DAG Series FXO Voice Gateway

User Manual V2.0

Dinstar Technologies Co., Ltd.

Address: Floor 6 Guoxing Building Changxing Road Nanshan District Shenzhen China 518052

Telephone: 86-755-26456664

Fax: 86-755-26456659

Email: sales@dinstar.com, support@dinstar.com

Website: www.dinstar.com

Revision Records

File Name	DAG Series FXO Voice Gateway User Manual
Document Version	2.0
Firmware Version	2.11.08.05
Date	2014/03/16
Revised by	Technical Support Department

Table of Contents

1. Equipment Introduction

1.1 Overview

Thanks for purchasing Dinstar DAG (hereinafter referred to as the DAG) series FXS analog voice gateway.DAG series FXO analog gateway is access gateway based on IP network. It can provide low cost, simple operation VoIP solutions for small enterprise, the family office, remote office and branch enterprise. DAG connects to analog telephone, fax and traditional analog PBX with standard voice interfaces and provided high quality voice service. DAG series VoIP access gateway adopted standard SIP protocol and compatible with leading IP PBX, soft-switch and SIP-based platform. DAG series FXS analog gateway includes following model:

- DAG1000-4O
- DAG1000-8O
- DAG1000-16O

This manual mainly to DAG2000-16O as example, introduce the function of devices and parameter configuration.

1.2 Equipment appearance

Figure 2-1DAG2000-8O

Figure 2-2DAG2000-16O

1.3 Power supply

DAG1000-4/8O is Cassette equipment with placed on desk, and adopts AC 110-240 V power supply, with the power adapter convert to 12VDC power.

Power parameters:

Input: 100-240V, 50-60Hz

Output: 12VDC

Notes: Because power adapter interface is different in different country, please confirm the interface standard with us before shipment.

1.4Network Applications

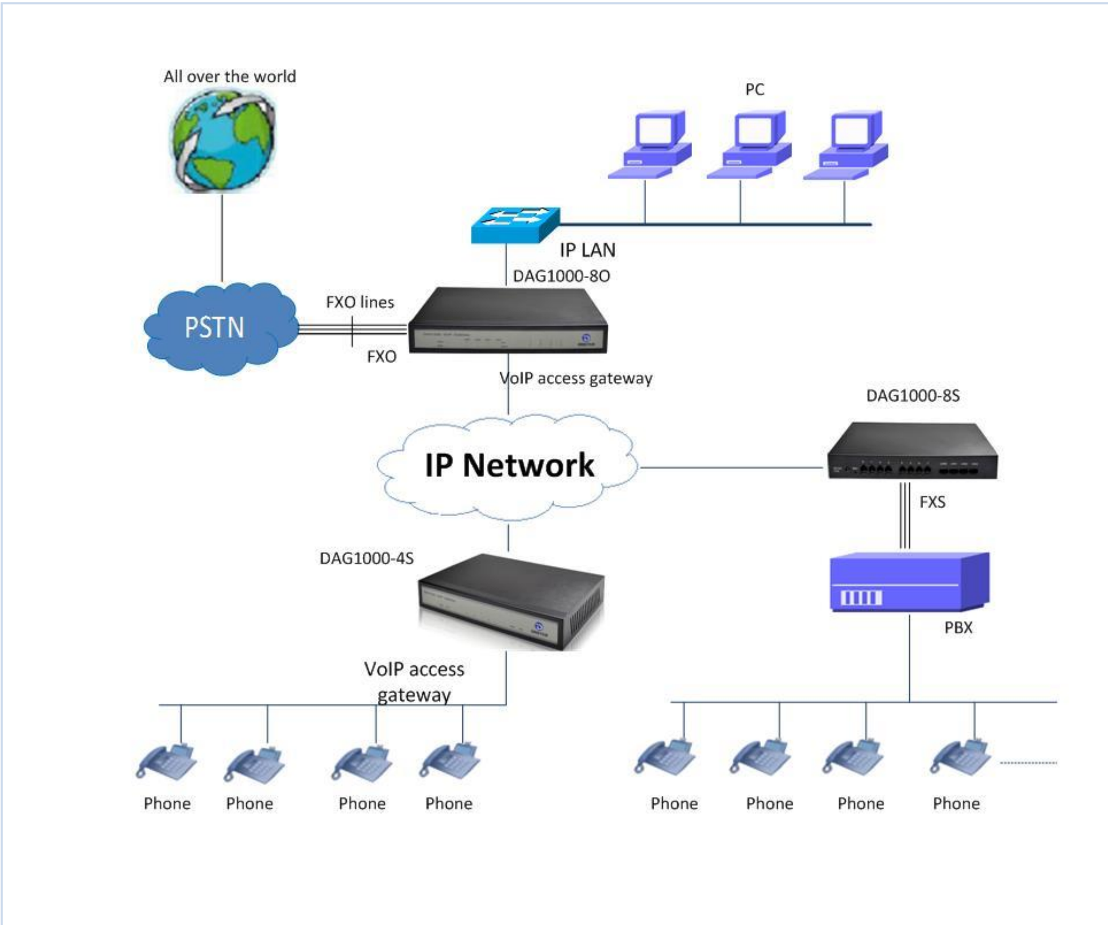


Figure 4-1：Network Applications

1.5 Functions and Features

1.5.1Protocol standard supported

- SIP V2.0 (RFC 3261,3262,3264)
- SDP (RFC 2327)
- REFER (RFC 3515)
- RTP/RTCP (RFC 1889,1890)
- STUN (RFC 3489)
- ARP/RARP (RFC 826/903)
- SNTP (RFC 2030)
- DHCP/PPPoE
- TFTP/HTTP/HTTPS
- DNS/DNS SRV (RFC 1706/RFC 2782)
- VLAN 802.1P/802.1Q
- Diff Server

1.5.2 Voice and Fax parameters

- G.711A/U law, G.723.1, G.729AB
- Comfortable Noise Generation (CNG)
- Voice Activity Detection (VAD)
- Echo Cancellation (G.168)
- Adaptive Dynamic Jitter Buffer
- Voice and fax gain control
- Modem
- T.38/Pass-through
- DTMF Mode: Signal/RFC2833/INBAND

1.5.3 Supplementary service

- Busy tone detection
- No current take out stitches detection
- Voice interrupted detection
- One stage dialing
- Two stage dialing
- PSTN exterior ports polling
- Polarity Reversal
- FAS（ Fake billing correction ）
- DC/AC impedance config
- Calls detection (Bellcore Type 1&2, ETSI,DTMF)

- Voice mail
- Direct IP Call
- IP Trunk

2. Basic Operations

2.1 Phone Call

2.1.1 Phone or Extension Number

1） FXO Call Out

- One stage dialing: After receiving phone number from softswitch/IPPBX, selected one PSTN call out through some selection rules such as round of selection.
- Two stage dialing: IPPBX extension dial FXO port SIP account, then after hearing dial tone, dial outside number.

2） Dial the number directly and press ＃.

- Dial outside number with FXO, when listen to audio "please dial the extension number" or second dial tone, and then dial callee number. After dialing completion, send callee number to IP server side, such as soft switch or IPPBX.
- Offhook auto-dial: Dial outside number with FXO, device will automatically connect to the specified extension or queue according to the default hotline number.

2.1.2 Direct IP Calls

DAG series device with FXS port allow two parties directly call through IP address. The user need only a simulation with the FXS port unit equipment linked together and set up calls not registered.

Elements necessary to completing a direct IP call：

1) Both DAG serial and other VoIP Device, have public IP addresses;

2) Both DAG serial and other VoIP Device are on the same LAN using private IP addresses;

3) Both DAG serial and other VoIP Device can be connected through a router using public or private IP addresses (with necessary port forwarding or DMZ).

Operation Process：

1）Pick up the analog phone then dial "*47"

2）Enter the target IP address.

【Note】: No dial tone will be played between step 1 and step 2

Examples:

If the target IP address is 192.168.0.160, the dialing convention is ***47,** then **192*168*0*160.** Followed by pressing the "#" key or wait 3 seconds. Complete signaling interactive soon after, he was called the unit can be heard ringing.

【Note】: You cannot make direct IP calls between FXS0 to FXS1 since they are using same IP. It only supports the default destination port 5060.

2.2 Call Features

DAG (FXS) support all traditional and senior phone function.

Table 2.2-1 Feature Codec

Feature Codec	Operation Instructions
***158#**	View the LAN port IP address
***159#**	View the WAN port IP address
***114#**	Inquire port account
150	Set the way of obtain IP address
157	Set network method
152	Set IP address
153	Set Subnet mask
156	Set default gateway IP address
***193#**	Obtain IP address through DHCP again

***160*1#**	Open WAN port to access web
***166*000000#**	Factory reset
***111#**	Restart device
***#**	Call hold
47	IP address call
***51#**	Enable call waiting
***50#**	Disable call waiting
87	Blind transfer
72	Enable Unconditional Call Forward
***73#**	Disable Unconditional Call Forward
90	Enable Busy Call Forward
***91#**	Disable Busy Call Forward
92	Enable No Answer Call Forward
***93#**	Disable No Answer Call Forward
***78#**	Enable DND
***79#**	Disable DND
***200#**	Access Voice mail
Flash/Hook	Switch between incoming calls, If not in session, flash/hook will switch a new channel for new call.

2.3 Sending and Receiving Fax

2.3.1 DAG（FXS）support four fax modes:

1）T.38（FoIP）

2）Pass-Through

3）Modem

4）adaptive

2.3.2 T. 38 and Pass-Through

T.38 is the preferred method because it is more reliable and works well in most network conditions. If the service provider supports T.38, please use this method by selecting T.38 as fax mode (default). If the service provider does not support T.38, pass-through mode may be used. If you have problems with sending or receiving Fax, toggle the Fax Tone Detection Mode setting.

3. Local IVR Operation

3.1 Inquire IP address

Analog phone connected with FXS ports of device, then pick up, after dial tone, dialing *158# to inquire LAN port IP address and dialing *159# to inquire WAN port IP address.

3.2 Factory Reset

After picking up, dial *166*000000#, then onhook and restart after “Setting successful”.

3.3 Configure LAN Port’s IP Address

Before configuration, please ensure:（1）The device is power on; （2）deviceis connectingto network;（3）Telephone is connecting to FXS port of device.

1) Configure dynamic IP address by DHCP：

Offhook; Dial “*150*2#”; Onhook;

If the equipment hint success, after 10 seconds, and restart the equipment.(Power-off then power-on)

2) Configure Static IP address

Offhook; Dial “*150*1#”; Onhook;

Then configure IP and mask as follow:

- Configure IP address：

Offhook; input "*152*172*16*0*100# "; onhook

- Configure subnet mask:

Offhook; input "*153*255*255*0*0# "; onhook

- Configure gateway IP address

Offhook; input "*156*172*16*0*1# "; onhook.

3) Query the IP address of device: Offhook, input"*158#"
4) If the DAG serial uses PPPoE method to get IP address, it need to configure by web browser.

【Note】: The telephone will play voice prompt "Setting successfully" if the step is correct

4. WEB Configuration

4.1 WEB Login

Device is connecting to network properly, refer to chapter 3 "Operation". Offhook and dial*158# to inquire device IP address.

4.1.1 Login

Device LAN port default IP address is 192.168.11.1, WAN port default obtain IP address by DHCP. Advice to modify the IP address of the local computer equipment and ensure that are on the same IP segment, with Windows 7 as an example, the local computer IP address change for 192.168.11.10:

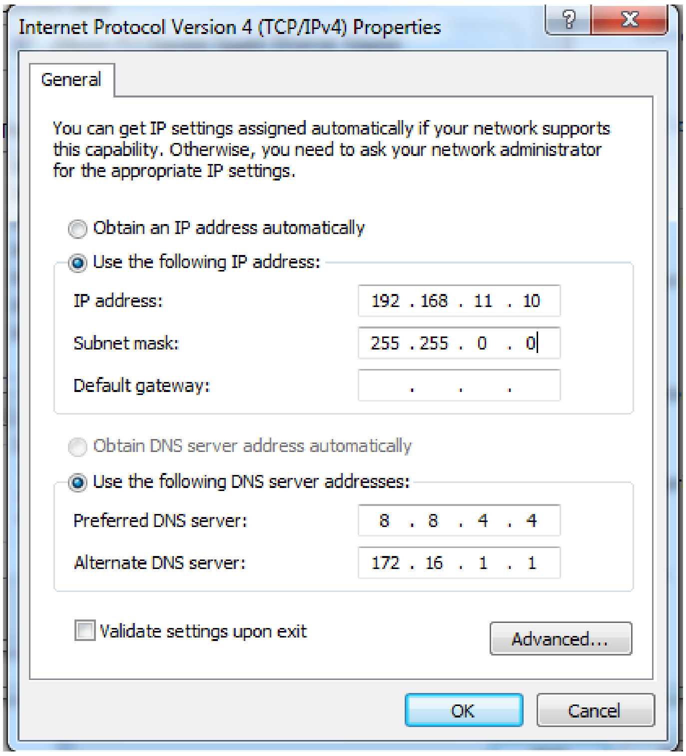


Figure 4.1-1Modify IP address

Check connection between computer and device, click “Start”-> “run”-> input “cmd”, run ping 192.168.11.10 –t order to check the connectivity between them.

4.1.2 Login WEB

Open web browser, then input IP address of device, Press“Enter”, it pop up logging on identity authentication interface.

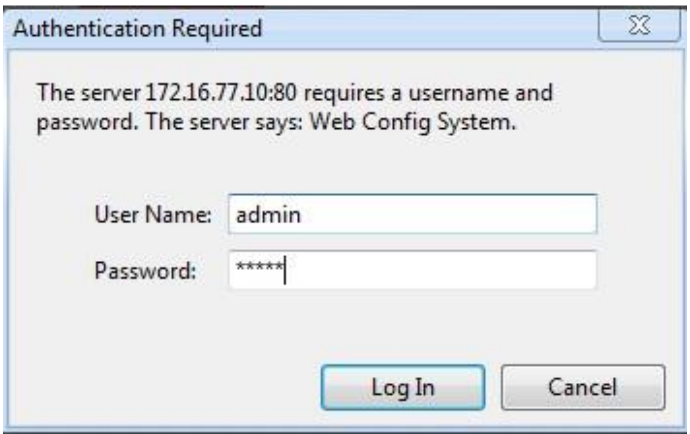


Figure 4.1-1 DAG FXS Login Interface

Default username and password: admin/admin, click “OK” to entry into web interface.

Figure 4.1-2 DAG Configure Interface

4.2 Navigation Tree

DAG series voice gateway web configuration interface mainly includes navigation tree and the right configuration interface. Choose navigation tree in order to entry into the configuration interface.

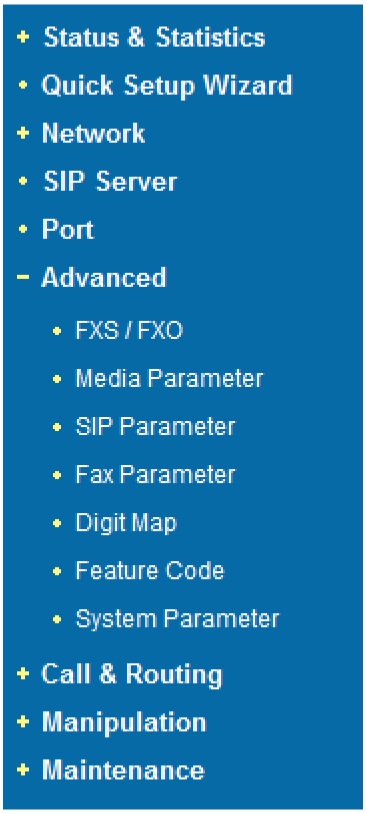


Figure 4.2-1 Navigation Tree

When device is in bridge mode, navigation tree won't display "routing configuration" items and the following "DHCP service", "DMZ host", "forward rules" and "static routing" and "ARP" etc.

