PLANET
Networking & Communication

User's Manual

4-Port SIP VoIP Gateway

► VGW-420FO

www.PLANET.com.tw

Copyright

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If User finds information in this manual that is incorrect, misleading, or incomplete, we would appreciate User comments and suggestions.

CE Mark Warning

This is a class B device. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the DC-plug or push the hardware Power Switch to OFF position to disconnect the device from the power circuit.

Without removing the DC-plug or switching off the device, the device will still consume power from the power circuit. In view of Saving the Energy and reducing the unnecessary power consumption, it is strongly suggested to switch off or remove the DC-plug from the device if this device is not intended to be active.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, their respective companies claim these designations as trademarks or registered trademarks.

Revision

User's Manual of 4- SIP VoIP Gateway

Model: VGW-420FO

Rev: 1.0 (2025, March)

Part No. EM-VGW-420FO_v1.0

Preface

Welcome

Thanks for choosing **VGW-420FO SIP VoIP Gateway.** We hope you will make optimum use of this flexible, feature-rich VoIP-to-FXO gateway. Please read this document carefully before installing the gateway.

About this manual

This manual provides information about the introduction of the gateway, and about how to install, configure or use the gateway.

For interoperability with different IPPBX/Softswitch platforms, you can refer to relevant configuration guide to different systems.

This manual is written with reference to the default configurations of the **VGW-420FO SIP VoIP Gateway**.

Intended audience

This manual is aimed primarily at network and system engineers, who will install, configure and maintain the gateway.

System engineers are persons who customize the configurations to meet the requirements of users.

Parts of the document containing description of telephony features are aimed at users who are the persons who will actually use the gateway

Contents

1 Introduction of VGW-420FO

1.1 Overview

High-performance VoIP Gateway

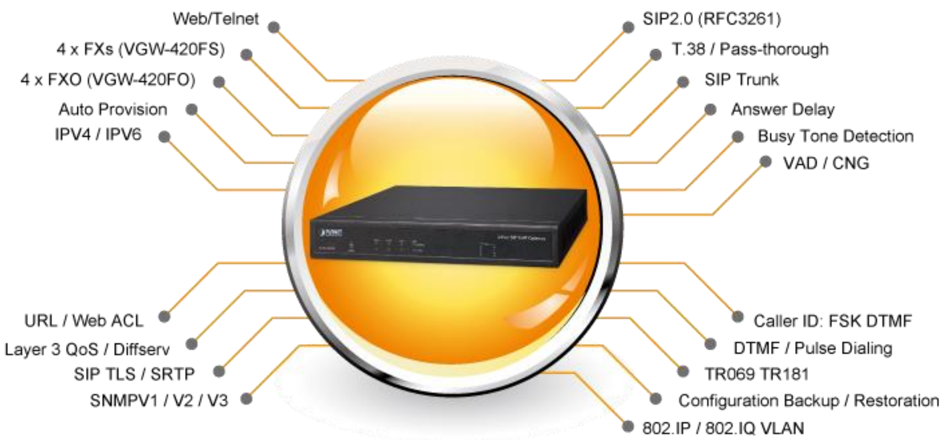
To build high-performance VoIP communications at a low cost, PLANET has launched the latest VoIP gateway model, the VGW-420FO enterprise-class 4-port SIP VoIP Gateway. The VGW-420FO gateway provides added flexibility during migration to Unified Communications by supporting the traditional analog devices. For example, the remote workers can dial in through a Unified VoIP Communication System just like an extension call but no long-distance call charge would occur. It also allows call to be transferred to anyone at any location within the voice system, which enables the enterprise to communicate more effectively and is helpful to streamline business processes.

VoIP Protocol Standard Compliance

The VGW-420FO supports Session Initiation Protocol 2.0 (RFC 3261) for easy integration with general voice over IP system. The VGW-420FO is able to broadly interoperate with equipment provided by VoIP infrastructure providers, thus enabling them to provide their customers with better multi-media exchange services.

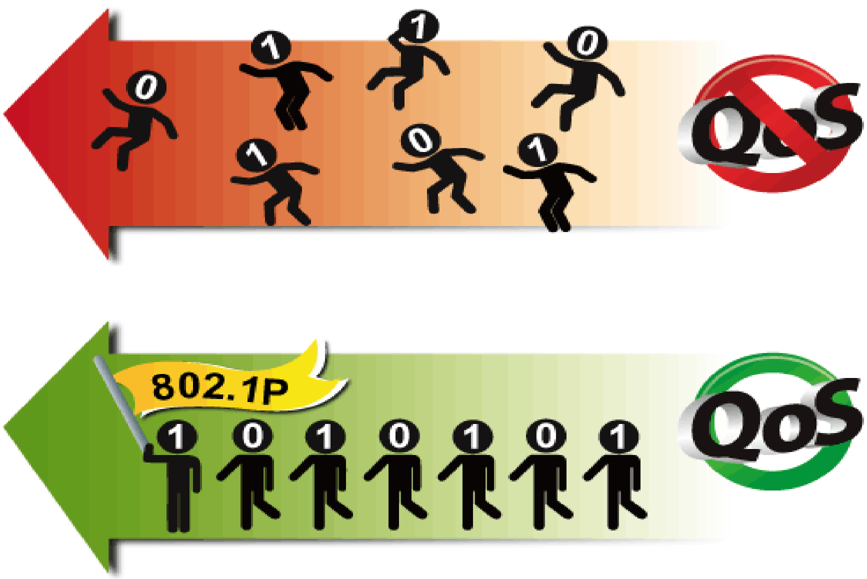
Enhanced, Full-Featured Business Gateway

The VGW-420FO is a full-featured enhanced business SIP Gateway that addresses the communication needs of the enterprises. It provides the 4-line FXO gateway with SIP protocol IP device which allows connection with 4 analog PSTN telephone lines set to make or receive VoIP call over Internet or VPN network. This VGW-420FO is suitable for office PABX to enable to have VoIP call without changing cabling, dial plan and extension number. The VGW-420FO supports all kinds of SIP-based gateway features and multiple contact filter functions, such as 4 SIP trunk accounts, both IPv6 and IPv4 protocols, flexible dial plan and route plan features, and switch analog and VoIP signal, to help both protocols to communicate.



Secure, High-quality VoIP Communication

The VGW-420FO effortlessly delivers secured toll voice quality by utilizing cutting-edge 802.1p QoS (Quality of Service), 802.1Q VLAN tagging, and IP ToS (Type of Service) technology. Using voice and data, VLAN can easily separate the data and voice, thus maintaining the best quality.



Caller ID Function

Both the FXO and FXS ports of the VGW-420 series (VGW-420FO/VGW-420FS) support caller ID function, help user identify calling number easily and verify number. It also helps to block anonymous call by filtering strange calls. The FXS port transmits Caller ID, while the FXO port receives Caller ID. The Caller ID interoperates with analog phones, public switched telephone networks (PSTN) and private branch exchanges (PBXs).

1.2 Product Features

- **Highlights**
  - Full SIP 2.0 compliance (RFC3261)
  - IPv6 and IPv4 protocols
  - Up to 32 SIP service domains
  - Caller ID
  - Auto HTTP provisioning and fax over IP
  - Flexible Route Plan, Dial Plan and SIP Trunk

- **Internet Features**
  - SNMP v1/v2c/v3
  - VLAN 802.1P and 802.1Q
  - Layer 3 QoS and DiffServ
  - STUN (RFC 3489) and Outbound Proxy
  - TR069 and auto provisioning
  - TLS/SRTP security

- **SIP Applications**
  - IETF SIP RFC3261 based on UDP/TCP/TLS
  - 4-line FXO connecting to PSTN line
  - Fax over T.38 and pass-through
  - ITU-T G.711 A-law, G.711 μ-law, G.723.1 and G.729 voice coding
  - In-band/out of band DTMF (RFC2833/SIP INFO)
  - Echo cancellation exceeding ITU-T G.168, up to 128ms tail length
  - SIP trunk
  - Caller ID: DTMF/FSK support

- **Call Features**
  - Call waiting/transfer (Blind transfer, Attend transfer)
  - Call hold/quick pick
  - Call forwarding unconditional
  - Call forwarding on no reply
  - Hotline/speed dial/direct IP call
  - Do Not Disturb (DND)/three-way conferencing

- **FXO Line Configuration**
  - Line ID/line phone number
  - Reverse polarity detection or generation for call establish and billing
  - VoIP dial to FXO/PSTN line
  - Outgoing SIP caller ID selection

- **Routing Plan**
  - Prefix match and length
  - Priority/Cycle/Simultaneous Ring

1.3 Function Specifications

Product	VGW-420FO
Hardware	
WAN	1 x 10/100BASE-TX RJ45 port
LAN	2 x 10/100BASE-TX RJ45 port
Voice	4 x RJ11 connection (4 x FXO)
Weight	853g
Dimensions (W x D x H)	242 x 152 x 35 mm
Power Requirements	100-240VAC, 50-60 Hz@ DC 12V 2A
Power Consumption	12W
Protocols and Standard	
FXO	Dial Mode: DTMF/Pulse Dialing Caller ID: FSK, DTMF Reverse Polarity Answer Delay Busy Tone Detection No Current Detection
Voice & Fax	G.711A/U law, G.723.1, G.729A/B, G.726 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 T.38/Pass-through Modem/POS DTMF mode: Signal/RFC2833/INBAND VLAN 802.1P/802.1Q Layer3 QoS and DiffServ

VoIP	Protocol: SIP v2.0 (UDP/TCP), RFC3261, SDP, cRTP (RFC2833), RFC3262, 3263, 3264, 3265, 3515, 2976, 3311 SIP TLS/SRTP RTP/RTCP, RFC2198, 1889 RFC4028 Session Timer RFC3266 IPv6 in SDP RFC2806 TEL URI RFC3581 NAT, rport Outbound Proxy DNS SRV/A Query/NATPR Query SIP Trunk Early Media/Early Answer NAT: STUN, Static/Dynamic NAT
Network	Static/Dynamic IP PPPoE DHCP Client IPv4/IPv6 TCP, UDP, TFTP, FTP, ARP,RARP, Ping, NTP, SNTP, HTTP/HTTPS, DNS Ping/Tracert DHCP Option 66,120,121 OpenVPN
Software Features	Port Group Web ACL Telnet ACL Action URL Digitmap Routing Rules based Prefixes Caller/Called Number Manipulation Speed Dial
Management	SNMP v1/v2c/v3

	TR069, TR181 Auto Provisioning Web/Telnet Configuration Backup/Restore Firmware Upgrade via Web CDR Syslog Network Capture NTP/Daylight Saving Time IVR Local Maintenance
Environments	
Operating Temperature	0 ~ 50 degrees C
Storage Temperature	-20 ~ 80 degrees C
Operating Humidity	10%~90% relative humidity, non-condensing
Emission	CE, FCC

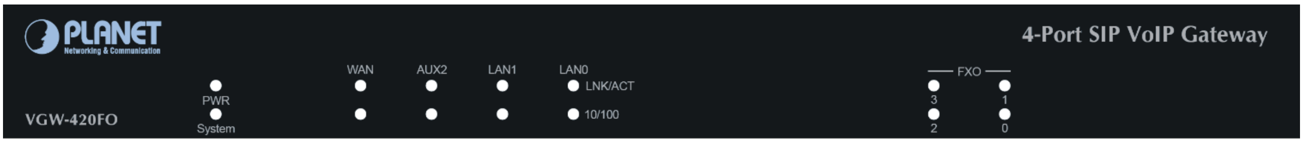
1.4 Ports and Connectors

The FXO analog gateway is available in the following configurations:

Model	Voice Channels	FXO Ports	Physical Port Labels
VGW-420FO	4	4	0-3

1.4.1 VGW-420FO

- **Front Panel**



■ LED Definition

- **System**

LED	Color	Function
PWR	**Green**	Lights to indicate the VoIP Gateway has power.
System	**Green**	Blinks to indicate the system is working.

■ RJ11 & 10/100BASE-TX Interfaces

LED	Color	Function	
FXO 0-3	Green	**Off:**	To indicate the FXO port is idle or faulty.
		On:	To indicate FXO port is currently working.
LAN 0-1 LNK/ACT	Green	**On:**	To indicate the port has link at 10/100Mbps.
		Blinks:	To indicate the port is actively sending or receiving data.
LAN 0-1 10/100	Amber	**Off:**	To indicate the port is working at 10Mbps.
		On:	To indicate the port is working at 100Mbps.
WAN LNK/ACT	Green	**On:**	To indicate the port has link at 10/100Mbps.
		Blinks:	To indicate the port is actively sending or receiving data.
WAN 10/100	Amber	**Off:**	To indicate the port is working at 10Mbps.
		On:	To indicate the port is working at 100Mbps.

■ Rear Panel

Port Name	**Connector**	**Description**
Power Jack	Power Jack	To connect DC 12V power supply.
WAN/LAN Port	RJ45	To connect to the IP network over a DSL modem or router or a LAN switch.
FXO Ports 0-3	RJ11	FXS ports to connect standard analog phone or fax machine or a PBX.

2 Basic Operations

2.1 Call Out and Call In via FXO Port

2.1.1 Call Out

One-stage Dialing: When the gateway receives a call from a softswitch or IPPBX, it checks the dialed number against the **Digit Map** settings (configured under *Advanced > Digit Map*). If there's a match, the system automatically selects an available FXO port based on the defined **port selection rules**, and the call is placed to the PSTN without user interaction.

Two-stage Dialing: In this method, the user first dials the FXO port's assigned SIP account number from an IPPBX extension. Once connected, a **dial tone** is heard, allowing the user to manually dial any desired PSTN number. This provides flexibility when routing through a specific FXO port or in scenarios requiring manual number entry.

2.1.2 Call In

When a caller dials the PSTN number connected to an FXO port on the gateway, they will hear either a **dial tone** or a **voice prompt** such as "Please dial the extension number."
The caller can then enter the desired extension or telephone number. Once dialing is complete, the gateway forwards the call to the appropriate IP server (e.g., softswitch or IPPBX) for routing.

Hotline auto-dialing: In this mode, when a caller dials the PSTN number linked to an FXO port, the gateway automatically routes the call to a **predefined extension or telephone number** without requiring user input. This is ideal for applications like hotline services, auto attendants, or direct-to-agent scenarios.

2.2 Description of Feature Codes

The VGW-420FO provides convenient telephone functions. Connect a telephone to the port and dial a specific feature code, and you can query corresponding information.

Feature Codes	Corresponding Function
***158#**	Dial *158# to inquire the IP address of LAN port.
***159#**	Dial *159# to inquire the IP address of WAN port.
***114#**	Dial *114# to query the phone number of an FXO port.
***115#**	Dial *115# to query the phone number of an FXO port group.
***168#**	Dial *168# to query the register status of an 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 to factory defaults.
***111#**	Dial *111# to restart the gateway.

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.

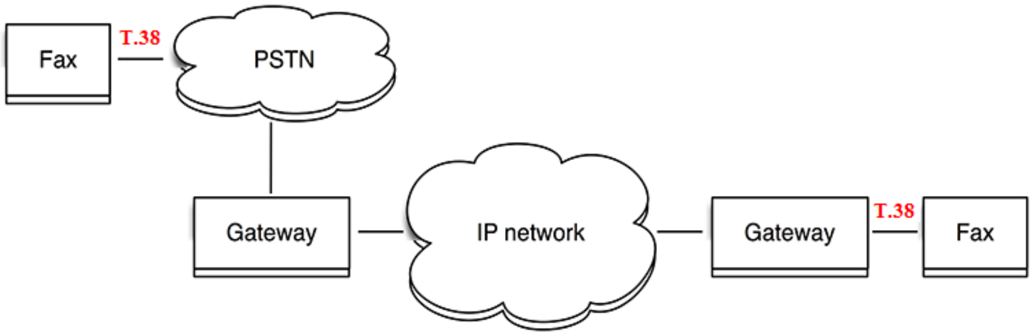
2.3 Sending and Receiving Fax

The VGW-420FO gateway supports four fax modes:

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

2.3.1 T. 38 and Pass-through

T.38: T.38 is an ITU recommendation for allowing transmission of fax over IP networks in real time. In 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. In the T.38 mode, fax traffic is carried in T.38 packages.



Pass-through: In 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.

2.4 Local IVR Operation

2.4.1 Inquire IP address

Connect a PSTN line to one of the FXO ports of the VGW-420FO, 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.

2.4.2 Factory Reset

Pick up the phone, and then dial *166*000000#. After hearing a voice prompt of 'setting successfully', hang up the phone and the gateway is reset to factory defaults.

2.4.3 Configure LAN Port's IP Address

Before configuration, please ensure:

- The VGW-420FO gateway is power on.
- Device has been connected to network.
- Telephone is connected to FXO port of the VGW-420FO.

Configure dynamic IP address by DHCP:

Pick up the phone, dial *150*2# and then hang up the phone.
If the voice prompt indicates 'setting successfully', please restart the VGW-420FO gateway after 10 seconds.

Configure static IP address:

Take the configuration of IP address '172.16.0.100' for an example.

Pick up the phone, dial *150*1# and then hang up the phone. Then configure IP address and mask as follows:

- Configure IP address
  Pick up the phone, dial *152*172*16*0*100# and then hang up the phone.
- Configure subnet mask
  Pick up the phone, dial *153*255*255*0*0# and then hang up the phone.
- Configure gateway IP address
  Pick up the phone, dial *156*172*16*0*1# and then hang up the phone.
- Query the IP address of the VGW-X20FS Series gateway:
  Pick up the phone, dial *158#.

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

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

3 Configurations on Web Interface

3.1 Logging in Web Interface

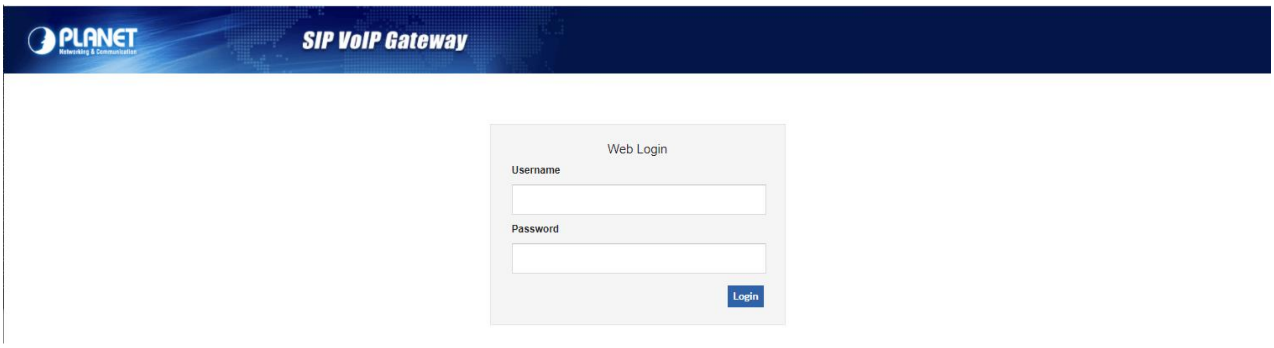
The VGW-420FO is easy to install by following the steps below.

Step 1：Connect a computer to a **LAN port** on the VGW-420FO. Your PC must be set to 192.168.0.X, the same domain as that of the VGW-420FO.

Step 2：Start a web browser. To use the user interface, you need a PC with Google Chrome, Microsoft Edge or Mozilla Firefox, or Safari (for Mac).

Step 3：Enter the default IP address of the VGW-420FO: **http://192.168.0.1** into the URL address box.

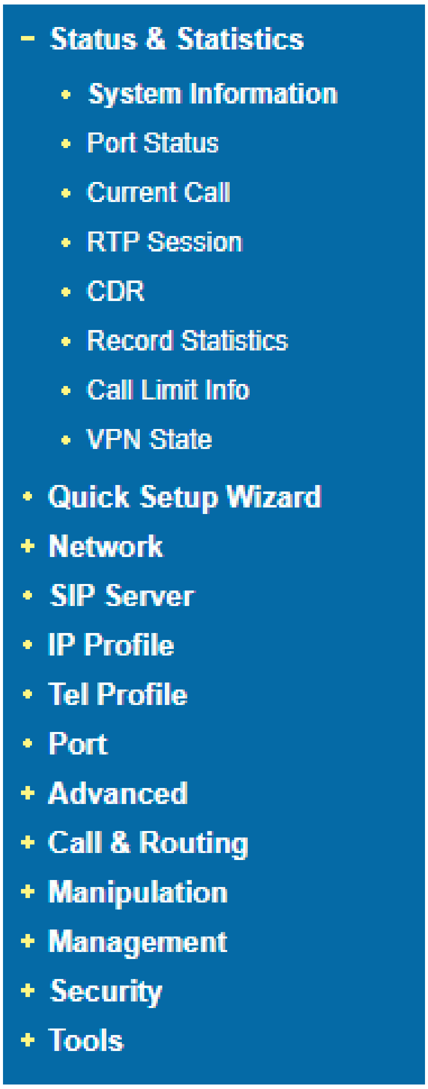
Step 4：Enter the default user name **admin** and the default password **admin**, and then click Login to enter Web-based user interface.



3.2 Navigation Tree

The web management system of the VGW-420FO gateway consists of the navigation tree and detailed configuration interfaces.

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



3.3 State and Statistics

3.3.1 System Information

On the System Information interface, you can view the information of device ID, MAC address, network mode, IP addresses, version information, sever register status and so on.

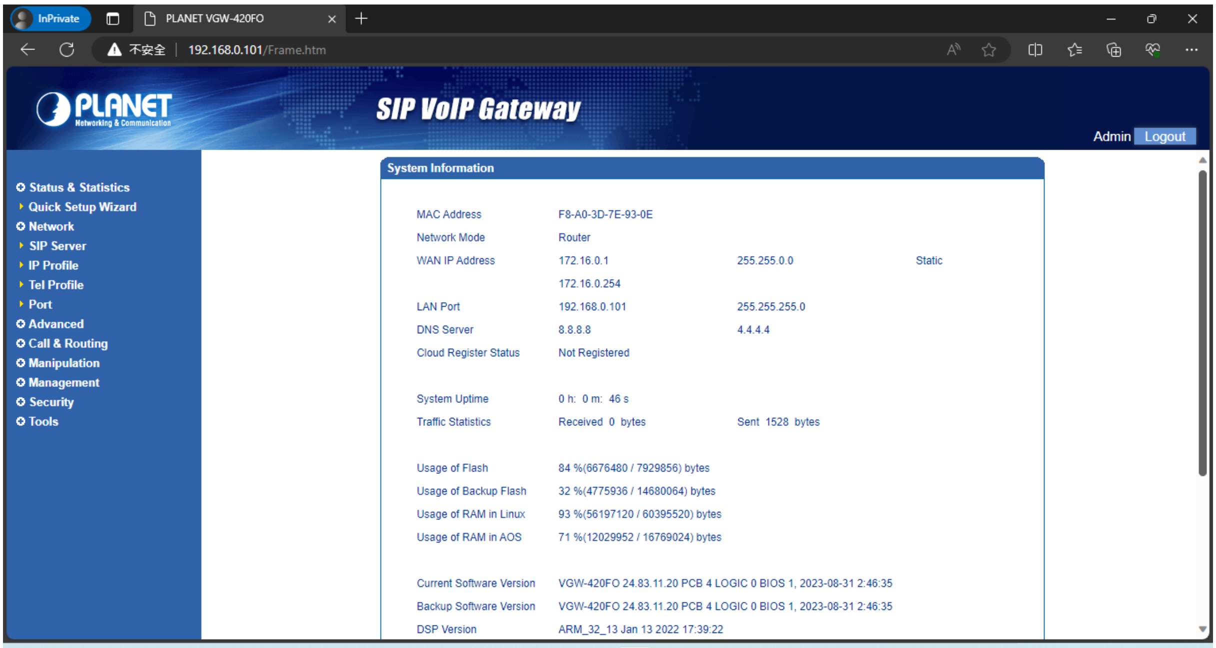


Figure 3.3-1: System Information

Explanation of items on System Information interface.

Parameter	Explanation
MAC Address	Hardware address of the LAN port.
Network Mode	Display network mode, including 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 VGW-420FO, 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 VGW-420FO. 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 VGW-420FO.

3.3.2 Port Status

On the **Status & Statistics →Port Status** page, you 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.

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

Figure 3.3-2: Port and Port Group Registration Information

SIP User status:

- Registered: The port is registered to SIP server successfully.
- Unregistered: The port fails to be registered to SIP server.

3.3.3 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.

Current Call

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

Refresh

Figure 3.3-3: Current Call Information

3.3.4 RTP Session Statistics

On the **Status & Statistics → RTP Session** page, you 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.

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

Figure 3.3-4: RTP Session Statistics

3.3.5 CDR Statistics

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.

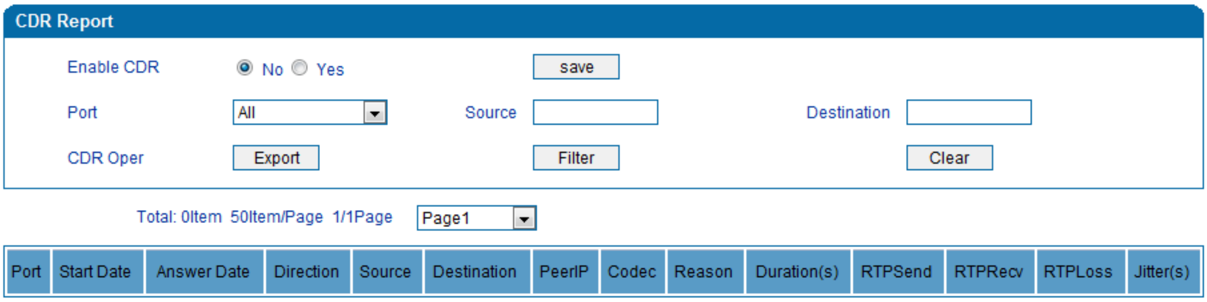


Figure 3.3-5: CDR Statistics

On the **Status & Statistic → CDR** interface, details of all calls through the ports of the VGW-420FO displayed. The CDR function can be enabled on this interface.

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 sent, RTP received, RTP loss rate, jitter.

3.3.6 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.

