DINSTAR FXS VoIP Gateway

User Manual V2.1

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	The FXS VoIP Gateway User Manual
Document Version	2.1
Firmware Version	2.18.02.05
Date	2014/01/16
Revised by	Technical Support Department

Table of Contents

Chapter1: Introduction

Welcome

Thanks for choosing DINSTAR FXS VoIP Gateway (hereafter named ***"GATEWAY", "DEVICE"***)! We hope you will make optimum use of this flexible, rich-features multi-ports VoIP to FXS gateway. Please read this document carefully before install your gateway.

About this manual

This manual provider information about and introduction of installing, configuring and using the gateway.

For interoperability with different IPPBX/Softswitch platform, you may refer to configure guide with different system.

This manual is available in different configurations. It is written with reference to the default configuration of the **DAG1000-8S** FXS VoIP Gateway.

Intended audience

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

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

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

Chapter2: Know your Gateway

Overview

DINSTAR FXS VoIP gateway is the gateway that provide voice service based on IP network. It's a cost-effective and flexible solution for SOHO (Small Office-Home office), remote office and branch enterprise, as well as Medium sized enterprise.

The GATEWAY connects to analog telephone, fax and traditional analog PBX with standard voice interfaces and provided high quality voice service.

The GATEWAY adopted standard SIP protocol and compatible with leading IP PBX, soft-switch and SIP-based platform.

The FXS analog gateway available in the following configurations:

Sr. No.	Model	Voice Channels	FXS Ports	Physical Port Labels
1	DAG1000-4S	4	4	0-3
2	DAG1000-8S	8	8	0-7
3	DAG2000-16S	16	16	0-15
4	DAG2000-24S	24	24	0-23
5	DAG2000-32S	32	32	0-31
6	DAG3000-112S	112	112	0-111

For a complete list of Hardware and Software features, refer to "product specifications".

This manual mainly to the DAG1000-8S as examples, introduce the function of devices and parameter configuration.

Equipment Appearance

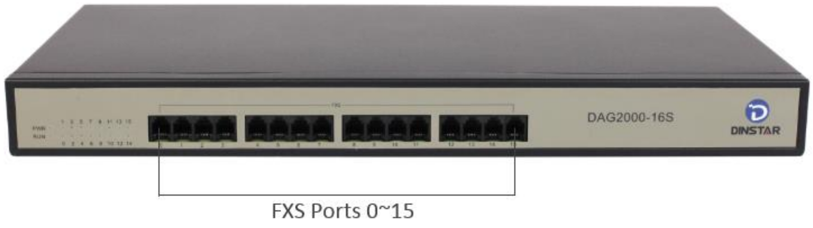
DAG1000-4S

DAG1000-8S

DAG2000-16S

DAG2000-32S

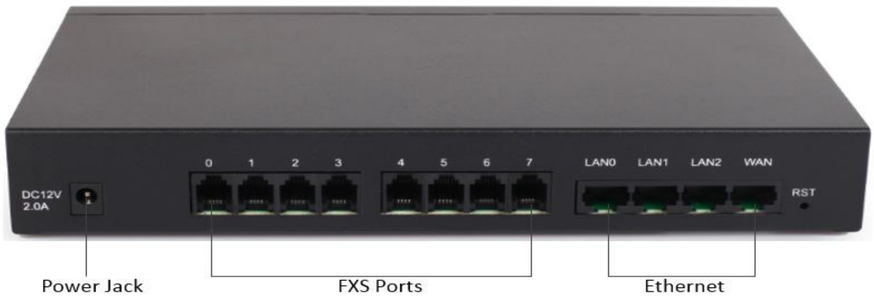
Ports and Connectors



Port Name	Connector	Description
100-240VAC 50-60Hz	AC Jack	To connect 110~240V 50-60Hz AC Power supply
Ethernet	RJ45	to connect to the IP network over a DSL modem or Router or a LAN switch
0-15	RJ11	FXS ports to connect standard analog phone or FAX machine or a PBX
Console	RJ45	Console port with RS232 standard to connect DB9 to RJ45 cable

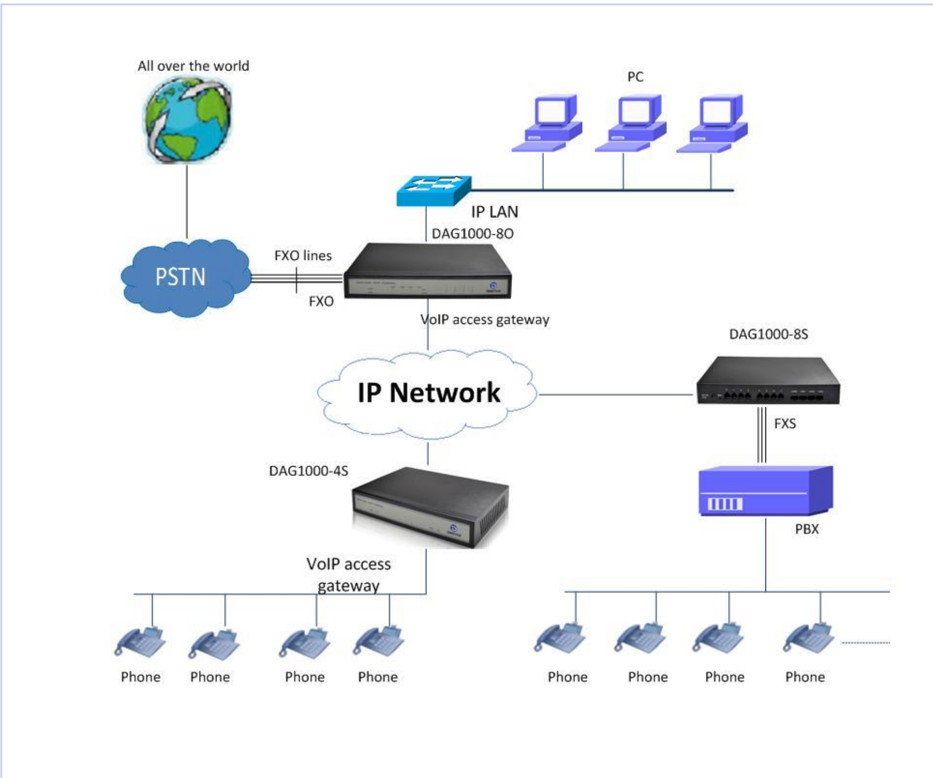
Port Name	Connector	Description
Ethernet	RJ45	to connect to the IP network over a DSL modem or Router or a LAN switch
FXS	RJ45	FXS ports with RJ45 connector that can be separated into 4 RJ11 connectors, to connect standard analog phone or FAX machine or a PBX

