DAG2000-32 FXS Voice Gateway

User Manual V2.0

Revision Records

File Name	DAG2000-32FXS Voice Gateway User Manual
Document Version	2.0
Firmware Version	2.15.02.02
Date	2012/03/16
Revised by	Technical Support Department

Table of Contents

1. Equipment Introduction

1.1 Overview

Thanks for purchasing Dinstar DAG2000-32 (hereinafter referred to as the DAG) FXS analog voice gateway.DAG2000 series FXS analog gateway is voice/fax access gateway based on IP network. It can provide high efficiency, high quality VoIP business for operators, the family office, remote office and branch enterprise. DAG2000 series VoIP access gateway adopted standard SIP protocol and compatible with leading IP PBX, soft-switch and SIP-based platform. DAG2000 series products used strong hardware technology solutions and have a good voice/fax handling ability, high stability. It is the best VOIP equipment choice for commercial.

DAG2000 series FXS analog gateway includes following model:

- DAG2000-16S
- DAG2000-24S
- DAG2000-32S

This manual mainly to DAG2000-32S as example, introduce the function of devices and parameter configuration.

1.2 Equipment appearance

Figure 2-1DAG2000-16S

Figure 2-2DAG2000-32S

1.3 Power supply

DAG2000 is standard rack equipment, and adopts AC 110-240 V power supply.

Power parameters:

Input: 100-240V, 50-60Hz

1.4 Network Applications

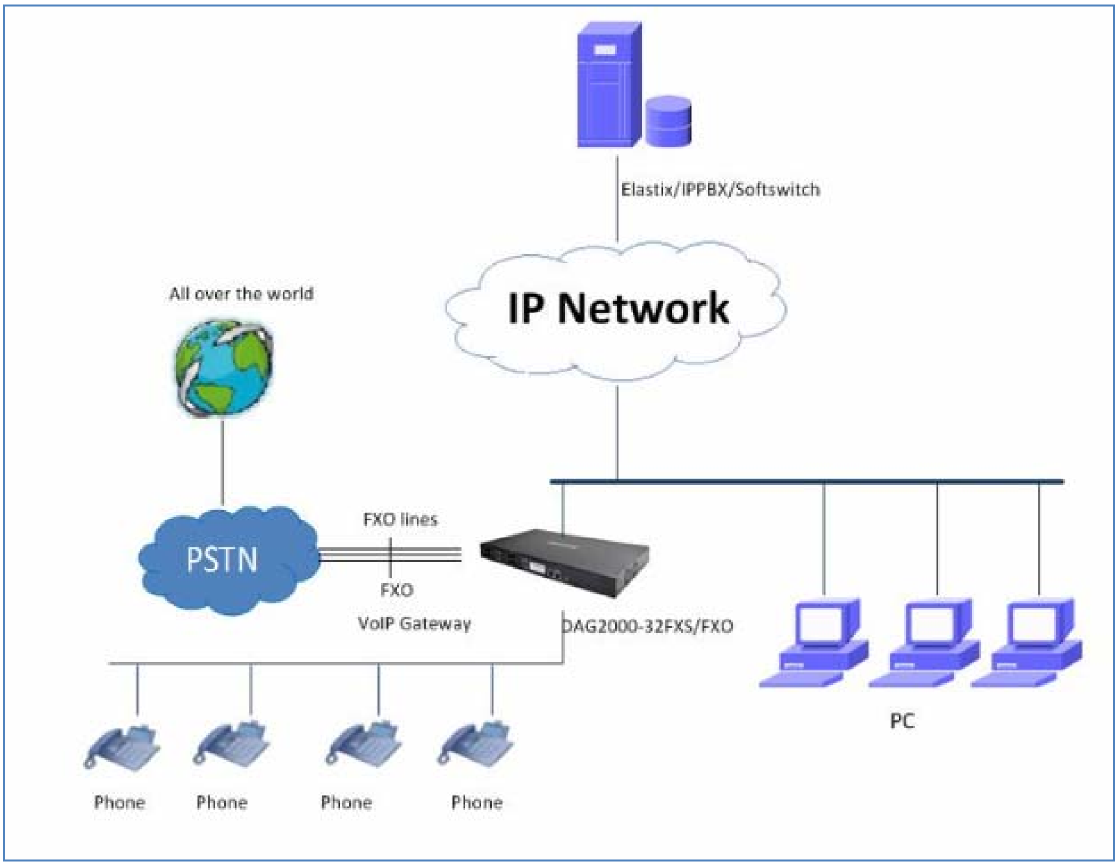


Figure 4-1：Network Applications

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

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

- Call waiting
- Call transfer (Blind transfer, Attend transfer,)
- Quick pick
- Call Forwarding Unconditional
- Call Forwarding on No Reply
- Hotline
- Call hold
- DND
- 3-way conference(24/32 port support)
- Voice mail
- Direct IP Call

2. Basic Operations

2.1 Phone Call

2.1.1 Phone or Extension Number

1) Dial the number directly and wait for 3 seconds (Default "*No dial timeout*");

2) Dial the number directly and press #.

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 Hold

Place a call on hold by pressing the "flash" button on the analog phone (if the phone has that button).Press the "flash" button again to release the previously held Caller and resume conversation. If no "flash" button is available, use "hook flash" (toggle on-off hook quickly). You may drop a call using hook flash.

2.3 Call Waiting

Call waiting tone (3 short beeps) indicates an incoming call, if the call waiting feature is enabled. Toggle between incoming call and current call by pressing the "flash" button. First call is placed on hold. Press the "flash" button to toggle between two active calls.

2.4 Call Transfer

2.4.1Blind Transfer

Blind transfer used to transfer call to the third party without inform caller. Assume that call Caller A and B are in conversation. A wants to Blind TransferB to C:

1) Caller A presses **FLASH** on the analog phone to hear the dial tone;

2) Caller A dials ***87** then dials caller C's number, and then # (or wait for 4 seconds);

3) Caller A will hear the confirm tone. Then, A can hang up.

Note:

"*Call features enable*" must be set to "Yes" in web configuration page. Caller A can place a call on hold and wait for one of three situations:

1) A quick confirmation tone (similar to call waiting tone) followed by a dial-tone. This

indicates the transfer is successful. At this point, Caller A can either hand up or make another call.

2）A quick busy tone followed by a restored call (on supported platforms only). This means the transferee has received a 4xx response for the INVITE and we will try to recover the call. The busy tone is just to indicate to the transferor that the transfer has failed.

3）Continuous busy tone. The phone has timed out.

2.4.2 Attended Transfer

Attended transfer allowsusers to confirm the third party response and decide whether to answer the calls and then transfer this call to the third party.

Assume that Caller A and B are in conversation. Caller A wants to *Attend Transfer* B to C:

1）Caller A presses **FLASH** on the analog phone for dial tone;

2）Dial Caller C's number followed by # (or wait for 3 seconds);

3）If Caller C answers the call, Caller A and Caller C are in conversation. Then A can hang up to complete transfer;

4）If Caller C does not answer the call, Caller A can press "flash" to resume call with Caller B.

2.4.3 3-way Conference

3-way conference：

1）Caller A call B,B pick up into call states;

2）Caller A hook flash, A and B into keep states, then C call A, A through to the phone.

3）A hook flash, then A、B、C into keep states, at this time if A press 1 key, then A and B continue to call; if A press 2 key, then A and B continue to call; if A press 3 key, then A、B、C three parties go to call.

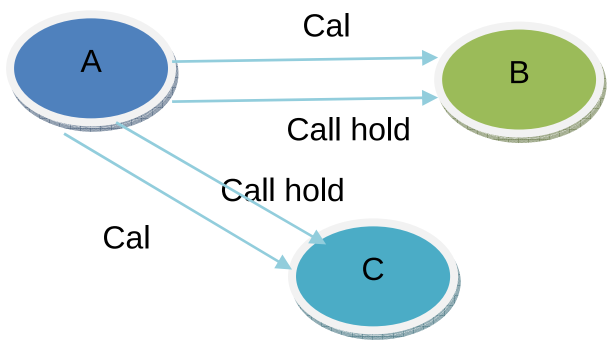


Figure 2.4-1：3-way Conference

2.5 Call Features

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

Table 2.5-1 Feature Codec

***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.

2.6 Sending and Receiving Fax

2.6.1 DAG（FXS）support four fax modes:

1）T.38（FoIP）

2）Pass-Through

3）Modem

4）adaptive

2.6.2 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 :

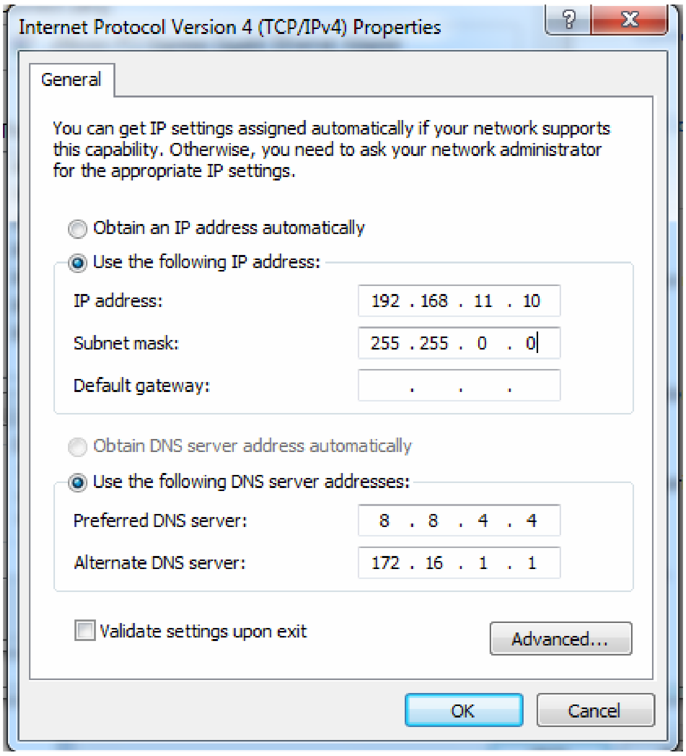


Figure 4.1-1Modify IP address

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.

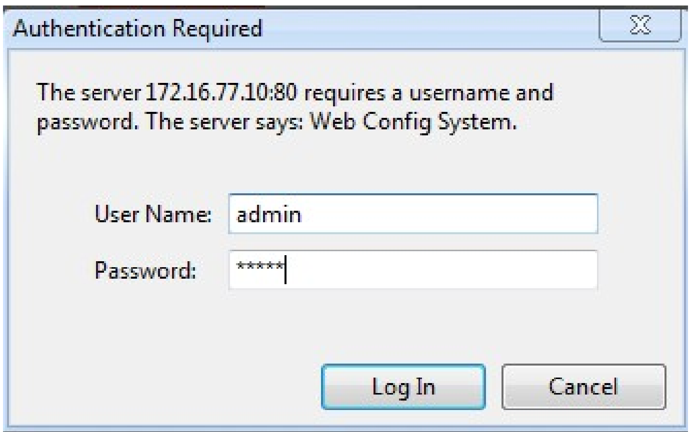


Figure 4.1-1 DAG FXS Login Interface

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

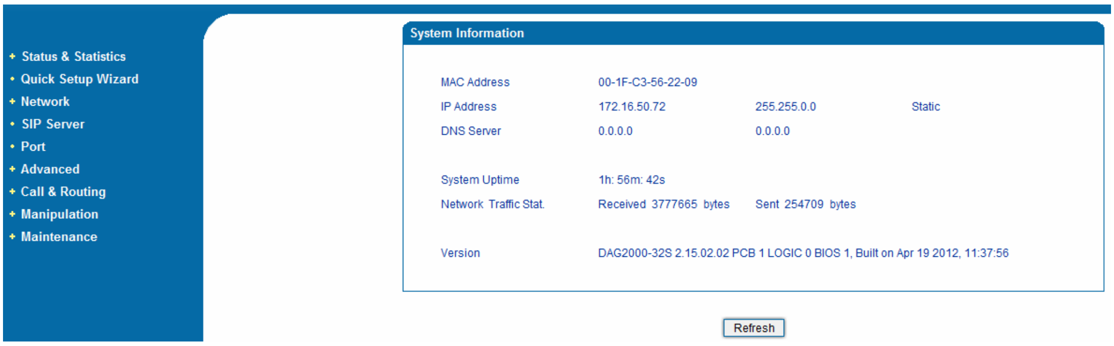


Figure 4.1-2 DAG Configure Interface

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.