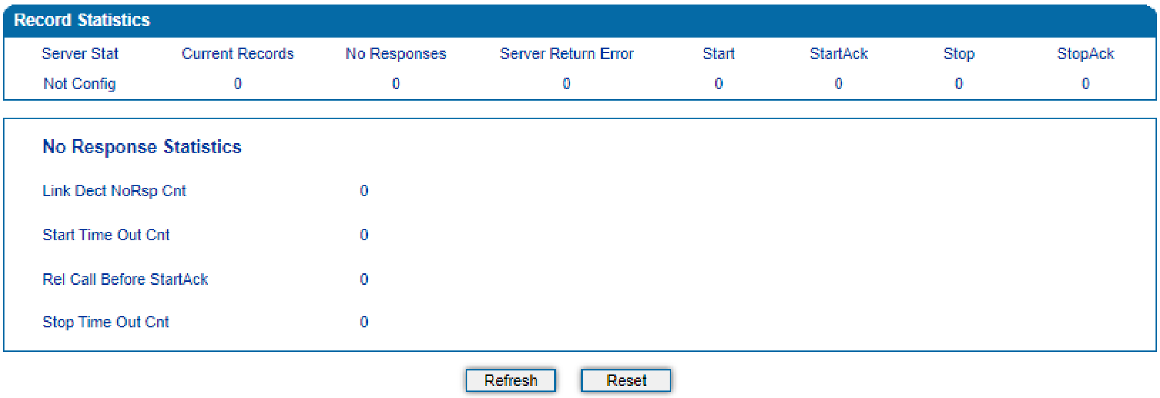


Figure 3.3-6: Record Statistics

3.3.7 Call Limit Info

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

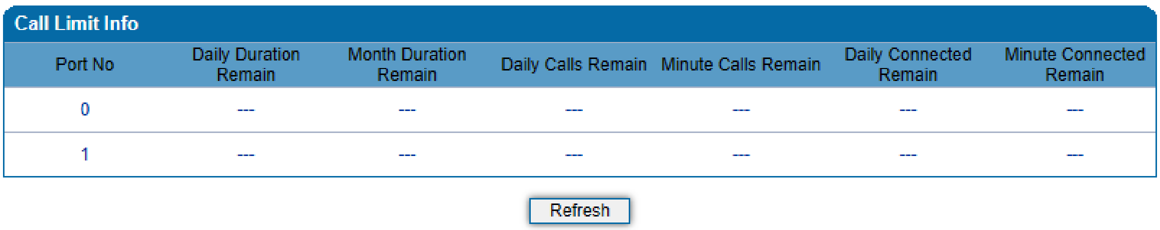


Figure 3.3-7: Call Limit Info

3.3.8 VPN State

On the **Status & Statistic → VPN State** page, VPN information including Protocol, State, IP Address, Gateway, Server Address, RX/TX Bytes, Connection Status, and 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

Figure 3.3-8: VPN State

3.4 Quick Setup Wizard

Quick setup wizard guides user to configuring 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, user is able to make voice call via the VGW-420FO Gateway.

3.5 Network Configuration

3.5.1 Local Network

The VGW-420FO Gateway has two kinds of network mode: route and bridge. When the gateway works in the route mode, it will work as a small router and NAT function is enabled. Under this situation, WAN port is normally connected to router/switch or ADSL MODEM, while LAN port is connected local computer or other network devices (such as Ethernet switches, hubs, etc.).

When the gateway works in the bridge mode, WAN port and LAN port are the same. The gateway serves as a two-port or four-port Ethernet switch. In this network mode, user only needs to configure the IP address of WAN port and DNS. In the router mode, the default LAN port IP will display and it can be changed by users.

DHCP:

Obtain IP address automatically.

Static IP Address:

Static IP address is a permanent IP address which is assigned by Internet Service Provider (ISP) and remains associated with a single computer over an extended period of time. This differs from a dynamic IP address**,** which is assigned *ad hoc* at the start of each session, normally changing from one session to the next.

PPPoE:

PPPoE is an acronym for point-to-point protocol over Ethernet, which relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections. PPPOE IP address refers to IP address assigned through the PPPoE mode. If you choose PPPoE, you need to fill in the account, password and service name, which are provided by telecom operator.

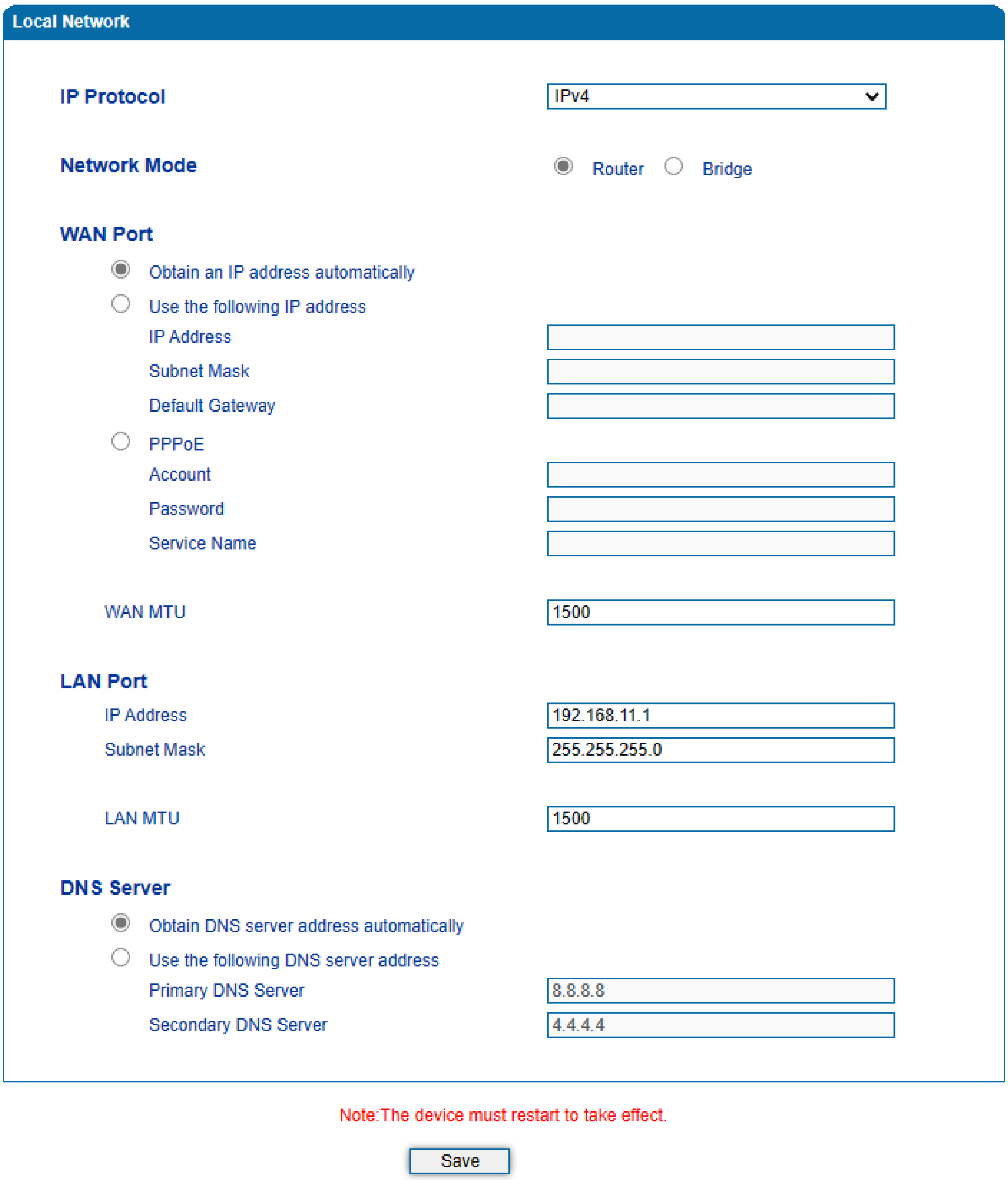


Figure 3.5-1: Route Mode

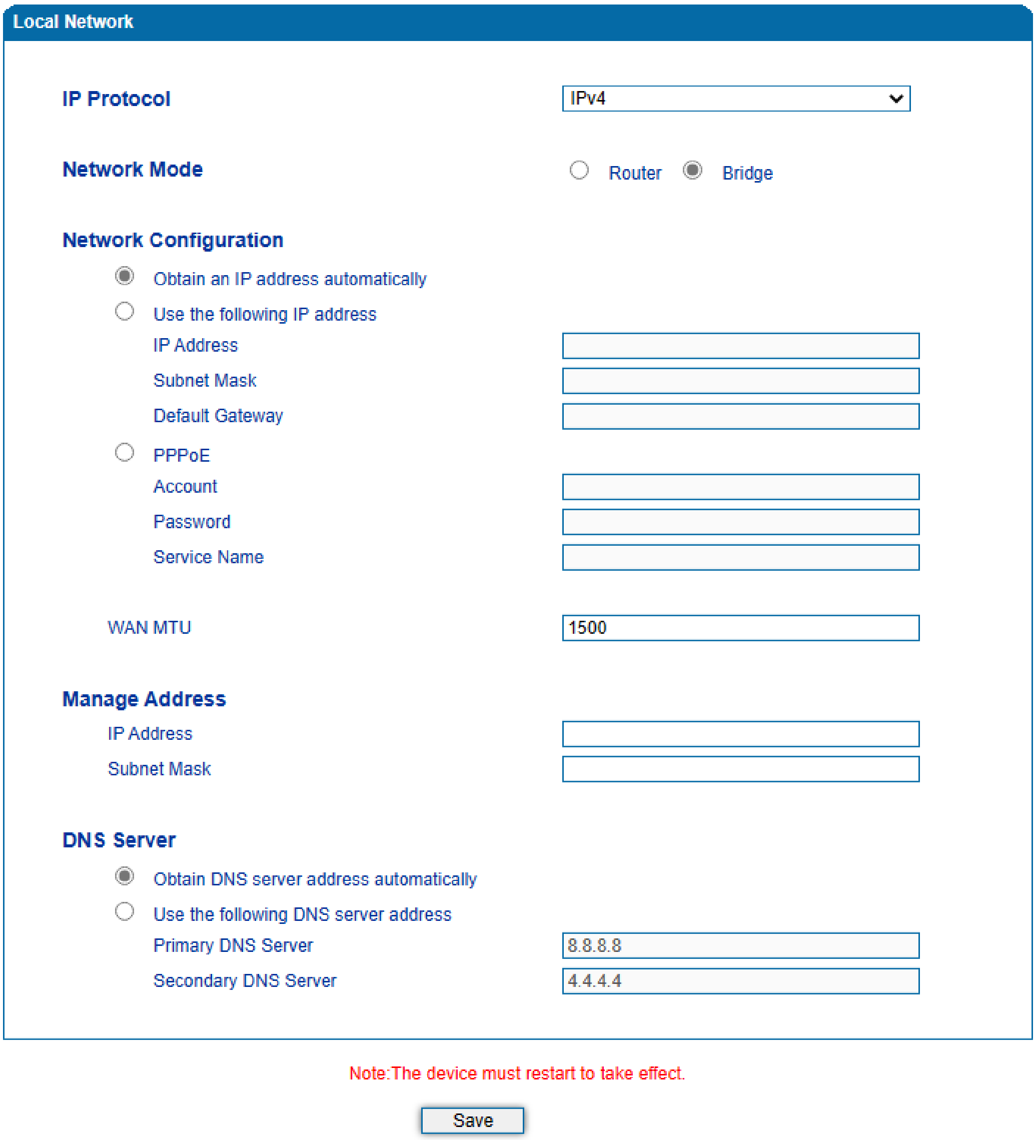


Figure 3.5-2: Bridge Mode

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

- If DHCP is selected to obtain IP address, please ensure DHCP server in the network works normally.
- When the gateway works in the route mode, the IP address of LAN port and that of WAN port cannot be in the same network segment; otherwise, the gateway can't work normally.
- When the gateway works in the route mode, log in to the gateway's web configuration interface via the LAN port.
- After the configurations are finished, please restart the gateway for the configurations to take effect.

3.5.2 VLAN（Virtual Local Area Network）

In order to control the impacts brought by broadcast storms, user can divide VLANs into three groups, namely VLAN1, VLAN2 and VLAN3. There are three kinds of VLANs, including data VLAN, voice VLAN and management VLAN. Different kinds of VLANs have different messages. 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.

802.1Q

The IEEE 802.1Q standard defines the architecture for Virtual Bridged LANs; the services provided in Virtual Bridged LANs and the protocols and algorithms are involved in the provisions of those services. No Quality of Service mechanisms are defined in this standard, but an important requirement for providing QoS is included in this standard, e.g. the ability to regenerate user priority of received frames using priority information contained in the frame and the User Priority Regeneration Table for the reception Port.

802.1P

IEEE 802.1P standard describes important methods for providing QoS at MAC level. IEEE 802.1p is in fact quite good. Lower priority level packets are not sent, if there are packets in queued in higher level queues. IEEE 802.1p describes no admission control protocols. It would be possible to give Network Control priority to all packets and the network would be easily congested.

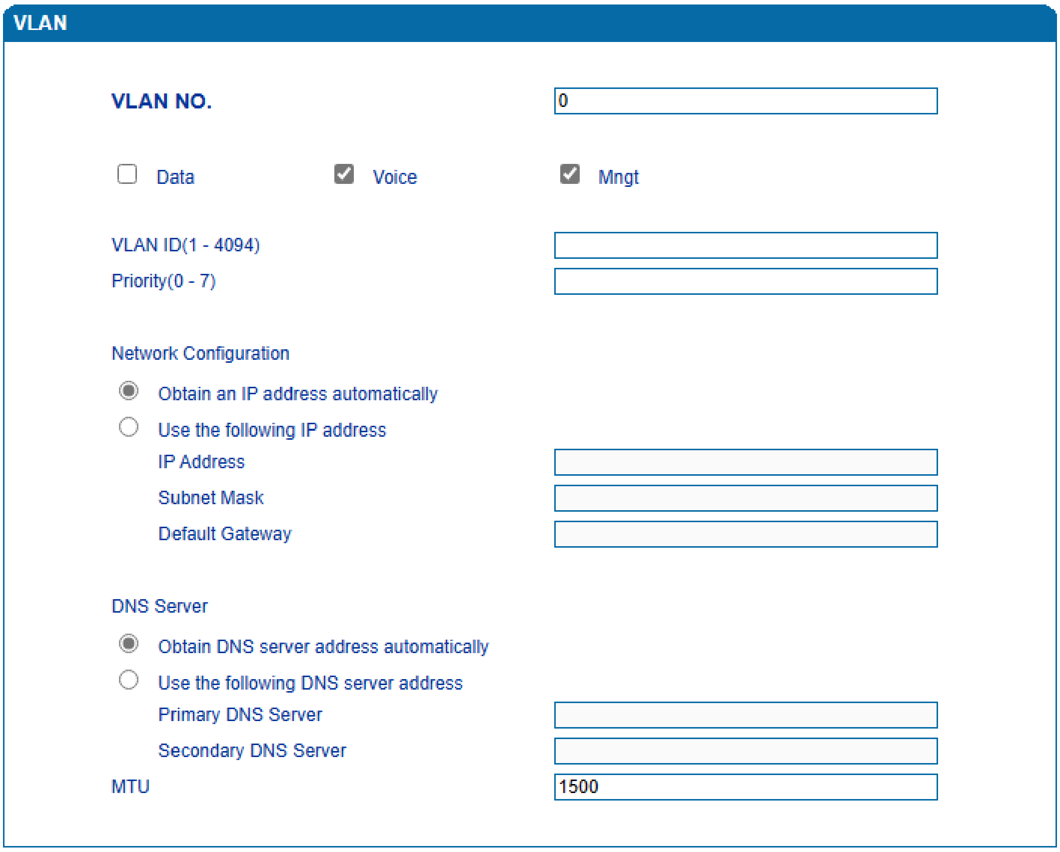


Figure 3.5-3: VLAN Parameter Configuration

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	User needs to restart the gateway for the configurations to take effect.

3.5.3 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 are the definitions 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.

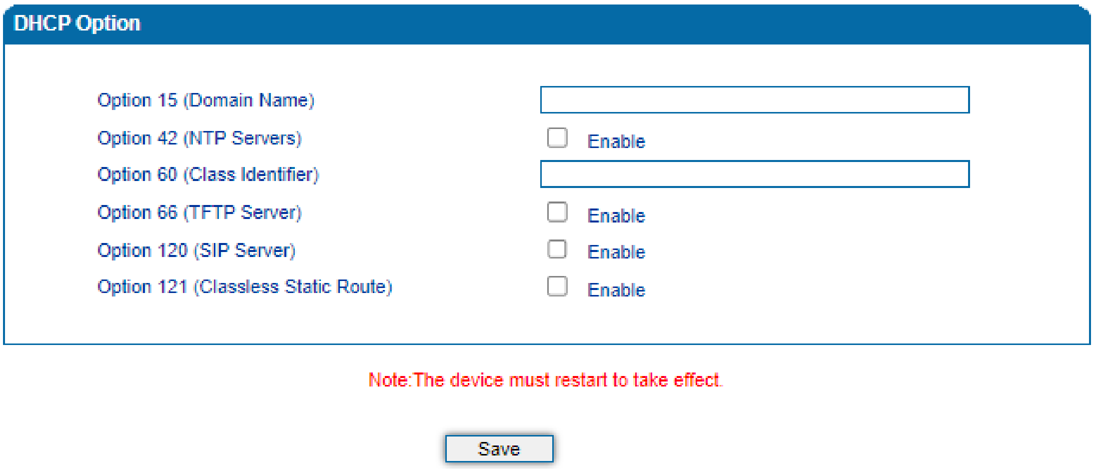


Figure 3.5-4: DHCP Option Parameter Configuration

Note	
	► User needs to restart the gateway for the configurations to take effect. ► Network Interface: Choose which VLAN to send request to DHCP server (or to receive information from DHCP server).

3.5.4 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.

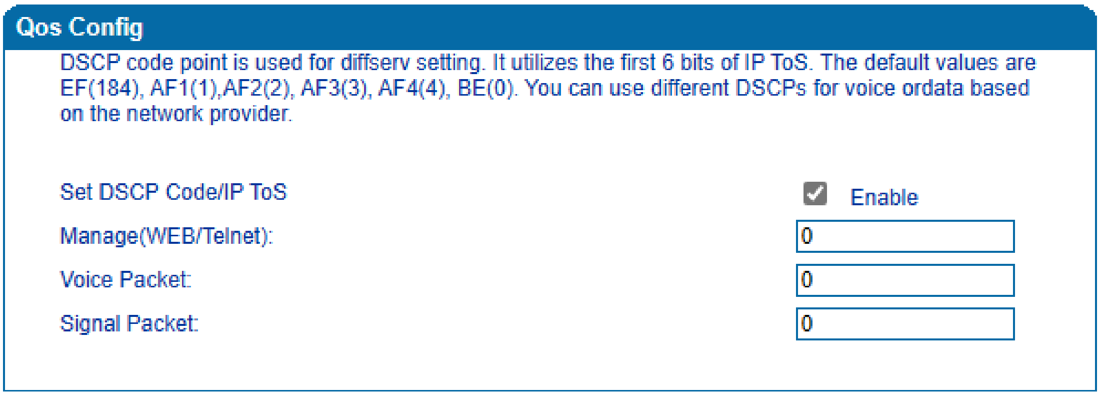


Figure 3.5-5: QoS Parameter Configuration

3.5.5 DHCP Server (Route Mode)

When the gateway works in the route mode, it works as a small router and user can its DHCP service so that the VGW-420FO Gateway serves as a DHCP server in the network.

- "Start address" and "end address" of the address pool determine the range of IP addresses which are automatically assigned to other devices.

- "IP Expire Time" means the service time of an assigned IP address. When the service time expires, the IP address will no longer be valid.

- The subnet mask, gateway, DNS and other information will be transferred to the network equipment through the DHCP protocol.

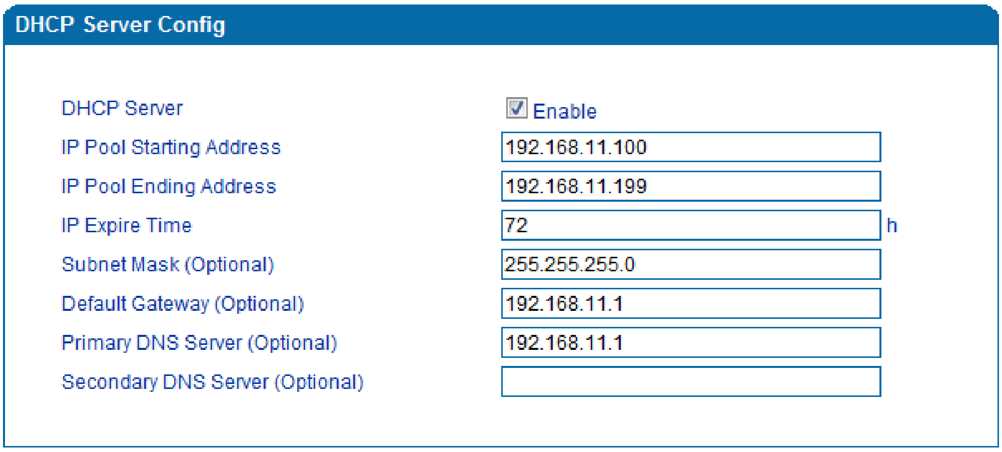


Figure 3.5-6: DHCP Server Configuration Interface

Note	When configuring the start IP address, end IP address, subnet mask and gateway IP address, please set them in the same network segment with the IP address of LAN port. Otherwise, other devices under the network will not work normally after they get the IP address assigned by the DHCP server. After the configurations are finished, please restart the VGW-420FO Gateway for the configurations to take effect.

3.5.6 DMZ Host (Route 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 te 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.

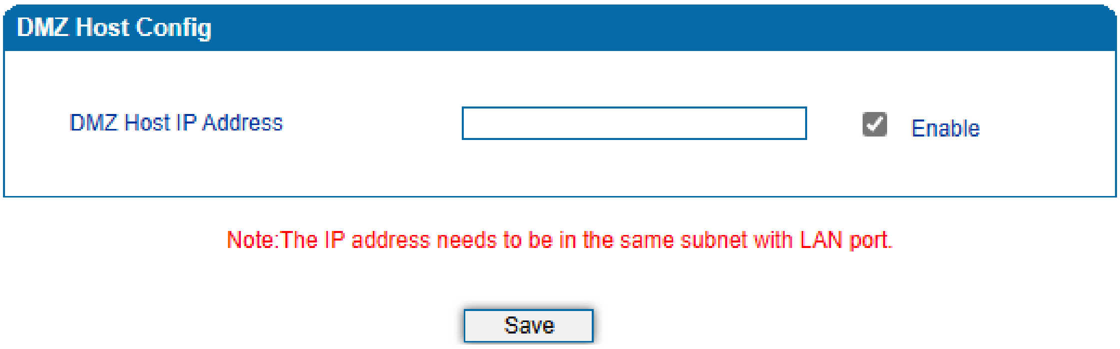


Figure 3.5-7: DMZ Configuration Interface

Note	After the configurations are finished, please restart the VGW-420FO Gateway for the configurations to take effect.

3.5.7 Forward Rule (Route Mode)

In some cases, LAN network equipment needs 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 ports (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.

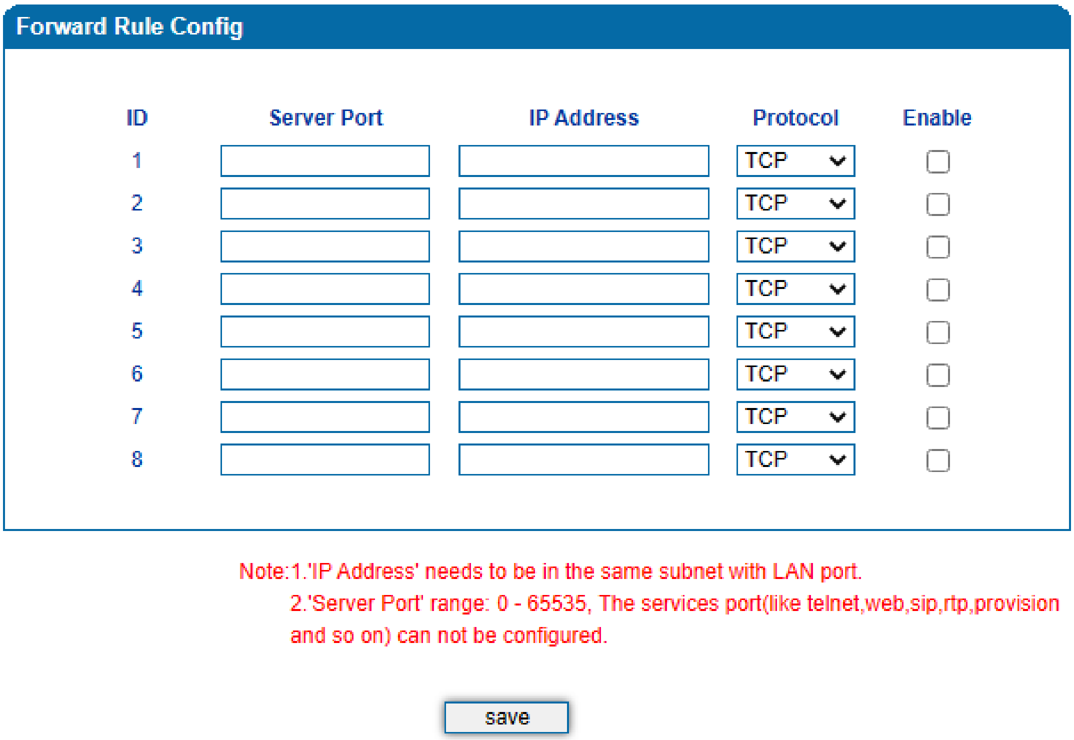


Figure 3.5-8: Configuration Interface for Forwarding Rules

3.5.8 Static Route (Route Mode)

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.

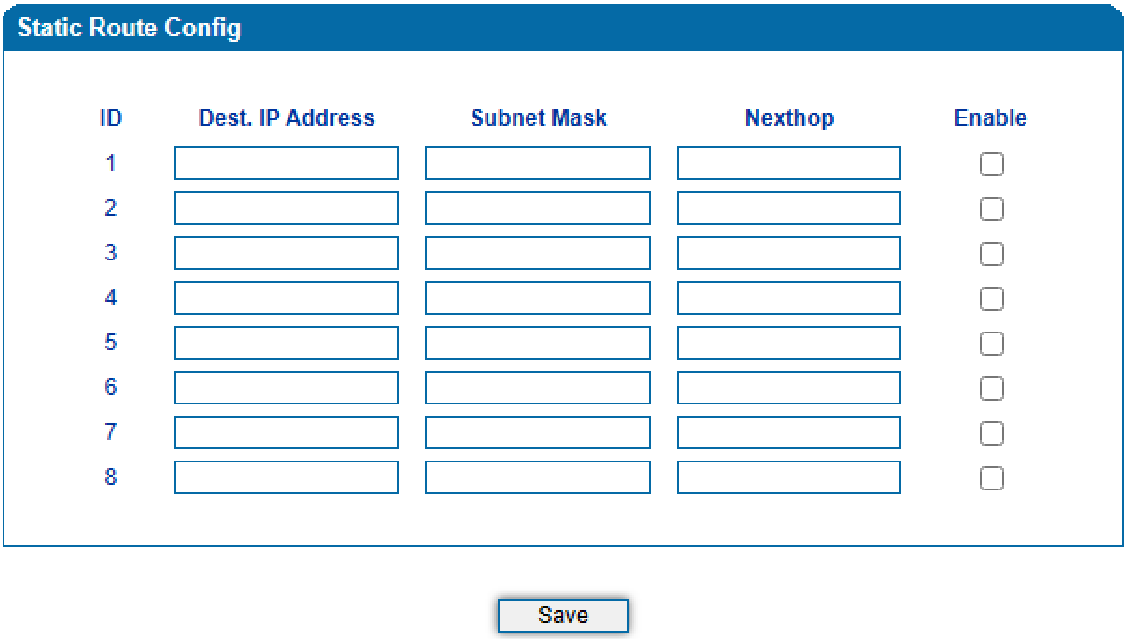


Figure 3.5-9: Configuration interface for Static Route

3.5.9 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.