4.3 State and Statistics

4.3.1 System Information

System information interface shows the run information as following figure 4.3.1 below:

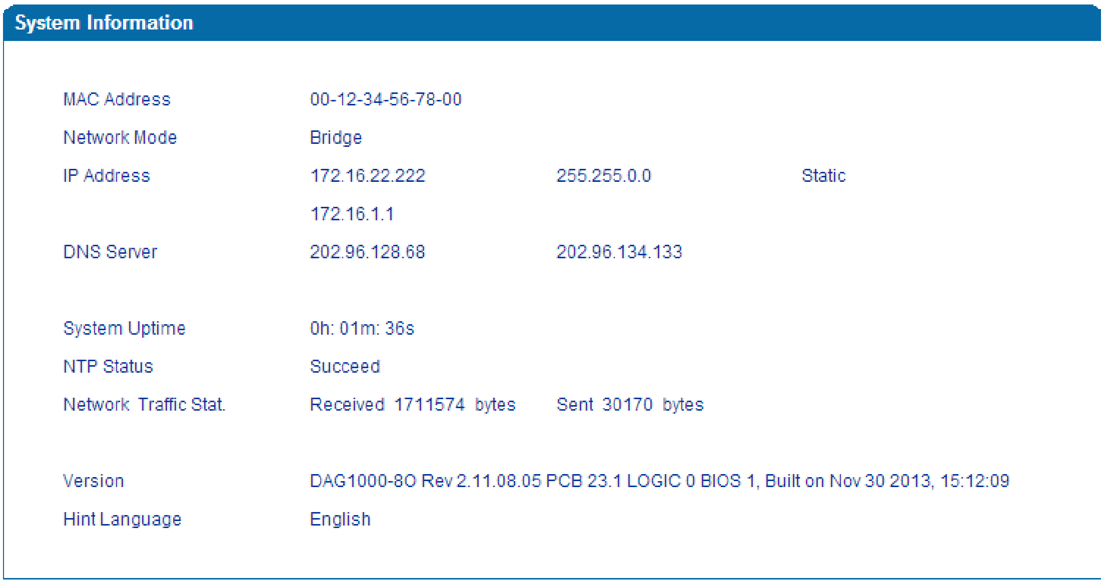


Figure 4.3-1 System Information

System information as follow:

Table 4.3-1 System Information Description

MAC address	WAN port hardware address. The device ID in HEX format.
Network Mode	Display network mode, include bridge and rout. If it is bridge, WAN port display Network, and the WAN port IP as same as the LAN port IP.
WAN Port	Shows WAN IP address of DAG , DHCP mode: all the field values for the Static IP mode are not used (eventhough 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 willestablish a PPPoE session if any of the PPPoE fields is set. Static IP mode: configure the IP address, Subnet Mask, Default Router IPaddress, DNS Server 1 (primary), DNS Server 2 (secondary) fields. These fieldsare set to zero

	by default.
LAN Port	Shows LAN IP address of DAG. If network Mode is bridge, LAN port won't display.
DNS Server	Display DNS server IP address and default gateway information
System Uptime	Time elapsed from device power on to now.
Network Traffic Statics	Total bytes of message received and sent by network port.
Version	Includes: product mode, software version, hardware version and built time etc.

4.3.2 Registration Information

Port Registration Information

Port No.	Type	Primary User ID	Primary User Status	Secondary User ID	Secondary User Status
---	---	---	---	---	---

Port Group Registration Information

Port Group	Port	Primary User ID	Primary User Status	Secondary User ID	Secondary User Status
0 <All Port>	0,1,2,3,4,5,6,7,8,9,10,11,12,13,	8888	Unregistered	---	---

Refresh

Figure 4.3-2 Port and Port group registration information

4.3.3 TCP/UDP Statistics

TCP/UDP Traffic

TCP Sent Packets	TCP Recv Packets	UDP Sent Packets	UDP Recv Packets
232	59	41	216

Refresh

Figure 4.3-3 TCP/UDP Statistics Information

Figure 4.3-3 shows TCP sending and receiving, UDP sending and receiving packets of statistical information since the device launched.

4.3.4 RTP Session Statistics

Figure 4.3-4 RTP Session Statistics

Figure 4.3-4 display real-time RTP conversation flow data information, includes:

Port, voice codec, packet period, local port, peer IP, peer port, sent packets, receive packets, lost packets, jitter and duration.

4.4 Quick Setup Wizard

Quick configuration guide will guide users to configure the device step by step. Users only need to configure network, SIP server and sip port in quick setup wizard. Basically, after these three steps, users are able to make voice call through device.

4.5 Network Configuration

4.5.1 Local Network

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

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

Note: DAG2000-16O just supports bridge mode. DAG1000-4/8O supports bridge and route mode.

Bridge mode

Network configuration of bridge mode:

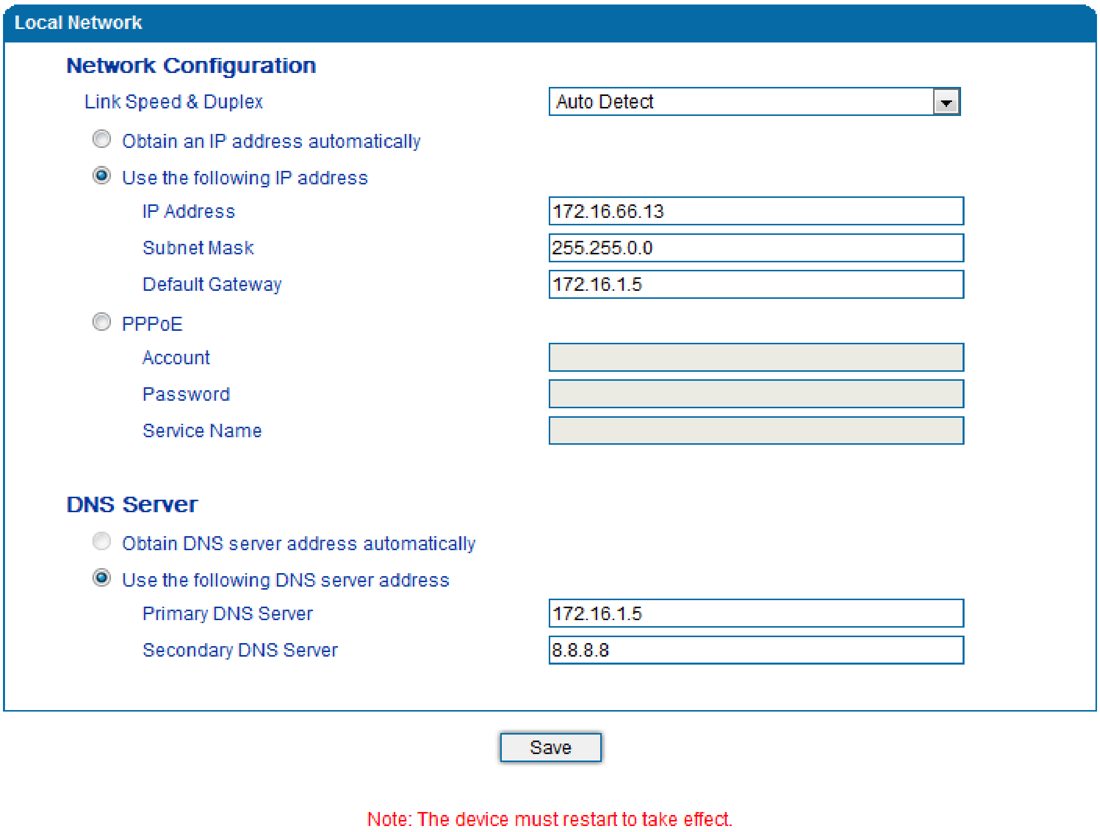


Figure 4.5-1 Local network

- "Link Speed &Duplex"used to select Ethernet port work mode, include 5 kinds of choice,"Auto Detect"、"10Mbps half-duplex"、"10Mbps full-duplex","100Mbpshalf-duplex","100Mbps full-duplex", default is "Auto Detec".
- When select"Obtain IP address automatically", DAG will obtain IP address by DHCP.
- When select "Use the following IP address", that configure DAG to fixed IP address mode.
- When select "PPPoE", please fill in account and password offered by ISP in internet account and password.

【Notes】:

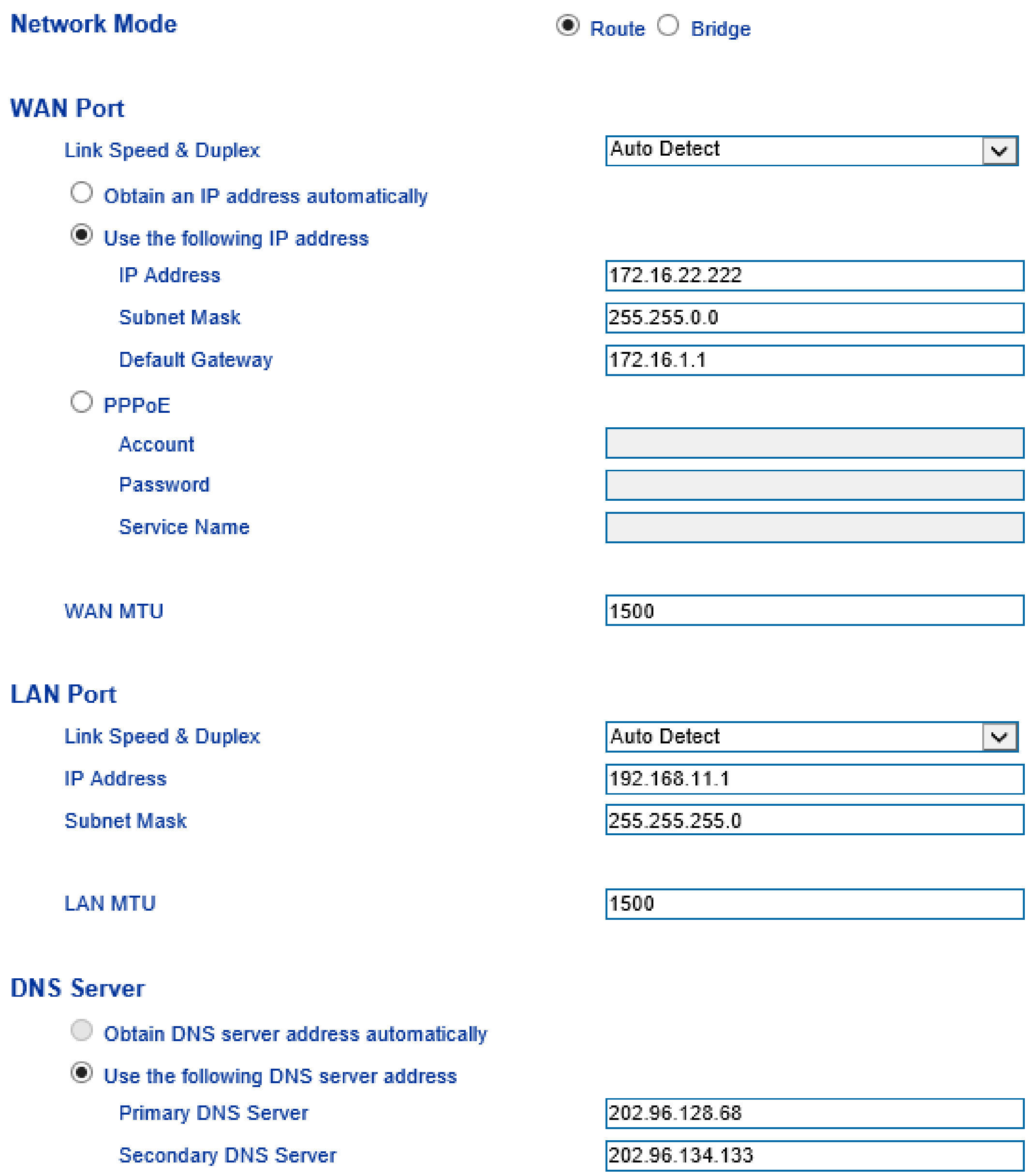
1） If select DHCP to obtain IP address, please ensure DHCP server in network and work normally.

2） After configuration, restart device configuration validation.

3）

- **Route Mode**

Network configuration of route mode:



Notes: The following settings are available on route mode only!

4.5.2 VLAN Parameter

Generally, Internet provides only Best Effort Service. Since ethernet is the most spread LAN access technology, importance of providing it a quality of service mechanism ought not to be neglected.

Ethernet technology also used as WAN technology, not only as LAN technology. Due to rapidly increasing use Internet through Public Switched Telecommunication Network (PSTN), Telephone Companies are forced to implement IP-based networks as their PSTN backbones. A network like this without any Quality of Service mechanisms would be disastrous. Just imagine yourself trying to get an emergency call through while others just surf the Internet.

1) 802.1Q

The IEEE 802.1Q standard defines architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs and the protocols and algorithms involved in the provision 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. abitity to regenerate user priority of received frames using priority information contained in the frame and the User Priority Regeneration Table for the reception Port.

2) 802.1p

IEEE 802.1p standard, Traffic class expediting and dynamic multicast filtering. It 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 is 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.

There are three VLAN: data VLAN, voice LAN and management VLAN. VLAN configuration interface as following figure 4-4-3:

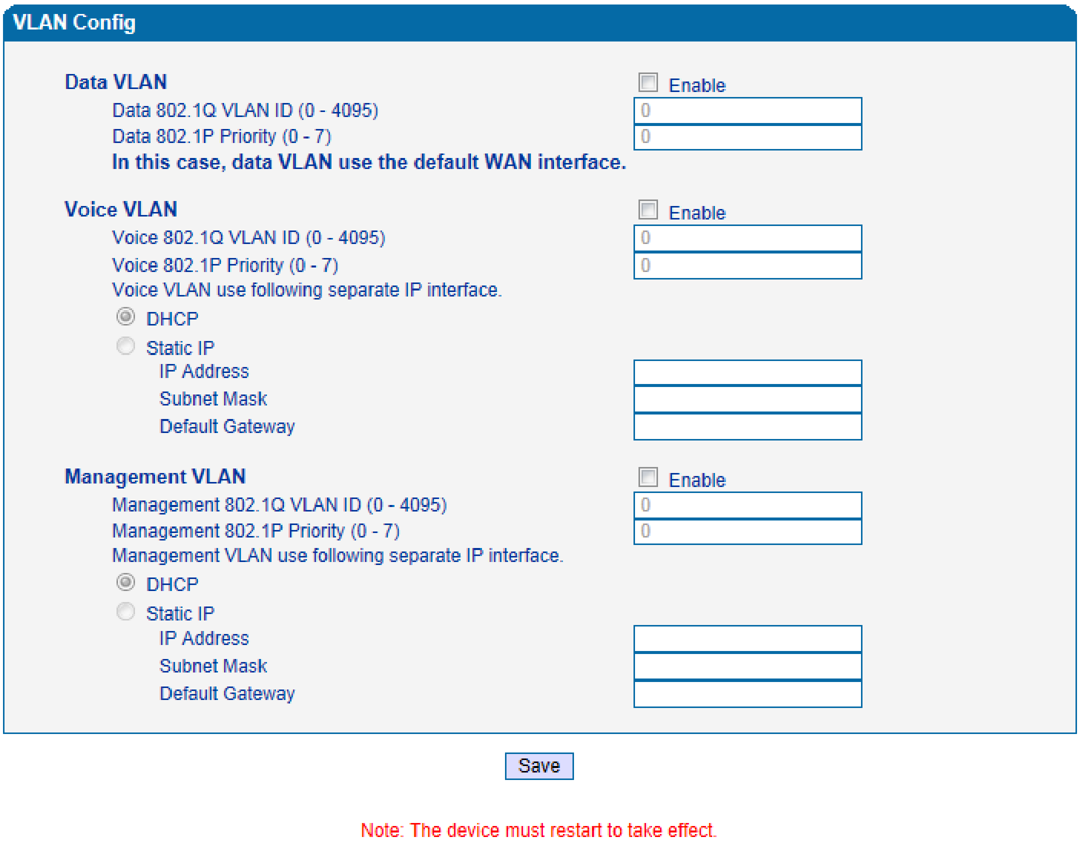


Figure 4.5-3 VLAN parameter configuration

Table 4.5-1VLAN parameter configuration

Data VLAN	Data 802.1Q VLAN ID(0-4095)	Fill out an ID to describe a data VLAN group,ID 0 used to management VLAN, can't used to service configure.
	Data 802.1p Priority（0-7）	802.1 protocol to control network traffic priority, Priority from 0-7.
Voice VALN	Voice 802.1Q VLAN ID(0-4095)	Fill out an ID to describe a voice VLAN group, ID 0 used to management VLAN, can't used to service configure.
	Voice 802.1p Priority（0-7）	802.1 protocol to control network traffic priority, Priority from 0-7.
	IP address	Can use dynamic or static IP address
	Voice VLAN DNS Server	Can use dynamic or static DNS server address
Management VLAN	Management 802.1Q VLAN ID(0-4095)	Fill out an ID to describe a data VLAN group, ID 0 used to management VLAN, can't used to service configure.
	Management 802.1p Priority（0-7）	802.1 protocol to control network traffic priority, Priority from 0-7.
	IP address	Can use dynamic or static IP address

	Management VLAN DNS server	Can use dynamic or static DNS server address

【Note】: restart the device to take configuration effect.