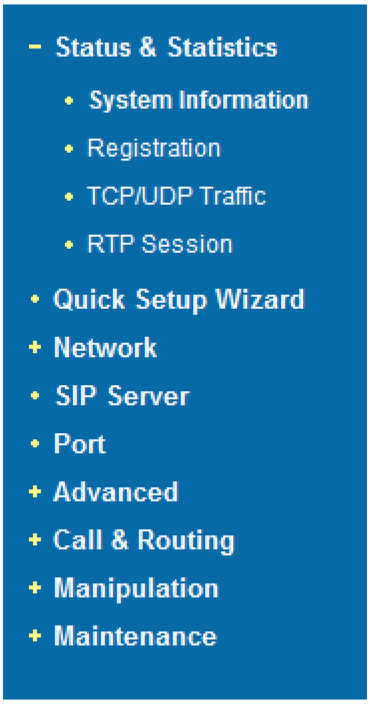


Figure 4.2-1 Navigation Tree

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.
IP Address	Shows LAN 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 wille stablish 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 field sare set to zero by default.
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
0	FXS	2200	Unregistered	---	---
1	FXS	2201	Unregistered	---	---
2	FXS	2202	Unregistered	---	---
3	FXS	2203	Unregistered	---	---
4	FXS	2204	Unregistered	---	---
5	FXS	2205	Unregistered	---	---
6	FXS	2206	Unregistered	---	---
7	FXS	2207	Unregistered	---	---
8	FXS	2208	Unregistered	---	---
9	FXS	2209	Unregistered	---	---
10	FXS	2210	Unregistered	---	---
11	FXS	2211	Unregistered	---	---
12	FXS	2212	Unregistered	---	---
13	FXS	2213	Unregistered	---	---
14	FXS	2214	Unregistered	---	---
15	FXS	2215	Unregistered	---	---
16	FXS	2216	Unregistered	---	---
17	FXS	2217	Unregistered	---	---
18	FXS	2218	Unregistered	---	---
19	FXS	2219	Unregistered	---	---
20	FXS	2220	Unregistered	---	---
21	FXS	2221	Unregistered	---	---
22	FXS	2222	Unregistered	---	---
23	FXS	2223	Unregistered	---	---
24	FXS	2224	Unregistered	---	---
25	FXS	2225	Unregistered	---	---
26	FXS	2226	Unregistered	---	---
27	FXS	2227	Unregistered	---	---
28	FXS	2228	Unregistered	---	---
29	FXS	2229	Unregistered	---	---
30	FXS	2230	Unregistered	---	---
31	FXS	2231	Unregistered	---	---

Figure 4.3-2 Port and Port group registration information

4.3.3 TCP/UDP Statistics

TCP/UDP Traffic

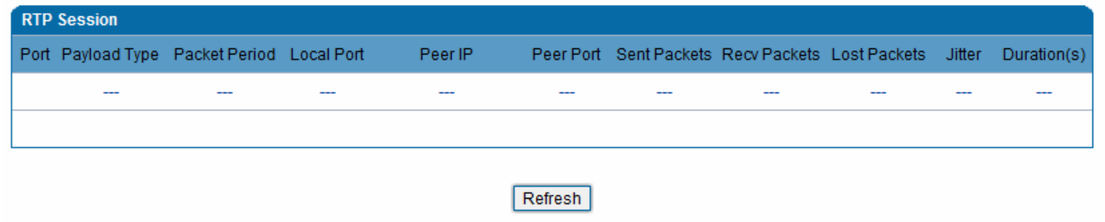
TCP Sent Packets	TCP Recv Packets	UDP Sent Packets	UDP Recv Packets
539	449	13395	8

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


RTP Session

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

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 2000 series have 4 Ethernet ports, and similar to a smaller switches. Network configuration below:

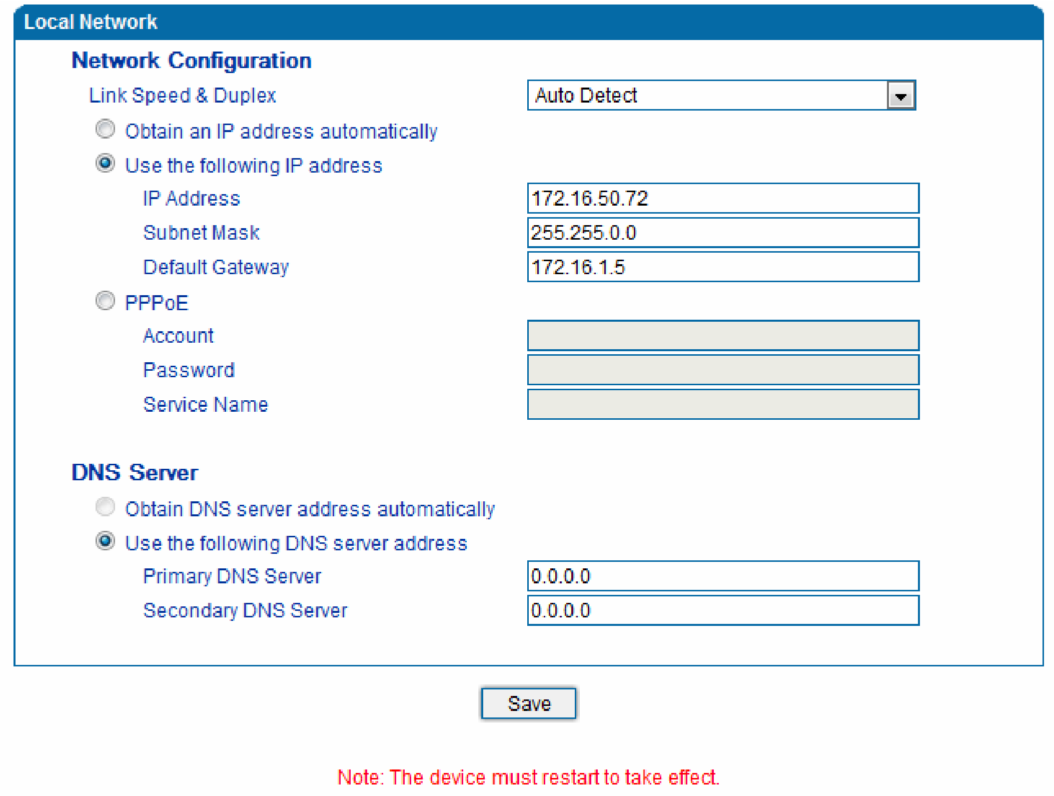


Figure 4.5-1Route Mode

- "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.

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. 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.

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 packet 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:

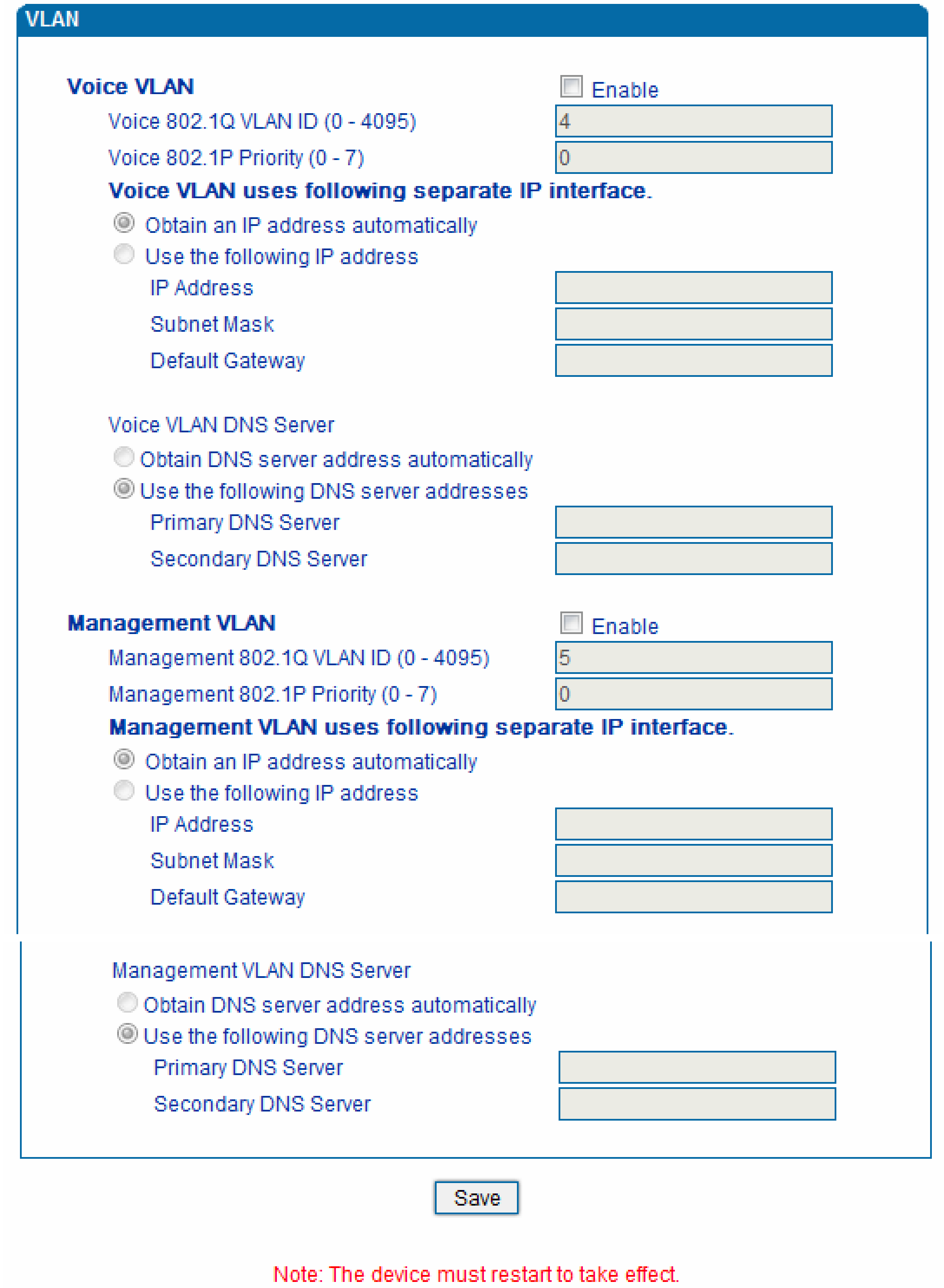


Figure 4.5-3 VLAN parameter configuration

Table 4.5-1 VLAN 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)	802.1p 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 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:

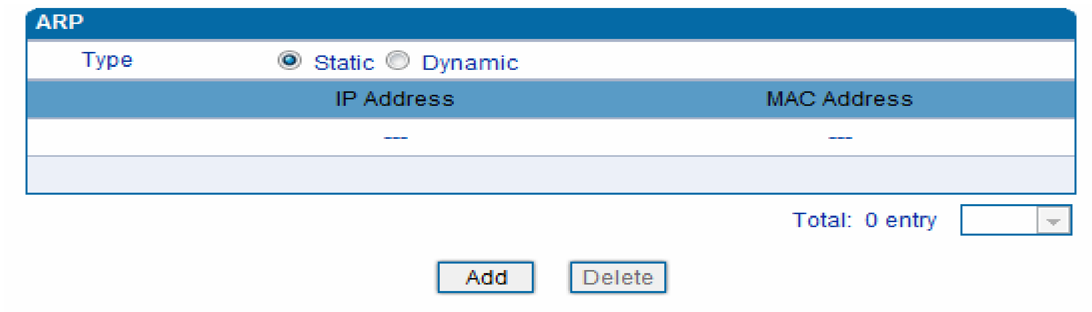


Figure 4.5-4 ARP Parameters

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:

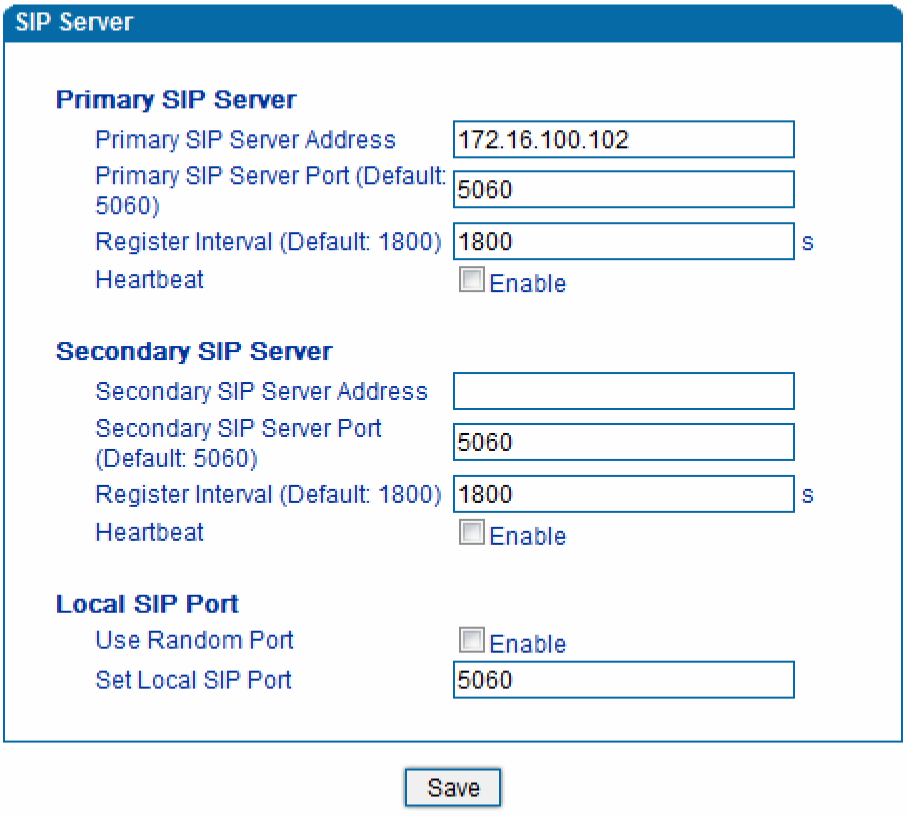


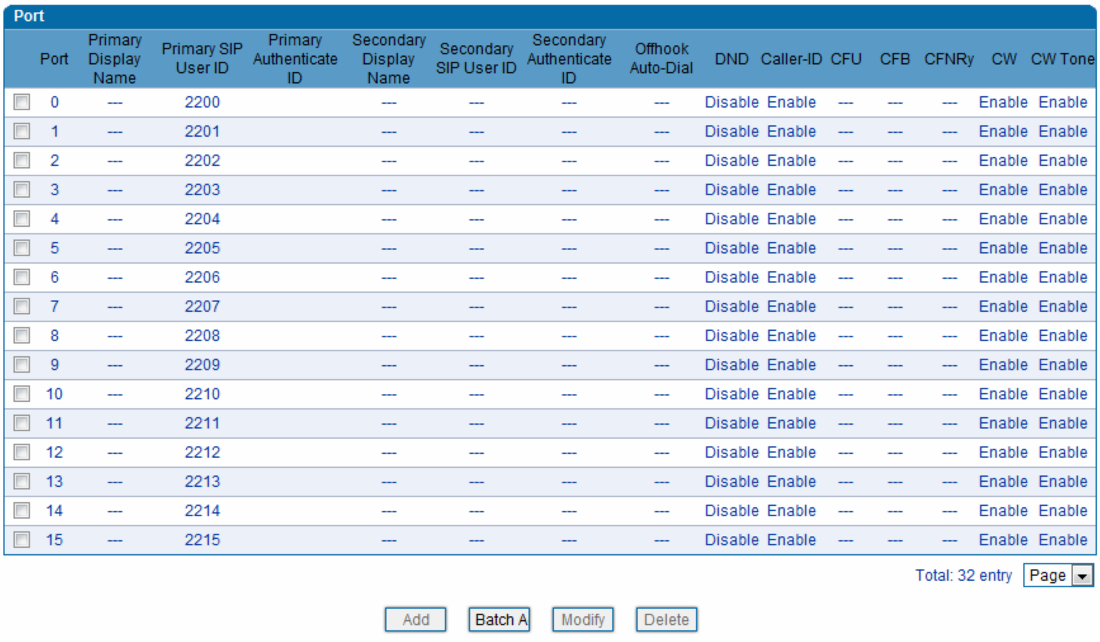
Figure 4.6-1 SIP Server Configuration Interface

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.



Port

Port	Primary Display Name	Primary SIP User ID	Primary Authenticate ID	Secondary Display Name	Secondary SIP User ID	Secondary Authenticate ID	Offhook Auto-Dial	DND	Caller-ID	CFU	CFB	CFNRy	CW	CW Tone
0	---	2200	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
1	---	2201	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
2	---	2202	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
3	---	2203	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
4	---	2204	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
5	---	2205	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
6	---	2206	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
7	---	2207	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
8	---	2208	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
9	---	2209	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
10	---	2210	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
11	---	2211	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
12	---	2212	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
13	---	2213	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
14	---	2214	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable
15	---	2215	---	---	---	---	---	Disable	Enable	---	---	---	Enable	Enable

Total: 32 entry Page

Add Batch A Modify Delete

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
DND	Do not disturb, the phone set won't receive any calls in case it enabled

Caller ID	Enable or disable caller ID for corresponding port
Number for CFU	call forward unconditional, all incoming calls willforward to pre-assigned number automatically
Number for CFB	Call forward on busy, if the line is busy, the call will forward to pre-assigned number automatically
Number for CFNRy	Call forward no reply, if the line is not answer the call, the call will forward to pre-assigned number automatically
Call Waiting	If call waiting enabled, it will send a special tone if another caller tries to reach you when you are using your telephone
Play Call Waiting Tone	Enable call waiting tone, caller will hear special tone.

4.8 Advanced

4.8.1 FXS parameters

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

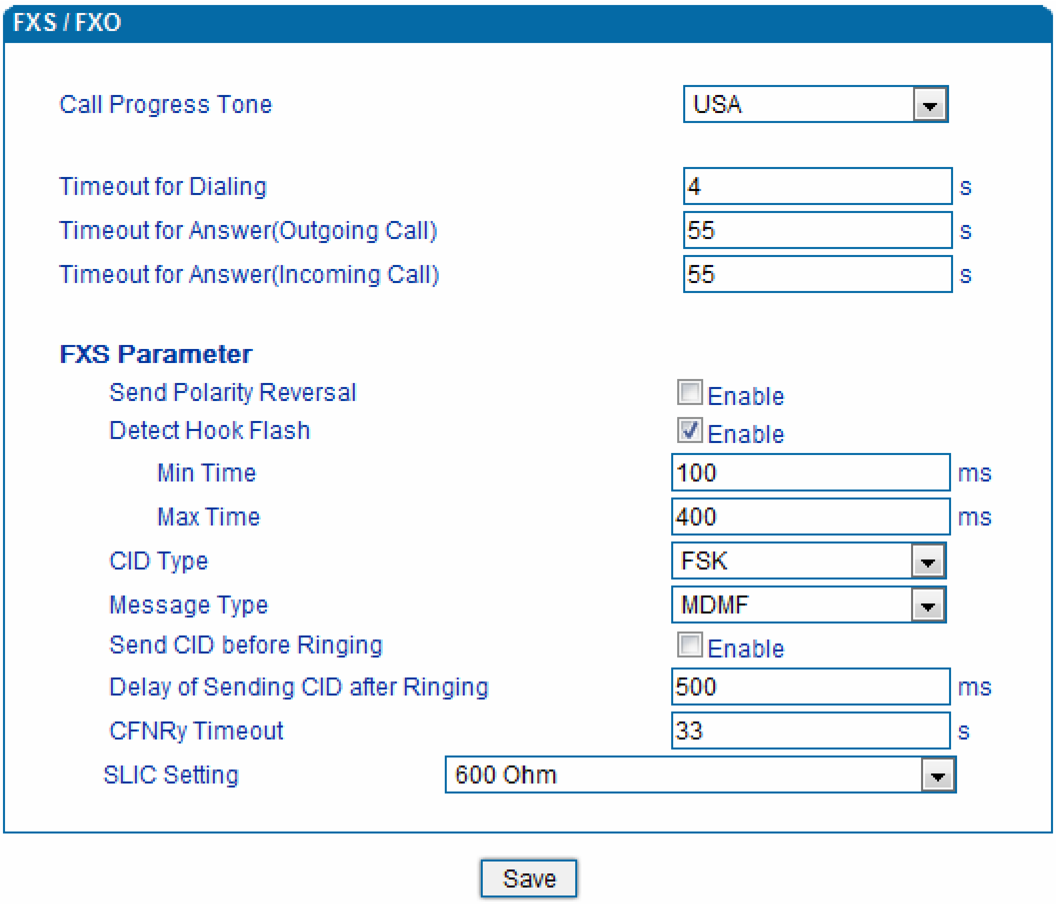


Figure 4.8-1 FXS Parameters Configuration Interface

FXS parameters description:

Call Process 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 whenmakes outgoing call on extension.
Timeout for answer(Incoming call)	This timer set how long the phone sets ringing when get incoming call
Send Polarity Reversal	Enable polarity reversal to billing.
Detect Hook flash	A protruding button where putting the receiver boards, called Flash. Always press is hang up, pick up the receiver, the fork lift machine from reed called, by hand clap called "Hook flash". Hook flash is a process that put the flash fast by pressing and let go. In essence is to cut off the dc access about 80 to 200 ms. Then switches don't think it's hang on, but keep the call, taking some other operating. The typical application of hook flash is the telephone switchboard. When need to transfer the call to other extension, then telephone hook flash to transfer the call.
CID Type	There are DTMF and FSK, General for the default.
Message Type	The call display formats SDMF and MDMF, General for the default
Send CID before Ringing	After enable this configuration, The DAG send caller to phone set before ringing, otherwise the caller ID will display after ringing.
Delay of sending CID after Ringing	Definite delay timer of caller ID while it set to send caller ID after ringing. Its Default value 500ms
SLIC Setting	Set the unit impedance