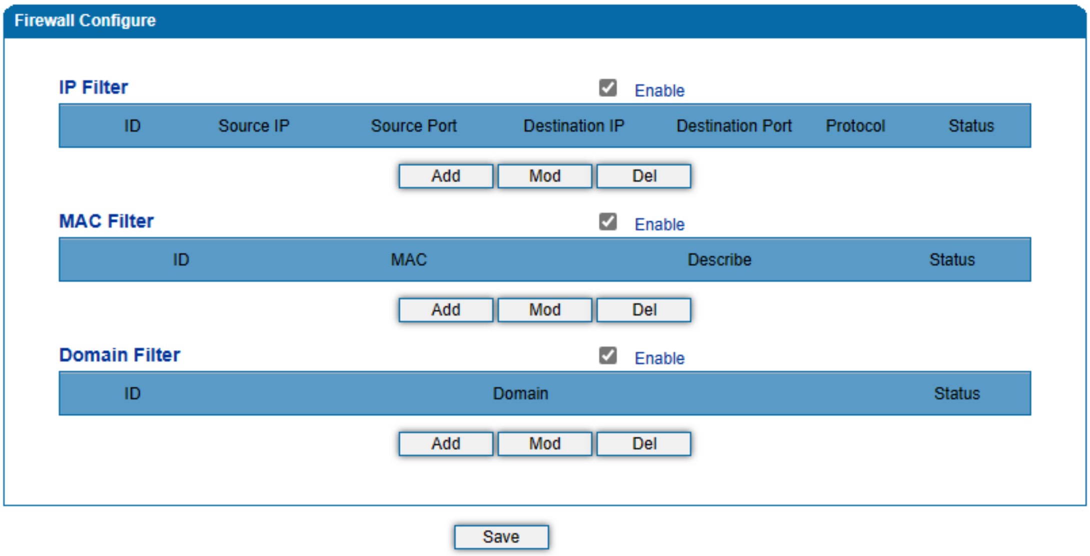


Figure 3.5-10: Configuration Interface for Firewall

3.5.10 ARP

ARP or address resolution protocol helps user 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. ARP is a tool that converts IP address into MAC address.

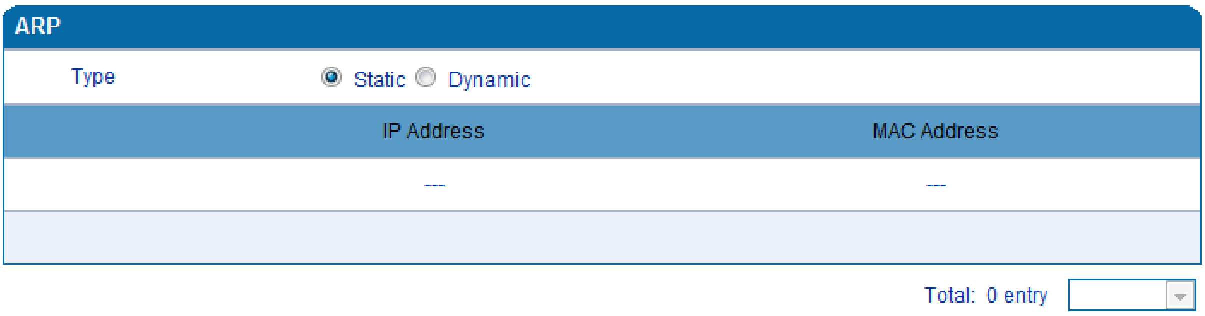


Figure 3.5-11: ARP Parameters

3.5.11 VPN

It generally refers to Virtual Private Network. VPN can create a private network over a public network for encrypted communication. The VGW-420FO Gateway currently supports only OpenVPN.

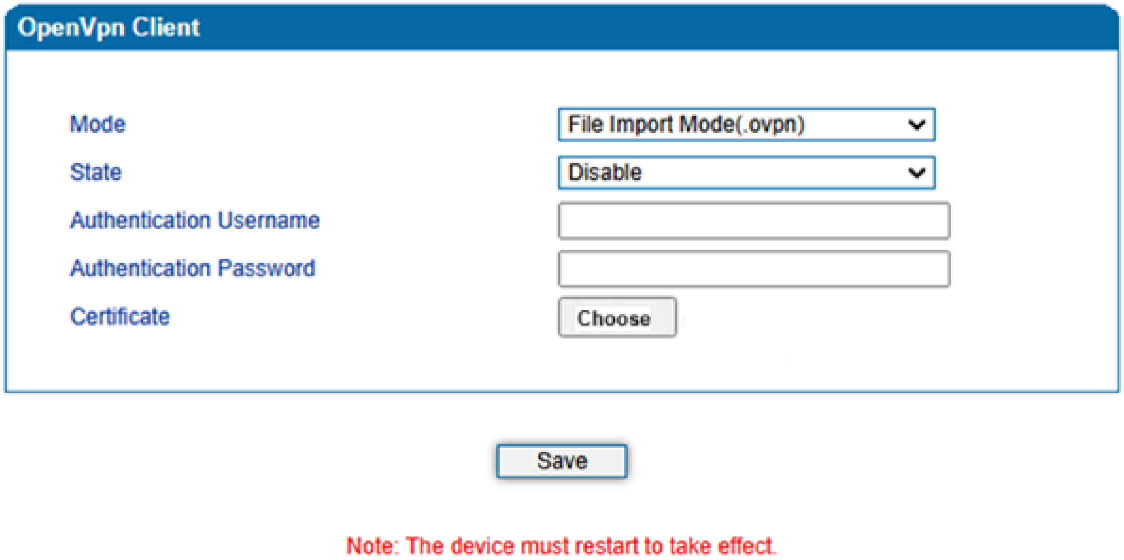


Figure 3.5-12: VPN Parameters

Explanation of VPN parameters:

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.

3.6 SIP Server

Introduction of SIP Server:

1) SIP server is the main component of VoIP network and is responsible for establishing all the 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.

2) 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 and conversational support, but also offers rich services such as Presence, Find-me and Music On Hold.

3) SIP server based on Linux platform like OpenSER, sipXecx, VoS, Mera or other.

4) SIP server based on Windows platform like mini SipServer, Brekeke, VoIPswitch or other.

5) Carrier-grade softswitch platform.

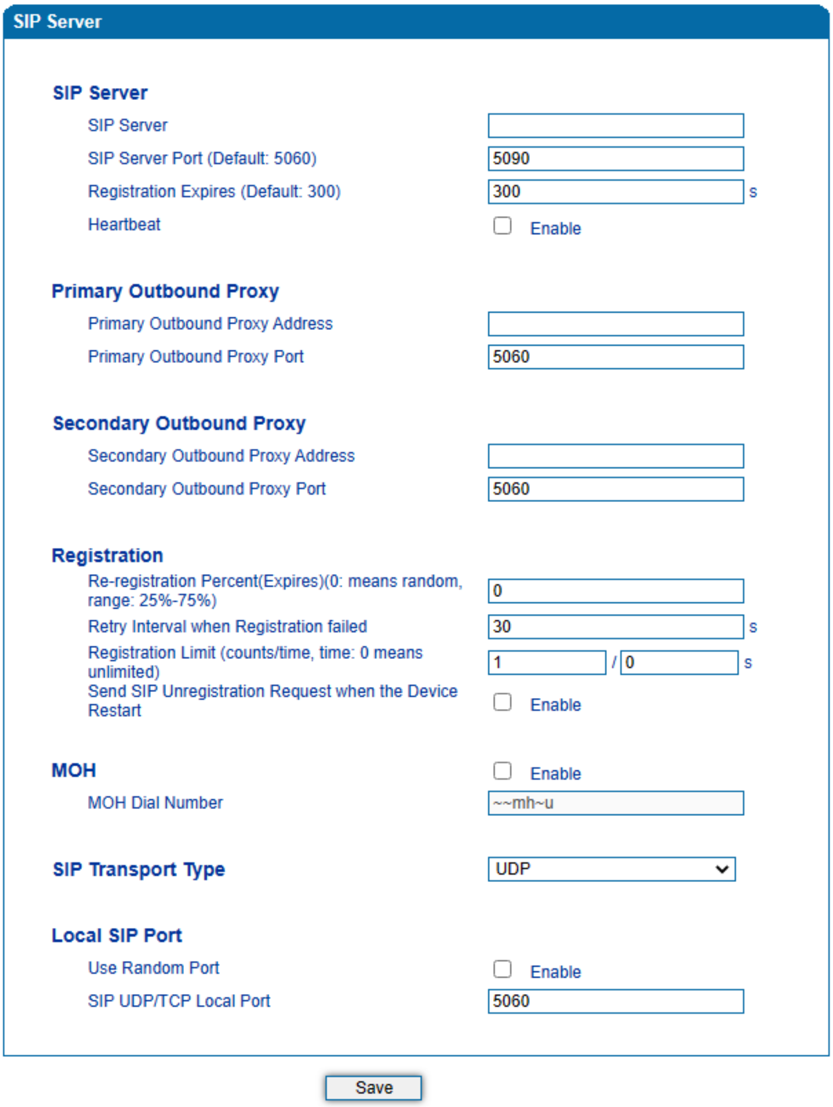


Figure 3.6-1: Configuration Interface for SIP Server

Explanation of SIP Server parameters:

Parameter	Explanation
SIP Server	The IP address or domain name of the SIP server is provided by service provider or system admin.
SIP Server Port (Default: 5060)	The server port of the SIP server is 5060 by default.
Registration Expiry (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 is provided by service provider.
Secondary Outbound Proxy Port	The server 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.

3.7 IP Profile

Introduction of IP Profile:

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

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

Add Modify Delete

Figure 3.7-1: Configuration Interface for IP Profile

3.8 Tel Profile

Introduction of Tel Profile:

Tel profile mainly consists of a series of line related parameters including fax, gain value, etc. which are used to configure different parameters for each port.

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

Note: The configuration will be synchronized to default TelProfile

Add Modify Delete

Figure 3.8-1: Configuration Interface for Tel Profile

3.9 Port

Introduction of 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.

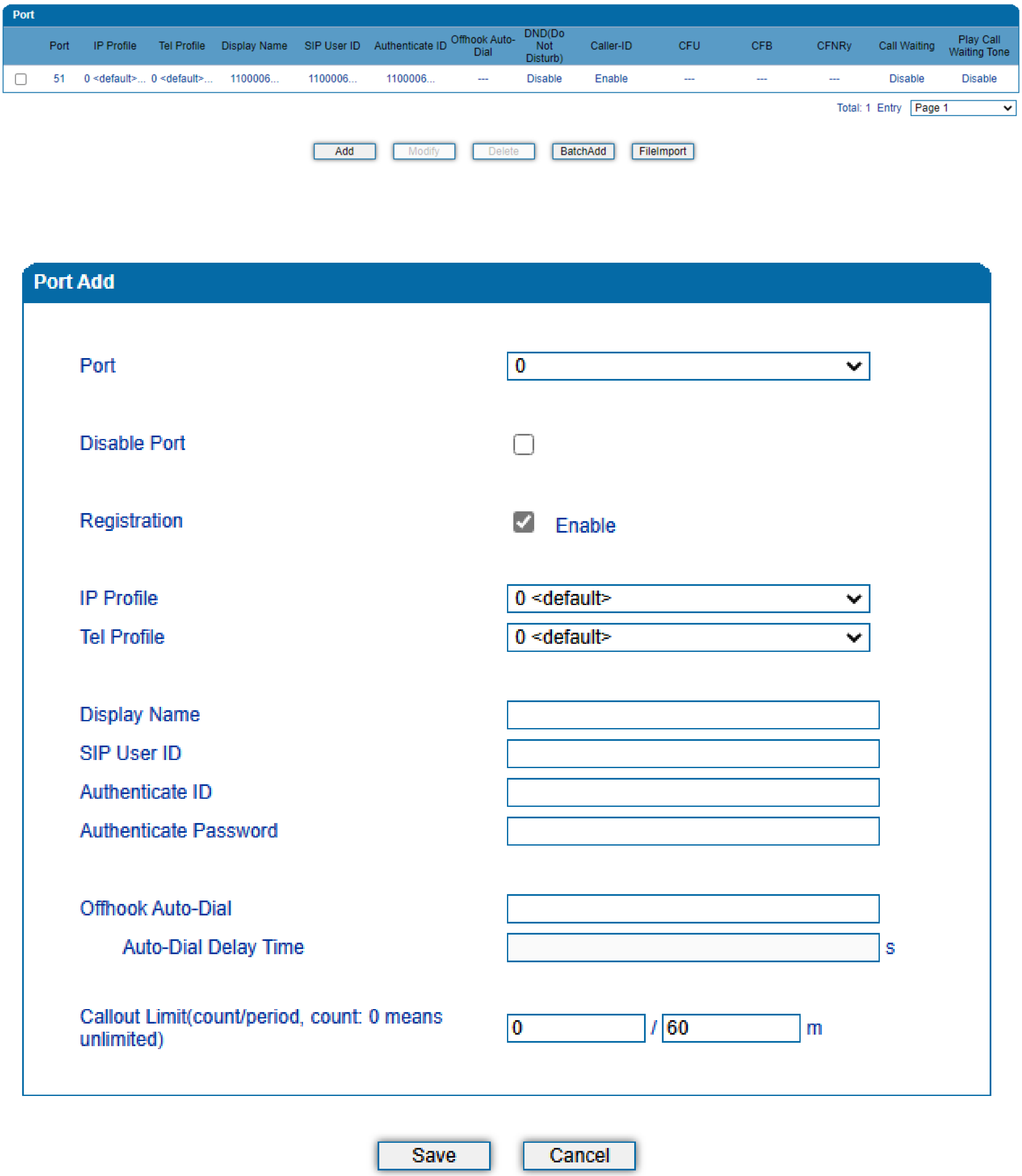


Figure 3.9-1: Configuration Interface for Port

Explanation of port parameters:

Parameter	Explanation
Port	The FXO port corresponding to this account
Disable Port	Whether to disable port temporarily
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 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 to 3 seconds, the auto-dial number is dialed after 3 seconds are over.
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.

3.10 Advanced

3.10.1 Line Parameters

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

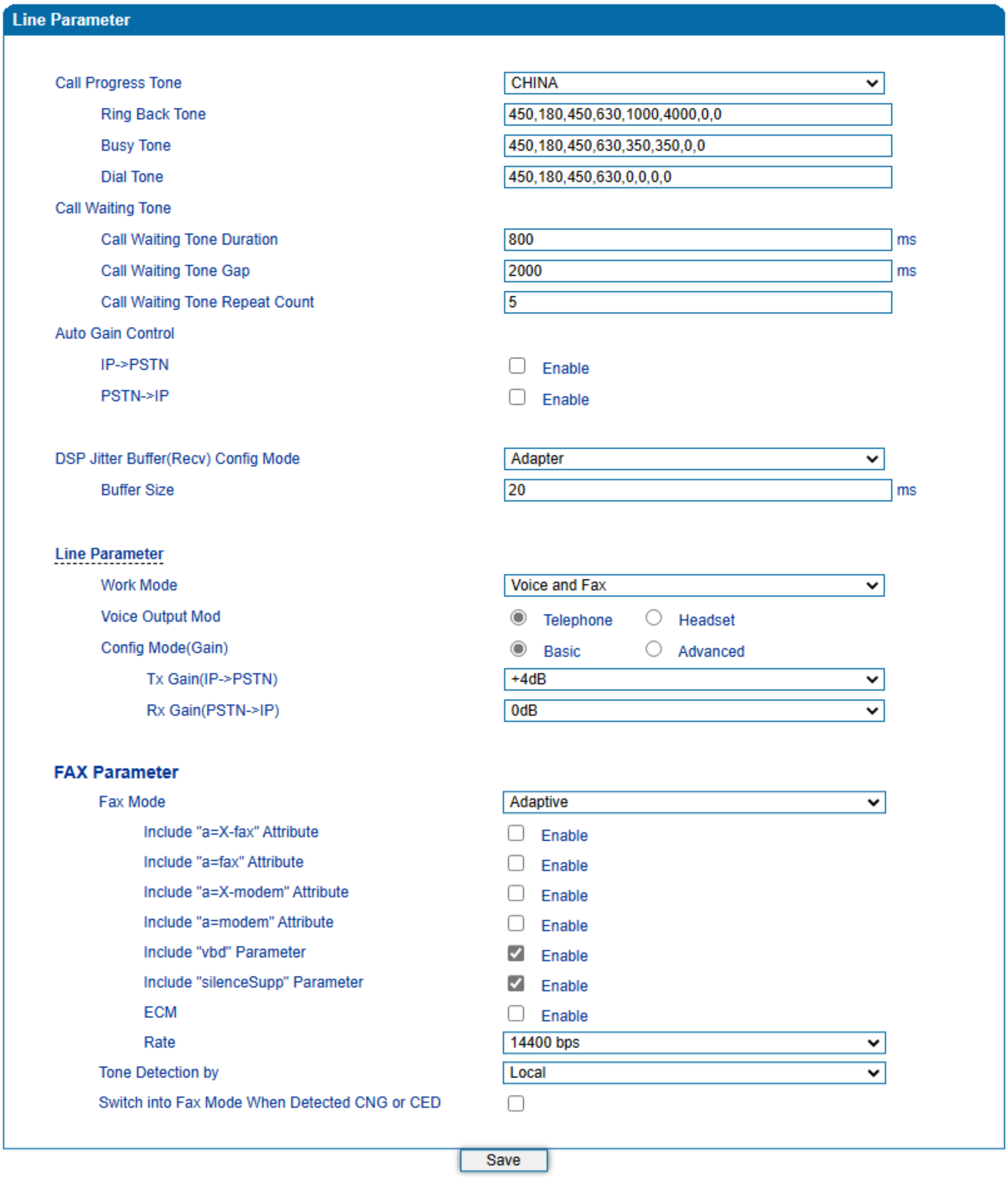


Figure 3.10-1 Configuration Interface for Line Parameters

Explanation of Line Parameters:

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 modes. There are several configure options: • Voice and Fax: 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 Mode	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 Detecting CNG or CED	If this parameter is enabled, the system will switch into fax mode when CNG or CED is detected.

3.10.2 FXO Parameter

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

An FXO (Foreign Exchange Office) port functions as a standard telephone interface, allowing the gateway to connect to analog lines such as those from a telecom provider or an internal PBX system.

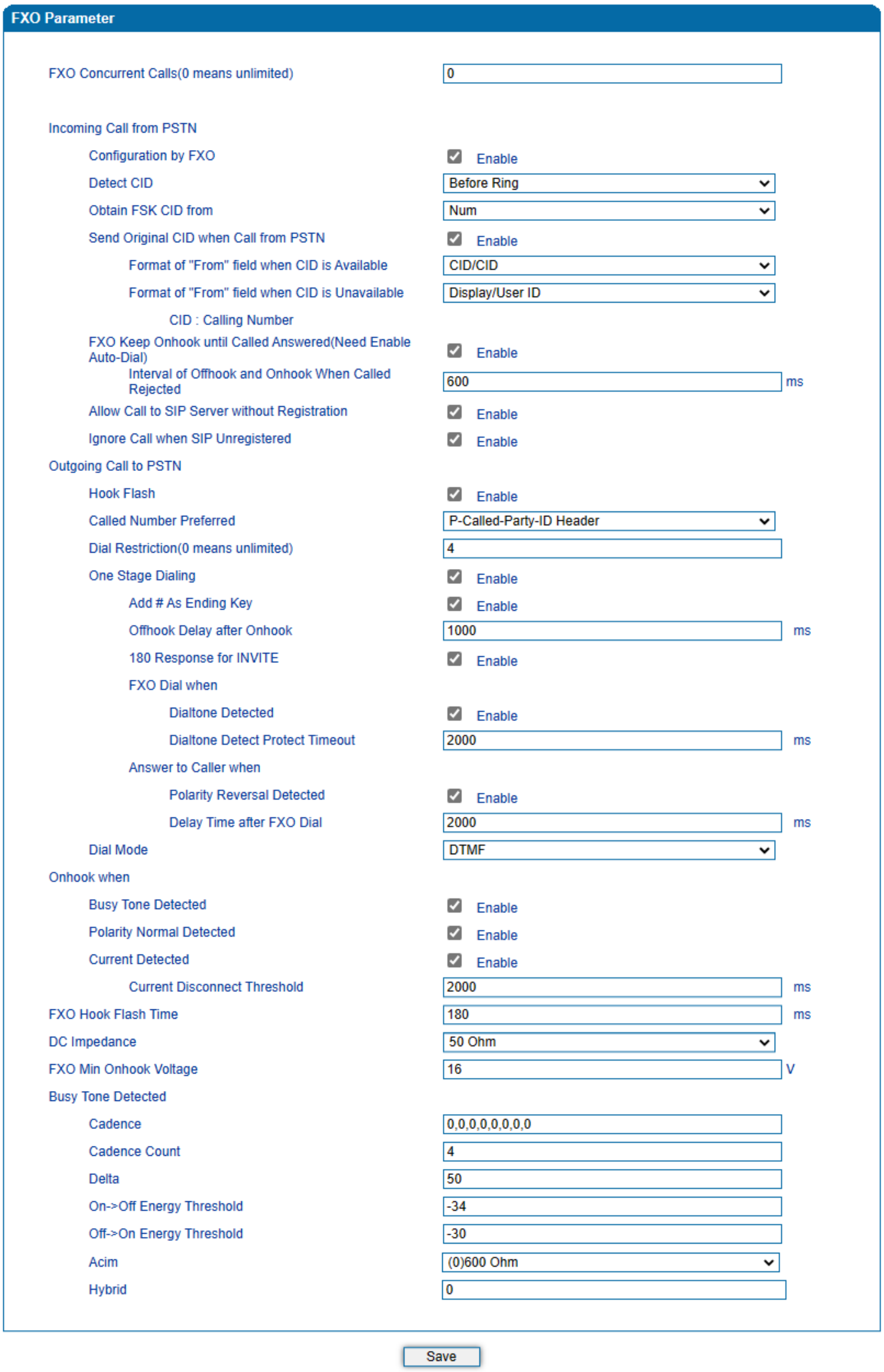


Figure 3.10-2 Configuration Interface for FXO Parameters

Explanation of FXO parameters:

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. 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 comes, 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, or 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, and 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.

