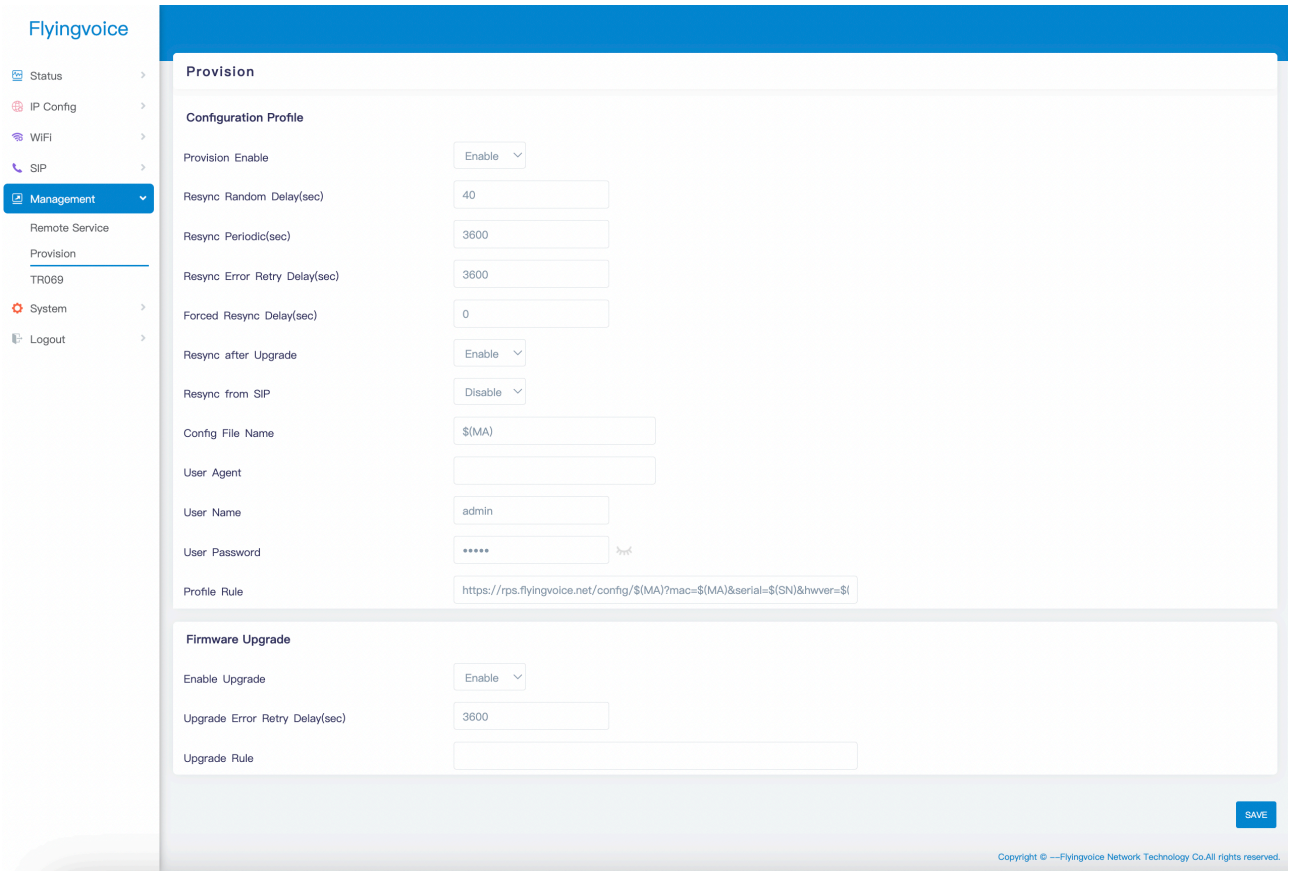
Periodic Inform Interval	The time interval at which scheduled notifications are sent to the ACS to report device status and information.
User Name	CPE username, used to verify the username when ACS connects to the device, the default is product model, like SR3000 or SR3000-lite.
Password	CPE password, used to verify the password when ACS connects to the device, the default is product serial number.

4. Provision Configuration

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.

Path: **Management** -> **Provision**,

as shown in the following figure:



Parameters	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.