4.8.2 Media Parameter

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

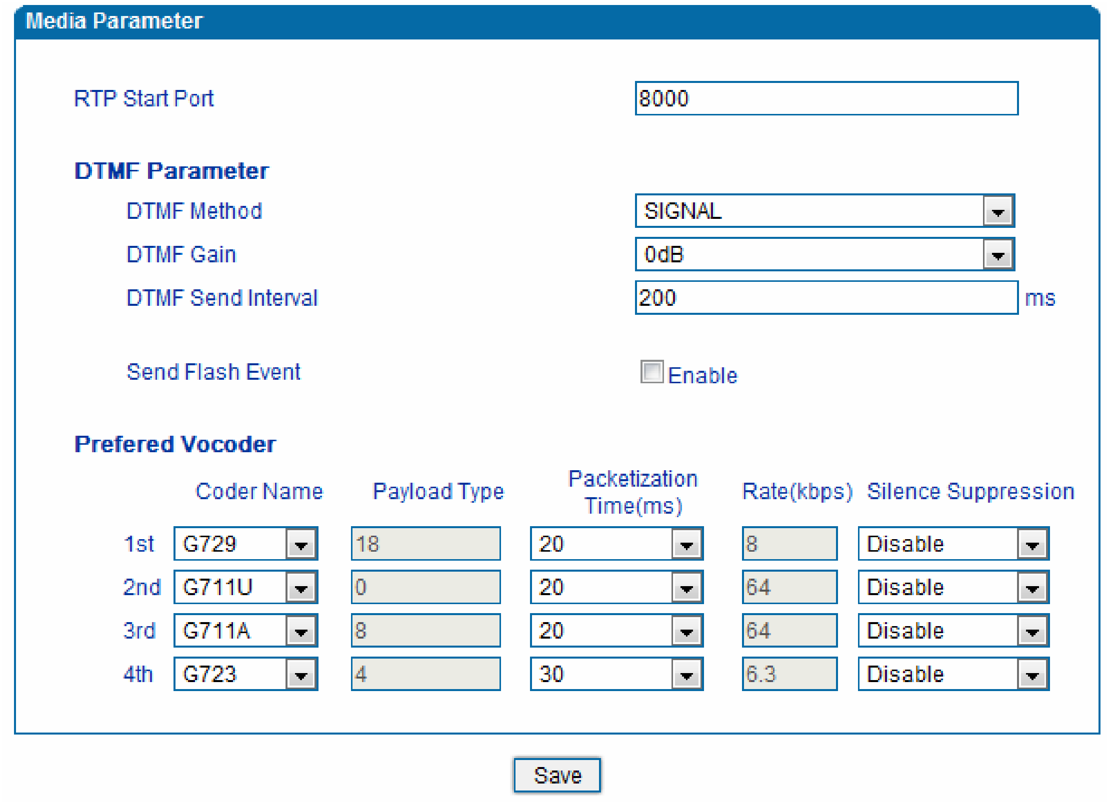


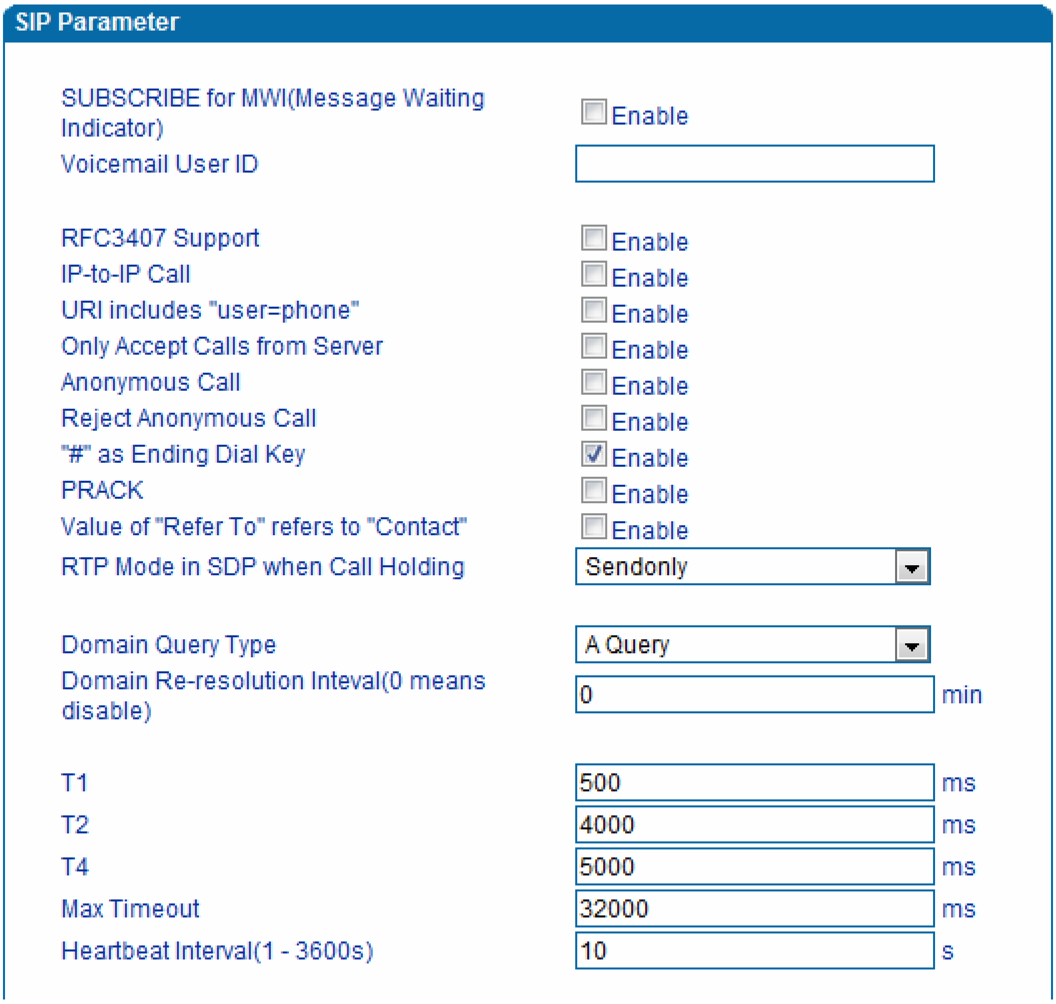
Figure 4.8-2 Media Parameter Configuration Interface

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



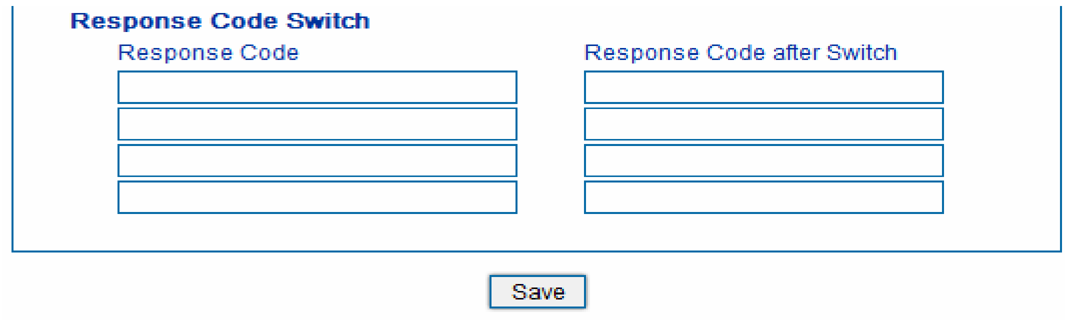


Figure 4.8-3 SIP Parameter Configuration Interface

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
RFC34077 Support	Docking parameters, the SDP simple ability statement
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 party contact with the third party through 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 Elastixas 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 :

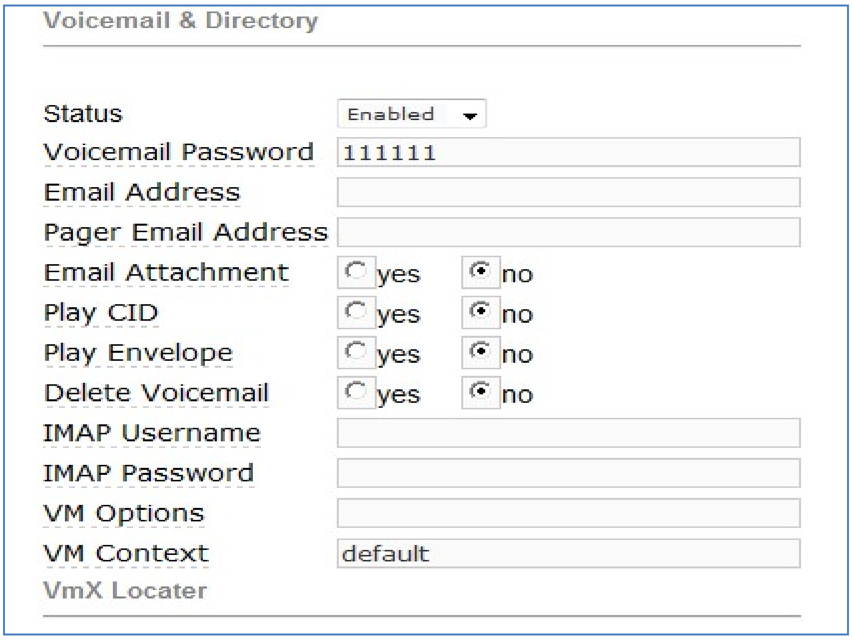


Figure 4.8-4 Elastix Voicemail Configuration Interface

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

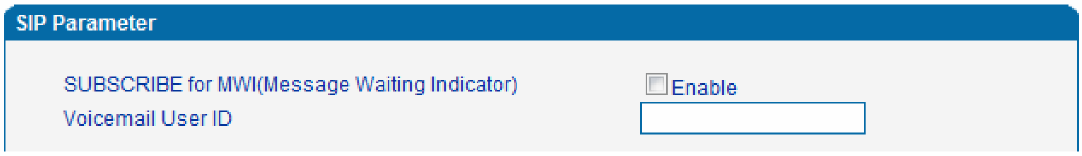


Figure4.8-6 Voice Mail Setting In SIP Parameter

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

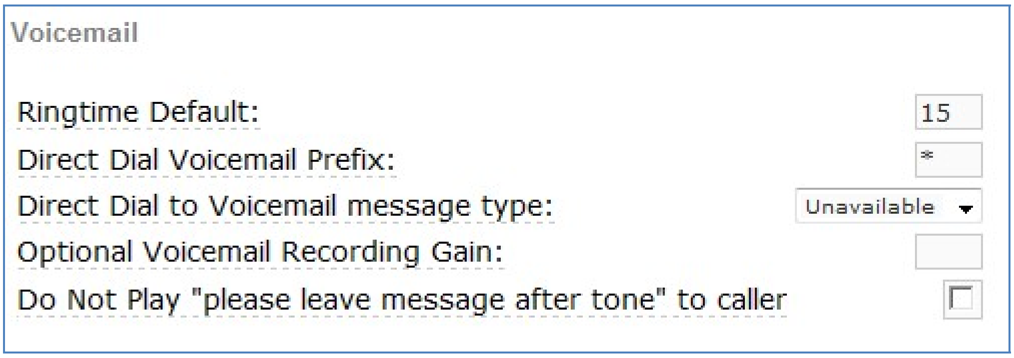


Figure 4.8-7 Voicemail Setting

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.