3.10.3 Media Parameter

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

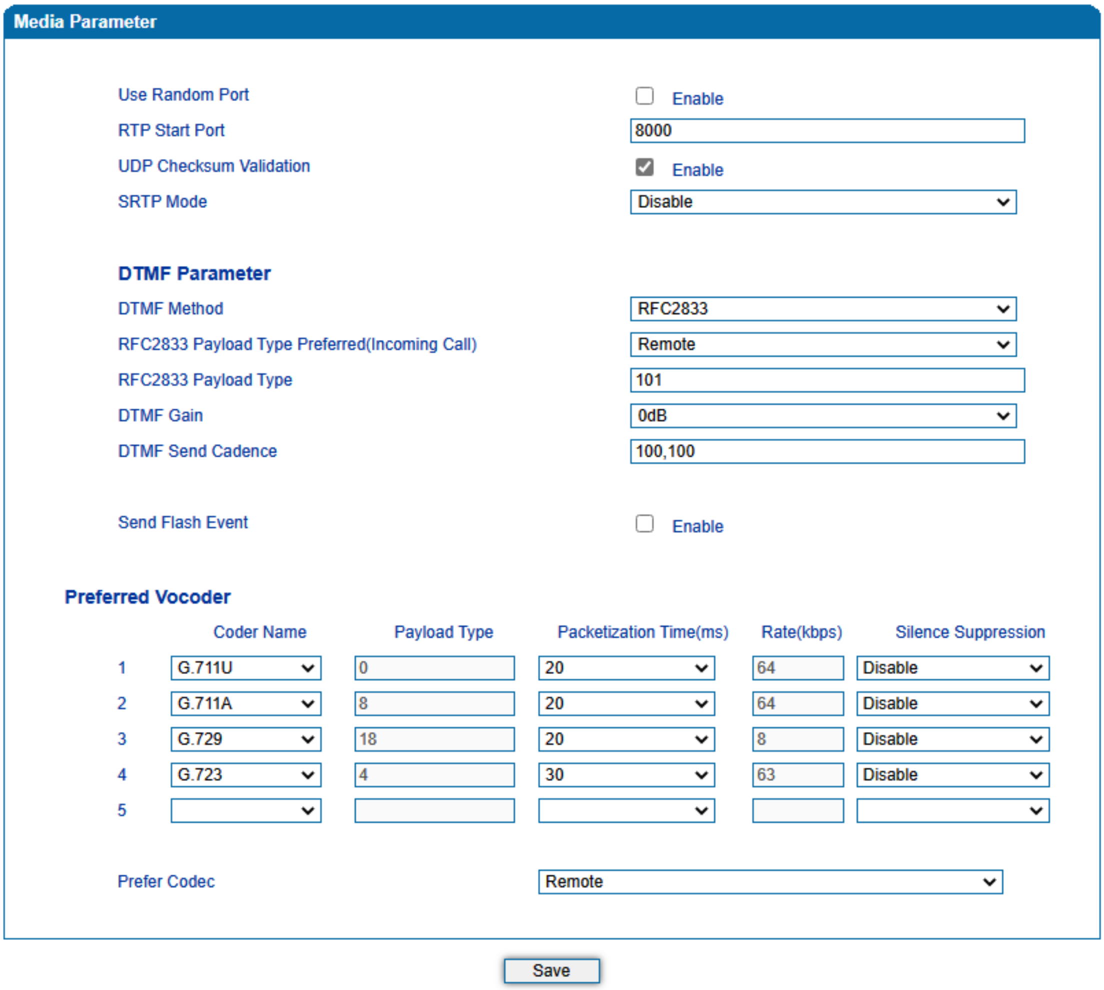


Figure 3.10-3 Configuration Interface for Media Parameters

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

3.10.4 Service Parameter

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

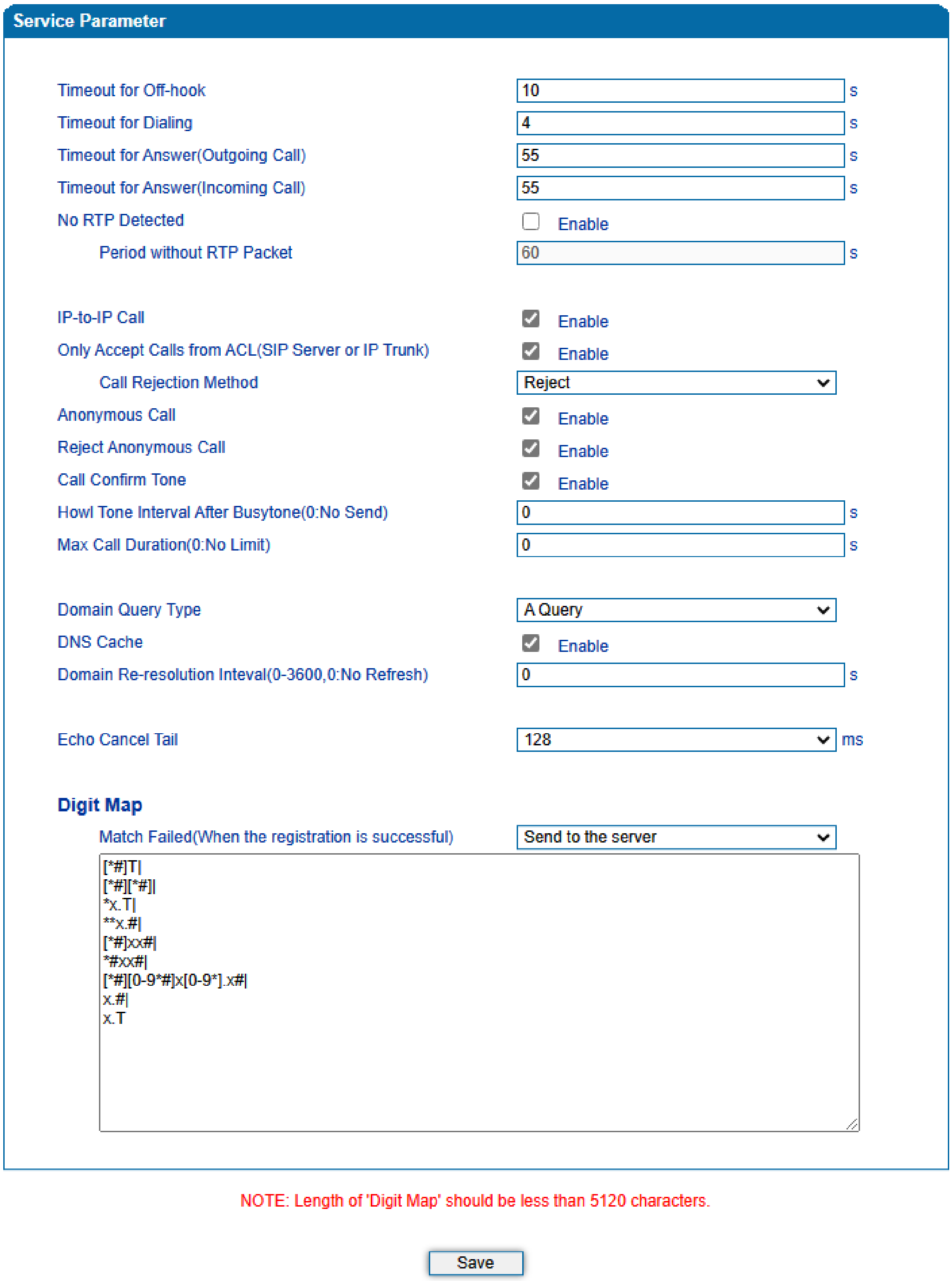


Figure 3.10-4 Configuration Interface for Service Parameters

Explanation of Service parameters:

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.

3.10.5 SIP Compatibility

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

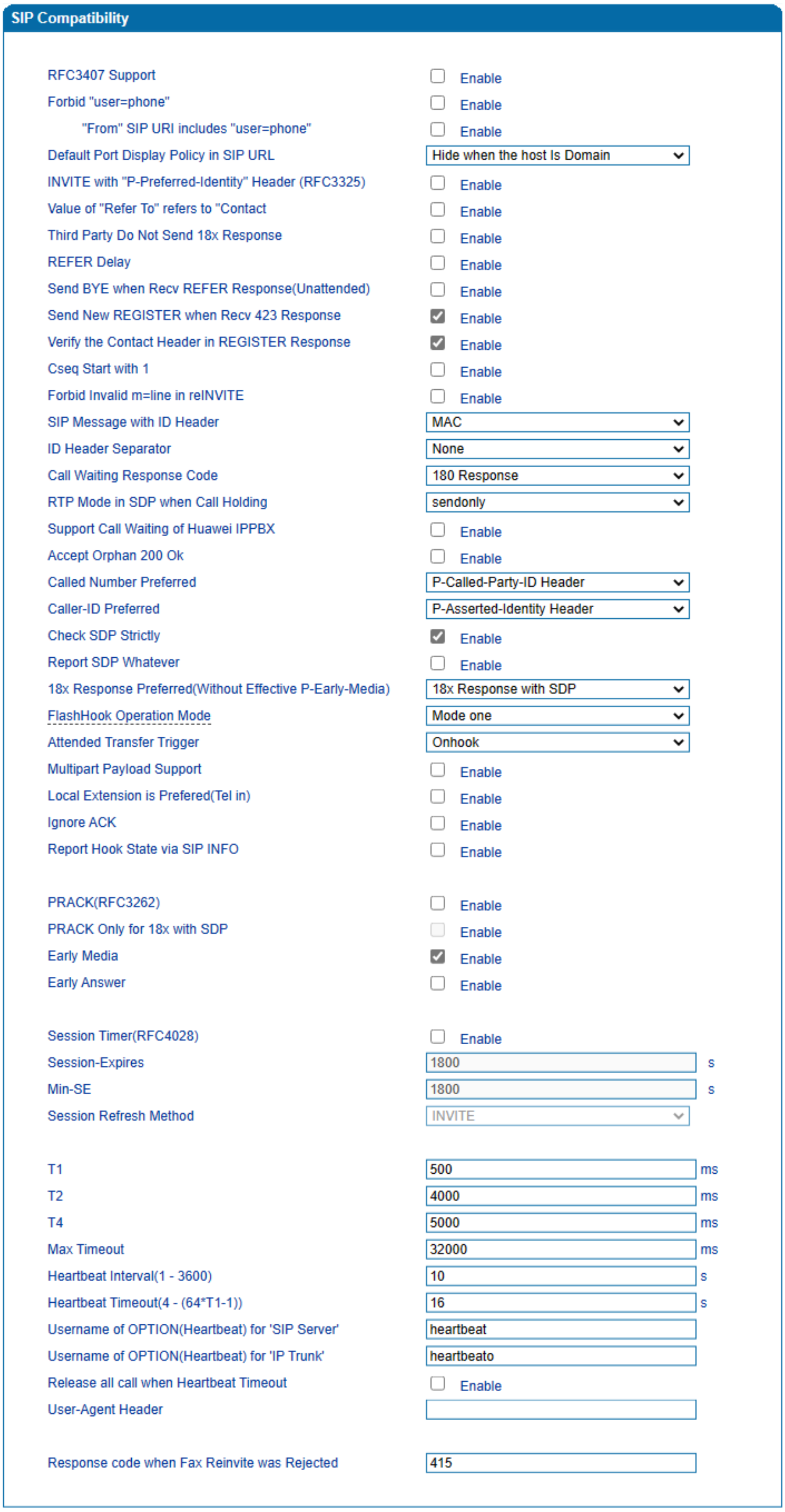


Figure 3.10-5 SIP Compatibility Configuration Interface

Explanation of SIP Compatibility 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.

3.10.6 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.

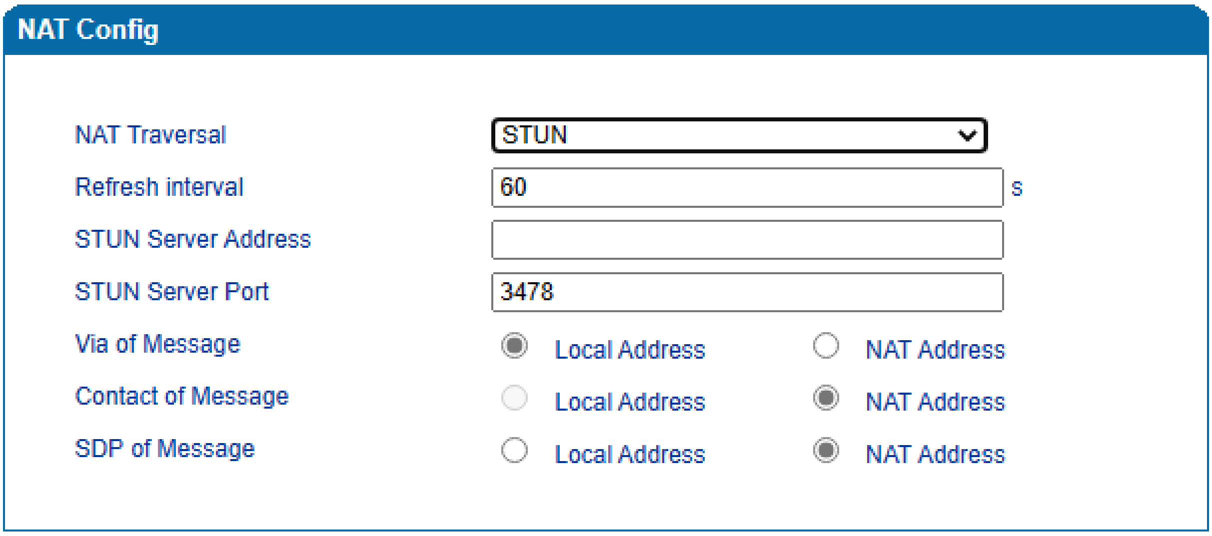


Figure 3.10-6 Configuration Interface for NAT Parameter

Explanation of NAT parameters:

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.

3.10.7 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.

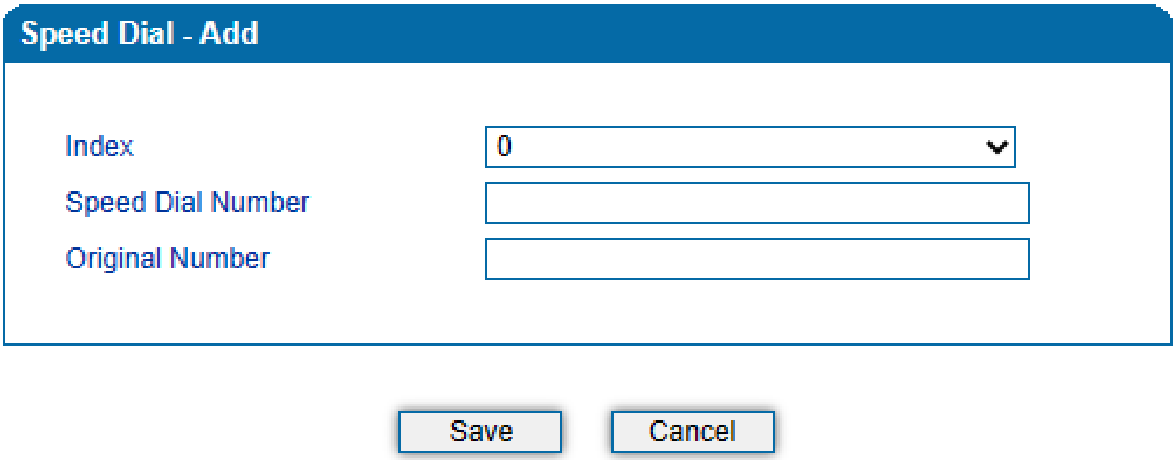


Figure 3.10-7 Configuration Interface for Speed Dial

3.10.8 Feature Code

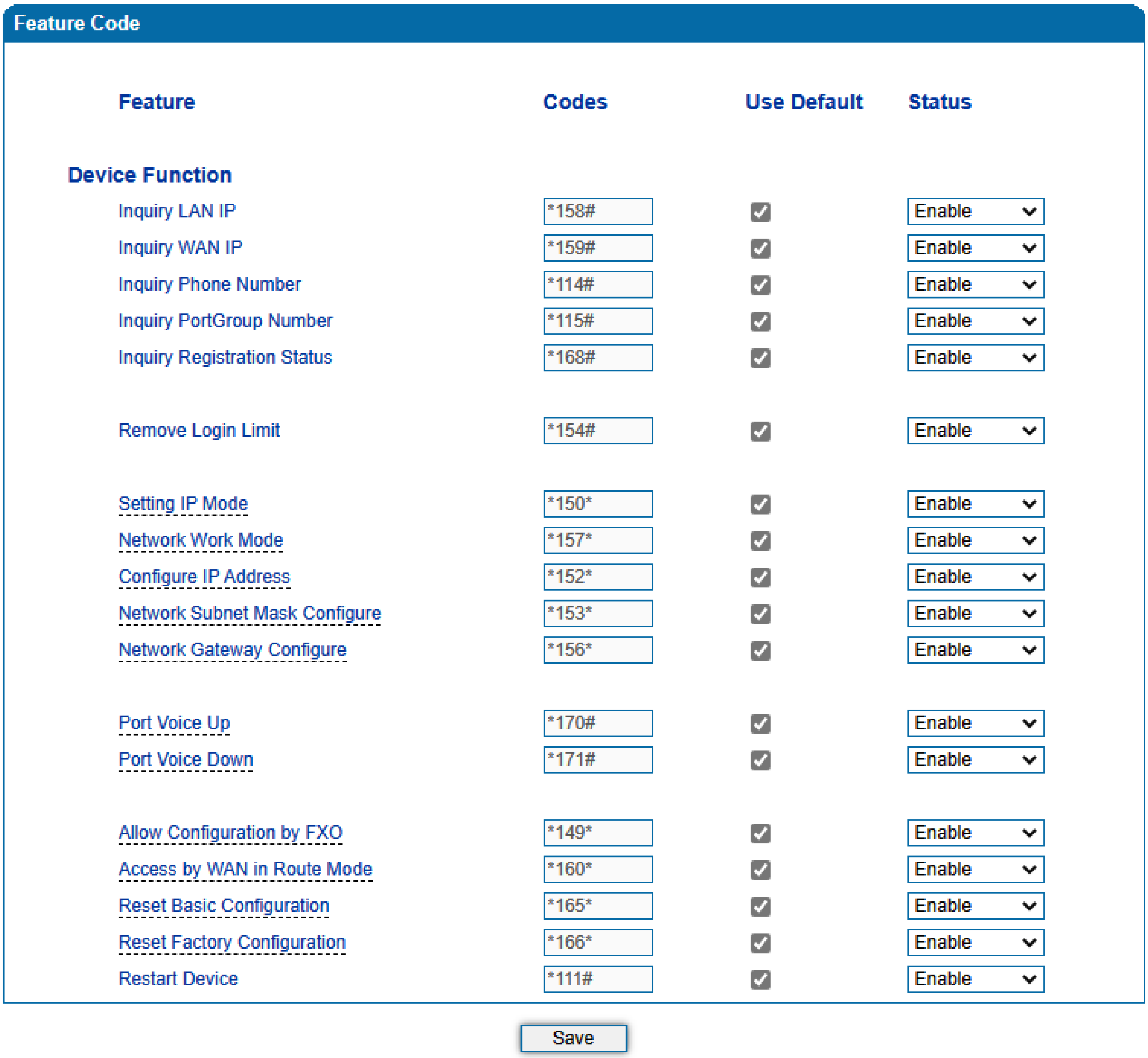


Figure 3.10-8 Configuration Interface for Feature Code

Explanation of Feature Code parameters:

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

3.10.9 System Parameter

System parameters include STUN, NTP, Provision, EB parameter and Telnet.

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.

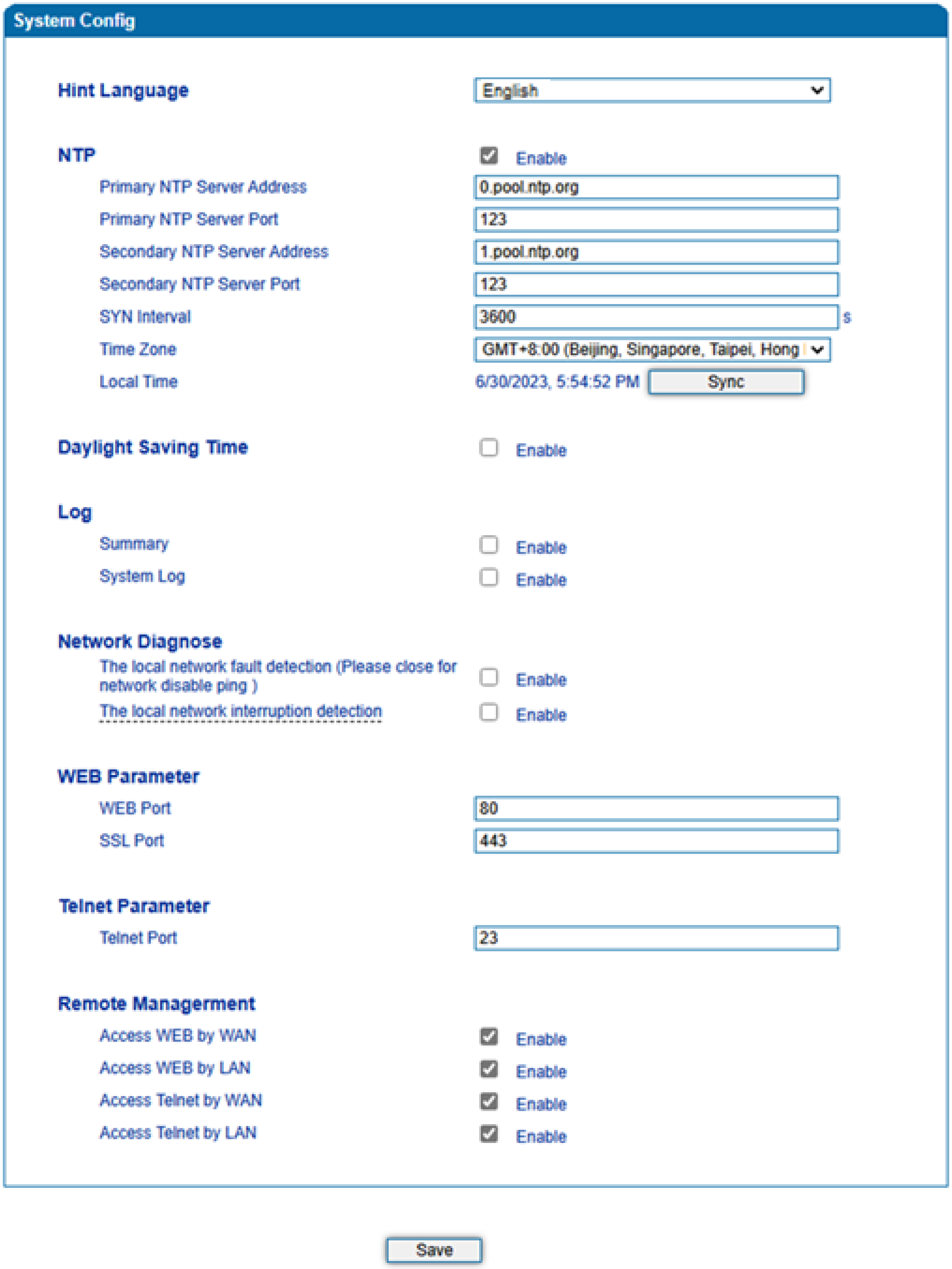


Figure 3.10-9 Configuration Interface for System Parameters

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 is us.pool.ntp.org by default.
Primary NTP Server Port	The server port of primary NTP server is 123 by default.
Secondary NTP Server Address	The IP address of secondary NTP server is 64.236.96.53 by default.
Secondary NTP Server Port	The service port of secondary NTP server is 123 by default.
SYN Interval	The interval to synchronize the time of the device is 3600s by default
Time Zone	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 is 80 by default.
SSL Port	The SSL port is 443 by default.
Telnet port	Listening port of telnet service is 23 by default.
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 the Web port and Telnet port configurations are finished, please restart the VGW-420FO Gateway for the configurations to take effect.

3.11 Call & Routing

3.11.1 Wildcard Group

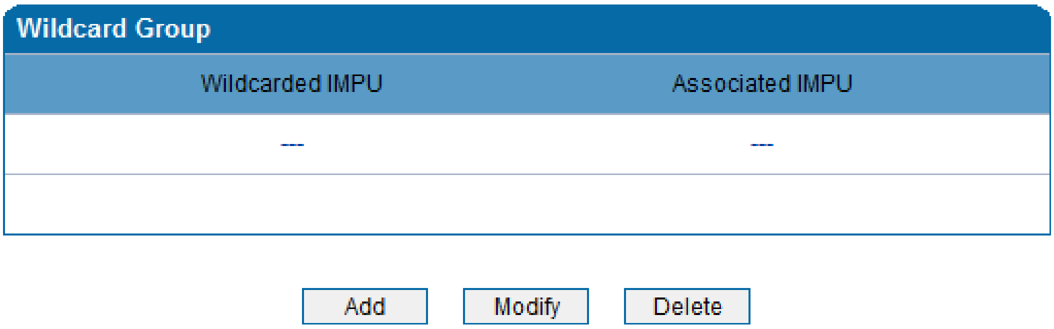


Figure 3.11-1 Wildcard Group

3.11.2 Port Group

On the **Port Group** interface, user can group several ports together and then set a strategy for port selection of the group. 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, and so on.

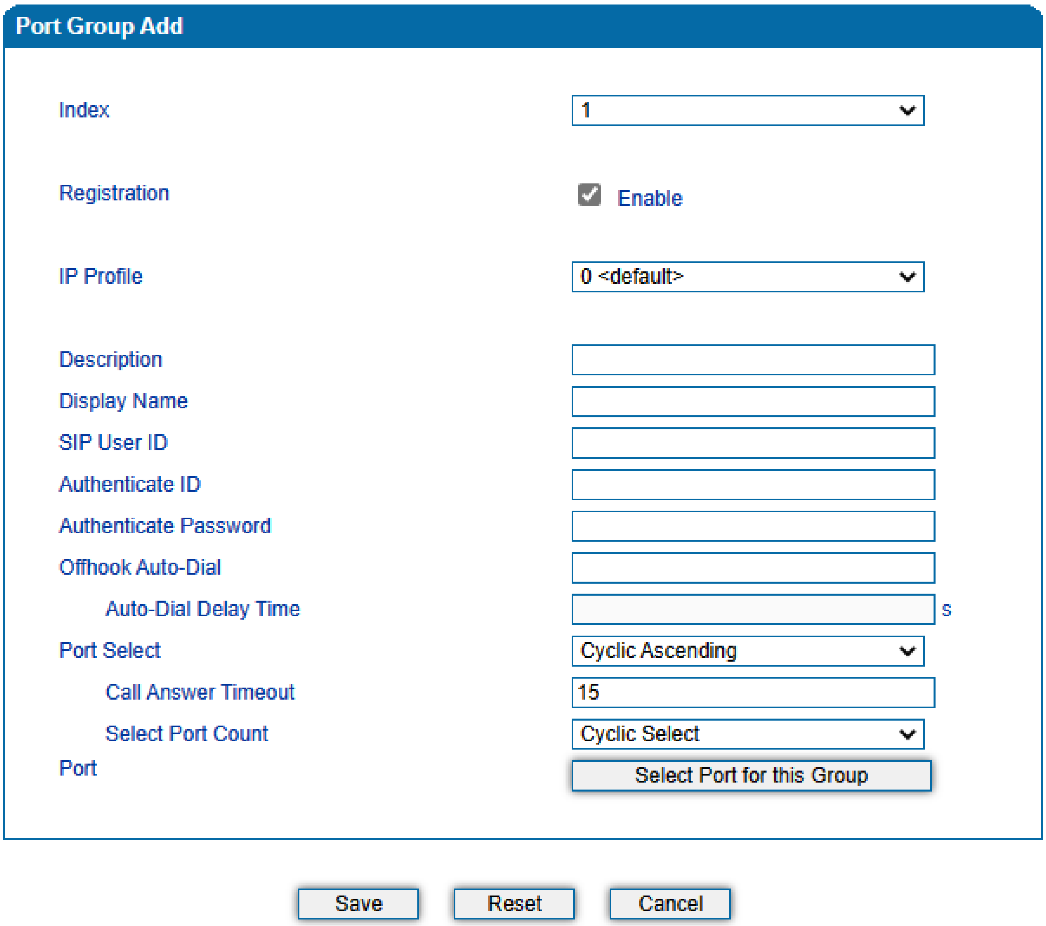


Figure 3.11-2 Configuration Interface for Port Group

Explanation of Port Group Parameters:

Parameter	Explanation
Index	The no. of the port group uniquely identifies a route.
Registration	Registration.
IP Profile	IP Profile.
Description	The description of the port group is used to identify the port group.
Display Name	Display name of the port group is 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 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.

3.11.3 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.

