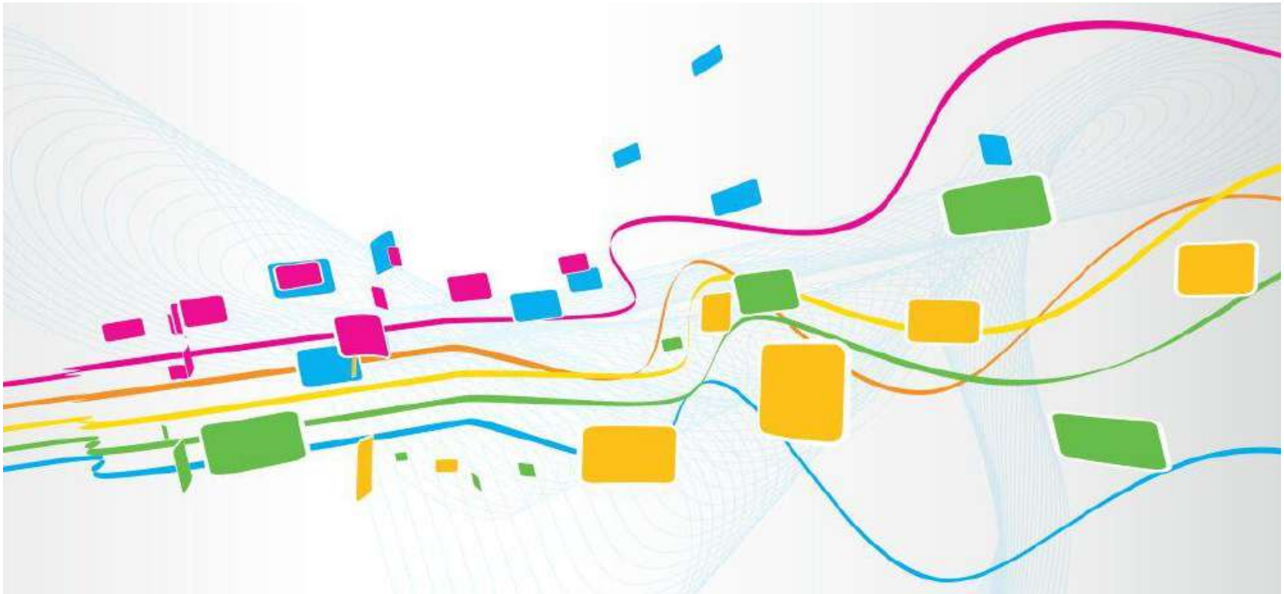
DAG Series FXO Analog Gateway

User Manual V2.0



Shenzhen Dinstar Co., Ltd.

Address: Floor 18, Building 7A, Vanke Cloud City Phase 1, Xingke 1st Street, Xili Sub-district, Nanshan District, Shenzhen.

Postal Code: 518052

Telephone: +86 755 61919966

Fax: +86 755 2645 6659

Email：sales@dinstar.com

Website: www.dinstar.com

Preface

Welcome

Thanks for choosing the **Dinstar’ s Product**! We hope you will make full use of this rich-feature FXO Gateway. Contact us if you need any technical support: +86-755-61919966.

About This Manual

This manual provides information about the introduction of the analog gateway, and about how to install, configure or use it. Please read this document carefully before install the gateway.

Note: All types of DAG series products in this user manual will be called as device or gateway!

Intended Audience

This manual is aimed primarily at the following people:

- Users
- Engineers who install, configure, and maintain the gateway.

Revision Record

Document Name	DAG Series FXO Analog Gateway User Manual
Document Version	2.0
Revised by	Ellie Zhang
Date	2023/07/05
Descriptions	(1) Add new parameters based on the new products. (2) Update the format of the document.

Contents

1 Product Introduction

1.1 Overview

Thanks for purchasing Dinstar DAG (Hereinafter referred to as the DAG) series FXO analog gateway. DAG series FXO analog gateways are multi-purpose IP-based voice gateways. DAG series FXO analog gateways support kinds of work places, for small business, work at home, remote office and branch businesses and provides a low cost, simple operation VoIP solution. FXO hybrid gateway can support network failure and power failure lifeline feature, flexibly achieve interoperability with simulation PBX and offer reliable voice quality assurance for the traditional voice transition to IP voice. It also supports standard SIP protocol and can be compatible mainstream IPPBX and softswitch platform. DAG series FXO analog gateway includes following model:

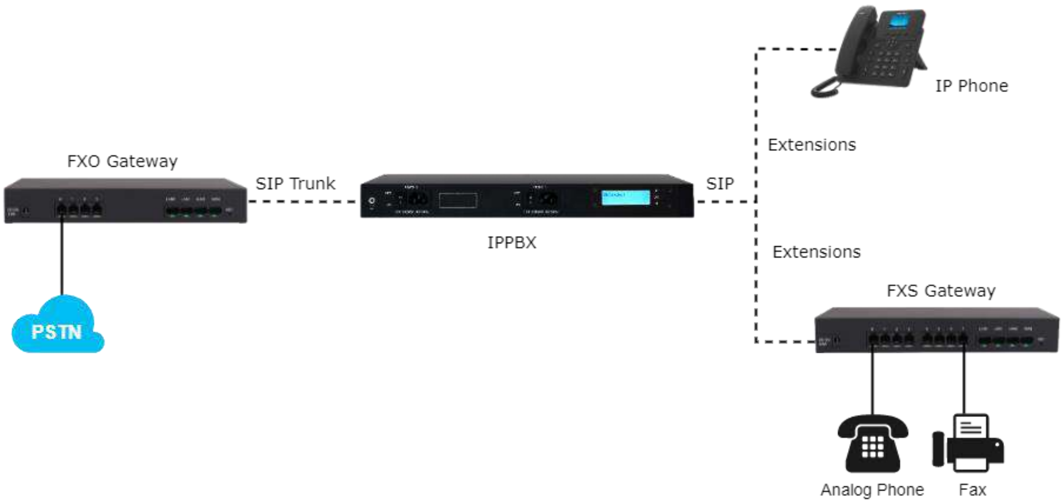
- DAG1000-2O，DAG1000-4O，DAG1000-8O
- DAG2000-16O

This manual mainly to DAG1000-2O as examples, introduce the function of devices and parameter configuration.

1.2 Application Scenario

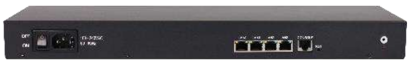
The application scenario of device is shown as follow:

Figure-Application Scenario of the device



1.3 Outlooks of Products

1.3.1 Outlooks of Device

Models	Front View	Rear View
DAG1000-2O		
DAG1000-4O		
DAG1000-8O		
DAG2000-16O		

1.3.2 Ports and Indicators

Number of Ports:

Port Type / Models	WAN	LAN	FXO
DAG1000-2O	1	1	2
DAG1000-4O	1	3	4
DAG1000-8O	1	3	8
DAG2000-16O	0	4	16

The description of indicators:

Indicator	Definition	Status	Description
PWR	Power Indicator	On	The gateway is powered on
		Off	The gateway is powered off or there is no power supply
RUN	Running Indicator	Slow Flashing	The gateway is running properly (Slow Flashing means the running indicator flashing for 2 seconds)
		Fast Flashing	SIP account is registered successfully (Fast Flashing means the running indicator flashing for 0.5 seconds)
		Off	The gateway is running improperly
FXO	FXO In-use Indicator	On	FXO port is currently occupied.
		Off	FXO Port is idle or faulty.

WAN/LAN	Network Link Indicator	Green Flashing	The gateway is properly connected to network.
		Off	The gateway is not connected to network or network connection is improper way.
	Network Speed Indicator	On	Work at 100Mbps.
		Off	Work at 10Mbps

1.4 Features & Functions

1.4.1 Protocol standard supported

- Protocol: SIP v2.0 (UDP/TCP), RFC3261 SDP, RTP(RFC2833), RFC3262, RFC3263, RFC3264, RFC3265, RFC3515, RFC2976, RFC3311
- SIP Trunk
- SIP TLS/SRTP
- RFC3266 IPv6 in SDP
- RFC2806 TEL URI
- RFC3581 NAT, rport
- Outbound Proxy
- RFC4028 Session Timer
- RTP/RTCP, RFC2198, RFC1889
- DNS SRV/ A Query/NATPR Query
- Early Media/Early Answer
- NAT: STUN, Static/Dynamic NAT

1.4.2 Voice Capabilities & Fax

- Modem/POS
- VLAN 802.1P/802.1Q
- Layer3 QoS and DiffServ
- T.38/Pass-through
- Silence Suppression
- Comfort Noise Generation (CNG)
- Voice Activity Detection (VAD)
- Echo Cancellation (G.168), with up to 128ms
- Adaptive (Dynamic) Jitter Buffer
- Programmable Gain Control
- Audio Codec: G.711A/U law, G.723.1, G.729A/B, G.726
- DTMF mode: Signal/RFC2833/INBAND

1.4.3 FXO

- Connector: RJ11
- FAS
- Caller ID: FSK, DTMF
- Polarity Reversal
- Answer Delay
- Busy Tone Detection
- No Current Detection
- Call Detection: Bellcore Type 1&2, ETSI, DTMF
- Dial Mode: DTMF/Pulse Dialing
- AC/DC Impedance Configuration

1.4.4 Maintenance

- CDR
- Syslog
- Web/Telnet

- SNMP v1/v2/v3
- TR069, TR181
- Auto Provisioning
- Network Capture
- Configuration Backup/Restore
- Firmware Upgrade via Web
- NTP/Daylight Saving Time
- IVR local Maintenance
- Cloud-based Management

2 Quick Installation

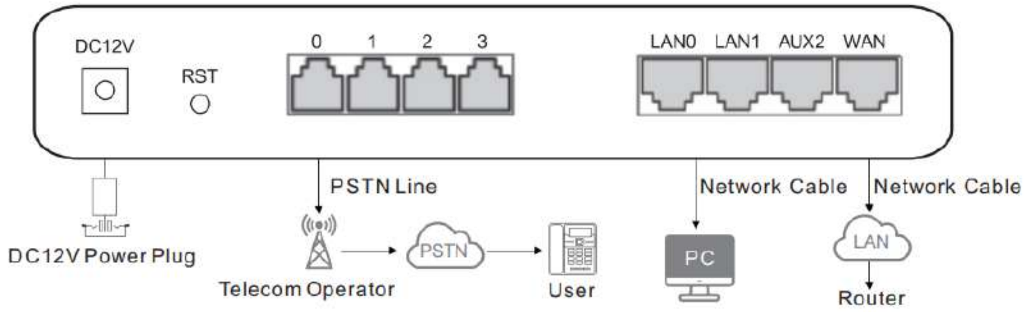
2.1 Installation Attentions

To avoid unexpected accident or device damage, please read the following instructions before installing the device:

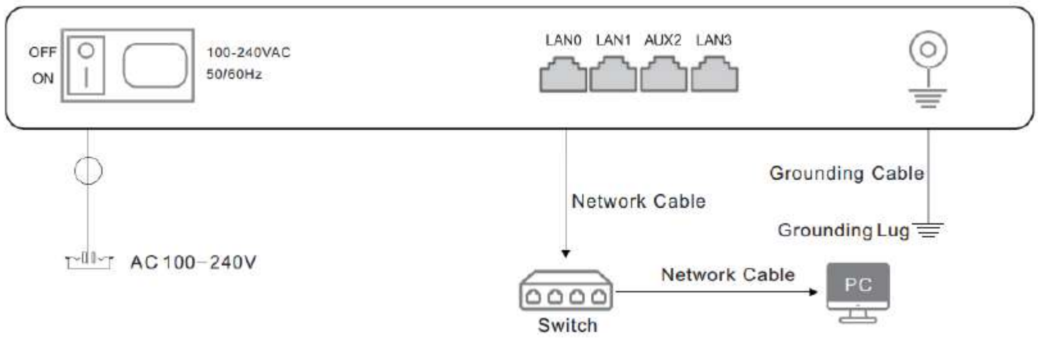
- Anti-jamming: to reduce the interference with telephone calls, it' s highly recommended that telephone lines connected to the gateway should be placed away from power cables;
- Power supply: DAG1000-2O, DAG1000-4O and DAG1000-8O are equipped with 12VDC power adapter, while DAG2000-16O accepts AC input voltage of 100-240V 50/60Hz. Please ensure safe and stable power supply;
- Network bandwidth: please ensure there is enough network bandwidth so as to guarantee stabilized running of the gateway;
- Ventilation: to avoid overheating, please do not pile up the gateway with other devices and make sure the gateway has good ventilation around;
- Temperature and humidity: to avoid any accident that might cause malfunction, it' s advised to install the gateway in an equipment room where temperature and humidity are appropriate;
- Mechanical load: please make sure the gateway is placed steadily to avoid damage. It is highly advised to horizontally place the gateway on a flat surface or a cabinet.

2.2 Installation Instructions

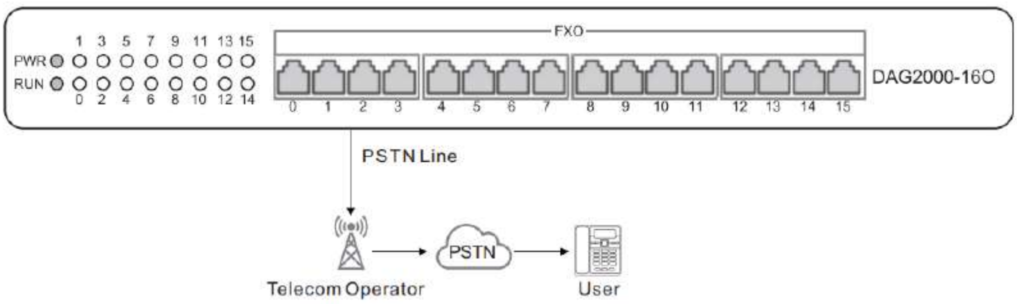
- DAG1000-2O/DAG1000-4O/DAG1000-8O
  - Connect gateway with network, and connect gateway with power input
  - Connect FXO port with PSTN line



- DAG2000-16O
  - Connect gateway with network, and connect gateway with power input



  - Connect FXO port with PSTN line



3 Basic Operation

3.1 Call out and Call in via FXO Port

3.1.1 Call Out

- One-stage Dialing: After the gateway receives a call number sent from softswitch or IPPBX, if the number matches one of the dialing rules set on Advanced Digit Map interface, the call will directly choose a FXO port to call out based on port selection rule.
- Two-stage Dialing: dial a FXO port's SIP account number from an extension of IPPBX, and then you will hear a dialing tone. After that, you will be able to dial any number of PSTN.

3.1.2 Call In

Dial the number of PSTN connected to a FXO port of the gateway, and then you will hear a dialing tone or a voice prompt of "please dial the extension number". Then dial the called number (extension number or telephone number), after the dialing is completed, the called number will be sent to IP server such softswitch or IPPBX.

Hotline auto-dialing: Dial the number of PSTN connected to a FXO port of the gateway, then the gateway will automatically route the call to designated extension number or telephone number according to preset hotline number.

3.2 Description of Feature Code

The device provides convenient telephone functions. Connect a telephone to the port and dial a specific feature code, and you can query corresponding information.

Code	Corresponding Function
*158#	Dial *158# to query LAN IP
*159#	Dial *159# to query WAN IP
*114#	Dial *114# to query the phone number of a FXO port
*115#	Dial *115# to query the phone number of a FXO port group
*168#	Dial *168# to query the register status of a FXO port
*154#	Dial *154# to remove login limit
150	Dial *150*1 to set IP address as static IP address; dial *150*2 to set IP address as DHCP IP address
157	Dial *157*0# to set Network Work Mode as Router mode Dial *157*1# to set Network Work Mode as Bridge mode
152	Dial *152* to set IPv4 address, for example: Dial *152*192*168*1*10# to set IPv4 address as 192.168.1.10
153	Dial *153* to set IPv4 netmask, for example: Dial *153*255*255*0*0*# to set IPv4 netmask as 255.255.0.0
156	Dial *156* to set IPv4 gateway, for example: Dial *156*192*168*1*1# to set IPv4 gateway as 192.168.1.1
*170#	Dial *170# to increase the sound volume of a FXO port
*171#	Dial *171# to decrease the sound volume of a FXO port
149	Dial *149*1 to enable FXO Configuration Dial *149*0 to disable FXO Configuration
160	Dial *160*1# to enable access of web through WAN port Dial *160*0# to disable access of web through WAN port Dial *160*3# to enable access of web through LAN port Dial *160*2# to disable access of web through LAN port Dial *160*5# to enable access of telnet through WAN port Dial *160*4# to disable access of telnet through WAN port Dial *160*7# to enable access of telnet through LAN port

	Dial *160*6# to disable access of telnet through LAN port
165	Dial *165*000000# to restore username/password and network configuration to factory defaults
166	Dial *166*000000# to reset factory configuration
***111#**	Dial *111# to restart the device

Note:

A voice prompt indicating successful configuration will be played after each configuration procedure. Please do not hang up the phone until hearing the prompt.

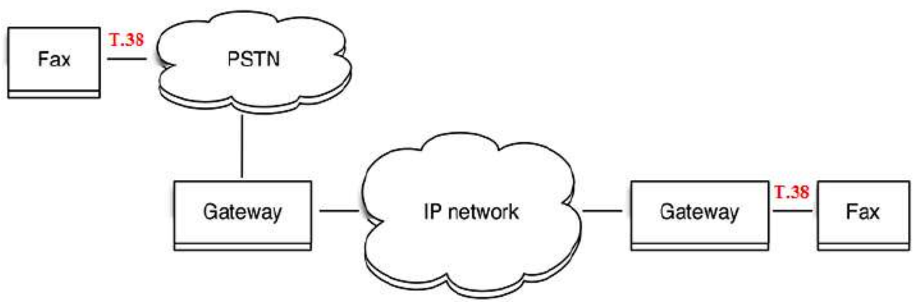
3.3 Send or Receive Fax

3.3.1 Fax Mode Supported

- T.38 (IP-based)
- Pass-Through（VBD)
- Adaptive Fax Mode (automatically match with the peer fax mode)

3.3.2 Explanation of T.38 and Pass-through

T.38: T.38 is an ITU recommendation for allowing transmission of fax over IP networks in real time. Under the T.38 mode, analog fax signal is converted into digital signal and fax signal tone is restored according to the signal of peer device. Under the T.38 mode, fax traffic is carried in T.38 packages.



Pass-through: Under the pass-through mode, fax signal is not converted and fax traffic is carried in RTP packets. It uses the G.711 A or G711U codec in order to reduce the damage to fax signal.

Adaptive Fax Mode: Automatically match with the fax mode of the peer device.

4 Local IVR Operation

4.1.1 Inquiring the IP address

Connect a PSTN line to one of the FXO ports of the gateway, and then use a mobile phone or a fixed telephone to dial the number of the PSTN line. After you hear a dialing tone or a voice prompt, dial *158# to inquire the IP address of the gateway.

4.1.2 Factory Reset

Connect a PSTN line to one of the FXO ports of the gateway, and then use a mobile phone or a fixed telephone to dial the number of the PSTN line. After hearing a dialing tone or a voice prompt, dial *166*000000#, and you will hear “successful setting”, then hang up the phone and the gateway is reset to factory defaults.

4.1.3 IP Address configuration

Before configuration, please ensure:

► The gateway is power on;

► Device has been connected to network;

► The PSTN line has been connected to the FXO port of the gateway.

Configure dynamic IP address by DHCP:

1) Pick up the phone
2) dial *150*2# and then hang up the phone
3) If the voice prompt indicates ‘setting successfully’, please restart the gateway after 10 seconds.

Configure Static IP address:

Take the configuration of IP address ‘172.16.0.100’ as example.

1) Pick up the phone,
2) dial *150*1# and then hang up the phone

Then configure IP address and subnet mask as follow:

► Configure IP address

1) Pick up the phone
2) dial *152*172*16*0*100# and then hang up the phone.

► Configure subnet mask

1) Pick up the phone
2) dial *153*255*255*0*0# and then hang up the phone.

► Configure gateway IP address

1) Pick up the phone
2) dial *156*172*16*0*1# and then hang up the phone.

► Query the IP address of the gateway:

1) Pick up the phone,
2) dial *158#.

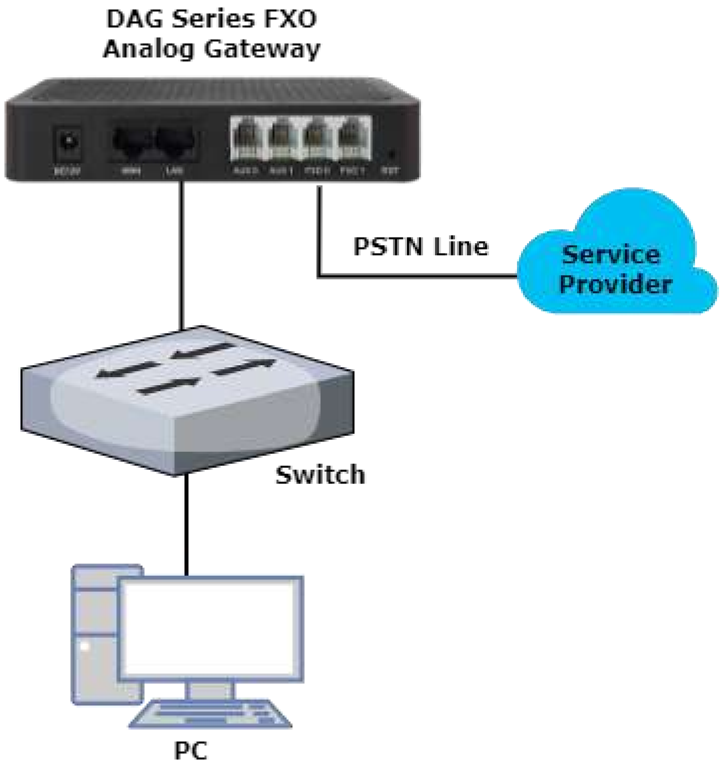
If the gateway uses PPPoE method to get IP address，the IP address needs to be configures through web browser.

Note: The telephone will play voice prompt “setting successfully” if the step is correct.

5 Configurations on Web Interface

5.1 Access WEB Interface

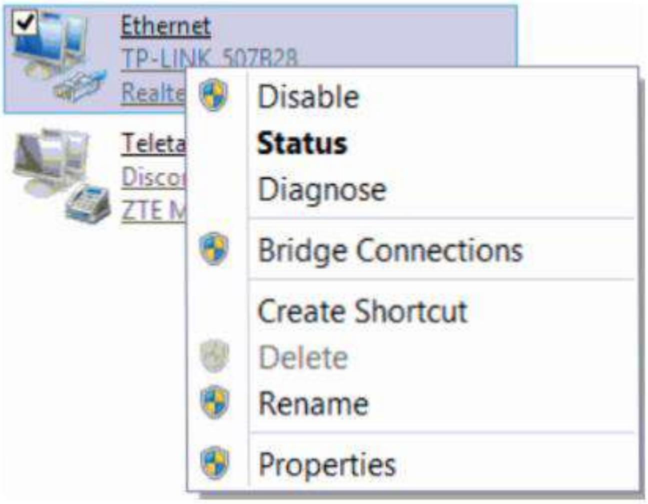
First, users connect the device to the network and refer to the network topology diagram for connection. Then refer to the chapter ***4 Local IVR Operation*** and dial *158# to query the IP address of the device.



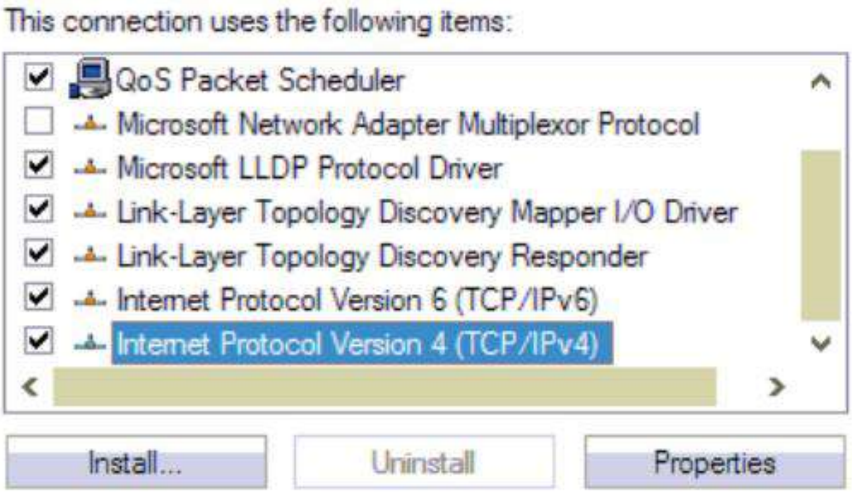
5.1.1 Preparation for Login

To log in the Web Management System of the gateway, firstly, you need to modify the IP address of PC which is used to access the gateway and to make it at the same network segment with the gateway.

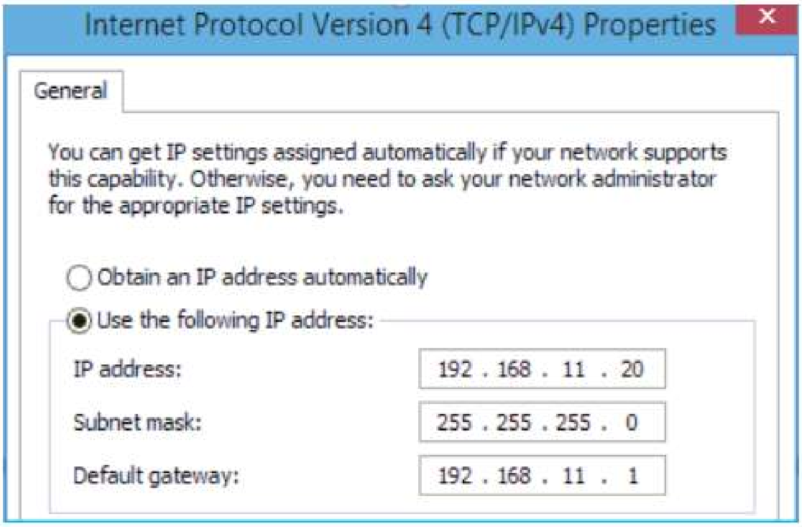
1. On the PC, click '**Network (or Ethernet) →Properties**'.



2. Double-click '**Internet Protocol Version 4 (TCP/IPv4)**'.



3. Select '**Use the following IP address**', and then enter an available IP address '192.168.11.XXX' which is at the same network segment with '192.168.11.1'.



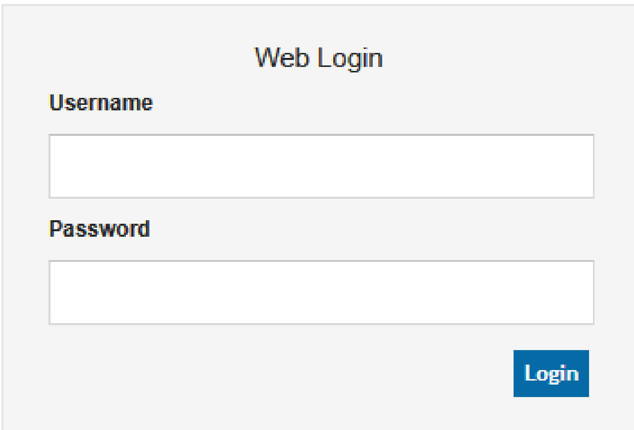
Then, check the connectivity between the PC and the device. Click **Start → Run** of PC and enter **cmd** to execute 'ping 192.168.11.1' to make sure the IP address is pingable.

5.1.2 **Log in WEB**

Open a web browser and enter the IP address (the default IP is 192.168.11.1). Then the login GUI will be displayed.

It is suggested that you should modify the username and password for security consideration.

Figure-Login GUI



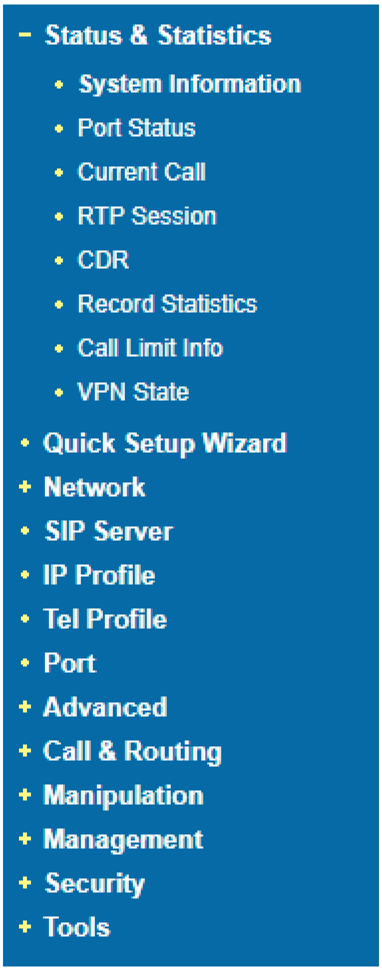
Both the default username and password are admin. Click Login to enter the web interface.

