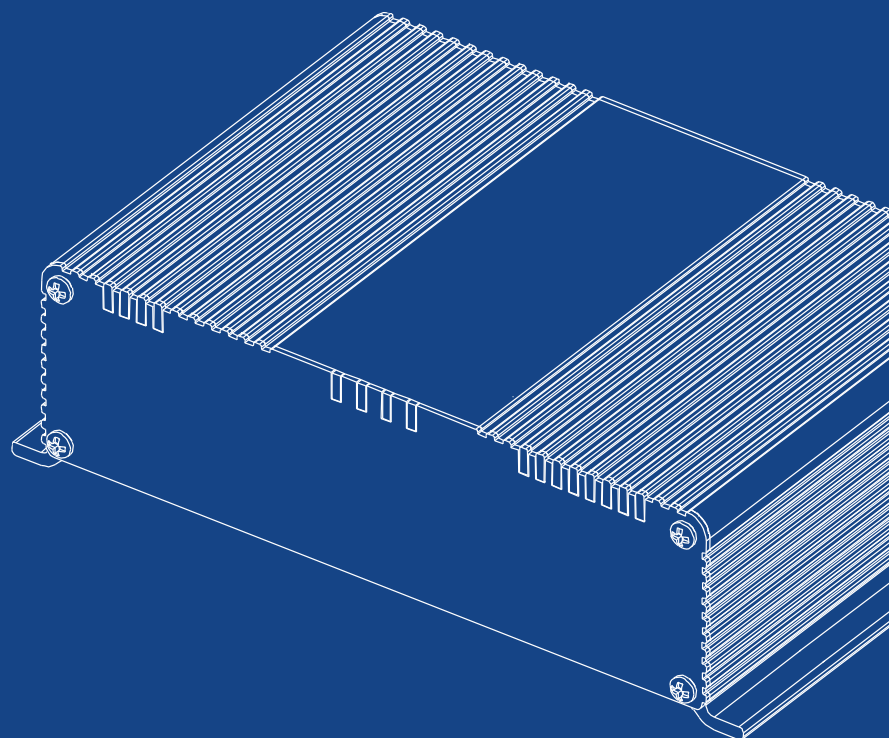




Vola PR08-Pro

User Guide

— Dual-WAN ATA with built-in battery



Revision

Release Version	Note	Date	Editor
V0.1.0	Initial Release	2025.01.20	Albert Yuan
V0.1.1	Updates the Shipping Mode Operation, Fix some mistakes.	2025.04.21	Albert Yuan

Statement

WARRENTY

Product specifications and information in this guide are subject to change without notice. All statements, information and recommendations in this guide are believed to be accurate and are provided without warranty of any kind, either expressed or implied. Users must take full responsibility for their product applications.

DISCLAIMER

VolaNetowrks Inc. disclaims all warranties with respect to this guide, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VolaNetowrks Inc shall not be liable for errors contained in this guide, or incidental or consequential damages in connection with the furnishing, performance or use of this guide.

LIMITATION OF LIABILITY

VolaNetowrks Inc. and/or its respective suppliers assume no responsibility for the suitability of the information contained in this document. The information is provided 'as is' without warranty of any kind by VolaNetowrks Inc. and is subject to change without notice. All risks are borne by the recipient except for those arising from the use of the information. In no event shall VolaNetowrks Inc. be liable for direct, indirect, incidental, special, punitive, or any other damages of any kind (including, but not limited to, loss of business profits, business interruption, or loss of business information), even if VolaNetowrks Inc. has been advised of the possibility of such damages.

ATTENTION

The telephone port (RJ11) on this device is only for connecting local analog terminals such as analog telephones, fax machines, alarm panel, etc. Do not connect it to the telephone port on the wall (PSTN line). Do not use the port as FXO port to connect any Telecommunication Network. Incorrect connection may lead to broken device.

CAUTION

If not handled properly, the batteries used in this equipment may present a risk of burnout or chemical burns. Do not replace the batteries in the device by yourself, as this may result in a risk of fire or explosion and void the device warranty.

Dispose of used batteries promptly in a manner authorized for your region. Do not dispose of the device or the battery in the device.

To replace the battery in the device, contact your dealer or our technical support: support@volanetworks.com.

Avoid using this product in hot environments. The battery charging circuit will stop charging when the temperature of the battery exceeds 60°C.

Do not dismantle, crush, or dispose of it fire or heat. Keep away from children.

Declaration of Conformity

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.

Table of Contents

REVISION.....	II
STATEMENT	III
DECLARATION OF CONFORMITY	V
ABOUT THIS GUIDE.....	1
CHAPTER 1 INTRODUCTION	2
1.1. HARDWARE INTRODUCTION.....	3
1.2. LED INDICATOR	5
1.3. HARDWARE INSTALLATION.....	6
CHAPTER 2 BASIC CONFIGURATION	9
2.1. DEVICE INITIALIZATION	10
2.2. WEB INTERFACE	10
2.2.1. LOGIN	10
2.2.2. SYSTEM STATUS	11
2.3. BASIC NETWORK CONFIGURATION.....	13
2.3.1. WAN SETTINGS	13
2.3.2. LAN SETTING.....	19
2.4. ADVANCED NETWORK CONFIGURATION.....	21
2.4.1. IPV6 WAN CONFIGURATION.....	22
2.4.2. IPV6 LAN SETTING	27
2.4.3. VPN SETTING.....	29
2.4.4. DMZ SETTING.....	32
2.4.5. DDNS SETTING.....	33
2.4.6. PORT SETTING	34
2.4.7. ROUTING SETTING.....	34
2.4.8. ADVANCE SETTING	36
CHAPTER 3 VOIP CONFIGURATION	37
3.1. ACCOUNT SETTINGS	38
3.2. FXS SETTING	41
3.2.1. CONFIGURE SIP ACCOUNTS.....	42
3.2.2. CONFIGURE CALL AUDIO.....	44

PR08-Pro User Guide

3.2.3. CONFIGURE THE FAX SERVICE	45
3.2.4. SUPPLEMENTARY SERVICE	46
3.2.5. ADVANCED SETUP	48
3.3. SIP SETTING.....	52
3.3.1. SIP PARAMETERS SETTING.....	52
3.3.2. NAT TRAVERSAL SETTING.....	54
3.4. VoIP QoS.....	55
3.5. CALL SETTING	56
3.5.1. VOLUME SETTINGS.....	57
3.5.2. REGIONAL RINGTONE SETTINGS	58
3.5.3. CALL FORWARD SETTINGS	60
3.5.4. FEATURE CODE.....	62
3.5.5. CPC CONTROL.....	63
3.5.6. FXS PORT POLARITY CONFIGURATION.....	64
3.5.7. MISCELLANEOUS.....	65
3.5.8. DIAL RULE	66
3.5.9. CALL LOG	68
<u>CHAPTER 4 MANAGEMENT CONFIGURATION</u>	<u>69</u>
4.1. MANAGEMENT	70
4.1.1. CONFIGURE FILE UPLOAD & DOWNLOAD	71
4.1.2. ADMINISTRATOR SETTINGS	71
4.1.3. NTP SETTINGS.....	74
4.1.4. SYSLOG SETTING	75
4.1.5. FACTORY DEFAULT	76
4.1.6. FIRMWARE UPGRADE	77
4.2. SCHEDULED TASKS.....	78
4.3. PROVISION	80
4.4. SNMP.....	83
4.5. TR069.....	84
4.6. POWER OUT.....	85
4.7. DIAGNOSIS	86
4.7.1. PACKET TRACE.....	86
4.7.2. PING TEST	86
4.7.3. TRACEROUTE TEST	87

About This Guide

Thank you for choosing Vola PR08-PRO, which is a highly integrated ATA gateway for POTS replacement solution, provides 8 FXS ports to support 8 external connections and easily connect to elevator emergency call panel, fire/burglar alarm panel, fax machines, ATM machines/POS terminals and so on. And the PR08-PRO is equipped with built-in battery, it integrates 2 gigabit WAN ports that support PoE out and network failover, 1UPS port, and 1 type-C USB ports that support external power banks to achieve 24h power outage running and ensure you an uninterrupted connection with calls and network. You can choose to use the PR08-PRO with Vola LM150 or third-party router to form a "4G/5G+POTS Replacement" IP communication solution.

Related Documentation

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

- Datasheet
- Quick Installation guide

Chapter 1 Introduction

This section describes the product's hardware, indicator lights, and installation procedures.

Topics:


[Hardware Introduction](#)

[LED Indicator](#)

[Hardware Installation](#)

1.1. Hardware Introduction

This section describes the exterior design and interfaces of the product.

Product	PR08-PRO
Appearance display	 <p>The image shows a 3D perspective view of the PR08-PRO device, a black, vertically-oriented unit with a ribbed front panel. Below the main device, several internal components are shown in an exploded view, including a green printed circuit board (PCB) with various components, a black metal chassis, a blue USB Type-C port, a DC jack, and other electronic components.</p>
PWR (Power supply)	19V / 3.42A
Interface	<p>2*WAN/10/100/1000Mbps, PoE out 2*LAN,10/100/1000Mbps 8*FXS 1*UPS port 1*USB(Type-C) 1*DC Jack</p>

Indicator	2*WAN Ports Indicator 2*LAN Ports Indicator 8*FXS Ports Indicator 1*UPS Indicator 1*USB Indicator 1*BAT Indicator 1*PWR Indicator
Structure	Cast aluminium alloy enclosure. Supports desktop installation and wall mounting.
Battery	Nominal Voltage: 10.95V Capacity: 3500mAh Maximum Charging Voltage: 12.6V

The descriptions of the corresponding interface are as follows:

Interface	Description
WAN	Connect to network adapters, router, modem or gateway to connect to external network, normally for internet connection. Support PoE out.
LAN	Connect to the devices in the local-area network.
FXS	Connect to alarm panel, analog phone or fax machine.
USB	Type-C port, connect to the power bank as the backup power to provide interrupted service during power failure. 65w PD power bank is Recommended for best experience.
UPS	Connect to receiving Power device (such as LM150), support Power out.
DC Jack	Connect the 19V power adapter.
Reset Button	Long press for 5s to reset the device to factory default Short press for < 5s to reboot the device

1.2. LED Indicator

This section describes the status of the indicators for power, LAN port, FXS port and BAT Indicator in different operating states.

Indicator	Status
WAN/LAN Port Indicator	Solid Green: Connection successful. Blinking Green(5Hz): Data transmission. Off: Disconnected.
FXS Port Indicator	Solid Green: Account Registered. Blinking Green(5Hz): Ringing, Off-hook, On Call. Off: Disconnected or Registration failure.
UPS Indicator	Solid Green: Power out after connection. Off: Disconnected or Insufficient device power (No output).
BAT Indicator	Solid Green: Built-in Battery is full Blinking Green(1Hz): Built-in Battery discharging. Solid Orange: Built-in Battery charging. Blinking Orange: Battery low Off: No Battery or Battery error
USB Indicator	Solid Orange: Power bank charging. Blinking Green(1Hz): 65W Power bank discharging. Blinking Orange(1Hz): Non-65W Power bank discharging. Off: Disconnected or No-charging.
PWR Indicator	Solid Green: Power On. Off: Power Off.

1.3. Hardware Installation

This section describes how the interface is mounted and how it is powered.

Topics:

[Installation Preparation](#)

[Installation Procedure](#)

TIPS: Before installing the device, check whether the equipment is complete and installation conditions are met. After unpacking the device, check whether the contents are complete against the quick installation guide. If you find that the contents in the packing box do not match the list, please contact us directly.

Device Power Supply

The device supports two power supply modes. When PR08-PRO is connected to normal DC power supply, or when it is connected to standard 65W power bank supply, it will automatically turn on the PoE Out function of WAN port.

WARNING:

Do not attempt to use an unsupported power adapter, and do not unplug the power when configuring or upgrading devices. Using other power adapters may damage the device and will void the manufacturer's warranty.

DC Power Supply

Device DC power input supports up to 19V 3.42A, please make sure the power adapter is correct before connecting.

Procedure:

1. Use a single-phase, three-core DC power socket, and ensure that the ground cable is properly grounded.
2. Connect the power adapter to the PWR port.
3. After plugging in the DC power supply, the PWR indicator will turn green and wait for the device to start up.