4.5.3 MAC Clone(Routing mode)

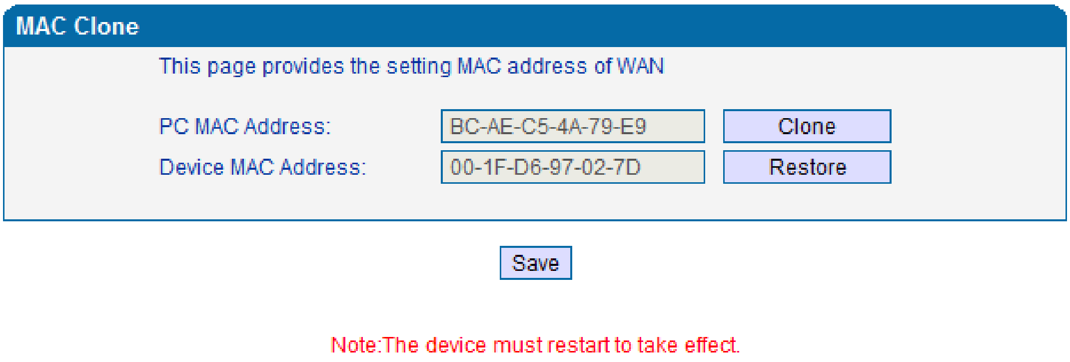


Figure 4.5-4 MAC Clone Interface

More client in LAN have already can't share internet used the traditional "gateway set law". Because IP address binding in only a legitimate MAC address by ISP. If the ISP's switch discover illegal MAC address, it will refuse service.

The best way is MAC clone for MAC binding. Most ADSL MODEM, broadband router, wireless router have this feature. The principle of MAC address clone is deliberately exposed MAC address of bound computer to the ISP server and let the ISP server think that used only a single piece of computer, in fact many computers in sharing the Internet.

This function used to prevent ISP limiting to share the Internet.

【Note】: restart device to take configuration effect.

4.5.4 DHCP Server (Routing mode)

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

Start and end address of address pool determine the range of IP address automatically assigned to other devices;

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

• Subnet mask, gateway, DNS and other information configured by DHCP protocol.

Configuration interface as figure 4.5-5：

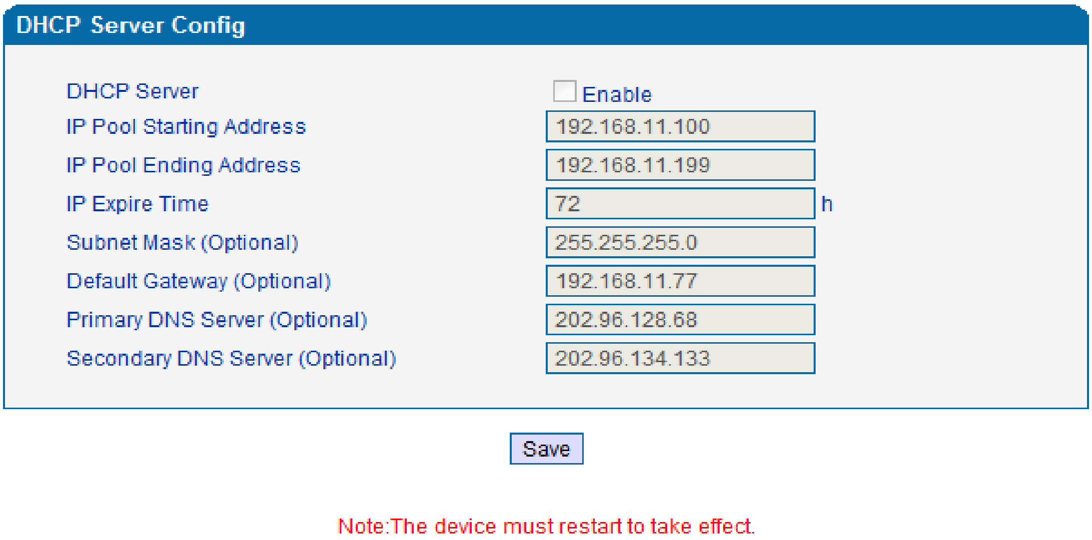


Figure 4.5-5 DHCP Configuration Interface

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

4.5.5 DMZ Host (Routing mode)

DMZ(Demilitarized Zone) connect web, e-mail etc. server allowed external to access to this area. Make the internal network located the back of the zone of confidence and not allow any access, separation of inside and outside the network, protect user information.DMZ can be understood that a special areas 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 come into 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 .

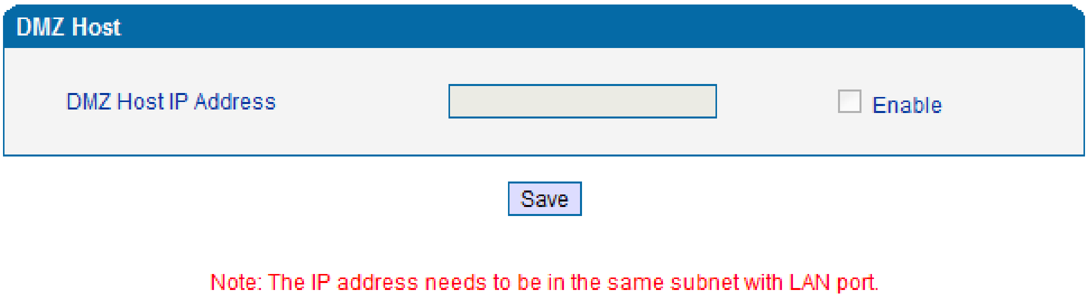


Figure 4.5-6 DMZ Configuration Interface

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

4.5.6 Forward Rule(Routing mode)

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

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

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

Port (0-1024) and all the foreign communication agreement; while the forward rule offers a

single or a few port foreign communication on some protocol. When the conflicts exist between forward rule and DMZ host,the configuration of forwarding rules is preferred.

Forward rule configuration interface as follows:

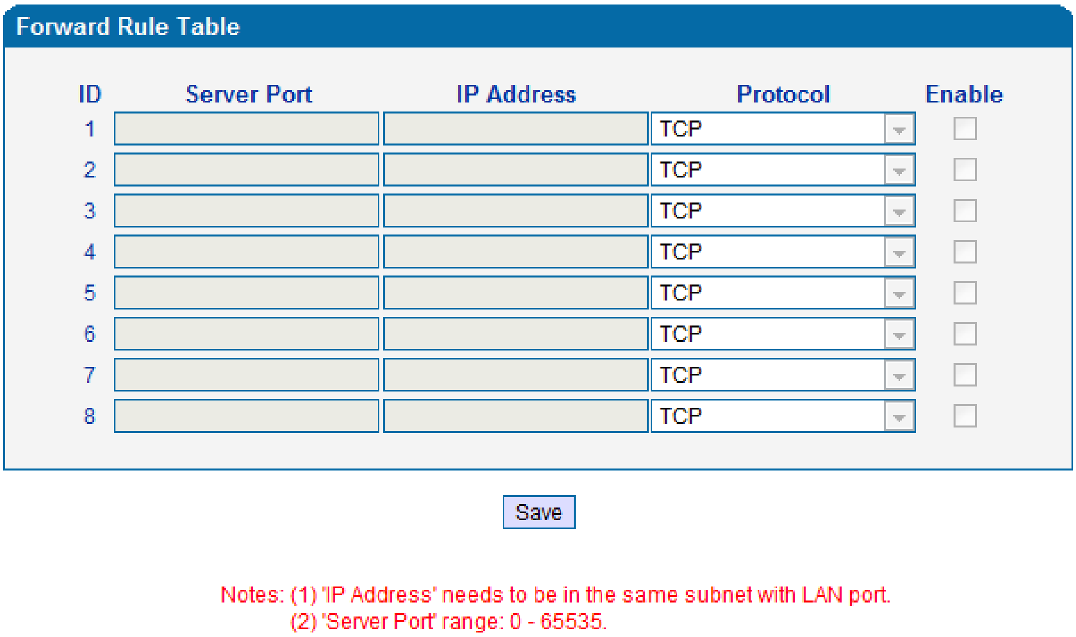


Figure 4.5-7 Forward rule configuration interface

4.5.7 Static Route Table

Static Route Table 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 need to be configured.

Static Route configuration interface as follows:

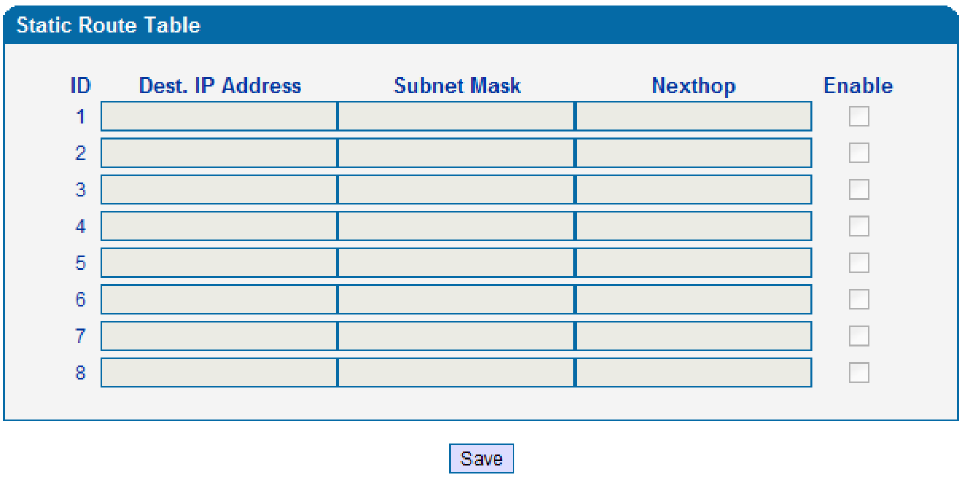


Figure 4.5-8 Static route configuration interface

4.5.8 ARP

ARP brief introduction:

ARP is address resolution protocol. After configuring ARP, users can get physical address through device IP address. Under TCP/IP network environment, each host is assigned a 32-bit IP address. But the message transmission needs to know the purpose the physical address of the party. ARP is a tool that converts IP address into MAC address.

ARP configuration interface as follows:

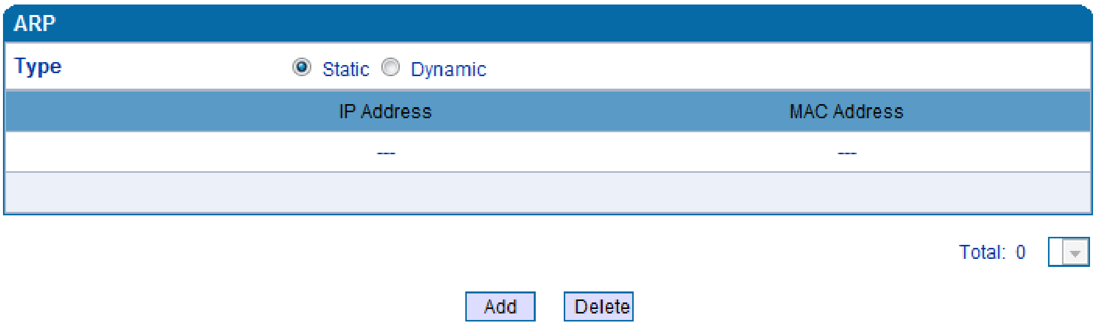


Figure 4.5-4 ARP Parameters

4.6 SIP Server

SIP server introduction:

1）SIP server is the main component of VoIP network and responsible for establishing all the SIP phone calls. SIP server also called SIP proxy server or registered server. IPPBX and the soft-switch can act as SIP server role.

2）Usually, SIP server does not participate in the media process.

In SIP network, the media always using end-to-end to hand the consultation. In some particular situation or business processing, such as “Music On Old”, SIP server will actively participate in the media negotiation. Simple SIP server is responsible only for establishment, maintenance and cleaning conversation, don't interfere in call. While relatively complex SIP server also called SIP PBX. It not only provides the basic call, and basic conversational support, also offer plenty of business, such as: Presence, Find-me, Music On Hold.

3）SIP server based on Linux platform, such as: OpenSER、sipXecx，VoS，Mera etc.

4）SIP server based on windows platform, such as :miniSipServer、Brekeke，VoIPswitch etc.

5）Carrier grade soft-switch platform, such as Cisco, Huawei, Zteetc.

SIP server configuration interface as follows:

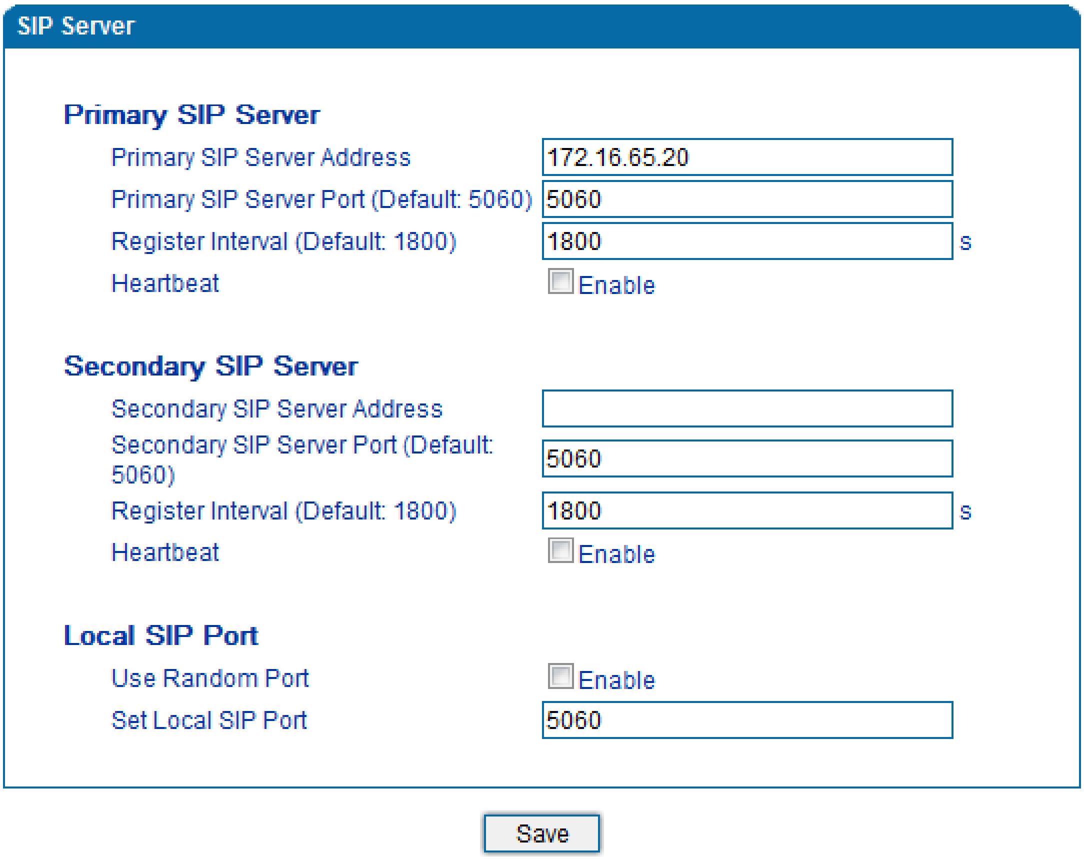


Figure 4.6-1 SIP Server Configuration Interface

SIP parameter description:

Primary SIP Server IP	SIP Server IP address or Domain name provided by VoIP service provider.
Primary SIP Server port	Service port, default is 5060
Register interval	protects registrar against excessively frequent registration refreshes while limiting the state.Every once in a while send request for registration to the terminal server, default is 1800s.