5.2 Navigation Tree

The web management system of the device consists of the navigation tree and configuration interfaces with more details.

Choose a node of the navigation tree to enter a configuration interface.

Figure-Navigation Tree of Web Interface



5.3 Status & Statistics

The 'Status & Statistics' menu mainly displays all kinds of information. It includes the following sub-menus: System Information, Port Status, Current Call, RTP Session, CDR, Record Statistics and Call Limit Info.

5.3.1 System Information

Log in the Web interface, and then click **Status & Statistics → System Information**, and the following page will be displayed. On the page, you can view the information of device ID, MAC address, IP addresses, version information, server register status and so on.

Figure-System Information

Table-Explanation of Items on System Information Interface:

Parameter	Explanation
Device ID	A unique ID of each device. This ID is used for warranty and cloud server authentication.
MAC address	Hardware address of the LAN port

Network Mode	Display network mode, include bridge and router. If it is bridge, WAN port display Network, and the WAN port as same as the LAN port.
WAN IP Address	Shows WAN IP address of DAG, DHCP mode: all the field values for the Static IP mode are not used (even though they are still saved in the Flash memory.) The DAG acquires its IP address from the first DHCP server it discovers from the LAN it is connected. Using the PPPoE feature: set the PPPoE account settings. The DAG will establish a PPPoE session if any of the PPPoE fields is set. Static IP mode: configure the IP address, Subnet Mask, Default Router IP address, DNS Server 1 (primary), DNS Server 2 (secondary) fields. These fields are set to zero by default.
LAN Port	Shows LAN IP address of DAG. if network Mode is bridge, LAN port won’t display.
DNS Server	IP addresses of primary DNS server and standby DNS server are displayed.
Cloud Register Status	Whether the device is registered to cloud or not.
System Uptime	The running time of the device since it is powered on.
System Time	The NTP synchronization time of the device
Traffic Statistics	Total bytes of message received and sent by device.
Usage of Flash	Detailed usage of Flash memory
Usage of Backup Flash	Detailed usage of Backup Flash memory
Usage of RAM in Linux	detailed RAM usage of Linux core

Usage of RAM in AOS	Detailed RAM usage of AOS
Current Software Version	The software version that runs on the device. Model name, version number and the software development date are displayed.
Backup Software Version	Backup software is for the purpose of backup. When the current software fails, the backup software version will work.
DSP Version	DSP version
U-BOOT Version	U-boot version
Kennel version	Linux Kennel version
FS Version	File system version
Hint Language	The current language of the DAG device

5.3.2 Port Status

On the **Status & Statistics →Port Status** page, users can view the port status of each port or port group.

The following figure shows the registration information of ports and port groups. Users can view the registration status of each port and port group of the device through this page.

Figure-Registration Status of Each Port or Port Group

Port

Port No.	Type	SIP User ID	User Status	Port Status	Call Status
0	FXO	---	---	Offline	Idle
1	FXO	---	---	Offline	Idle

Port Group

Group	Port	SIP User ID	User Status
---	---	---	---

Refresh

SIP User status:

- Registered: the port or port group is registered to SIP server successfully;
- Unregistered: the port or port group fails to be registered to SIP server.

5.3.3 Current Call

On the **Status & Statistics → Current Call** page, users can view the call statistics of each port of the device, including: port, type, source, destination, connected time, and duration.

Figure-Current Call

Current Call

Port	Type	Source	Destination	Connected Time	Duration(s)
---	---	---	---	---	---

Refresh

5.3.4 RTP Session

On the **Status & Statistics → RTP Session** page, users can view the real-time RTP session information, including: port, source, destination, payload type, packet period, local port, peer IP, peer port, sent packets, received packets, lost packets rate, jitter, and duration.

Figure-Real-time RTP Session Information

RTP Session

Port	Source	Destination	Payload Type	Packet Period	Local Port	Peer IP	Peer Port	Sent Packets	Recv Packets	Lost Packets Rate(%)	Jitter	Duration(s)
---	---	---	---	---	---	---	---	---	---	---	---	---

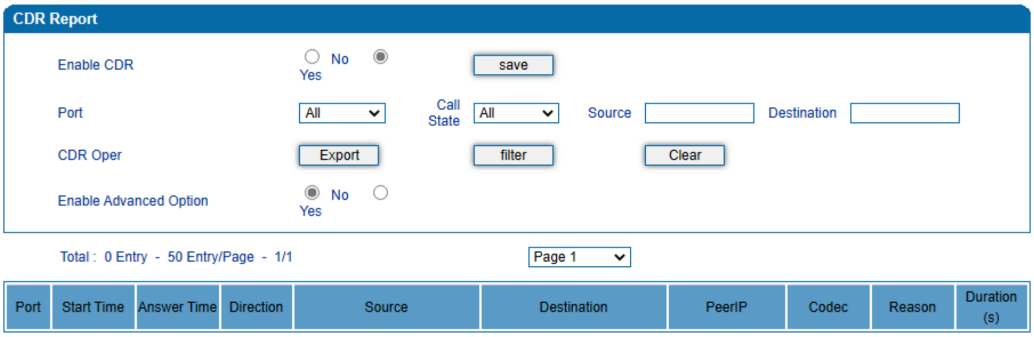
Refresh

5.3.5 CDR

CDR (**Call Detail Record):** is a data record produced by a telephone exchange or a telecommunication device, which contains the details of a telephone call that passes through the device.

On the **Status & Statistic → CDR** page, users can enable the CDR function and view the details of all calls through the ports of the device. Users can also export, filter, or clear the CDRs.

Figure-CDRs of Ports



Parameter	Explanation
Enable CDR	whether CDR is enabled; check Yes, the CDRs will be displayed after the call; or the CDRs will not be displayed after the call ends
Port	Select one port or all ports to filter CDRs
Call State	Filter CDRs according to the call state, users can select All, Not Answer, Complete and Fail
Source	Filter CDRs according to the caller
Destination	Filter CDRs according to the callee
Export	Export the CDRs to local computer (file name is cdr.txt)
Filter	Filter the CDRs according to port, call state, caller and callee
Clear	Clear all the CDRs
Enable Advanced Option	When the advanced option is enabled, it will display the peer port, local IP, local port, end code, RTP send, RTP received, RTP loss rate, jitter

5.3.6 Record Statistics

On the **Status & Statistic → Record Statistics** page, record statistics including server status, count of current records, count of no response, count of server return errors, count of record starts, count of record startAck, count of record stops and count of stopAck are displayed.

Figure-Record Statistics

Record Statistics

Server Stat	Current Records	No Responses	Server Return Error	Start	StartAck	Stop	StopAck
Not Config	0	0	0	0	0	0	0

No Response Statistics

Link Dect NoRsp Cnt	0
Start Time Out Cnt	0
Rel Call Before StartAck	0
Stop Time Out Cnt	0

Refresh Reset

5.3.7 Call Limit Info

If you configure call limit on the "**Call & Routing -> Call Limit**" for the port, users can check the remaining call duration and number of calls of the configured port.

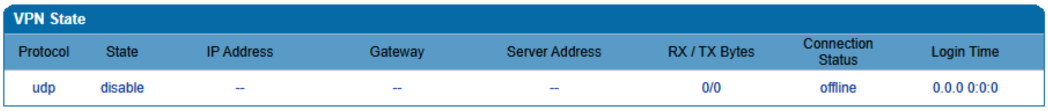
Call Limit Info

Port No	Daily Duration Remain	Month Duration Remain	Daily Calls Remain	Minute Calls Remain	Daily Connected Remain	Minute Connected Remain
0	---	---	---	---	---	---
1	---	---	---	---	---	---

Refresh

5.3.8 VPN State

On the **Status & Statistic → VPN State** page, VPN information including Protocol, State, IP Address, Gateway, Server Address, RX / TX Bytes, Connection Status, Login Time are displayed.



VPN State

Protocol	State	IP Address	Gateway	Server Address	RX / TX Bytes	Connection Status	Login Time
udp	disable	--	--	--	0/0	offline	0.0.0 0:0:0

5.4 Quick Setup Wizard

Quick setup wizard guides user to configure the device step by step. User only needs to configure network, SIP server and SIP port in the Quick Setup Wizard interface. Basically, after these three steps, users can make voice call via the device.

For the configurations of network, SIP server and SIP port, please refer to 5.5 , 5.6 and 5.9 .

5.5 Network

5.5.1 Local Network

DAG FXO gateway has two kinds of work mode: router and bridge. When DAG is in router mode, the DAG will work as small router and NAT function has enabled. In this situation, WAN port is normally connecting to uplink router/switch or ADSL MODEM, LAN port used to connect local computer or other network device (such as Ethernet switches, Hubs etc.). When DAG is in bridge mode, WAN and LAN port are the same. The DAG just work as two ports or four ports Ethernet switch.

When it set to bridge mode, only need to configure WAN port IP address and DNS. If set to router mode, default LAN port IP will display and it can be change by users.

On **Network → Local Network** page, users can configure the IP protocol, WAN Dual Mode, network configuration, manage address, and DNS server address of the device.

The device supports both IPv4 and IPv6 IP protocols and two network configuration methods (DHCP or static IP address).

Figure-Local Network Setting-Router Mode

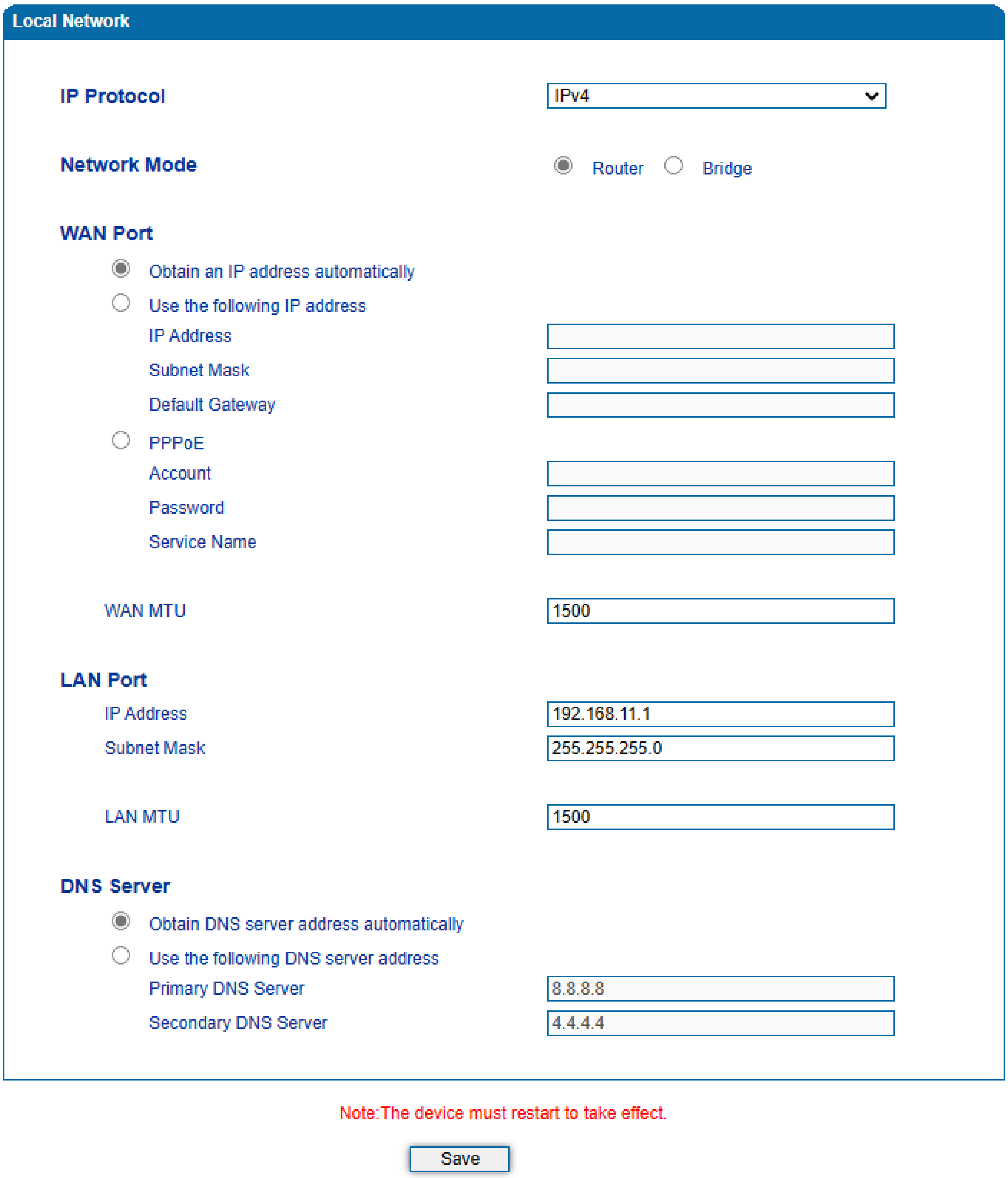
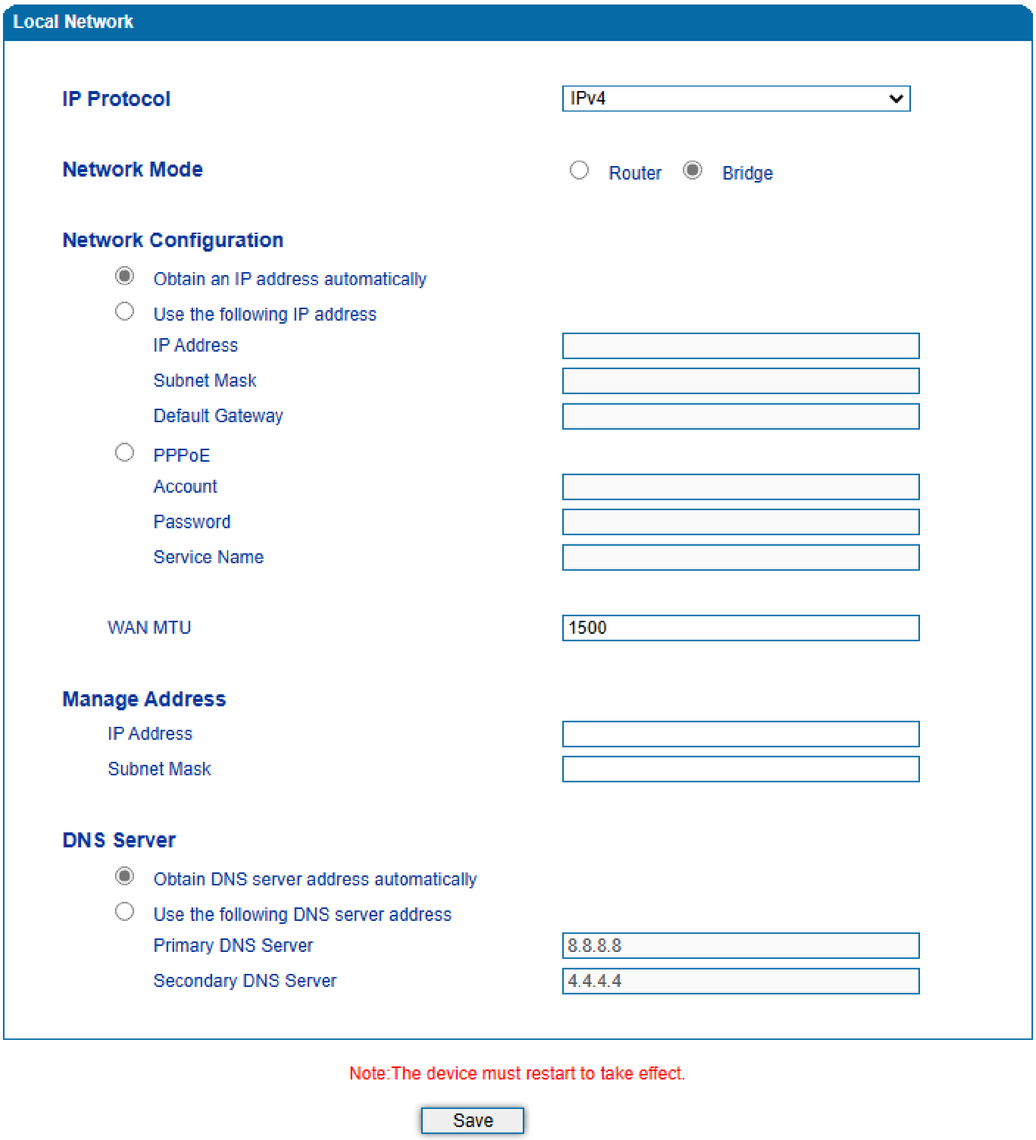


Figure-Local Network Setting-Bridge Mode



Parameter	Explanation
IP Protocol	There are 2 IP protocols the device supported, IPv4 or IPv6
Network Mode	Set the network mode of the device, Router or Bridge
Obtain an IP address automatically	The device obtains IP address through DHCP server
Use the following IP address	Set a static IP address for the device

Account	Account for connecting to PPPoE server
Password	Password for connecting to PPPoE server
Service Name	It needs to be set in the PPPoE server, and the connection will be successful if it is consistent, otherwise it will fail.
WAN MTU	Set the MTU value of WAN port, and the valid range is from 512-1500.
LAN MTU	Set the MTU value of LAN port, valid range is 512-1500 and cannot be higher than WAN MTU.
Manage Address	Set the IP address of the Manage Address. The device can be accessed through the manage address.
Obtain DNS server address automatically	The device obtains DNS server address through DNS server
Use the following DNS server address	Set a static DNS server address for the device
Primary DNS Server	Primary DNS Server
Secondary DNS Server	Set secondary DNS server for the device

Note: The device must restart to take effect.

5.5.2 VLAN (Virtual Local Area Network)

In order to control the impacts brought by broadcast storms, you can divide the local-area network into three VLAN groups, including data VLAN, voice VLAN and management VLAN on the **Network → VLAN** page.

Management VLAN transmits management-related packets, such as packets of SNMP, TR069, Web and Telnet, while voice VLAN transmits the signals and voices produced by the device itself. Data VLAN transmits data packets.

Figure-Configure VLAN

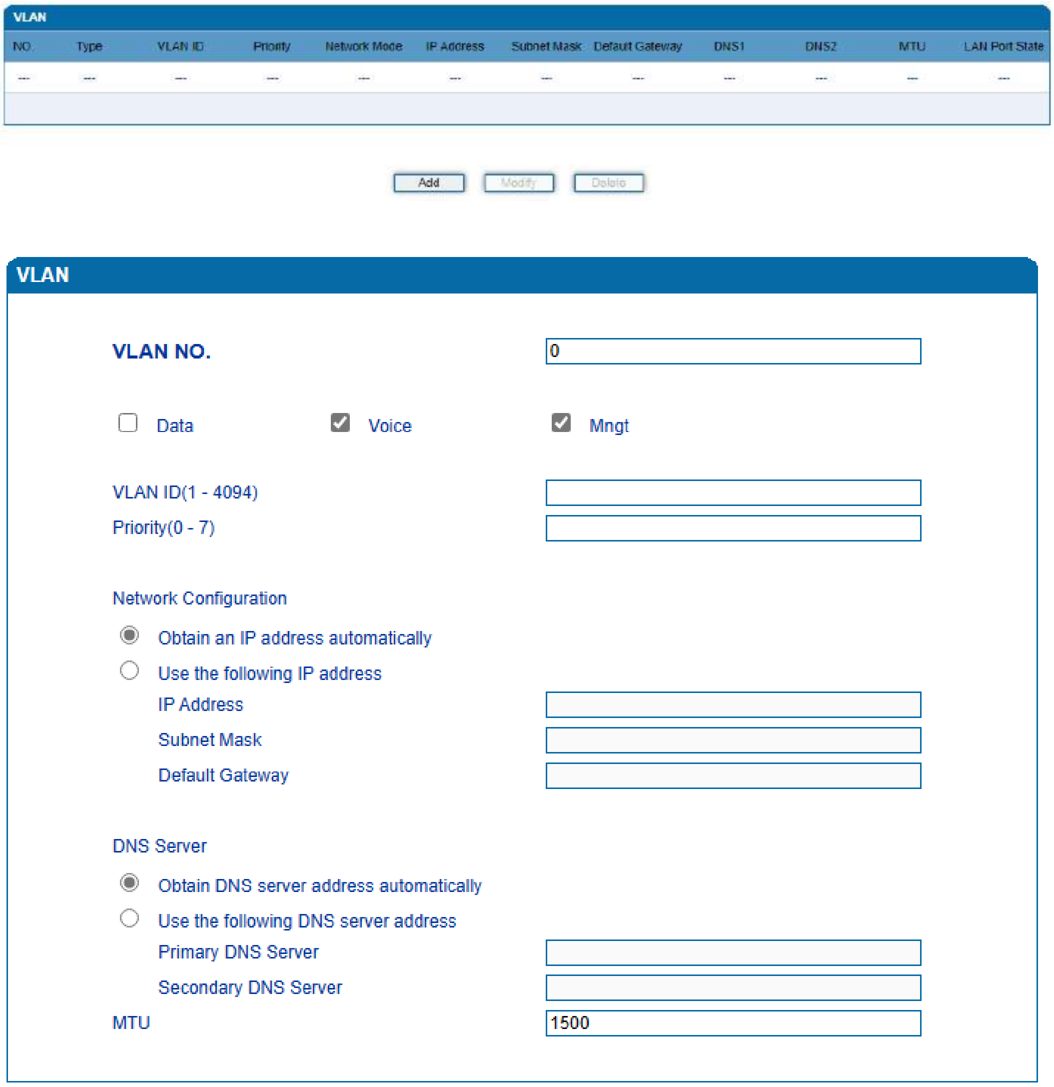


Table-Explanation of VLAN Parameters

Parameter	Explanation
VLAN1/VLAN2/VLAN3	The device supports three VLANs at most. Please enable VLAN according to actual needs.
Data/Voice/Management	Select what kind of messages are allowed to go through this VLAN. For example, if the checkbox on the left of data is selected, it means data messages are subject to the following network setting of this VLAN.

VLAN ID(1-4094)	Set an ID to identify a VLAN based on 802.1Q protocol. Range is from 1 to 4094.
Priority (0-7)	Set the priority of a VLAN based on 802.1P protocol. 0 is the highest priority.
Obtain an IP address automatically	The device obtains IP address through DHCP server
Use the following IP address	Set a static IP address for the device
IP Address	Set the IP address of the VLAN interface
Subnet Mask	Set the subnet mask of the VLAN interface
Default Gateway	Set the default gateway address of the VLAN interface
Obtain DNS server address automatically	The device obtains DNS server address through DNS server
Use the following DNS server address	Set a static DNS server address for the device
Primary DNS Server	Set a primary DNS server address for the device
Secondary DNS Server	Set a secondary DNS server address for the device
MTU	Set the MTU value of the VLAN interface

【Note】: After the configurations are finished, you need to restart the device for the configurations to take effect.

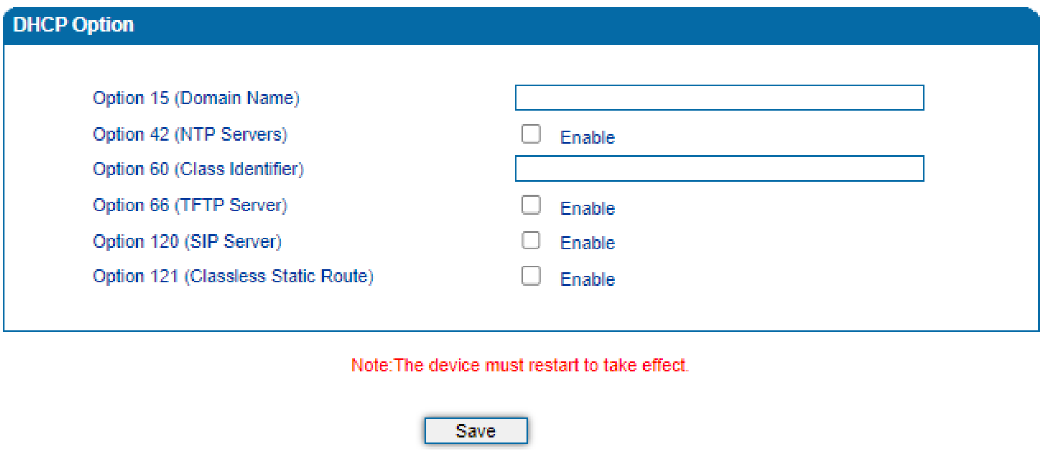
5.5.3 DHCP Option

When the device works as a DHCP client and applies for an IP address, DHCP server will return packets which include an IP address as well as configuration information of enabled option fields.

The following is the meaning of the option fields involved in the device (that means the following option fields are enabled, DHCP server will return information of corresponding option fields:

- Option 15: to set a DNS suffix;
- Option 42: to specify NTP server;
- Option 60: to define VCI (vendor class identifier) of device on the DHCP server;
- Option 66: to specify TFTP server which will assign software version to device;
- Option 120: to fetch SIP server address;
- Option 121: to obtain classless static route. The device will add these static routes to the static route table after it fetches them from DHCP server.

Figure-Configure DHCP Option

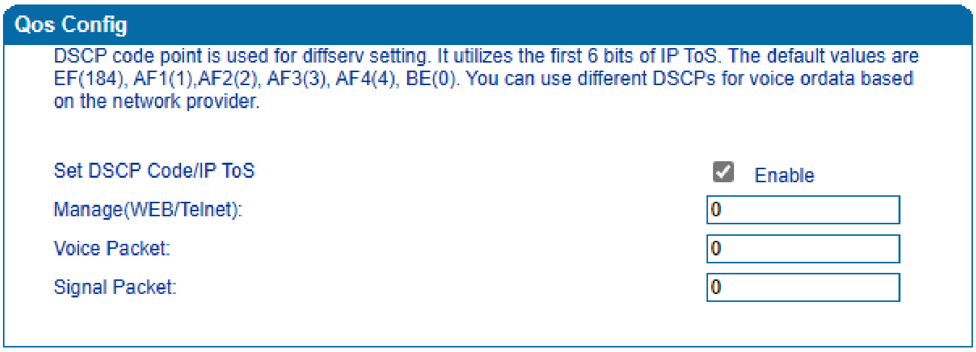


Network Interface: choose which VLAN to send request to DHCP server (or to receive information from DHCP server).

5.5.4 **QoS**

The device can label QoS priority on the IP messages it sends out, so as to resolve network delay or network congestion. Meanwhile, the device can give different QoS tags for management-related packets of Web/Telnet, voice packets and signal packets.

Figure-QoS



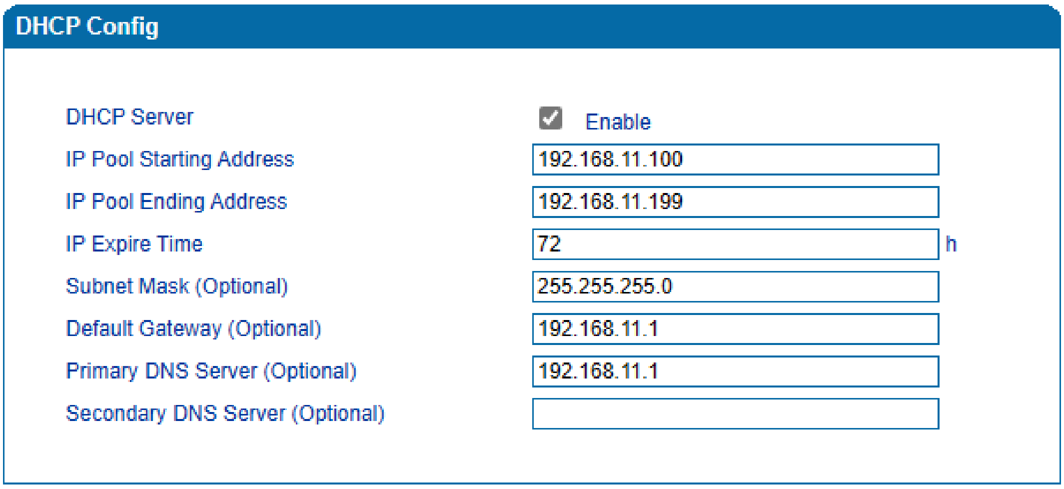
5.5.5 **DHCP Server (Router mode)**

Under router mode, DAG network part as a small router to configure DHCP service, that DAG as a DHCP server in network.