Console	RJ45	Console port with RS232 standard to connect DB9 to RJ45 cable



Port Name	Connector	Description
DC12V 2.0A	DC Jack	to connect 12VDC,2A Power adapter
0-7	RJ11	FXS ports to connect standard analog phone or FAX machine or a PBX
Ethernet	RJ45	LAN0~LAN2 to connect with local PC, WAN port to connect the IP network over a DSL modem or Router or a LAN switch

Network Applications



Network Applications

Functions and Features

Protocol 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

Voice and Fax parameters

- G.711A/U law, G.723.1, G.729AB,iLBC,AMR
- 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

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(1/2/4 port support)
- Voice mail
- Direct IP Call

Chapter3: Basic Operations

Phone Call

Dial mobile phone or Extension Number

- Dial the number directly and wait for 3 seconds (Default "*No dial timeout*");
- Dial the number directly and press #.

Direct IP Calls

THE GATEWAY 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：

- Both the GATEWAY and other VoIP Device, have public IP addresses;
- Both the GATEWAY and other VoIP Device are on the same LAN using private IP addresses;
- Both the GATEWAY and other VoIP Device can be connected through a router using public or private IP addresses (with necessary port forwarding or DMZ).

Operation Process：

- Pick up the analog phone then dial "*47"
- 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.

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.

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.

Call Transfer

Blind 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 Transfer B to C:

- Caller A presses **FLASH** on the analog phone to hear the dial tone;
- Caller A dials ***87** then dials caller C's number, and then # (or wait for 4 seconds);
- 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:

- 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.
- 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.
- Continuous busy tone. The phone has timed out.

Attended Transfer

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

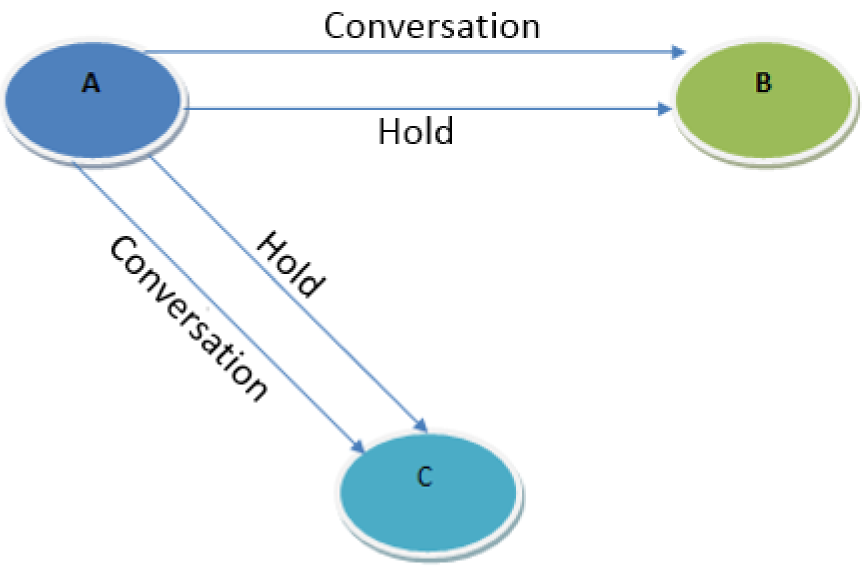
Assume that Caller A and B are in conversation. Caller A wants to *Attend Transfer* B to C:

- Caller A presses **FLASH** on the analog phone for dial tone;
- Dial Caller C's number followed by # (or wait for 3 seconds);
- If Caller C answers the call, Caller A and Caller C are in conversation. Then A can hang up to complete transfer;
- If Caller C does not answer the call, Caller A can press "flash" to resume call with Caller B.

3-way Conference

3-way conference：

- Caller A call B,B pick up into call states;
- Caller A hook flash, A and B into keep states, then C call A, A through to the phone.
- 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.



Call Features

The GATEWAY (FXS) support all traditional and senior phone function.

Table 2.5-1 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.

Sending and Receiving Fax

THE GATEWAY（FXS）support four fax modes:

- T.38 (FoIP)
- Pass-Through
- Modem
- Adaptive

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.

Local IVR Operation

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.