Heartbeat	Heartbeat message detect the connection status between device and SIP server.
Secondary SIP Server IP address	Backup SIP Server's IP address or Domain name provided by VoIP service provider.
Secondary SIP Server port	Service port, default is 5060
Secondary SIP server Register interval	protects registrar against excessively frequent registration refreshes while limiting the state.Every once in a while send request for registration to the terminal server, default is 1800s.
Secondary SIP heartbeat	Heartbeat message detect the connection status between device and SIP server.
Use Random Port	Random SIP service ports for DAG
Set Local SIP port	Default SIP service port is 5060.

4.7 Port Configuration

Port parameters include: Send gain, receive gain, primary display name etc.

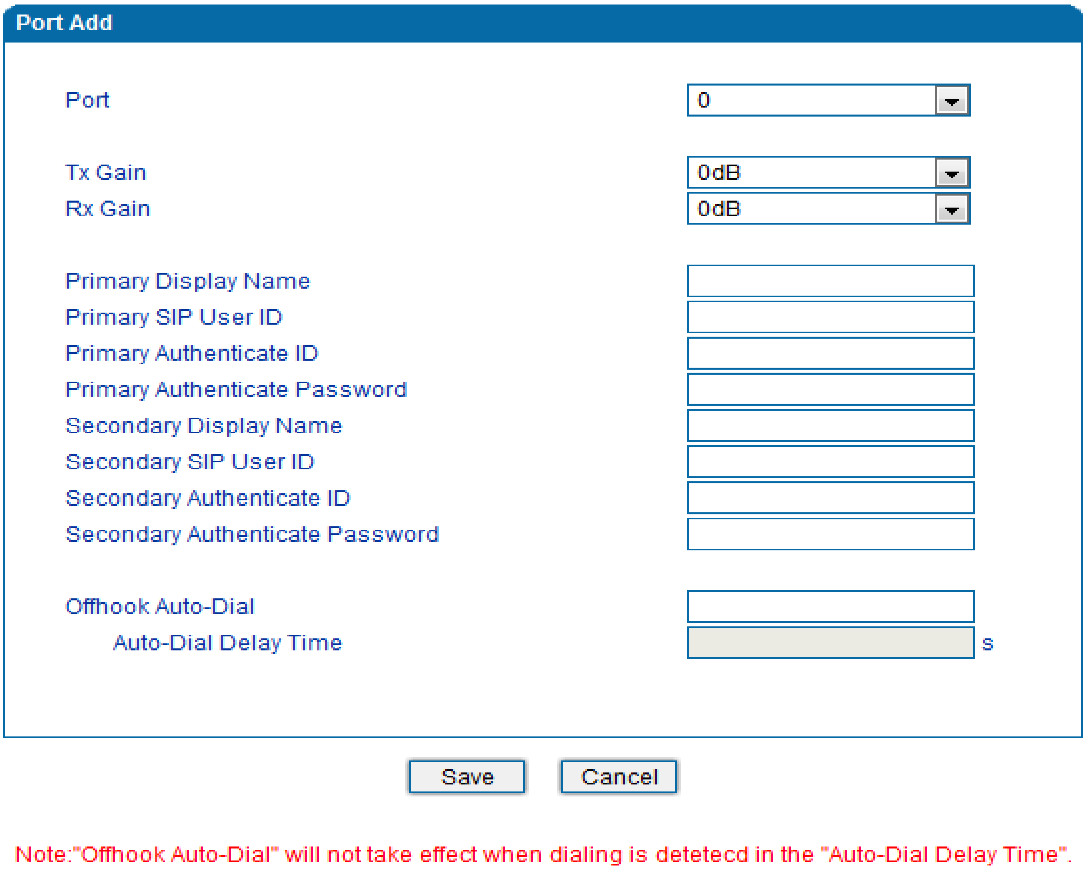


Figure 4.7-1 Port configuration interface

Port parameters introduce as follows:

Tx Gain	It is use to control the volume of conversation, Adjust "TX gain" will affect the end users voice size, the default value is 0. Its value range from-10 – 10 dB
Rx Gain	It is use to control the volume of conversation, Adjust "RX gain" will affect the end users voice size, the default value is 0. Its value range from -10 – 10 dB
Primary /Secondary SIP Display Name	Primary /Secondary SIP account description. Its purpose is so you can identify the SIP account with a meaningful name
Primary /Secondary SIPUser ID	User account information, provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
Primary/Secondary SIP Authenticate ID	SIP service subscriber's Authenticate ID used for authentication. Can be identical to or different from SIP User ID.
Primary/Secondary Authenticate password	SIP password which registers to soft switch/SIP server
Offhook Auto-dial	Pre-assign an extension or phone number so that automatically dial a number as soon as you pick up the phone set
Auto-dial Delay Time	Delay 0-3 seconds to automatically dial a number, 0 means dial number immediately

4.8 Advanced

4.8.1 FXS/FXO

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

FXO as ordinary telephone interface, and need to remote provide current. FXO may connect company's internal PBX service extension and the telecom outside, generally speaking, FXO is a telephone. So just lead a inside to FXO port from company's internal, or directly line a straight up in FXO from the telecom.

FXO parameters include: Call progress Tone, Timeout for Dialing, Send Polarity Reversal etc. Configuration interface as follow:

Basic Parameters:

Call Progress Tone	USA	
Timeout for Dialing	4	s
Timeout for Answer(Outgoing Call)	55	s
Timeout for Answer(Incoming Call)	55	s
No RTP Detected	☑ Enable	
Period without RTP Packet	30	s

- **Call Progress Tone:** Hear the dial tone when pick up the phone. Choose the national standards from the drop-down box. Default is the United States.
- **Timeout for Dialing**: With the help of dialing timeout, you can limit the time while users typing the digits from an extension. If the timeout expire while the user is typing in the extension then DAG will consider the extension as complete and it will try to send to SIP server. Default value is 4 seconds.
- **Timeout for Answer (Outgoing Call):** This timer set how long the caller party waiting when makes outgoing call on extension.
- **Timeout for answer (Incoming call):** This timer set how long the phone sets ringing when get incoming call.
- **No RTP Detect:** This option is to disconnect call when there is no RTP received. Default value is 90s

Incoming call setting and Caller ID

Incoming Call from PSTN	
Configuration by FXO	☑ Enable
Detect CID	After Ring
Send Original CID when Call from PSTN	☑ Enable
Format of "From" field when CID is Available	Display/CID
Format of "From" field when CID is Unavailable	Display/User ID
CID : Calling Number Name : Calling Name	
FXO Keep Onhook until Callee Answered	☐ Enable
Play Hint to FXO	☑ Enable
Allow Call to SIP Server without Registration	☑ Enable

- **Configuration by FXO:**

When the call from FXO interface, users can be enable or disabled FXO allocation function. FXO configuration function includes: detect CID, Send original CID, Play hint to

FXO.

- **Detect CID**: to enable caller ID detection for incoming calls. The gateway has two modes: Before ring and after ring.

  Before ring: the FXO port will detect CID first, then ringing to the port. It takes about few seconds to detect CID in generally.

  After ring: the FXO port will ringing to FXO port then start to detect CID

- **Send Original CID when Call from PSTN**
  - **From Mode when CID Is Available**

    Used to configure "From" Mode when Caller ID Is Available when call from PSTN to VoIP. The SIP header should be matched with follow formats:

    Display/CID: From: "Mike"<sip:CID@host.com>;tag=51088abb

    User ID/CID: From:"201"<sip:CID@host.com>;tag=51088abb

    CID/CID: From: Caller ID <sip: Caller ID@host.com>;tag=51088abb

    CID/User ID: From:"Caller ID"<sip:201@host.com>;tag=51088abb

  - **From Mode when Caller ID Is Unavailable**

    Used to configure "From" Mode when Caller ID Is Unavailable

    Anonymous : From: <sip: Anonymous @host.com>;tag=51088abb

    Display/User ID: From: "Mike"<sip: 201 @host.com>;tag=51088abb

- **Keep onhook until callee answered**

  When the gateway get incoming call from PSTN network, the modular will answer the call then start to DTMF or route to destination hotline number. While this option enabled, the modular won't answer the call but routing to destination hotline number till it getting answer.

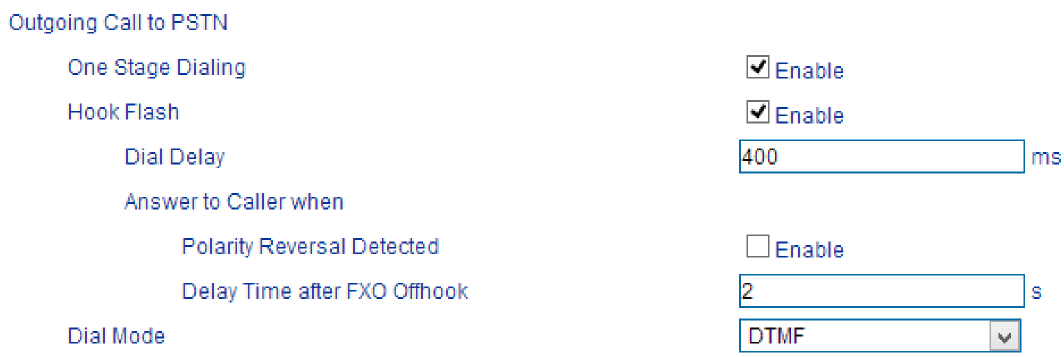
- **Play Hint to FXO**

  Enable this function, when call from PSTN to FXO port, FXO port will play prompt tone "please dial the extension number".

- **Allow Call to SIP Server without Registration**

  To enable peer to peer call without registration.

Outgoing call Parameters



- **One Stage Dialing**

  Enable this function, FXO port directly sent the dial number, without call extension.

- **Dial Delay**

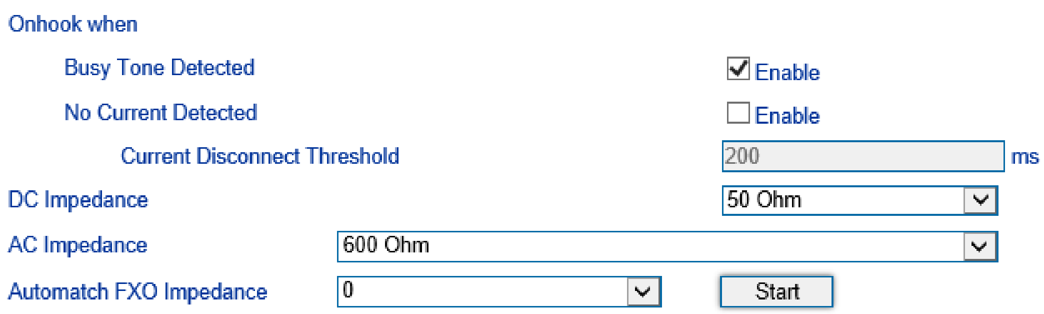
  Timer of outgoing call dialing. To call out while match with routing rule successfully.

- **Polarity Reversal Detect**

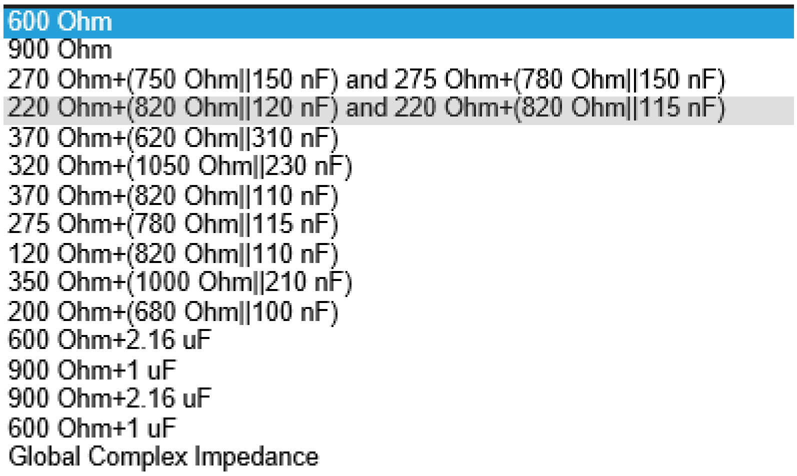
  To enable or disable Polarity Reversal.

- **Delay Time after FXO Offhook**

  Timer of the gateway to send SIP 200OK to VoIP. In case the fixed line doesn't supply answer signal, the gateway will send answer signal to VoIP side.



- **Busy Tone Detected**
  The FXO port will release while busy tone detected.
- **No current detected**
  The FXO port will release while no current detected on the phone line.
- **AC/DC impedance**
  To match with the impedance of phone line automatically or configure impedance manually. Here is the list that support on the gateway:



4.8.2 Media Parameter

Media parameter mainly include: RTP start port, DTMF parameter, PreferedVocoder. Configuration Interface as follow:

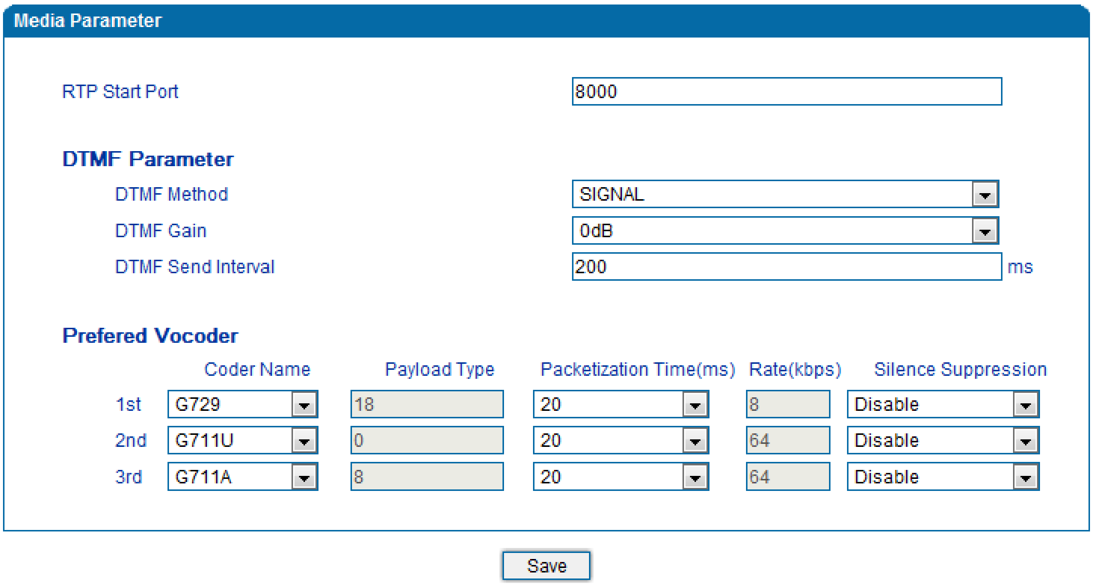


Figure 4.8-2 Media Parameter Configuration Interface

Media parameter description:

RTP Start Port	Default RTP port 8000
DTMF Method	SINGAL、INBAND、RFC2833
RFC2833 Payload Type Optimization	It is configurable When RFC2833 is selected, payload negotiation parameter with remote side, it includes two options: Local and remote

RFC2833 Payload Type	Payloadvalue, default is 101
DTMF Gain	Default is 0 DB
DTMF Send Interval	DTMF send signal interval, default is 200ms.
Coder Name	DAG supports G729、G711U、G711A、G723. while it make outgoing call, G.729 will used as figure 4.8.2 displayed
Payload Type	Each kind of coding has a unique type load value, refer toRFC3551
Packetization Time	Voice package time
Rate	Voice data flow rate, system default
Slience Suppression	Default is disable, if enable, according to the current noise environment dynamically adjust mute inhibit threshold,thus in the user in silent state stop transmission background noise bag and save about VoIP bandwidth.In the low bandwidth environment, can reduce the network congestion, greatly improving VoIP call effect.