Starting and ending address of address pool determine the range of IP address automatically assigned to other devices;

IP Expire Time means use time of assigned IP address. More than the lease time, if the IP address is not used by network equipment, IP address will be recovered;

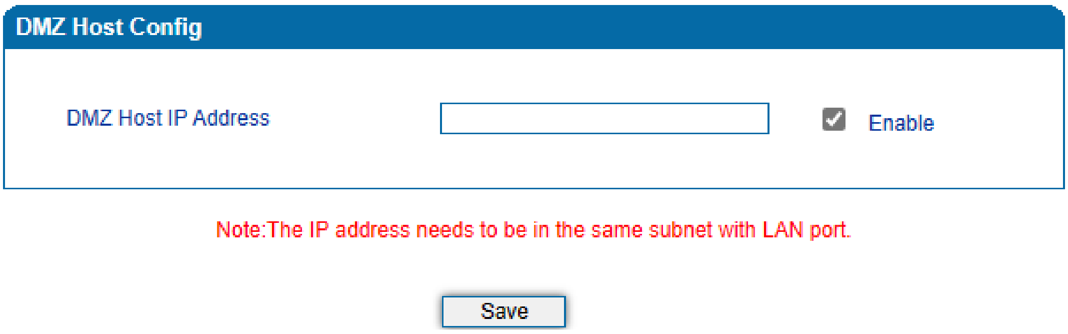
Subnet mask, gateway, DNS server and other information configured by DHCP protocol. Configuration interface as the following figure：



【Note】: When configure starting and ending IP address, subnet mask and gateway, please set the same segment with LAN port. Otherwise, device will not work normally. After configuration, restart device configuration validation.

5.5.6 DMZ Host (Router mode)

DMZ (Demilitarized Zone) connects web, e-mail etc. Server allowed external to access to this area. Make the internal network located the back of the zone of confidence and not allow any access, separation of inside and outside the network, protect user information. DMZ can be understood that a special area of the network and different from the external network or intranet. Public server that does not contain confidential information usually placed in DMZ, such as web, Mail, FTP etc. Accuser from intranet can visit the service of DMZ, but can't contact with confidential or private information stored in the network. Even if DMZ server is damaged, it will not be confidential information in the internal network.



【Note】: After configuration, restart device configuration validation.

5.5.7 Forward Rule (Router mode)

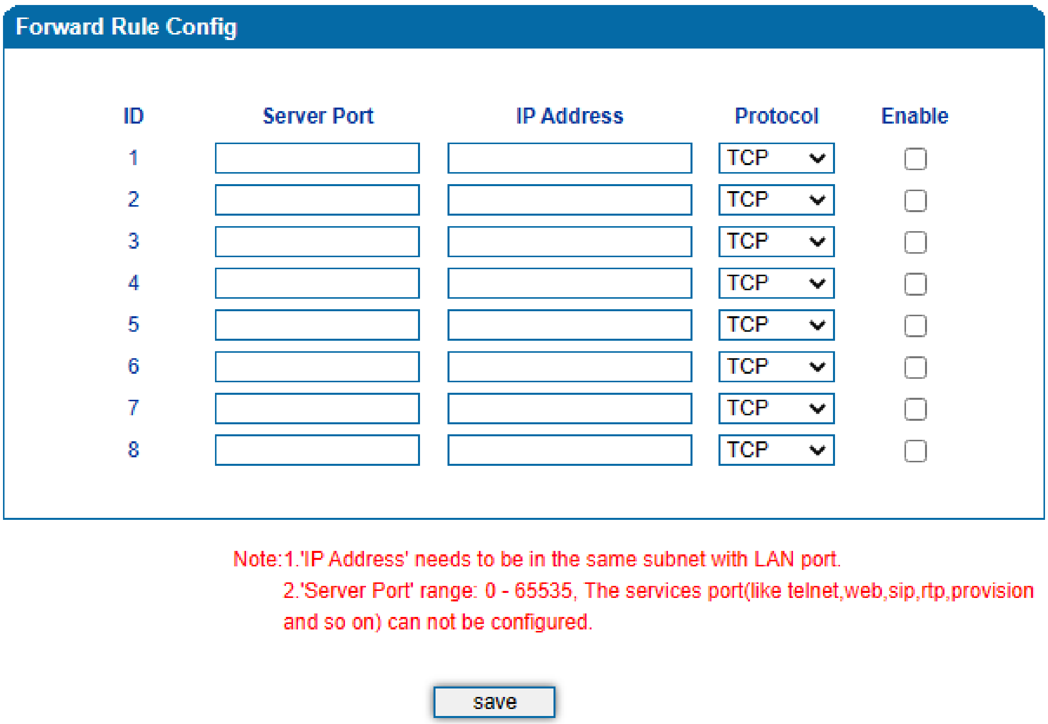
In some cases, LAN network equipment need to provide some communication in WAN network (such as port for 21 FTP service), This time can be configured forwarding rules for the network equipment.

Service ports namely the need to provide service network mouth WAN ports, IP address that LAN network provide services to the mouth of the network equipment IP address, the protocol is TCP or UDP.

The different between forward rule and DMZ host is that DMZ Host offers continuous multiple

Port (0-1024) and all the foreign communication agreement; while the forward rule offers a single or a few ports foreign communication on some protocol. When the conflicts exist between forward rule and DMZ host, the configuration of forwarding rules is preferred.

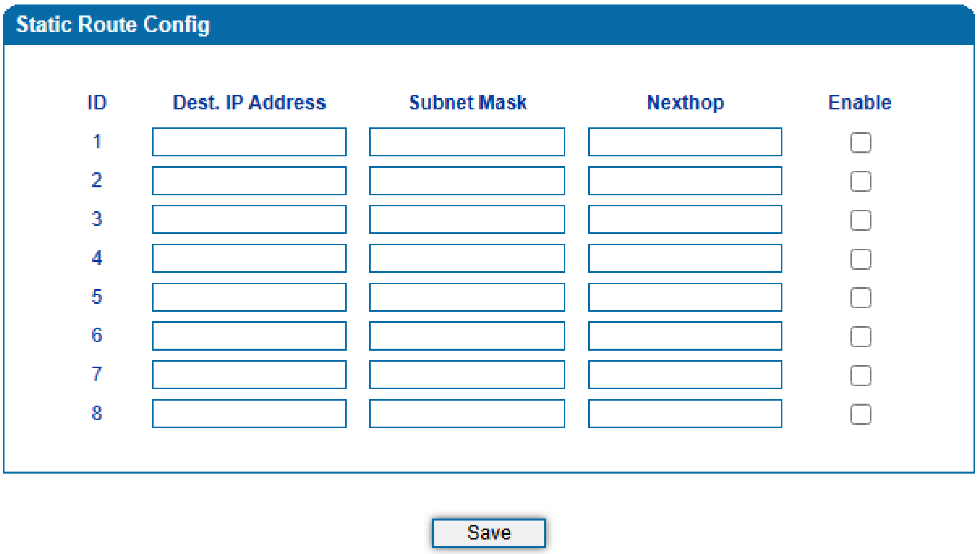
Forward rule configuration interface as follows:



5.5.8 **Static Route**

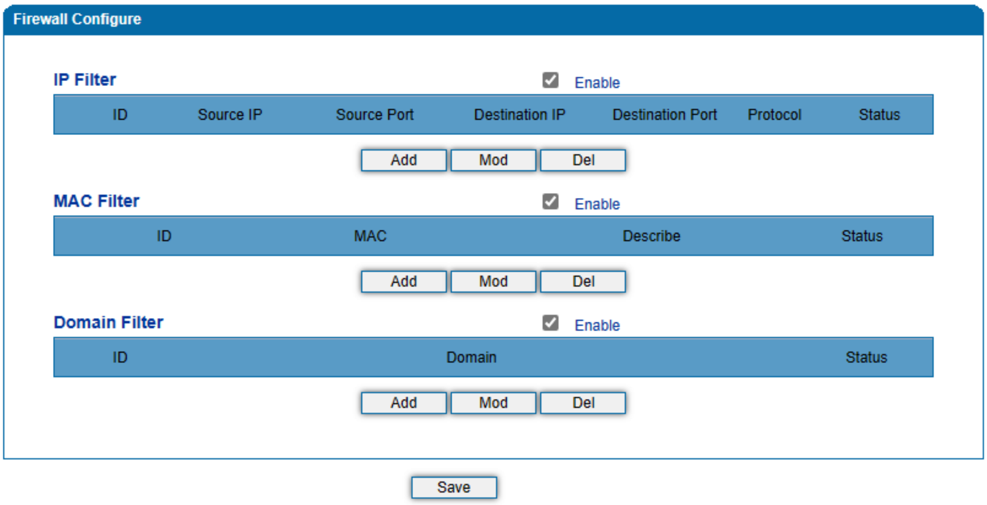
Static Route is IP communication direction in network, generally do not need to configure static route. When there are many segments in LAN network and need to complete some specific application among these segments, the static route needs to be configured.

Static Route configuration interface as follows:



5.5.9 **Firewall**

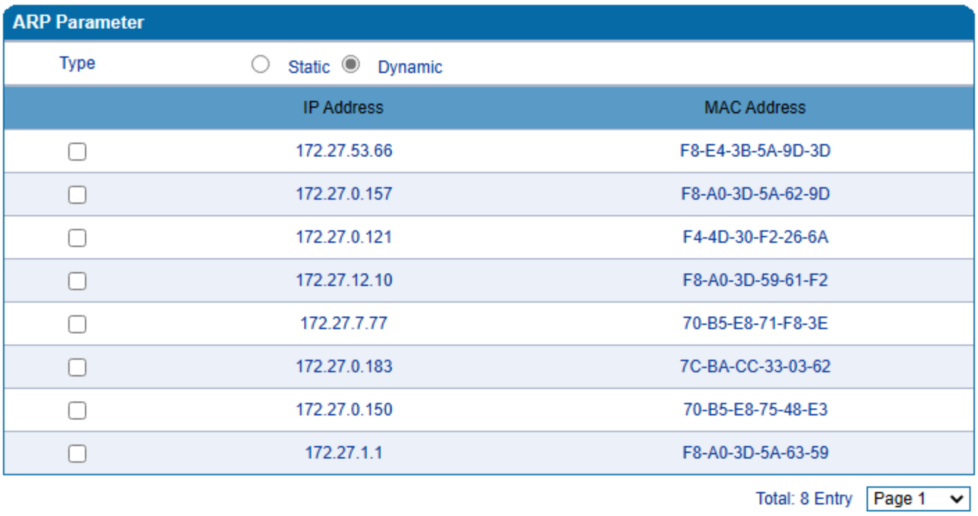
The firewall disables or enables the clients under the LAN Network to access the external network by setting filtering rules. The filtering rules include: IP filter, MAC filter and domain filter. The firewall configuration interface is shown in the following figure:



5.5.10 **ARP**

ARP is an address resolution protocol, which helps to get the MAC address of a device through its IP address. Under TCP/IP network environment, each host is assigned with a 32-bit IP address, but MAC address needs to be known for message transmission in the physical network. In the above case, ARP can help convert IP address into MAC address.

Figure-ARP



5.5.11 VPN

VPN: It generally refers to Virtual Private Network. VPN can create a private network over a public network for encrypted communication. The device currently supports only OpenVPN.

Table-Parameter Explanation of VPN

Parameter	**Explanation**
Mode	File import mode and advanced mode can be selected, and the default is File import mode
State	Enable or disable VPN
Authentication Username	Set Authentication Username
Authentication Password	Set Authentication Password
Certificate	Upload the certificate used to connect to the VPN

5.6 SIP Server

SIP server is the main component of SIP/IP network and is responsible for establishing all SIP calls. SIP server is also called SIP proxy server or register server. Both IPPBX and softswitch can act as the role of SIP server.

Figure-Configure SIP Server Information

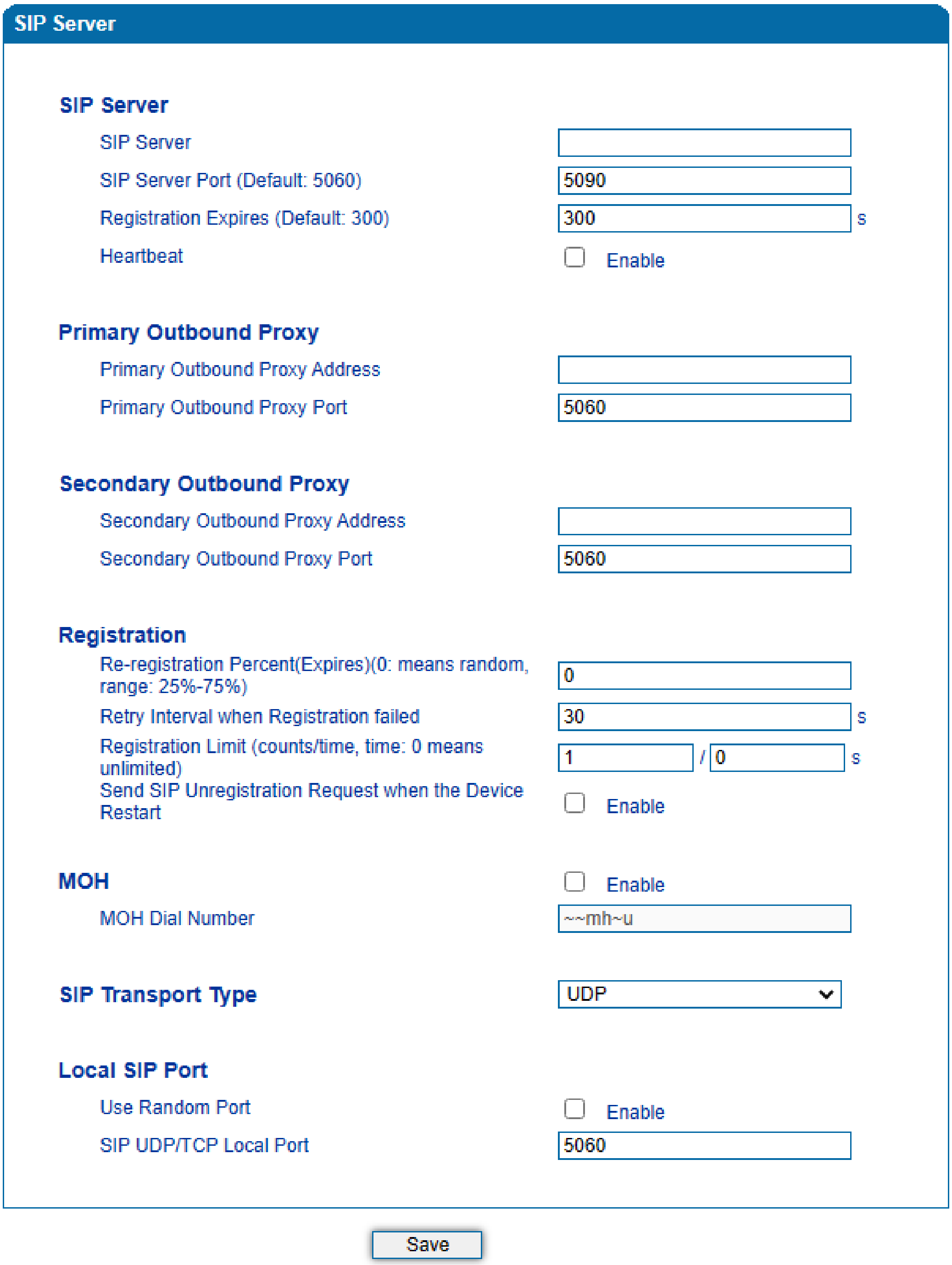


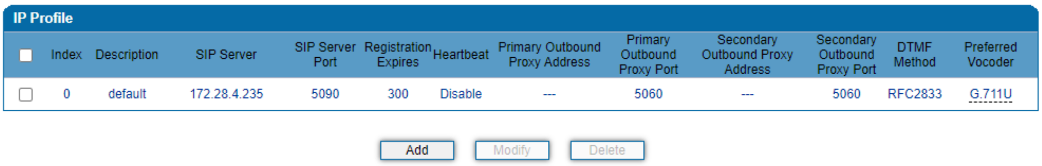
Table-Parameter Explanation of SIP Server

Parameter	Explanation
SIP Server	The IP address or domain name of the SIP server. It is provided by service provider or system admin.
SIP Server Port (Default: 5060)	The service port of the SIP server. It is 5060 by default.
Registration Expires (Default: 300)	It is used to avoid excessively frequent registrations. When the time that is set expires, the device will send register request to the SIP server. The time is 300s by default.
Heartbeat	Heartbeat is used to check the connection between the device and SIP server.
Primary Outbound Proxy Address	The IP address or domain name of primary outbound proxy server, which is provided by service provider.
Primary Outbound Proxy Port	The service port of the primary outbound proxy server.
Secondary Outbound Proxy Address	The IP address or domain name of secondary outbound proxy server, which is provided by service provider.
Secondary Outbound Proxy Port	The service port of the secondary outbound proxy server.
Re-registration Percent (Expires) (0: means random, range: 25%-75%)	Within the specified interval, the registration duration * re-registration percent, the terminal will resend the registration request to the server (default is 0, which means random)
Retry Interval when Registration failed	The retry interval after a registration fails. Default: 30s

Registration Limit (counts/time, time: 0 means unlimited)	The number of registrations per second (0 means unlimited)
Send SIP Unregistration Request when the Device Restart	All SIP accounts are logged out and then re-registered after the device is rebooted
MOH	The MOH (Music on Hold) feature provides music play to callers when their call is placed on hold. When enabled, users can configure the number to call on hold.
MOH Dial Number	Initiating a call to a set number after the call is placed on hold
SIP Transport Type	The way of SIP-based transmission. It can be UDP, TCP, TLS or Automatic. Default: UDP.
Use Random Port	If this parameter is selected, the local port of the device for using SIP services is chosen by random.
SIP UDP/TCP Local Port	The UDP/TCP port of device for using SIP services. Default SIP UDP/TCP local is 5060.

Usually, SIP server does not participate in media processing. Under SIP network, media always use end-to-end negotiating. Simple SIP server is only responsible for the establishment, maintenance and cleaning of sessions, while relatively-complex SIP server (SIP PBX) not only provides basic calling/RTP and commutation support, but also offers rich services such as Presence, Find-me and Music On Hold. Some customers may install gateways and work with various SIP/medial systems. SIP server based on Linux platform, such as: Kamailio/OpenSIPS, Asterisk/FreePBX, FreeSWITCH, VoS, Mera etc. SIP server based on windows platform, such as: 3CX, Brekeke, VoIPswitch etc. Carrier-grade soft switch platform, such as Cisco, Huawei, ZTE etc.

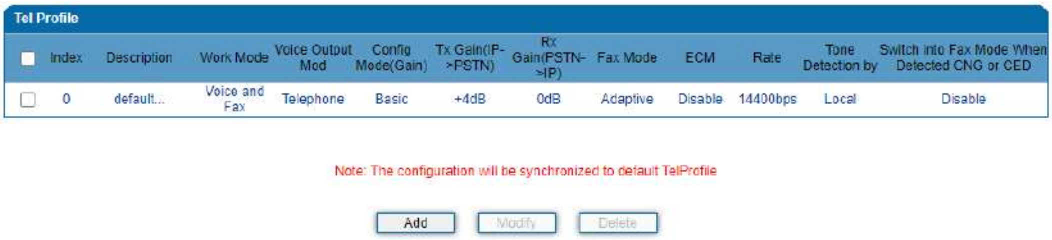
5.7 **IP Profile**


IP Profile

	Index	Description	SIP Server	SIP Server Port	Registration Expires	Heartbeat	Primary Outbound Proxy Address	Primary Outbound Proxy Port	Secondary Outbound Proxy Address	Secondary Outbound Proxy Port	DTMF Method	Preferred Vocoder
☐	0	default	172.28.4.235	5090	300	Disable	---	5060	---	5060	RFC2833	G.711U

IP profile is mainly consisting of a series of IP related parameters include SIP server, outbound proxy, DTMF, codecs etc. which are used to configure different parameters for each port.

5.8 **Tel Profile**


Tel Profile

	Index	Description	Work Mode	Voice Output Mod	Config Mode(Gain)	Tx Gain(IP->PSTN)	Rx Gain(PSTN->IP)	Fax Mode	ECM	Rate	Tone Detection by	Switch into Fax Mode When Detected CNG or CED
☐	0	default...	Voice and Fax	Telephone	Basic	+4dB	0dB	Adaptive	Disable	14400bps	Local	Disable

Tel profile is mainly consisting of a series of line related parameters include FAX, gain value etc. which are used to configure different parameters for each port.

5.9 **Port**

A unique SIP account used for registration can be configured for each port of device. Parameters of the SIP account include port number, whether to register, primary display name, primary SIP user ID, primary Authenticate ID, primary Authenticate password, off-hook auto-dial number, caller ID and so on.

Figure-Configure SIP Account for Port Registration


Port

	Port	IP Profile	Tel Profile	Display Name	SIP User ID	Authenticate ID	Offhook Auto-Dial	DND(Do Not Disturb)	Caller-ID	CFU	CFB	CFNRy	Call Waiting	Play Call Waiting Tone
☐	51	0 <default>...	0 <default>...	1100006...	1100006...	1100006...	---	Disable	Enable	---	---	---	Disable	Disable

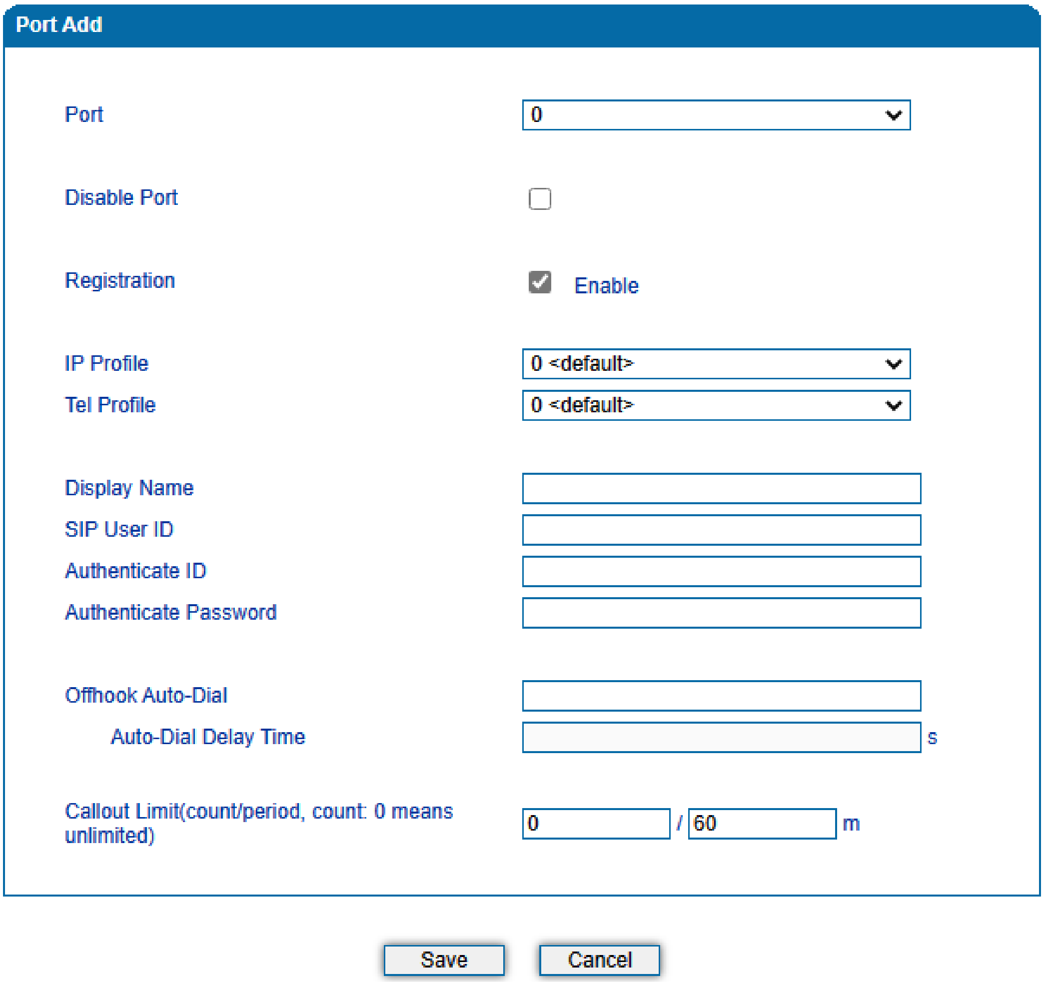


Table-Explanation of Parameters Related to SIP Registration

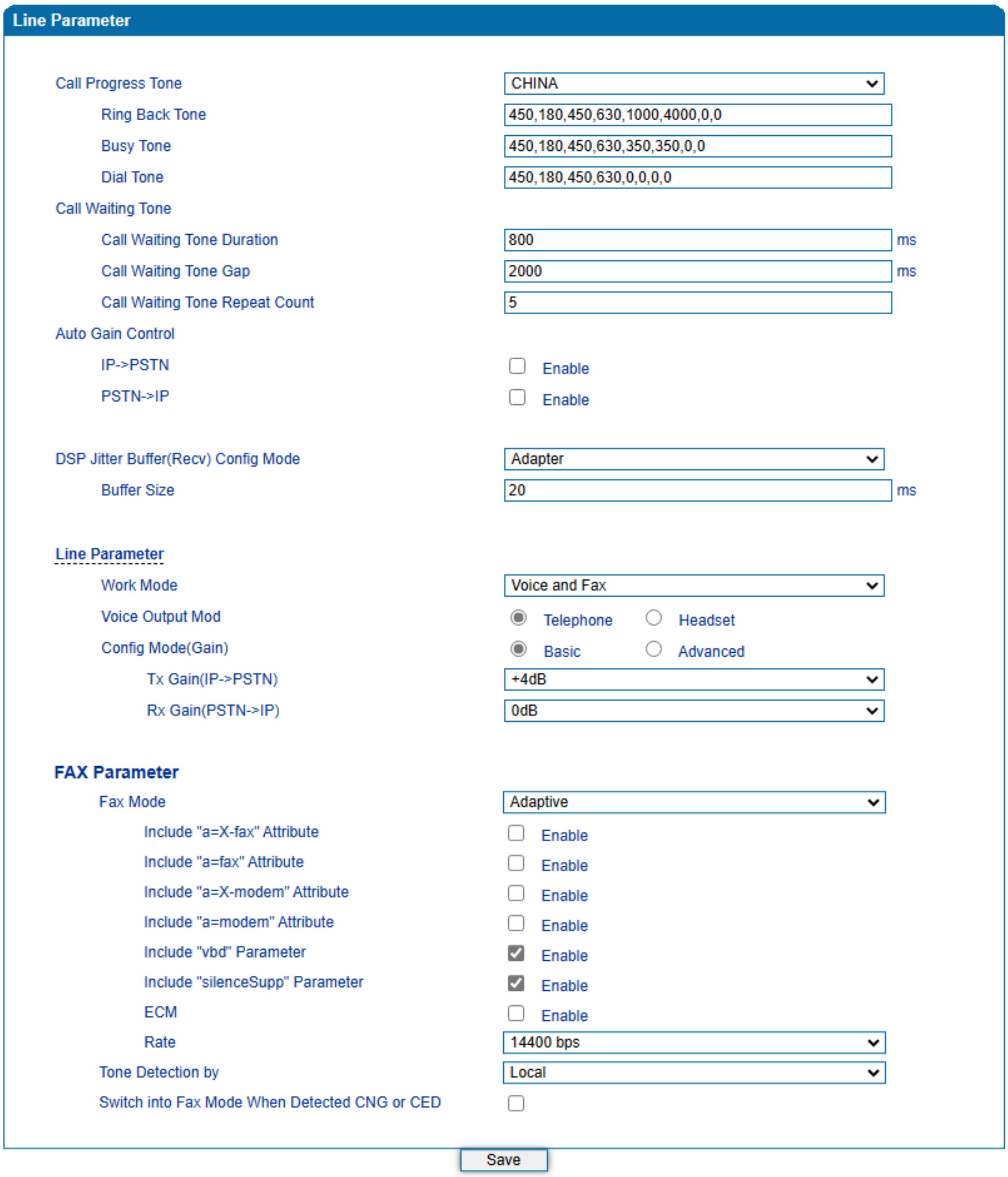
Parameter	Explanation
Port	The FXO port corresponding to this account
Disable port	Whether to disable port temporally
Registration	Whether to enable registration for the port
IP Profile	Assign IP profile (which need to be created in advance)
Tel Profile	Assign Tel profile (which need to be created in advance)
Display name	Description of SIP account. It is used to identify the SIP account.