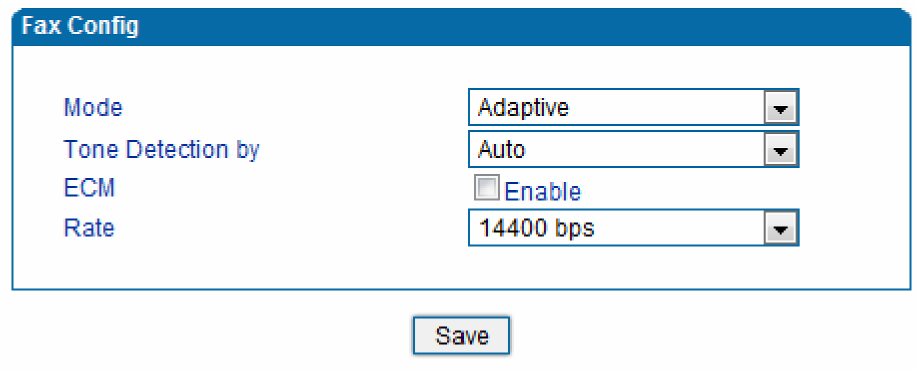


Figure 4.8-8 Fax Parameter Configure Interface

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

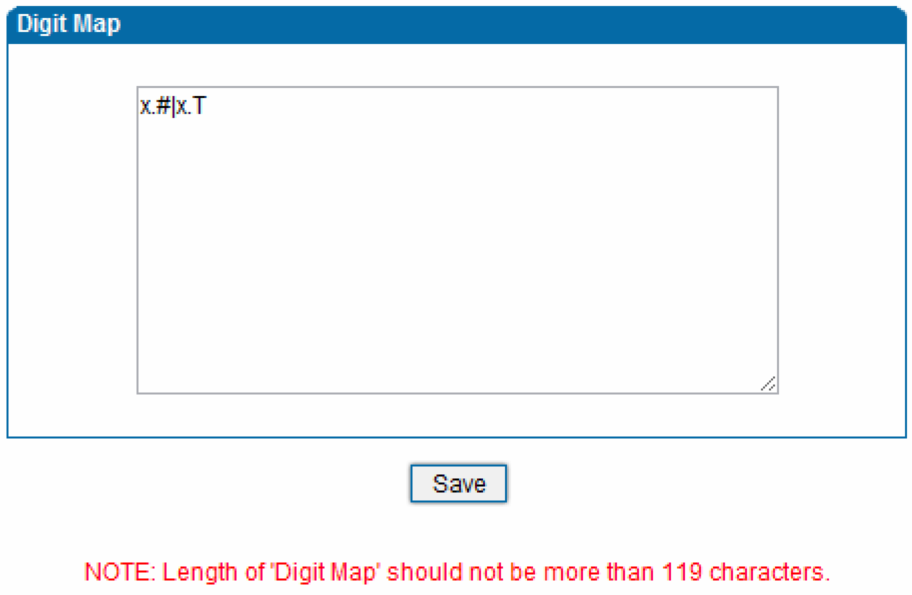


Figure 4.8-9Digit Map

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

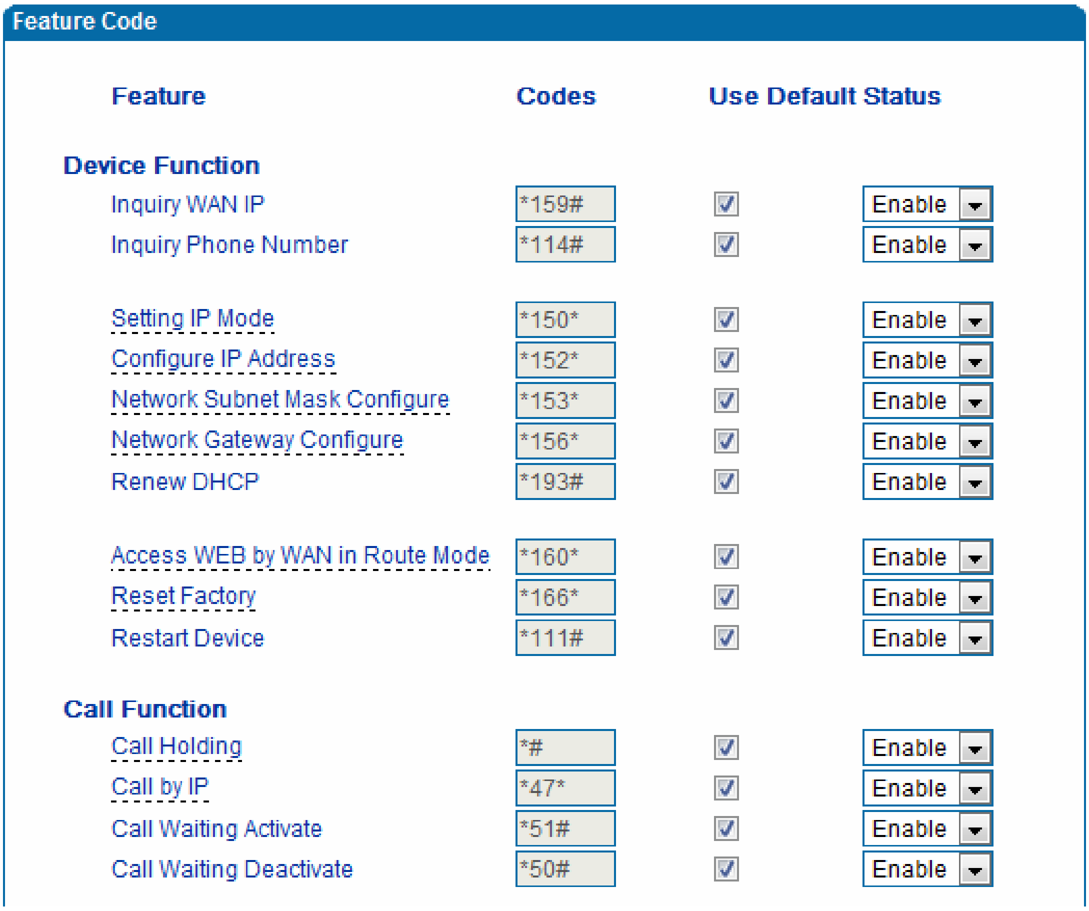
Means that first is "13","15" or "18", followed by 8 digits.

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:



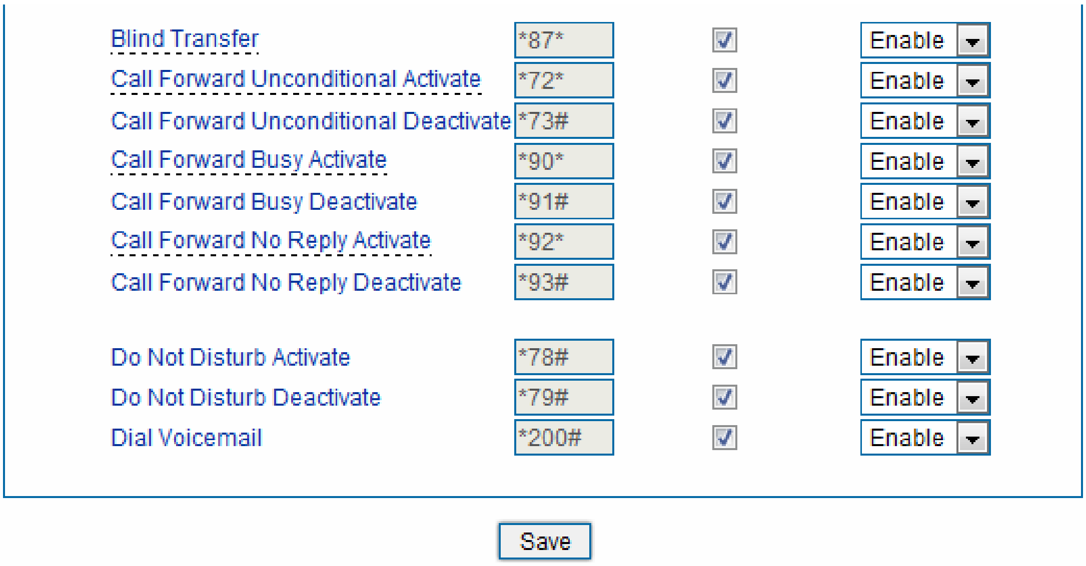


Figure 4.8-10 Feature Code Configuration Interface

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 pppoe modem, *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

NAT traversal has two modes: STUN, static NAT. When select STUN, STUN server should be configured; select static NAT, just configure NAT IP address.

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.

3) Provision : Auto Provisioning can be used to provide general and specific configuration

parameters ("Settings") to the DAGsand to manage firmware actualization.

System parameter configuration interface as follow:

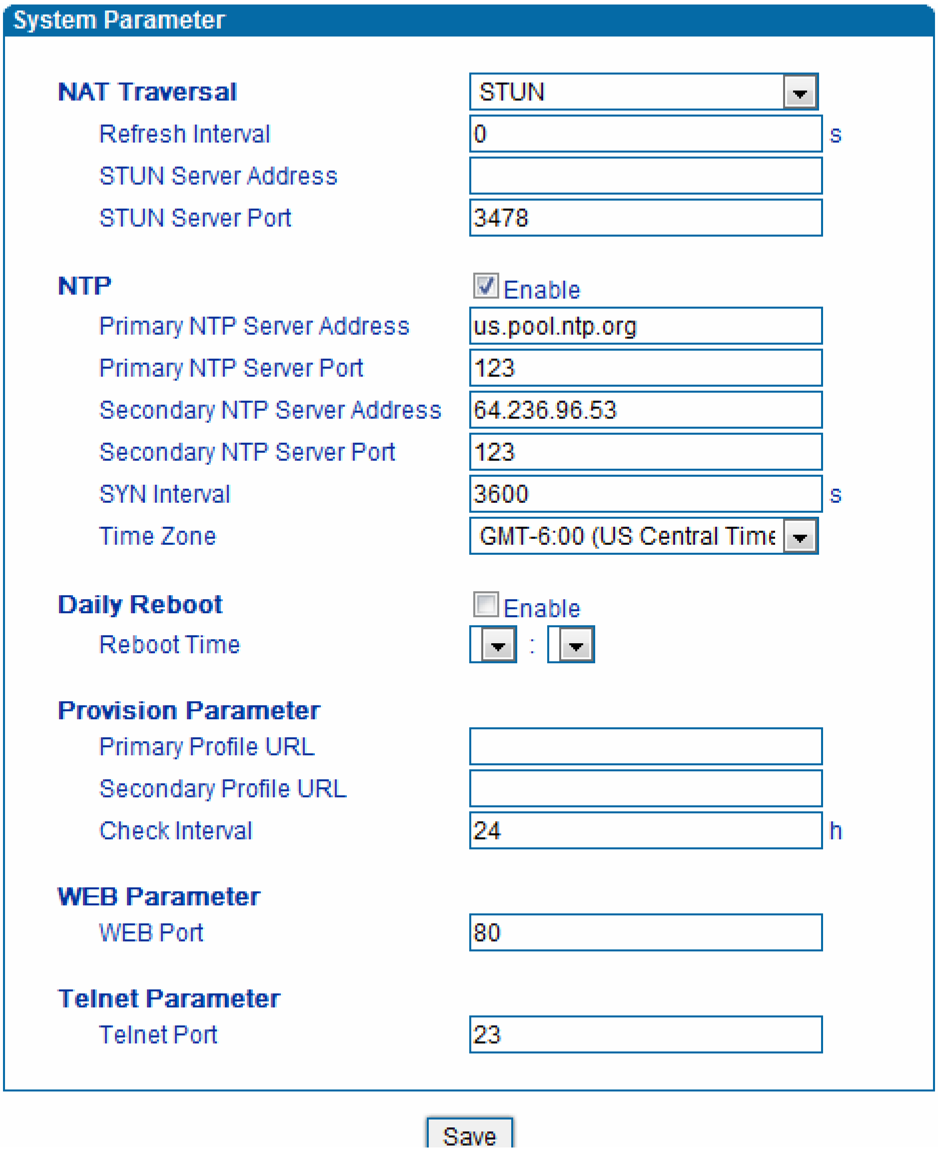


Figure 4.8-11System Configuration Interface

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.
Primary Provision server IP	Server IP address or domain provided by Provision server.
Secondary Provision server IP	Server IP address or domain provided by Provision server.
Check Interval	Every once in a while check whether a program or configuration files need to be updated. System default 24 hours
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:

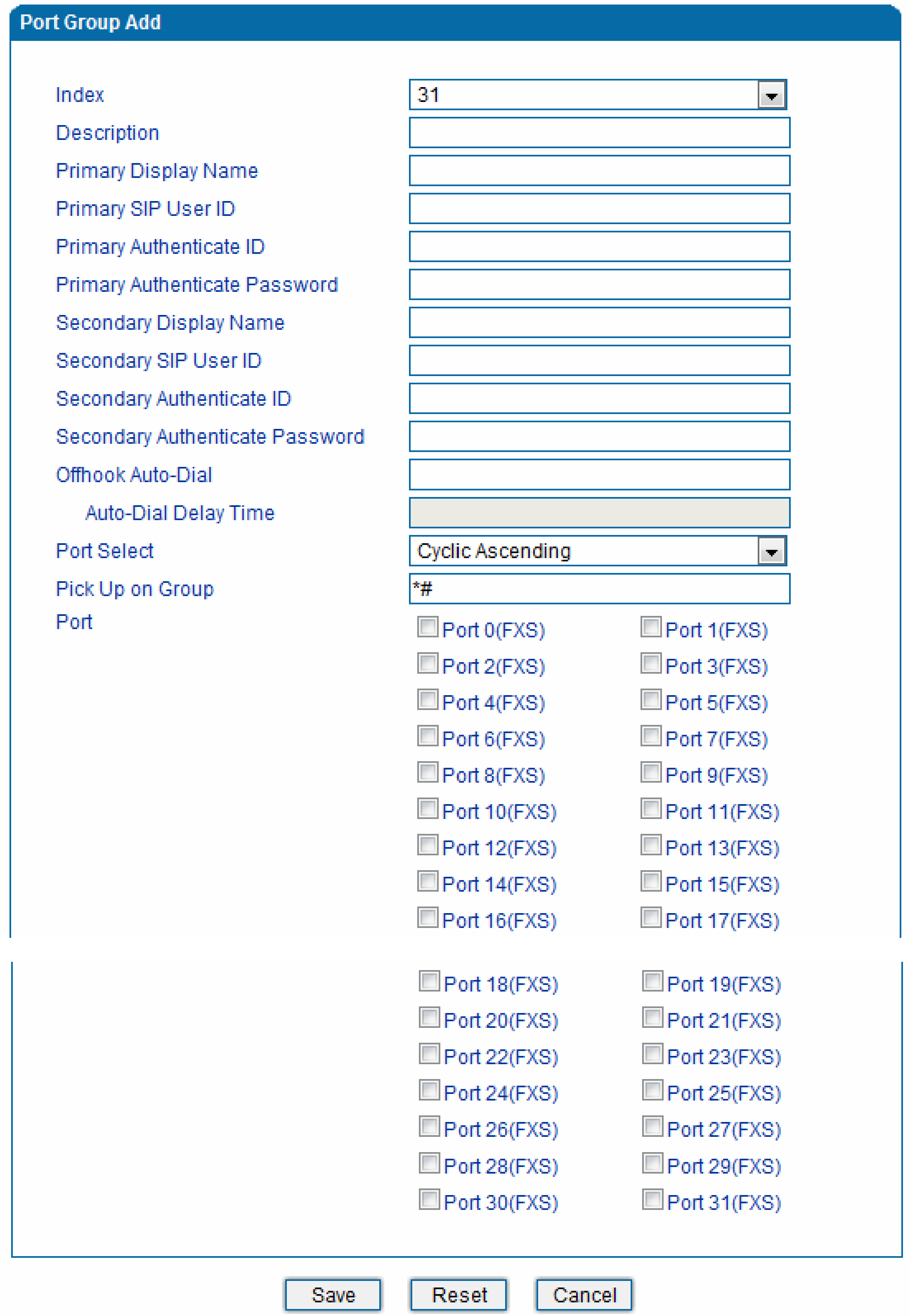


Figure 4.9-1 port group configuration interface

Index	Port group number, It uniquely identifies a route, range from 0-7
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=z9hG4bK776asdhds 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
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
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.