Power Bank Supply

PR08-PRO supports power bank power supply. It is recommended to choose a 65W power bank with PD3.0 protocol for charging. At this time, the two WAN ports can be used as PoE Out ports and UPS port can output up to 12V.

Note: Some power bank may not correctly output power for PR08-PRO or cannot automatically output power, please use PD 3.0 power bank with 65w or more for best effect. Please check the specification of your power bank before install the devices.

Procedure:

1. Plug the power bank into the device's USB port via the Type-C cable.
2. After plugged in, the USB indicator on the device will turn to green(If the power of Powerbank is not enough, the light will be orange).

TIPS:

1. The installation site must meet the conditions for connecting devices to external devices, including power cables, network cables, and PC. Use a single-phase, three-core DC power socket, and ensure that the device is properly grounded.
2. The environment of the installation site should ensure sufficient air flow to facilitate the heat dissipation of the equipment, the appropriate working temperature of the equipment is 0°C ~ 50°C and support working from -40°C ~ 85° (not recommended).

Ethernet Port Access

Before using the device, it must be properly connected:

1. Connect the device WAN port to the modem with an Ethernet cable
2. Connect the PC to the LAN port of the device using an Ethernet cable
3. When the connection is complete, the WAN/LAN port indicator on the device will turn green.

Shipping Mode

To turn off the battery, please follow:

1. Make sure the device is fully boot up, and the power adapter is disconnected;
2. Long press the reset button for over 5s until all LEDs are turned on;
3. Release the Reset button, all LEDs will be turned off;
4. The device now enter shipping mode.
(If it doesn't work, wait for complete startup and perform it again)

Chapter 2 Basic Configuration

This section describes basic configuration of the device through web interface, include the following topics:

Topics

[Device Initialization](#)

[Web Interface](#)

[Basic Network Configuration](#)

[Advanced Network Configuration](#)

2.1. Device Initialization

After the device is powered on and started, perform the following steps:

1. If the power indicator is normal, ensure that the network cable connected to the adapter can access the Internet properly. The device works in DHCP mode by default.
2. To configure or view device information, connect the LAN port of the device to the PC's RJ45 port. After the connection is successful, the PC will obtain an IP address of 192.168.1.x and can access to the PR08-PRO.

2.2. Web Interface

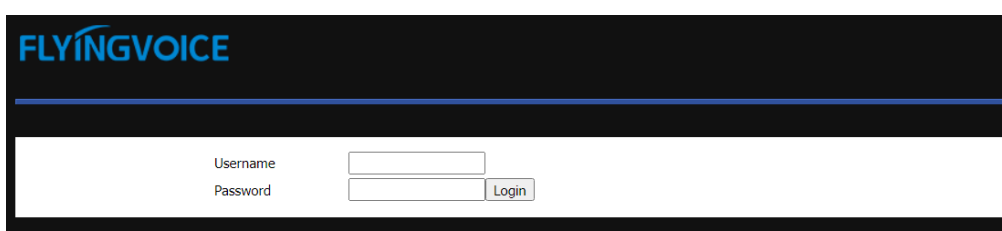
This section describes how to log in to the device web interface and view system information.

2.2.1. Login

You can view the device status on the web page:

1. Enter the IP address of the LAN port in the browser to enter the login page
2. Input Username / Password (admin / last 6 digits of SN number)

For user level, enter user/last 6 digits of SN number to login. Different user level can configure different items. You can check the SN number on the label of device.



The screenshot shows the login interface for the FLYINGVOICE device. At the top, the 'FLYINGVOICE' logo is displayed in blue on a black background. Below the logo is a white rectangular area containing the login form. The form has two input fields: 'Username' and 'Password'. To the right of the 'Password' field is a 'Login' button.

After successfully login, the device status information page is displayed by default, where you can view the system information, Intranet host information, and system logs of the device

2.2.2. System Status

Procedure

1. Navigate to **Status** -> **Basic**

The screenshot shows the 'Status' page in the PR08-Pro web interface. The navigation tabs at the top are 'Status', 'Network', 'SIP Account', 'Phone', and 'Administration'. Under 'Status', there are sub-tabs for 'Basic', 'LAN Host', and 'Syslog'. The main content area is divided into two sections: 'Product Information' and 'PowerBank Information'. On the right side, there is a 'Help' section with descriptions for 'Product Information', 'Line Status', 'Network Status', and 'System Status'.

Product Information	
Product Name	PR08-PRO
Internet (WAN) MAC Address	00:21:F2:54:97:A7
Internet (WAN2) MAC Address	00:21:F2:54:97:A8
PC (LAN) MAC Address	00:21:F2:54:97:A6
Hardware Version	V1.5
Loader Version	V3.52(Mar 2 2024 17:21:56)
Firmware Version	FVGW V0.2.18 (202410292104)
Serial Number	VOLA00124B00007

PowerBank Information	
USB1 Status:	Not connected
USB1 Actual Output:	0.00V 0.00A
Battery Status	Battery charged fully
Battery Percentage	100%
PoE1 Output Status	On
PoE2 Output Status	On
UPS Output Status	Normal
Total Output Status	Normal

Help	
Product Information:	It shows the basic information of the product.
Line Status:	Displays current line registration status, as well as primary and back-up SIP server IP address information.
Network Status:	Displays the network status and detailed information about WAN, LAN, Wi-Fi & VPN.
System Status:	It shows current time and running time of the product.

System information includes:

Product Information (Product Name, MAC Address, Hardware Version, Firmware Version, Serial Number, etc.

LAN Host includes:

- IPv4 LAN Host Information (MAC Address, IP Address, Interface Type, Address Source, Expires, Host Name, Status)
- IPv6 LAN Host Information (MAC Address, IPv6 Address, Expires)

LAN Host Info							
MAC Address	IP Address	Interface Type	Address Source	Expires	Host Name	Status	
88:A4:C2:B9:34:31	192.168.1.2	Other	Static	0:0:0	Unknown	Active	

IPv6 LAN Host Info		
MAC Address	IPv6 Address	Expires

System log includes:

- The system records the configuration information in real time;
- Support refresh logs, clear all logs, save and export logs;

Status
Network
SIP Account
Phone
Administration

Basic
LAN Host
Syslog

```

Manufacturer:FLYINGVOICE
ProductClass:PR08
SerialNumber:HG8A1708000131
BuildTime:202309211749
IP:192.168.1.1
HWVer:V1.4
SWVer:V0.1.10
<Thu Jan 1 08:00:41 1970> provision[1780]: provision v1.2 start
<Thu Jan 1 08:00:42 1970> udhcpd[1411]: received SIGTERM
<Thu Jan 1 08:00:42 1970> dnsmasq[1683]: started, version 2.80 cachesize 150
<Thu Jan 1 08:00:42 1970> dnsmasq[1683]: overflow: 3 log entries lost
<Thu Jan 1 08:00:43 1970> udhcpd[2114]: started, v1.30.1
<Thu Jan 1 08:00:48 1970> provision[1780]: Profile Rule [https://rps.flyingvoice.net/config/1853e0285322?mac=1853e02853...
<Thu Jan 1 08:00:49 1970> rmmmod: module is not loaded
<Thu Jan 1 08:00:52 1970> goahead[2640]: webs start...
<Thu Jan 1 08:00:53 1970> snmpd[2913]: start
<Thu Jan 1 08:00:55 1970> ipphone[2478]: [UI] ***system booting***
<Thu Jan 1 08:00:56 1970> ipphone[2478]: [UI] SW:142(120106174008)
<Thu Jan 1 08:00:57 1970> ipphone[2478]: [UI] UISignalControl[30][9000][30][9000][9000]
<Thu Jan 1 08:00:57 1970> provision[1780]: File does not exist or server is unreachable
                    
```

2.3. Basic Network Configuration

PR08-PRO supports different network access modes for WAN port and IP address Settings for LAN port.

2.3.1. WAN Settings

In this section, you can set different WAN configurations, including DHCP, static IP, and PPPoE.

Topics

[WAN Network Settings](#)

[DHCP Mode Setting](#)

[Static IP Mode Setting](#)

[PPPoE Mode Setting](#)

DHCP Mode Setting

Procedure

1. Navigate to **Network** -> **WAN**
2. Select **DHCP** in WAN IP Mode

The screenshot shows a web-based configuration interface with a top navigation bar containing tabs for Status, Network, SIP Account, Phone, and Administration. Under the Network tab, there are sub-tabs for WAN, LAN, IPv6 Advanced, IPv6 WAN, IPv6 LAN, VPN, DMZ, DDNS, Port Setting, and Routing. The 'INTERNET' section is active, and the 'WAN' settings are displayed. The 'WAN IP Mode' is set to 'DHCP'. The 'DHCP Server' field is empty. 'MAC Address Clone' is set to 'Disable'. 'LAN Connection Mode' is set to 'NAT'. 'DNS Mode' is set to 'Auto'. There are also empty input fields for 'Primary DNS' and 'Secondary DNS'.

TIPS:

- The built-in DHCP server assigns a dedicated IP address to each local client.
- The factory default DHCP mode allows the device to automatically obtain an IP address from the DHCP server without manually assigning an IP address to the client.
-

Parameter	Description
WAN IP Mode	Default DHCP.
DHCP Server	Enter the specified DHCP server address or domain.
MAC Address Clone	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> MAC Address Clone <input type="text" value="Enable"/> MAC Address <input type="text" value="88:a4:c2:b9:34:31"/> <input type="button" value="Get Current PC MAC Address"/> </div> Select “enable” to enable this function. After this function is enabled, you need to enter the MAC address of the bound PC. You can also click the button “Get current PC MAC Address” to obtain the MAC address of the current PC.
LAN Connection Mode	Bridge or NAT mode is optional. The default is NAT mode.
DNS Mode	option: automatic or manual:

	<p>If automatic is selected, devices on the LAN port automatically obtain the primary DNS and secondary DNS.</p> <p>If Manual is selected, you need to manually enter the primary DNS and secondary DNS.</p>
--	--

Static IP Mode Setting

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 interface.

The screenshot shows the 'INTERNET' configuration page with the 'WAN' tab selected. Under 'WAN IP Mode', the dropdown is set to 'Static'. Below this, the IP Address is 192.168.1.104, Subnet Mask is 255.255.255.0, and Default Gateway is 192.168.1.1. The DNS Mode is set to 'Manual', with empty fields for Primary and Secondary DNS.

Parameter	Description
WAN IP Mode	Select Static IP.
MAC Address Clone	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> MAC Address Clone Enable ▾ MAC Address 88:a4:c2:b9:34:31 Get Current PC MAC Address </div> Select “enable” to enable this function. After this function is enabled, you need to enter the MAC address of the bound PC. You can also click the button “Get current PC MAC Address” to obtain the MAC address of the current PC.
LAN Connection Mode	Bridge or NAT mode is optional. The default is NAT mode.
IP Address	Enter the fixed IP address received from the ISP.

Subnet Mask	Enter the subnet mask of the IP address.
Default Gateway	Enter the local gateway address.
DNS Mode	The default is manual. You need to manually enter the primary DNS and secondary DNS.

PPPoE Mode Setting

PPPoE is a point-to-point protocol on the Ethernet. It relies on two standards: PPP and Ethernet, through which it connects users to the Internet with a common broadband medium, such as a single DSL line, wireless device, or cable modem.

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

The descriptions are as follows:

Parameter	Description
WAN IP Mode	Select PPPoE.
MAC Address Clone	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> MAC Address Clone Enable ▾ MAC Address 88:a4:c2:b9:34:31 Get Current PC MAC Address </div> Select whether to enable this function. After this function is enabled, you need to enter the MAC address of the bound PC. You can also click to obtain the MAC address of the current PC.
LAN Connection Mode	Bridge or NAT mode is optional. The default is NAT mode.