SIP User ID	User ID of the SIP account, which is provided by VoIP service provider (ITSP) for registration. Usually, it is in the form of digits similar to phone number or an actual phone number.
Authenticate ID	SIP service subscriber’ s authenticate ID used for authentication of registration. It can be identical to or different from SIP User ID.
Authenticate Password	SIP service subscriber’ s authenticate ID used for authentication of registration
Offhook Auto-Dial	An extension or phone number is pre-assigned here so that the number is automatically dialed as soon as user picks up the phone
Auto-Dial Delay Time	How long the auto-dial number is prolonged. If it is set as 3s, the auto-dial number is dialed after 3 seconds passed.
Callout Limit	The number of outgoing calls available in the current minute. Calls cannot be made if the number of times is exceeded. The default is 0, which means no limit.

5.10 Advanced

5.10.1 Line Parameter

On the **Advanced→ Line Parameter** page, you can configure Line parameters which include for call progress tone, auto gain control, fax parameters and so on.



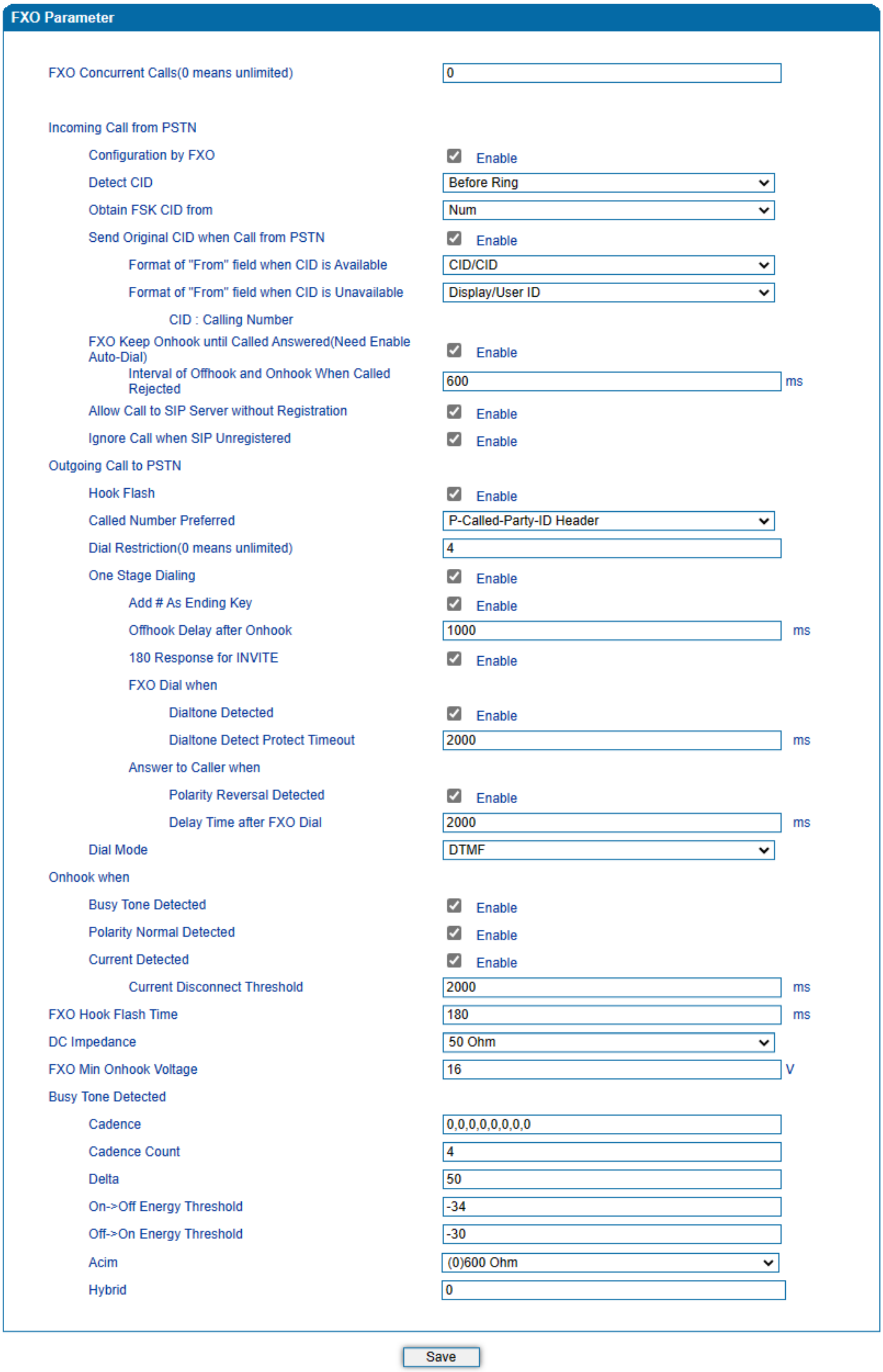
Parameter	Explanation
Call Process Tone	The signal tone standard after a phone is picked up. Choose national standards from the drop-down box. Default value is USA.
Call Waiting Tone	Set the duration, gap and repeat count of call waiting tone
Auto Gain Control	Whether to enable automatic gain control
DSP Jitter Buffer(Recv) Config Mode	It supports two modes, static and adapter
Line Parameter	
Work Mode	To set the ports work in both Voice and Fax mode. There are several configure options: • Voice and FAX: to be able to make call and use FAX service • Voice Only: allows to make call only, Fax doesn’t work if you connect a fax machine • Fax Only: allows to make Fax call only. • POS only: allows to connect POS terminal only
Voice Output Mod	It supports two voice output modes: telephone and headset
Config Mode(Gain)	It can adjust the Tx gain and Rx gain, and supports both basic and advanced configuration modes
FAX Parameter	
Fax Mode	There are three fax modes: T.38, T.30(Pass-through), and Adaptive.
Include “a=X-fax” Attribute	If this parameter is enabled, “a=X-fax” attribute will be carried in SDP

Include “a=fax” Attribute	If this parameter is enabled, “a=fax” attribute will be carried in SDP
Include “a=X-modem” Attribute	If this parameter is enabled, “a=X-modem” attribute will be carried in SDP
Include “a=modem” Attribute	If this parameter is enabled, “a=modem” attribute will be carried in SDP
Include "vbd" Parameter	If this parameter is enabled, “a=gpmd:0 vbd=yes” attribute will be carried in SDP
Include "silenceSupp" Parameter	If this parameter is enabled, “a=silenceSupp:off” attribute will be carried in SDP
ECM	Whether to enable ‘Error Correction Mode’ (ECM).
Rate	The rate of sending or receiving fax, default value is 14400bps.
Tone Detection by	Fax sound is detected by caller, callee or automatically.
Switch into Fax Mode When Detect CNG or CED	If this parameter is enabled, the system will switch into fax mode when CNG or CED is detected.

5.10.2 FXO Parameter

FXO full name is Foreign Exchange Office. It is a kind of voice interface, and a trunk connected between central exchange switches and telephone exchange system. To central office speaking, it simulates a PABX extension, and can connect common phones and a multiplexer. It also is FXO interface connected with SPC exchanges.

FXO as ordinary telephone interface, and need to remote provide current. FXO may connect company' s internal PBX service extension and the telecom outside. Configuration interface as follow:



Parameter	Explanation
FXO Concurrent Calls(0 means unlimited)	Limit the number of concurrent FXO calls (0 means no limit, and the maximum number is the total number of FXO ports) which means the number of call requests received by the gateway per second. to prevent the call server from initiating large number of calls instantly, causing traffic shocks. It is designed to prevent the server from initiating large number of calls at the same time and causing traffic shocks.
Incoming Call from PSTN	
Configuration by FXO	When the incoming call from PSTN, you can enable or disable the FXO configuration. The FXO configuration function includes Detect CID, Send Original CID and so on.
Detect CID	When a call comes to the FXO port, FXO detects the calling number and the order of ringing. The system has two modes: first ringing and then detecting CID, first detecting CID and then ringing. The PSTN line sending CID methods usually include: sending CID before ringing, and sending CID after ringing. Therefore, when FXO detects CID, it needs to be set according to the way of PSTN line sending CID.
Send Original CID when Call from PSTN	When enabled, the caller ID of the extension will display on the PSTN side when dialing the extension. When it is not enabled, the caller ID of the extension will be display the number of the FXO port.
FXO Keep Onhook until Called Answered(Need Enable Auto-Dial)	After enabled, when the PSTN calls into the FXO gateway, the FXO device will go off-hook after the extension number dialed is connected. If this function is disabled, when the user dials in to the FXO port, the FXO first off-hook, and then initiates a call request to the IP.

Allow Call to SIP Server without Registration	Allow the port to initiate a call request without registering to the SIP Server. At this time, the device works in point-to-point mode.
Ignore Call when SIP Unregistered	When enabled, the device will ignore incoming calls when the FXO port registration fails.
Outgoing Call to PSTN	
Hook Flash	When enabled, the device supports Hook Flash.
Called Number Preferred	When making an outgoing call, the device obtains the called number from the SIP message of the remote end. According to the content of the SIP request, the called number may be obtained from the following three fields: ● P-Called-Party-ID Header ● Request-line ● To header
Dial Restriction(0 means unlimited)	When FXO gateway calls the PSTN, set a simultaneous dialing limit (0 means no restriction).
One Stage Dialing	Enabled by default, the call mode of FXO gateway means that when the FXO device makes an outgoing call, the called number obtained from the SIP message is sent to the analog end digit by digit at a time.
Add # As Ending Key	When FXO gateway makes an outgoing call, it will automatically add # after the original number as the end key to dial out together.
Offhook Delay after Onhook	When FXO gateway calls the PSTN, the delay time for the FXO device to go off-hook after on-hook (default 1000ms).
180 Response for INVITE	When the device receives the INVITE request from the remote end, it sends 180 as a temporary response code to the IP side.

FXO Dial when	
Dial tone Detected	When FXO dials to the PSTN side, the FXO port will automatically dial to the PSTN side if it detects a dial tone from the PSTN line
Dial tone Detect Protect Timeout	Configure the Dial tone Detect Protect Timeout, the range is from 100ms to 65535ms.
Answer to Caller when	
Polarity Reversal Detected	When FXO gateway calls the PSTN, the way that FXO answers the caller is to detect the polarity reversal. After enabled, if a polarity reversal is detected, it will be reported to the caller for response. If the PSTN side cannot provide the polarity reversal detected, this function is invalid.
Delay Time after FXO Dial	The time for the FXO device to detect the polarity reversal and answer the caller should be less than this value. The system defaults to 10s. If the time is exceeded, the called is considered to have answered. This parameter is mostly used when there is no reverse polarity on the PSTN.
Dial Mode	FXO gateway calls the PSTN and supports 3 dialing methods: DTMF, Pulse, Pulse before DTMF
On-hook when **Busy Tone Detected/** **Polarity Normal Detected/** **Current Detected**	After enabling this function, the FXO gateway calls the PSTN, the FXO device hang up when: busy tone detected, polarity normal detected and current detect.
Current Disconnect Threshold	When enabled, the FXO port will hang when the current polarity of the FXO port is returned to normal

FXO Hook Flash Time	When FXO is hung, it needs to wait for a period of time to take it Off-hook, and send a Hook Flash signal to the PSTN side during that interval. The default is 180ms.
DC Impedance	The impedance parameters when FXO gateway is connected to PBX or PSTN.
FXO Min Onhook Voltage	Minimum on-hook voltage of gateway.
Busy Tone Detected	
Cadence	The busy tone detection cadence needs to be set according to the busy tone system of the PSTN. If you do not know the busy tone standard, you can use the busy tone detection function to detect the busy tone cadence.
Cadence Count	The cadence count is used to detect the validity of the busy tone. When multiple busy tone beats are continuously detected, it is as a valid busy tone.
Delta	The error value of busy tone detection cadence.
On->Off Energy Threshold	The energy threshold of busy tone from On to Off.
Off->On Energy Threshold	The energy threshold of busy tone from Off to On.
Acim	The value of AC impedance.
Hybrid	The value of hybrid balance parameters.

5.10.3 Media Parameter

Media parameters mainly include RTP start port, DTMF parameter, preferred Vocoder, etc.

Figure-Configure Media Parameters

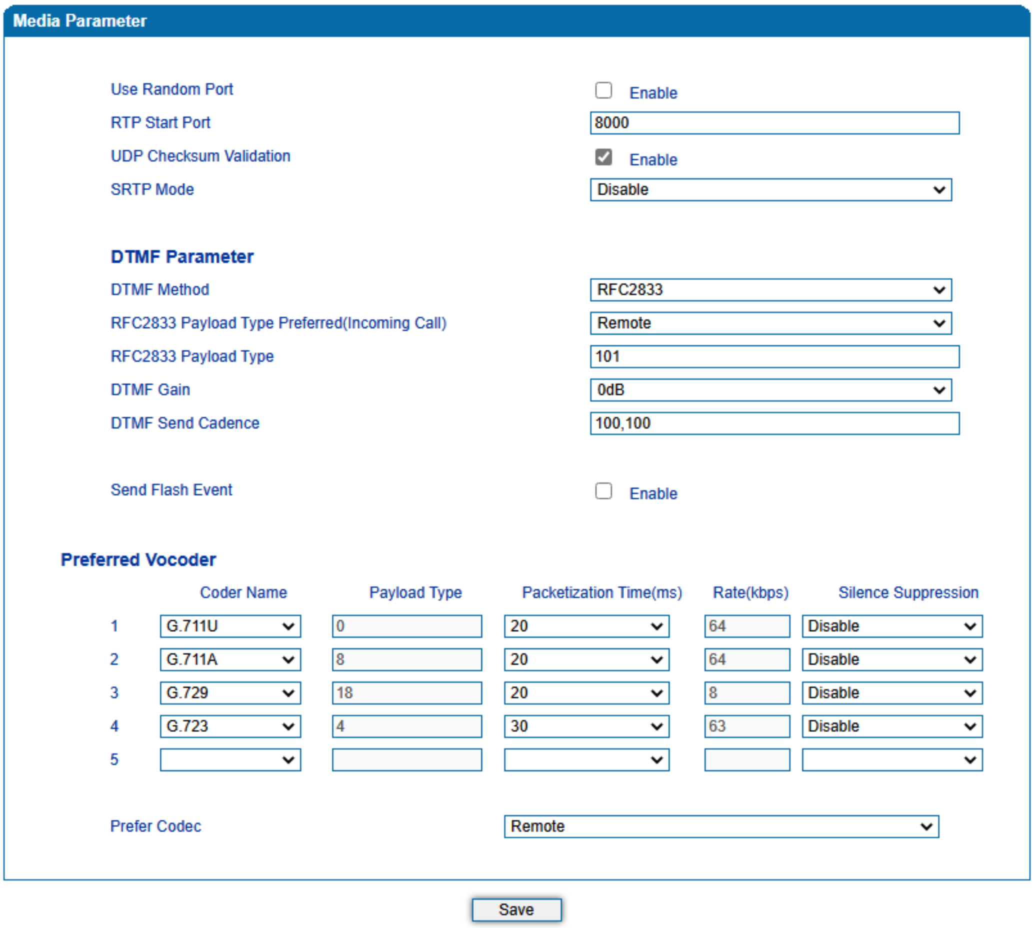


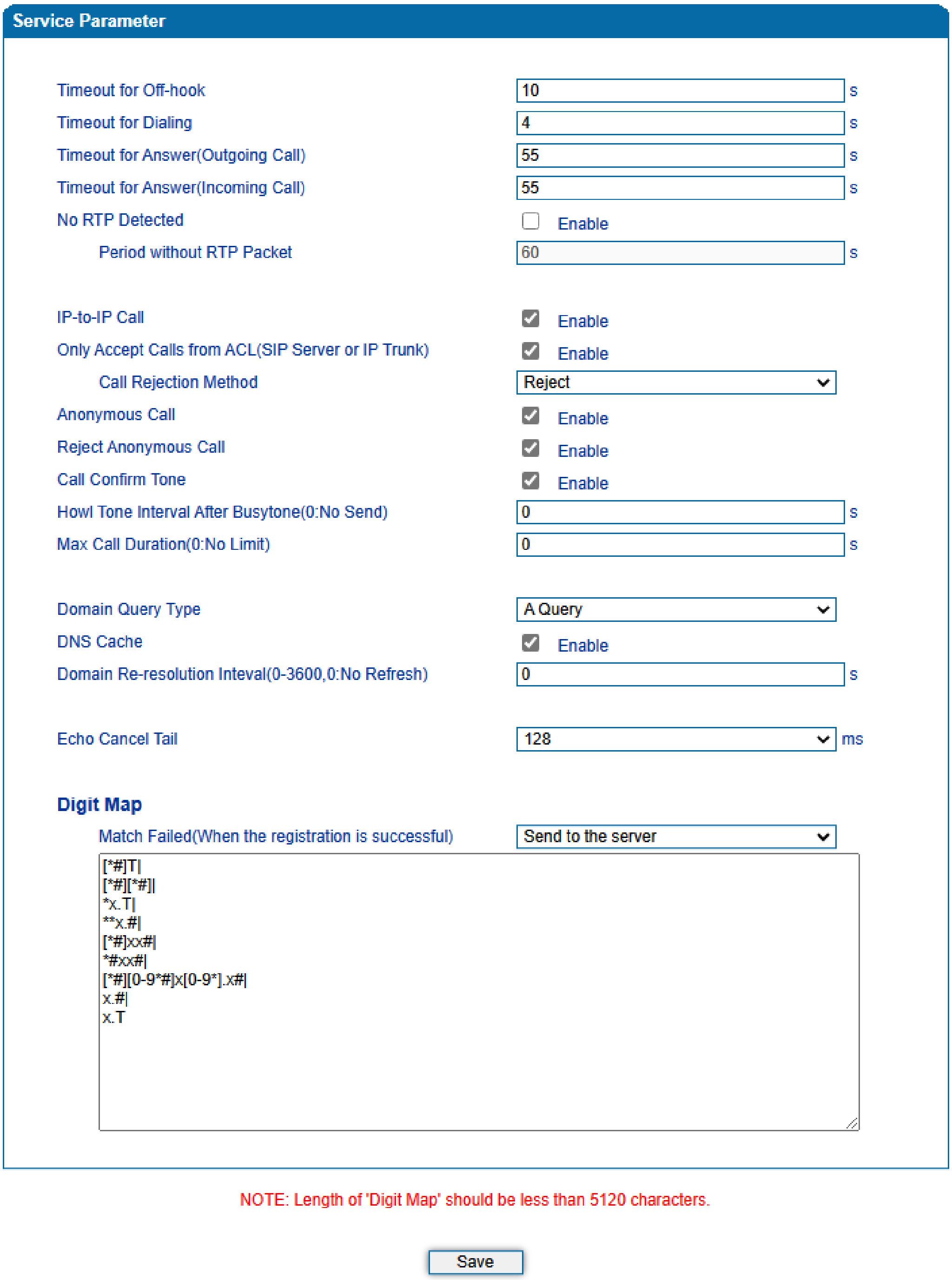
Table-Explanation of Media Parameters

Parameter	Explanation
Use Random Port	Create a random RTP start port
RTP Start Port	When 'Use Random Port' is not selected, you need to configure a start port for RTP. Default RTP start port is 8000
UDP Checksum Validation	Choose whether to enable header checksum of UDP
SRTP Mode	Configure whether RTP is encrypted
DTMF Parameter	
DTMF Method	Include SINGAL, INBAND and RFC2833

RFC2833 Payload Type Preferred (Incoming Call)	For an incoming call, choose local or remote RFC2833 payload type as the preferred payload type
RFC2833 Payload Type	Local payload value, default value is 101
DTMF Gain	Default value is 0 DB
DTMF Send Cadence	Time interval for DTMF signal transmission, default is 100 ms.
Send Flash Event	If this parameter is enabled, the device will send flash-hook event to remote terminal, and thus user does not need to handle it locally
Preferred Vocoder	
Coder Name	The device supports G.729, G.711U, G.711A, G.723, G.726-16/24/32/40. When outgoing calls are made, G.729 will be used.
Payload Type	Each kind of coding has a unique load value, refer to RFC3551.
Packetization Time	The time for voice packaging
Rate	Voice data flow rate; It is defaulted by system.
Silence Suppression	Default value is 'disabled'. If this parameter is enabled, VoIP transmission bandwidth can be saved, and meanwhile network congestion can be avoided.
Prefer Codec	Choose local or remote codec as the preferred codec

5.10.4 Service Parameter

Service parameters include timeout for dialing, digitmap, MWI message and so on.



Parameter	Explanation
Timeout for off-hook	Mainly used to define a timer that when the user is off hook an analog phone without dial any digits
Timeout for dialing	With the help of dialing timeout, you can limit the time between two digits while users are typing the digits of a number through an extension. If the timeout expires, the gateway will consider the dialing has finished and will try to send message to SIP server. Default value is 4 seconds.
Timeout for answer (Outgoing call)	This parameter determines how long the caller party will wait for answer when making outgoing calls through a phone.
Timeout for answer (Incoming call)	This parameter determines how long the phone rings when there are incoming calls
No RTP Detected	If this parameter is enabled, the situation will be detected when there is no RTP packets received during the set time period.
Period without RTP Packet	The time period when there is no RTP packets received.
IP-to-IP Call	If this parameter is enabled, user can dial IP address through a phone to call destination gateway.
Only Accept Call from ACL (SIP server or IP Trunk)	If this parameter is enabled, the device only accepts incoming call from SIP server only. Default value is ‘not enable’.
Anonymous Call	If this parameter is enabled, ‘anonymous’ will be included in SIP message. And the calls made by the device are anonymous.
Reject Anonymous Call	If this parameter is enabled, all anonymous calls will be rejected. Default value is ‘not disable’.

Call Confirm Tone	When enabled, the device will play back a ringback tone even if the device does not receive a 180 response
Howl Tone Interval After Busytone(0:No Send)	The time interval for Howler tone after playing Busytone
Max Call Duration(0:No Limit)	When the duration of call is reach the set time, the call will hang up directly (default is 0, 0 means unlimited)
Domain Query Type	Set the query of the domain name, and support three query methods: A query, SRV query and NAPTR query
DNS Cache	When enabled, the device will not initiate domain name query requests to DNS servers during the re-resolution interval.
Domain Re-resolution Interval(0-3600,0:No Refresh)	Configure the domain name re-resolution interval. The range is 0-3600, and 0 means no refresh
Echo Cancel Tail	Configure echo cancellation duration

Digitmap is used for number dialing of calls through the ports of the device.

Parameter		**Explanation**
Supported Objects	Digit	0-9
	T	Timer
	DTMF	A digit, a timer, or one of the symbols of A, B, C, D, #, or *
Range	[ ]	One or more DTMF symbols enclosed in the [], but only one DTMF symbol can be selected
Range	()	One or more expressions enclosed the (), but only one can be selected

Separator	|	Separate expressions or DTMF symbols.
Subrange	-	Two digits separated by hyphen (-) which matches any digit between and including the two digits.
Wildcard	x	Matches any digit of 0 to 9
Modifiers	.	Matches 0 or more times of the preceding element
Modifiers	?	Matches 0 or 1 times of the preceding element

5.10.5 SIP Compatibility

SIP parameters include attended transfer trigger, early media, session timer, heartbeat interval and so on.

Figure-Configure SIP Parameters

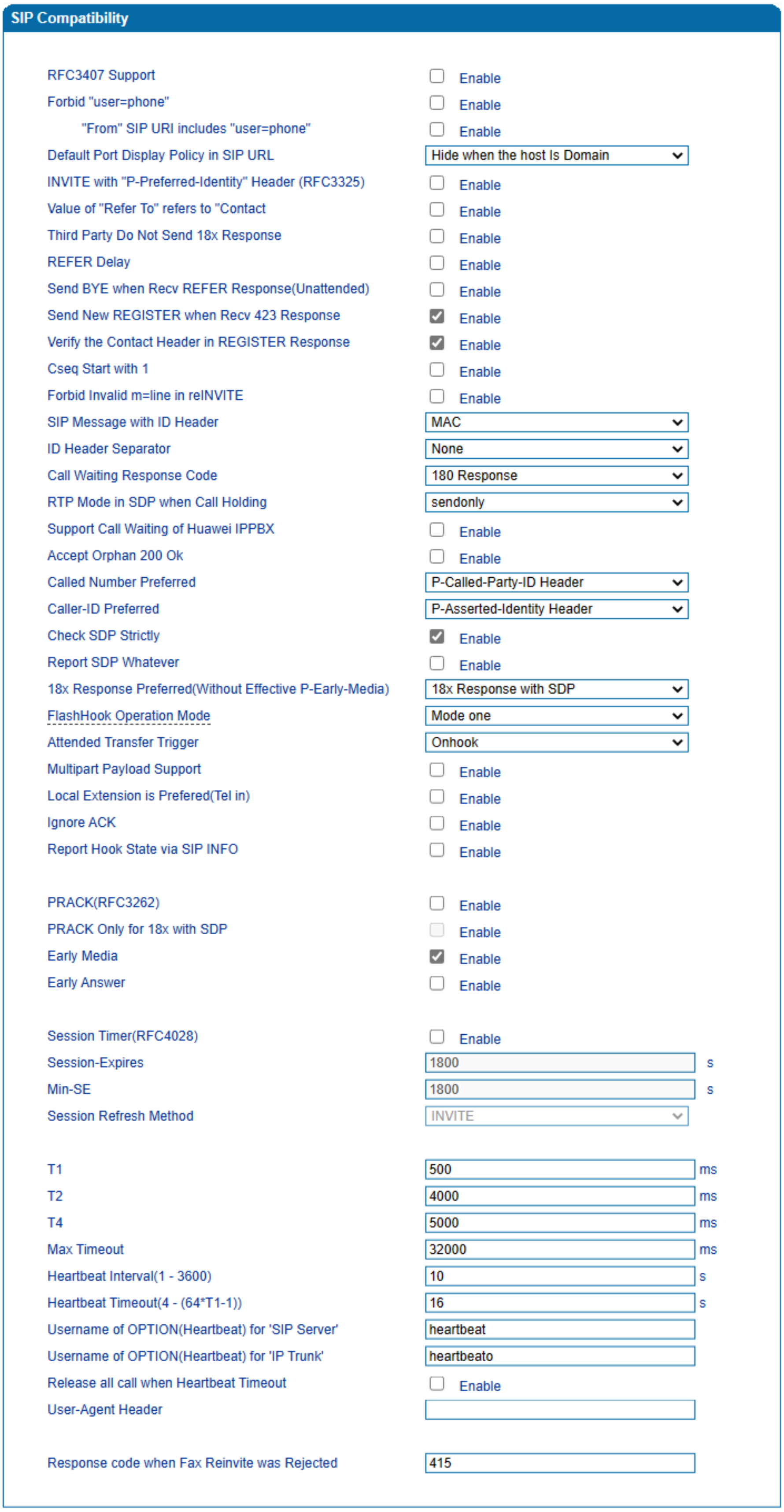


Table-Explanation of SIP Parameters

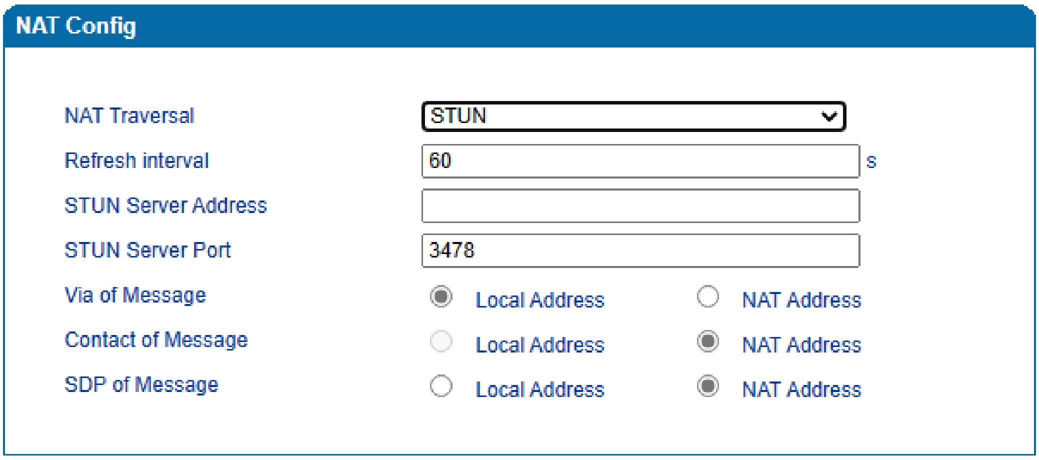
Parameter	Explanation
RFC3407 Support	Whether to enable RFC3407 support. If this parameter is enabled, the device will support RFC3407 which defines the SDP capability of backward compatibility.
Forbid "user=phone"	When disabled, the "user=phone" is not carried in the URI
"From" SIP URI includes "user=phone"	If this parameter is enabled, 'user=phone' will be contained in URI. When calls are routed to PSTN network, the called number will be got from user name. Default value is 'not enable'.
Default Port Display Policy in SIP URL	It supports Hidden, Display and Hide when the host Is Domain.
INVITE with "P-Preferred-Identity" Header (RFC3325)	If this parameter is enabled, "P-Preferred-Identity" header will be added in INVITE message for anonymous call (Support RFC3325).
Value of "Refer To" refers to "Contact	If this parameter is enabled, 'contract header' needs to be filled in in the 'refer to' field of a SIP message.
Third Party Do Not Send 18x Response	If this parameter is enabled, the third party will not send 18x response during an attended transfer.
REFER Delay	When the call is in blind transfer status, as a call transfer initiator, it only received a 200 OK from remote side and then send REFER.
Send BYE when Recv REFER Response(Unattended)	If this parameter is enabled, the third party will send BYE to release session after receiving REFER during a blind transfer.