Factory Reset

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

Configure LAN Port’s IP Address

Before configuration, please ensure:

- The device is power on;
- Device is connecting to network;
- Telephone is connected to FXS port of device.

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)

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.

- Query the IP address of device: Offhook, input“*158#”

If the THE GATEWAY 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

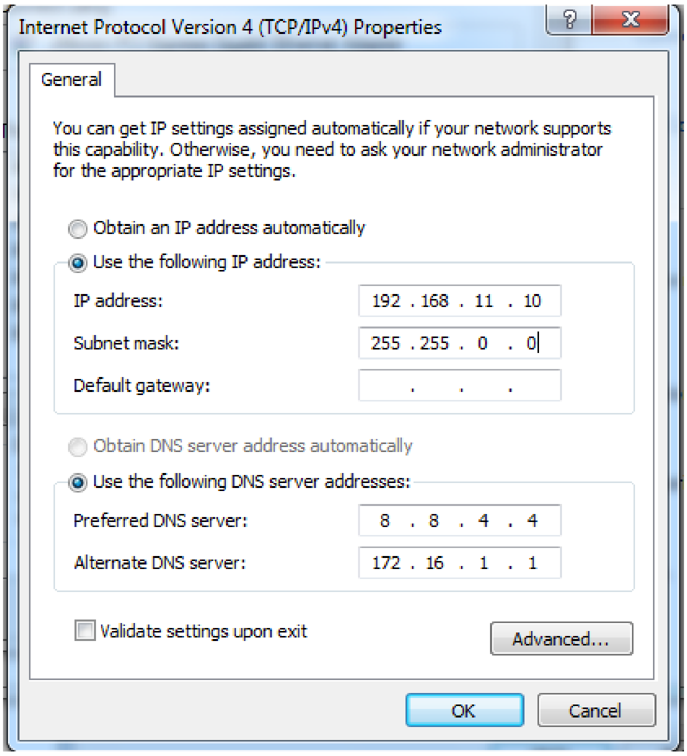
Chapter4: Web Configuration

Getting start

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

Network connection

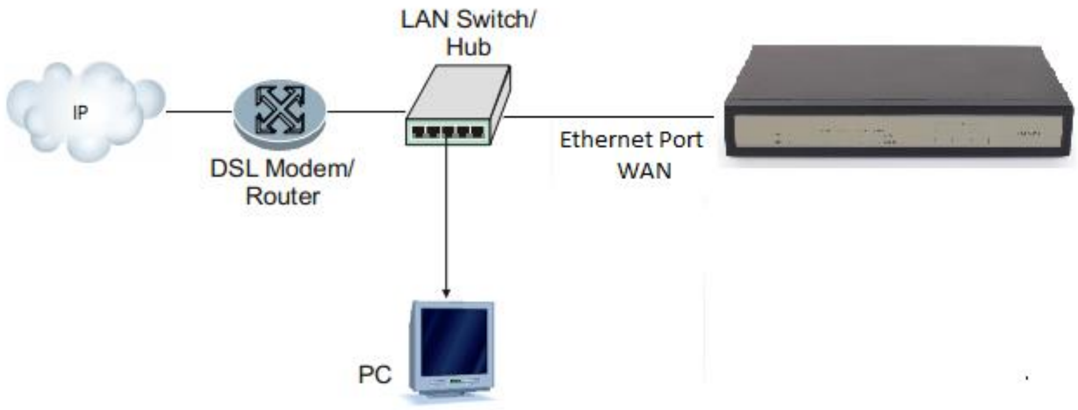
Device LAN port default IP address is 192.168.11.1, WAN port default obtain IP address by DHCP. Advice to modify the IP address of the local computer equipment and ensure that are on the same IP segment, with Windows 7 as an example, the local computer IP address change for 192.168.11.10：



Modify IP address

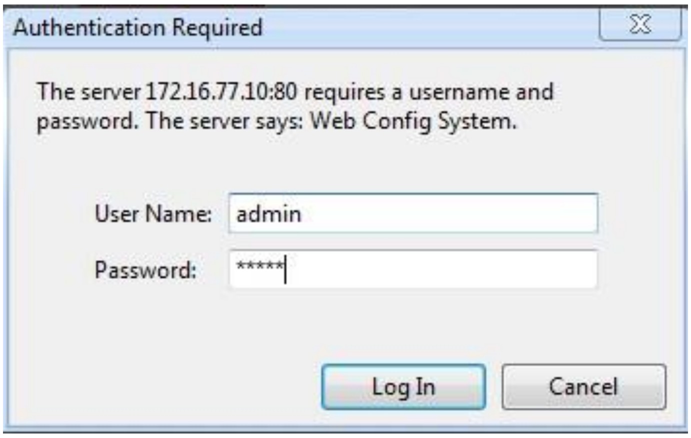
Check connection between computer and device, click "Start"-> "run"-> input "cmd", run ping 192.168.11.10 –t order to check the connectivity between them.

Connect to private network (behind NAT)



Get Web access

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

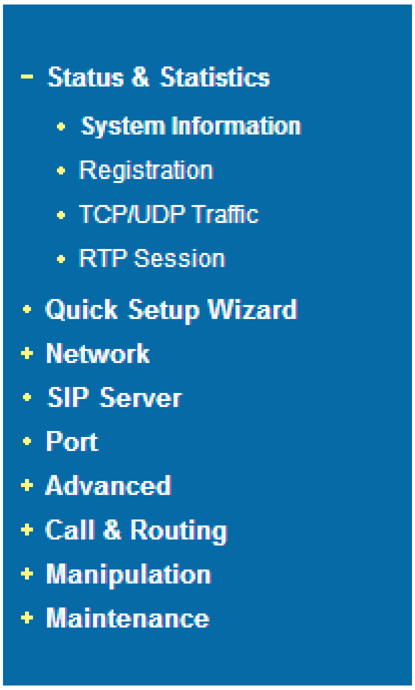


The GATEWAY Login Interface

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

Navigation Tree

The GATEWAY 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.