DNS Mode	<p>option: automatic and manual: If automatic is selected, devices on the LAN port automatically obtain the primary DNS and secondary DNS. If Manual is selected, you need to manually enter the primary DNS and secondary DNS.</p>
PPPoE Account	Enter the PPPoE account obtained from the ISP.
PPPoE Password	Enter the PPPoE password obtained from the ISP.
Confirm Password	Enter the PPPoE password again.
Service Name	<p>Enter the PPPoE authentication service name. If it is empty, the service name is automatically detected.</p>
Operation Mode	<div data-bbox="571 860 1145 949" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Operation Mode Keep Alive ▾</p> <p>Keep Alive Redial Period (0-3600s) <input style="width: 60px;" type="text" value="5"/></p> </div> <p>Option: Keep Alive, On Demand, Manual, the default is Keep Alive:</p> <p>If you choose Keep Alive, the redial is automatically reconnected within a redial period, you need to set an redial period. The default value is 5s.</p> <p>If you choose On Demand, 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. You need to set the idle time on demand. The default value is 5min.</p> <p>If you choose Manual, dial by manually clicking on the connection, the device does not dial automatically.</p>

2.3.2. LAN Setting

You can assign IP addresses to devices on the LAN interface.

Procedure

1. Navigate to **Network** -> **LAN**
2. Select Local DHCP Server as Enable

Parameter	Description
Local IP Address	Enter the local IP address of the device on the LAN. The IP addresses of all devices on the LAN must be in the same network segment as this IP address. The default gateway address is 192.168.1.1.
Local Subnet Mask	Enter the subnet mask to determine the network size (default: 255.255.255.0).
Local DHCP Server	Whether to enable the DHCP server.
DHCP Start Address	After the DHCP server is enabled, this is needed to be filled. Enter 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.

DHCP End Address	<p>After the DHCP server is enabled, this is needed to be filled. Enter a valid IP address as the end IP address sent by the DHCP server to the DHCP client.</p>
DNS Mode	<p>Option: automatic and manual: If automatic is selected, devices on the LAN port automatically obtain the primary DNS and secondary DNS. If Manual is selected, you need to manually enter the primary DNS and secondary DNS.</p>
Client Lease Time	<p>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.</p>
DHCP Static Allotment	<div data-bbox="564 846 1131 949" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Operation Mode On Demand ▼</p> <p>On Demand Idle Time (0-60m) 5</p> </div> <p>You can add multiple DHCP static assignment rules, enter MAC address and IP address and reserve an IP address for a specified mac address. For each assignment rule, you can also edit/delete it.</p>

2.4. Advanced Network Configuration

This section describe the advanced network configuration, including IPv6 WAN/LAN, VPN, DMZ, DDNS, Port Setting, Routing and so on.

Topic

[IPv6 Advance Setting](#)

[IPv6 WAN Setting](#)

2.4.1. IPv6 WAN Configuration

Topic

[DHCPv6 mode](#)

[Static IPv6 mode](#)

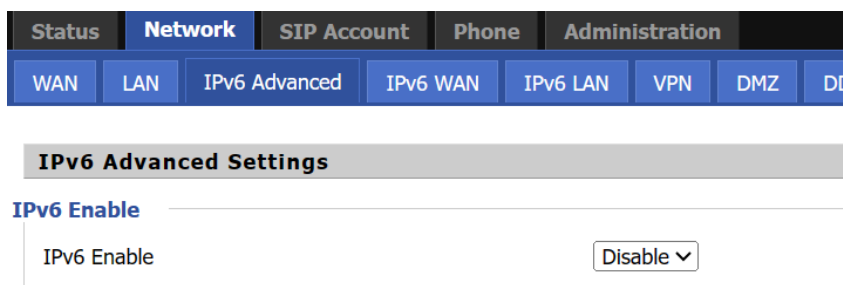
[IPv6 LAN mode](#)

IPv6 Enable

You can select to Enable or disable IPv6.

Procedure

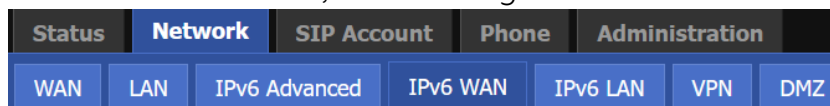
1. Navigate to **Network** -> **IPv6 Advanced**



DHCPv6 mode

Procedure

1. Navigate to **Network** -> **IPv6 WAN**
2. Set DHCPv6 mode, Save settings



IPv6 WAN Setting

IPv6 WAN Setting

Connection Type	<input type="text" value="DHCPv6"/>
DHCPv6 Address Settings	<input type="text" value="Stateless"/>
Prefix Delegation	<input type="text" value="Disable"/>

Parameter	Description
Connection Type	Option: DHCPv6, static IPv6, or PPPoE. The default mode is DHCPv6.
DHCPv6 Address Settings	Option: Stateless, Stateful.
Prefix Delegation	Option: whether to enable prefix distribution.

Static IPv6 mode

Status	Network	SIP Account	Phone	Administration				
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	DMZ	DDNS	Port

IPv6 WAN Setting

IPv6 WAN Setting

Connection Type STATIC IPv6 ▾

IPv6 Address

IPv6 Prefix Length (0-128)

Default IPv6 Gateway

Primary DNS Server

Secondary DNS Server

Parameter	Description
Connection Type	Select static IPv6.
IPv6 Address	Enter the fixed IP address received from the ISP.
IPv6 Prefix Length	Enter the IPv6 address prefix length, ranging from 0 to 128.
Default IPv6 Gateway	Enter the IPv6 address of the local gateway.
Primary DNS Server	Enter the primary DNS server address.
Secondary DNS Server	Enter the secondary DNS server address.

PPPoE mode

Status	Network	SIP Account	Phone	Administration				
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	DMZ	DDNS	Port Setting

IPv6 WAN Setting	
-------------------------	--

IPv6 WAN Setting

Connection Type	PPPoE ▾
PPPoE Create Method	Share with IPv4 ▾
Address Mode	Dynamical IP ▾
PPPoE Account	<input type="text"/>
PPPoE Password	<input type="password"/>
Confirm Password	<input type="password"/>
Service Name	<input type="text"/>
	Leave empty to resolve this field automatically
Operation Mode	Keep Alive ▾
Keep Alive Redial Period (0-3600s)	<input type="text" value="5"/>
Prefix Delegation	Disable ▾

Parameter	Description
Connection Type	Select PPPoE mode.
PPPoE Create Method	The default is shared with IPv4. You can optionally create a new PPPoE.
Address Mode	Option: dynamic address, static address. The default is dynamic address, If static address is selected, manually enter an IPv6 address.
PPPoE Account	Enter the PPPoE account obtained from the ISP.
PPPoE Password	Enter the PPPoE password obtained from the ISP.
Confirm Password	Enter the PPPoE password again.
Service Name	Enter the PPPoE authentication service name. If it is empty, the service name is automatically detected.

<p>Operation Mode</p>	<p>Option: Keep Alive, On Demand, Manual, the default is Keep Alive: If you choose Keep Alive, the redial is automatically reconnected within a redial period, you need to set an redial period. The default value is 5s.</p> <div data-bbox="568 421 1251 524" style="border: 1px solid black; padding: 5px;"> <p>Operation Mode Keep Alive ▾ Keep Alive Redial Period (0-3600s) 5</p> </div> <p>If you choose On Demand, 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. You need to set the idle time on demand. The default value is 5min.</p> <div data-bbox="568 770 1251 891" style="border: 1px solid black; padding: 5px;"> <p>Operation Mode On Demand ▾ On Demand Idle Time (0-60m) 5</p> </div> <p>If you choose Manual, dial by manually clicking on the connection, the device does not dial automatically.</p>
<p>Prefix Delegation</p>	<p>Whether to enable prefix distribution.</p>

2.4.2. IPv6 LAN Setting

DHCPv6 mode

Procedure

1. Navigate to **Network** -> **IPv6 LAN**
2. Select DHCPv6 Status as **Enable**
3. Select DHCPv6 Mode as **stateful** or **Stateless**

The screenshot shows the 'IPv6 LAN Setting' configuration page. The navigation tabs at the top include Status, Network (selected), SIP Account, Phone, and Administration. Below these are sub-tabs for WAN, LAN, IPv6 Advanced, IPv6 WAN, IPv6 LAN (selected), VPN, DMZ, DDNS, Port Setting, and Routing. The main configuration area is titled 'IPv6 LAN Setting' and contains the following fields:

- IPv6 Address: fec0::1
- IPv6 Prefix Length: 64 (0-128)
- DHCPv6 Server: (empty)
- DHCPv6 Status: Disable (dropdown)
- DHCPv6 Mode: Stateless (dropdown)
- Domain Name: (empty)
- Server Preference: 255 (0-255)
- Primary DNS Server: (empty)
- Secondary DNS Server: (empty)
- Lease Time: 86400 (0-86400sec)
- IPv6 Address Pool: (empty) - (empty) / (empty)
- Router Advertisement: (empty)
- Router Advertisement: Disable (dropdown)
- Advertise Interval: 30 (10-1800sec)
- RA Managed Flag: Disable (dropdown)
- RA Other Flag: Enable (dropdown)
- Prefix: (empty) / (empty)
- Prefix Lifetime: 3600 (0-3600sec)

Parameter	Description
IPv6 Address	Enter the fixed IP address received from the ISP.
IPv6 Prefix Length	Default is 64, 0-128
DHCPv6 Server	Whether to enable prefix distribution.
DHCPv6 Status	DHCPv6 Status provides the option to choose between 'disable' and 'enable,' allowing users to control the activation status of DHCPv6 functionality.

DHCPv6 Mode	DHCPv6 Mode offers a choice between stateless and stateful modes, allowing users to opt for dynamic IPv6 address assignment with or without additional configuration parameters.
Domain Name	Domain name of the provider network.
Server Preference	DHCPv6 server preference level.
Primary DNS Server	Enter the primary DNS server address.
Secondary DNS Server	Enter the secondary DNS server address
Lease Time	Enter the expiration date of the IP address assigned by DHCP.
IPv6 Address Pool	Enter the starting range of IPv6 addresses
Router Advertisement	Default is Disable, Enable
Advertise Interval	Enter the time interval for sending advertisements, default 30
RA Managed Flag	Disable, Enable
RA Other Flag	Disable, Enable
Prefix	Enter the IPv6 address prefix.
Prefix Lifetime	Enter the expiration date of the prefix (Prefix) in the IPv6 address

2.4.3. VPN Setting

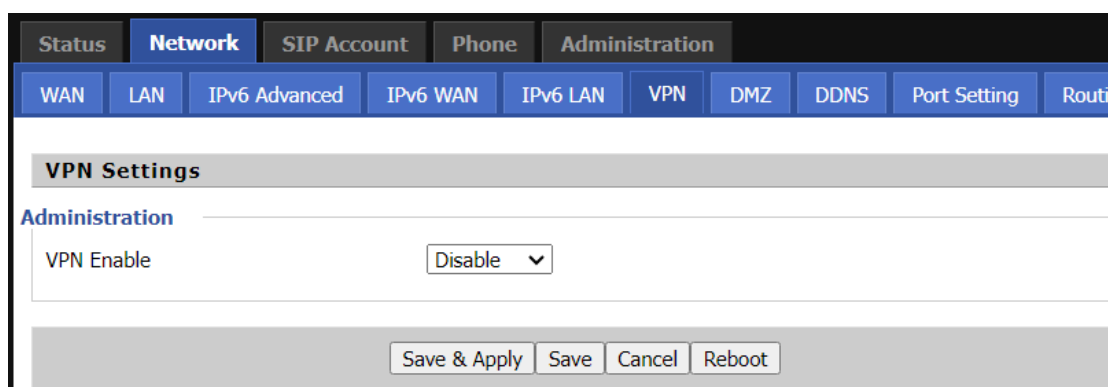
VPN is a technology that creates a private network over a public network. The connection between any two nodes of the VPN network doesn't have the end-to-end physical link required by the traditional private network, but is built on the network platform provided by the public network service provider, and user data is transmitted in the logical link. With VPN technology, users can establish a private connection and transfer data between any two devices on a public network, and the PR08-PRO supports PPTP, L2TP, and OpenVPN.

Topics

[Set PPTP mode](#)

[Set L2TP mode](#)

[Set OpenVPN mode](#)



Set PPTP mode

Procedure

1. Navigate to Network->VPN
2. Select VPN Enable -> **PPTP** mode

The screenshot shows the 'VPN Settings' page under the 'Administration' tab. The 'VPN Enable' dropdown menu is set to 'PPTP'. Below it are input fields for 'Initial Service IP', 'User Name', and 'Password'. At the bottom, there are three dropdown menus, all set to 'Disable', for 'VPN As Default Route', 'MPPE Stateful', and 'Require MPPE'.