Send New REGISTER when Recv 423 Response	If this parameter is enabled, the value of 'expires' header will be automatically updated and REGISTER will be re-sent after receiving of 423 response.
Verify the Contact Header in REGISTER Response	Enabled it, the contact header will be verified, if the verification failed, the registration will be failed.
Cseq Start with 1	If this parameter is enabled, the value of CSeq starts with '1'.
Forbid Invalid m=line in reINVITE	If this parameter is enabled, the device will prevent 'invalid m=line' from being carried in the SDP of re-INVITE.
SIP Message with ID Header	SIP header carries two types of IDs with MAC or SN.
ID Header Separator	ID header separator for MAC or SN.
Call Waiting Response Code	User can choose 180 or 182 as call waiting response code
RTP Mode in SDP when Call Holding	Use 'send only' or 'inactive' as RTP mode during call holding.
Support Call Waiting of Huawei IPPBX	If this parameter is enabled, the device will support call waiting of Huawei IPPBX.
Accept Orphan 200 OK	If this parameter is enabled, the device will support different 'to-tag 200 OK' in an INVITE session.
Called Number Preferred	Choose P-Called-Party-ID header or Request-Line
Caller-ID Preferred	Choose P-Asserted-Identity header or From Header
Check SDP Strictly	Strictly or not for SDP check.
Report SDP whatever	when enabled, even if 200 OK is received, the device will report SDP

18x Response Preferred(Without Effective P-Early-Media)	It supports 18x Response with SDP, Last 18x Response, and Local Ring Tone Only.
Flashhook Operation Mode	Choose Mode one, Mode two or Mode three
Attended Transfer Trigger	Choose 'Onhook' or 'Flashhook +4'
Multipart Payload Support	Support MIME types.
Local Extension is Prefered(Tel in)	When enabled, the device matches the called number with the extension number on the device before sending the number to the server. If the match is successful, the local extension will ring, if the match is unsuccessful, an invite message will be sent to the server.
Ignore ACK	If enabled it, When the device is off-hook, and even though SIP UA does not receive ACK message, the, the device do not resend 200 OK response.
Report Hook State via SIP INFO	If enabled it, whether the device is in Off-hook or on-hook status, SIP-INFO will send.
PRACK(RFC3262)	If this parameter is enabled, the device supports reliable transmission of provisional response
PRACK Only for 18x with SDP	If this parameter is enabled, only PRACK will be sent when there's SDP in 18x response
Early Media	If this parameter is enabled, the device supports the receiving of Early Media.
Early Answer	If this parameter is enabled, the device supports early answer
Session Timer (RFC4028)	Whether to enable 'session timer', default value is 'not enable'.
Session-Expires	The interval for refreshing session; default value is 1800s. The Session-Expires header field conveys the session interval for a SIP session.

Min-SE	The minimum interval for refreshing session; default value is 1800s. The Min-SE header field indicates the minimum value for the session interval.
Session Refresh Method	The method to refresh session; default value is INVITE.
T1	Value of T1 timer in SIP protocol, default is 500ms
T2	Value of T2 timer in SIP protocol, default is 4000ms
T4	Value of T4 timer in SIP protocol, default is 5000ms
Max Timeout	The max timeout of sending or receiving SIP messages, default is 32000ms
Heartbeat Interval	The interval for sending heartbeat message, Default is 10s.
Heartbeat Timeout	The timeout for heartbeat message to be sent, default to 16s
Username of OPTION(Heartbeat) for "SIP Server"	The user ID part of OPTION SIP message in the heartbeat request for SIP server
Username of OPTION(Heartbeat) for "IP TRUNK"	The user ID part of OPTION SIP message in the heartbeat request for IP trunk
Release all call when Heartbeat Timeout	Then the heartbeat timeout expired, all the calls will be released or terminated.
User-Agent Header	Customize the UA header
Response code when Fax Reinvite was Rejected	Customized the SIP response code for Fax rejection.

5.10.6 **NAT Parameter**



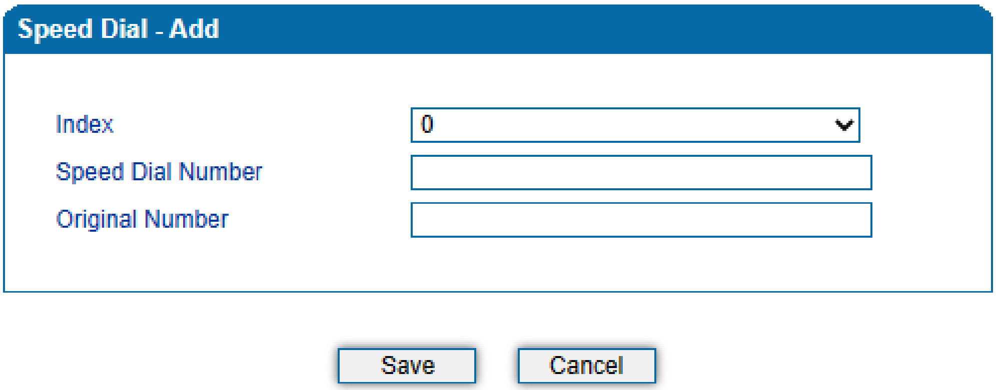
NAT Traversal (Network Address Translator Traversal) is a computer networking technique of establishing and maintaining Internet protocol connections across gateways that implement network address translation (NAT). NAT breaks the principle of end-to-end connectivity originally envisioned in the design of the Internet.

STUN (Simple Traversal of UDP over NATs) is a lightweight protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public Internet. It also provides the ability for applications to determine the IP addresses allocated to them by the NAT. STUN works with many existing NATs, and does not require any special behavior from them. STUN doesn’t support TCP connection and H.323.

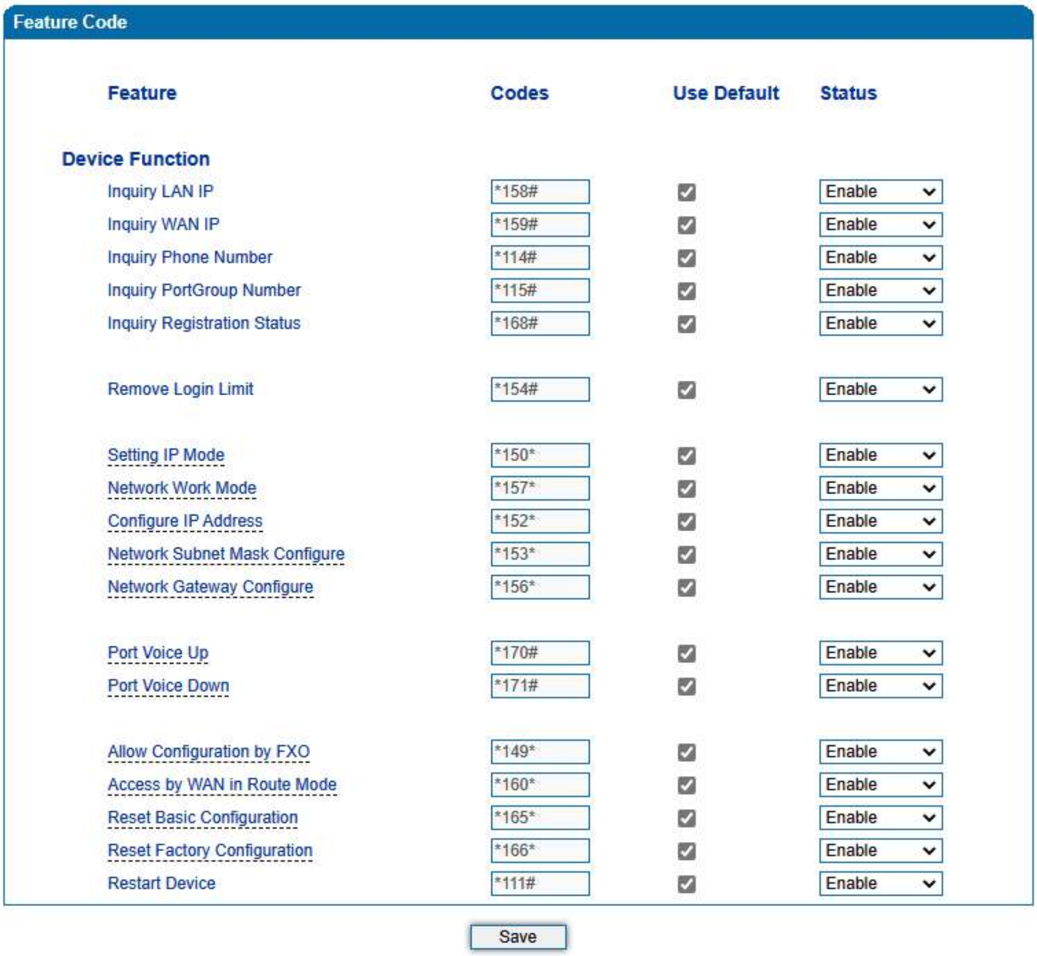
Parameter	Explanation
NAT Traversal	The device supports 4 types of NAT traversal methods: STUN, static NAT, dynamic NAT and DTR.
NAT IP	When static NAT is selected as the NAT traversal method, a static NAT address needs to be configured
Refresh interval	When STUN is selected as the NAT traversal method, the device queries the NAT address at certain intervals
STUN Server Address	Configure IP address of STUN server (it support IP address or domain name)
STUN Server Port	Configure port of STUN server
Via of Message	Via header in SIP messages uses local network address or NAT address
Contact of Message	Contact header in SIP messages uses local network address or NAT address
SDP of Message	SDP in SIP messages uses local network address or NAT address
DTR Server Address	Configure IP address of DTR server.
DTR Server Port	Configure port of DTR server.
DTR Password	Configure password of DTR password.

5.10.7 Speed Dial

Speed dial is a function that is available on telephones which provides an easy method of calling a telephone number by pressing fewer digits on the keypad. The tool enables one to save, organize, and have easy and quick access to regularly dialed numbers.



5.10.8 Feature Code



Parameter	Explanation
Inquiry LAN IP	Dial*158# to obtain device’ s LAN port IP address
Inquiry WAN IP	Dial *159# to query device’ s WAN port IP address
Inquiry Phone Number	Dial*114# to obtain port account
Inquiry Port Group Number	Dial *115# to obtain port group number
Inquiry Registration Status	Dial *168# to query the register status of a FXO port
Remove Login Limit	Dial *154# to remove login limit
Setting IP Mode	*150*0#, means ppp modem, *150*1#, means static IP, *150*2#, means obtain IP address by DHCP, *150*3#, means PPPoE.
Network Work Mode	Dial *157*0# to set Network Work Mode as Router mode Dial *157*1# to set Network Work Mode as Bridge mode
Configure IP Address	*152*+IP, set gateway IP address
Network subnet mask configure	*153*+subnet mask, set gateway subnet mask
Network Gateway Configure	*156*+gateway IP, set gateway
Port Voice Up	Dial *170# to increase the sound volume of a FXO port
Port Voice Down	Dial *171# to decrease the sound volume of a FXO port
Allow Configuration by FXO	Dial *149*1 to enable FXO Configuration Dial *149*0 to disable FXO Configuration

Access by WAN in Route Mode	Dial *160*1# to enable access of web through WAN port Dial *160*0# to disable access of web through WAN port Dial *160*3# to enable access of web through LAN port Dial *160*2# to disable access of web through LAN port Dial *160*5# to enable access of telnet through WAN port Dial *160*4# to disable access of telnet through WAN port Dial *160*7# to enable access of telnet through LAN port Dial *160*6# to disable access of telnet through LAN port
Reset Basic Configuration	Dial *165*000000# to restore default username/password and network configuration
Reset Factory Configuration	*166*000000#, reset factory
Restart Device	*111#, restart device

5.10.9 System Parameter

System parameters include NTP, daylight saving time, daily reboot time, web parameter, telnet parameter and remote management. NTP (Network Time Protocol) is a computer time synchronization protocol.

Figure-Configure System Parameters

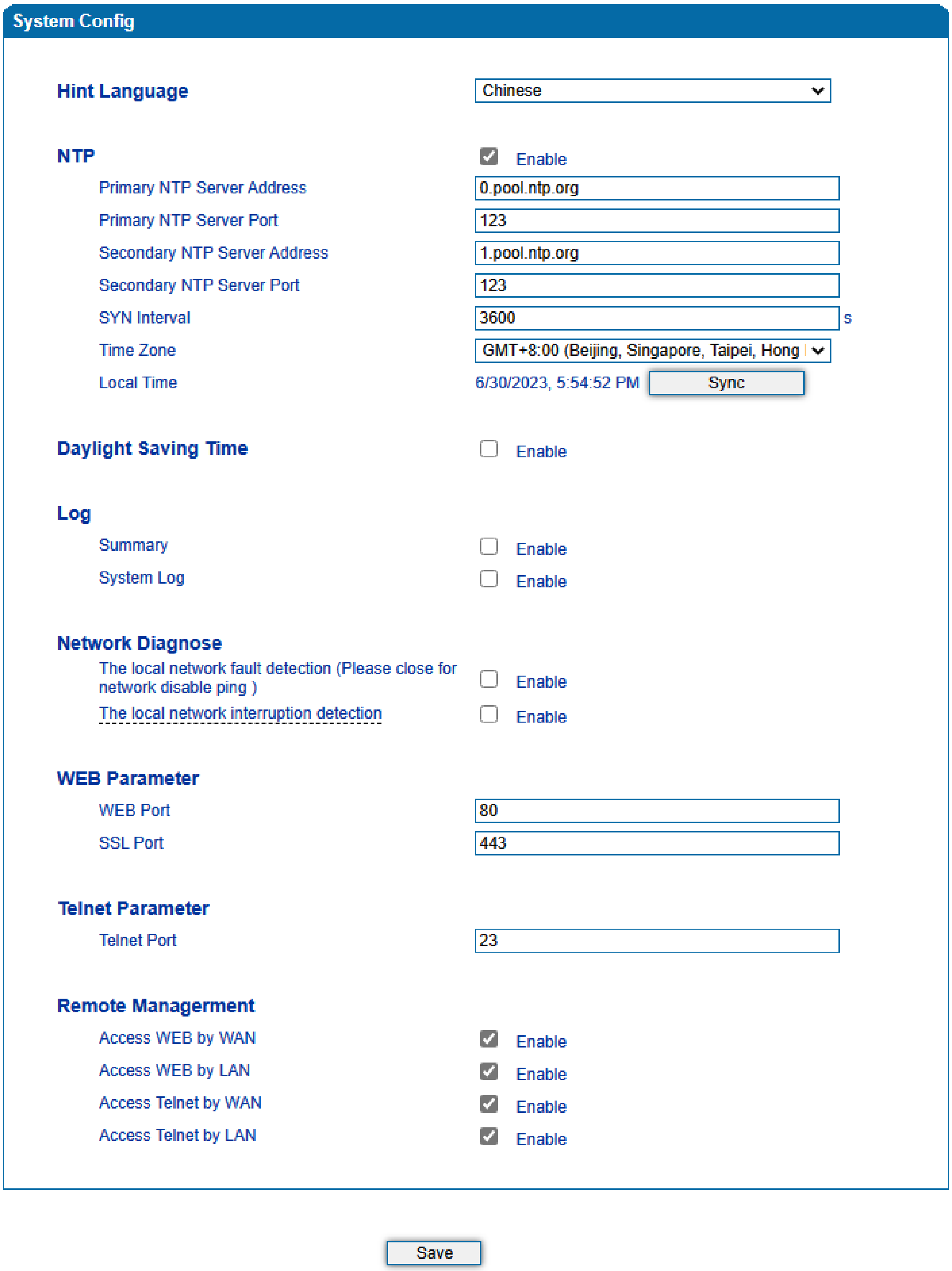


Table-Explanation of System Parameters

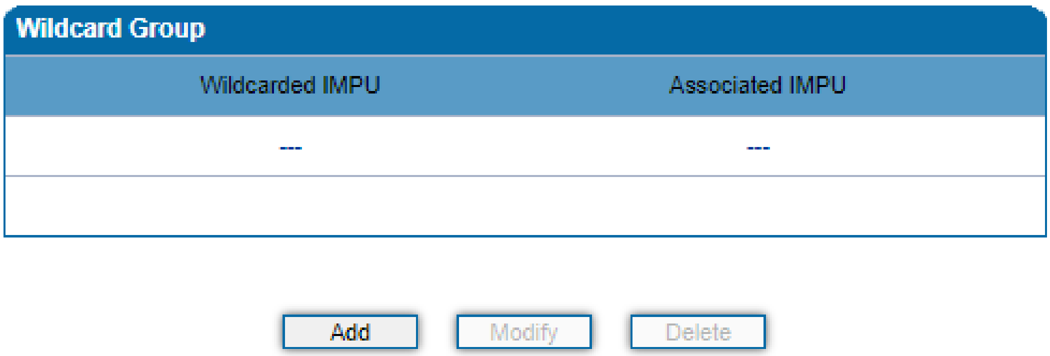
Parameter	Explanation
Hint Language	Set hint language
NTP	To enable or disable NTP
Primary NTP server address	The IP address of primary NTP server; default IP address is us.pool.ntp.org.
Primary NTP server port	The service port of primary NTP server; default port is 123.
Secondary NTP server address	The IP address of secondary NTP server; Default IP address is 64.236.96.53
Secondary NTP server port	The service port of secondary NTP server; Default port is 123
SYN Interval	The interval to synchronize the time of the device. Default value is 3600s.
Time Zone	The time zone of the device; Default configuration is United States central time, Chicago.
Local Time	Synchronize local time
Daylight Saving Time	Enable or disable daylight saving time
Summary	Save the information on reboot to the summary file.
System Log	Save the operation log to a log file.
The local network fault detection (Please close for network disable ping)	Enable local network fault detection.
The local network interruption detection	Enable the local network interruption detection.

WEB Port	The web port of the device; Default port is 80
SSL Port	The SSL port; Default is 443
Telnet port	Listening port of telnet service; Default port is 23
Access WEB by WAN	If enabled, the WEB can be accessed through the IP address of WAN port, if disabled, the WEB cannot be accessed through the IP address of WAN port.
Access WEB by LAN	If enabled, the WEB can be accessed through the IP address of LAN port, if disabled, the WEB cannot be accessed through the IP address of LAN port.
Access Telnet by WAN	If enabled, the Telnet can be accessed through the IP address of WAN port, if disabled, the Telnet cannot be accessed through the IP address of WAN port.
Access Telnet by LAN	If enabled, the Telnet can be accessed through the IP address of LAN port, if disabled, the Telnet cannot be accessed through the IP address of LAN port.

【Note】After Web port and Telnet port are configured, please restart the device for the configurations to take effect.

5.11 Call & Routing

5.11.1 Wildcard Group

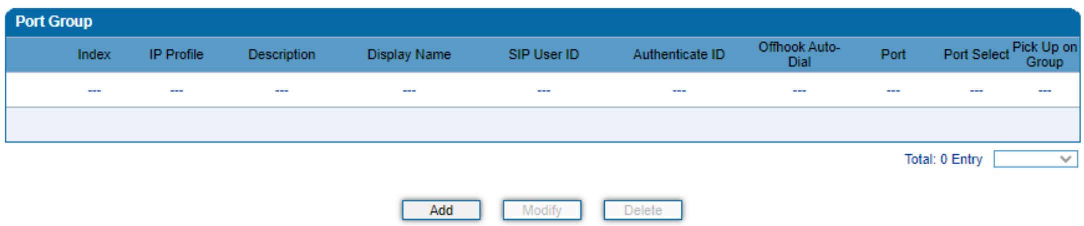


5.11.2 Port Group

When two or more ports need to register with a same SIP account, you can group the ports together and then set an account for the group on the **Call & Routing → Port Group** page.

Parameters of port group include registration, primary display name, primary SIP user id, primary authentication ID and password, secondary display name, secondary SIP user id, secondary authentication ID and password, off-hook auto dial, auto dial delay time, port select, etc.

Figure-Add Port Group



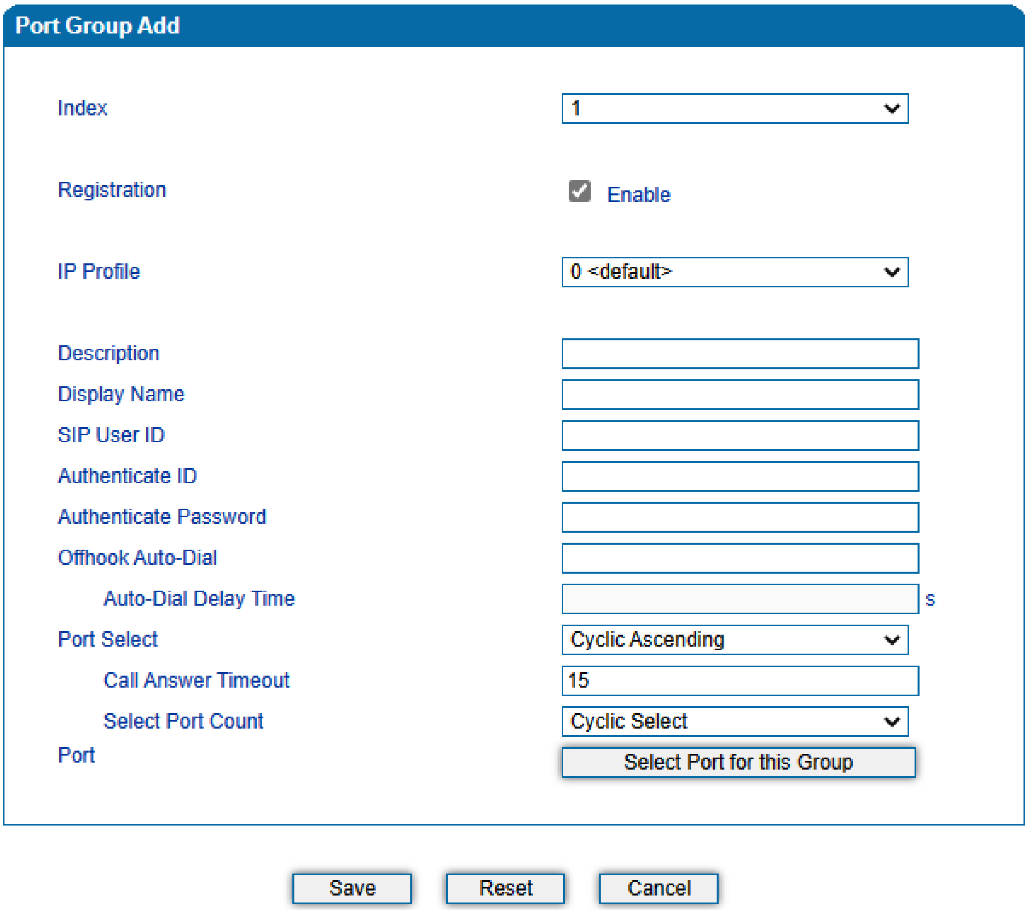


Table-Parameter Explanation of Port Group

Parameter	Explanation
Index	The NO. of the port group; It uniquely identifies a route.
Registration	Registration
IP Profile	IP Profile
Description	The description of the port group; it is used to identify the port group.

Display Name	Display name of the port group, which will be used in SIP message, for example: INVITE sip:bob@biloxi.com SIP/2.0 Via: SIP/2.0/UDPpc33.atlanta.com;branch=z9hG4bK776asdhds Max-Forwards: 70 To: Bob <sip:bob@biloxi.com> From: Alice <sip:alice@atlanta.com>;tag=1928301774 Here Bob and Alice are the display name
SIP User ID	User ID of this SIP account, which is provided by VoIP service provider (ITSP). It is usually in the form of digit similar to phone number or an actual phone number.
Authenticate ID	SIP service subscriber's ID for authentication; it can be identical to or different from SIP User ID.
Authenticate Password	SIP service subscriber's password for authentication
Offhook Auto-Dial	An extension or phone number is pre-assigned here so that the number is automatically dialed as soon as user picks up the phone
Auto-dial Delay time	How long auto-dialing will be delayed

Port Select	It specifies the policy for selecting a port for ringing in the port group • Ascending: the device always selects a port from the minimum number. • Cyclic ascending: the device always selects a port from a number next to the number selected last time. If the maximum number was selected last time, the next selected number is the minimum number. The sequence moves in cycles like this. • Descending: the device always selects a port from the maximum number. • Cyclic descending: the device always selects a port from a number next to the number selected last time. If the minimum number was selected last time, the next selected number is the maximum number. The sequence moves in cycles like this. • Group ring: all ports ring at the same time
Call Answer Timeout	Time for Ring group is expired, select next port for ring. Default time is 15s and rang from 10-120s.
Select Port Count	Support Port Count: Cyclic Select and Only Once.
Port	Select ports for this port group

5.11.3 IP Trunk

A peer-to-peer VoIP call occurs when two VoIP phones communicate directly over IP network without IP PBXs between them. IP trunk helps establish peer-to-peer call between gateway and VoIP phones. IP trunk will be used in routing configuration.

Figure-Configure IP Trunk

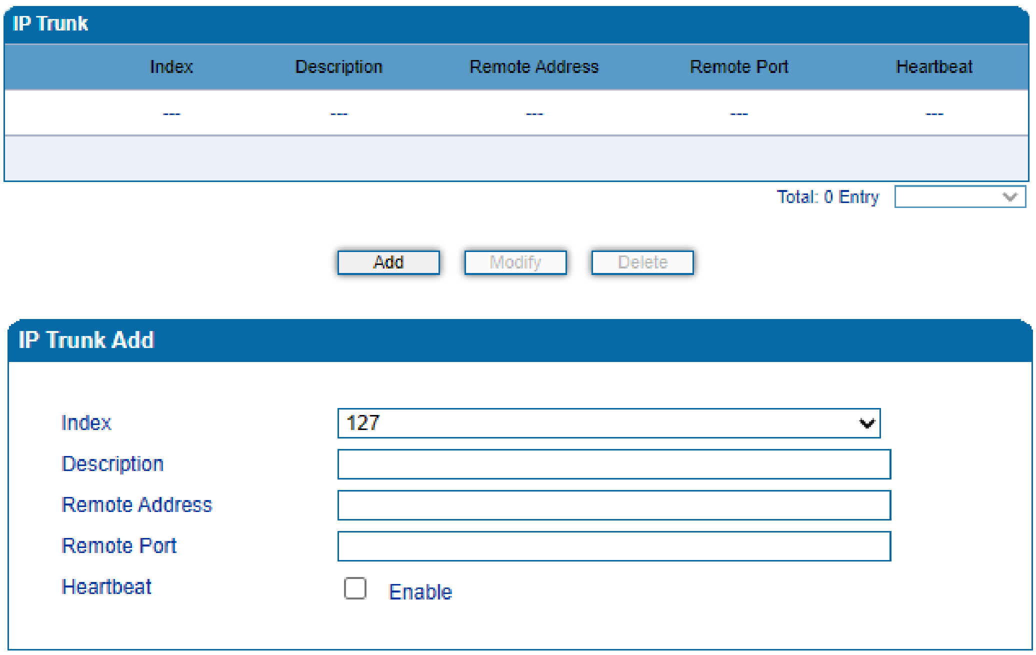


Table-Explanation of IP Trunk Parameters

Parameter	Explanation
Index	The No. of the IP trunk; range is from 0 to 127.
Description	The description of the IP trunk; it is used to n identify the IP trunk.
Remote Address	IP address or domain name of the peer device
Remote Port	SIP port of the peer device
Heartbeat	Whether to enable the ‘Heartbeat’ function for the IP trunk. Default value is ‘not enable’. If heartbeat is enabled, the device will send “OPTION” to the peer device.