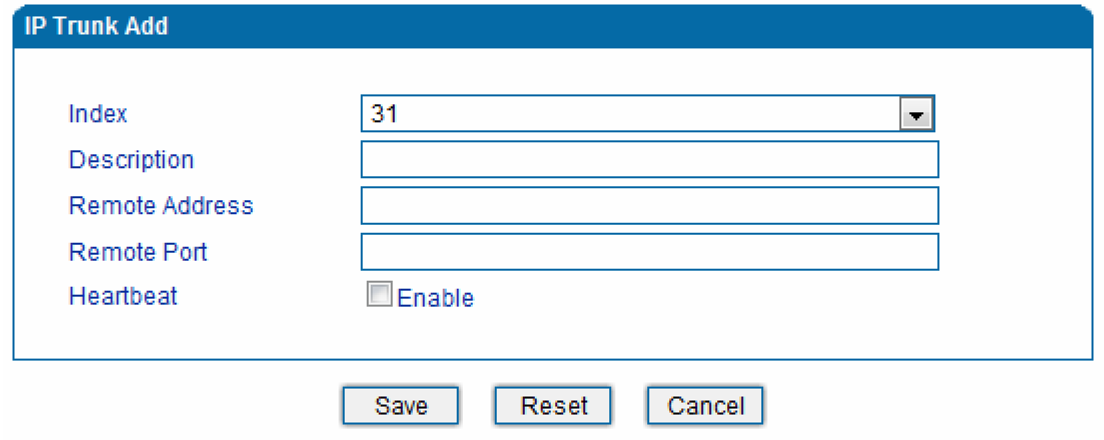
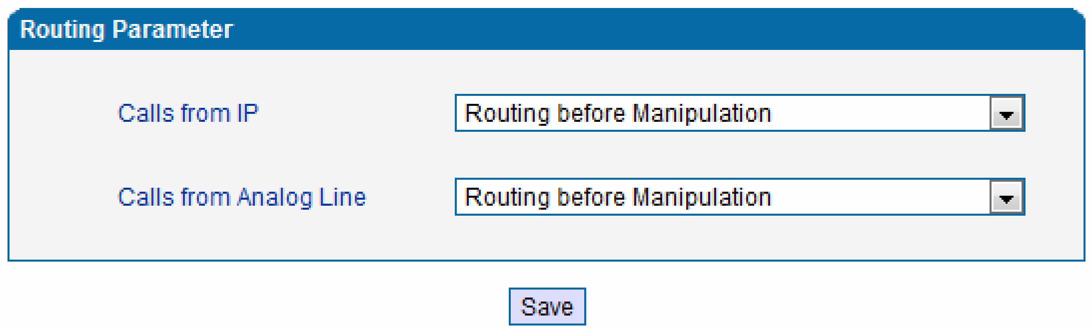