4.8.3 SIP Parameter

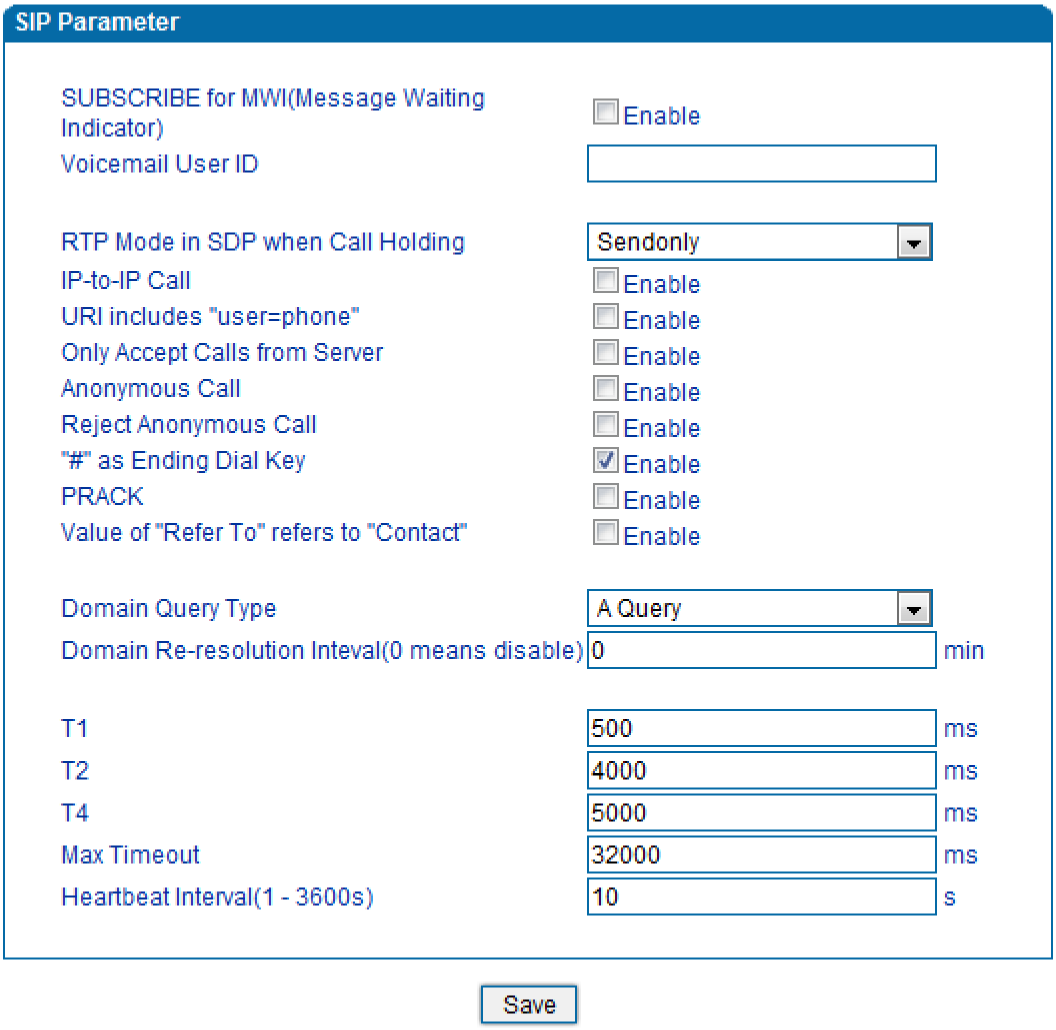


Figure 4.8-3 SIP Parameter Configuration Interface

SIP parameter description：

SUBSCRIBE for MWI	Voicemail message indicator, it is to be realized in the way of NOTIFY
Voicemail User ID	Access code to voicemail box
RTP Mode in SDP when Call Holding	When call come into holding, if select to receive and not send packet, then the local can hear call waiting tone. If select to not receive and not send packet, then doesn’t play call waiting tone.
IP-to-IP Call	Enable this function, users may use the * business call IP address on the phone.
URI Includes user=phone	SIP carries the information, the system defaults not open.
Only Accept Call from Server	Default is no, it indicates the DAG accept incoming call from SIP server only

Anonymous Call	Enable anonymous call,"anonymous" will include in SIP message
Reject Anonymous Call	Enable this function, reject all anonymous call. Disable by default
# as ending Dial Key	Dial-up, use # as a end descriptor.
PRACK	RFC3262 defined an optional extension methods—PRACK（provisional ack）, Used to support the reliability of the temporary response.
Value of "Refer To" refers to "Contact"	Its function is to require the receiving partycontact with the third partythrough the use of supplied in the request in the address information. "Refer to" field of SIP message fill in "contact header".
Domain Query Type	There are two modes option: A QUERY and SRV QUERY. Default is A QUERY.
Domain Re-resolution Interval	Default 0: forbidden
T1	T1 timer of SIP protocol, default is 500ms
T2	T2 timer of SIP protocol, default is 400ms
T4	T4 timer of SIP protocol, default is 500ms
Max Timeout	The max timeout of sending or receiving, default is 32s
Heartbeat Interval	Default is 10s.

Voice mail instructions:

Here DAG work with Elastix the example, introduces how voicemail work in DAG.

1）DAG register to Elastix server. Corresponding extension number enable voice mail function in Elastix and set password. As below：

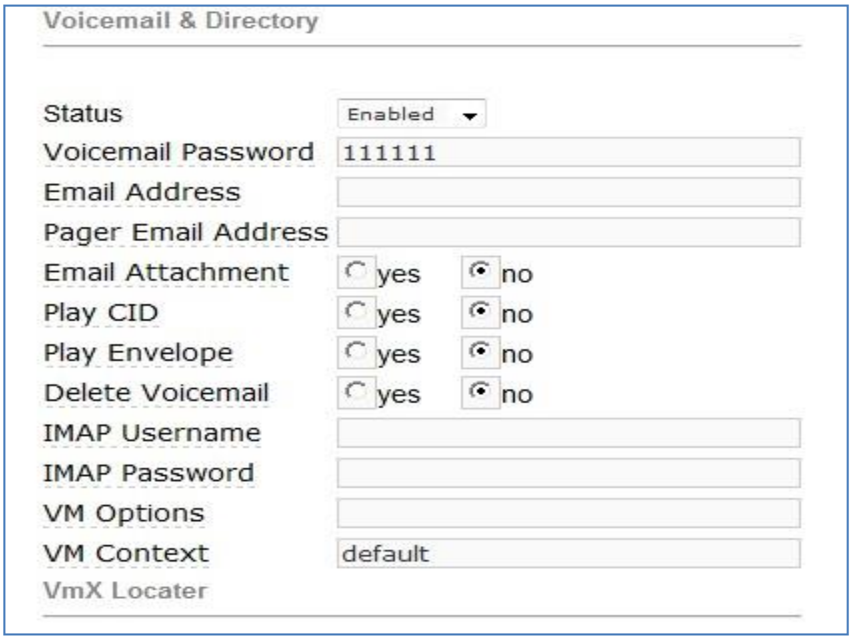


Figure 4.8-4 Elastix Voicemail Configuration Interface

2）check feature code in Elastix and change it as necessary. Its default feature codes setting as below:

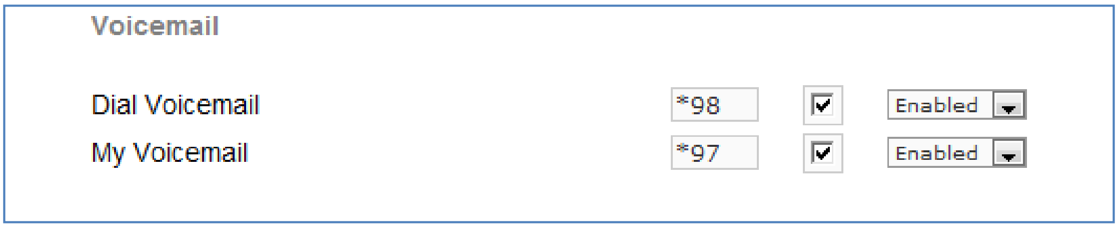


Figure 4.8-5 Elastix Voicemail Setting

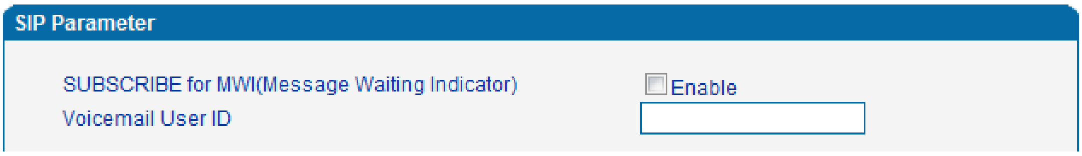


Figure4.8-6 Voice Mail Setting In SIP Parameter

3）Enable voice mail in DAG and Elastix will ask you to leave a message after ringing 15 seconds, then Elastix will record and display your message.

Figure 4.8-7 Voicemail Setting

4）DAG dial *200#, then dial voicemail account and thenask password for Validation. After that the user will hear voice message.

4.8.4 Fax Parameter

Fax introduction：

DAG fax parameter includes: fax mode, Fax sound detection party, ECM, Rate.

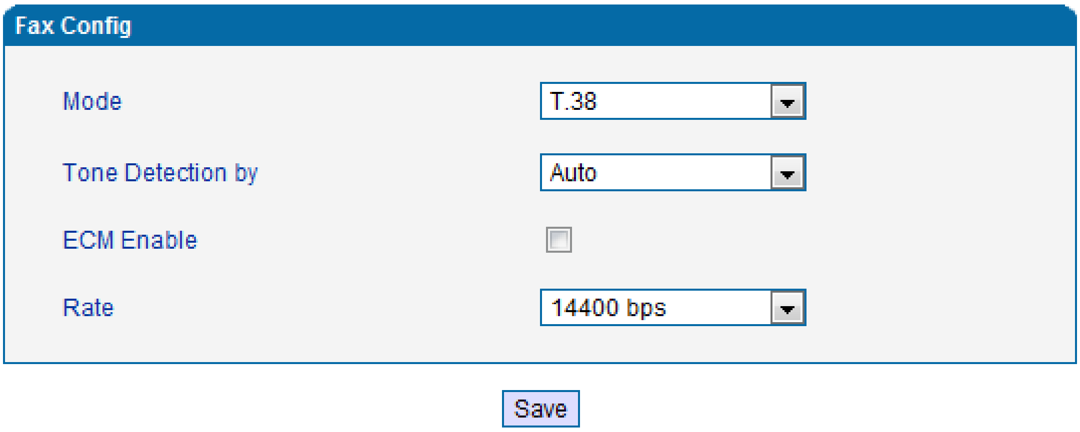


Figure 4.8-8 Fax Parameter Configure Interface

Fax parameter description:

Mode	Fax mode support T.38, T.30 (Pass-through),Modem, Adaptive.
Tone Detection by	Fax sound detection mode: Caller, Callee, Automatic.
ECM	Fax error correction information
Rate	The rate of sending and receiving.

4.8.5 Digit Map

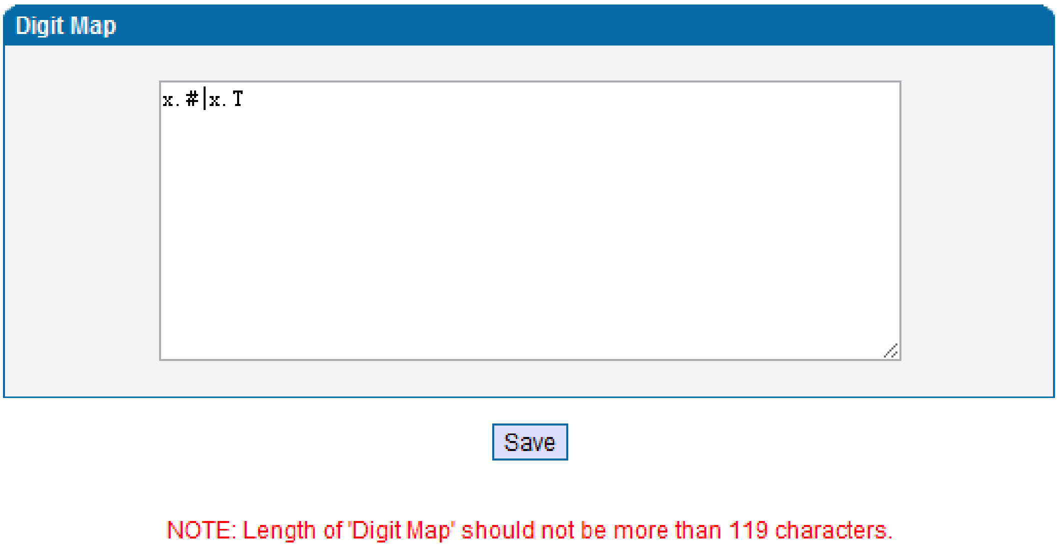


Figure 4.8-9Digit Map

Gateway is collect digits dialed by user, if received a number to be immediately report, the efficiency is too low and a large number of take up network resources. A reasonable method is concentration sending a message after receiving all number. How to judge the gateway receiving all number is the difficulties of this method. The solution is the call agent loading a "Digit Map" to gateway.

Digit Map includes a series figure characters, when the dial-up sequence and one received a character string matching, it means the number has received neat. Digital string contains characters allowed：data0~9, letterA~D,"#","*", letter T, letter x and ".". "|" parts of each string is a choice of dial-up solutions; "[]"means choose anyone;"*"means one reports; letter T means detected timer overtime; x means any data; "."means multiple characters can be behind，include 0; "#"means report immediately.

Digit Map Syntax:

1. Supported objects

   Digit: A digit from "0" to "9".

   Timer: The symbol "T" matching a timer expiry.

   DTMF: A digit, a timer, or one of the symbols "A", "B", "C", "D", "#", or "*".

2. Range []

One or more DTMF symbols enclosed between square brackets ("[" and "]"), but only one can be selected.

3. Range ()

One or more expressions enclosed between round brackets ("(" and ")"), but only one can be selected.

4. Separator

|: Separated expressions or DTMF symbols.

5. Subrange

-: Two digits separated by hyphen ("-") which matches any digit between and including the two. The subrange construct can only be used inside a range construct, i.e., between "[" and "]".

6. Wildcard

x: matches any digit ("0" to "9").

7. Modifiers

.: Match 0 or more times.

8. Modifiers

+: Match 1 or more times.

9. Modifiers

?: Match 0 or 1 times.

Example:

Assume we have the following digit maps:

1. xxxxxxx | x11

and a current dial string of "41". Given the input "1" the current dial string becomes "411". We have a partial match with "xxxxxxx", but a complete match with "x11", and hence we send "411" to the Call Agent.

2. [2-8] xxxxxx | 13xxxxxxxxx

Means that first is "2","3","4","5","6","7" or "8", followed by 6 digits;

or first is 13, followed by 9 digits.