Parameter	Description
VPN Enable	Select PPTP.
Initial Service IP	Enter the IP address of the VPN server.
User Name	Enter the user name.
Password	Enter the password.
VPN As Default Route	Whether to enable the VPN as the default route.
MPPE Stateful	Whether to enable the MPPE (Microsoft point-to-point encryption) protocol.
Require MPPE	Option: MPPE uses 40-bit encryption and 128-bit encryption.

Set L2TP mode

Status	Network	SIP Account	Phone	Administration					
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	DMZ	DDNS	Port Setting	Routing

VPN Settings	
Administration	
VPN Enable	L2TP <input type="button" value="v"/>
Initial Service IP	<input type="text"/>
User Name	<input type="text"/>
Password
L2TP Tunnel Name	<input type="text"/>
L2TP Tunnel Password
VPN As Default Route	Disable <input type="button" value="v"/>
L2TP Eogre	Disable <input type="button" value="v"/>
Authentication method	PAP <input type="checkbox"/> CHAP <input type="checkbox"/> CHAPsv2 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/>
MPPE	Disable <input type="button" value="v"/>
Eogre Remote Ip	<input type="text"/>
Birdge WLAN Interface Name	
PR08-285312(ra0)	<input type="checkbox"/>
PR08-5G-285312(rai0)	<input type="checkbox"/>
VLAN ID	<input type="text"/>

Parameter	Description
VPN Enable	Select L2TP (Layer 2 Tunnel Protocol).
Initial Service IP	Enter the IP address of the VPN server.
User Name	Enter the user name.
Password	Enter the password.
L2TP Tunnel Name	Enter the name of the L2TP tunnel.
L2TP Tunnel Password	Enter the password of the L2TP tunnel.
VPN As Default Route	Whether to enable the VPN as the default route.

Set OpenVPN mode

The screenshot shows a web interface with a navigation bar at the top containing tabs: Status, Network, SIP Account, Phone, Administration, WAN, LAN, IPv6 Advanced, IPv6 WAN, IPv6 LAN, VPN, DMZ, DDNS, Port Setting, and Routing. Below the navigation bar is a 'VPN Settings' section with an 'Administration' sub-section. The settings are as follows:

VPN Enable	OpenVPN ▼
OpenVPN TLS Auth	Disable ▼
OpenVPN TLS Crypt	Disable ▼
VPN As Default Route	Disable ▼

Parameter	Description
VPN Enable	Select OpenVPN.
OpenVPN TLS Auth	Whether to enable OpenVPN TLS authentication.
OpenVPN TLS Crypt	Whether to enable OpenVPN TLS encryption.
VPN As Default Route	Whether to enable the VPN as the default route.

2.4.4. DMZ Setting

DMZ (Demilitarized zone) is to solve the problem that the external network users can not access the internal network server after the installation of the firewall. And set up a buffer between the non-secure system and the secure system, also the buffer between internal network and external network of small network area. In this small network area, you can place some server facilities that must be public, such as enterprise Web servers, FTP servers. On the other hand, the internal network is more effectively protected through the DMZ. Because this network deployment, compared with the general firewall solution, the attacker from the external network has one more barrier, after the DMZ host is set in the LAN, the host will be completely exposed to the WAN, which can realize two-way unlimited communication. Adding clients to the DMZ can create insecurity in the local network, so don't use this option easily.

Procedure

1. Navigate to **Network** -> **DMZ Setting**

Demilitarized Zone (DMZ)

DMZ Setting

DMZ Enable Enable ▾

DMZ Host IP Address Get Current PC IP

Parameter	Description
DMZ Enable	Whether to enable the DMZ.
DMZ Host IP Address	Enter the IP address of the specified DMZ host, or obtain the IP address of the current PC with one click.

2.4.5. DDNS Setting

DDNS, namely dynamic DNS server is used to map the user dynamic IP address to a fixed DNS. Every time the user connects to the network, the client program will send the dynamic IP address of the host to the server program located on the host of the service provider, and the server program is responsible for providing DNS services and implementing dynamic domain name resolution.

Procedure

1. Navigate to **Network->DDNS**.

DDNS Setting

DDNS Setting

Dynamic DNS Provider NONE ▾

Account

Password

DDNS URL

Status NONE

Parameter	Description
Dynamic DNS Provider	Default NONE, option: Dyndns.org, www.no-ip.com two DNS service providers.
Account	Enter the account provided by ISP.
Password	Enter the password provided by ISP.
DDNS URL	Enter the dynamic DNS domain name or IP address.

Status	Check whether DDNS is successfully upgraded.
--------	--

2.4.6. Port Setting

On this page, you can set the rate and working mode of each network port. All ports are automatically detected by default, and the maximum speed is 1000Mbps. Manually, you can select the port rate of 10Mbps or 100Mbps, and the working mode of half-duplex or full-duplex is suitable for different network environments of the device.

Procedure

1. Navigate to **Network -> Port Setting**

Port Setting

Port Setting

WAN Port Speed Nego	Auto ▼
LAN1 Port Speed Nego	Auto ▼
LAN2 Port Speed Nego	Auto ▼
LAN3 Port Speed Nego	Auto ▼

Parameter	Description
WAN Port Speed Nego	Default for automatic detection. Optional for 100Mbps full duplex, 100Mbps half duplex, 10Mbps full duplex, 10Mbps half duplex, select the rate negotiation method supported by the WAN port.
LAN1~3 Port Speed Nego	Default automatic detection. Optional for 100Mbps full duplex, 100Mbps half duplex, 10Mbps full duplex, 10Mbps half duplex, select the rate negotiation method supported by the LAN1~3 ports.

2.4.7. Routing Setting

On this page, you can manually add and configure one or more static routing rules in this interface, and route to the destination terminal through the set network interface.

Procedure

1. Navigate to **Network->Routing Setting**
2. Fill in the information in the blank "Add a routing rule", and click Apply
3. A new route will be displayed under the blank "Current Routing Table in the system"

Static Routing Settings

Add a routing rule

Destination	<input type="text"/>
Host/Net	Host ▾
Gateway	<input type="text"/>
Interface	LAN ▾
Comment	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Current Routing Table in the system

No.	Destination	Mask	Gateway	Flags	Metric	Interface	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>							

StaticRoute (Option 121)

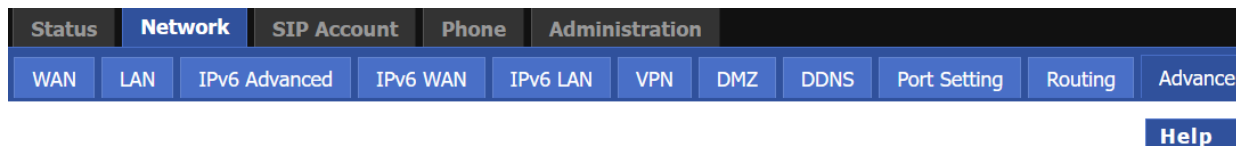
StaticRoute (Option 121)	Disable ▾
--------------------------	-----------

Parameter	Description
Destination	Enter the destination IP address of the routing terminal.
Host/Net	Option: Host or Net, target host or network selection. If Net is selected, enter the subnet mask.
Gateway	Enter the gateway IP address.
Interface	The default is LAN, Option: INTERNET, VOICE, TR069, VPN.
Comment	Enter the description of the route.
Current Routing Table in the system	After entering the preceding routing rules and submit them, you can view them here.
Static Route	Whether to enable static routes.

2.4.8. Advance Setting

Procedure

1. Navigate to **Network** -> **Advance**



Most Nat connections (512-8192)	4096
MSS Mode	<input checked="" type="radio"/> Manual <input type="radio"/> Auto
MSS Value (1260-1460)	1440
Anti-DoS-P	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Conflict Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Conflict Detection Interval(0-3600s)	600

Parameter	Description
Most Nat connections	The default maximum number of Nat connections is 4096.
MSS Mode	Option: Manual, Automatic.
MSS Value	Enter the TCP value to limit the maximum number of bytes sent at the application layer. The default value is 1440.
Anti-DoS-P	This parameter is optional.
IP Conflict Detection	Whether to enable the parameter, the connected terminal will display a message when an IP conflict occurs.
IP Conflict Detection Interval	Enter the interval for detecting IP address conflict. The default value is 600s.

Chapter 3 VoIP Configuration

This section describes VoIP configuration of the device through web interface, include the following topics:

Topics:

[Account Settings](#)

[FXS Setting](#)

[SIP Setting](#)

[VoIP QoS](#)

[Call Setting](#)

3.1. Account Settings

PR08-PRO integrates 8 FXS ports, supports 8 external analog phones, and configures 8 accounts.

On this page, you can set registration information for each FXS port.

Procedure

1. Navigate to **VoIP-> Account**.

Parameter	Description
Start Port Num	This parameter is used to quickly configure multiple accounts in sequence. Enter the number of the first FXS port, such as 1.
End Port Num	This parameter is used to quickly configure multiple accounts in sequence. Enter the number of the end FXS port, such as 8.
Display Name	Enter the extension name of the FXS port. When configure multiple port, this is for the “Start Port Num”.

Phone Number	Enter the extension number registered with the SIP server. When configure multiple port, this is for the "Start Port Num".
Account	Enter the SIP account registered with the SIP server for each FXS port. When configure multiple port, this is for the "Start Port Num".
Password	Enter the password registered with the SIP server for each FXS port. When configure multiple port, this is for the "Start Port Num".
Step Length	Enter the step interval of the account, which is used to quickly configure multiple port accounts. For example, if the step interval enter the 1, the registered account of the start port is increased by 1, if the start account is set to 301, the registered account will be increased to 302, 303, and so on. The phone number, display name, password will also increase by the rules above.
Set button	Click to make the above setting takes effect, please remember to click "save" button when you finish editing.
Start Port Num	Used to clear registered port accounts, enter the number of the first port to be cleared, such as 1.
End Port Num	Used to clear registered port accounts, enter the number of the end port to be cleared, such as 8.
Clear button	Click to clear the port registration account, from the start port number to the end port number.
FXS1~8 Display Name	If you want to configure a single FXS port, enter the phone display name for the port.
FXS1~8 Phone Number	If you want to configure a single FXS port, enter the phone number for the port.
FXS1~8 Account	If you want to configure a single FXS port, enter the SIP account registered with the SIP server for the port.
FXS1~8 Password	If you want to configure a single FXS port, enter the password registered with the SIP server for the port.
FXS1~8 Enable Select box	Whether to enable account registration on the port.

Other Settings button	After you click, you will be automatically transferred to FXS Settings, which are used to set other configuration of the port.
-----------------------	--

After the above basic account information is configured, click Save and apply, you can dial each other. For the configuration of registration server, please check the next chapter.

3.2. FXS Setting

On this page, you can set registration server information, call audio code, fax mode, call service, and speed dial for different ports in batches.

Topics

[Configure SIP Accounts](#)

[Configure Call Audio](#)

[Configure the Fax Service](#)

[Supplementary Service](#)

[Advanced Setup](#)

3.2.1. Configure SIP Accounts

Before configuring, make sure the analog device has access to the FXS port.

Procedure

1. Navigate to **VoIP-> FXS Settings**

Parameter	Description
Port	Select to configure the corresponding FXS port.
Port Enable	Whether to enable the SIP account of this port.
Outgoing Call without Registration	Whether to enable the IP direct dial function without registration.
Missed Call Log	Whether to enable the real-time recording of missed calls.
Proxy Server	Enter the domain name or IP address of the registered SIP server.

Proxy Port	Enter the port number of the VoIP service supported by the SIP server. The default is 5060.
Outbound Server	Enter the domain name or IP address of the outbound server.
Outbound Port	Enter the service port number of the outbound server.
Backup Outbound Server	Enter the domain name or IP address of the backup outbound server.
Backup Outbound Port	Enter the service port number of the backup outbound server.
Display Name	Enter the phone display name of the FXS port.
Phone Number	Enter the phone number registered with the SIP server for the FXS port.
Account	Enter the SIP account name registered with the SIP server for the FXS port.
Password	Enter the password registered with the SIP server for the FXS port.