5.11.4 Routing Parameter

Routing parameter determines a call routed before or after manipulation.

Figure-Configure Routing Parameter

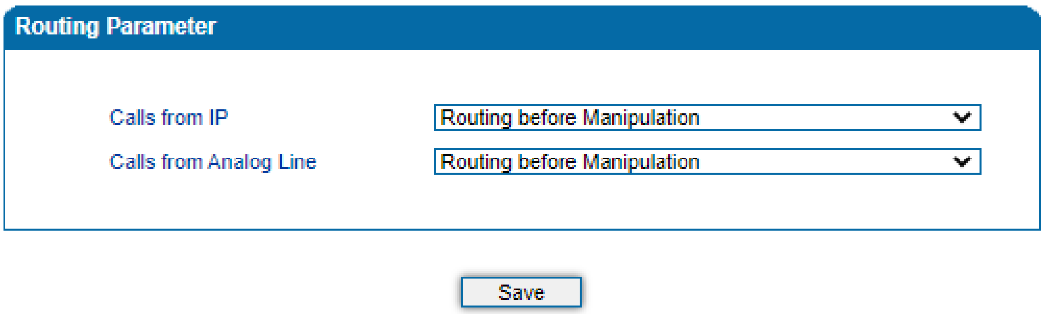


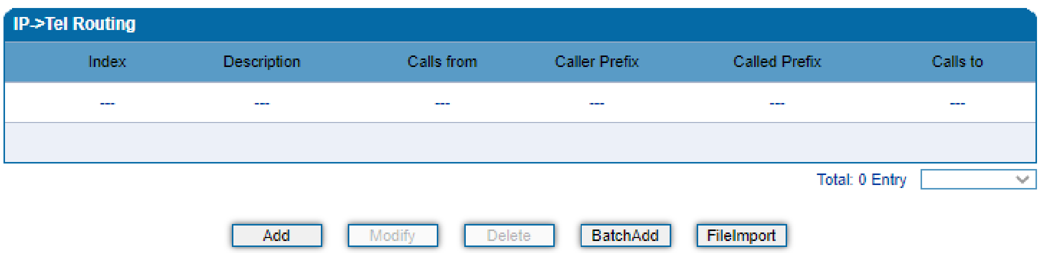
Table-Explanation of Routing Parameters

Parameter	Explanation
Calls from IP	Choose calls from IP network are routed before manipulation or after manipulation.
Calls from Analog Line	Choose calls from analog lines are routed before manipulation or after manipulation.

5.11.5 IP → Tel Routing

Calls from IP network can be routed to port or port group of the device through **IP →Tel routing**.

Figure-Add IP →Tel Routing



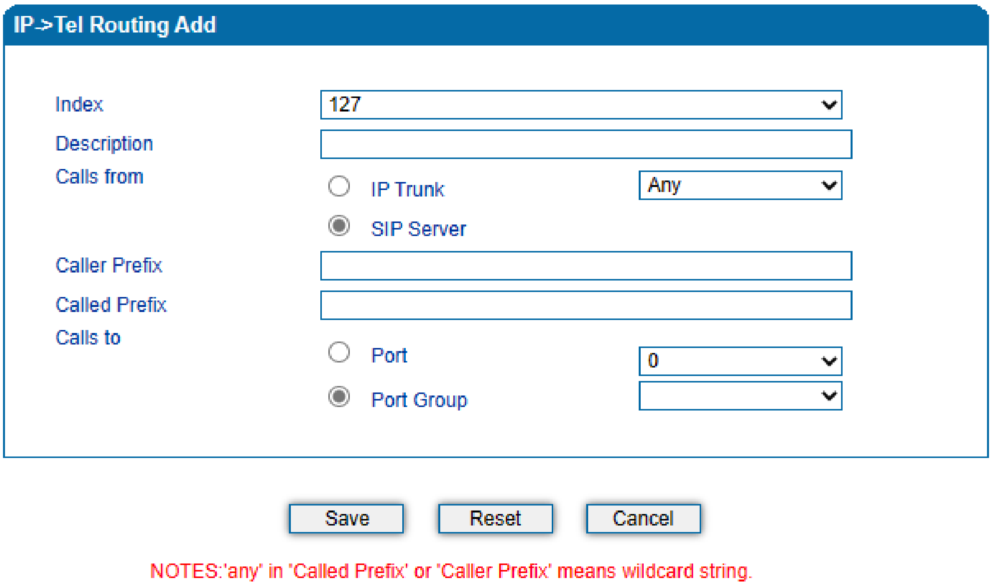


Table-Parameter Explanation of IP →Tel Routes

Parameter	Explanation
Index	Index of the IP →Tel routing; range is from 0 to127; 0 is the highest priority.
Description	Description of the IP →Tel routing; it is used to identify the IP → Tel routing.
Calls from	Choose calls from IP trunk or SIP server; 'any' means any IP addresses.
Caller Prefix	The prefix of the caller number, which helps match routing exactly. Its length is less than or equal to the caller number. For example, if caller number is 2001, the caller prefix can be 200 or 2. 'Any' means the prefix matches any caller number.
Callee Prefix	The prefix of the called number, which helps match routing exactly. Its length is less than or equal to the called number. If the called number is 008675526456659, the called prefix can be 0086755 or 00. "any" means the prefix matches any called number
Calls to	Which port or port group to which calls are routed.

5.11.6 **Tel → IP/Tel Routing**

Calls from the port or port group can be routed to IP trunk or ports of SIP server/other device through Tel →IP/Tel routing.

Figure-Add Tel →IP/Tel Route

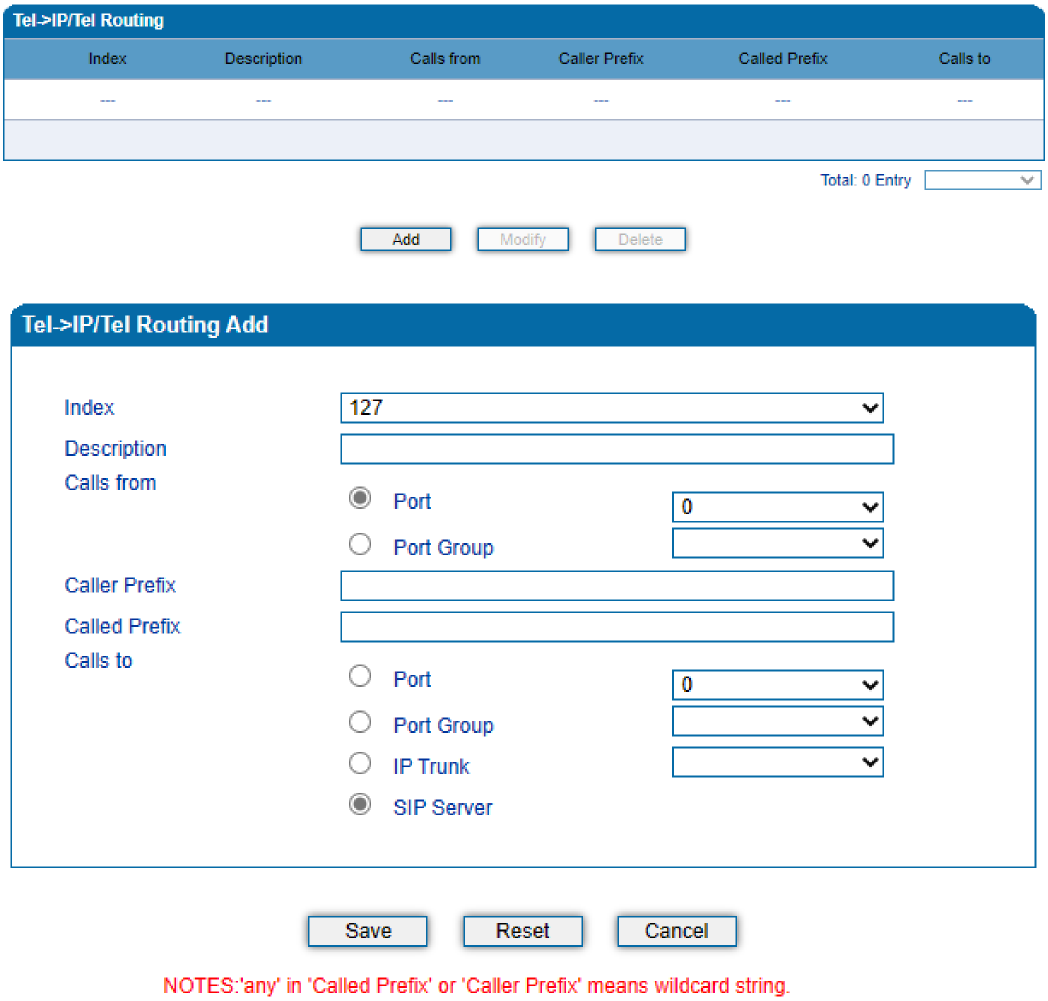


Table-Explanation of Tel →IP/Tel Route

Parameter	Explanation
Index	The index of this Tel →IP/Tel routing; range is from 0 to 127. Each index cannot be used repeatedly. Routing priority: 0 is the highest priority.
Description	The description of this Tel →IP/Tel routing; it is used to identify the routing.
Calls From	Choose calls are from a port or a port group
Caller Prefix	The prefix of the caller number, which helps match routing exactly. Its length is less than or equal to the caller number. For example, if caller number is 2001, the caller prefix can be 200 or 2. 'any' means the prefix matches any caller number.
Called Prefix	The prefix of the called number, which helps match routing exactly. Its length is less than or equal to the called number. If the called number is 008675526456659, the called prefix can be 0086755 or 00. "any" means the prefix matches any called number.
Calls to	Choose calls are routed to a port, port group, IP trunk or SIP server

Notes:

1) 0 means no limit

2) The call limit only affects the outgoing call from the FXO port

3) The day/month limit will be automatically reset when the NTP time synchronization is successful.

5.11.7 **Call Limit**

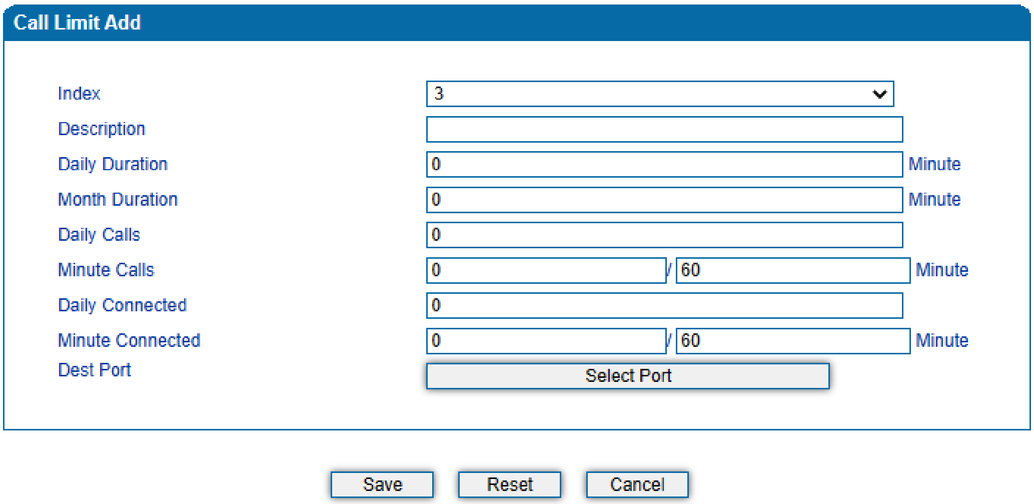


Table-Explanation of Call Limit

Parameter	**Explanation**
Index	The index of call limit.
Description	The description of this call limit; it is used to identify the limiting.
Daily Duration	The maximum duration of a daily call.
Month Duration	The maximum duration of a monthly call.
Daily Calls	The times of daily calls.
Minute Calls	The times of a minute calls.
Daily Connected	The times of daily connected calls.
Minute Connected	The times of mi connected calls. The times of calls made in minute.
Dest Port	Select the port that needs to be call limit.

5.12 Manipulation

Number manipulation refers to the change of a called number or a caller number during calling process when the called number or the caller number matches the existing rules.

5.12.1 IP → Tel Called

On the **IP → Tel Called submenu** page, you can set rules for manipulating the called number of IP → Tel calls.

Figure-Add IP →Tel Called Number Manipulation

Table-Explanation of Parameters for IP →Tel Called Number Manipulation

Parameter	Explanation
Index	The index of this manipulation; range is from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Description of this manipulation; it is used to identify this manipulation.
Calls From	Determine the calls come from IP trunk or SIP server
Caller Prefix	Set a prefix for caller number. The prefix’ s length is less than or equal to that of the caller number, which helps to match the caller number of this call. If caller number is 2001, the caller prefix can be 200 or 2. “any” means match any caller number.
Called Prefix	Set a prefix for called number. The prefix’ s length is less than or equal to called number, which helps to match the called number. If called number is 008675526456659, the called prefix can be 0086755 or 00. “any” means match any called number.
Calls to	Determine the call is routed to a port or a port group.
Stripped Digits from Left	The number of digits which are lessened from the left of the called number
Stripped Digits from Right	The number of digits which are lessened from the right of the called number
Prefix to Add	The prefix added to the called number after its digits are lessened.
Suffix to Add	The suffix added to the called number after its digits are lessened.

Number of Digits to Leave from Right	For an incoming call, reserved digits from callee number, starting count numbers from right of callee number.

5.12.2 Tel → IP/Tel Caller

On the **Tel → IP/Tel Caller** page, you can set rules for manipulating the caller number of Tel → IP/Tel calls.

Figure-Add Tel → IP/Tel Caller Number Manipulation

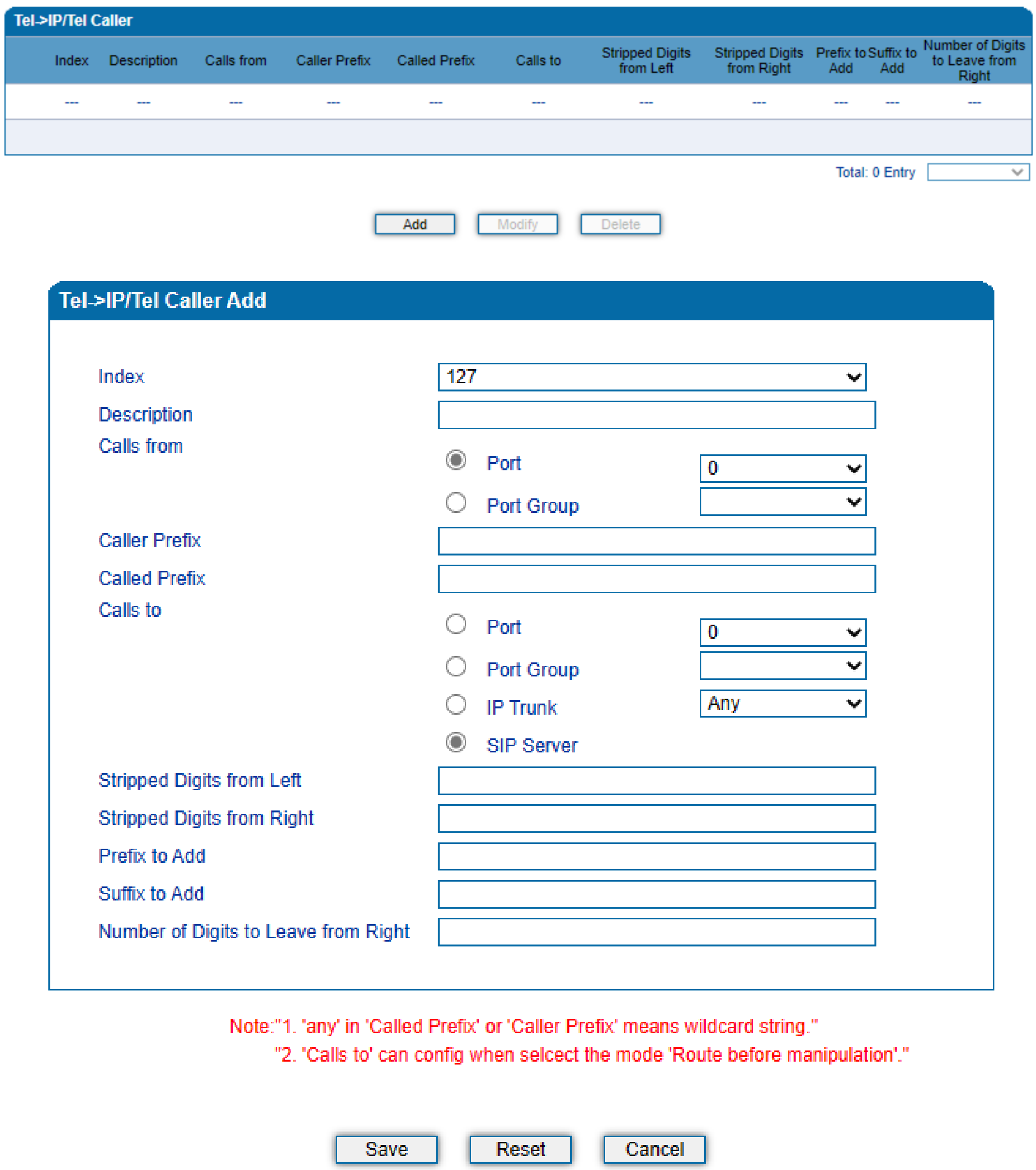


Table-Explanation of Parameters for IP →Tel Called Number Manipulation

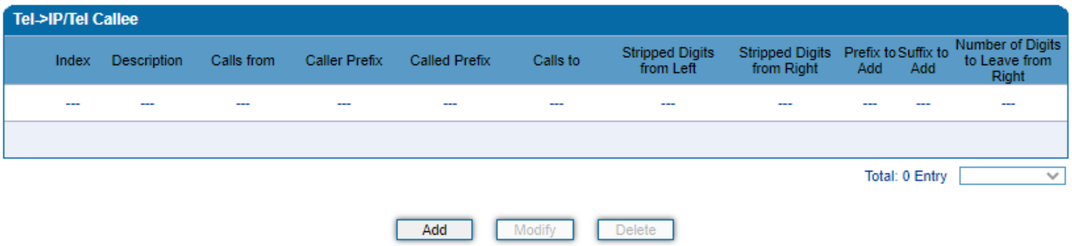
Parameter	Explanation
Index	The index of this manipulation; range is from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Description of this manipulation; it is used to identify this manipulation.
Calls From	Determine the calls come from a port or a port group.
Caller Prefix	Set a prefix for caller number. The prefix's length is less than or equal to that of the caller number, which helps to match the caller number of this call. If caller number is 2001, the caller prefix can be 200 or 2. 'any' means match any caller number.
Called Prefix	Set a prefix for called number. The prefix's length is less than or equal to called number, which helps to match the called number. If called number is 008675526456659, the called prefix can be 0086755 or 00. 'any' means match any called number.
Calls to	Determine the call is routed to a port, a port group, an IP Trunk or a SIP server.
Stripped Digits from Left	The number of digits which are lessened from the left of the caller number
Stripped Digits from Right	The number of digits which are lessened from the right of the caller number
Prefix to Add	The prefix added to the caller number after its digits are lessened.
Suffix to Add	The suffix added to the caller number after its digits are lessened.

Number of Digits to Leave from Right	For an incoming call, reserved digits from callee number, starting count numbers from right of callee number.

5.12.3 Tel → IP/Tel Called

On the **Tel → IP/Tel Called** page, you can set rules for manipulating the called number of Tel → IP/Tel calls.

Figure-Add Tel → IP/Tel Callee Number Manipulation



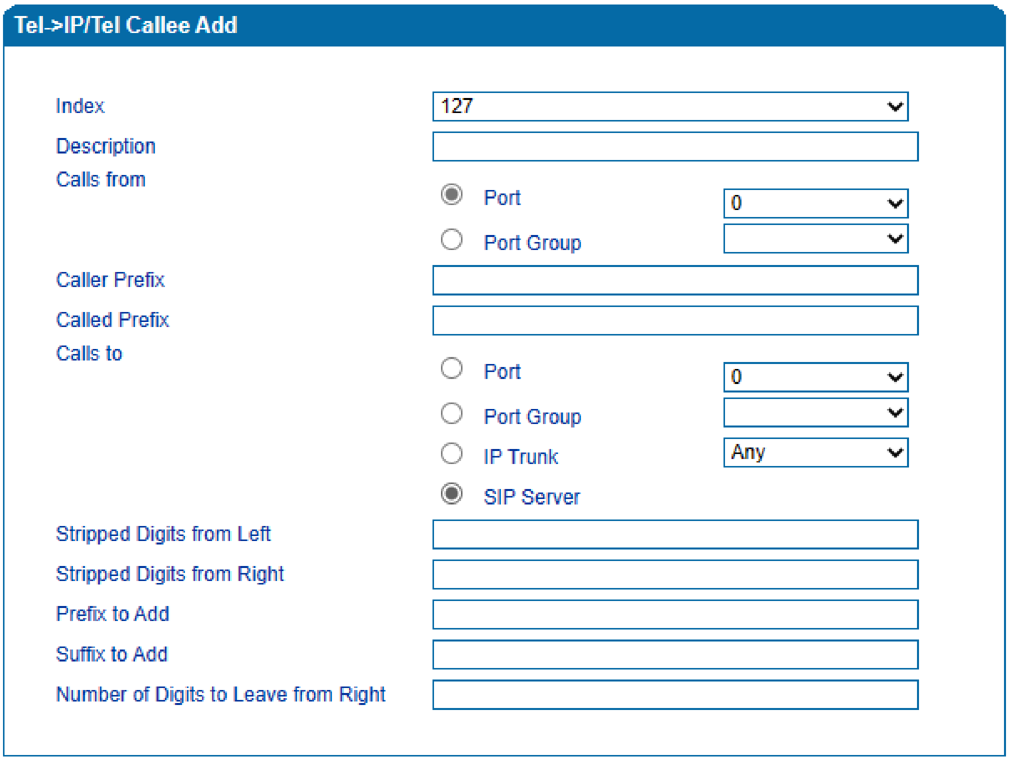


Table-Explanation of Parameters for Tel → IP/Tel Callee Number Manipulation

Parameter	Explanation
Index	The index of this manipulation; range is from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Description of this manipulation; it is used to identify this manipulation.
Calls From	Determine the calls come from a port or a port group.
Caller Prefix	Set a prefix for caller number. The prefix' s length is less than or equal to that of the caller number, which helps to match the caller number of this call. If caller number is 2001, the caller prefix can be 200 or 2. 'any' means match any caller number.
Called Prefix	Set a prefix for called number. The prefix' s length is less than or equal to called number, which helps to match the called number. If called number is 008675526456659, the called prefix can be 0086755 or 00. 'any' means match any called number.
Calls to	Determine the call is routed to a port, a port group, an IP trunk or a SIP server.
Stripped Digits from Left	The number of digits which are lessened from the left of the called number
Stripped Digits from Right	The number of digits which are lessened from the right of the called number.
Prefix to Add	The prefix added to the called number after its digits are lessened.
Suffix to Add	The suffix added to the called number after its digits are lessened.

Number of Digits to Leave from Right	For an incoming call, reserved digits from callee number, starting count numbers from right of callee number.

5.13 Management

5.13.1 TR069

TR069 is short for Technical Report 069, which provides a commonly-used framework and protocol for next-generation network devices. As an application-level protocol on top of IP TR069 has no limitation to access ways of network devices.

Under the network management model of TR069, ACS (Auto-Configuration Server) works as a management server, responsible for managing CPEs (Custom Premise Equipment).

ACS URL (auto-configuration server URL address) is provided by service provider. The ACS URL generally starts with http:// or https://

Username and password are used for ACS authentication.

Figure-Configure TR069 Parameter

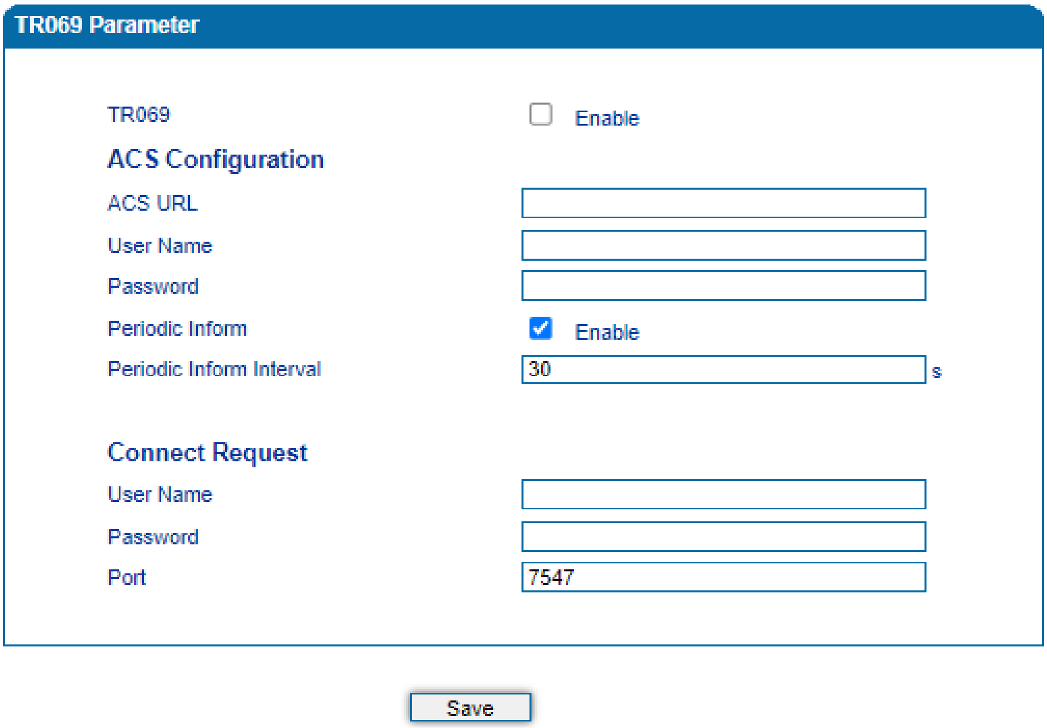


Table-Explanation of TR069 Parameters

Parameter	Explanation
TR069	Choose whether to enable TR069; it is ‘not enable’ by default.
ACS URL	The IP address or domain name of ACS, which is provided by service provider.
Username (ACS)	Username of ACS, which is provided by service provider.
Password (ACS)	Password of ACS, which is provided by service provider.
Periodic Inform	Choose whether to enable ‘Periodic Inform’ ; if it is enabled, ACS will connect to CPE every 30 seconds (if the interval is set as 30 seconds).
Periodic Inform Interval	The interval set for periodic connection between ACS and CPE.
Username (CPE)	Username of CPE
Password (CPE)	Password of CPE
Port	The port to connect CPE and ACS

5.13.2 SNMP

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been developed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

Figure-Configure SNMP Parameters

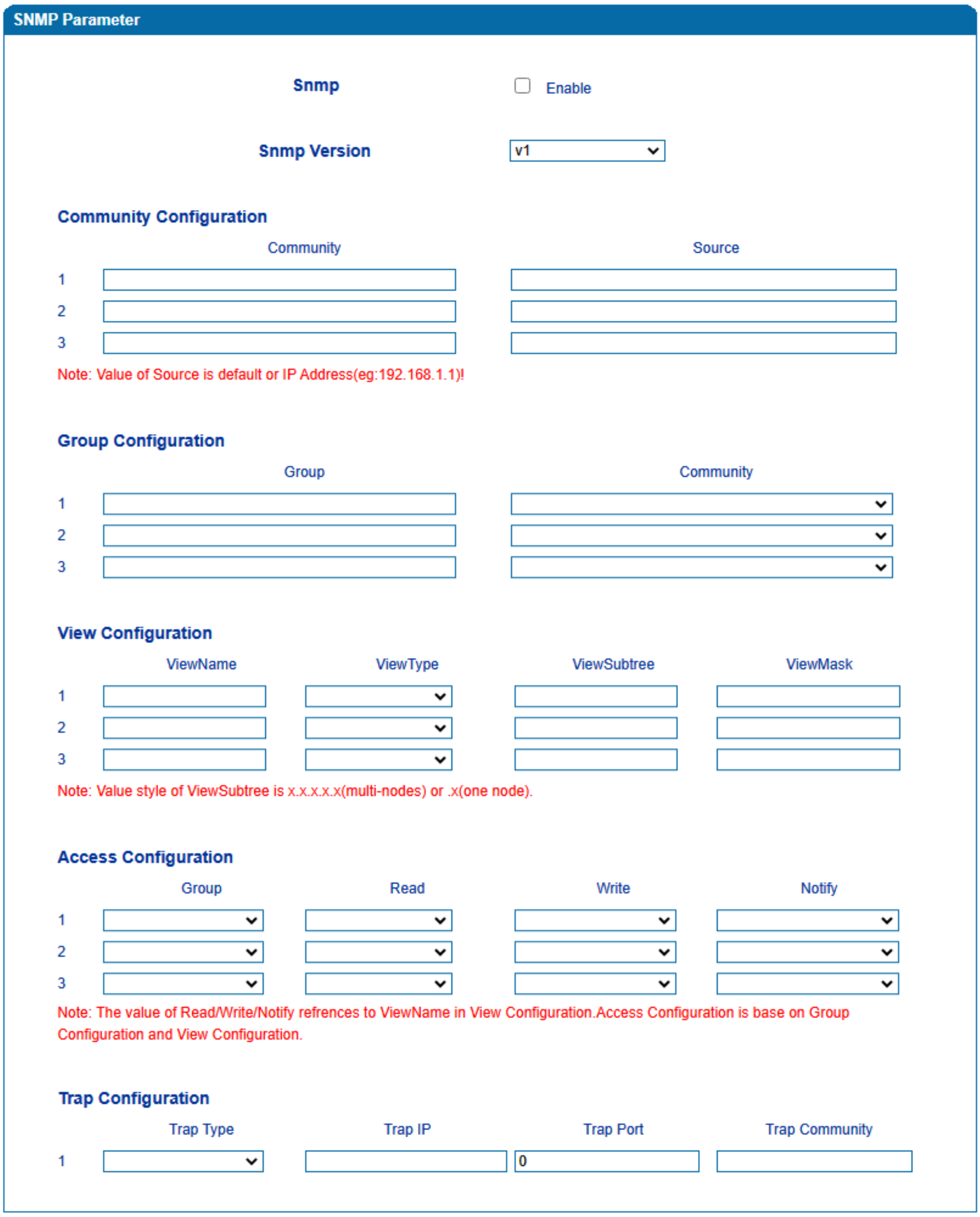


Table-Explanation of SNMP Parameters

Parameter	Explanation
SNMP	The device supports three versions of SNMP, namelyV1、V2C and V3.
Community Configuration	Community configuration exists in V1, V2C and V3. **Community:** fill in a community name used to read through SNMP protocol; it is a character string. **Source:** The IP address of SNMP server. SNMP server cannot identify the packets sent from the gateway unless the community configured in the gateway matches with the community configured in SNMP server.
Group Configuration	Group configuration exists in V1 and V2C and V3. **Group:** fill in a group name which is used to identify the group; it’s a character string. **Community:** fill in a community which means this community has joined in the group. In the following, access permission of read, write and notify is configured for each group.
View Configuration	View configuration exists in V1, V2C and V3. **ViewName:** fill in a view name which is used to identify this view. **ViewType:** choose ‘Included’ or ‘Excluded’. ‘Included’ means the view includes the OID of the corresponding ViewSubtree, while ‘Excluded’ means the OID of the corresponding ViewSubtree is excluded from this view. **ViewSubtree:** fill in the OID of the view subtree. **ViewMask:** it is used to withdraw a row of a table, such as an Ethernet port.