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.

State and Statistics

System Information

You can view the information of Device ID, MAC address, IP addresses, version information and Sever registration status

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

Figure 4.3-1 System Information

System information as follow:

System Information Description

Device ID	An unique ID of each device, this ID is use for cloud server authentication and warrantee purpose
MAC address	WAN port hardware address. The device ID in HEX format.
Network Mode	Display network mode, include bridge and router. **Bridge mode**, the Ethernet port will work as a small lanswitch. **Router Mode,** NAT feature will be enabled in this mode. WAN port IP only display while the gateway set to **Router Mode**.
Network	Display WAN and LAN port IP address, subnet mask and the way of obtain IP address.

WAN IP Address	Shows WAN IP address of the gateway , DHCP mode: all the field values for the Static IP mode are not used (even though they are still saved in the Flash memory.) The GATEWAY 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 gateway will establish a PPPoE session if any of the PPPoE fields is set. Static IP mode: configure the IP address, Subnet Mask, Default Router IP address, DNS Server 1 (primary), DNS Server 2 (secondary) fields. These fields are set to zero by default.
LAN IP address	Shows LAN IP address of the gateway. 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.
NTP Status	Succeed: the gateway is sync to NTP server successful Failed: failed to sync to NTP server then you should check network connection/NTP server
NTP time	Current time of the gateway
Network Traffic Statics	Total bytes of message received and sent by network port.
Usage of Flash	Detailed usage of Flash memory
Usage of RAM in Linux	Detailed RAM usage of Linux core
Usage of RAM in AOS	Detailed RAM usage of AOS
Current Software Version	Software version that running on the gateway. The version number consist of Model Name, Version number, Built date
Backup Software Version	There are two zone to storage software version. Backup software is for roll back purpose while current software fail. The backup software version consist of Model Name, Version number, built date
U-boot	U-boot version
Kennel version	Linux Kennel version
FS Version	File system version

Hint Language	Hit language of the gateway

Registration Information

Port Registration Information					
Port No.	Type	Primary User ID	Primary User Status	Secondary User ID	Secondary User Status
0	FXS	100	Registered	---	---
1	FXS	101	Registered	---	---
2	FXS	102	Registered	---	---
3	FXS	103	Registered	---	---
4	FXS	104	Registered	---	---
5	FXS	105	Registered	---	---
6	FXS	106	Registered	---	---
7	FXS	107	Registered	---	---

Port Group Registration Information					
Port Group	Port	Primary User ID	Primary User Status	Secondary User ID	Secondary User Status
7 <108>	0,1,2,3,	108	Registered	---	---

Port and Port group registration information

Primary/Secondary User status:

- Registered: the port is register to SIP server successfully
- Unregistered: failed to register to SIP server

TCP/UDP Statistics

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

Refresh

TCP/UDP Statistics Information

The picture show above is TCP sending and receiving, UDP sending and receiving packets of statistical information since the device launched.

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)
	---	---	---	---	---	---	---	---	---	---

Refresh

Figure 4.3-4 RTP Session Statistics

The picture show above is 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.

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.

Network Configuration

Local Network

The GATEWAY has two kinds of work mode: route and bridge. When the GATEWAY is set rout mode, the GATEWAY 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 the GATEWAY is set bridge mode, WAN and LAN port are the same. The GATEWAY 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. Network configure interface as below:

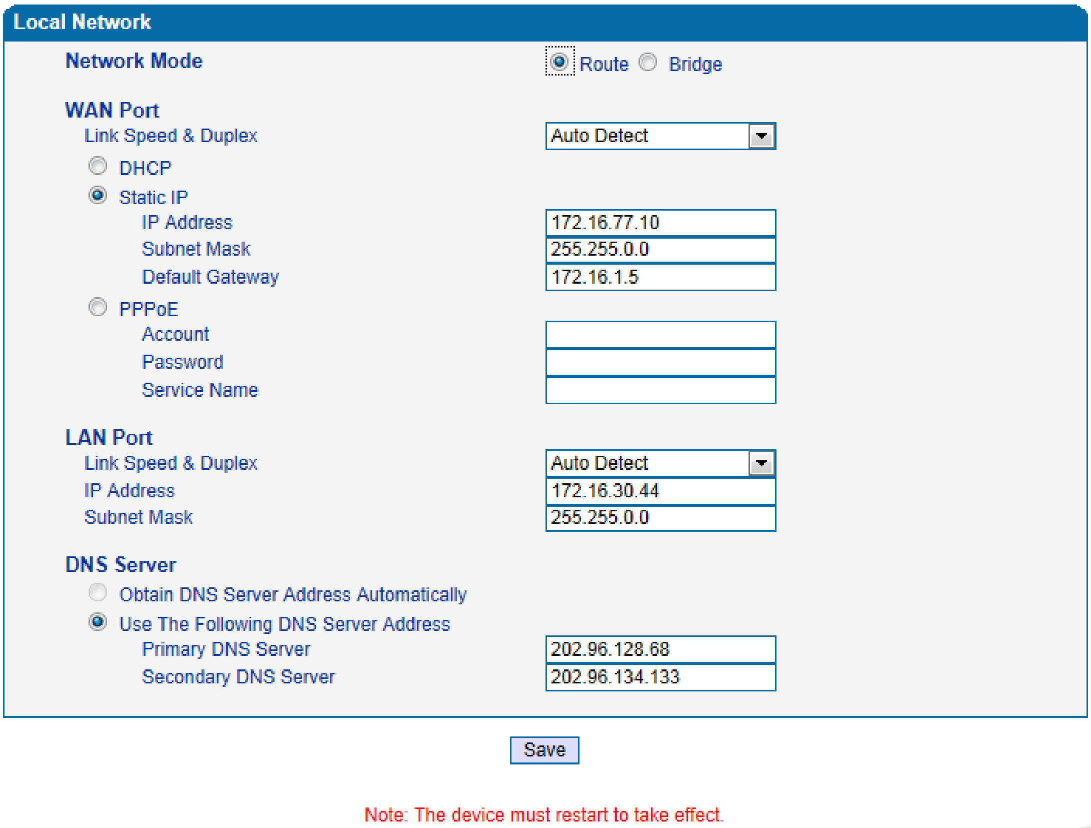
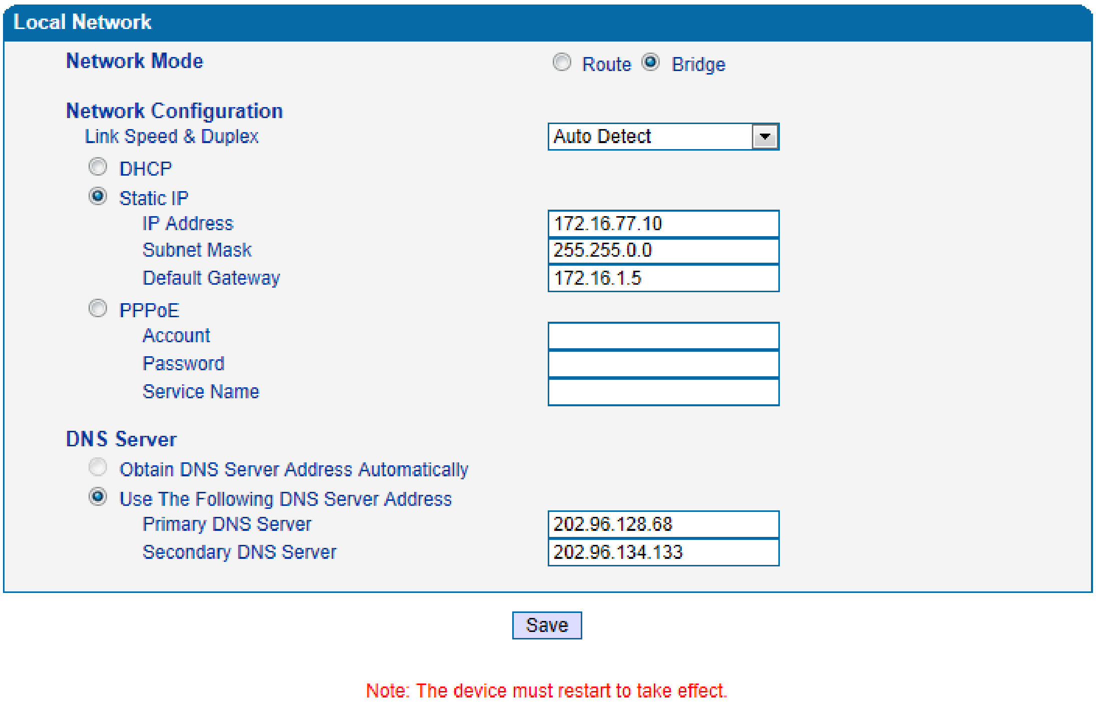


Figure 4.5-1Route Mode



Bridge 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 Detect".
- When select "Obtain IP address automatically", the GATEWAY will obtain IP address by DHCP.
- When select "Use the following IP address", that configure the GATEWAY to fixed IP address mode.
- When select "PPPoE", please fill in account and password offered by ISP in internet account and password.

【Notes】:

- If select DHCP to obtain IP address, please ensure DHCP server in network and work normally.
- Under route mode, please configure LAN port and WAN port in different segment, otherwise the GATEWAY can't work normally.
- Under route mode, login the GATEWAY configuration interface only used LAN port.
- After configuration, restart device configuration validation.

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.

- 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.

- 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 below:

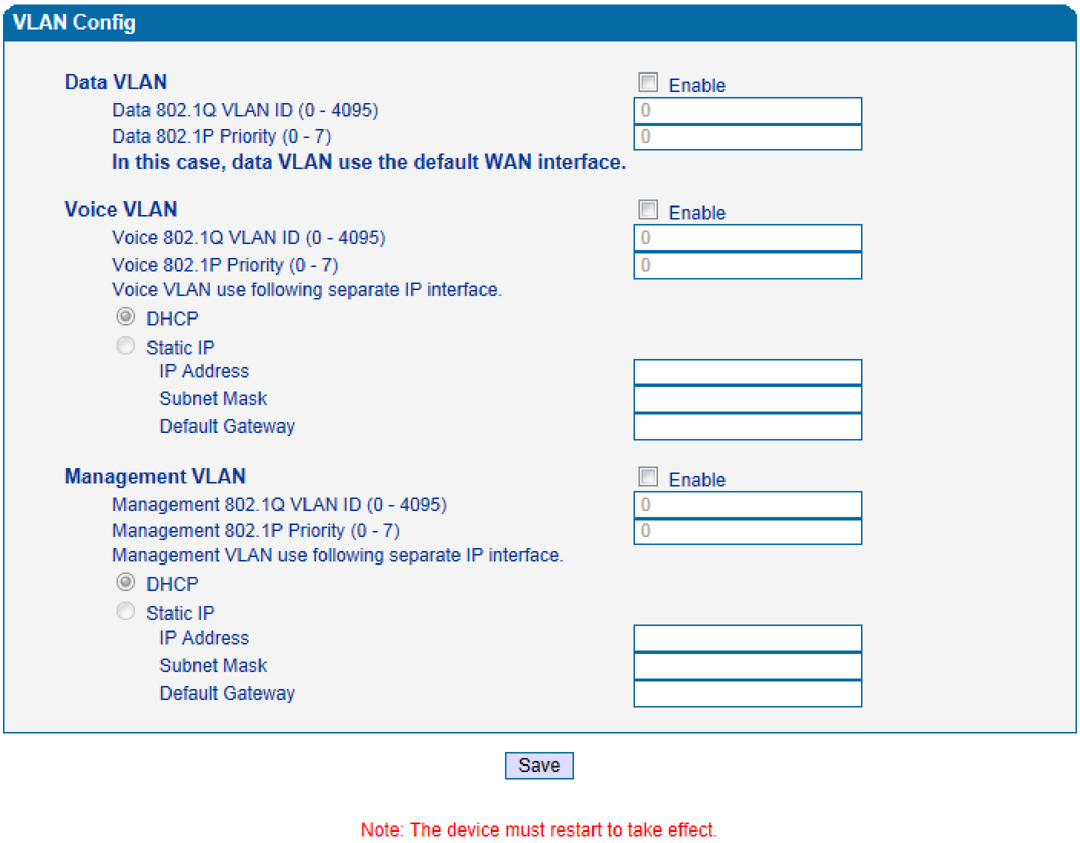


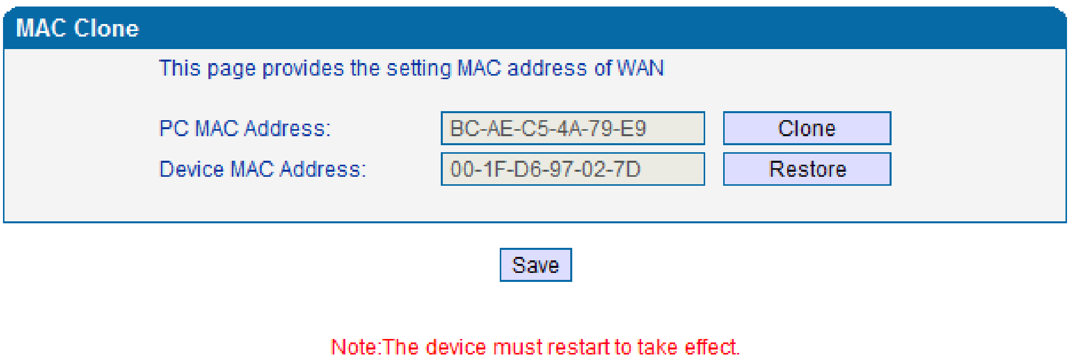
Figure 4.5-3 VLAN parameter configuration

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 use 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.

MAC Clone (Routing mode)



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.

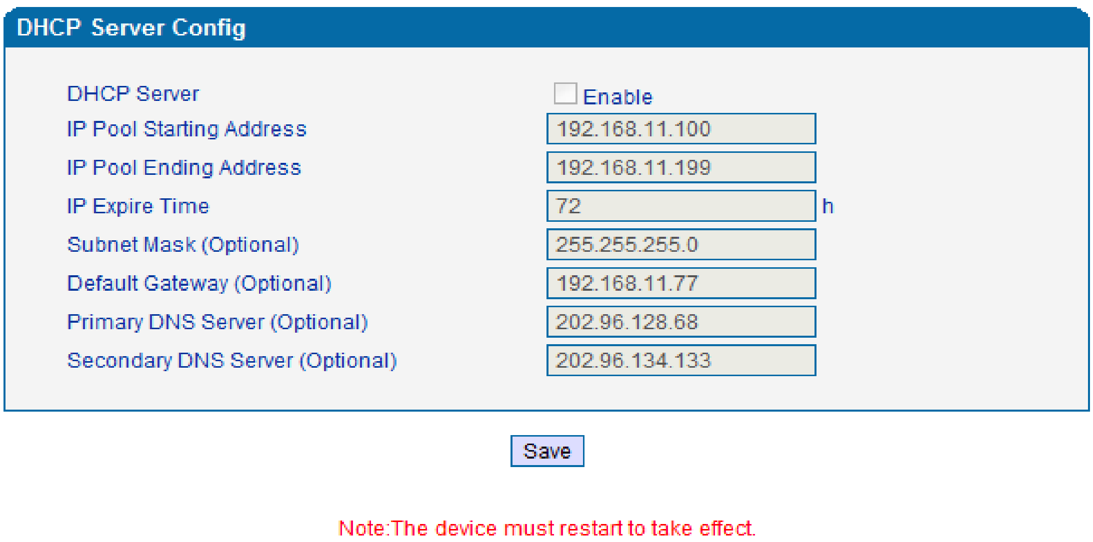
DHCP Server (Routing mode)