3.2.2. Configure Call Audio

Audio Configuration

Codec Setup

Audio Codec Type 1	G.711U	Audio Codec Type 2	G.711A
Audio Codec Type 3	G.729	Audio Codec Type 4	G.722
Audio Codec Type 5	G.723	Audio Codec Type 6	G726-32
Audio Codec Type 7	AMR-WB	Audio Codec Type 8	PCMU-WB
Audio Codec Type 9	PCMA-WB	Audio Codec Type 10	AMR-NB
G.723 Coding Speed	5.3k bps	Packet Cycle (ms)	20
Echo Cancel	Enable	Use First Matching Vocoder in 200OK SDP	Disable
Auto Gain Control	Disable	Packet Cycle Follows Remote SDP	Disable
Codec Priority	Remote		
Local DTMF Duration(40~2000ms)	100		

Parameter	Description
Audio Codec Type1~10	Option: G.711A, G.711U, G.722, G.729, G.723, G.726-32, iLBC, ARM-WB, PCMU-WB, PCMA-WB, ARM-NB 11.Select a priority based on the serial number of the coding mode.
G.723 Coding Speed	Option: 5.3kbps, 6.3kbps.
Packet Cycle	Set the RTP packaging period. Option: 10, 30, 40, 50, or 60ms. The default is 20ms.
Echo Cancel	Whether to enable echo cancellation.
Auto Gain Control	Whether to enable automatic gain control, automatic gain control is a control method that makes the gain of the amplifier circuit automatically adjust with the signal strength.
Codec Priority	Option: remote or local priority.
Use First Matching Vocoder in 200OK SDP	When this is se to enable, the device will use the first matching vocoder in the received 200OK SDP as the codec.
Packet Cycle Follows Remote SDP	Whether the packaging period is dominated by the remote end.
Local DTMF Duration	Enter the duration of each DTMF signal, default for 100ms.

3.2.3. Configure the Fax Service

FAX Configuration

FAX Mode	T.30 ▾	Bypass Attribute Value	fax/modem ▾
Enable T.38 CNG Detect	Disable ▾	Enable T.38 CED Detect	Enable ▾
Enable T.38 V21 Detect	Disable ▾	Enable gpmd attribute	Disable ▾
T.38 Redundancy	Disable ▾	Max Fax Rate	14400 ▾

Parameter	Description
FAX Mode	Option: T.30, T.38, Bypass 3 fax modes.
Bypass Attribute Value	Default fax/modem, option: X-fax/X-modem or disable. If the X-fax/X-modem is selected, the fax receiver initiates packets to negotiate fax parameters. The X-fax is a slow fax, and the X-modem is a high-speed fax.
Enable T.38 CNG Detect	Whether to enable CNG detection.
Enable T.38 CED Detect	Whether to enable CED detection.
Enable T.38 V21 Detect	Whether to enable T.38 V21 detection.
Enable gpmd attribute	Whether to enable gpmd attribute.
T.38 Redundancy	Whether to allow T.38 redundancy.
Max Fax Rate	The default fax rate is 14400bps. Option: 9600bps or 4800bp.

3.2.4. Supplementary Service

Supplementary Service Subscription

Supplementary Services

Call Waiting	<input type="text" value="Enable"/>	Hotline	<input type="text"/>
Enable MWI	<input type="text" value="Enable"/>	Voice Mailbox Numbers	<input type="text"/>
MWI Subscribe Enable	<input type="text" value="Disable"/>	VMWI Serv	<input type="text" value="Enable"/>
Disable MWI Tone	<input type="text" value="Disable"/>	Subscribe Expires	<input type="text" value="3600"/>
Outgoing Call Block Password	<input type="text" value="****"/>	Outgoing Call Active Password	<input type="text" value="****"/>
Emergency Call Num	<input type="text"/>	Link Down Hotline	<input type="text" value="Enable"/>
DND	<input type="text" value="Disable"/>		

Speed Dial

Speed Dial 2	<input type="text"/>	Speed Dial 3	<input type="text"/>
Speed Dial 4	<input type="text"/>	Speed Dial 5	<input type="text"/>
Speed Dial 6	<input type="text"/>	Speed Dial 7	<input type="text"/>
Speed Dial 8	<input type="text"/>	Speed Dial 9	<input type="text"/>

Parameter	Description
Call Waiting	Whether to enable call waiting. After enable the function, a special pause tone is heard when another call comes in during the call. You can press *77 to hold a call to connect to a new call. You can switch between two calls by pressing *77.
Hotline	Enter a hotline number. After the number is set successfully, the hotline number is automatically dialed after the phone picks up.
Enable MWI	<p>Whether to enable MWI (message waiting instruction). If you need to use voice mailbox, please enable it.</p> <p>When a voice message or text message is received, MWI has 3 ways to prompt: the LCD interface appears the prompt message, the voice message icon, and the power indicator slowly flashes red. After you listen to or delete all voice messages, the voice icon disappears and the power indicator turns off.</p> <p>The actual prompt way depends on specific phone in use.</p>

Voice Mailbox Numbers	Enter the feature code of the voice mailbox provided by the SIP service provider. For example, the feature code of the voice mailbox on the Elatix platform is *97.
MWI Subscribe Enable	Whether to enable MWI subscription function. After enable the function, the phone will resend the MWI subscription request before the MWI subscription period expires.
VMWI Server	Whether to enable VMWI server function.
Disable MWI Tone	Whether to disable the MWI's message prompt tone.
Subscribe Expires	Enter the MWI subscription period. The default is 3600s.
DND	Whether to enable the DND function. After this function is enabled, all the incoming calls can be rejected.
Speed Dial 2~9	It can quickly set 8 speed dial numbers, enter the target number, and you can call with one key. For example, fill in the number 12345678 in the blank "Speed Dial2", when you dial 2, 12345678 will be dialed.

3.2.5. Advanced Setup

Advanced

SIP Advanced Setup

Domain Name Type <input type="text" value="Enable"/> DTMF Type <input type="text" value="Inband"/> RFC2833 Payload (>=96) <input type="text" value="101"/> Caller ID Header <input type="text" value="FROM"/> Session Refresh Time (sec) <input type="text" value="0"/> Refresher <input type="text" value="UAC"/> Initial Reg With Authorization <input type="text" value="Disable"/> Primary Server Detect Interval <input type="text" value="0"/> NAT Keep-alive Interval (10-60s) <input type="text" value="15"/> Anonymous Call Block <input type="text" value="Disable"/> Use OB Proxy in Dialog <input type="text" value="Disable"/> Enable Reg Subscribe <input type="text" value="Disable"/> Dial Prefix <input type="text"/> Hold Method <input type="text" value="ReINVITE"/> Only Recv Request From Server <input type="text" value="Enable"/> RPort <input type="text" value="Enable"/> SIP Encrypt Type <input type="text" value="Disable"/> SRTP <input type="text" value="Disable"/> Country Code <input type="text"/> Tel URL <input type="text" value="Disable"/> Send Option Only Using Backup <input type="text" value="Disable"/> Remove All Bindings <input type="text" value="Disable"/> VAD&CNG <input type="text" value="Disable"/> Return Code When Refuse <input type="text" value="404(Not Found)"/> SIP Send MAC <input type="text" value="Disable"/> P-Early Media Support <input type="text" value="Enable"/> SIP Session ID Support <input type="text" value="Disable"/> SIPS Scheme Enable When TLS <input type="text" value="Disable"/> SDP UNENCRYPTED SRTP Enable <input type="text" value="Disable"/>	Carry Port Information <input type="text" value="Disable"/> Register Refresh Interval (sec) <input type="text" value="3600"/> Remove Last Reg <input type="text" value="Enable"/> Min Session Timer(sec) <input type="text" value="90"/> Enable SIP OPTIONS <input type="text" value="Disable"/> Reply 182 On Call Waiting <input type="text" value="Disable"/> Max Detect Fail Count <input type="text" value="3"/> Anonymous Call <input type="text" value="Disable"/> Proxy DNS Type <input type="text" value="A Type"/> Complete Register <input type="text" value="Disable"/> Reg Subscribe Interval (sec) <input type="text" value="0"/> User Type <input type="text" value="Phone"/> Request-URI User Check <input type="text" value="Enable"/> Server Address <input type="text"/> VPN <input type="text" value="Disable"/> RTP Encrypt Type <input type="text" value="Disable"/> SRTP Encryption <input type="text" value="AES_CM & ARIA_CM"/> Remove Country Code <input type="text" value="Disable"/> Hold SDP Attribute Inactive <input type="text" value="Disable"/> Enable SIP 100REL <input type="text" value="Disable"/> Early Media Support <input type="text" value="Enable"/> Return Code When DND <input type="text" value="404(Not Found)"/> SIP Send Line <input type="text" value="Disable"/> SIP Remote-Party-ID <input type="text" value="Disable"/> Callee ID Header <input type="text" value="PAID-RPID"/> Use Connection Port <input type="text" value="Enable"/>
--	---

RTP Advanced Setup

RTP Port Min <input type="text" value="0"/>	RTP Port Max <input type="text" value="50000"/>
(0 means auto select)	
Symmetric RTP <input type="text" value="Disable"/>	

Parameter	Description
Domain Name Type	Whether to enable domain name identification in SIP URI.
Carry Port Information	Whether to carry port information of the SIP URI.
DTMF Type	Select the DTMF processing mode. Option: In-band, RFC2833, or SIP Info.

RFC2833 Payload	Enter the payload of RFC2833. The default is 101.
Register Refresh Interval	Refresh interval between two registration messages. The default is 3600s.
Caller ID Header	The default is FROM, option: PAID, PAID-FROM, RPID-PAID-FROM, PAID-RPID-FROM, RPID-FROM. Displays the caller number and caller name after the header field in the packet in the incalling prompt.
Remove Last Reg	Whether to remove the last registration message.
Session Refresh Time	Enter the interval between two sessions. The default is 0s, which means real-time refresh.
Min Session Timer	Enter the minimum session interval. The default is 90s, which means sending a packet every 90 seconds indicates that the call is still on.
Refresher	Option: UAC or UAS for initiating and receiving transaction requests.
Enable SIP OPTIONS	Whether to enable SIP Option detection function.
Initial Reg With Authorization	Whether to carry authentication information during registration.
Reply 182 On Call Waiting	Whether to send 182 SIP message during call waiting.
Primary Server Detect Interval	Enter the Primary Server Detect Interval, the default is 0s.
Max Detect Fail Count	Enter the maximum number of detection failures. The default number is 3.
NAT Keep-alive Interval	Enter the NAT Keep-alive Interval, The value ranges from 10 to 60s.
Anonymous Call	Whether to enable the anonymous call function.

Proxy DNS Type	Set the type of the DNS server. The default type is A. The options are DNS SRV, automatic, and DNS NRPTR.
Enable Reg Subscribe	Whether to enable the registration subscription. If it is enabled, subscription messages will be sent after registration.
Reg Subscribe Interval	Enter the registration subscription time, the default is 0s.
Dial Prefix	Enter the prefix number before dialing. Generally used for external calls.
Hold Method	Option: call hold REINVITE or INFO.
RPort	Whether to enable the RPort mechanism. The Rport field is added to the Via header field of the packet to route the response through the Rport mechanism.
VPN	Whether to enable the VPN function.
SIP Encrypt Type	Whether to encrypt SIP packets. Option: N2C1, N2C2, RC4.
RTP Encrypt Type	Whether to encrypt RTP packets. Option: N2C1, N2C2, CALLID-XOR.
SRTP	Whether to enable the SRTP function.
SRTP Encryption	After SRTP is enabled, the available encryption modes for SRTP are AES_CM&ARIA_CM, ARIA_CM&AES_CM, AES_CM ONLY, ARIA_CM ONLY.
Country Code	Enter the country code to support the channel of the local country.
Remove Country Code	Whether to remove the country code.
Send Option Only Using Backup	Whether to send Option packets only when the backup server is used.