3. (13 | 15 | 18)xxxxxxxxx

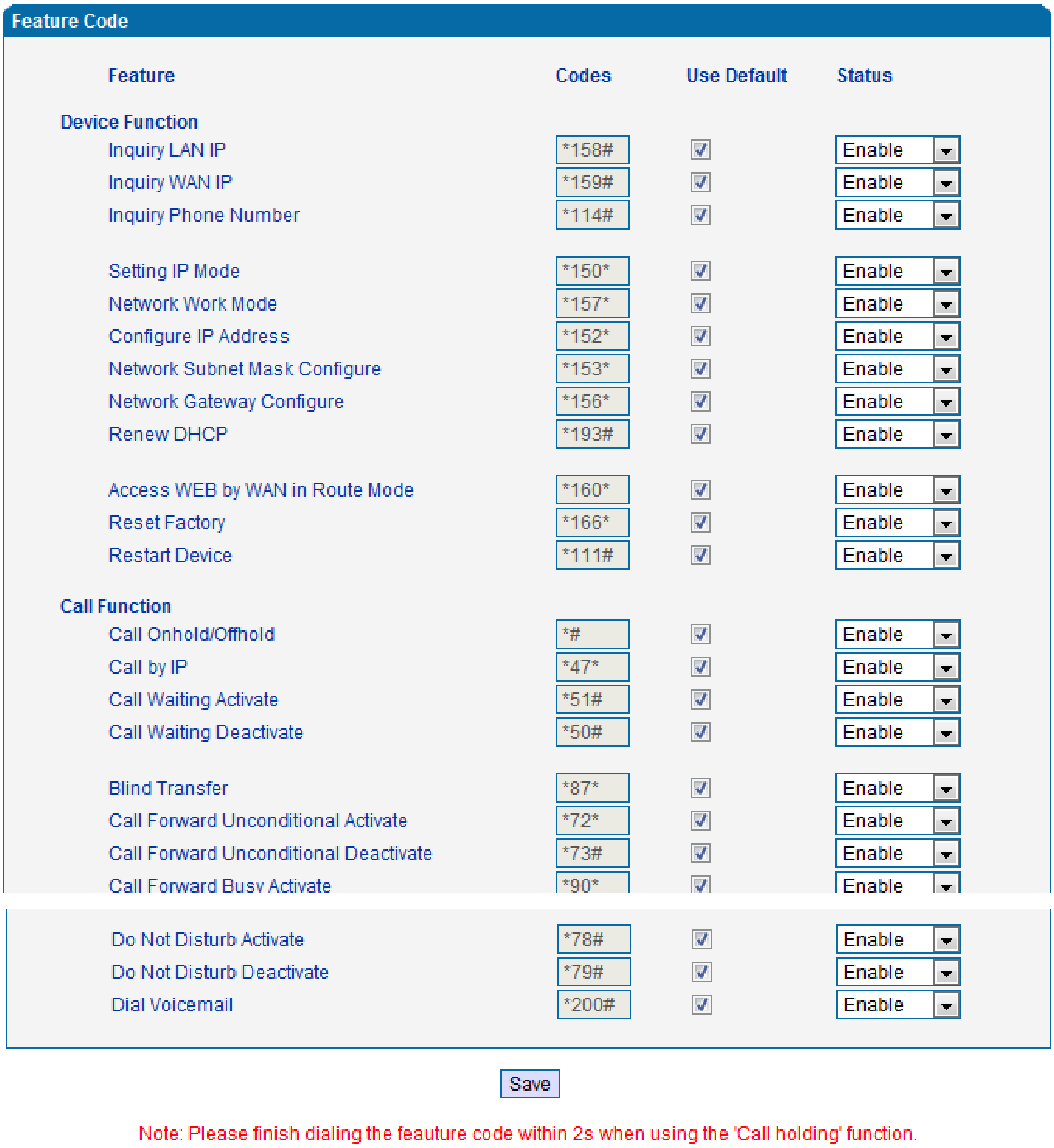
Means that first is "13","15" or "18", followed by 8 digits.

4. [1-357-9]xx

Means that first is "1","2","3" or "5" or "7","8","9", followed by 2 digits.

4.8.6 Feature Codec

Feature codec includes device function and call function. Feature codec as follow:



Feature Code

Feature	Codes	Use Default	Status
Device Function			
Inquiry LAN IP	*158#	☑	Enable
Inquiry WAN IP	*159#	☑	Enable
Inquiry Phone Number	*114#	☑	Enable
Setting IP Mode	*150*	☑	Enable
Network Work Mode	*157*	☑	Enable
Configure IP Address	*152*	☑	Enable
Network Subnet Mask Configure	*153*	☑	Enable
Network Gateway Configure	*156*	☑	Enable
Renew DHCP	*193#	☑	Enable
Access WEB by WAN in Route Mode	*160*	☑	Enable
Reset Factory	*166*	☑	Enable
Restart Device	*111#	☑	Enable
Call Function			
Call Onhold/Offhold	*#	☑	Enable
Call by IP	*47*	☑	Enable
Call Waiting Activate	*51#	☑	Enable
Call Waiting Deactivate	*50#	☑	Enable
Blind Transfer	*87*	☑	Enable
Call Forward Unconditional Activate	*72*	☑	Enable
Call Forward Unconditional Deactivate	*73#	☑	Enable
Call Forward Busy Activate	*90*	☑	Enable
Do Not Disturb Activate	*78#	☑	Enable
Do Not Disturb Deactivate	*79#	☑	Enable
Dial Voicemail	*200#	☑	Enable

Save

Note: Please finish dialing the feauture code within 2s when using the 'Call holding' function.

Figure 4.8-10 Feature Code Configuration Interface

Inquire WAN port IP address	Dial*159# to obtain device WAN port IP address
Inquire Phone Number	Dial*114# to obtain port account
Setting IP Mode	*150*0#, means pppmodem, *150*1#, means static IP, *150*2#, means obtain IP address by DHCP, *150*3#, means pppoe.
Network Work Mode	*157*0#, set network work mode to routing mode; *157*1#, set network work mode to 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
Renew DHCP	*193#, set dynamic IP again
Access Web by Wan in Rout Mode	Allow access web through WAN port：*160*1#; don't allow access web through WAN port：*160*0#
Reset Factory	*166*000000#, reset factory
Restart Device	*111#, restart device
Call onhold/offhold	When call process, dial*# into call hold.（Recovery the call through hook flash or *#）
Call by IP	Directly dial the end user IP to call
Call Waiting Activate	*51#, enable call waiting function
Call Waiting Deactivate	*50#, forbid call waiting function
Blind Transfer	If the call transfer to 801, first hook flash and then dial the * 87 * 801#
Call Forward Unconditional Activate	*72*+ phone number#, transfer the call from the phone number
Call Forward Unconditional Deactivate	*73#, forbid call forward unconditional
Call Forward Busy Activate	*90*+ forward busy number#
Call Forward Busy Deactivate	*91#, forbid call forward busy
Call Forward No Reply Activate	*92*+ forward no reply number#
Call Forward No Reply Deactivate	*93#, close this function
Do Not Disturb Activate	*78#, enable DND function
Do Not Disturb Deactivate	*79#, close DND function
Dial Voicemail	*200#, visit voice mail box

Note: * Private services are open by default

4.8.7 System Parameter

System parameters include: STUN、NTP、Provision、WEB parameter、Telnet.

1）STUN：STUN（Simple Traversal of UDP over NATs）is a network protocol. It allows users back of NAT find their own public network address, NAT type and internet end port have been bound by NAT for a local port. Two back of NAT router devices established UDP communication through this information.

STUN doesn't support TCP connection and H.323.

2）NTP：Network Time Protocol（NTP）is a computer time synchronization protocol.

System parameter configuration interface as follow:

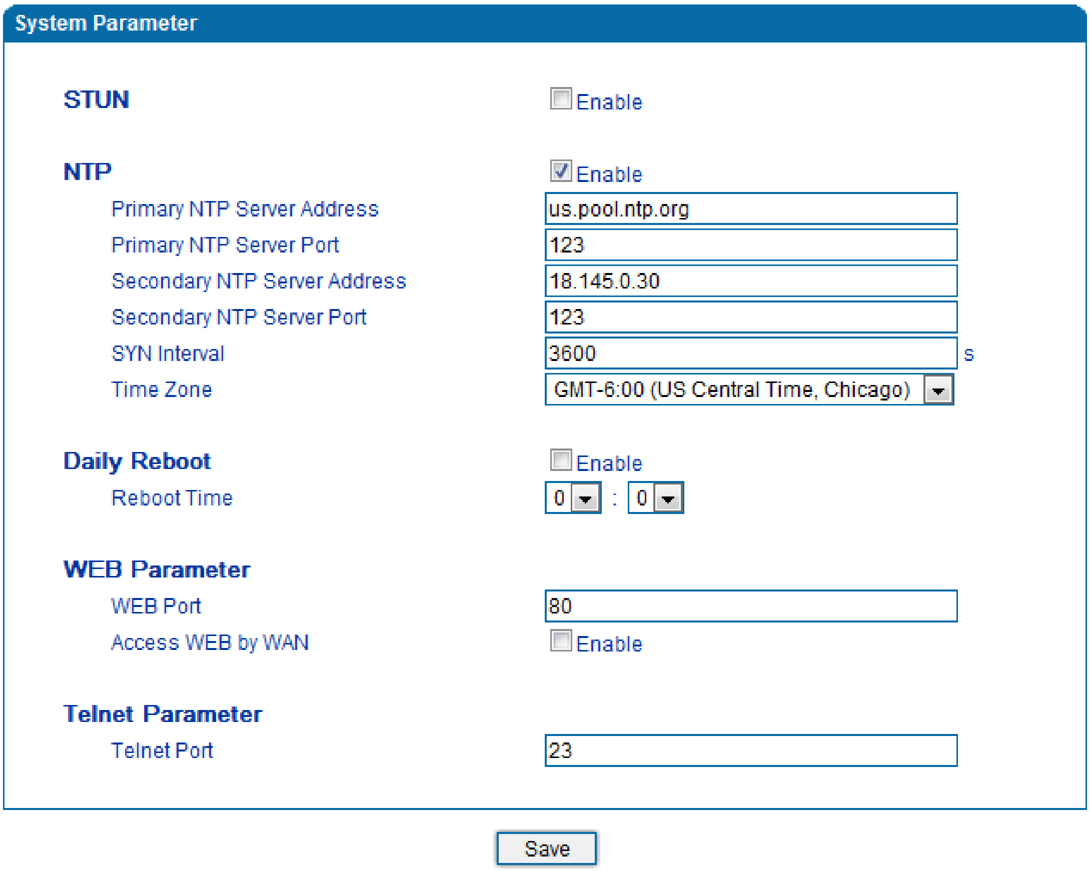


Figure 4.8-11System Configuration Interface

STUN Server Address	STUN server IP address
STUN Server Port	STUN server port
Primary NTP server address	Primary NTP server IP address, system default is us.pool.ntp.org
Primary NTP server port	Default is 123
Secondary NTP server address	Default is 18.145.0.30
Secondary NTP server port	Default is 123
SYN Interval	Every certain time synchronization gateway time, the system default every 3600 s synchronous once.
Time Zone	Time zone can be chosen. System default the United States central time, Chicago.
Reboot time	Set a restart time for device, the device will reboot at this time.
WEB Port	Gateway web port, default is 80
Access Web by WAN	Enable or disable accessing web by WAN
Telnet Port	Telnet service port, default is 23.

4.9 Call & Routing

4.9.1 Port Group

Port group parameter include: Index, description etc. Port group configure interface as follow:

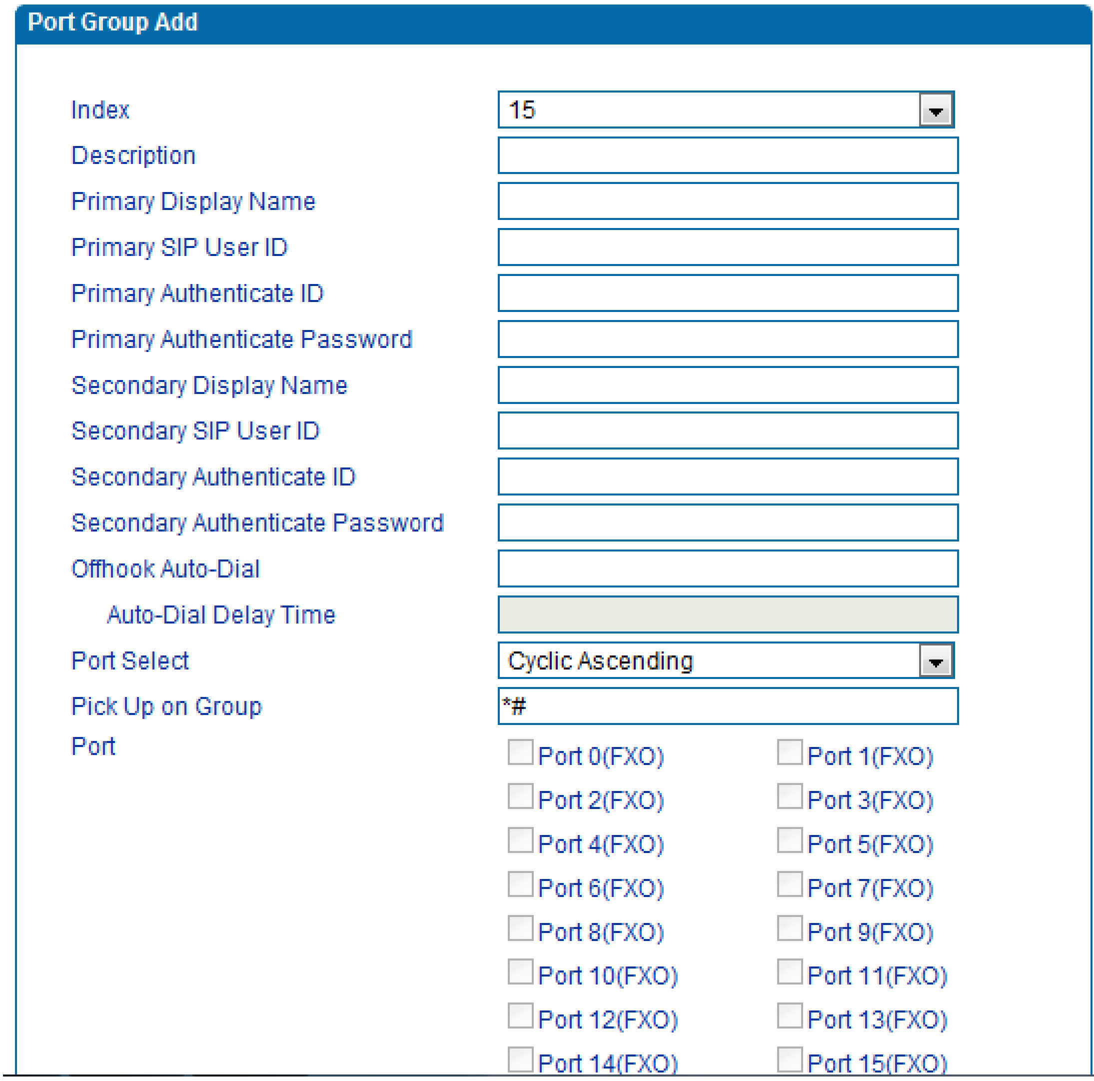


Figure 4.9-1 port group configuration interface

Index	Port groupNumber, It uniquely identifies a route,range from 0-15
Description	Port group description,its purpose is so you can identify the port group with a meaningful name
Primary/Secondary Display Name	Port group display, which will be used in SIP message, example: INVITE sip:bob@biloxi.com SIP/2.0 Via:SIP/2.0/UDPpc33.atlanta.com;branch=z9hG4bK776as dhds Max-Forwards: 70 To: Bob <sip:bob@biloxi.com> From: Alice <sip:alice@atlanta.com>;tag=1928301774 Here Bob and Alice is the display
Primary/Secondary SIP User ID	User account information, provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
Primary/Secondary Authenticate ID	SIP service subscriber's Authenticate ID used for

	authentication. Can be identical to or different from SIP User ID.
Primary/Secondary Authenticate Password	Password of SIP user ID
Offhook Auto-Dial	Set Auto-dial number to complete one stage dialing.
Auto-Dial delay time	Delay time of FXO port send auto-dial number.
Port Select	• It specifies the policy for selecting port in a port group • Ascending: the system always selects a port from the minimum number. The preferential selection of the port can be realized through this mode • Cyclic ascending: when system selects ports' Priority, it always begin from the number next to the number selected last time, if the maximum priority number is selected last time, then the next number is the minimum priority number, and move in cycles like this • Descending: when system selects ports' priority, it always begin to select from the maximum priority number • Cyclic descending: when system selects ports' Priority, it always begin from the number before to the number selected last time, if the minimum priority number is selected last time, then the next number is the maximum priority number, and move in cycles like this • Group ring: all ports ringing at the same time
Pick Up on Group	Press "*# +extension number" to decide which extension on the phone.
Port	Add some ports to the same group

4.9.2 IP Trunk

A peer-to-peer VoIP call occurs when two VoIP phones communicate directly over IP without IP PBXs between them. A peer-to-peer call can be initiated directly by dialing destination phone number in DAGs and also receiving incoming calls from other peer to peer gateway. IP trunk is help to DAGs establish peer-to-peer call between DAGs and other VoIP phones. IP trunk will be used in routing configuration.