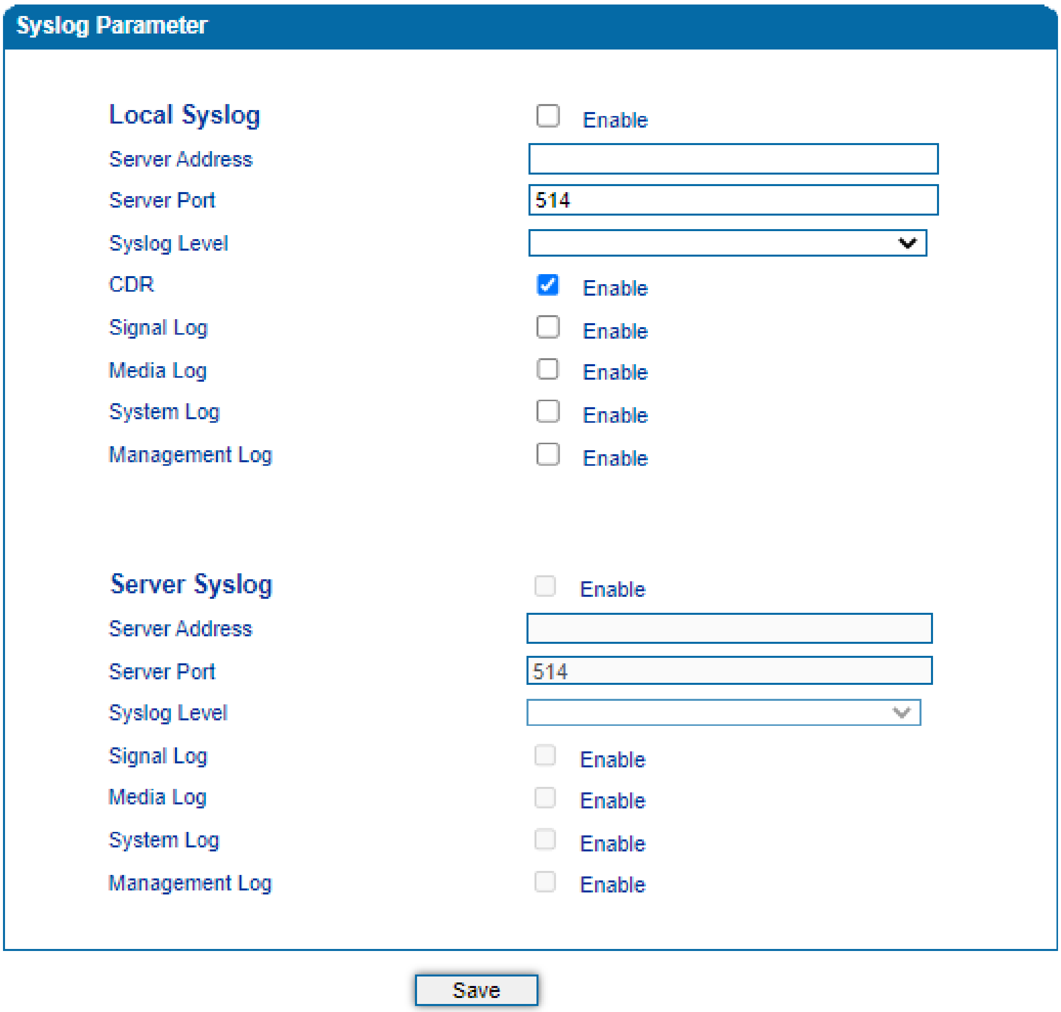
Access Configuration	Access configuration exists in V1, V2C and V3, under which permission of read, write or notify is configured for a community group. **Group:** choose a group name that has been configured. **Read:** Choose a 'read' view for the group. **Write:** Choose a 'write' view for the group. **Notify:** Choose a 'notify' view for the group.
Trap Configuration	Trap configuration exists in V1, V2C and V3, which is aimed to send trap alarm. **Trap Type:** Choose V1, V2C and Inform. **Trap IP:** the IP address of the destination SNMP server where trap alarm is sent. **Trap Port:** the port of the destination SNMP server, which will receive trap alarm. **Trap Community:** the community configured in the destination SNMP server.
User Configuration	User configuration exists in V3. When V3 transmits SNMP packets in an encryption way, this item needs to be configured. **User:** fill in a user name used to authenticate. **AuthType:** choose MD5 or SHA as authentication type. **AuthPassword:** the password used to authenticate. **Privacy Type:** Choose DES, AES or AES 128 as encryption type. **Privacy Password:** the encryption password.

5.13.3 **Syslog**

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores messages, and the software that reports and analyzes messages. It also provides a means to notify administrators of problems or performance.

Syslog levels include: EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO and DEBUG.

Figure-Configure Syslog Parameters



When the device registers to Cloud server, local syslog will be changed to non-configurable and all logs will be stored on the Cloud server.

5.13.4 **Provision**

Provision is used to make the device automatically upgrade with the latest firmware stored on an http server, a ftp server or a tftp server. Please refer to the Instruction for Using Provision.

Figure-Provision

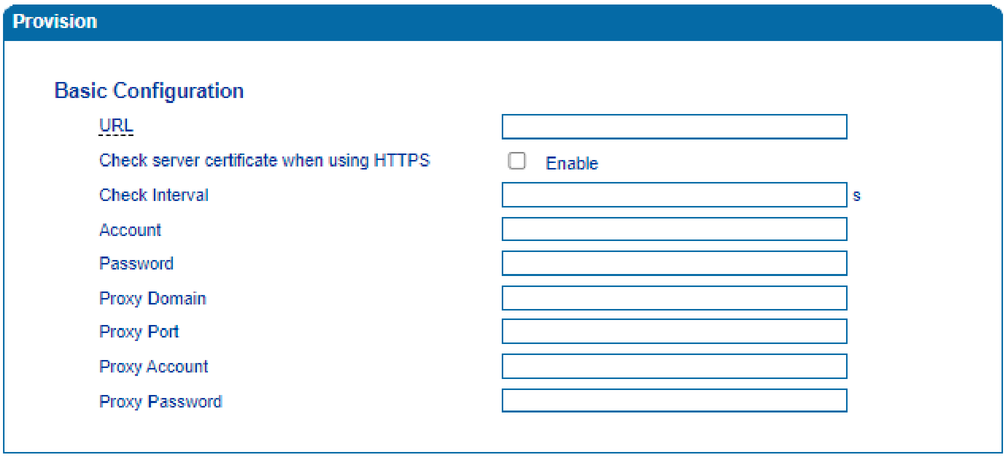


Table-Explanation of Provision Parameters

Parameter	**Explanation**
URL	URL of provisioning server, support HTTP, TFTP, FTP
Check server certificate when using HTTPS	Check server certificate when using HTTPS
Check Interval	The interval to check whether there is new firmware version on the provisioning server
Account	Account for logging in provisioning server
Password	Password for logging in provisioning server
Proxy Domain	Proxy Domain
Proxy Port	Proxy Port
Proxy Account	Proxy Account
Proxy Password	Proxy Password

5.13.5 Cloud server

You can register the device to cloud server, and then the device can be managed by the cloud server.

Figure-Configure Cloud Server

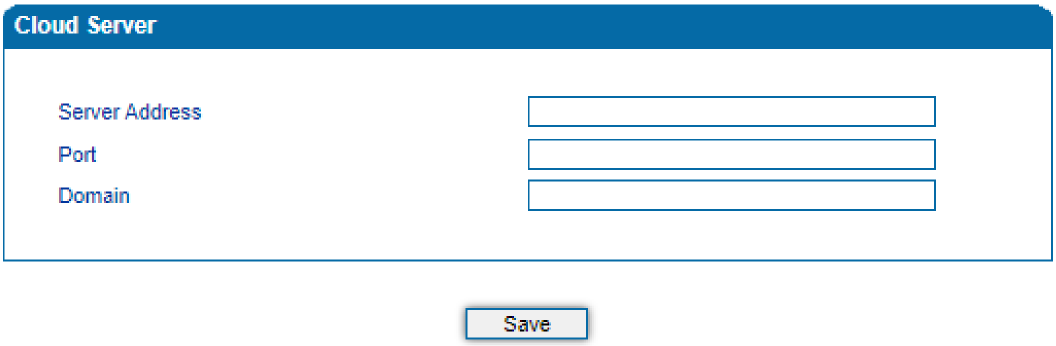


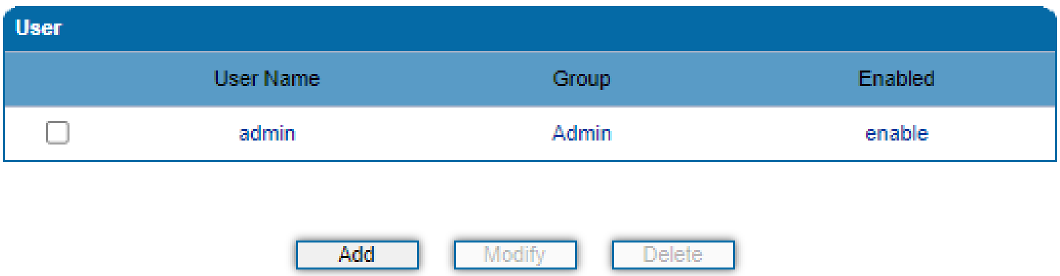
Table-Explanation of Parameters for Cloud Server

Parameter	Explanation
Server Address	The IP address of the cloud server
Port	The listening port of the cloud server
Domain	The domain name of the cloud server

5.13.6 User Manage

On the **Management → User Manage** page, the administrator of the device can classify users in different groups, and set login username and password for each user.

Figure-Modify Username and Password



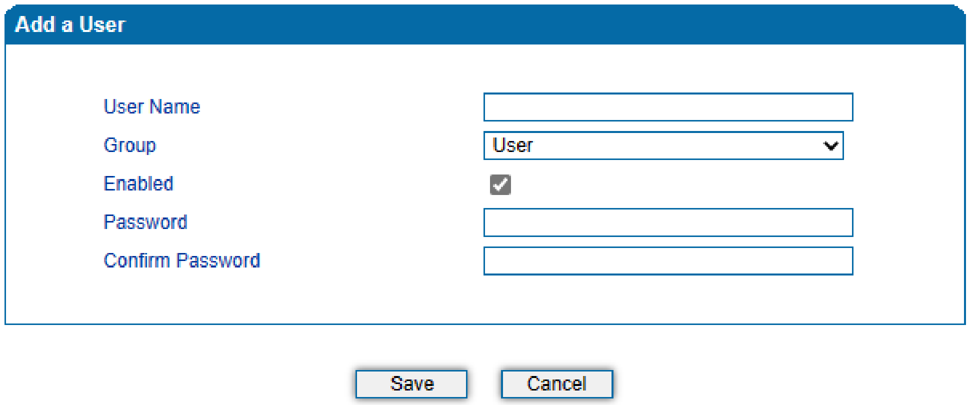


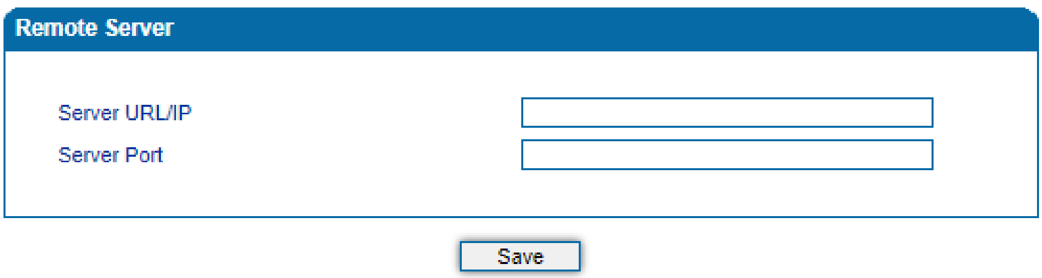
Table-Explanation of Parameters for adding a User

Parameter	Explanation
Username	Username
Group	Support User and Guest
Enabled	Enabled
Password	Password
Confirm Password	Confirm password

5.13.7 Remote Server

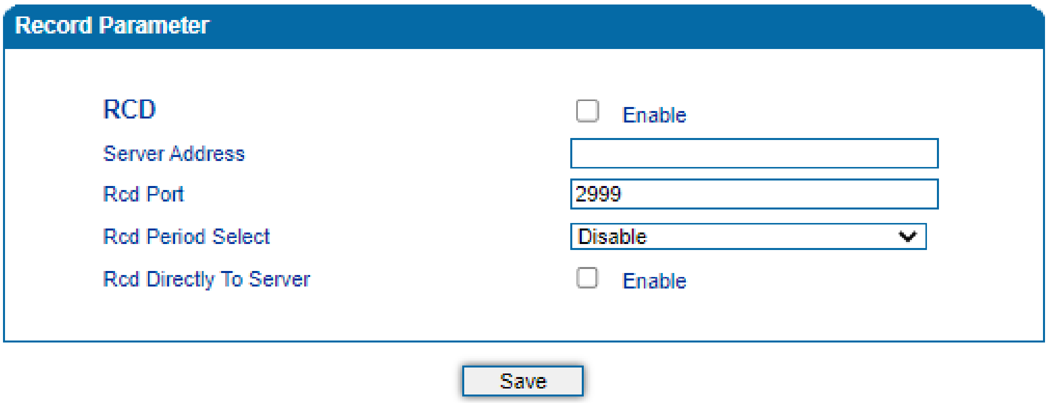
In case that you need remote technical support, technical support engineers can connect your device with a service server on the **Management →Remote Server** page, so as to better help you to solve problems.

Figure-Configure Remote Server



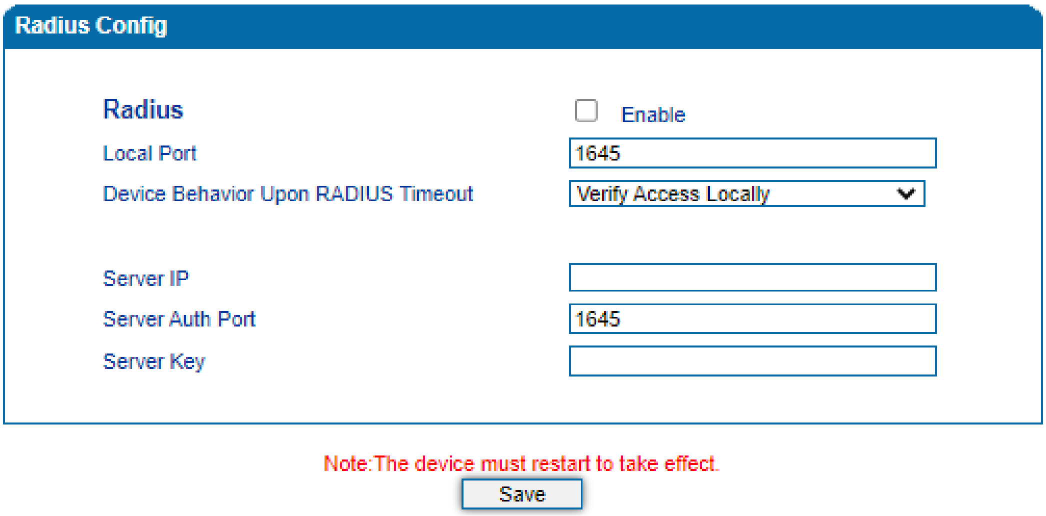
Parameter	Explanation
Server URL/IP	Server URL/IP
Server Port	Server Port

5.13.8 Record Parameter



Parameter	Explanation
RCD	Enable or disable the recording function
Server Address	Set recording server address, and support IP address or domain name
Rcd Port	Set the recording server port, the default is 2999
Rcd Period Select	Support setting 3 recording time periods, the recording function will be enabled within the time period.
Rcd Directly To Server	Recording can be sent directly to the server in a NAT environment.

5.13.9 Radius Parameter



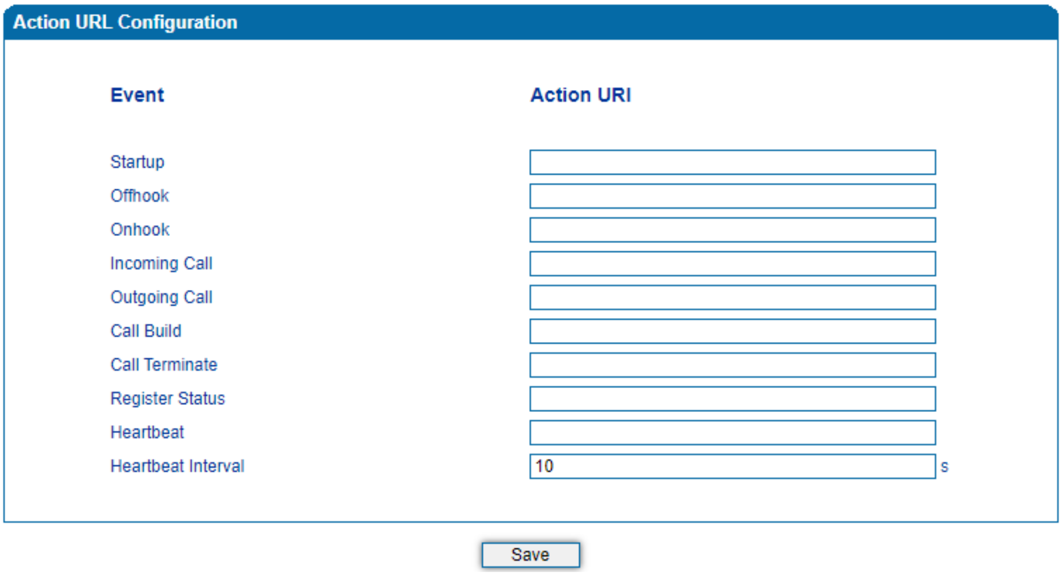
Parameter	Explanation
Radius	Enable or disable Radius
Local Port	Port of the local Radius client
Device Behavior Upon RADIUS Timeout	Support Verify Access Locally and Deny Access.
Server IP	IP address of the Radius server
Server Auth Port	Authentication port of Radius server
Server Key	The authentication key for the Radius server

5.13.10 Action URL

Action URL is a means of allowing VoIP platform/VoIP server to learn about the statuses of the device. This is realized by GET request over the HTTP protocol. During the transmission of status, some data (such as device ID, mac address, called/caller number, IP address) carried in GET request can also be reported to VoIP platform/VoIP server.

The data that can be carried in GET request, please refer to the notes on the **Management → Action URL** page.

Figure-Configure Action URL



Event: Statuses of device, which will be reported to VoIP platform/VoIP server.

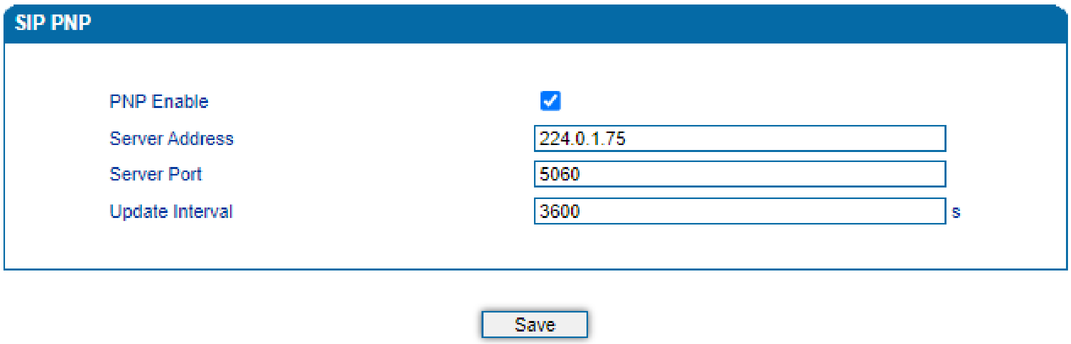
Action URL: for example, http://host:port/file.php?macaddr=$mac, among which 'host' means the HTTP server's IP address or domain name, 'port' means the http server's listening port, 'file.php' means the script that will process this request, and '$mac' means the parameter carried in the request when this request is sent out.

Heartbeat: heartbeat packets are sent to URL by the device, used to examine the connection between the device and HTTP/HTTP server.

5.13.11 SIP PNP

Gateway can restore or upgrade the system firmware by SIP PNP method. The process of SIP PNP is follow:

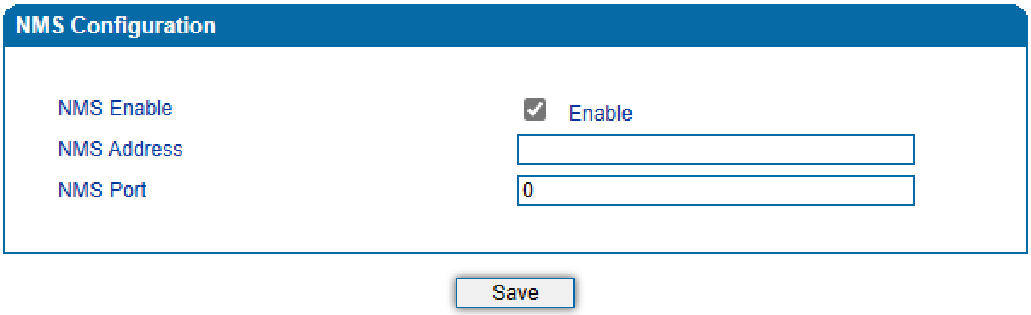
- Gateway reproducibly send SIP subscribe requests to broadcast.
- Once, the gateway received Notify message from a server and get a URL.
- Gateway sends the request to the URL, then start provision for restore or upgrade



Parameter	Explanation
PNP Enable	Enable or disable PNP
Server Address	The IP address of the SIP PNP server, and the default is 224.0.1.75
Server Port	Port of the SIP PNP server, and the default is 5060
Update Interval	Send subscription messages periodically, and the default is 3600s

5.13.12 NMS Configuration

Network Management System (NMS) is an easy-to-use and centralized tool to manage, monitor and troubleshoot of all the devices including Gateways, IP Phones, IP PBXs, Session Border Controllers, and SIP Intercoms. With device management, alarm system, service management, log management, report management and statistical analysis, it allows enterprises and service providers to centrally and easily deploy and manage a large network of devices.



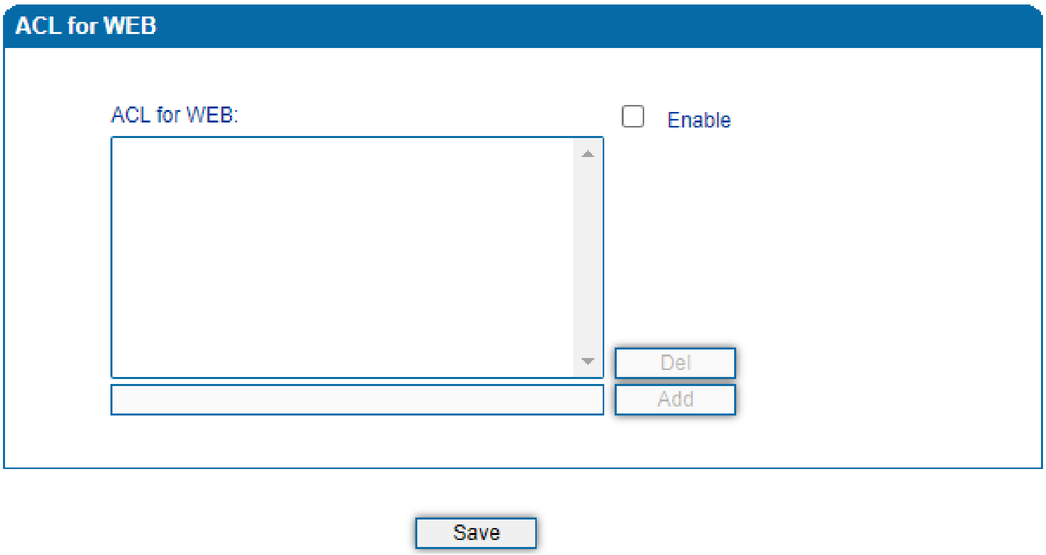
Parameter	Explanation
NMS Enable	Enable NMS
NMS Address	IP address or domain address of the NMS server
NMS Port	Port of the NMS server, the default is 0

5.14 Security

5.14.1 WEB ACL

ACL (Access Control List) for Web is used to configure IP addresses that are allowed to access the Web Interface of the device. The IP address list can’t be null once ACL is enabled.