Hold SDP Attribute Inactive	Whether to keep the SDP property inactive.
Enable SIP 100REL	Whether to enable intermediate state response confirmation, which means temporary response confirmation.
VAD&CNG	Whether to enable VAD voice activity detection and CNG comfort noise generation.
Early Media Support	Whether to support early media, if it is enabled, the calling party can still generate media streams with the network when the called party does not answer the call.
Return Code When Refuse	Option: return code 404, 480, 486, 603.
Return Code When DND	Option: DND return code 404, 480, 486, 603.
SIP Remote-Party-ID	Whether to enable the header field of calling party information in SIP calls.
Callee ID Header	Default PAID-RPID, option: DIALED, RFC4916, RPID-PAID-CONTACT, PAID-RPID-CONTACT.
RTP Port Min	Enter the minimum port number for RTP packets. The default is 0s, which means automatically selected.
RTP Port Max	Enter the maximum port for RTP packets.
Symmetric RTP	Whether to enable the symmetric RTP mechanism.

3.3. SIP Setting

On this page, you can set SIP parameters that will be registered with the SIP platform or PBX. Ensure that the parameter settings match those of the device.

Procedure

1. Navigate to VoIP->SIP Setting.

3.3.1. SIP Parameters Setting

SIP Parameters

SIP Parameters

SIP T1	<input type="text" value="500"/>	ms	Max Forward	<input type="text" value="70"/>
SIP User Agent Name	<input type="text"/>		Max Auth	<input type="text" value="2"/>
Reg Retry Intvl	<input type="text" value="30"/>	sec	Reg Retry Long Intvl	<input type="text" value="1200"/> sec
Mark All AVT Packets	<input type="button" value="Enable"/>		RFC 2543 Call Hold	<input type="button" value="Enable"/>
Service Type	<input type="button" value="Common"/>		DNS Refresh Timer	<input type="text" value="0"/> sec
TLS Version	<input type="button" value="TLSv1.0"/>		Signal Port	<input type="text" value="52449"/>
IPv4/IPv6	<input type="button" value="IPv4"/>		Max Random SIP Port	<input type="text" value="60000"/>
All Lines Single SIP Port	<input type="button" value="Enable"/>			
Use Random SIP Port	<input type="button" value="Enable"/>			
Min Random SIP Port	<input type="text" value="50000"/>			

Response Status Code Handling

Retry Reg RSC

Parameter	Description
SIP T1	T1 is the time of each hop on the network. The default is 500ms.
Max Forward	Enter the maximum number of hops allowed. The default is 70.
SIP User Agent Name	Enter the header domain name requested by the SIP UAS.
Max Auth	Enter the maximum number of authentication failures. The default is 2.

Reg Retry Intvl	Enter the interval for sending registration requests again after registration fails. The default is 30s.
Reg Retry Long Intvl	Enter the long interval for sending registration requests again after registration fails. The default is 1200s.
Mark All AVT Packets	Whether to mark all AVT packets.
RFC 2543 Call Hold	Whether to enable REC2543 call hold.
Service Type	Optional service types are common, Broadsoft or AICaTel.
DNS Refresh Timer	Enter the DNS refresh interval. The default is 0s, which means refresh in real time.
TLS Version	Option: v1.0 or v1.2.
IPv4/IPv6	Option: IPv4, IPv6 or IPv4&IPv6.
All Lines Single SIP Port	Whether to allow all lines to use the same SIP port.
Signal Port	Enter the SIP port number, the default is 52449.
Use Random SIP Port	Whether to enable random SIP ports.
Min Random SIP Port	After random SIP port is enabled, enter the minimum random SIP port number (50000 by default).
Max Random SIP Port	After random SIP port is enabled, enter the maximum random SIP port number (60000 by default).

3.3.2. NAT Traversal Setting

NAT traversal refers to network address translation, which converts a private (reserved) address into a valid public IP address.

NAT Traversal			
NAT Traversal			
NAT Traversal	<input type="text" value="Disable"/>	STUN Server Address	<input type="text"/>
NAT Refresh Interval (sec)	<input type="text" value="60"/>	STUN Server Port	<input type="text" value="3478"/>

Parameter	Description
NAT Traversal	Whether to disable the NAT traversal mode or enable the STUN mode.
STUN Server Address	STUN is the application of NAT session traversal. Enter the IP address assigned by the NAT device to the STUN client.
NAT Refresh Interval	Enter the interval for refreshing NAT. The default is 60s.
STUN Server Port	Enter the STUN service port number. The default is 3478.

3.4. VoIP QoS

QoS services can improve the quality of voice applications.

Procedure

1. Navigate to **VoIP** -> **VoIP QoS**.

QoS Settings

Layer 3 QoS

SIP QoS(0-63)	<input type="text" value="46"/>
RTP QoS(0-63)	<input type="text" value="46"/>

Parameter	Description
SIP QoS / RTP QoS	Enter the DSCP value of SIP/RTP packets. The value ranges from 0 to 63. For voice traffic transmission, the general DSCP value is set to 46 by default.

3.5. Call Setting

On this page, you can configure the call volume, ring tone, call transfer, function keys, CPC control, digital map, and call log.

Topics

[Volume Settings](#)

[Regional ringtone Settings](#)

[Call Forward](#)

[Feature Code](#)

[CPC Control](#)

[FXS Port Polarity Configuration](#)

[Miscellaneous](#)

[Dial Rule](#)

[Call Log](#)

3.5.1. Volume Settings

Procedure

1. Navigate to **Phone -> Preferences**

Preferences	
Volume Settings	
Handset Input Gain	5 ▾
DTMF Volume (0~-45)	-19
Handset Volume	5 ▾

Parameter	Description
Handset Input Gain	The value of the handset MIC input volume ranges from 0 to 7. The default is 5.
Handset Volume	The value of the handset speaker output volume ranges from 0 to 7. The default is 5.
DTMF Volume	Indicates the audio power level of the DTMF signal. It ranges from 0 to -45dbm. The default is -19dbm.

3.5.2. Regional ringtone Settings

Regional

Tone Type	USA <input type="button" value="v"/>		
Dial Tone	<input type="text"/>		
Busy Tone	<input type="text"/>		
Off-hook Warning Tone	<input type="text"/>		
Ring Back Tone	<input type="text"/>		
Call Waiting Tone	<input type="text"/>		
Ringing Cadence	<input type="text"/>		
Holding Tone	<input type="text"/>		
Min Jitter Delay (0-600ms)	<input type="text" value="60"/>	Max Jitter Delay (20-1000ms)	<input type="text" value="240"/>
Ringing Time (10-300sec)	<input type="text" value="60"/>		
Ring Waveform	Sinusoid <input type="button" value="v"/>	Ring Voltage (40-63 Vrms)	<input type="text" value="45"/>
Ring Frequency (15-30Hz)	<input type="text" value="25"/>	VMWI Ring Splash Len (0.1-10sec)	<input type="text" value="0.5"/>
Flash Time Max (0.2-1sec)	<input type="text" value="0.9"/>	Flash Time Min (0.1-0.5sec)	<input type="text" value="0.1"/>
R Timeout Interval(min 1s)	<input type="text" value="1"/>		

Parameter	Description
Tone Type	Option: ringtone type in different countries.
Dial Tone	Enter the key tone script for dialing, including rhythm and frequency: <ul style="list-style-type: none"> · Syllable - total length (segment: On = time, off = time (frequency)) · Frequency - dBm @ frequency For example, 350@-19,440@-19; (2. 1 /. 1/1 + 2); 10(* / 0 / 1 + 2).
Busy Tone	Enter the tone script of the busy tone.
Off-hook Warning Tone	Enter the tone script of the off-hook warning tone.
Ring Back Tone	Enter the tone script of the ring back tone.
Call Waiting Tone	Enter the tone script of the call waiting tone.
Ringing Cadence	Enter the tone script of the ringing cadence.
Holding Tone	Enter the tone script of the holding tone.
Min Jitter Delay	Enter the minimum jitter delay. The jitter delay of the device uses the adaptive mechanism. The default is 60ms.

Max Jitter Delay	Enter the minimum jitter delay. The default is 240ms.
Ringing Time	Enter the ring duration. The default is 60s.
Ring Waveform	Option: Sinusoid or Trapezoid.
Ring Voltage	Enter the ringing voltage, default 45Vrms.
Ring Frequency	Enter the ringing frequency, default 25Hz.
VMWI Ring Splash Len	Enter the VMWI ringing duration, default 0.5s.
Flash Time Max	Enter the maximum interval between two flapping springs. The default is 0.9s.
Flash Time Min	Enter the minimum interval between two flapping springs. The default is 0.1s.
R Timeout Interval	The R key is the key on the analog phone, used to hang up/hold the call, or with the digital key can transfer the call, form a tripartite meeting, etc.Enter the timeout period of the key. The default is 1s.

3.5.3. Call Forward Settings

On this page, you can set different call forward types, including unconditional forward, busy forward, no answer forward, and hang up forward.

Features

All Forward	<input type="button" value="Disable"/>	Busy Forward	<input type="button" value="Disable"/>
No Answer Forward	<input type="button" value="Disable"/>	Transfer On-hook	<input type="button" value="Enable"/>

Call Forward

All Forward	<input type="text"/>	Busy Forward	<input type="text"/>
No Answer Forward	<input type="text"/>	No Answer Timeout(S)	<input type="text" value="20"/>

Parameter	Description
All Forward	Whether to enable unconditional call transfer. After it is enabled, you need to enter the destination extension number. When the peer end calls the original extension, the call is automatically transferred to the specified destination extension.
Busy Forward	Whether to enable transfer on busy. After this is enabled, you need to enter the destination extension number. When the peer end calls the original extension, but the original extension is in a call, then the call is automatically transferred to the destination extension.
No Answer Forward	Whether to enable the call transfer without answer function. After it is enabled, you need to enter the destination extension number and timeout period of no answer. When the peer end calls the original extension, but the original extension does not answer, the call is automatically transferred to the destination extension after the timeout period lasts.
Transfer On-hook	Whether to enable transfer on hang up. After it is enabled, when the peer end calls the original extension but the original extension ends the call, the call is automatically transferred to the destination extension.
All Forward	Enter the destination extension after All Forward is enabled.

Busy Forward	Enter the destination extension after Busy Forward is enabled.
No Answer Forward	Enter the destination extension after No Answer Forward is enabled.
No Answer Timeout	Enter the ring duration when no answers. The default is 20s.

3.5.4. Feature Code

On this page, you can set the feature codes of different function keys to quickly implement different functions with digital keys.

Feature Code

Hold Key Code	<input type="text" value="*77"/>	Conference Key Code	<input type="text" value="*88"/>
Transfer Key Code	<input type="text" value="*98"/>	IVR Key Code	<input type="text" value="****"/>
Flash Digit Control	<input type="text" value="Disable"/>		
Enable R Key	<input type="text" value="Disable"/>	R Key Cancel Code	<input type="text" value="R1"/>
R Key Hold Code	<input type="text" value="R2"/>	R Key Transfer Code	<input type="text" value="R4"/>
R Key Conference Code	<input type="text" value="R3"/>	R Key Reject 2nd Call Code	<input type="text" value="R0"/>
Flash As R Key	<input type="text" value="Disable"/>	Speed Dial Code	<input type="text" value="*74"/>
Cfwd All Act Code	<input type="text" value="*72"/>	Cfwd All Deact Code	<input type="text" value="*73"/>
Cfwd Busy Act Code	<input type="text" value="*90"/>	Cfwd Busy Deact Code	<input type="text" value="*91"/>
Cfwd No Ans Act Code	<input type="text" value="*52"/>	Cfwd No Ans Deact Code	<input type="text" value="*53"/>
DND Act Code	<input type="text" value="*78"/>	DND Deact Code	<input type="text" value="*79"/>

Parameter	Description
Hold Key Code	Enter the feature code, you can dial the feature code to hold a call quickly. The default is *77.
Conference Key Code	Enter the feature code of a three-party conference. The default is *88.
Transfer Key Code	Enter the feature code of the call transfer. The default is *98.
IVR Key Code	Enter the feature code of the voice menu. The default is ****.
Enable R Key	Whether to enable R key.
R Key Cancel Code	After the R key is enabled, the R key can be combined with numeric keys to cancel the key function. The value ranges from R+0 to R+9.
R Key Hold Code	After the R key is enabled, the R key can be combined with numeric keys to hold a call. The value ranges from R+0 to R+9.
R Key Transfer Code	After the R key is enabled, the R key can be combined with numeric keys to transfer calls. The value ranges from R+0 to R+9.
R Key Conference Code	After the R key is enabled, the R key can be combined with numeric keys to complete the conference function. The value ranges from R+0 to R+9.