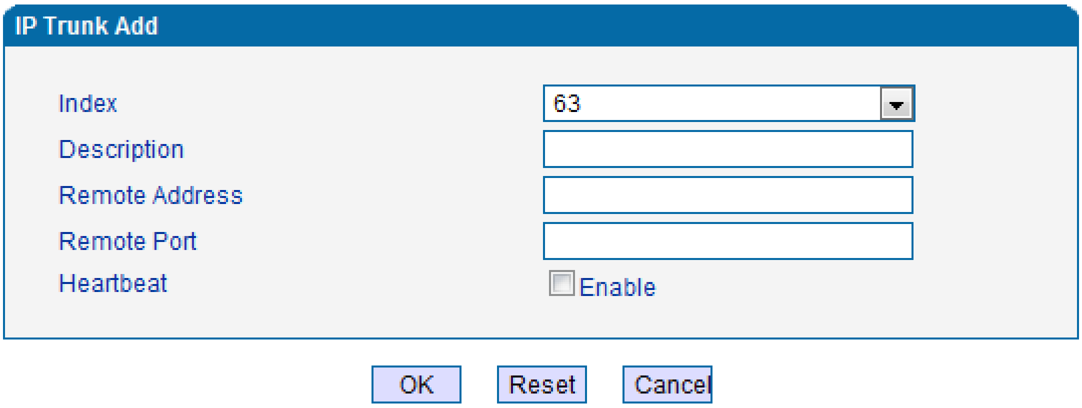
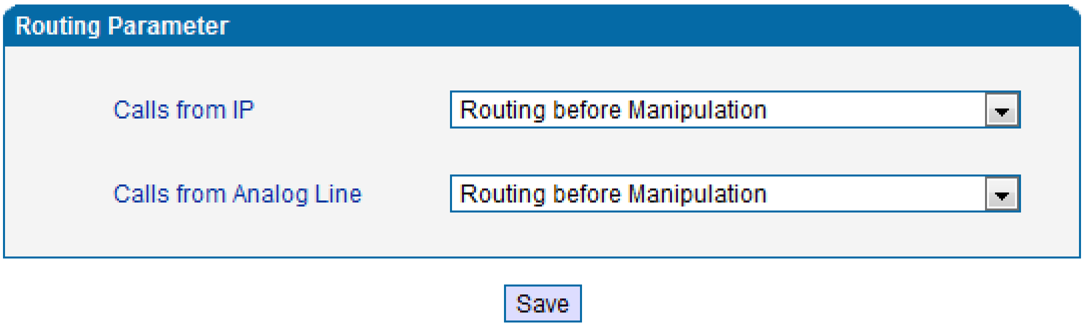


Figure 4.9-2 IP Trunk Configuration Interface

Index	IP trunk number, it is range from 0 to 63
Description	The description of IP trunk, its purpose is so you can identify the IP trunk with a meaningful name
Remote Address	Peer IP address or domain name
Remote Port	Peer SIP port
Heartbeat	Default is disable, if enable, DAG will send “OPTION” to peer device

4.9.3 Routing Configuration

Figure 4.9-3 Routing Parameter Configuration Interface



This option determines the following routing of call take effect before or after manipulation.

4.9.4 IP-Tel Routing

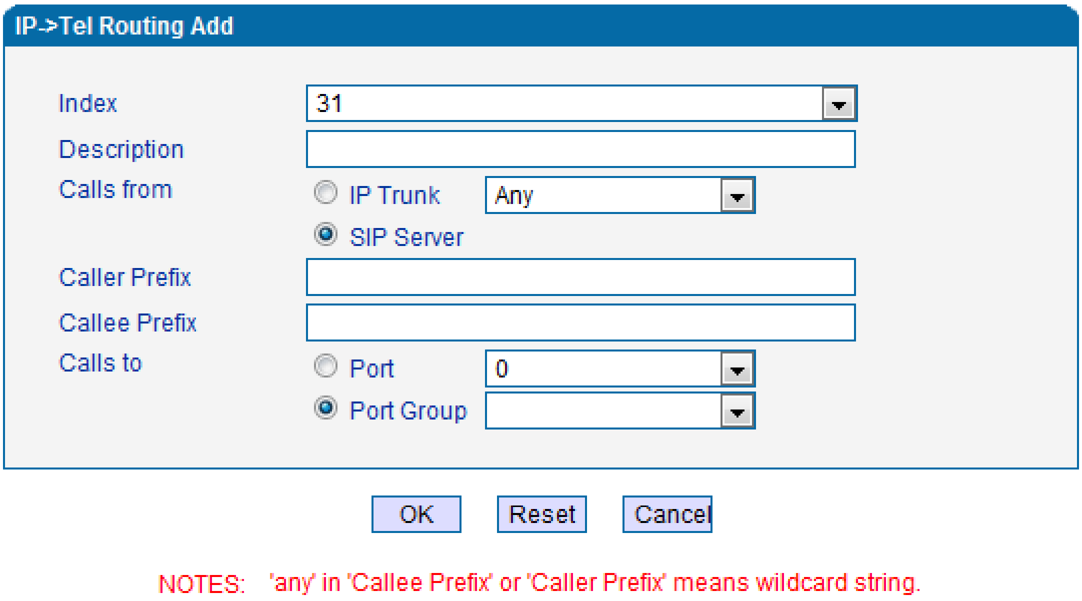


Figure 4.9-4 IP-Tel Routing Parameter

Index	Routing priority: 0-31, 0 is the highest priority.
Description	its purpose is so you can identify theIP0->Tel routing with a meaningful name
Calls from	IP Trunk/SIP Server, any means any IP
Caller Prefix	Caller number Prefix, its length normally less or equal to caller number, which helps to matching routing exactly. if caller number is 2001, the caller prefix can be 200 or 2. "any" means match any caller number like "bob1","29801"
Callee Prefix	Called number Prefix, its length normally less or equal to callednumber, which helps to matching routing exactly. if called number is 008675526456659, the called prefix can be 0086755 or 00.,"any" means match any called number
Calls to	This call routing is routing to port or port group

4.9.5 Tel-IP/Tel Routing

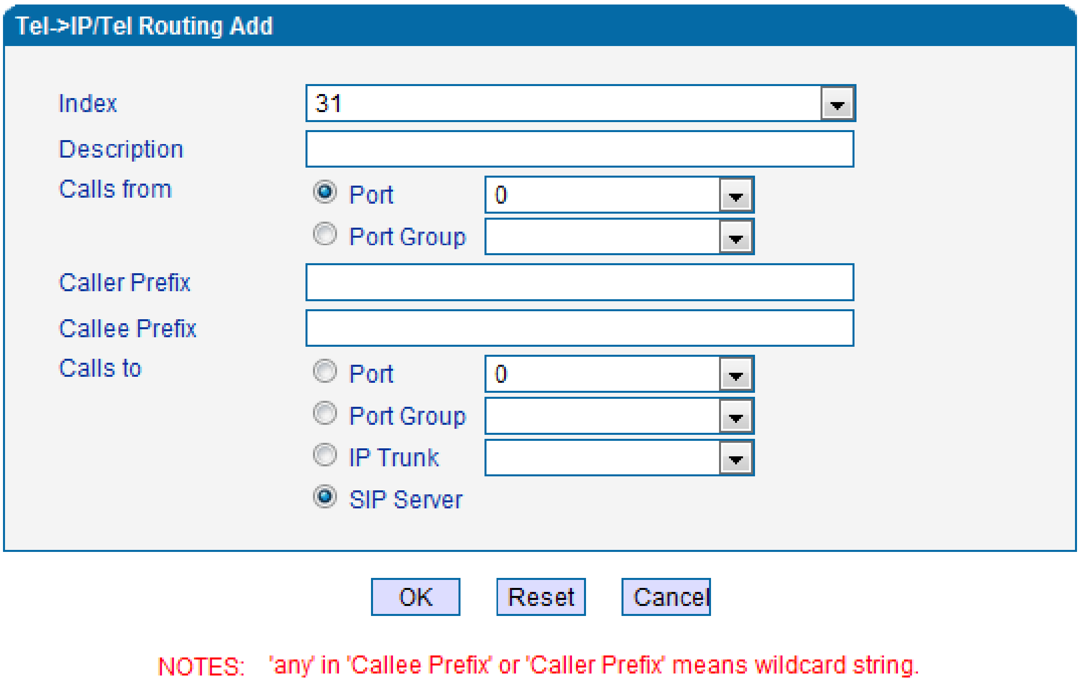


Figure 4.9-5 Tel-IP/Tel Parameters Configuration

Index	Routing priority :0-31, 0 is the highest priority.
Description	its purpose is so you can identify the routing with a meaningful name
Calls From	Tel-IP call select port or port group
Caller Prefix	Caller number Prefix, its length normally less or equal to caller number, which helps to matching routing exactly. if caller number is 2001, the caller prefix can be 200 or 2. “any” means match any caller number like “bob1”,”29801”
Callee Prefix	Called number Prefix, its length normally less or equal to called number, which helps to matching routing exactly. if called number is 008675526456659, the called prefix can be 0086755 or 00., “any” means match any called number
Calls to	This call routing is routing to port, port group, IP trunk and SIP server.

4.10 Manipulation Configuration

4.10.1 IP-Tel Callee

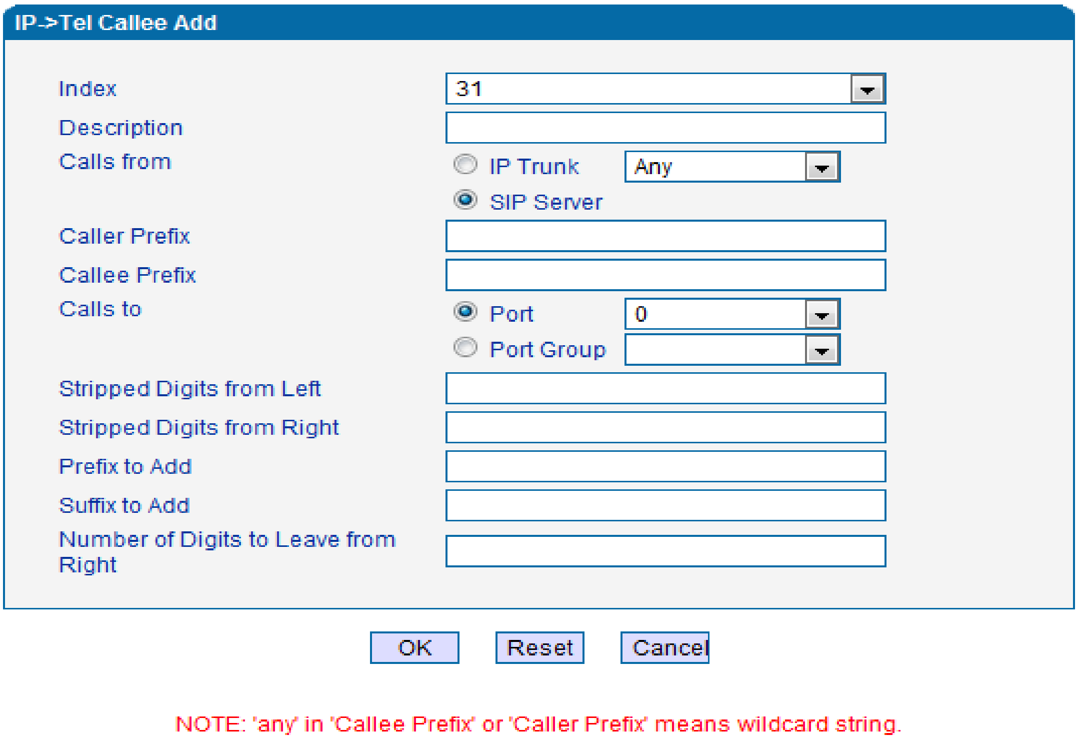


Figure 4.10-1 IP-Tel Callee number configuration

Calls From	This call come from IP trunk or SIP server.
Caller Prefix	Caller number Prefix, its length normally less or equal to caller number, which helps to matching routing exactly. if caller number is 2001, the caller prefix can be 200 or 2. "any" means match any caller number like "bob1","29801"
Callee Prefix	Called number Prefix, its length normally less or equal to called number, which helps to matching routing exactly. if called number is 008675526456659, the called prefix can be 0086755 or 00., "any" means match any called number
Calls to	This call routing is routing to port, port group
Stripped Digits from Left	Remove the called number digits from the left
Stripped Digits from Right	Remove the called number digits from the right
Prefix to Add	Add a number prefix

Suffix to Add	Add a number suffix
Number of Digits to Leave from Right	Starting from the right to retain the called number digits

4.10.2 Tel-IP Caller

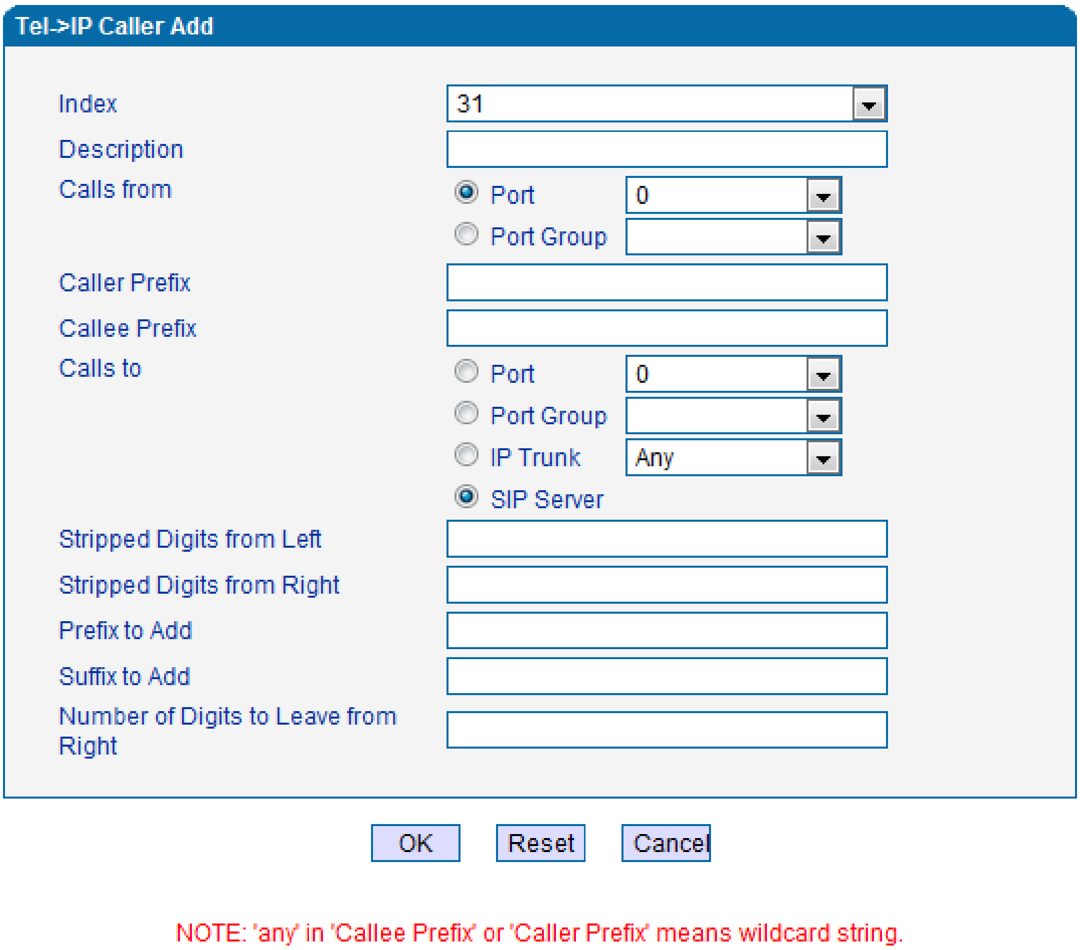


Figure 4. 10-2 Tel-IP Caller

Configuration parameters are the same with "IP->Tel Callee".