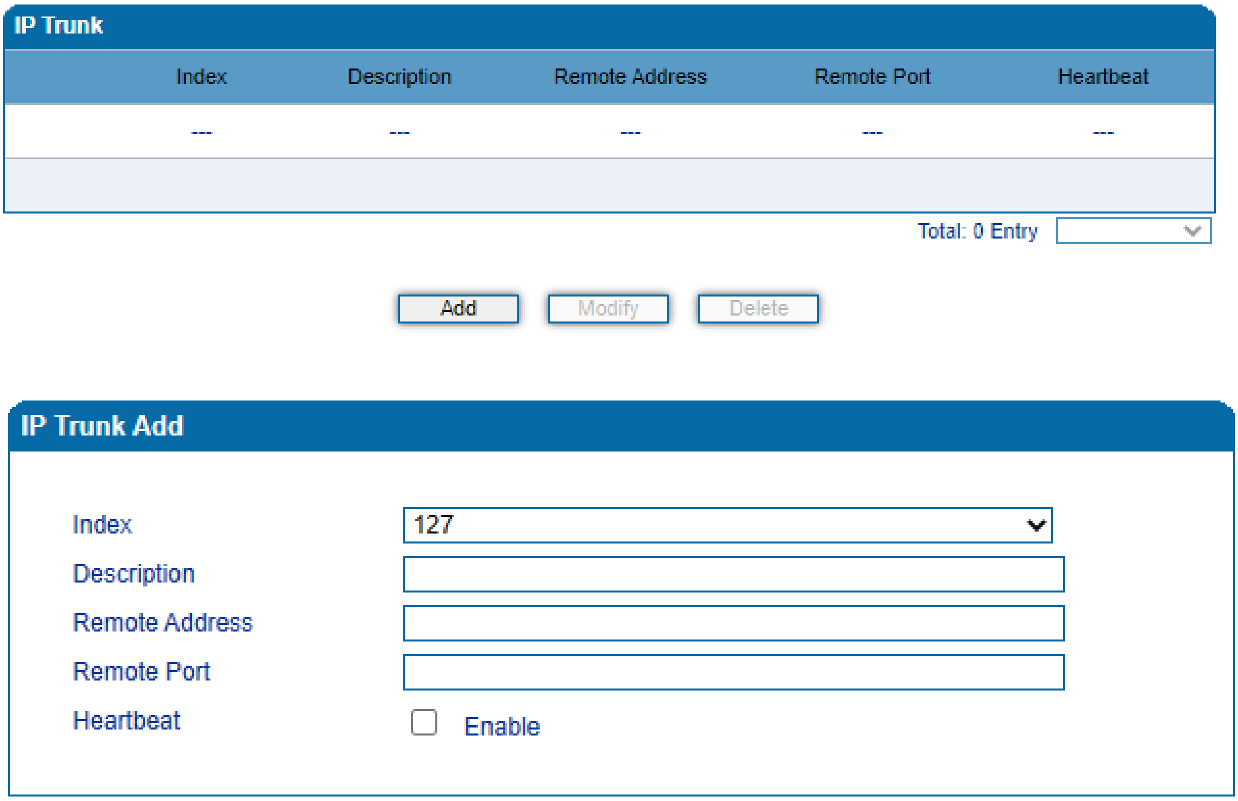


Figure 3.11-3 IP Trunk Configuration Interface

Explanation of IP Trunk Parameters:

Parameter	Explanation
Index	The no. of the IP trunk ranges from 0 to 127.
Description	The description of the IP trunk 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.

3.11.4 Routing Parameter

Routing parameter determines a call routed before or after manipulation.

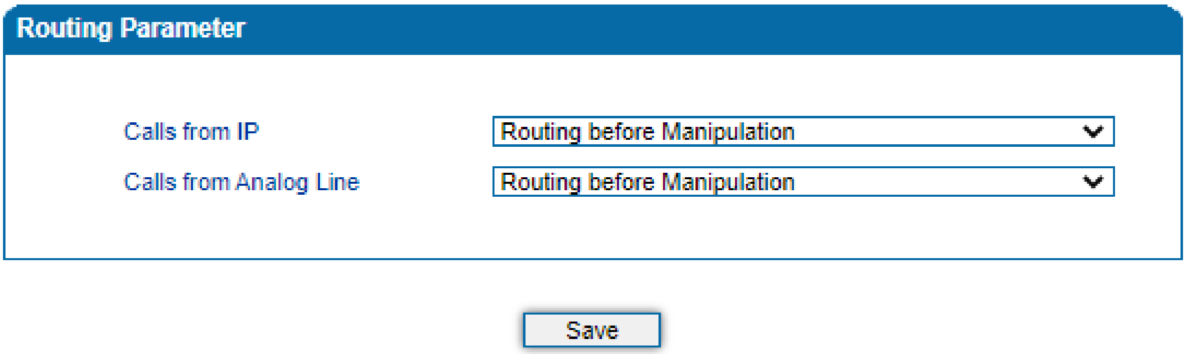


Figure 3.11-4 Configuration Interface for Routing Parameter

Explanation of Routing Parameters:

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

3.11.5 IP -> Tel Routing

Calls from IP network can be routed to port or port group of the device through IP -> Tel Routing.

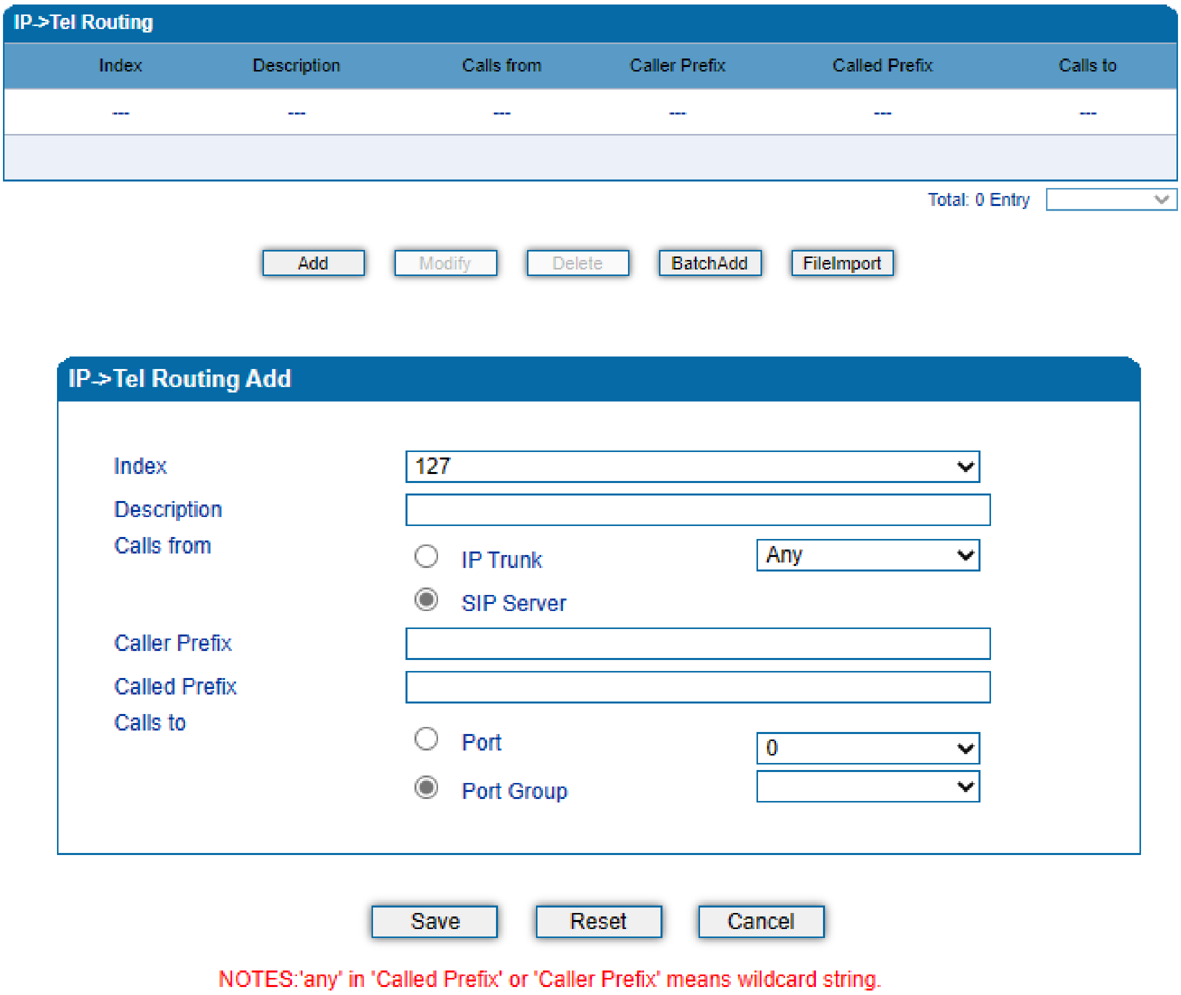


Figure 3.11-5 Configuration Interface for IP -> Tel Routing Parameter

Explanation of IP -> Tel routing Parameters:

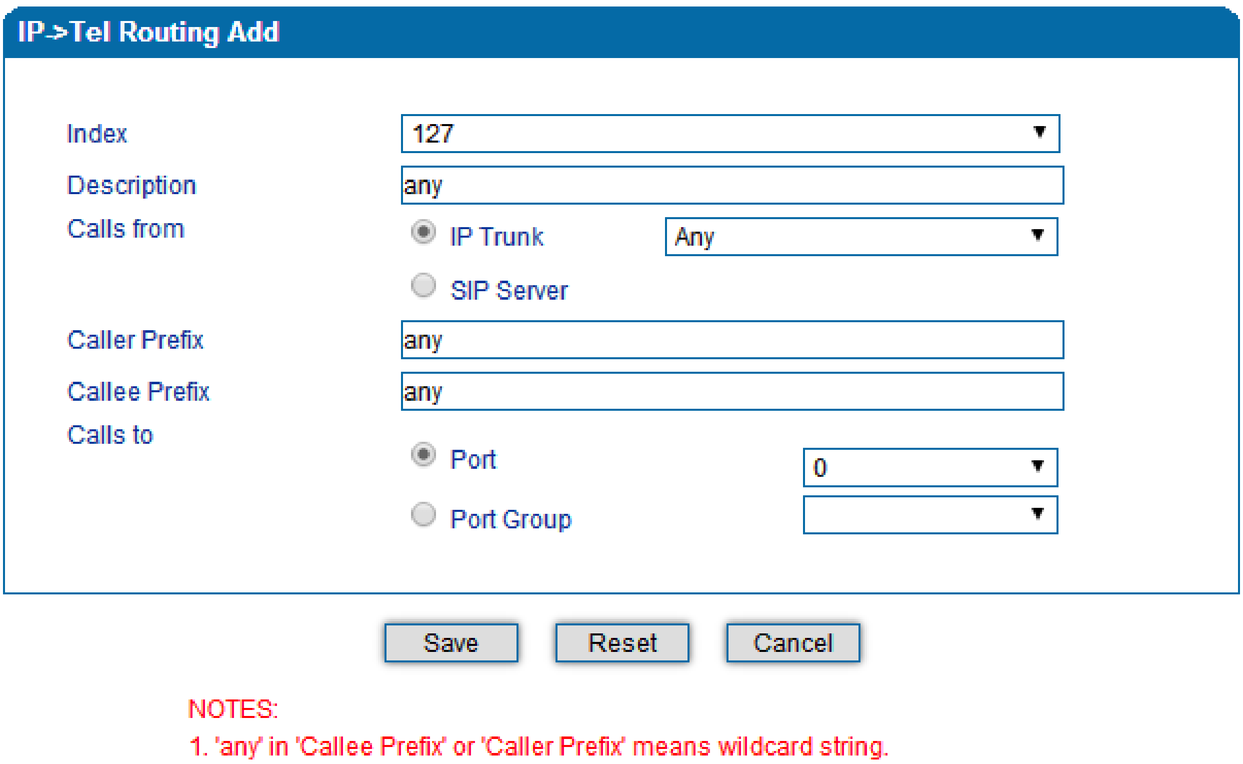
Parameter	**Explanation**
Index	Index of the IP →Tel routing; range is from 0 to127; 0 is the highest priority.
Description	Description of the IP →Tel routing is used to identify the IP → Tel routing.
Calls from	Chosen calls from IP trunk or SIP server; 'any' means any IP addresses.

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.
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	Which port or port group to which calls are routed.

Routing Rule Examples

Route any calls from any IP to specific port

After entering the Web interface, click **Call & Routing → IP-Tel Routing** in the navigation tree on the left, and then click **Add** to create a new routing rule.

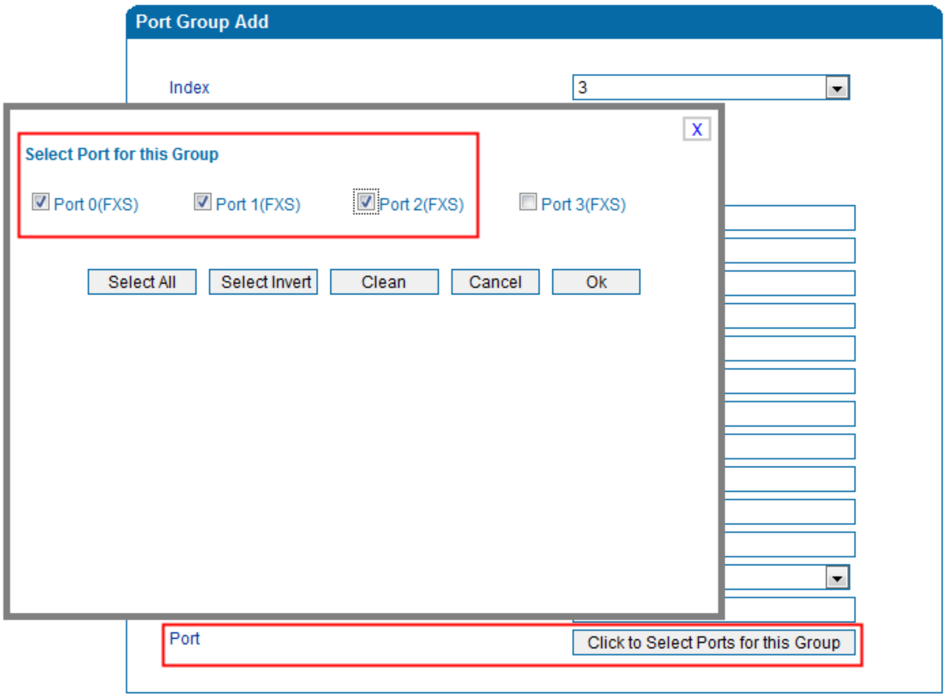


In the example above, all calls will be routed to port 0 when the routing rule is matched.

Route any calls from any IP to specified port group

▶Create port group

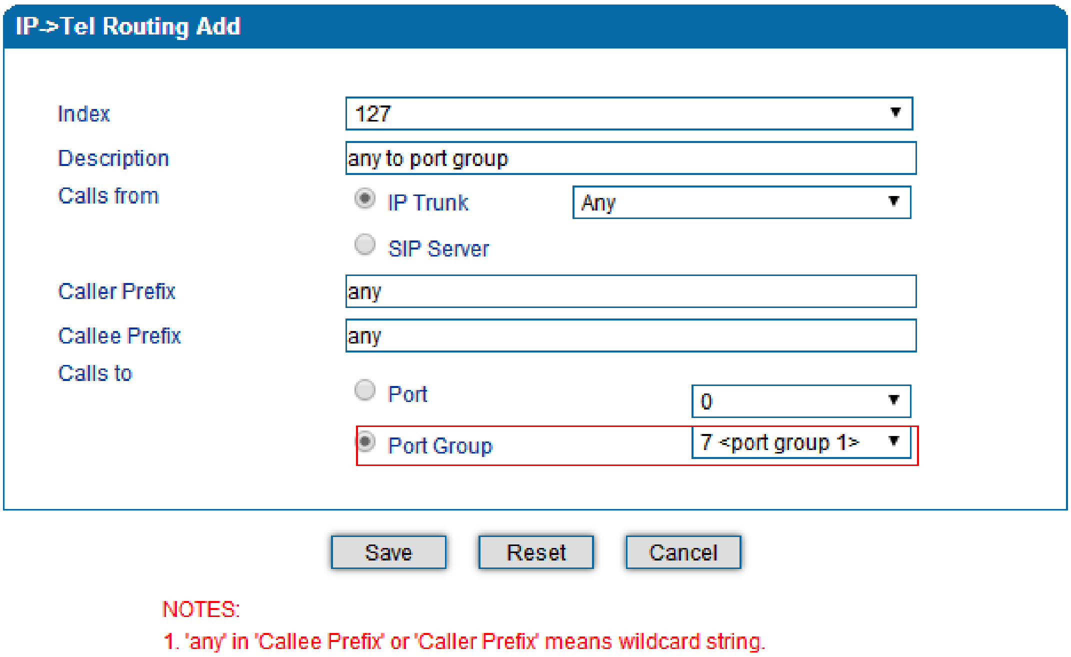
Before we can route calls to a port group, create the port group first as shown below. On the **Call & Routing → Port** Group, click **Add** to create a new port group.



Port 0 to port 2 are assigned to port group 7.

▶Route any calls to the port group

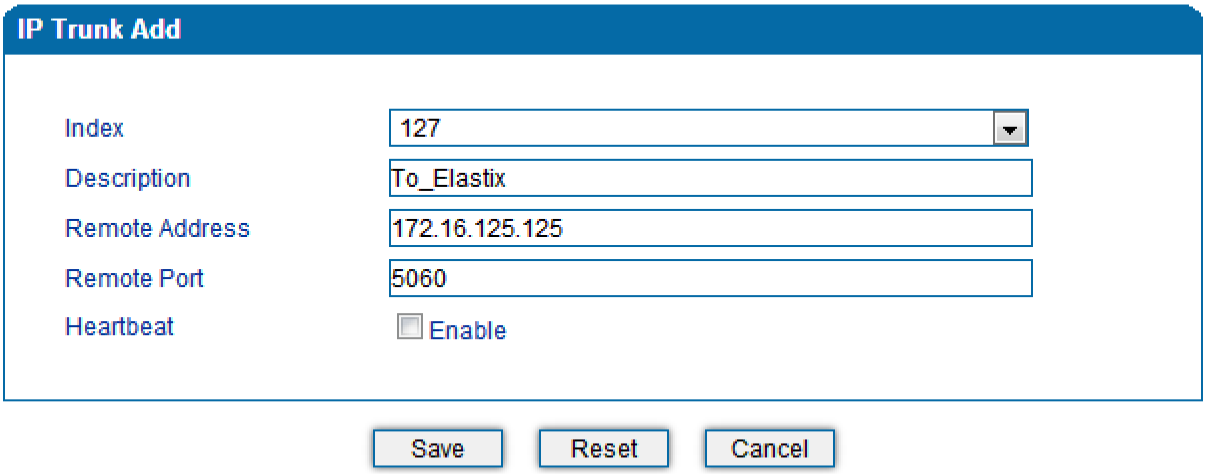
On the **Call & Routing → IP-Tel Routing** interface, click **Add** to create a new routing rule.



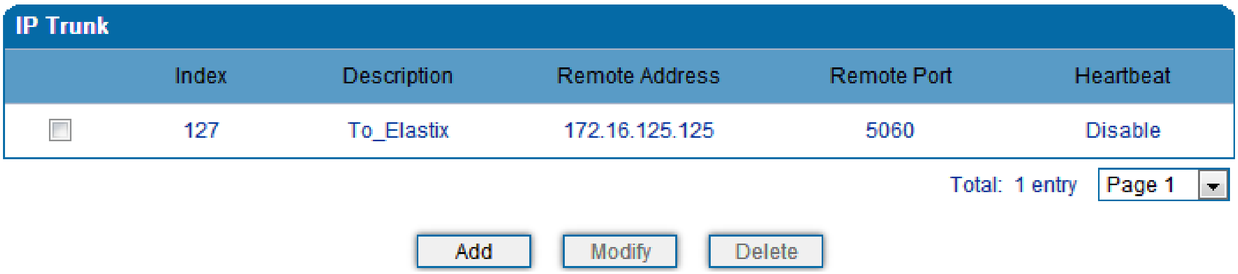
As shown above, if the routing rule is matched, calls will be routed to port group 7.

Route any calls from any port to specific SIP IP trunk

Create IP Trunk on the **Call & Routing → IP Trunk** interface:



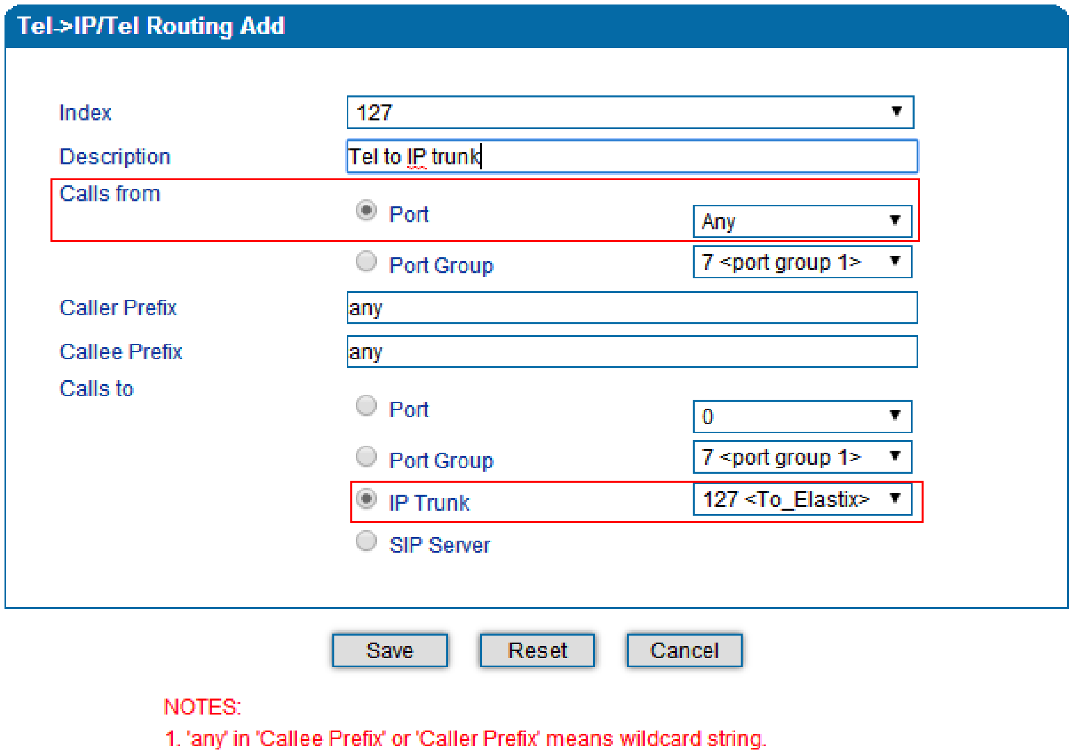
After IP Trunk is created, check the following configuration:



As shown above, the IP trunk is created, and the remote end IP address is 172.16.125.125, the SIP port is 5060.

Create Tel -> IP routing rule

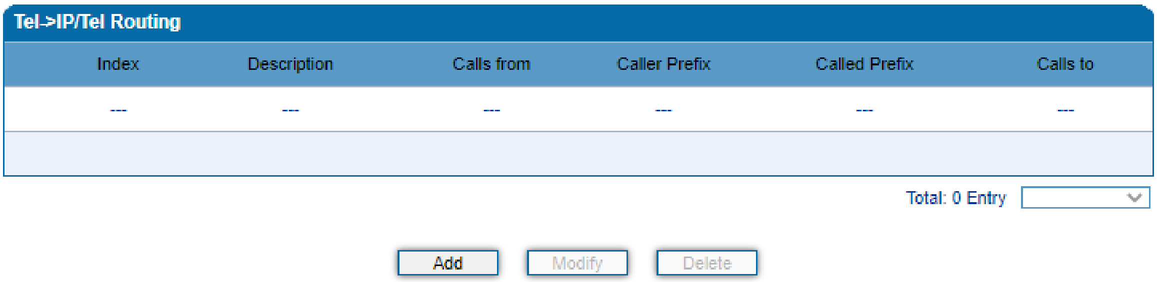
On the **Call & Routing →Tel-IP Routing** interface, click “Add” to create a new Tel → IP routing rule.



All Tel calls from any caller number to any called number will be routed to IP trunk 127.

3.11.6 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.



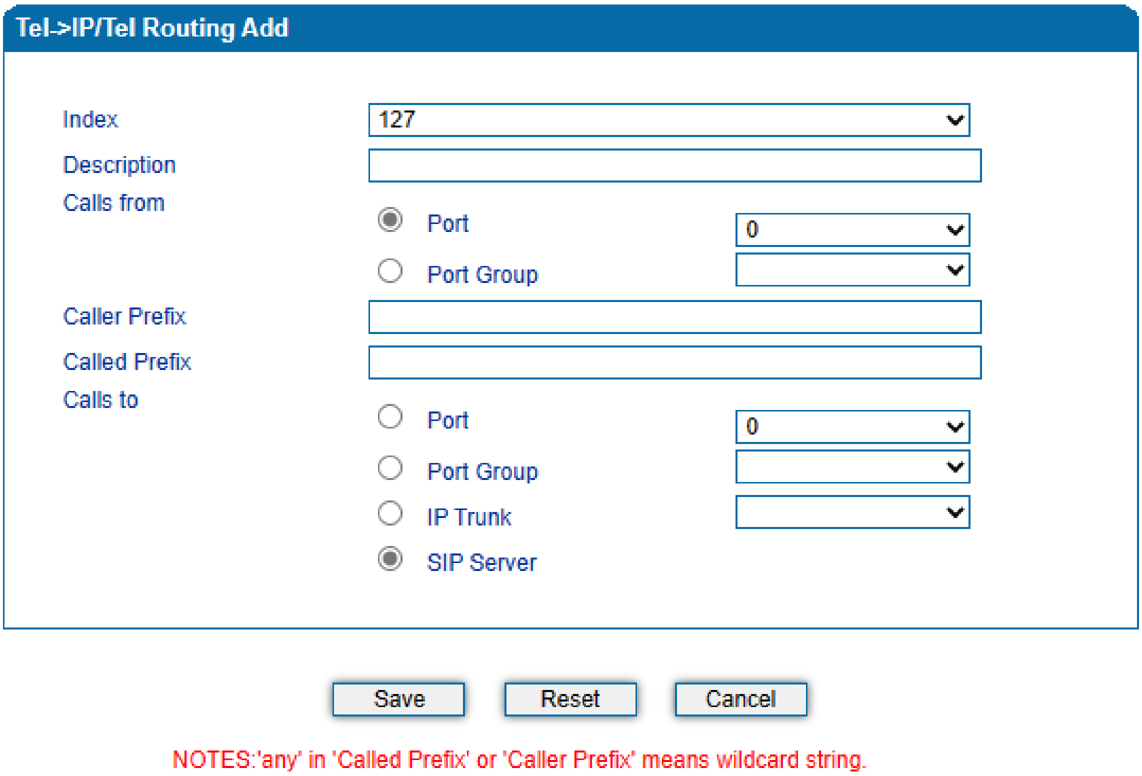


Figure 3.11-6 Configuration Interface for Tel -> IP/Tel Routing Parameter

Explanation of Tel -> IP/Tel Routing Parameters:

Parameter	Explanation
Index	The index of this Tel →IP/Tel routing ranges 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 is used to identify the routing.
Calls From	Chosen 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	Chosen calls are routed to a port, port group, IP trunk or SIP server.

Note

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.

3.11.7 Call Limit

Call Limit from the Call & Routing can add the Call Limit parameters.