Figure 4.9-2 IP Trunk Configuration Interface

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

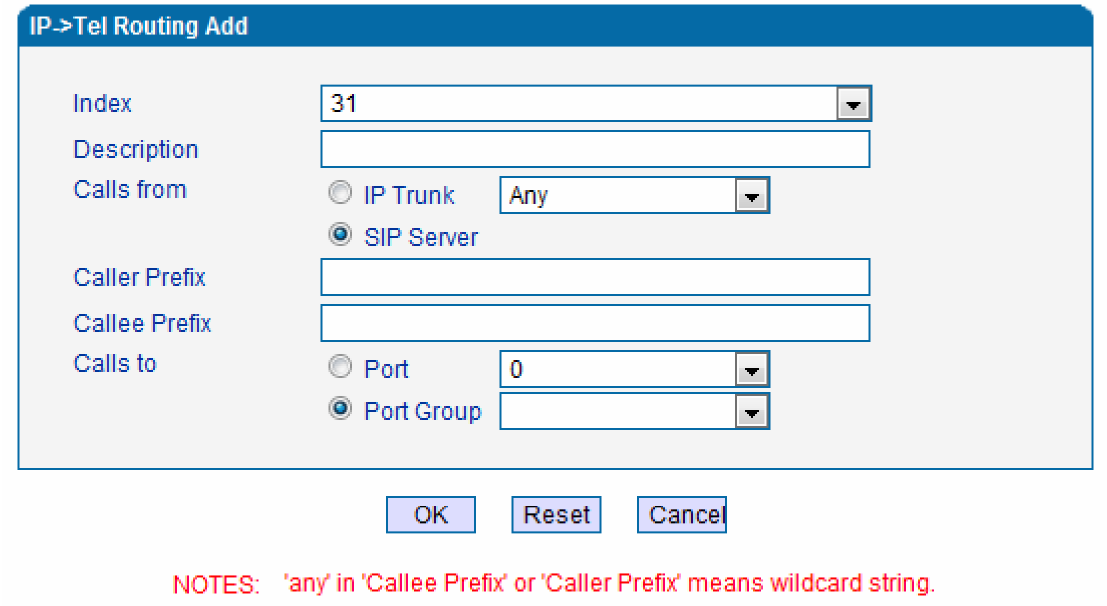


Figure 4.9-4 IP-Tel Routing Parameter

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

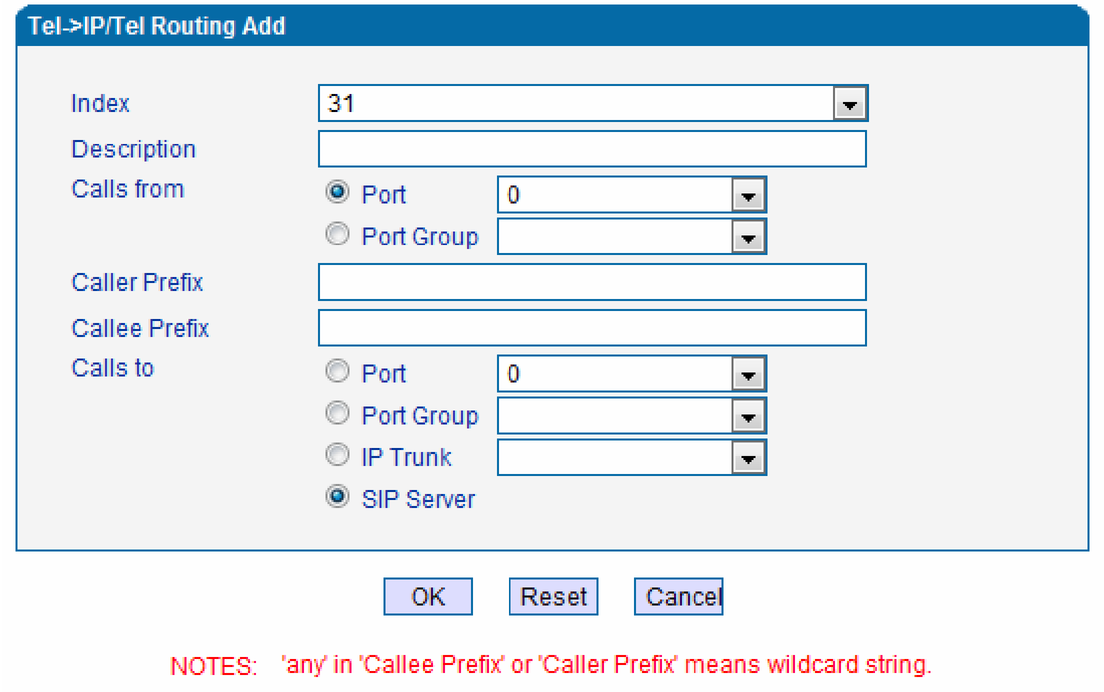


Figure 4.9-5 Tel-IP/Tel Parameters Configuration

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

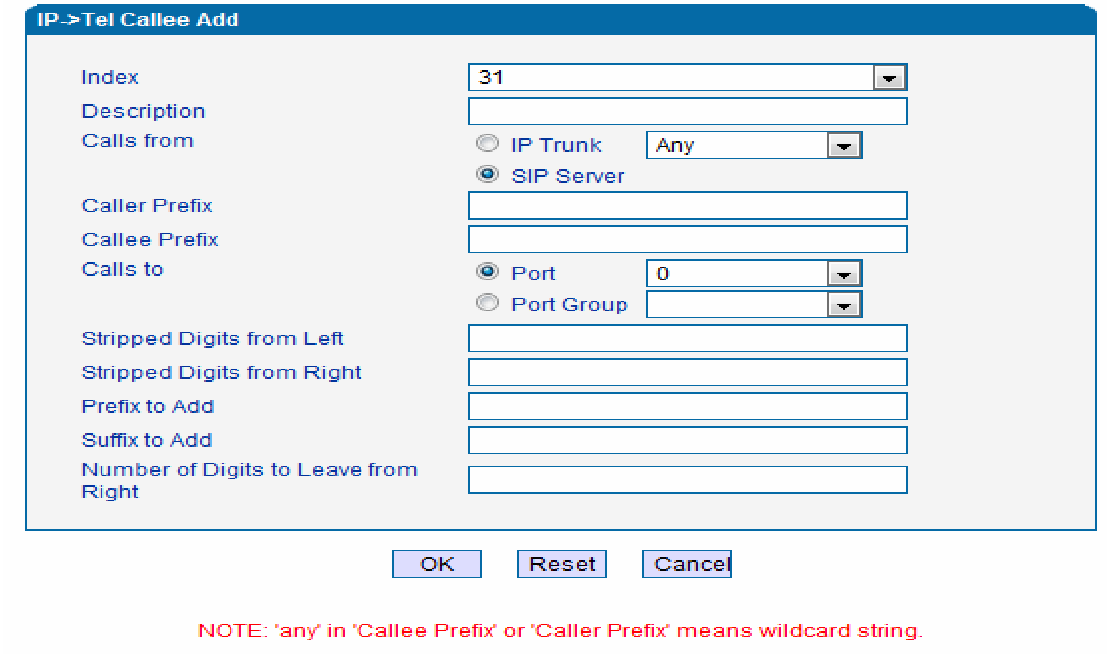


Figure 4.10-1 IP-Tel Callee number configuration

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

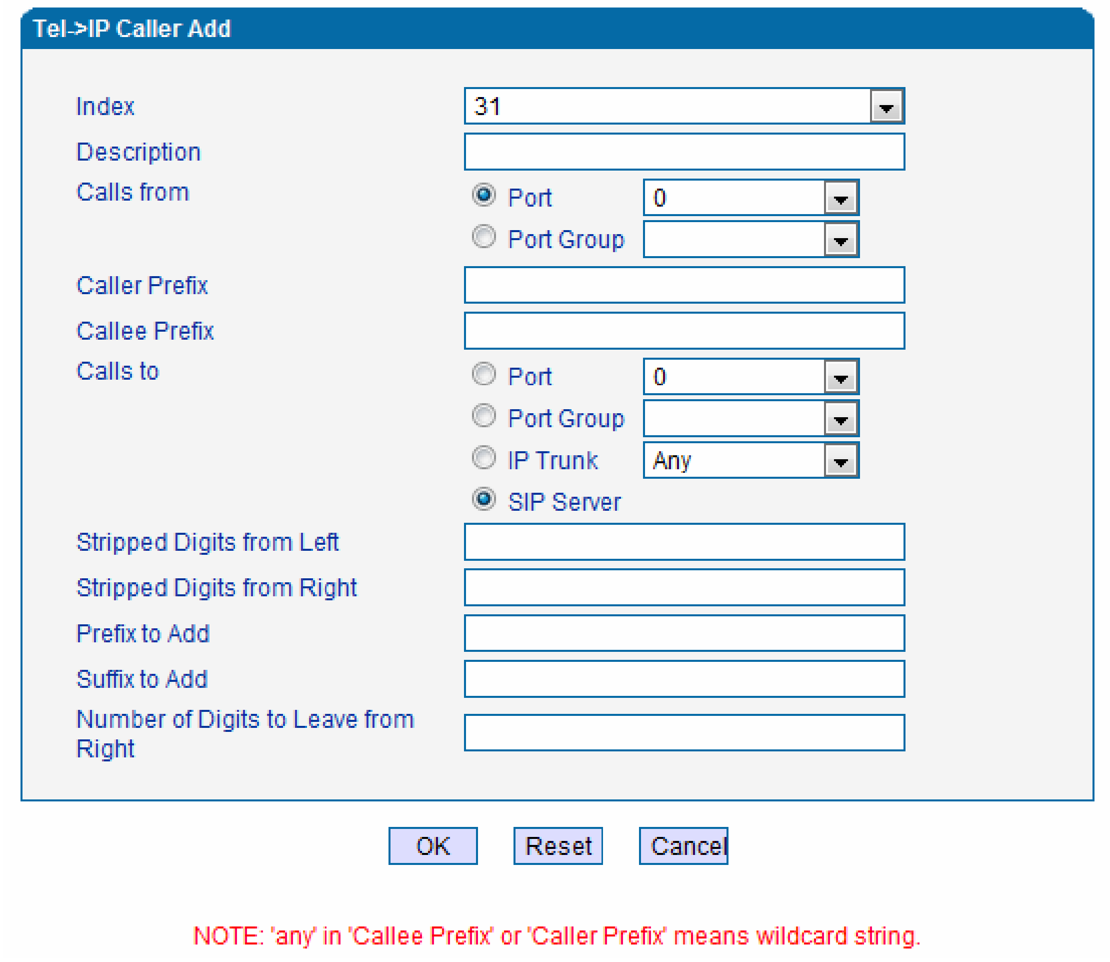


Figure 4．10-2 Tel-IP Caller

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

4.10.3 Tel-IP Callee

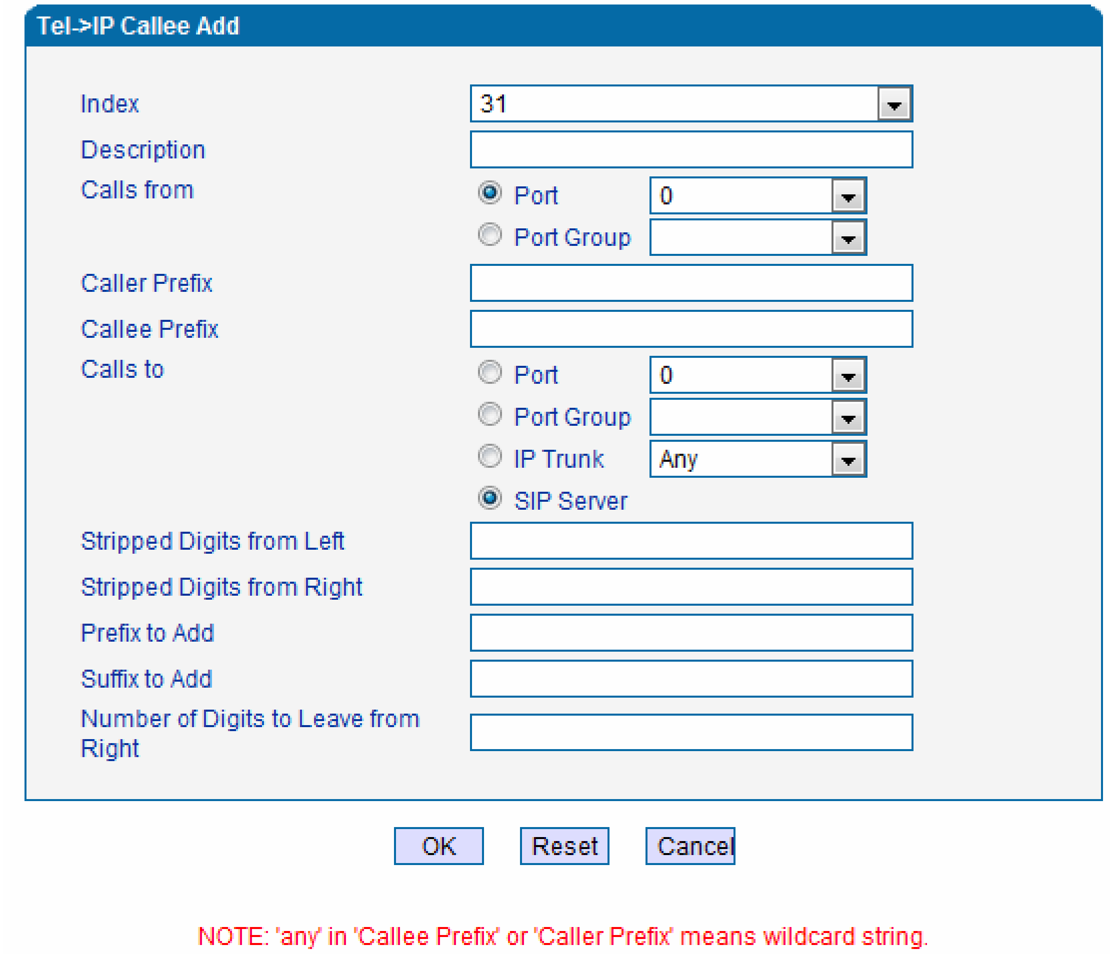


Figure 4.10-3 Tel-IPCallee

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

4.11 Maintenance

4.11.1 SNMP Parameter

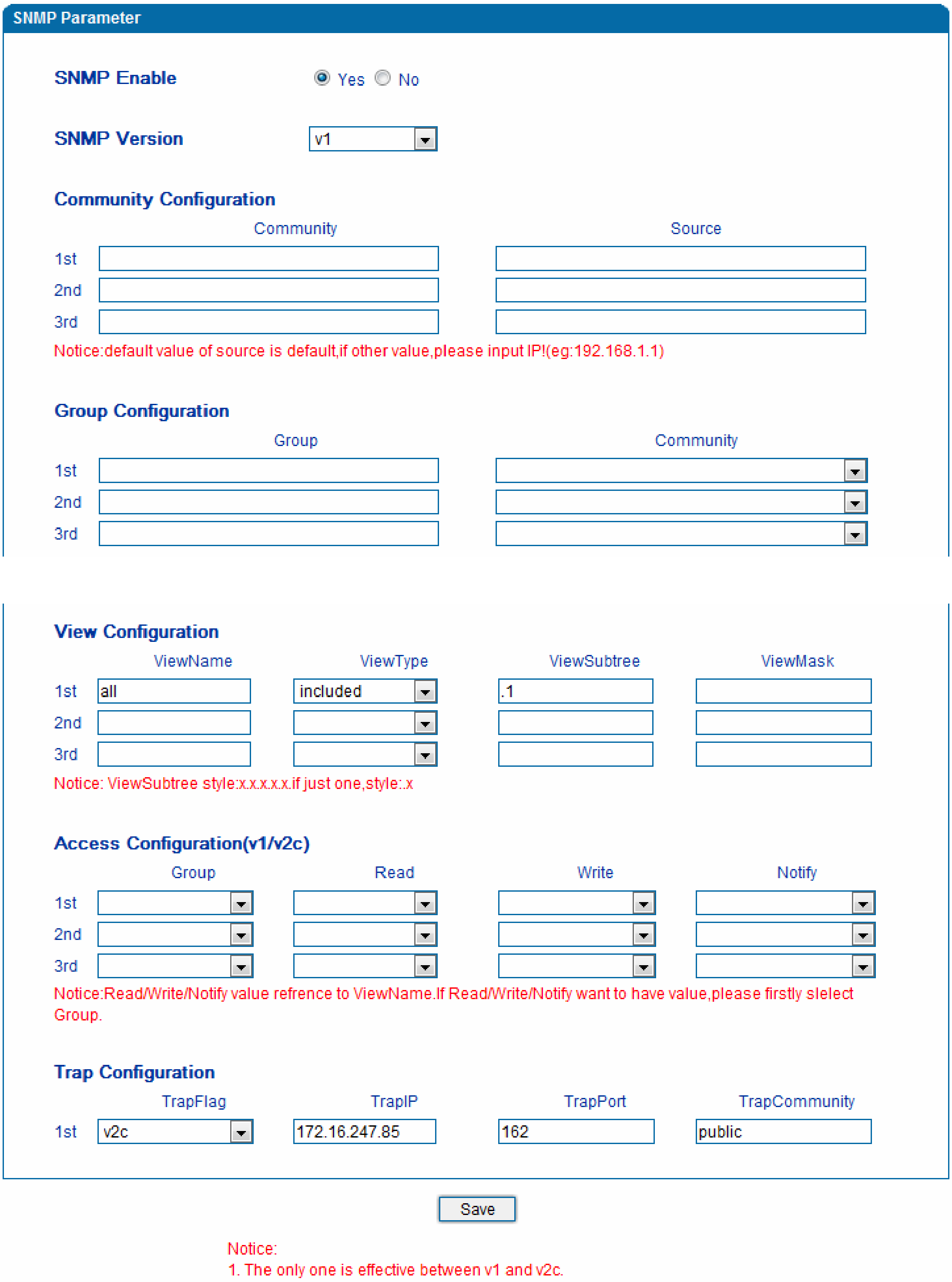


Figure 4.11-1(1) SNMP Parameter V1/V2

Simple Network Management Protocol (SNMP) is application layer protocol, and used to manage communication line. This equipment supported three versions: V1, V2C and V3. In addition to V3 version, the other two versions do not support encryption. However, the service is usually located on the edge of the network devices, security risk, it is best to disable, to be used again.

Community Configuration	Community	The name of network management server managed equipment
	Source	Network management server address
Group Configuration	Group	Name of community group, different versions can use a same group name
	Community	Community join the group
View Configuration	View name	The name of description mib tree
	View type	There are Included and excluded options
	View subtree	Displayed OID of access parameters
	View mask	The same with equipment subnet mask. Generally don't configure
Access Configuration(V1, V2c)	Group	Joined community groups
	Read	Read parameters of mib view
	Write	Write parameters of mib view
	Notify	Equipment send notify parameters to NM server
Trap Configuration	Trap Flag	Version of SNMP
	Trap IP	Device to inform the NM server's IP address. The IP can be configured the same with source IP in community, also be different.
	Trap Port	Default service port is 162
	Trap Community	The same with "community" in community configuration

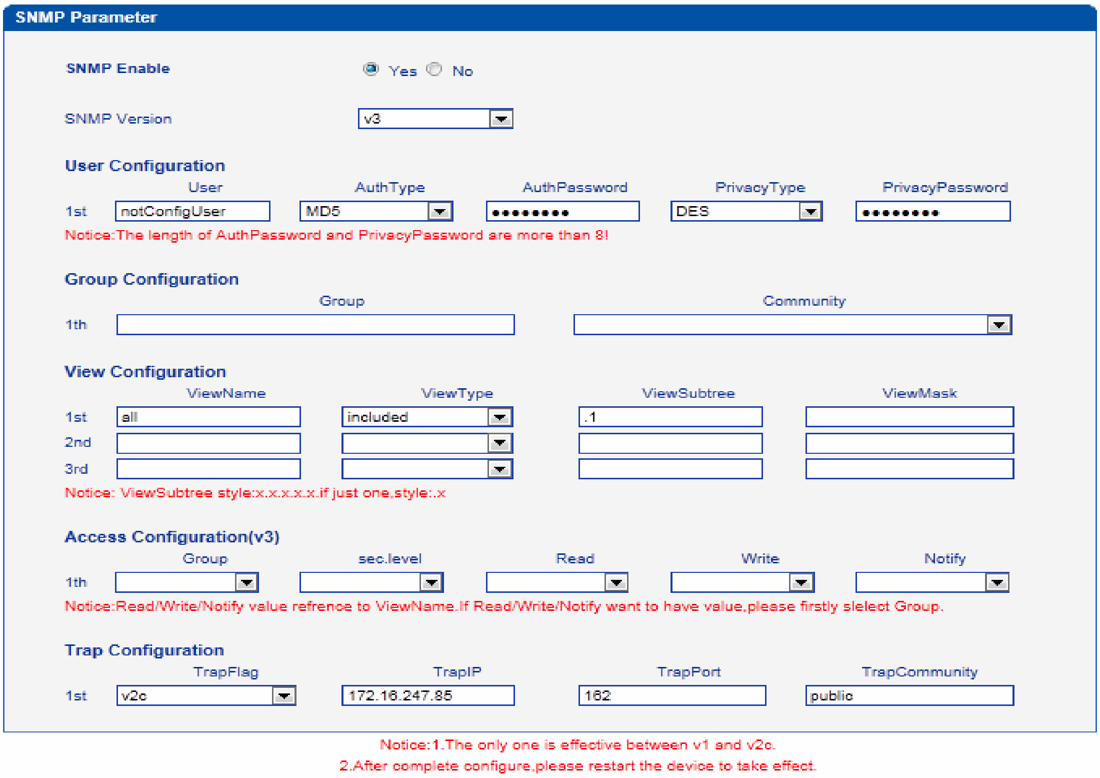


Figure 4.11-1(2) SNMP Parameter V3

User Configuration	User	Network management server management device by username
	Auth Type	Supported two auth type: MD5 and SHA
	Auth Password	Authentication password
	Privacy Type	Supported three privacy type: DES, AES and AES128
	Privacy Password	Privacy password
Group Configuration	Group	Users can use the same group name in different versions
	Community	That is user name
View Configuration	View Name	The name of description mib tree
	View Type	There are Included and excluded options
	View Subtree	Displayed OID of access parameters
	View Mask	The same with equipment subnet mask. Generally don't configure
Access Configuration	Group	Fill in group name
	Sec. level	There are two methods: authentication and authpriv. If select "authentication", users will just configure authentication information, but not privacy information
	Read	Read parameters of mib view
	Write	Write parameters of mib view
	Notify	Equipment send notify parameters to NM server

Trap Configuration	Trap Flag	Version of SNMP
	Trap IP	Device to inform the NM server's IP address. The IP can be configured the same with source IP in community, also be different.
	Trap Port	Default service port is 162
	Trap Community	The same with "community" in community configuration

Note: After configuration, please restart equipment to take effect.