4.10.3 Tel-IP Callee

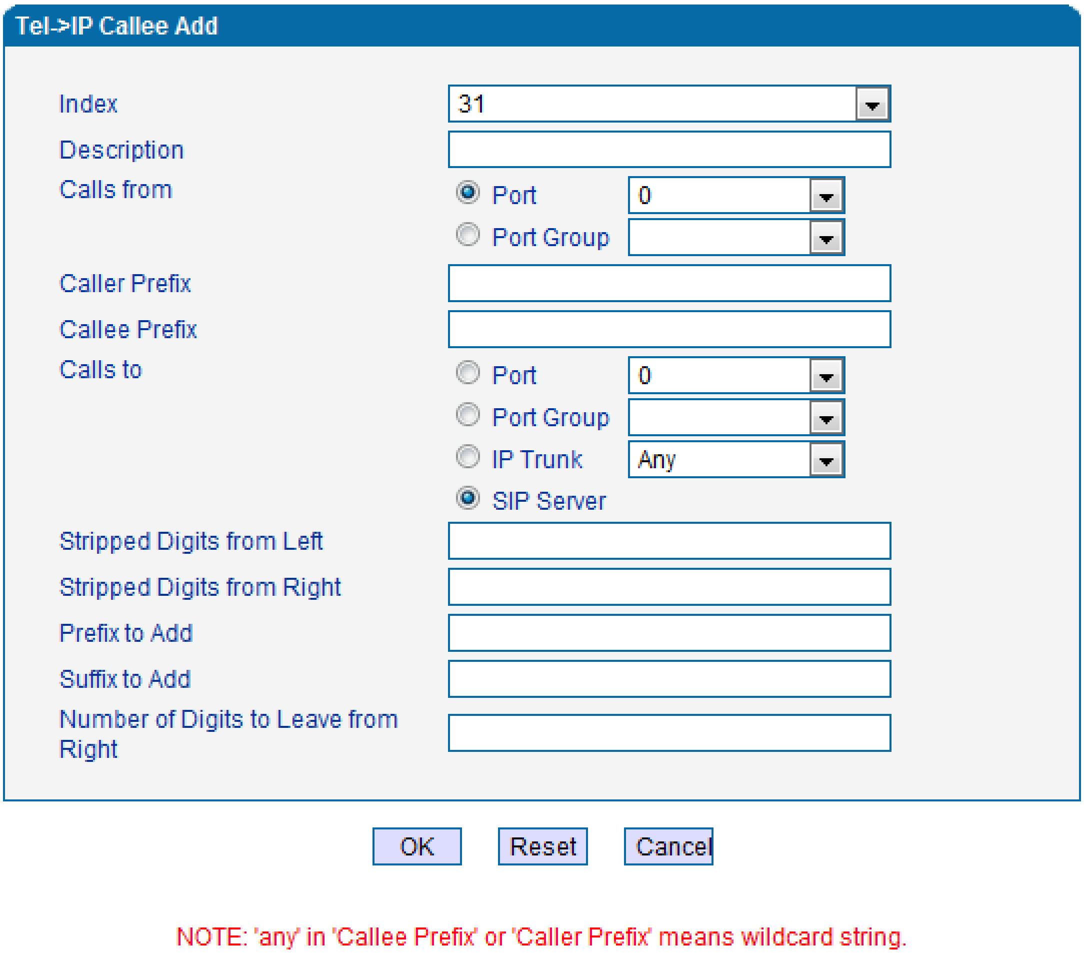


Figure 4.10-3 Tel-IPCallee

Configuration parameters are the same with "Tel->IP Caller".

4.11 Maintenance

4.11.1 syslog Parameter

Syslog is a protocol used in (TCP/IP) network transmission of record of the standard file information.

Syslog agreement belongs to a kind of master slave agreement: Syslog sender will sent a small text information (less than 1024 bytes) to syslog the receiver. The receiver are: "syslogd"、"syslog daemon" or syslog server. Syslog message can be transferred by TCP/UDP.

Syslog level：

- none　　Used to misarrange
- debug　　Not including function conditions or the question of other information
- notice　　importance common conditions
- warning　　Early warning information
- error　　Stop error conditions of tools or some part of the realization of the function subsystem

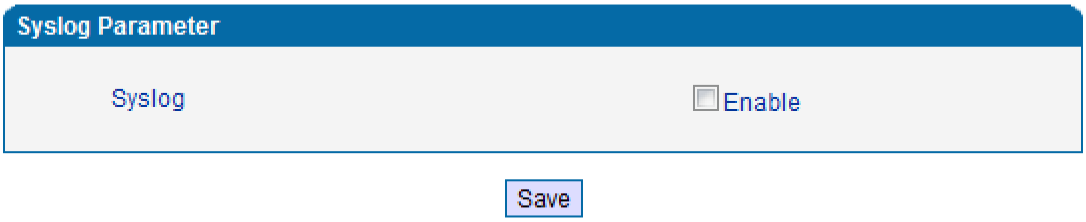


Figure 4.11-1 Syslog Parameter Configuration

Enable send CDR, and then send communication information to syslog server.

4.11.2 Firmware Upload

The process of firmware upload：

1）Click "Firmware Upload"

2) Browse files and choose the loading program (Name the file extension. ldf)

3) Click "Upload", the upload process will last about 60s and device can automatically restart after uploading.（The firmware update process don't shut off the power）

Figure 4.11-2 Firmware upload Configuration

4.11.3 Data Backup

The process data backup:

1) Click "Data Backup"

2) Click "Backup" to backup data to PC.

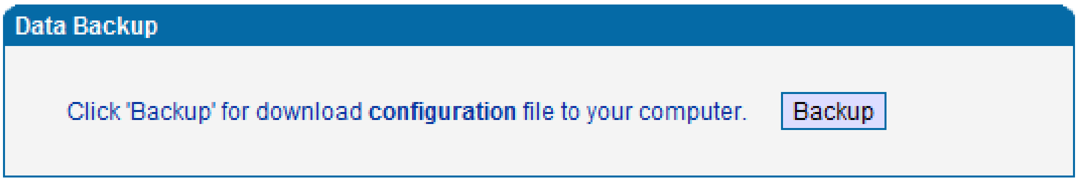


Figure 4.11-3 Data Backup Interface

4.11.4 Data Restore

The processes of data restore:

1) Click "Data Restore"

2) Browse file, select data file.

3) Click "Restore" and then import successfully, the device will restart automatically.

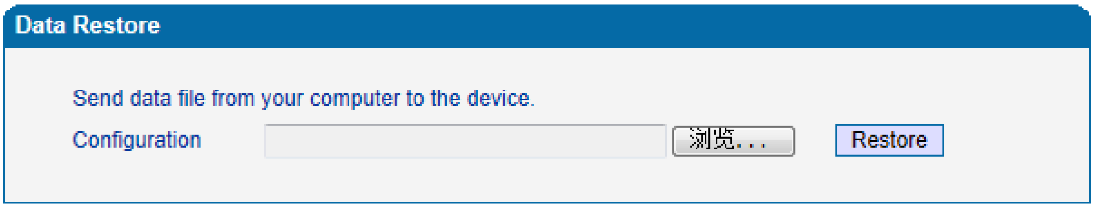


Figure 4.11-4 Data Restore Interface

4.11.5 Ping Test

Send test data packets to IP, check each other whether have response and statistical response time. It is ping. Used to test internet and analyzed network fault.

Application format：Ping IP address. It is used to check the network connectivity or network connection speed command.

Pinginstructions:

1) Click "ping test"

2) Fill IP address or domain connected, click start.

3) Received a message indicates that network connection normal, or network connected to a fault.

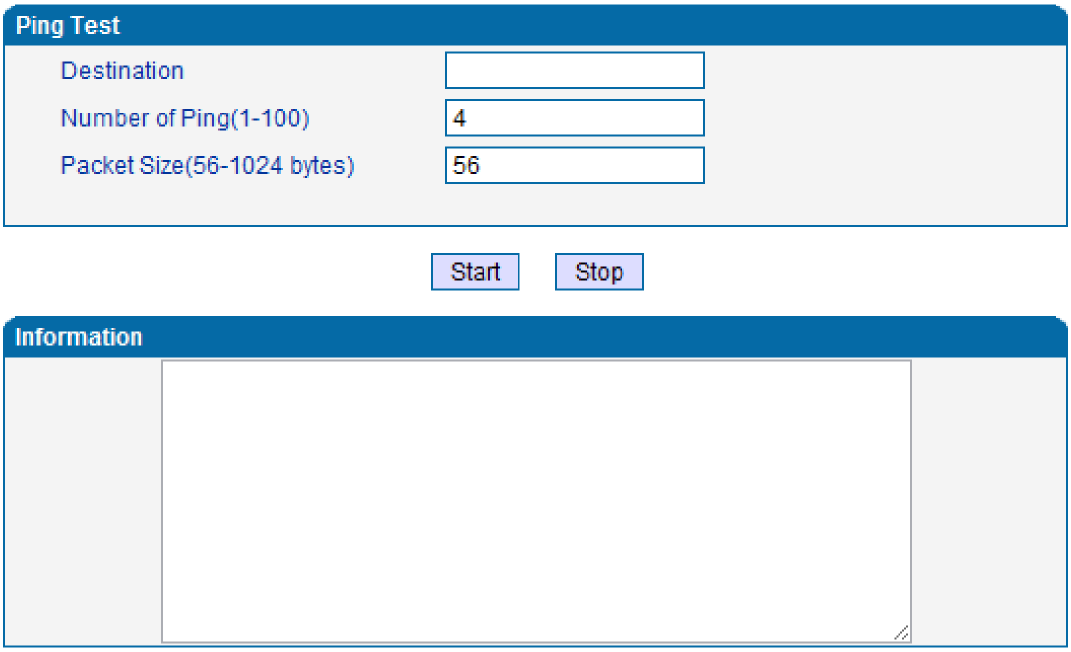


Figure 4.11-5 Ping Parameter Interface

4.11.6 Tracert Test

Tracert is trace router and used to tracking routing.

Tracert sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host. Determining the intermediate routers traversed involves adjusting the time-to-live (TTL), aka hop limit, Internet Protocol parameter. Frequently starting with a value like 128 (Windows) or 64 (Linux), routers decrement this and discard a packet when the TTL value has reached zero, returning the ICMP error message ICMP Time Exceeded. Tracert works by increasing the TTL value of each successive set of packets sent. The first set of packets sent have a hop limit value of 1, expecting that they are not forwarded by the first router. The next set have a hop limit value of 2, so that the second router will send the error reply. This continues until the destination host receives the packets and returns an ICMP Echo Reply message.

Trace route uses the returned ICMP messages to produce a list of hops (which usually consists of routers and layer 3 switches) that the packets have traversed. The timestamp values returned for each router along the path are the delay (aka latency) values, typically measured in milliseconds for each packet.

Tracert introduce：

1) Click tracert test.

2) Fill IP address or domain connected, click start.

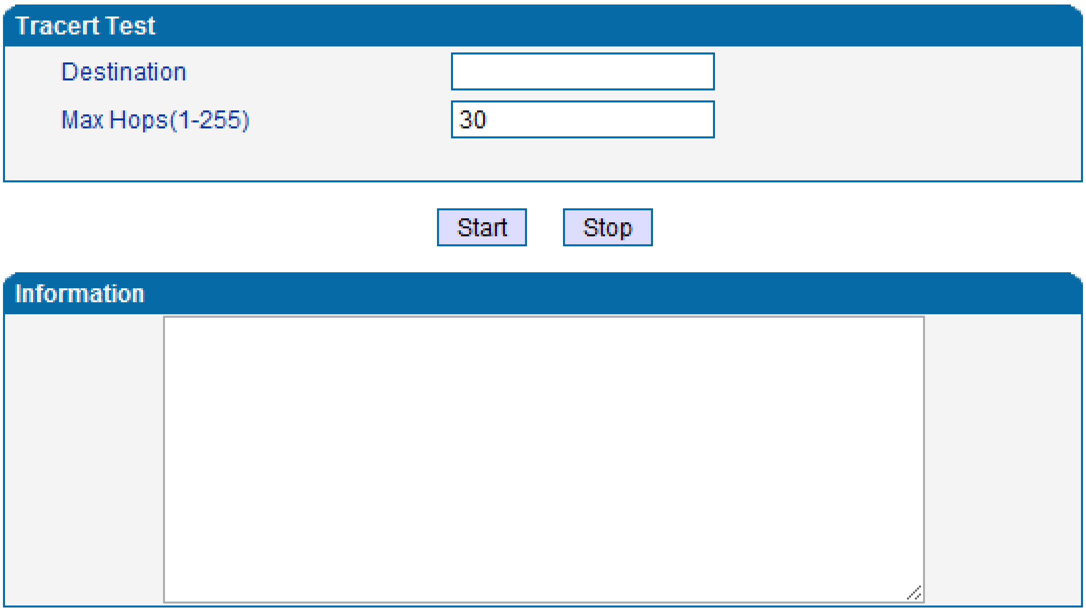


Figure 4.11-6 Tracert Test Interface

4.11.7 Password Modification

Includes WEB username and password, Telenet username and password modify.

Note：Default web and telnet username and password is: admin, admin.

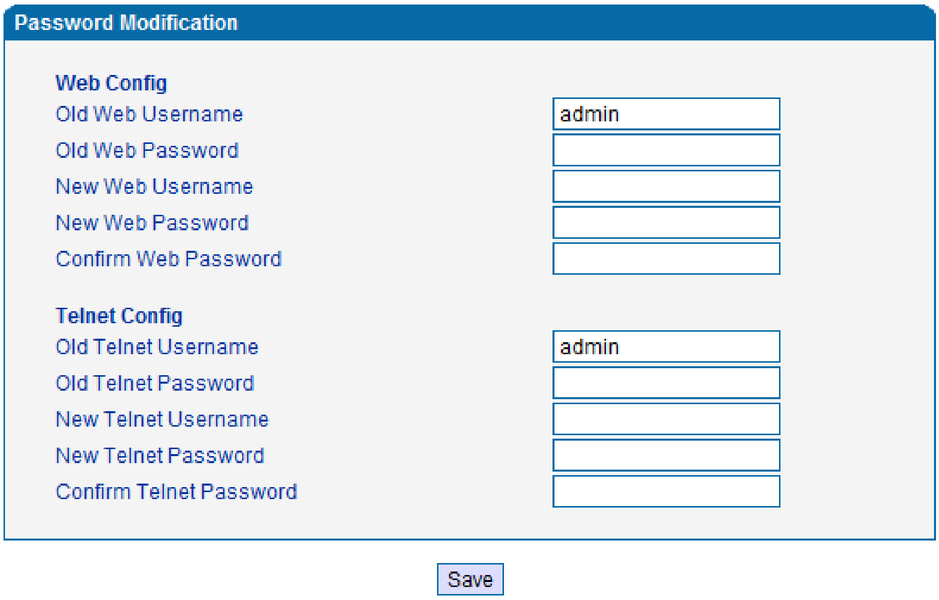


Figure 4.11-7 Password Modification Interface

4.11.8 Factory Reset

Click “Apply” to restore the factory settings.

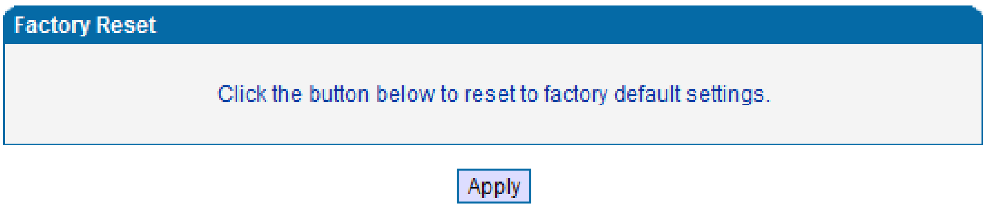


Figure 4. 11-8 Factory Reset Interface

4.11.9 Device Restart

Click the “Save” button in the Configuration page to save the changes to the equipment configuration. The following screen confirms that the changes are saved. If the changes need restart, reboot or power cycle the equipment to make the changes take effect.

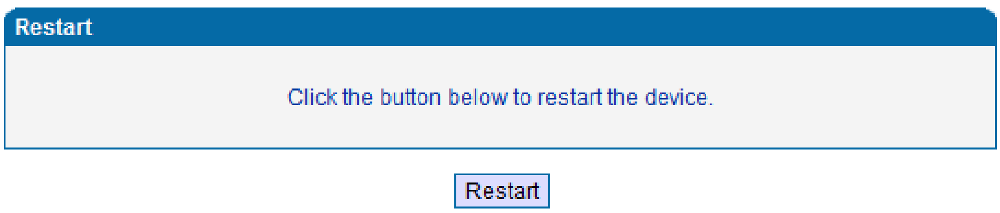


Figure 4.11-9 Device Restart

5. Glossary

- DNS：Domain Name System
- SIP：Session Initiation Protocol
- TCP：Transmission Control Protocol
- UDP：User Datagram Protocol
- RTP：Real Time Protocol
- PPPOE：point-to-point protocol over Ethernet
- VLAN：Virtual Local Area Network
- ARP：AddressResolution Protocol
- CID：Caller Identity
- DND：Do NOT Disturb
- DTMF：Dual Tone Multi Frequency
- NTP：Network Time Protocol
- DMZ：Demilitarized Zone
- STUN：Simple Traversal of UDP over NAT
- PSTN：Public Switched Telephone Network