R Key Reject 2nd Call Code	After the R key is enabled, the R key can be combined with numeric keys to reject the second call. The value ranges from R+0 to R+9.
Flash As R Key	Whether to use the R key as the Flash break key.
Speed Dial Code	Enter the feature code of the speed dial number. The default value is *74.

3.5.5. CPC Control

On this page, you can set the CPC function. That is, after the peer device hangs up the call, the analog phone under the PR08-PRO automatically hangs up. The hang up process changes from busy tone to silent tone, and finally to off tone.

CPC Control

CPC Enable	<input type="text" value="Disable"/>	CPC Duration (sec)	<input type="text" value="0"/>
CPC Delay (sec)	<input type="text" value="0"/>		

Parameter	Description
CPC Enable	Whether to enable the CPC function.
CPC Duration	Enter the silence duration before the local device hangs up. The default is 0s.
CPC Delay	Enter the busy tone duration before the local device hangs up. The default is 0s.

3.5.6. FXS Port Polarity Configuration

On this page, you can set the polarity reversal of an FXS port. It is used with an FXO gateway to detect the polarity reversal signal to determine whether an analog phone connected to establish a call or hangs up. For call charging, you can also record the start time and end time of a call.

FXS Port Polarity Configuration

Idle Polarity	Forward ▾	Caller Conn Polarity	Forward ▾
Called Conn Polarity	Forward ▾		

Parameter	Description
Idle Polarity	Choose the polarity which you want to set before a call is connected from the drop-down menu. The possible values are Forward or Reverse. The default value is Forward.
Caller Conn Polarity	Choose the polarity which you want to set after an outbound call is connected from the drop-down menu. The possible values are Forward or Reverse. The default value is Forward. When reverse is selected a reverse signal is generated when the local end initiates a call. When the FXO gateway detects the signal, it initiates a call to the peer end, which means the call starts.
Called Conn Polarity	Choose the polarity which you want to set after an inbound call is connected from the drop-down menu. The possible values are Forward or Reverse. The default value is Forward. When reverse is selected, a reverse signal is generated when the local end picks up the phone and answers the call, indicating that the call is started. After the call ends, a reverse pole signal is generated, indicating that the call is over.

3.5.7. Miscellaneous

On this page, you can set other call functions, such as incoming call display and dial timeout.

Miscellaneous

Loop Current	<input type="text" value="26"/>	Impedance Matching	<input type="text" value="US PBX,Korea,Taiwan(600)"/>
CID Service	<input type="text" value="Enable"/>	CWCID Service	<input type="text" value="Disable"/>
Caller ID Method	<input type="text" value="Bellcore"/>	Call Immediately Key	<input type="text" value="#"/>
Dial Time Out (IDT)	<input type="text" value="5"/>	Enable Escaped Char	<input type="text" value="Disable"/>
ICMP Ping	<input type="text" value="Disable"/>	On-hook Voltage	<input type="text" value="48"/>
Bellcore Style 3-Way Conference	<input type="text" value="Disable"/>	Hook Flash Number Enable	<input type="text" value="Disable"/>
Ring Offset (0-50 V)	<input type="text" value="0"/>		
Info Content Type	<input type="text" value="broadsoft"/>		

Parameter	Description
Loop Current	Enter the circuit current value after off-hook. The default is 26A.
Impedance Matching	It used to adjust load power and suppress signal reflection, default US PBX,Korea,Taiwan(600).
CID Service	Whether to enable caller ID. After it is enabled, the phone number of an incoming call is displayed when the phone rings.
CWCID Service	Whether to enable the CWCID (Call Waiting Calling Number Identification) service. After it is enabled, call waiting phone numbers are displayed.
Caller ID Method	Option: Caller ID method: Bellcore, DTMF, ETSI, RAS, etc.
Dial Time Out	Enter the delay period from dialing to auto dial, the default is 5s.
Call Immediately Key	Whether to enable special characters as call keys. The value can be * or #.
ICMP Ping	Whether to enable the ICMP Ping service. When enabled, the phone pings the SIP server at intervals. Otherwise, an empty hello packet will be sent to the SIP server.
Enable Escaped Char	Whether to allow the use of special characters to escape.

Bellcore Style 3-way Conference	Whether to enable Bellcore Style conference. When this is enable, user can create 3-way conference with “flash”button.
On-Hook Voltage	Enter the off-hook voltage. The default value is 48V.
Ring Offset(0-50V)	Enter the Offset voltage.The default value is 0V.
Info Content Type	Choose the type of Info content from Broadsoft, hook-flash, telephone-event, dtmfinfo+xml, dtmf-relay.
Hook Flash Number Enable	Whether to enable Hook Flash Number

3.5.8. Dial Rule

On this page, you can set the digit map function and define call rules for FXS accounts.

Procedure

1. Navigate to **Phone -> Dial Rule**

Dial Rule

General

Dial Rule Disable ▾

Unmatched Policy Accept ▾

No.	Line	Digit Map	Action	Move Up	Move Down	
	Line1 ▾		Deny ▾			<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Parameter	Description
Dial Rule	Optioanl whether to enable the dial rule function, All subsequent Settings are based on enabling this.
Unmatched Policy	Whether to accept unmatched policies: If reject, only the number in the digitmap rule can be successfully called. If accept, you can successfully call any number, not limited to the number of the data rule.

Line	<p>Since PR08-PRO supports 8 accounts, you can choose account 1 to account 8.</p>
Digit Map	<p>Enter the digital map rule: Support valid characters: 0 1 2 3 4 5 6 7 8 9 * #; Support enter the extension numbers with valid characters, such as 1500; Support replacement rules, such as <5:2>, then the entered 5 is replaced with 2; Support matching sequence extension, such as [2-5], then support 2, 3, 4, 5; Support matching x extension, such as x, support 1, 2, 3 and any other legal characters; Support matching x. extension, such as 01., support 01, 011, 0111.....; Support interval dial tone, such as 1,2, there will be a dial tone after dialing 1, and the dial tone will end after entering 2; Support setting delay, such as 1500T10, after dialing 1500, it will be delayed for 10s to automatically call out.</p>
Action	<p>Option: deny or dial out. After the digit map rule is enabled, if set as dial out, which means can be called out normally; if set as deny, the number of the digit map rule will fail to call out.</p>

3.5.9. Call Log

On this page, you can view the local number, remote number, call start time, and call duration in call records, including the redial call list (outgoing call list), answer call list, and missed call list.

Procedure

1. Navigate to **Phone -> Call Log**

Redial List					
Index	Local Number	Remote Number	Start Time	Duration	<input type="checkbox"/>
1	7008	123	09/22 16:05	00:00:01	<input type="checkbox"/>
2	7008	123	09/22 16:05	00:00:01	<input type="checkbox"/>
3	801	802	09/22 16:07	00:00:01	<input type="checkbox"/>
4	801	802	09/22 16:35	00:00:12	<input type="checkbox"/>
5	803	801	09/22 16:38	00:00:11	<input type="checkbox"/>
6	801	802	09/22 16:38	00:00:07	<input type="checkbox"/>
7	804	804	09/22 16:41	00:03:19	<input type="checkbox"/>
8	804	804	09/22 16:41	00:03:01	<input type="checkbox"/>
9	802	83	09/22 16:42	00:00:17	<input type="checkbox"/>
10	802	803	09/22 16:42	00:00:12	<input type="checkbox"/>
11	802	03	09/22 16:43	00:00:14	<input type="checkbox"/>

Answered Calls					
Index	Local Number	Remote Number	Start Time	Duration	<input type="checkbox"/>
1	801	803	09/22 16:38	00:00:09	<input type="checkbox"/>
2	801	803	09/22 16:54	00:00:21	<input type="checkbox"/>
3	804	803	09/22 16:58	00:00:11	<input type="checkbox"/>
4	801	803	09/22 17:15	00:00:05	<input type="checkbox"/>

Missed Calls					
Index	Local Number	Remote Number	Start Time	Duration	<input type="checkbox"/>
1	802	804	09/22 16:46	00:00:00	<input type="checkbox"/>

Chapter 4 Management Configuration

This section mainly introduces software upgrade, NTP time zone, administrator settings, Power Out setting, Remote control and other related configurations.

Topics:

[Management](#)

[Firmware Upgrade](#)

[Scheduled Tasks](#)

[Provision](#)

[SNMP](#)

[TR069](#)

[Power Out](#)

[Diagnosis](#)

4.1. Management

On this page, users can upload configuration files to configure the device, configure the web login account and password, configure the display language, configure the VPN, configure the telnet, configure the time and date, configure the system local and remote logs, configure the factory status, and so on.

Topics

[Configure File Upload & Download](#)

[Administrator Settings](#)

[NTP Settings](#)

[Syslog Setting](#)

[Factory Default Setting](#)

4.1.1. Configure File Upload & Download

Procedure

1. Navigate to Administration -> Management.

Save Config File

Config File Upload & Download

Local File

Choose File

No file chosen

Upload

Download

Parameter	Description
Local File	Click the Select File button to go to local file browsing and select the configuration file in cfg format.
Upload	After selecting the configuration file, click the Upload button to import the configuration file to the web background.
Download	Click the Download button to automatically download the configuration file in cfg format.

4.1.2. Administrator Settings

PR08-PRO supports 3 user levels, which are basic, normal, admin. The display and configuration contents of different user levels after logging in to the web are different.

And the default login password for admin is last 6 digits of SN number.

After obtaining the device, User should change the password in time to avoid the unavailability of the device caused by abnormal modification of advanced Settings.

On this page, you can set a new user name and password. The password must be confirmed twice and contains a maximum of 25 characters.

Administrator Settings

Password Reset

User Type	Admin User ▾
New User Name	admin
New Password	<input type="text"/> (The maximum length is 25)
Confirm Password	<input type="text"/>

The administrator can also change the display language here, the default is English, and 20 languages can be selected.

Language

Language	English ▾
----------	-----------

The administrator can also enable the VPN function here.

VPN Access

Management Using VPN	Disable ▾
----------------------	-----------

The administrator can also set up remote web login here.

Web Access

Remote Web Login	Enable ▾
Https Web Access	Enable ▾
Web Port	80
Web SSL Port	443
Web Idle Timeout (0 - 60min)	50
Allowed Remote IP (IP1;IP2;...)	0.0.0.0

Parameter	Description
Remote Web Login	Whether to enable or disable the Remote Web Login.
Https Web Access	Whether to enable Https access to the Web, Https access is to use SSL protocol for access, you need to set up the website as an SSL secure site.
Web Port	Fill in the port number for logging in the Web via Internet port and PC port, for Http server, the general default is 80.
Web SSL Port	Support https access, can be connected to the device via SSL, fill in the SSL port number, generally default 443.
Web Idle Timeout	Fill in the Web idle timeout time, i.e., no operation on the Web idle, will automatically exit the login, the length of the default 5 minutes.

Allowed Remote IP	Fill in the IP address of the remote device, so that it supports remote access to the Web, more than one separated by a semicolon.
-------------------	--

Administrators can also set Telnet here.

Telnet Access

Remote Telnet	<input type="button" value="Enable"/> ▾
Telnet Port	<input type="text" value="23"/>
Allowed Remote IP (IP1;IP2;...)	<input type="text" value="0.0.0.0"/>
HostName	<input type="text" value="PR08"/>

Parameter	Description
Remote Telnet	Whether to enable remote Telnet function to support line other devices Telnet connection to the device.
Telnet Port	Fill in the port number for Telnet to the device, default 23.
Allowed Remote IP	Fill in the IP address of the remote device to enable it to connect to the device remotely, and separate more than one device with a semicolon.
HostName	Fill in the name of the device to be displayed after successful connection, the default is the device model PR08-PRO.

4.1.3. NTP Settings

The administrator can set the time and date here.