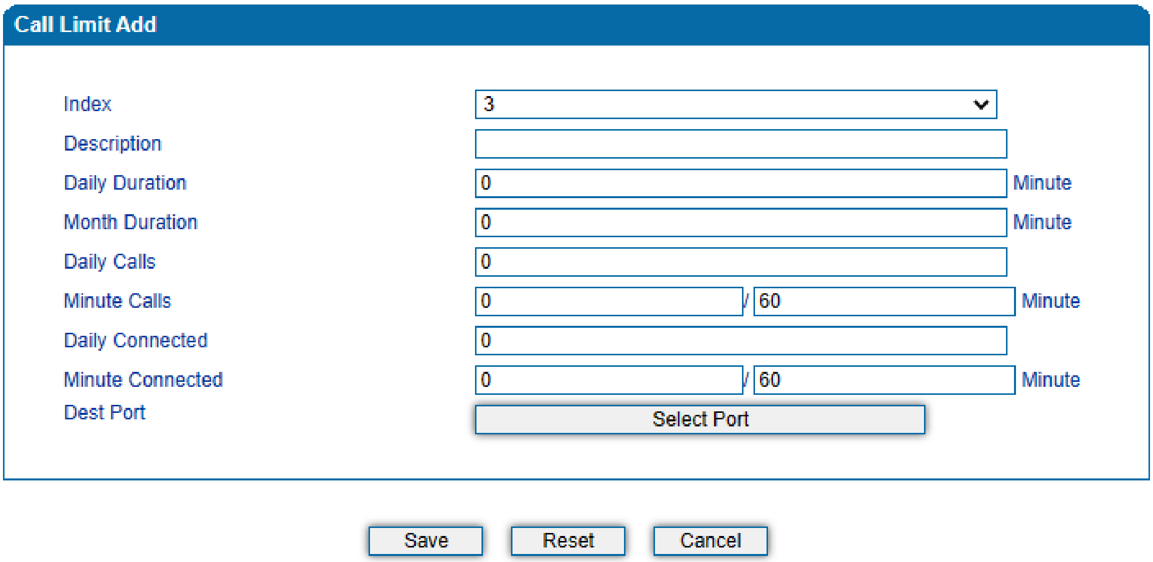


Figure 3.11-7 Configuration Interface for Call Limit Parameter

Explanation of Call Limit Parameters:

Parameter	Explanation
Index	The index of call limit.
Description	The description of this call limit is used to identify the limit.
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 min. connected calls. The times of calls made in minute.
Dest Port	Select the port that needs to be call limit.

3.12 Manipulation Configuration

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 preset rules.

3.12.1 IP -> Tel Called

On the IP -> Tel called submenu page, user can set rules for manipulating the called number of IP -> Tel calls.

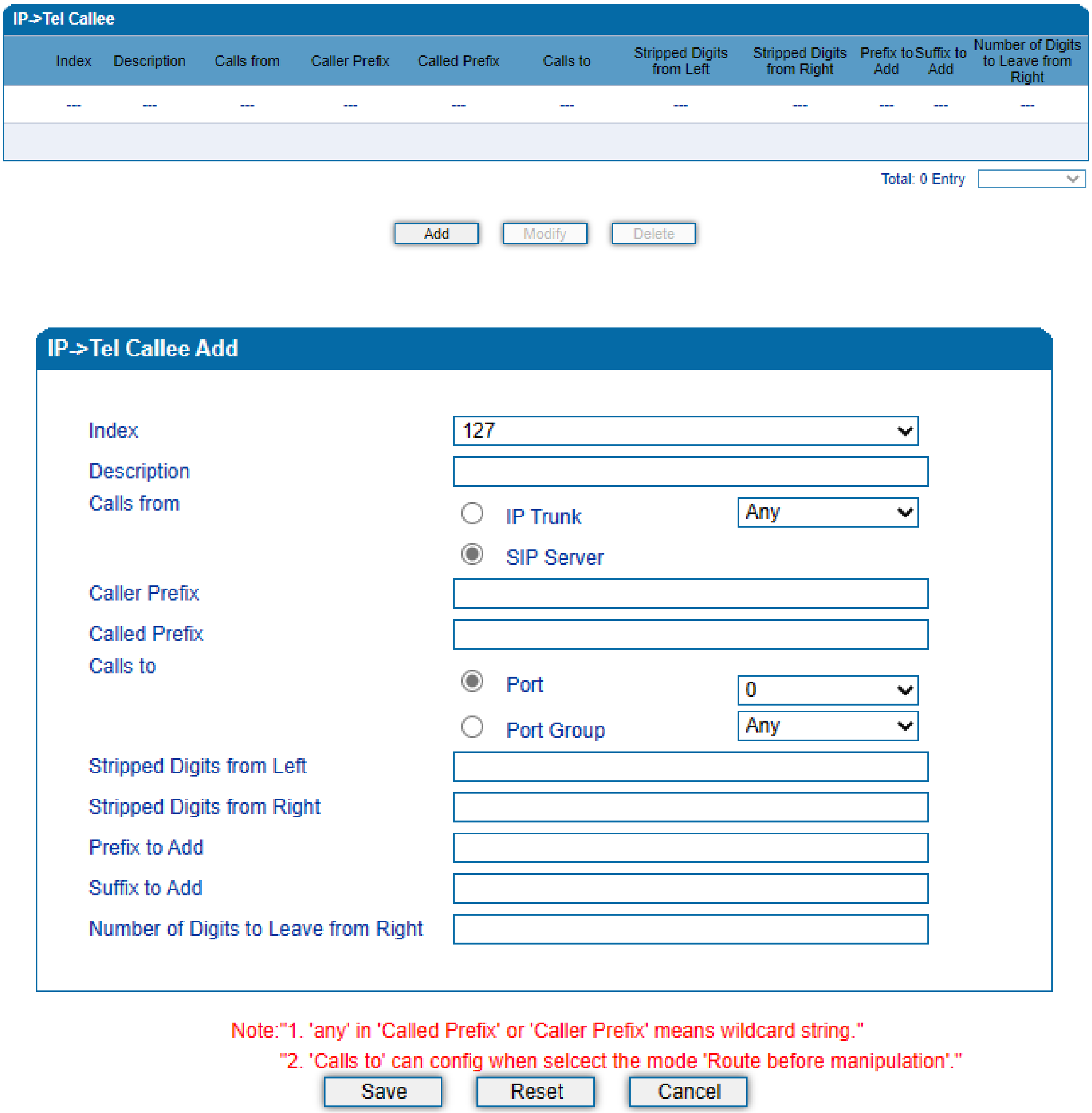


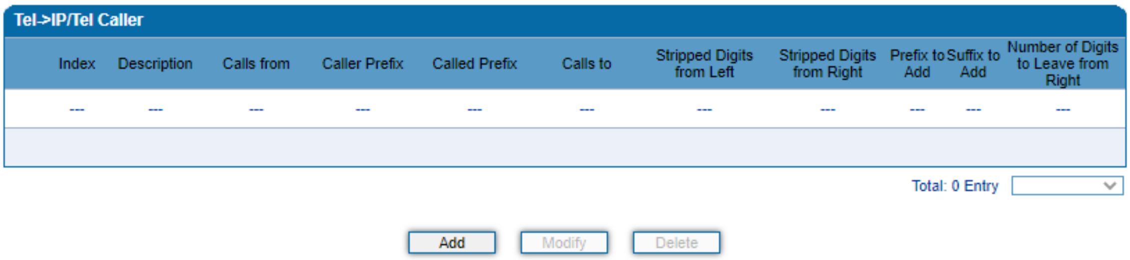
Figure 3.12-1 Configuration Interface for IP -> Tel Called Parameter

Explanation of IP -> Tel Called Parameters:

Parameter	Explanation
Index	The index of this manipulation ranges from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority.
Description	Description of this manipulation 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 is reduced from the left of the called number.
Stripped Digits from Right	The number of digits is reduced from the right of the called number.
Prefix to Add	The prefix added to the called number after its digits are reduced.
Suffix to Add	The suffix added to the called number after its digits are reduced.
Number of Digits to Leave from Right	For an incoming call, reserved digits from called number, starting count numbers from right of called number.

3.12.2 Tel -> IP/Tel Caller

On the Tel -> IP/Tel caller page, user can set rules for manipulating the caller number of Tel -> IP/Tel calls.



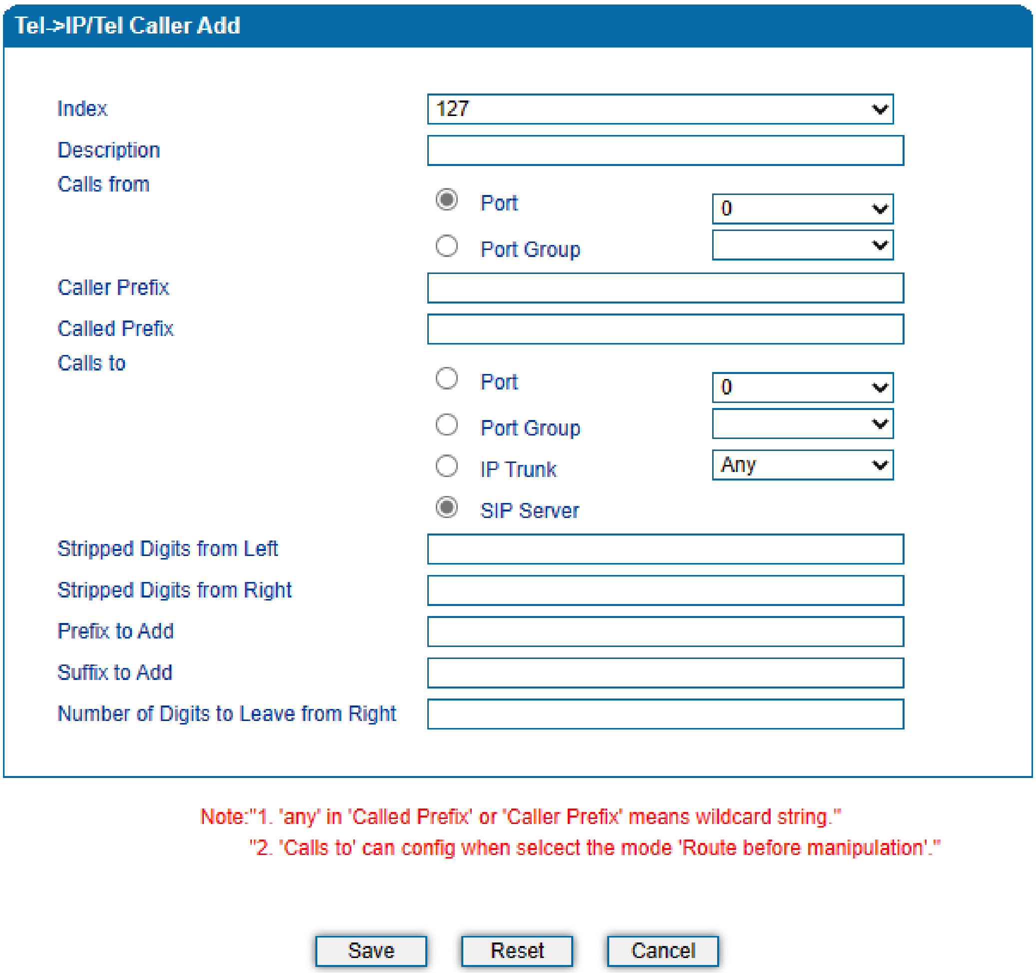


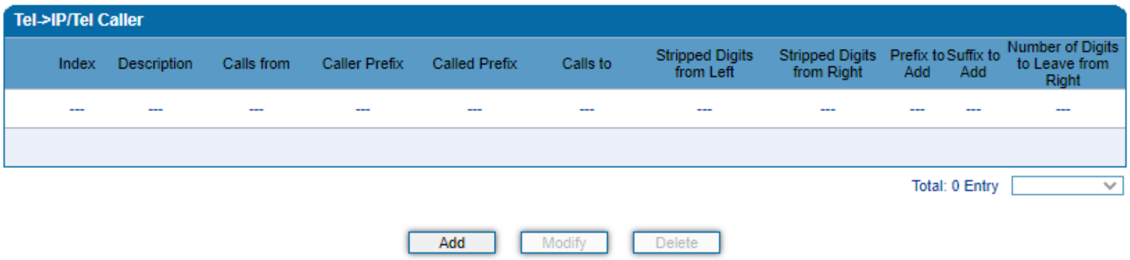
Figure 3.12-2 Configuration Interface for Tel -> IP/Tel Caller Parameter

Explanation of Tel -> IP/Tel Caller Parameters:

Parameter	Explanation
Index	The index of this manipulation ranges from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority.
Description	Description of this manipulation 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 is reduced from the left of the caller number.
Stripped Digits from Right	The number of digits is reduced from the right of the caller number.
Prefix to Add	The prefix added to the caller number after its digits are reduced.
Suffix to Add	The suffix added to the caller number after its digits are reduced.
Number of Digits to Leave from Right	For an incoming call, reserved digits from called number, starting count numbers from right of called number.

3.12.3 Tel -> IP/Tel Called

On the Tel -> IP/Tel called page, user can set rules for manipulating the called number of Tel -> IP/Tel calls.



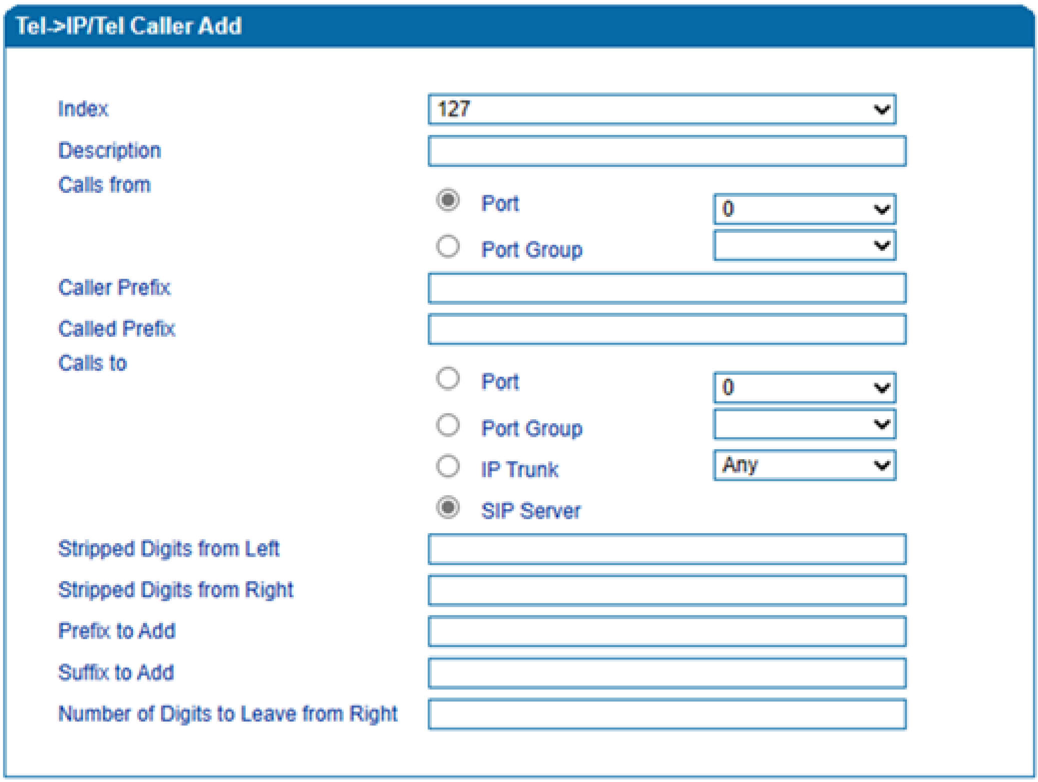


Figure 3.12-3 Configuration Interface for Tel -> IP/Tel Caller Parameter

Explanation of Tel -> IP/Tel Called Parameters:

Parameter	Explanation
Index	The index of this manipulation ranges from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority.
Description	Description of this manipulation 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 is reduced from the left of the caller number.
Stripped Digits from Right	The number of digits is reduced 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 reduced.
Number of Digits to Leave from Right	For an incoming call, reserved digits from called number, starting count numbers from right of called number.

3.13 Management

3.13.1 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.

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.

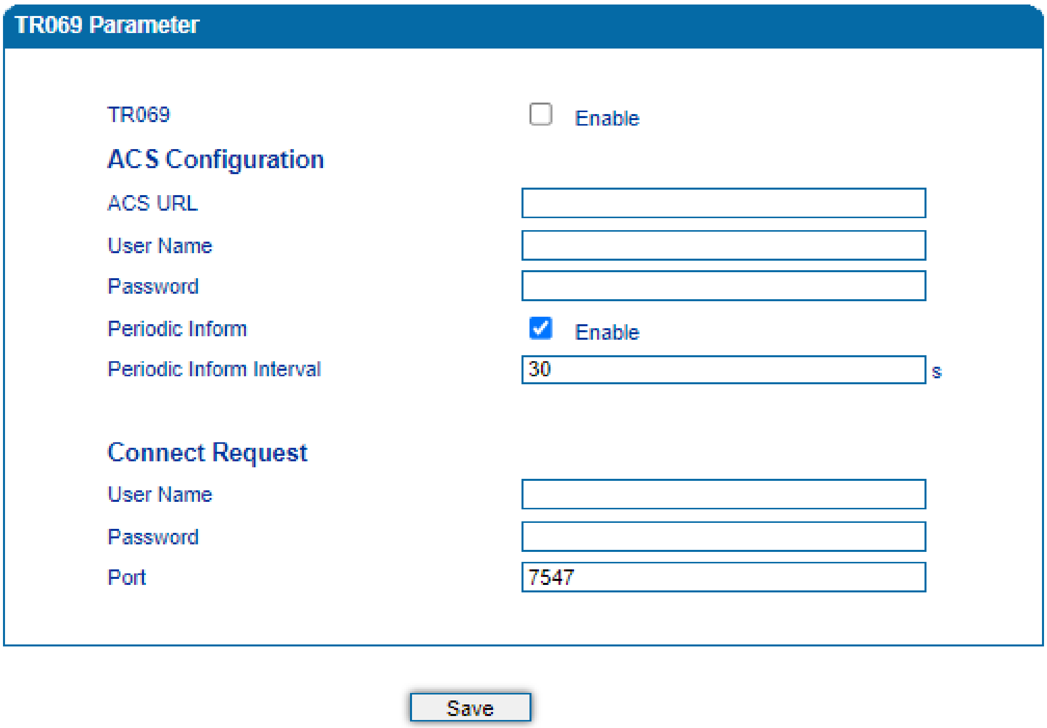


Figure 3.13-1 Configuration Interface for TR069 Parameter

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.

3.13.2 SNMP (Simple Network Management Protocol)

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.

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.

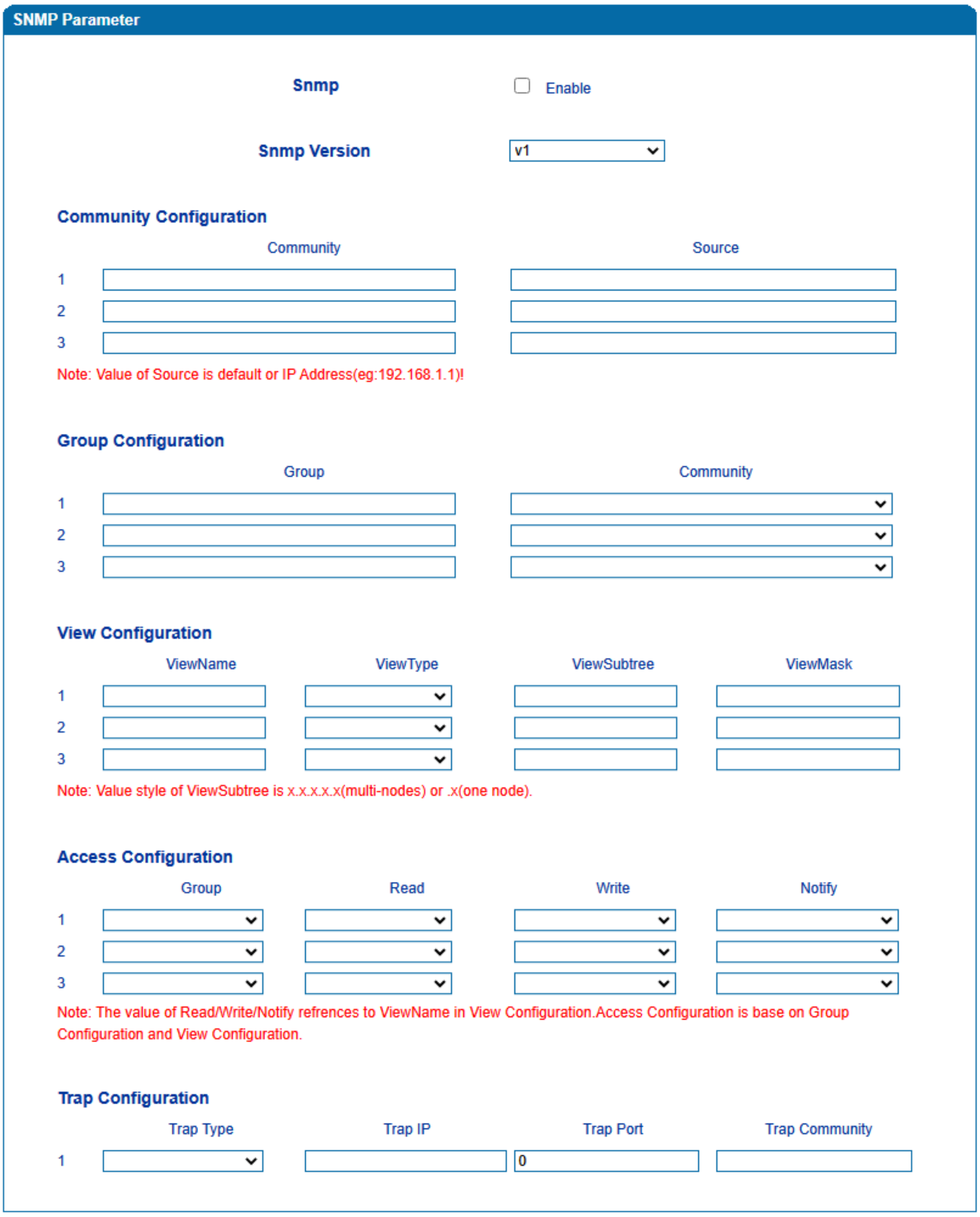
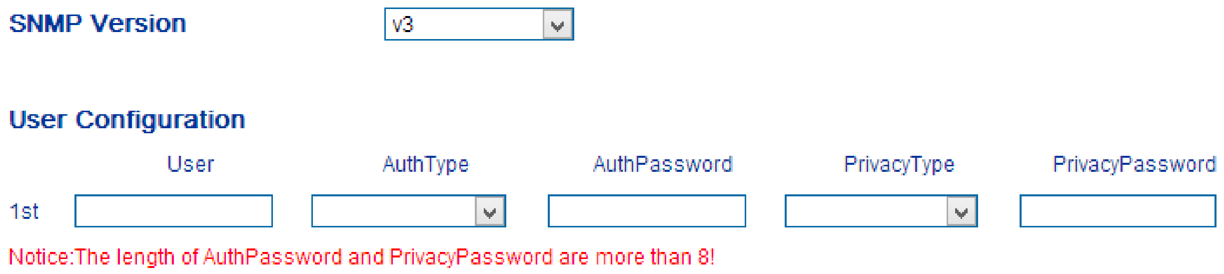


Figure 3.13-2 Configuration Interface for SNMP Parameter

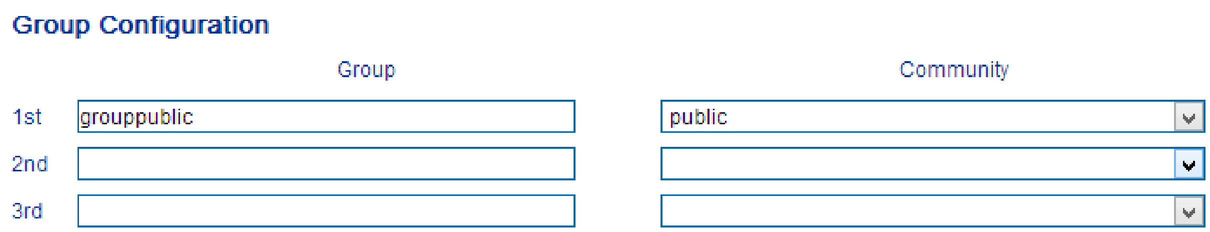
User configuration is only available on SNMP v3.



Group configuration

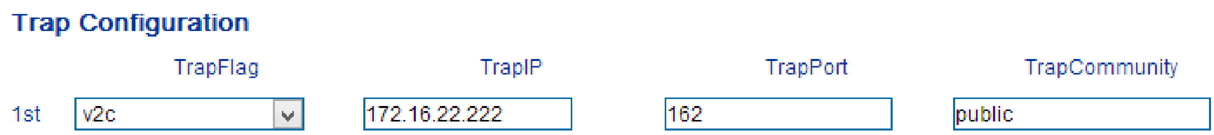
Group: community group name which consist of character string.

Community: let community join the community group which configured above.



Trap configuration

Trap configuration is enabled to configure Trap Server IP and port. This setting is available for SNMP v2c and v1.



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.

3.13.3 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 issue or performance.