Figure-Add IP Address to Web ACL

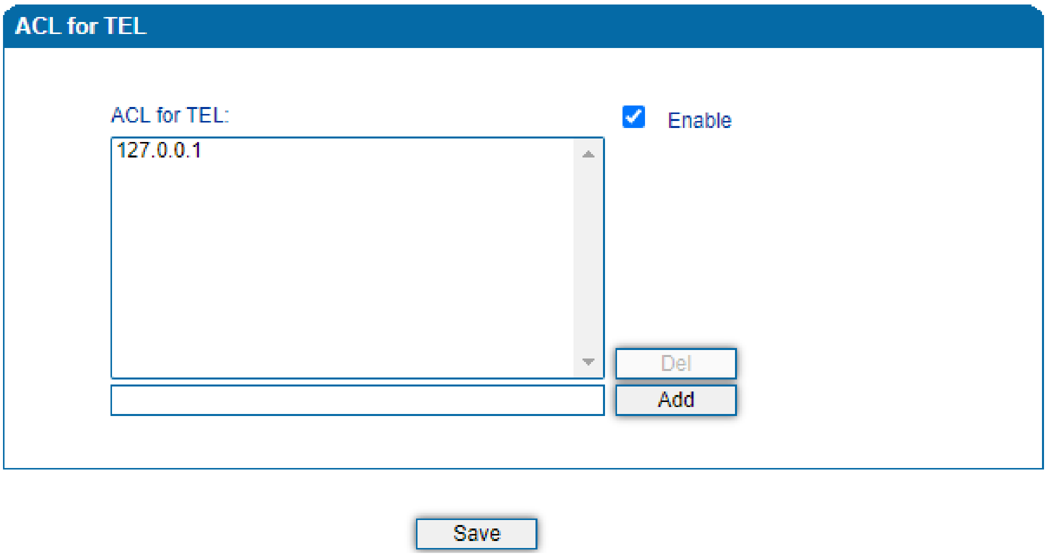


Parameter	Explanation
ACL for WEB	ACL for WEB
Del	Delete IP address
Add	Add IP address

5.14.2 Telnet ACL

ACL (Access Control List) for Telnet is used to configure IP addresses that are allowed to access the Telnet Interface of the device. The IP address list can’ t be null once ACL is enabled.

Figure-Add IP Address to Telnet ACL



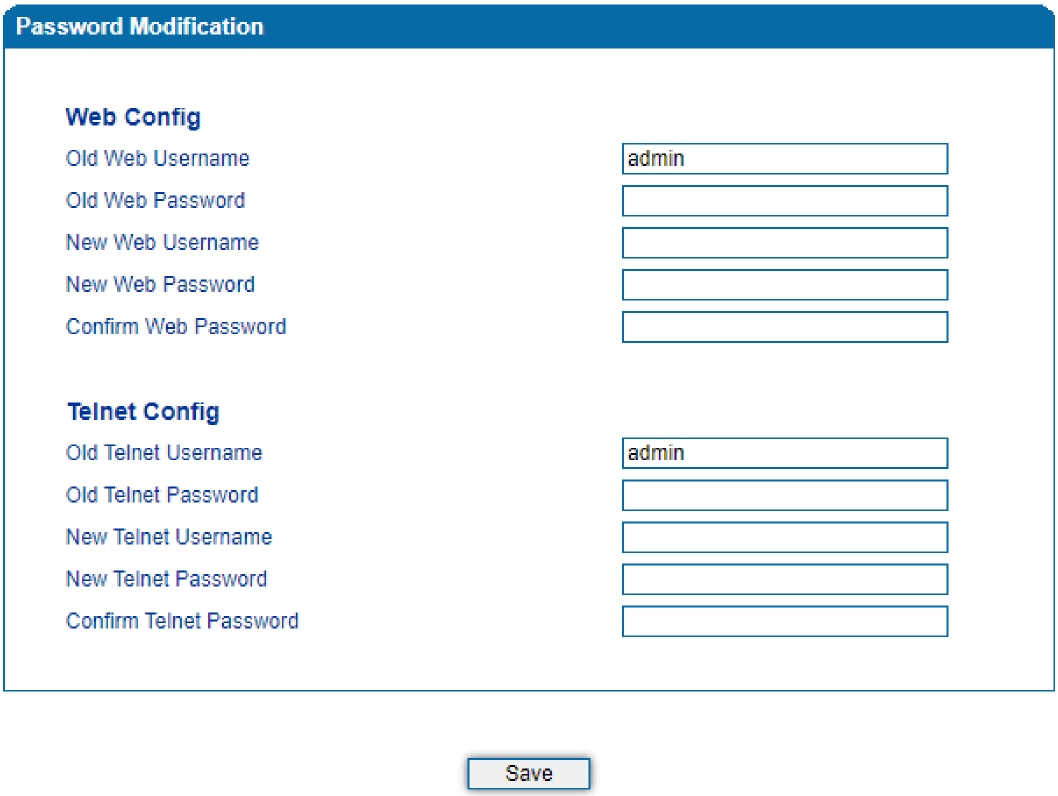
Parameter	Explanation
ACL for TEL	ACL for Telnet
Del	Delete IP address
Add	Add IP address

5.14.3 **Passwords**

You can configure or modify the username and password for logging in the Web interface and the Telnet interface of the device on this page.

Note: Both the username and password of Web and Telnet are 'admin' and 'admin' by default. It is advised to modify username and password for security consideration.

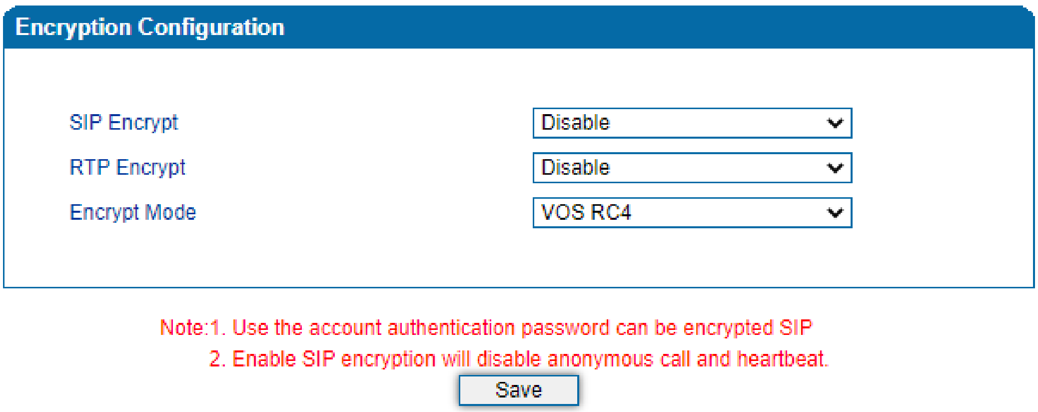
Figure-Modify Username and Password



5.14.4 Encrypt

When the device is registered to a VOS softswitch, you can encrypt SIP and RTP for the VOS softswitch.

Figure-Encrypt SIP and RTP



Note: If SIP encryption is enabled, heartbeat and anonymous calls should be disabled.

5.15 Tools

5.15.1 Firmware Upload

On the **Tools → Firmware** Upload page, you can upload a new firmware version from a local folder.

Figure-Upload Firmware

Steps of Firmware Uploading:

Step 1. Check the current firmware version on the **Status & Statistics →System Information** page.

Step 2. Prepare firmware package.

Step 3. Upload firmware, select the package from a specific folder on the computer and click the **Upload** button.

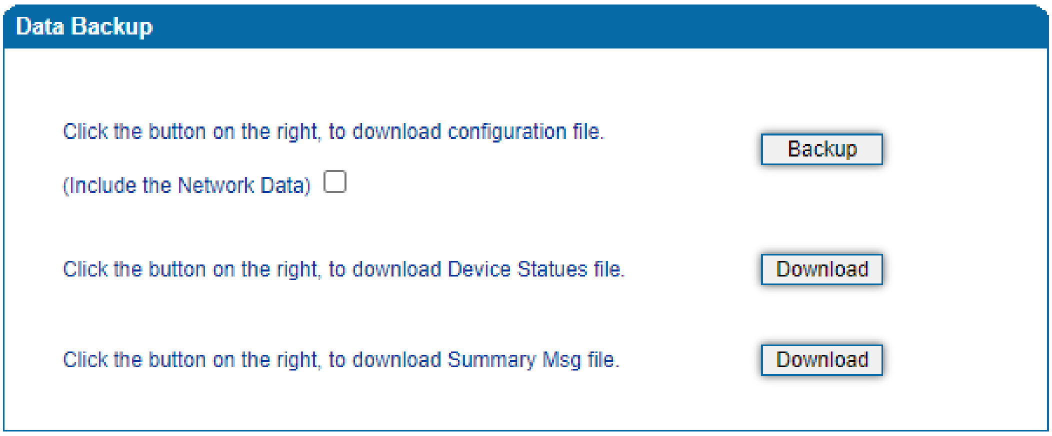
Step 4. Keep waiting until it prompts ‘Software loaded successfully!’

Step 5. Reboot the device on the **Tools → Device Restart** page.

5.15.2 **Data Backup**

On the **Tools → Data Backup** page, you can download and backup configuration data, device status and summary messages on local computer.

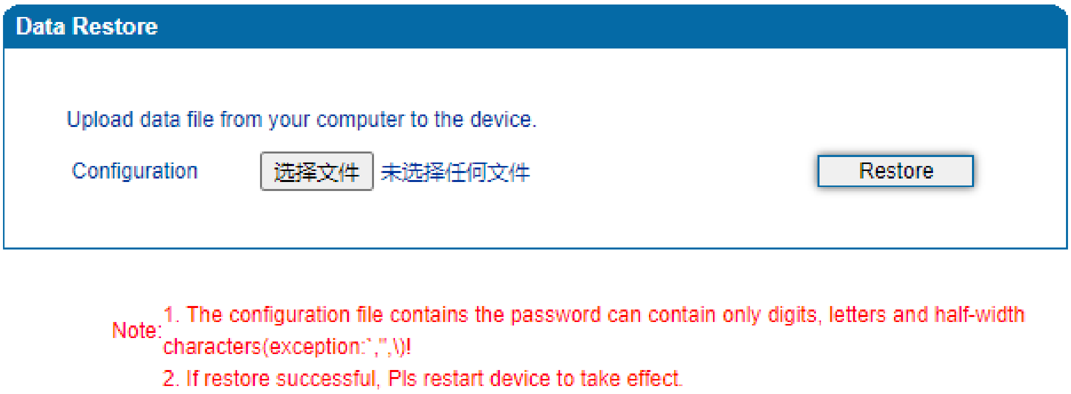
Figure-Backup Data



5.15.3 **Data Restore**

On the **Tools → Data Restore** page, you can restore configuration data through uploading a data file from local computer. The restored configurations will take effect after the device is restarted.

Figure-Restore Data



5.15.4 **FXO Test**

FXO test consists of two parts: Impedance Test and Auto-detect Busy Tone.

- **Impedance Test**

The impedance test of FXO port means the technical staff can match the impedance of the FXO port. The tested port must be online.

Figure-Impedance Test

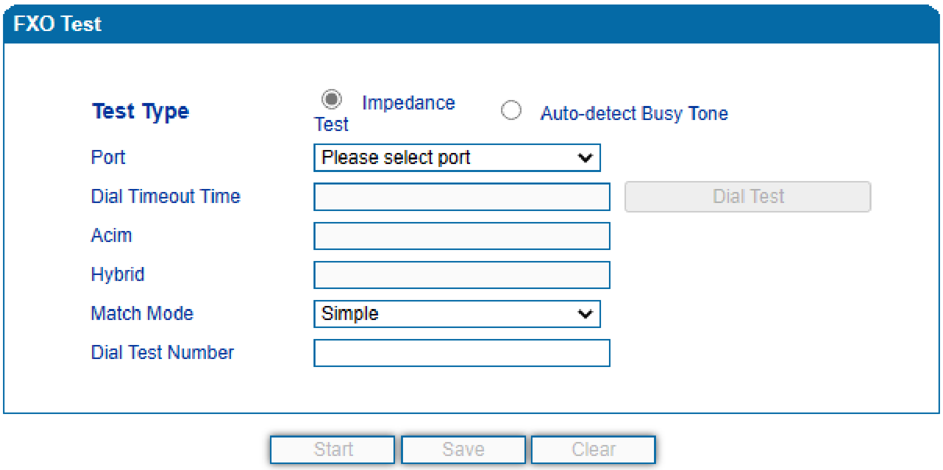


Table-Explanation of Parameters for Impedance Test

Parameter	Explanation
Test Type	Choose a type to test
Port	Choose a port to test
Dial Timeout Time	Set the dialing timeout time. If you are not sure, you can also perform a "Dial Test" first (go to step 2 for details)
Acim	Display the current impedance value of the FXO port (displayed value, cannot be modified)
Hybrid	Display the current hybrid parameters of the FXO port (displayed value, cannot be modified)
Match Mode	Match mode: Simple, Standard and Exact (The higher the mode, the higher the accuracy and the longer it takes).
Dial Test Number	Fill in the test number

Steps of impedance test:

1) Go to Tools> FXO Test> Impedance Test

2) Fill in the dial timeout time (if you don't know the dial timeout time, you can perform the dial timeout test first (about 10 seconds), after selecting the online port to be tested, click "Dial test", and the timeout time will be displayed after the test is completed)

3) Select the match mode, test port, and test number, etc., and click "Start" (different modes, time and accuracy are also different, the simple mode is about 15 minutes, the standard mode is about 30 minutes, and the exact mode is about 45 minutes);

4) After the test is completed, the Acim and Hybrid values will be displayed.

Notes:

1) The dial test number can be configured by itself, but it cannot be the same as the service number.

2) If you do not click to save the result, after restarting, the dialing timeout time, dialing test number and impedance value will be invalid.

3) Please do not leave this page before the test is completed to avoid errors.

- **Auto-detect Busy Tone**

Busy tone detection can only select the online port. The testing steps are as follows:

Figure-Auto-detect Busy Tone

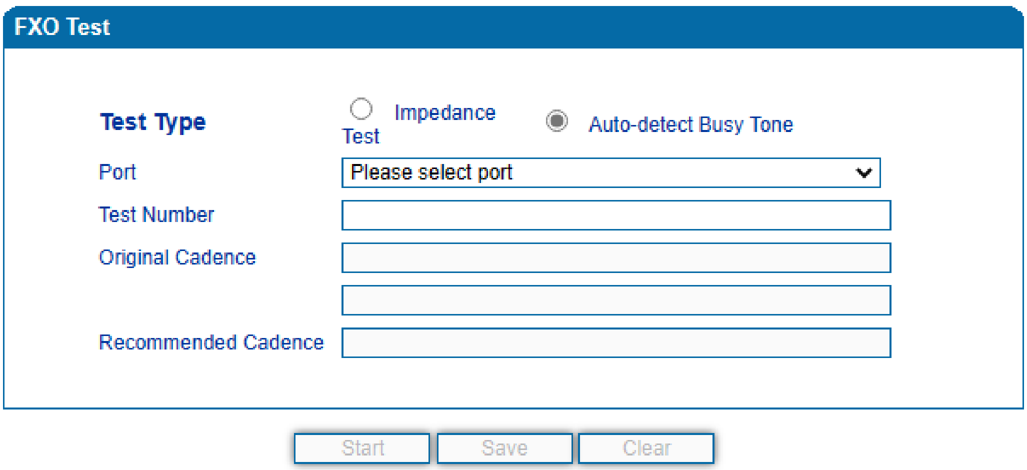


Table-Explanation of Parameters for Auto-detect Busy Tone

Parameter	Explanation
Test Type	Choose a type to test
Port	Choose a port to test
Test Number	The destination number for busy tone detection (see step 2 for details)
Original Cadence	The original busy tone cadence captured during the detection
Recommended Cadence	Recommended busy tone cadence after detection

Steps of Auto-detect Busy Tone:

1) Navigate to Tools > FXO Test > Auto-detect Busy Tone

2) Select the online port to be tested and fill in the test number (Make sure that the busy tone service has opened for this number. Its advised to use a PSTN line to connect telephone for test. If this parameter is null, it means no number is dialed)

3) Click 'Start', it will take about 1 minute, please do not leave this page

4) After the test is completed, the original cadence and recommended cadence are displayed, Please save the result after finishing, otherwise you can clear the results and retest.

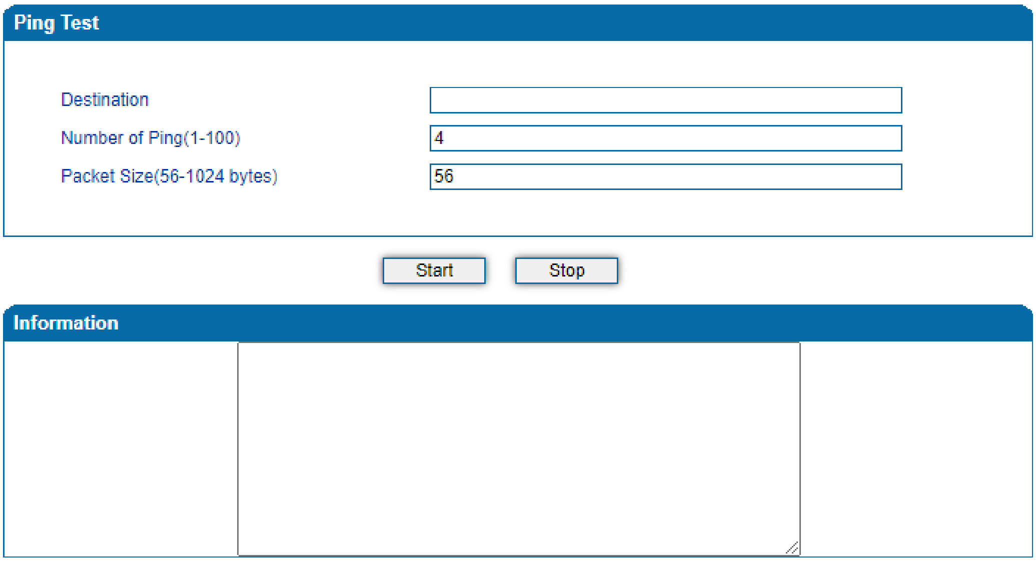
5.15.5 Ping Test

Ping is used to examine whether a network works as normal through sending test packets and calculating response time.

Instructions for using Ping:

1. Enter the IP address or domain name of a network, a website or a device in the input box of Ping, and then click **Start**.
2. If related messages are received, it means the network connection works as normal; otherwise, the network connection is down.

Figure-Execute Ping Test



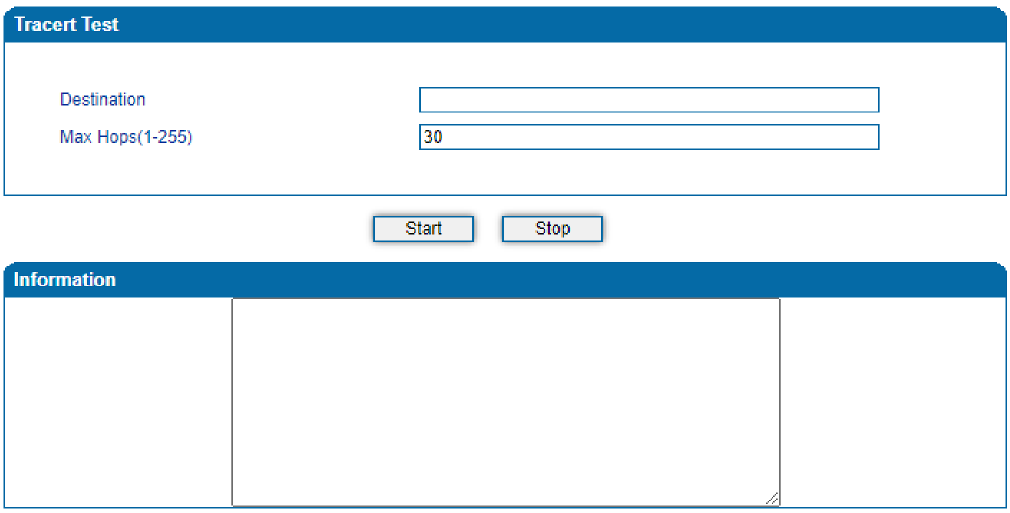
5.15.6 **Tracert Test**

Tracert is short for traceroute, used to track a route from one IP address to another.

Instruction for using Traceroute:

1. Enter the IP address or domain name of a destination device in the input box of Traceroute, and then click **Start**.

Figure-Execute Tracert Test



Destination: the IP address or domain name of a destination device that needs to be tracked.

Max Hops: the maximum hops for searching the above IP address or domain name. For example, if ‘max hops’ is set as 30, and the configured IP address or domain name cannot be reached within 30 hops, it’ s thought that the IP address or domain name cannot be searched.

2. View the route information from the returned message.

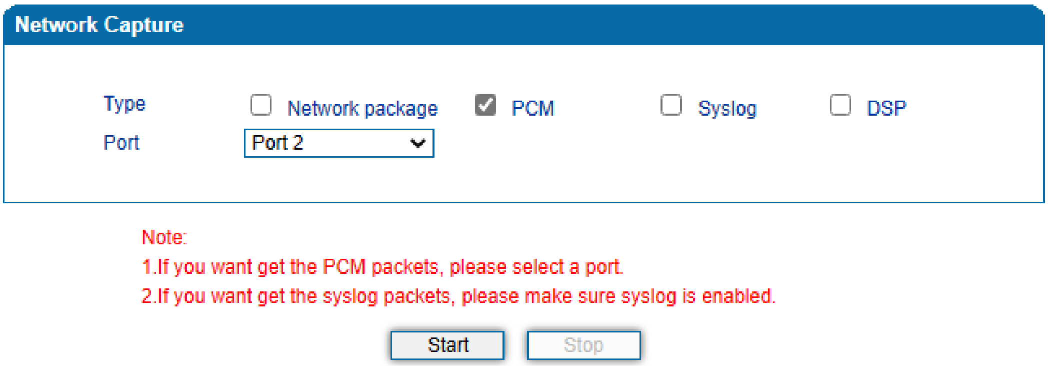
5.15.7 Network Capture

Network capture is an important diagnostics tool for maintenance. It is used to capture data packages of the available network ports.

PCM Capture:

PCM capture helps to analysis voice stream between analog phone and DSP chipset.

Figure-Capture PCM Packages



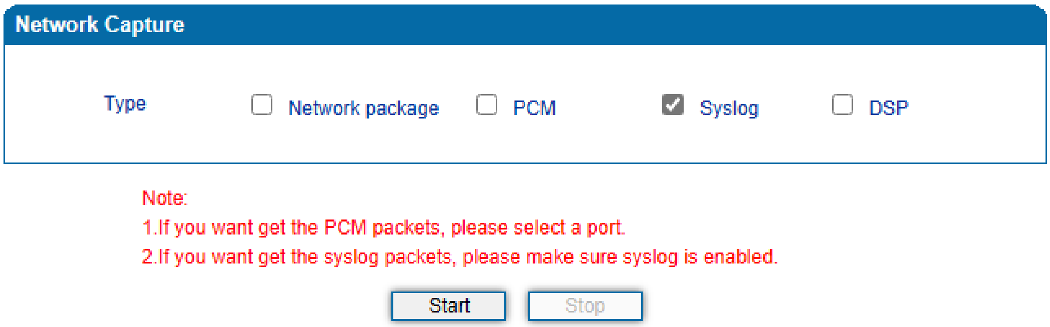
- Click “*Start*’ to enable PCM capture
- Dialing out through the device, start talking a short while then hang up the call.
- Click ‘*Stop*’ to disable network capture
- Save the file to local computer

The captured package is named ‘capture(x).pcap’. x is the serial number of the capturing and will be added 1 in next time.

Syslog Capture:

Syslog capture is another way to obtain syslog which is the same as remote syslog server and file log. The captured file is saved as pcap format so that it can be opened in some of capturing software like Wireshark, Ethereal software etc.

Figure-Capture Syslog Packages



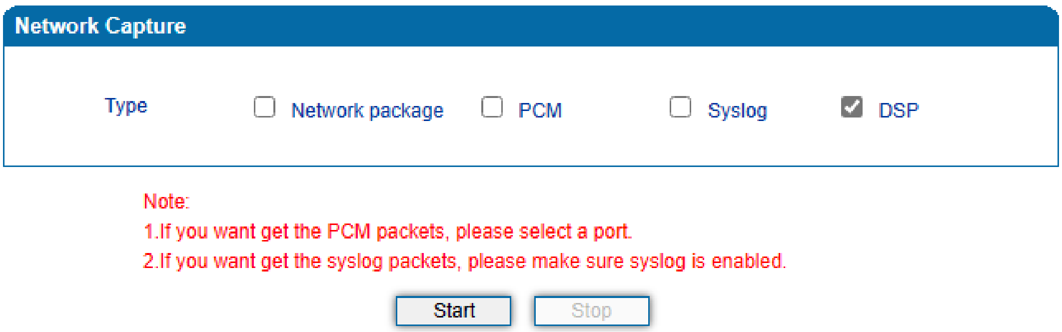
- Click “Start’ to enable syslog capture
- Dialing out through the device, start talking a short while then hang up the call.
- Click ‘Stop’ to disable syslog capture
- Save the capture to local computer

The capture package is named ‘capture(x).pcap’ . x is the serial number of capturing and will be added 1 in next time.

DSP Capture:

DSP capture helps to analyze voice stream inside DSP chipset. The DSP chipset will handle RTP from IP network as well as voice stream from analog phone.

Figure-Capture DSP Packages



- Click Start to enable DSP capture

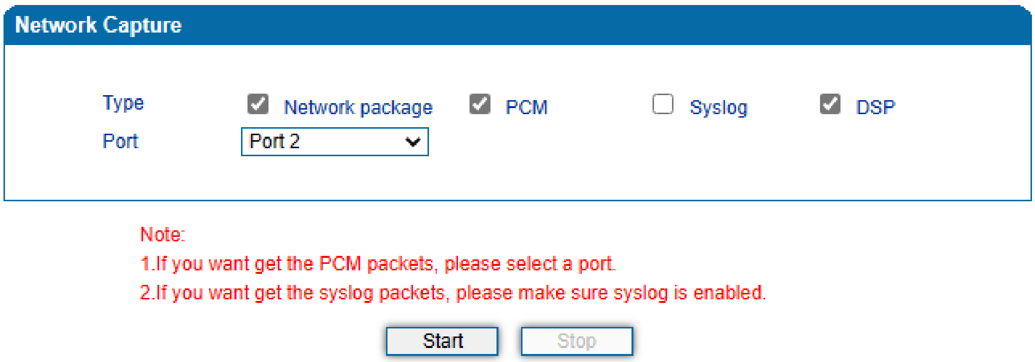
- Dialing out through the device, start talking a short while then hang up the call.
- Click Stop to disable DSP capture
- Save the capture to local computer

The captured package is named 'capture(x).pcap' . x is the serial number of the capturing and will be added 1 in next time.

Customized Capture:

This menu provides more options to capture specific packages according to actual needs.

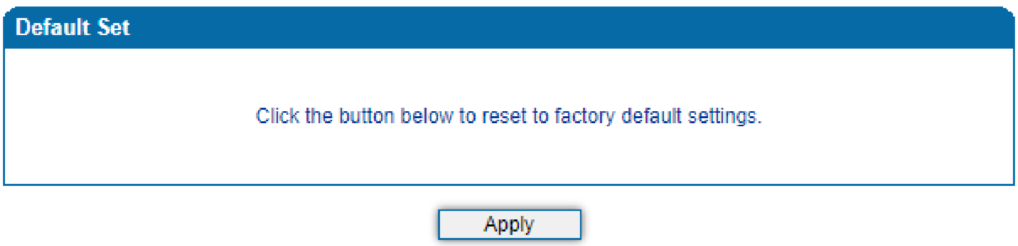
Figure-Customized Capturing



5.15.8 Factory Reset

Click 'Apply' to restore configurations of the device to the factory default settings.

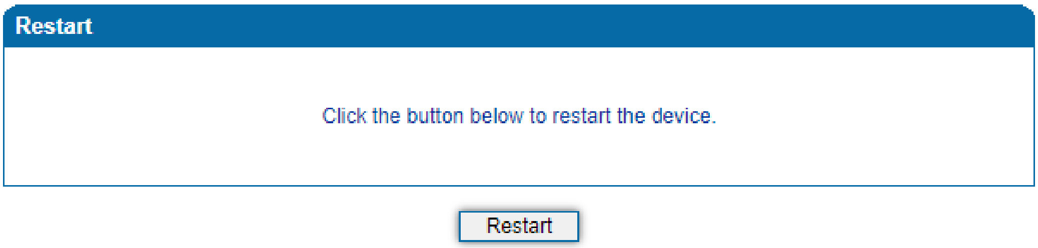
Figure-Reset Device to Factory Default Setting



5.15.9 Device Restart

If some parameters are changed, you are required to restart the device for the configurations or changes to take effect.

Figure-Restart Device



6 Glossary

Abbr.	Full Name
ARP	Address Resolution Protocol
CID	Caller Identity
DNS	Domain Name System
DND	Do NOT Disturb
DTMF	DTMF：Dual Tone Multi Frequency
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DDNS	Dynamic Domain Name Server
DSP	Digital Signal Process
NTP	Network Time Protocol
PPPOE	Point-to-point Protocol over Ethernet
PSTN	Public Switched Telephone Network
PCM	Pulse Code Modulation
QoS	Quality of Service
VLAN	Virtual Local Area Network
SIP	Session Initiation Protocol
STUN	Simple Traversal of UDP over NAT

SNMP	Simple Network Management Protocol
RTP	Real Time Protocol
UDP	User Datagram Protocol