Time/Date Setting	
NTP Settings	
NTP Enable	Enable ▾
Option 42	Disable ▾
Current Time	2023 - 10 - 08 . 14 : 16 : 48
Sync with host	Sync with host
Time Zone	(GMT+08:00) China Coast, Hong Kong ▾
Primary NTP Server	pool.ntp.org
Secondary NTP Server	cn.pool.ntp.org
NTP synchronization (1 - 1440min)	60

Parameter	Description
NTP Enable	Whether to enable the NTP (Network Time Protocol) switch, used to synchronize the time.
Option 42	Whether to enable DHCP Option 42, which is used to specify the server that provides NTP/SNTP service.
Current Time	Displays the current date and time: year, month, day, hour, and second.
Sync with host	Click it to synchronize the time of the device with the PC host automatically.
Time Zone	Optional time zone, default is (GMT+08:00) China Coast, Hong Kong.
Primary NTP Server	Fill in the IP address or domain name of the preferred NTP server.
Secondary NTP Server	Fill in the IP address or domain name of the alternative NTP server.
NTP synchronization	Fill in the NTP synchronization period, the period length can be 1~1440 minutes, default 60 minutes.

4.1.4. Syslog Setting

System Log Setting

Syslog Setting

Enable Syslog	Enable ▾
Syslog Level	INFO ▾
Enable Remote Syslog	Disable ▾
Remote Syslog Server	<input type="text"/>

Parameter	Description
Enable Syslog	Whether to enable system logging function.
Syslog Level	System logging level, option: INFO, DEBUG. DEBUG is the lowest level and can be used for development and debugging; INFO information log, used to feedback the current state of the system to the end user, can not be changed arbitrarily.
Enable Remote Syslog	Whether to enable the remote system log function.
Remote Syslog Server	Fill in the IP address or domain name of the server for remote system logging.

4.1.5. Factory Default

You can restore the factory by clicking the button on the Web or Reset button on the device.

Procedure

1. Navigate to **Administration > Management -> Factory Default Setting**
2. Click the Button
3. Reboot the device if there is a prompt
4. You can also long press the Reset button on the device for 5s to reset the device, or short press for less than 5s to reboot the device

Note: please make sure you save the settings before reboot.

Factory Default Setting

Factory Default Setting

Factory Default Lock

Disable ▾

Factory Default

Reset to Factory Default

Factory Default

Parameter	Description
Factory Default Lock	Whether to lock the restore factory state, when it is on, the device will not be the factory default state after reset.
Reset to Factory Default	When clicked, the device will be restored to the factory default state.

4.1.6. Firmware Upgrade

On this page, you can upgrade the device firmware version.

Path: Administration->Firmware Upgrade.

Firmware Management

Firmware Upgrade

Local Upgrade

No file chosen

Parameter	Description
Local Upgrade	After clicking, you can browse the local folder and select the standard firmware version file provided by Vola.
Upgrade	After clicking, the device starts to upgrade the firmware and the upgrade process cannot be interrupted.

4.2. Scheduled Tasks

On this page, you can set scheduled tasks, including scheduled device reboot and scheduled PPPoE.

Procedure

1. Navigate to **Administration** -> **Scheduled Tasks**.

Scheduled Tasks

Scheduled Reboot

Scheduled Reboot	Disable ▾
Scheduled Mode	Every Day ▾
Time	00 ▾ : 00 ▾

Scheduled PPPoE

Scheduled PPPoE	Disable ▾
Scheduled Mode	Every Day ▾
Time	00 ▾ : 00 ▾

Parameter	Description
Scheduled Reboot	Whether to enable timed reboot of the device.
Scheduled Mode	After enabling timed reboot, you can select the period of reboot: daily, weekly, once only, running days. If you select Daily, you need to select a specific time, i.e., restart the device at a certain time and minute every day; If you select Weekly, you need to check the weekday, and you need to select a specific time, i.e., restart the device at a certain time and minute on the weekday;

	<p>If you select Once only, you need to select a specific time, that is, only reboot the device once at a certain time and minute on the set day;</p> <p>If you choose to run days, you need to fill in the value of days running from the day, and you need to choose a specific time, that is, since the day of the setting of a few days from the day of a certain hour and a certain minute will reboot the device.</p>
Time	Select a specific reboot time (such and such a minute).
Scheduled PPPoE	Enable or disable the PPPoE reboot timer function.
Scheduled Mode	<p>After enabling Timed Reboot PPPoE, you can select the period of reboot: daily, weekly, and only once.</p> <p>If you select Daily, you need to select a specific time, i.e., restart PPPoE at a certain time and minute every day;</p> <p>If you select Weekly, you need to check the weekday, and you need to select a specific time, i.e., restart PPPoE at a certain time and minute on the weekday;</p> <p>If you select Once only, you need to select a specific time, that is, restart PPPoE only once at a certain time and minute on the set day;</p>
Time	Select a specific time to restart (a certain hour and a certain minute).

4.3. Provision

On this page, you can configure Provision related parameters, which supports 3 methods, TFTP (support option 66), HTTP and HTTPS.

Provision	
Configuration Profile	
Provision Enable	Enable ▾
Resync on Reset	Enable ▾
Resync Random Delay (sec)	40
Resync Periodic (sec)	3600
Resync Error Retry Delay (sec)	3600
Forced Resync Delay (sec)	14400
Resync after Upgrade	Enable ▾
Resync from SIP	Enable ▾
Option 66	Enable ▾
Option 67	Enable ▾
Config File Name	\$(MA)
User Agent	
HTTP Authentication	Basic ▾
User Name	
Password	
Profile Rule	https://rps.flyingvoice.net/config/\$(MA)?mac=\$(MA)&sc
Configuration Profile2	
User Agent	
HTTP Authentication	Basic ▾
User Name	
Password	
Profile Rule	https://prv4.flyingvoice.net/config/\$(MA)?mac=\$(MA)&sc
Firmware Upgrade	
Enable Upgrade	Enable ▾
Upgrade Error Retry Delay (sec)	3600
Upgrade Rule	

Parameter	Description
Provision Enable	Whether to enable the Provision.
Resync on Reset	Whether configuration synchronization is triggered at each reboot except for parameter updates and firmware upgrades.

Resync Random Delay	<p>Sets the maximum delay time for requesting file synchronization, default for 40 seconds.</p> <p>With the interval from 0 to 40 seconds, a value is generated randomly and the device waits for the interval of this value before requesting the Provision server.</p> <p>When filled in with 0, it indicates that the feature is disabled as a way to prevent a large number of devices from sending too many server requests at the same time.</p>
Resync Periodic	Fill in the cycle time for the device to automatically resynchronize with the server, default 3600 seconds.
Resync Error Retry Delay	Fill in the interval time for re-synchronization again after synchronization error, default 3600 seconds.
Forced Resync Delay	Fill in the forced synchronization time, i.e., 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 the interval time to guarantee that the device is forced to re-synchronize after being idle, default 14400 seconds.
Resync after Upgrade	Whether to trigger resynchronization after each firmware upgrade.
Resync From SIP	Whether to enable resynchronization from SIP.
Option 66	Whether to allow enabling DHCP option 66.
Option 67	Whether to allow enabling DHCP option 67.
Config File Name	Fill in the configuration file name.
User Agent	Fill in the user agent name.
HTTP Authentication	HTTP authentication methods, option: Basic, Digest. Basic authentication sends the user and password encrypted by base64 to the server for authentication; Digest authentication is to combine the specific value in the 401 message responded by the server with the user name and password to get a value by irreversible digest algorithm, and then send the user name and this digest value to the server for authentication.
User Name	Fill in the username required for HTTP authentication.
Password	Fill in the password for HTTP authentication.

Profile Rule	Fill in the path URL of the configuration file to complete the synchronization command, which is a TCP/IP operation and an associated URL. The TCP/IP operation can be TFTP, HTTP, or HTTPS.
Enable Upgrade	Whether to upgrade the firmware when resynchronizing.
Upgrade Error Retry Delay	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, default 3600 seconds.
Upgrade Rule	Fill in the path where the upgrade firmware file is located under the server.

4.4. SNMP

SNMP Simple Network Management Protocol, users can configure the PC and PR08-PRO in the same network segment, through the function with the MIB file to realize the automatic configuration of the device information node.

SNMP Configuration

SNMP Configuration

SNMP Service	Disable ▾
Trap Server Address	<input type="text"/>
Read Community Name	public
Write Community Name	private
Trap Community	trap
Trap Period Interval (sec)	300

Parameter	Description
SNMP Service	Whether to enable SNMP function.
Trap Service Address	Fill in the Trap's server address, usually the IP address of the PC.
Read Community Name	Fill in the read-only passphrase, the password and string value used to request information from the device via SNMP.
Write Community Name	Fill in the Read/Write passphrase, the password and string value used to write configuration values to the device via SNMP.
Trap Community	Fill in the passphrase, the password and string value used to retrieve Trap from the device.
Trap Period Interval (sec)	Fill in the time interval for Trap to be sent from the device, default 300 seconds.

4.5. TR069

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

TR-069 Configuration

ACS

TR-069 Enable	<input type="text" value="Disable"/>
CWMP	<input type="text" value="Enable"/>
TLS version	<input type="text" value="TLSv1"/>
ACS URL	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Enable Periodic Inform	<input type="text" value="Enable"/>
Periodic Inform Interval	<input type="text" value="3600"/>

Connection Request

User Name	<input type="text" value="PR08"/>
Password	<input type="text" value="*****"/>

Parameter	Description
TR-960 Enable	Optional to enable or disable the TR069 function.
CWMP	Whether to enable the CWMP protocol function, which is mainly used for remote management of network devices with a large number of configurations in the gateway center.
TLS version	Optional version V1, V1_2 of TLS.
ACS URL	Fill in the URL of the server for TR069, the default is the ACS server address of Vola Networks
User Name	Fill in the username for the TR069 server connection.
Password	Fill in the password used for the TR069 server connection.
Enable Periodic Inform	Optionally enable periodic notification to inform the user periodically about connection settings.
Periodic Inform Interval	Fill in the time interval for the TR069 server to send periodic notification messages, default 3600 seconds.
User Name	User name of the TR069 server connection to the PR08-PRO.
password	Password for the TR069 server to connect to the PR08-PRO.

4.6. Power Out

This interface allows users to set the PR08-PRO to support PoE and UPS discharges in different states.

Power Out Configuration

Power Out Configuration

UPS

AutoSwitch ▾

POE1

AutoSwitch ▾

POE2

AutoSwitch ▾

Parameter	Description
UPS Out	<p>You can select 3 states: AutoSwitch, Always On, Always Off, default for AutoSwitch.</p> <p>AutoSwitch: When PR08-PRO is connected to DC normal power supply, or when it is connected to standard 65W mobile power supply, it automatically turns on the UPS discharge; When PR08-PRO is connected to non-65W mobile power supply, it will automatically turn off the UPS discharge.</p> <p>Always On: UPS discharge is always on in any state. Always Off: UPS discharge is always turned off in any state.</p>
WAN1/WAN2 PoE Out	<p>You can select 3 states: Autoswitch, always on, always off, default auto switch.</p> <p>AutoSwitch: When PR08-PRO is connected to DC normal power supply, or when it is connected to standard 65W mobile power supply, it will automatically turn on the network port PoE Out; When PR08-PRO is connected to non-65W mobile power supply, it will automatically turn off the UPS discharge.</p> <p>Always On: Network port PoE Out is always turned on in any state. Always Off: Network port PoE Out is always turned off in any state.</p>

4.7. Diagnosis

Users can perform packet tracing, ping test and traceroute test in this interface to diagnose the connection status of the device.

Topics

[Packet Trace](#)

[Ping Test](#)

[Traceroute test](#)

4.7.1. Packet Trace

Users can use the packet tracing function to intercept the sent packets. Click Start button to start data tracing, click Stop to stop capturing packets. Click Save button to save the captured packets.

Packet Capture

Packet Capture

Tracking Interface	WAN ▾
Filtering Rule	ALL Packets ▾
Upload Packet Enable	Disable ▾
Packet Capture	<input type="button" value="start"/> <input type="button" value="stop"/> <input type="button" value="save"/>

4.7.2. Ping Test

Fill in the destination IP address or host name and click Submit, the device will execute the ping test.

Ping Test

Ping Test

Dest IP/Host Name	<input type="text"/>
<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>	
<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>

4.7.3. Traceroute test

Fill in the destination IP address or host name, select IPv4 or IPv6, and then click Submit, the device will execute route traceroute test.

Traceroute Test

Traceroute Test

Dest IP/Host Name

IPv4/IPv6 ▾