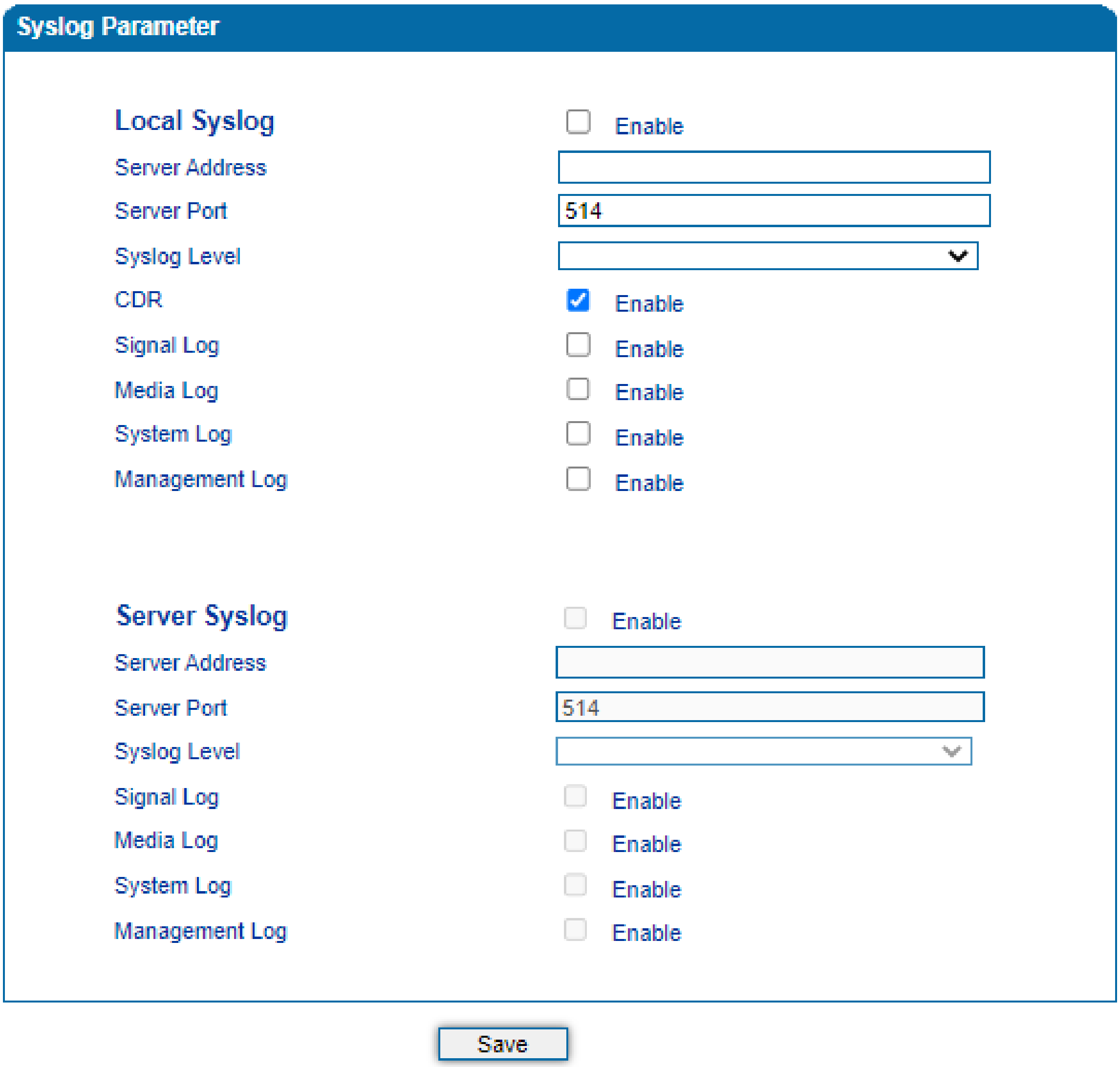


Figure 3.13-3 Configuration Interface for Syslog Parameter

3.13.4 Provision

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

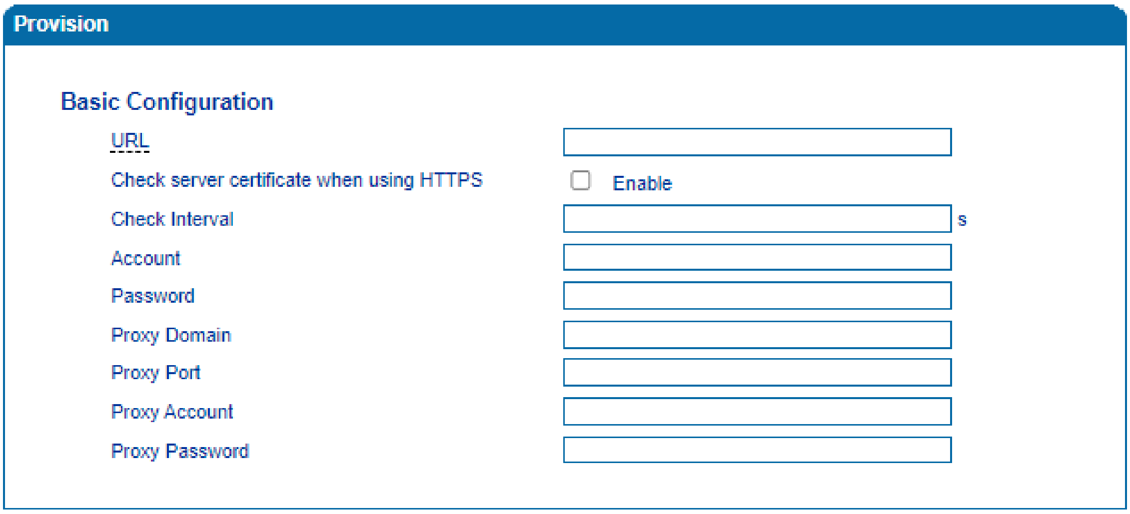


Figure 3.13-4 Configuration Interface for Provision Parameter

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.

3.13.5 Cloud Server

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

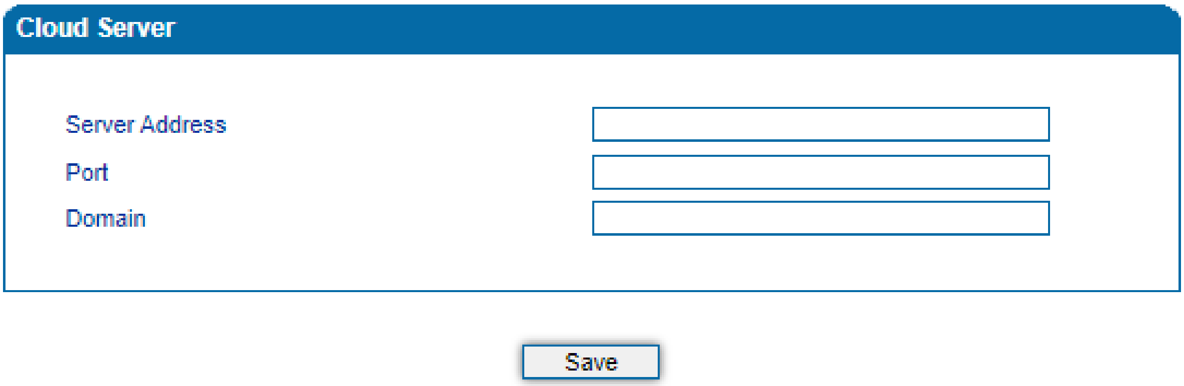


Figure 3.13-5 Configuration Interface for Cloud Server Parameter

Explanation of Cloud Server Parameters:

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.

3.13.6 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.

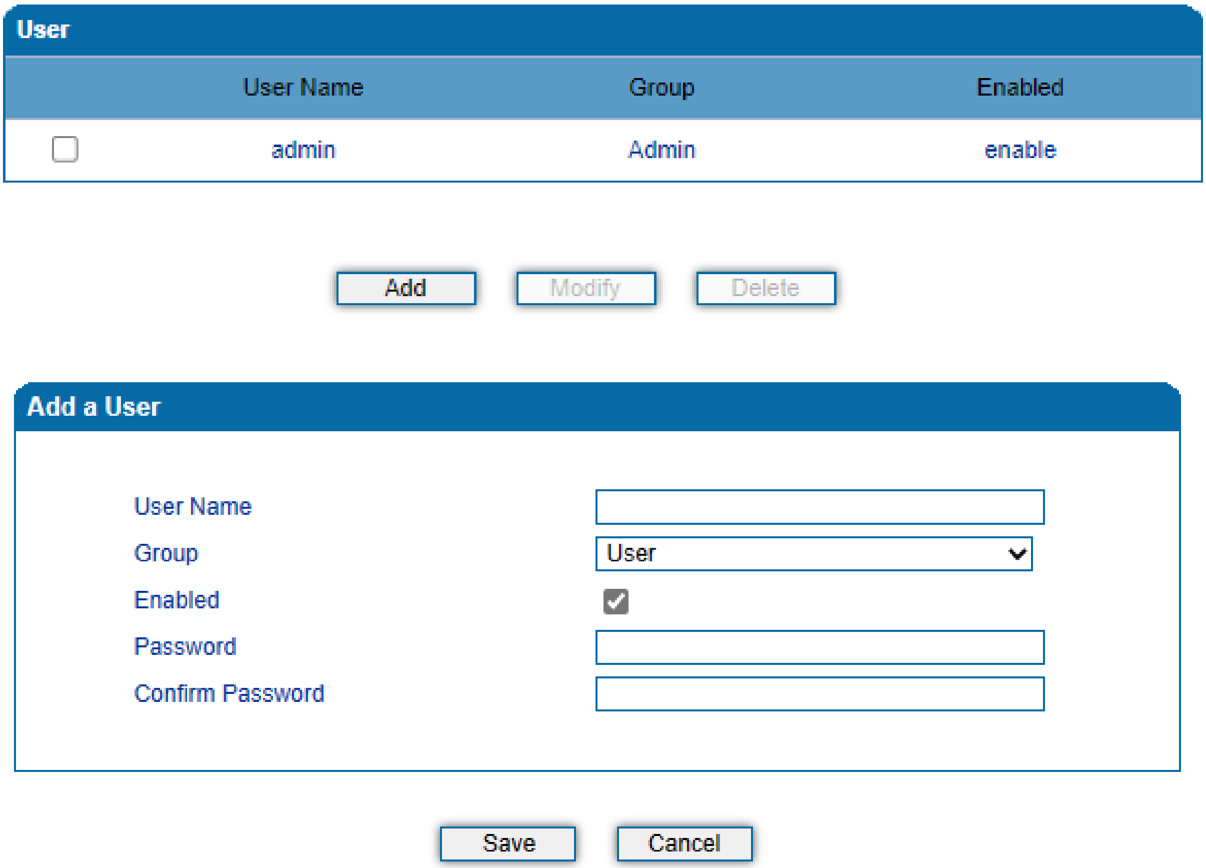


Figure 3.13-6 Configuration Interface for User Manage Parameter

Explanation of User Manage Parameters:

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

3.13.7 Remote Server

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

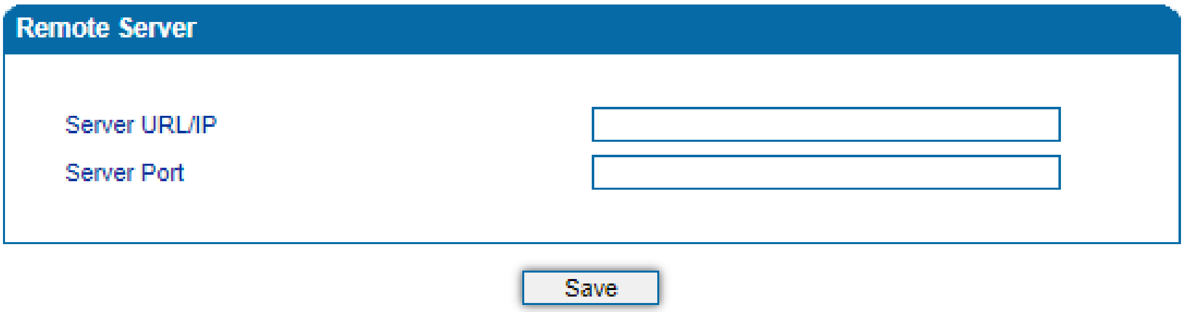


Figure 3.13-7 Configuration Interface for Remote Server Parameter

Explanation of Remote Server Parameters:

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

3.13.8 Record Parameter

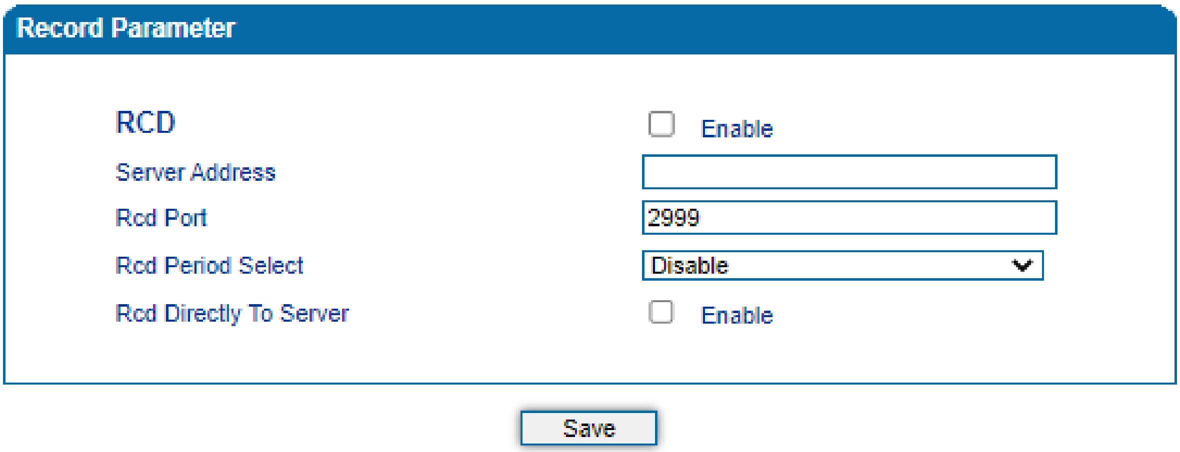


Figure 3.13-8 Configuration Interface for Record Parameter

Explanation of Record Parameters:

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.

3.13.9 RADIUS Parameter

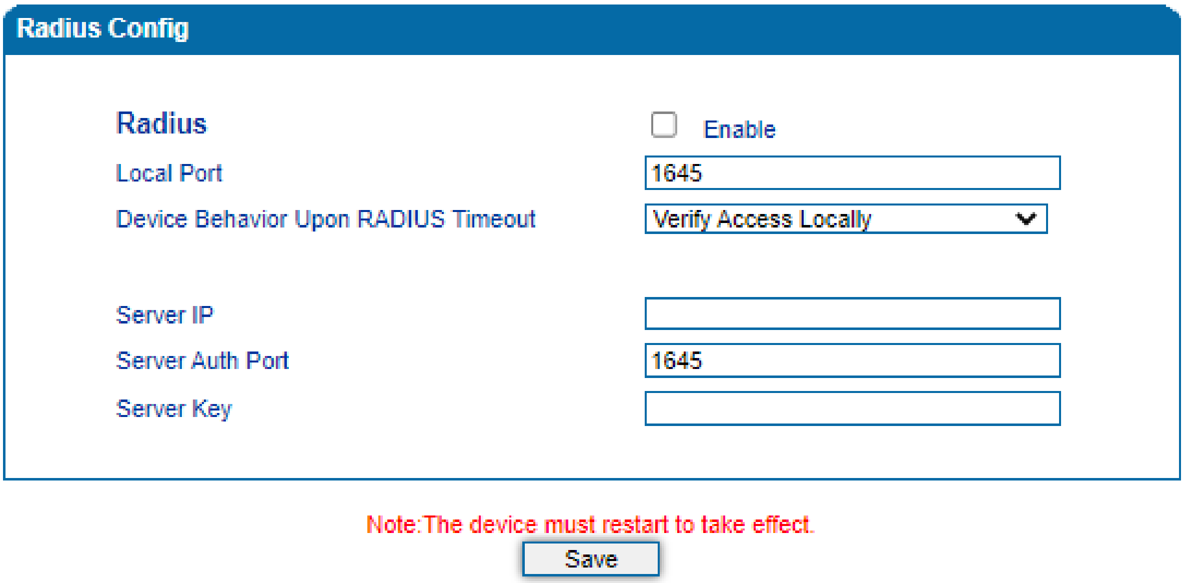


Figure 3.13-9 Configuration Interface for RADIUS Parameter

Explanation of RADIUS Parameters:

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.

3.13.10 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, and IP address) carried in GET request can also be reported to VoIP platform/VoIP server.

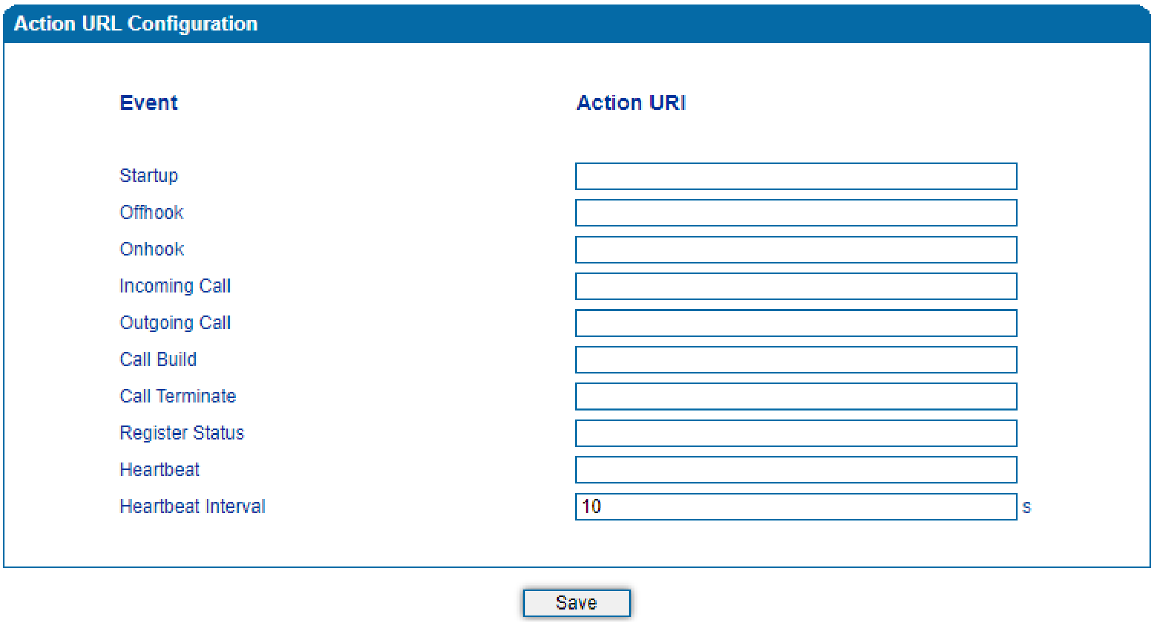


Figure 3.13-10 Configuration Interface for Action URL Parameter

Explanation of Action URL Parameters:

Parameter	Explanation
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.

3.13.11 SIP PNP

The VGW-420FO Gateway can restore or upgrade the system firmware by SIP PNP method. The process of SIP PNP is as follows:

- Gateway sends 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 restoration or upgrade

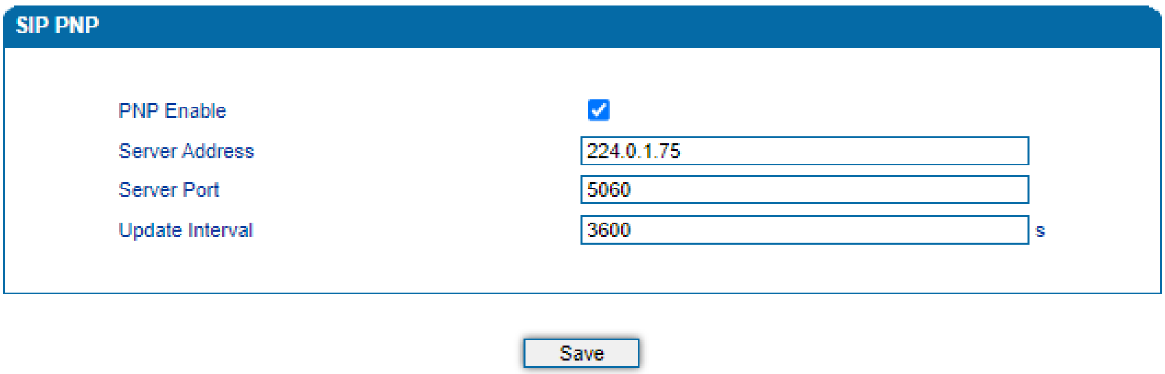


Figure 3.13-11 Configuration Interface for SIP PNP Parameter

Explanation of SIP PNP Parameters:

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

3.13.12 NMS Configuration

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.

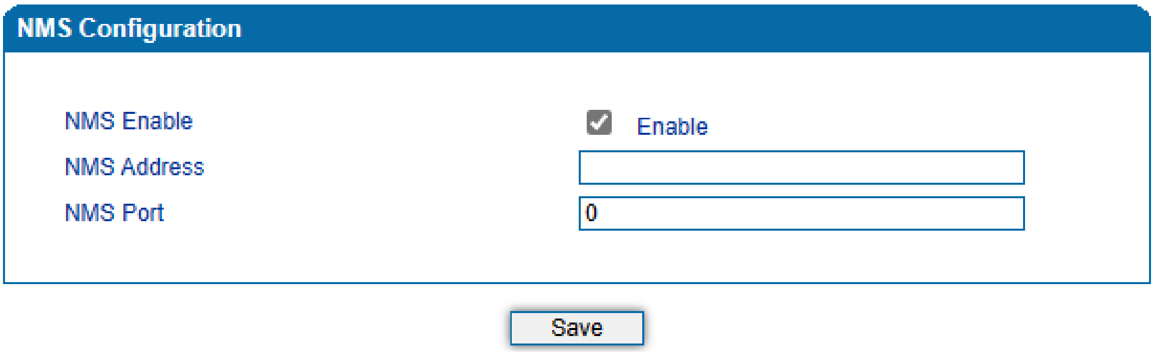


Figure 3.13-12 Configuration Interface for NMS Configuration Parameter

Explanation of SIP PNP Parameters:

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.

3.14 Security

3.14.1 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.

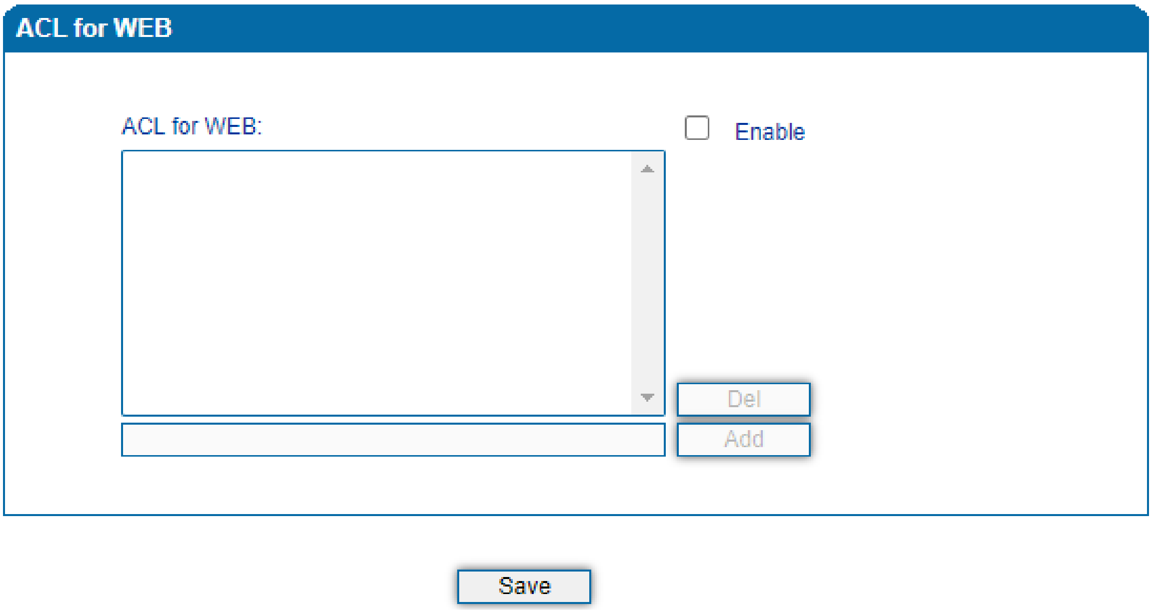


Figure 3.14-1 Configuration Interface for Web ACL Parameter

Explanation of Web ACL Parameters:

Parameter	Explanation
ACL for Web	ACL for Web.
Del	Delete IP address.
Add	Add IP address.

3.14.2 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.