Users can manage and configure gateway on remote NM server through SNMP configuration. But in order to security, recommend this option to open when needed.

4.11.2 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

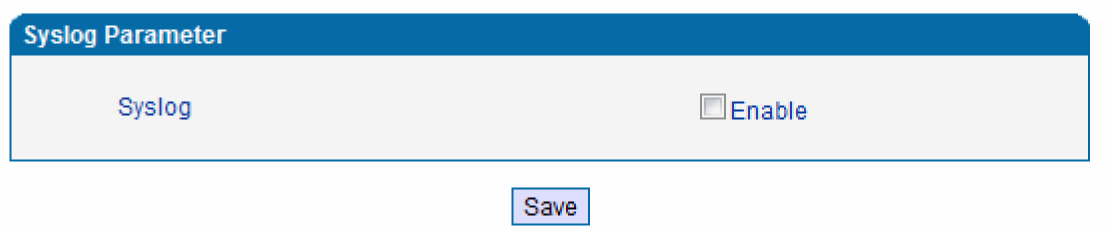


Figure 4.11-2 Syslog Parameter Configuration

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

4.11.3 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 4.11-3 Firmware upload Configuration

4.11.4 Data Backup

The process data backup:

1) Click “Data Backup”

2) Click “Backup” to backup data to PC.

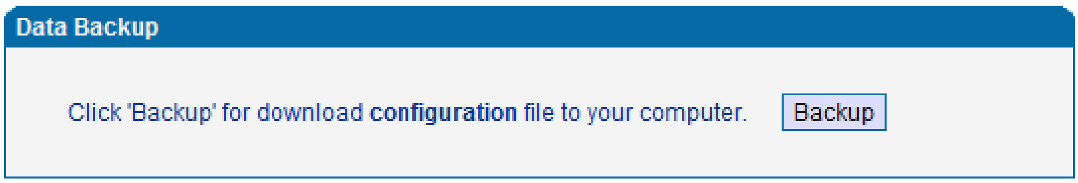


Figure 4.11-4 Data Backup Interface

4.11.5 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.

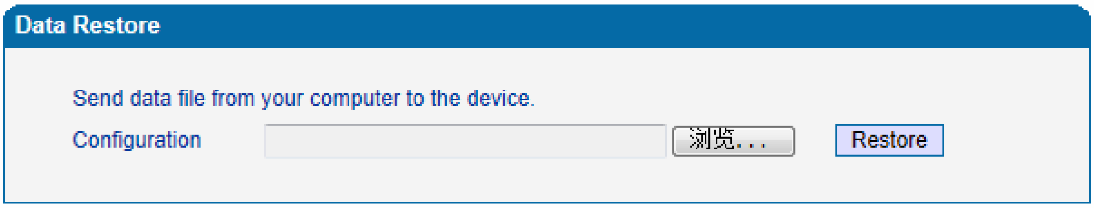


Figure 4.11-5 Data Restore Interface

4.11.6 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.

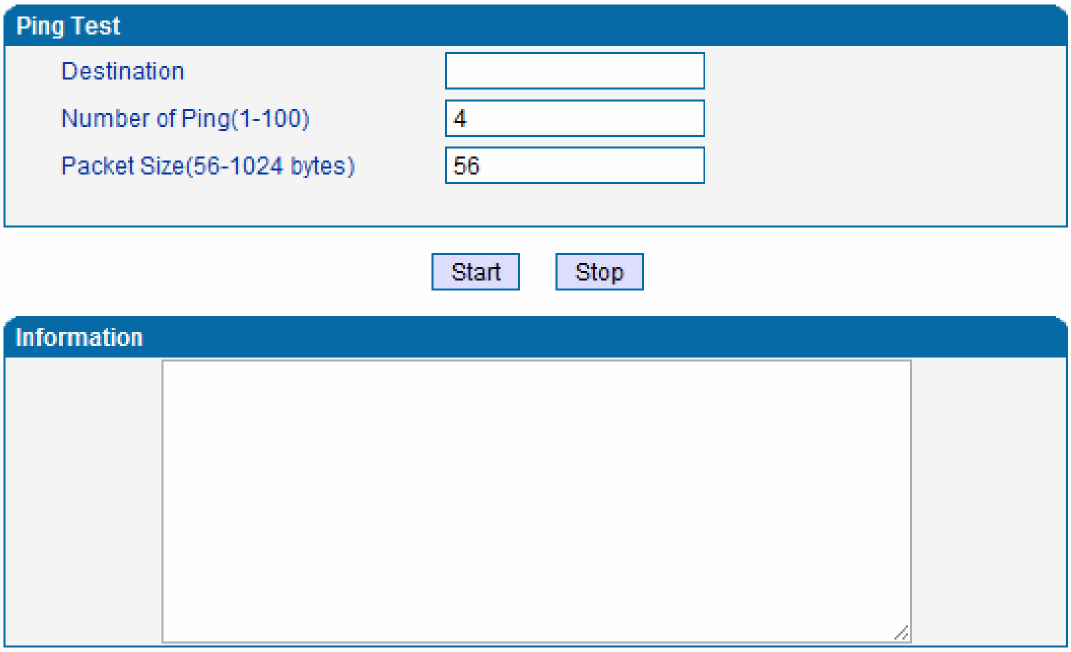


Figure 4.11-6 Ping Parameter Interface

4.11.7 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.

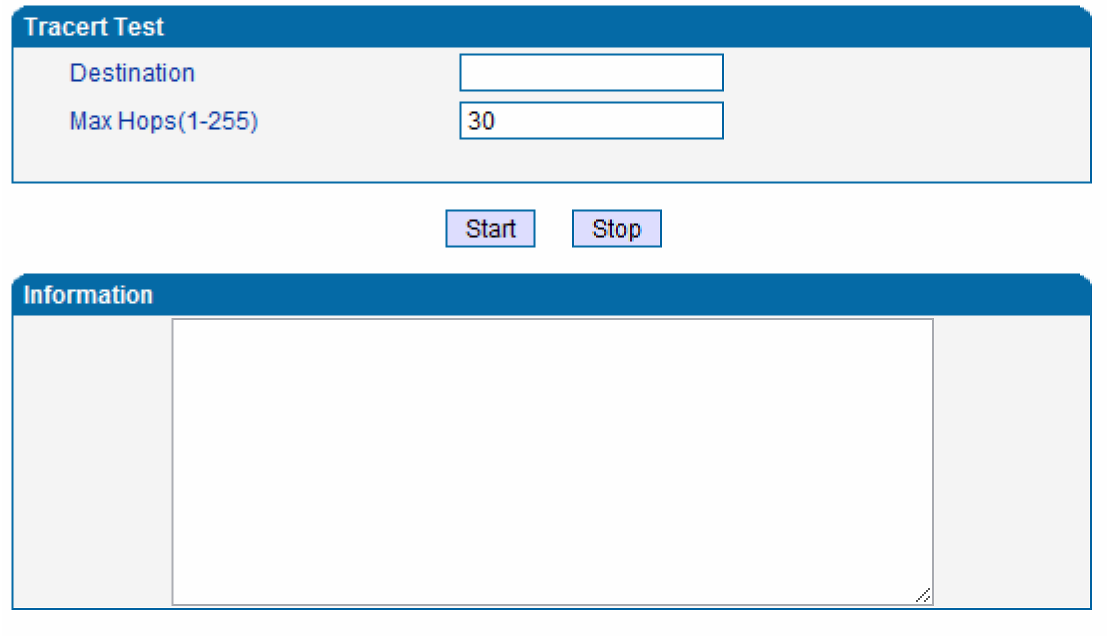


Figure 4.11-7 Tracert Test Interface

4.11.8 Password Modification

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

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

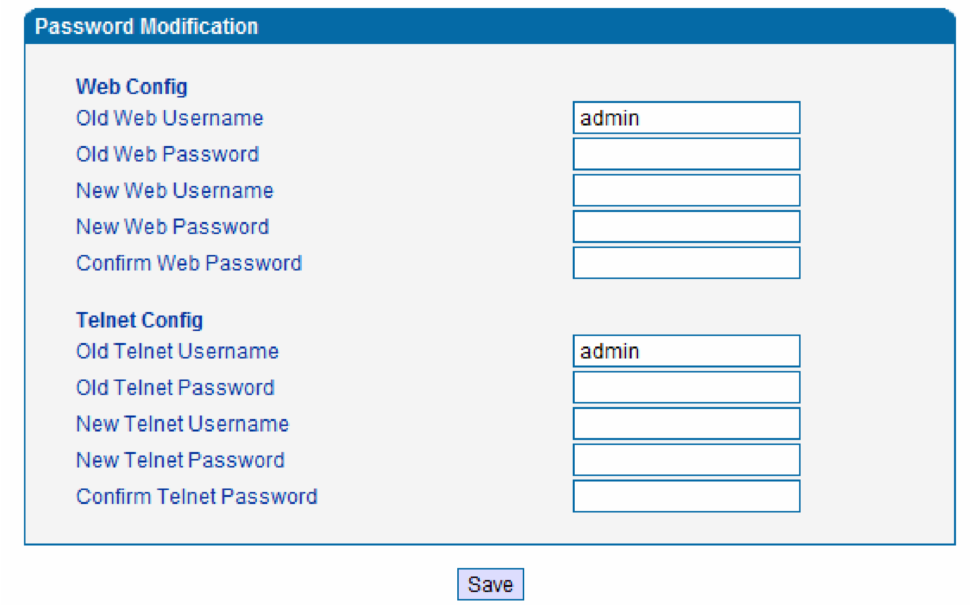


Figure 4.11-8 Password Modification Interface

4.11.9 Factory Reset

Click “Apply” to restore the factory settings.

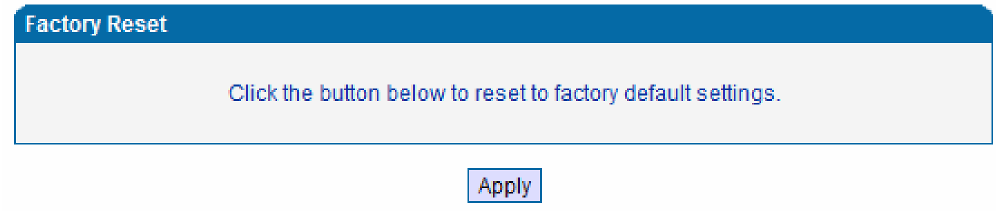


Figure 4.11-9 Factory Reset Interface

4.11.10 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.

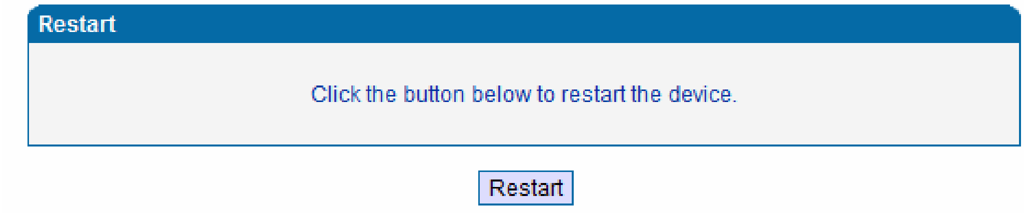


Figure 4.11-10 Device Restart

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