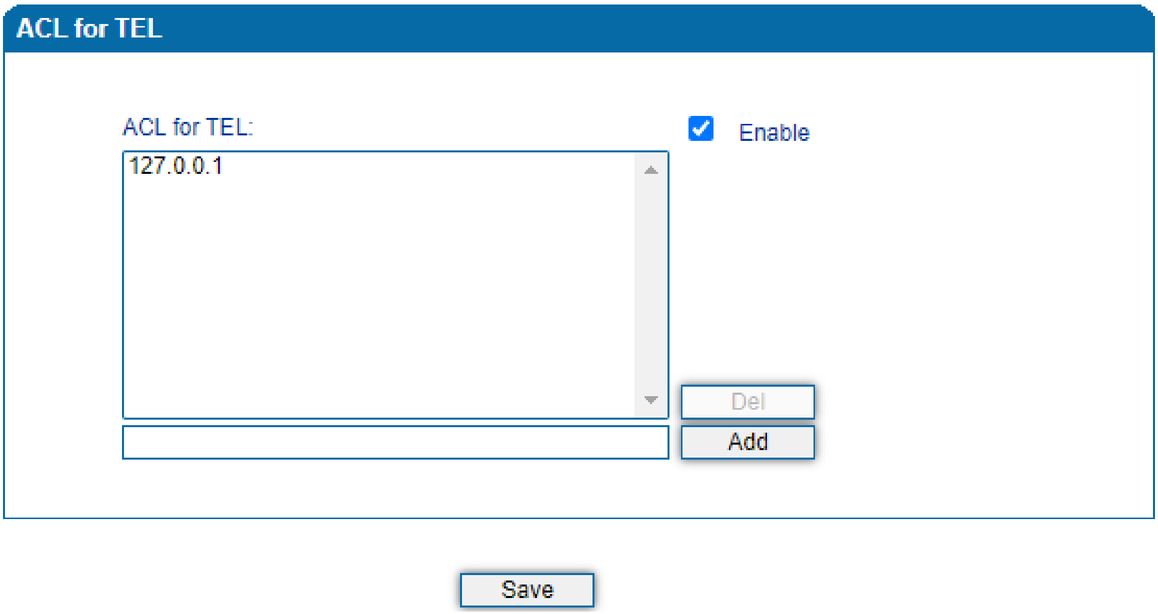


Figure 3.14-2 Configuration Interface for Telnet ACL Parameter

Explanation of Telnet ACL Parameters:

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

3.14.3 Password

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

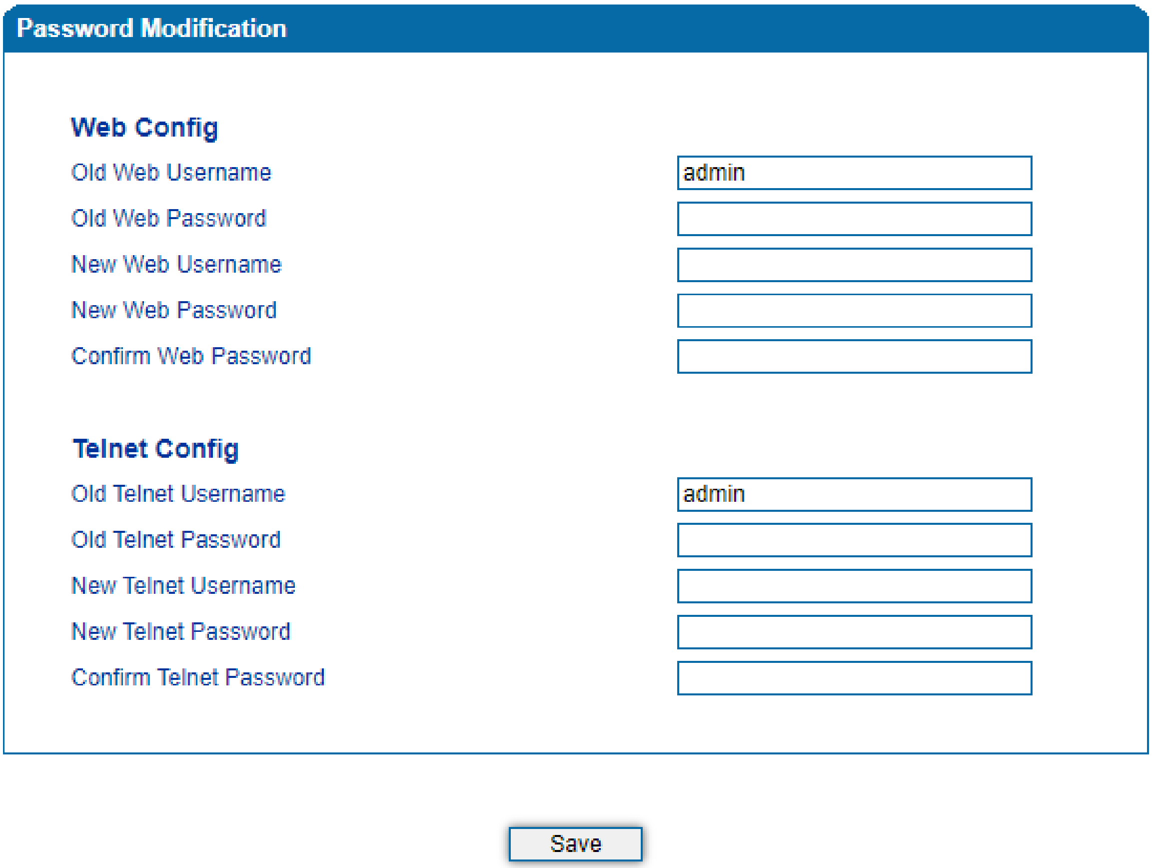


Figure 3.14-3 Configuration Interface for Password Parameter

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

3.14.4 Encrypt

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

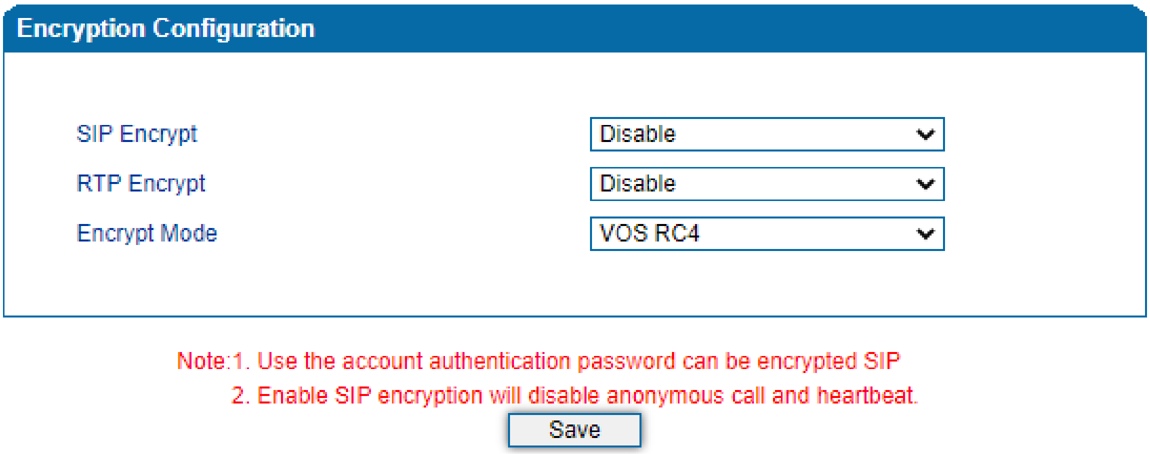


Figure 3.14-4 Configuration Interface for Encrypt Parameter

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

3.15 Tools

3.15.1 Firmware Upload

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

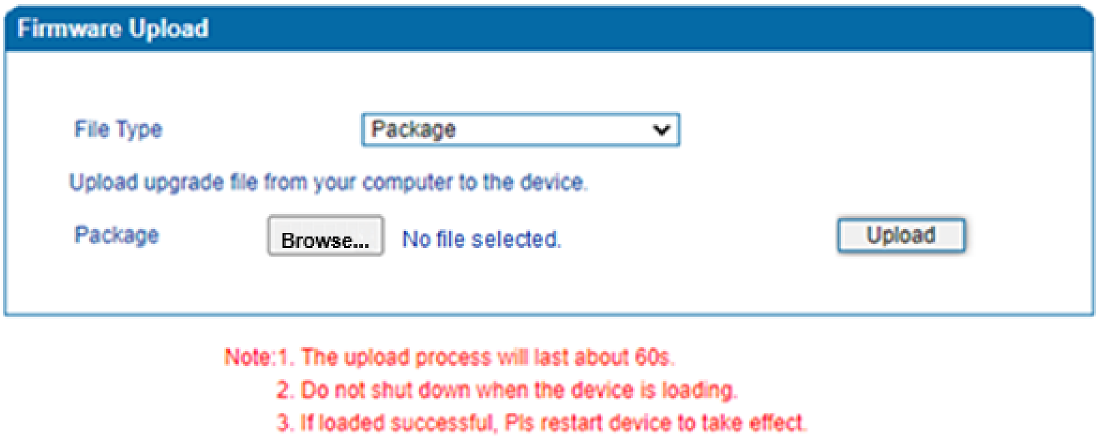


Figure 3.15-1 Configuration Interface for Firmware Upload Parameter

Firmware Uploading Procedure:

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.

3.15.2 Data Backup

On the **Tools → Data Backup** page, user can download and back up configuration data, device status and summary messages on local computer workstation.

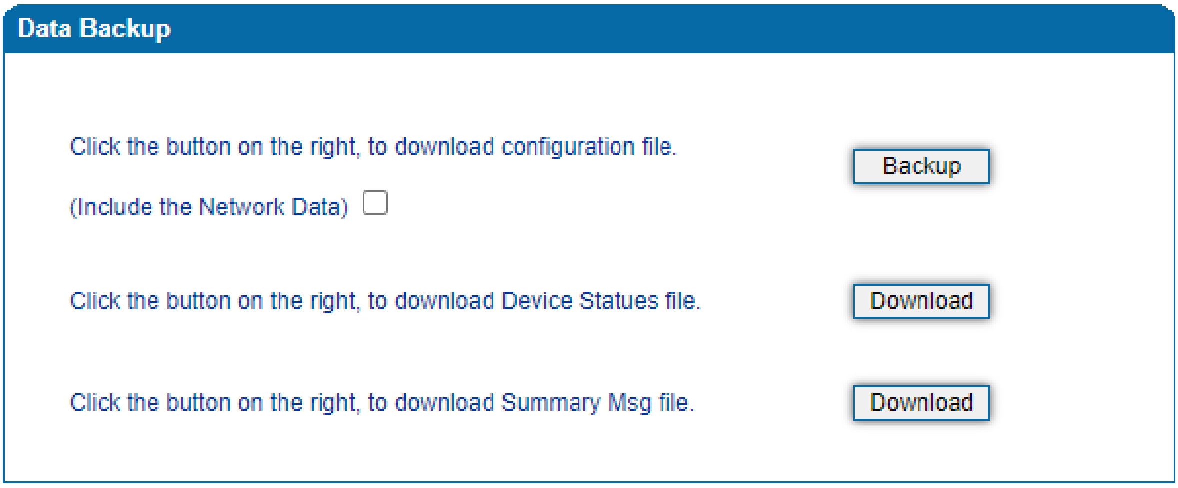


Figure 3.15-2 Configuration Interface for Data Backup Parameter

3.15.3 Data Restore

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

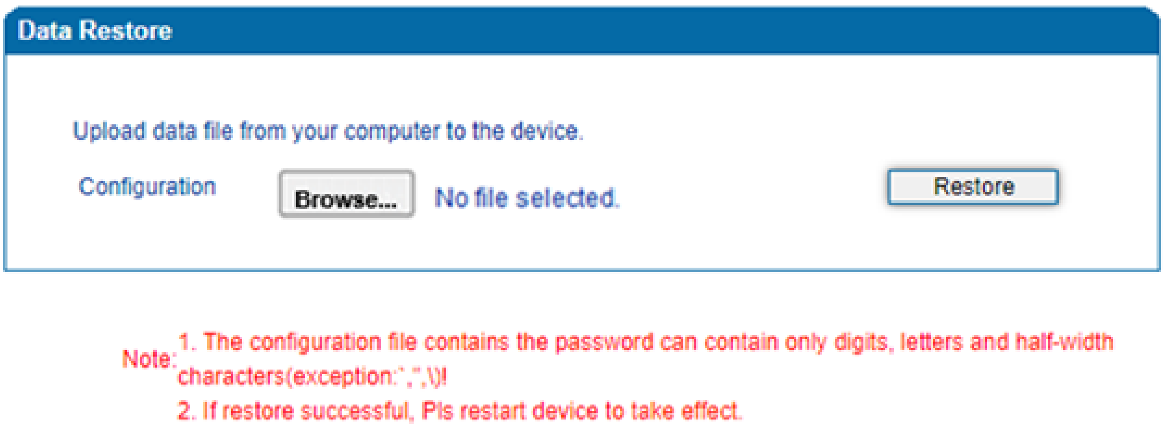


Figure 3.15-3 Configuration Interface for Data Restore Parameter

3.15.4 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.

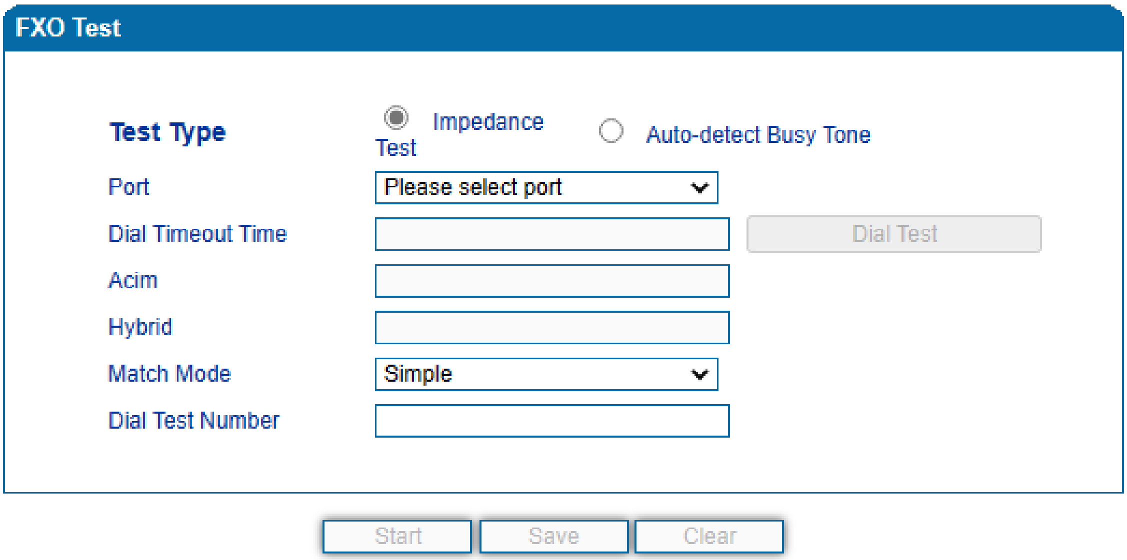


Figure 3.15-4 Configuration Interface for FXO Test Parameter

Explanation of FXO Test Parameters:

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.

Note	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:

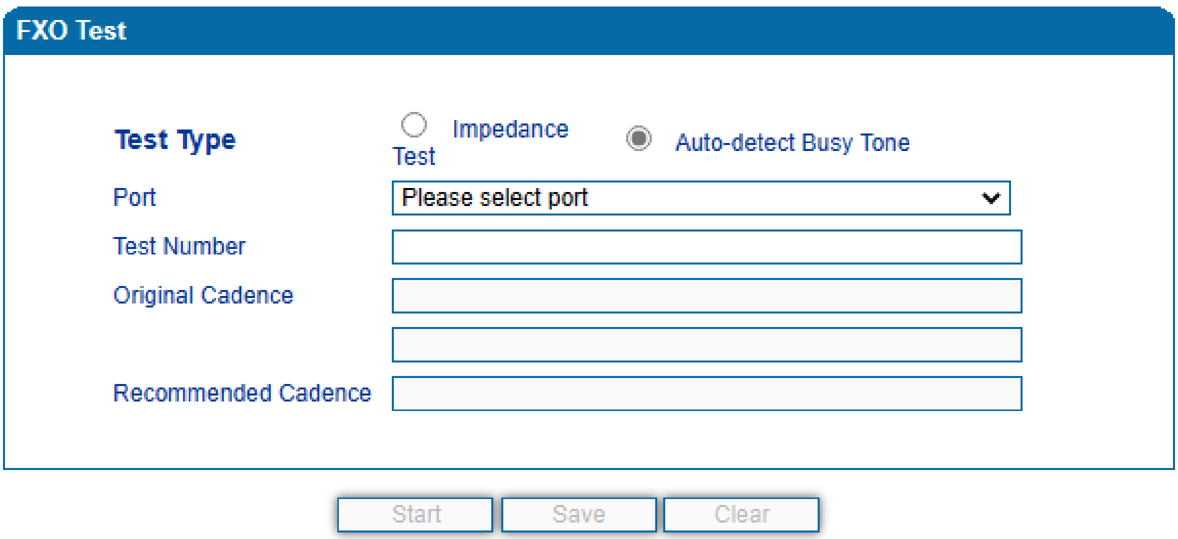


Figure 3.15-4 Configuration Interface for Auto-detect Busy Tone Test Parameter

Explanation of Auto-detect Busy Tone Parameters:

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. It's 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.

3.15.5 Ping Test

Ping is used to examine whether a network works normally 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 normally; otherwise, the network connection is down.

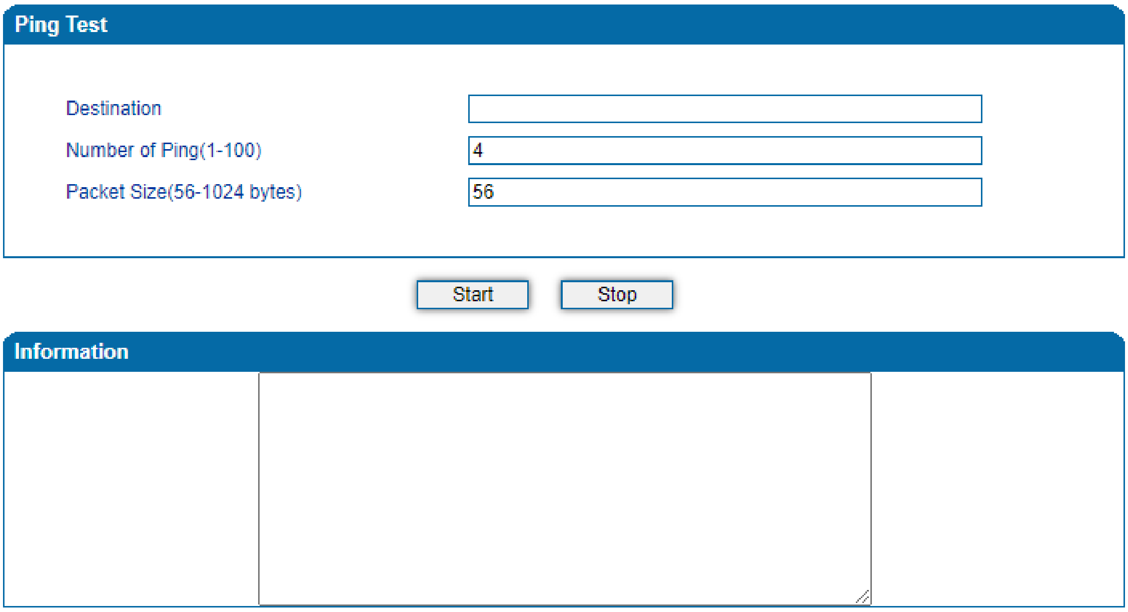


Figure 3.15-5 Configuration Interface for Ping Test Parameter

3.15.6 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**.

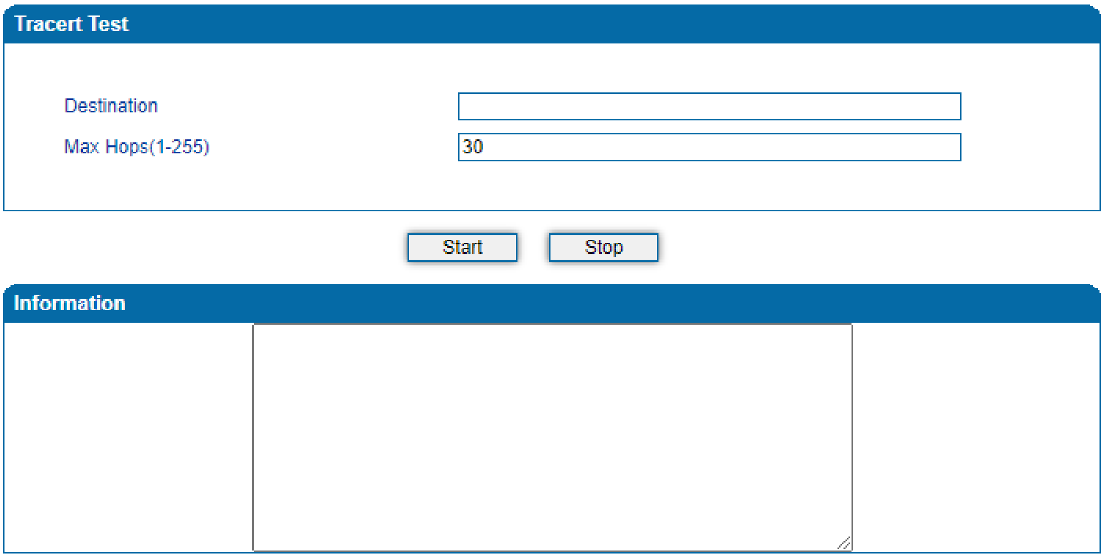


Figure 3.15-6 Configuration Interface for Tracert Test Parameter

Explanation of Tracert Test Parameters:

Parameter	Explanation
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 to 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.

3.15.7 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 analyze voice stream between analog phone and DSP chipset.

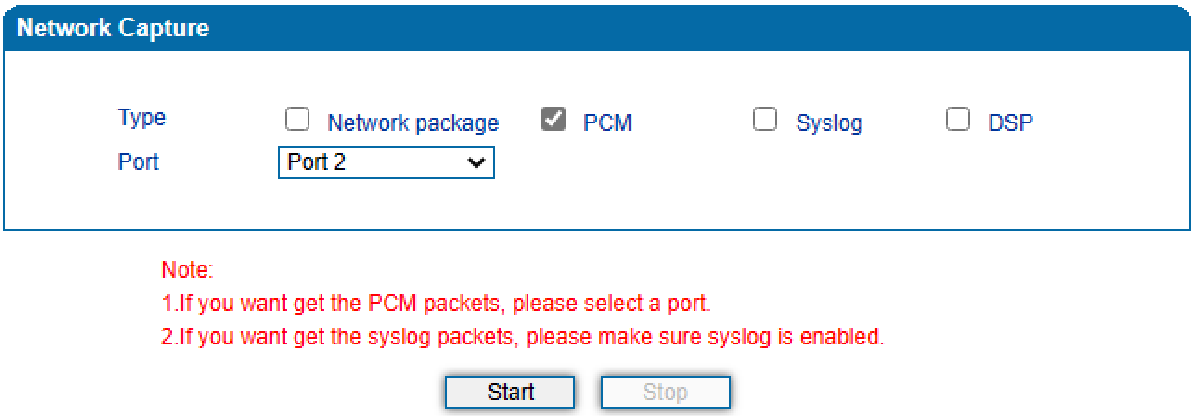


Figure 3.15-7 Configuration Interface for PCM Capture Parameter

PCM Capture Procedure:

- 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 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.

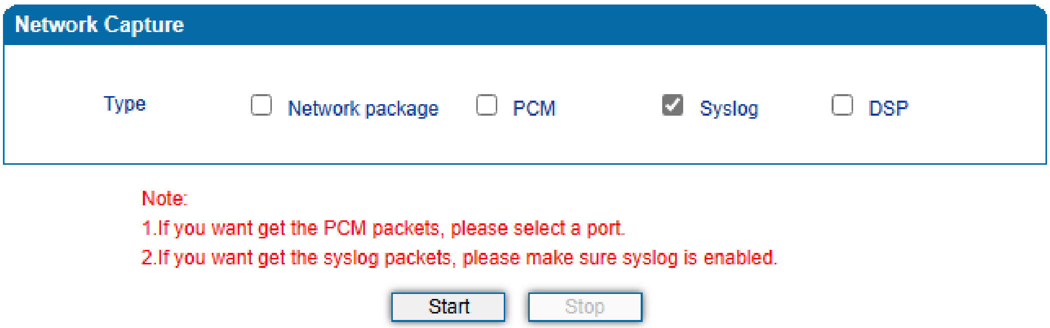


Figure 3.15-7 Configuration Interface for Syslog Capture Parameter

Syslog Capture Procedure:

- 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 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.

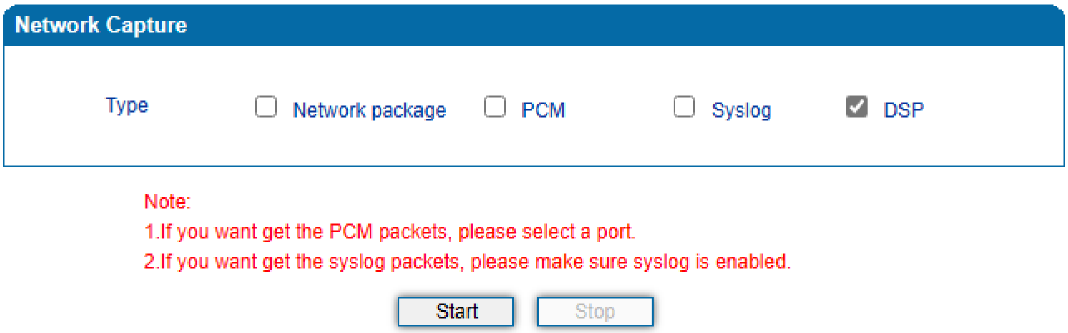


Figure 3.15-7 Configuration Interface for DSP Capture Parameter

DSP Capture Procedure:

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

Customized Capture:

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

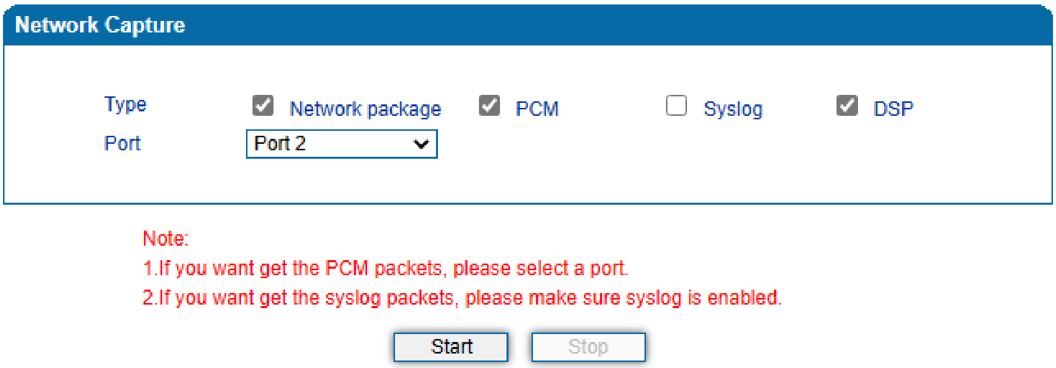


Figure 3.15-7 Configuration Interface for Customized Capture Parameter

3.15.8 Factory Reset

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

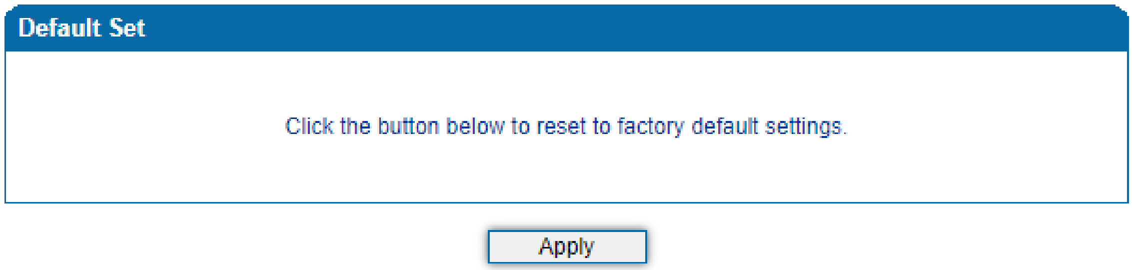


Figure 3.15-8 Configuration Interface for Factory Default Parameter

3.15.9 Device Restart

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

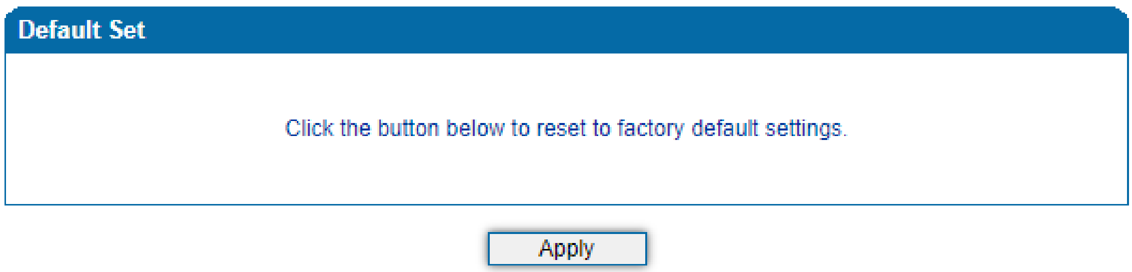


Figure 3.15-9 Configuration Interface for Device Restart Parameter