Under route mode, the GATEWAY network part as a small router to configure DHCP service, that the GATEWAY 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 below:

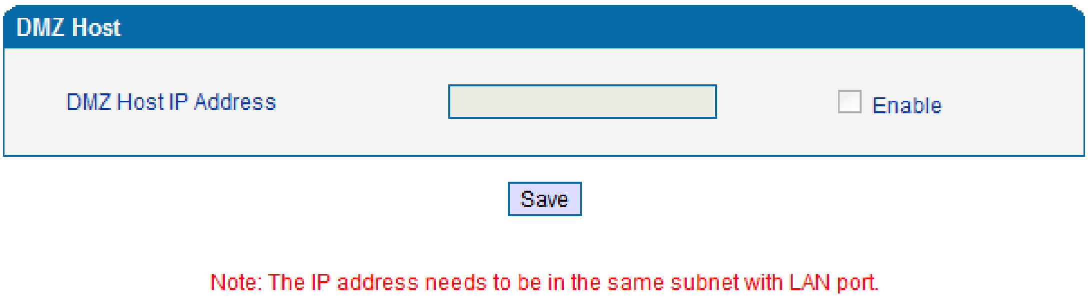


Configuration Interface

【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.

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.



DMZ Configuration Interface

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

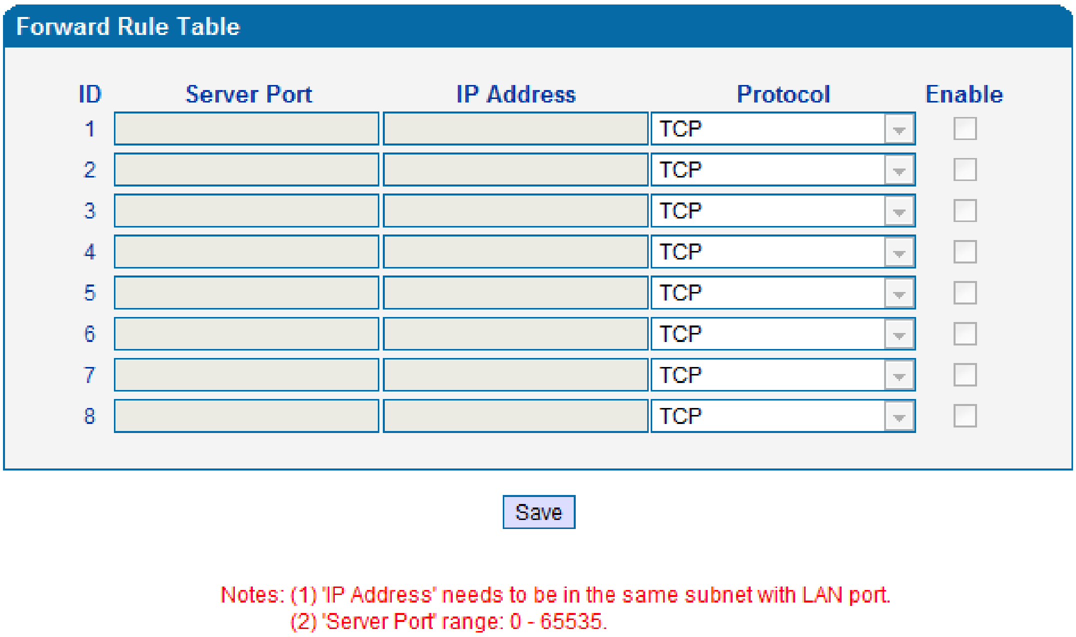
Forward Rule (Routing mode)

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:

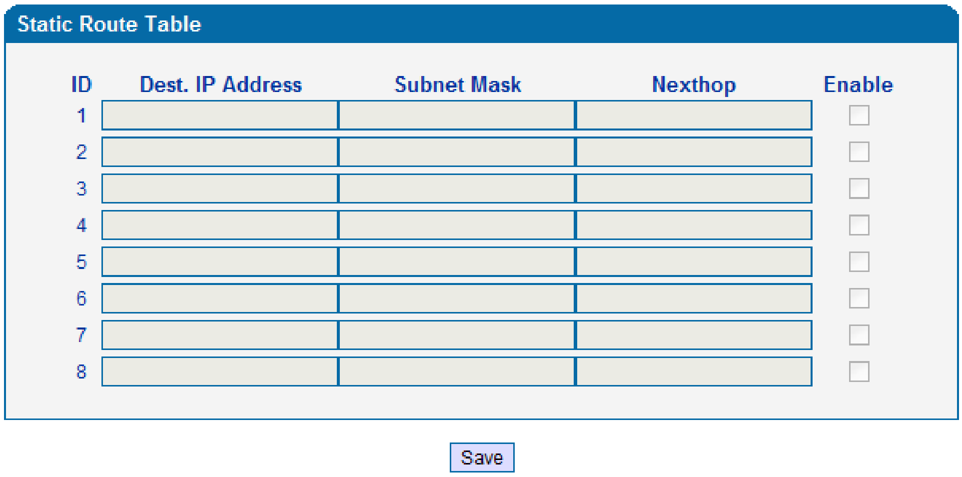


Forward rule configuration interface

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:



Static route configuration interface

ARP

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:

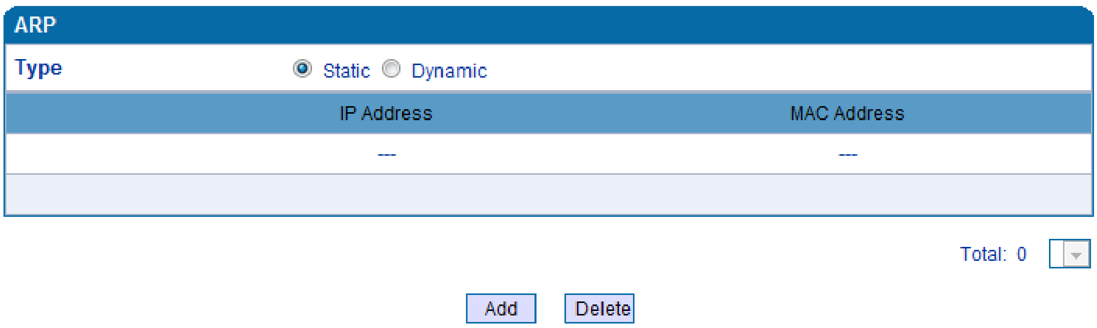


Figure 4.5-9 ARP Parameters

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.

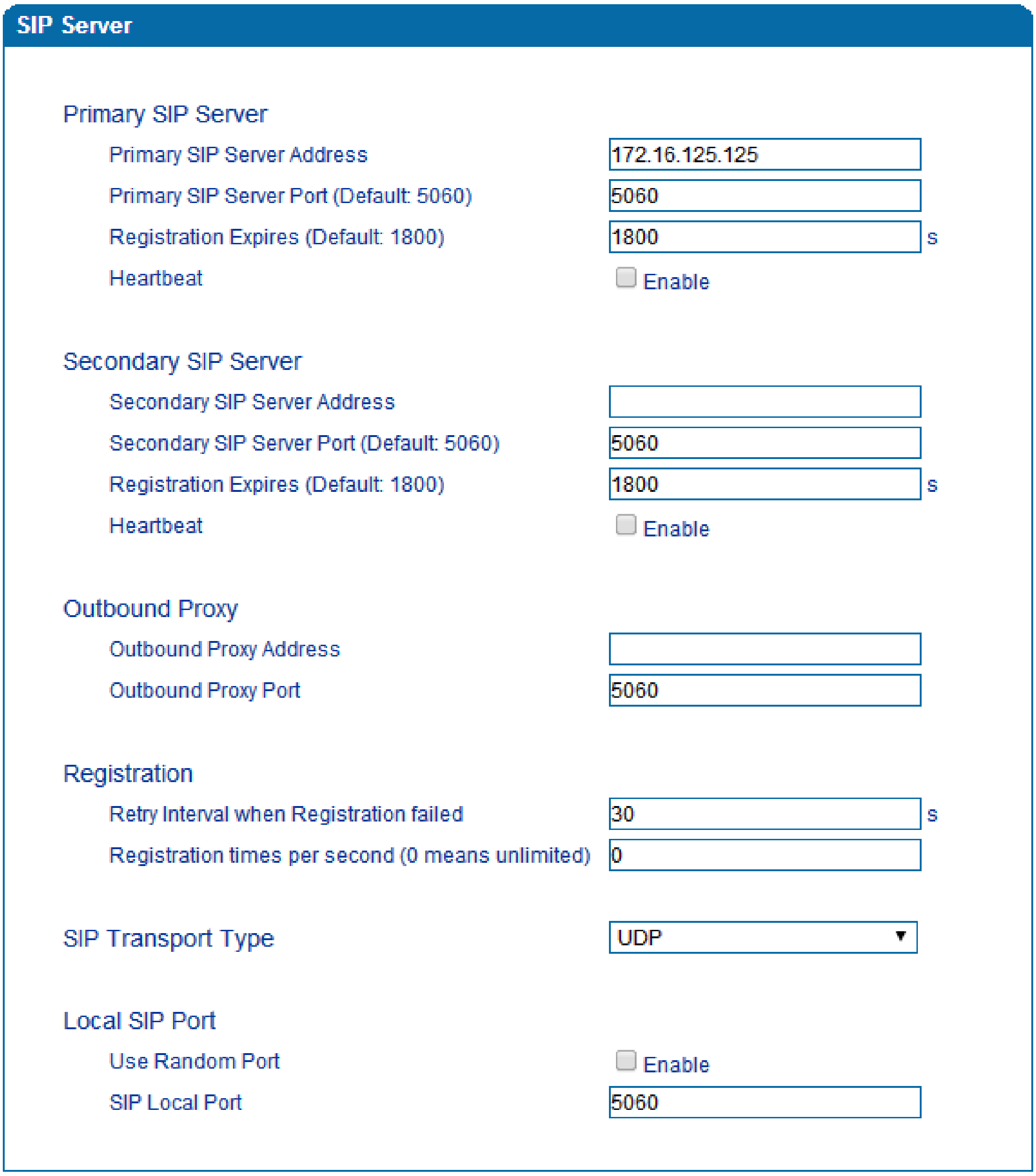
In SIP network, the media always using end-to-end to hand the consultation. In some particular situation or business processing, such as “Music On Hold”, SIP server will actively participate in the media negotiation. Simple SIP server is responsible only for establishment, maintenance and cleaning conversation, 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 :mini SipServer、Brekeke，VoIPswitch etc.

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

SIP server configuration interface as follows:



SIP Server Configuration Interface

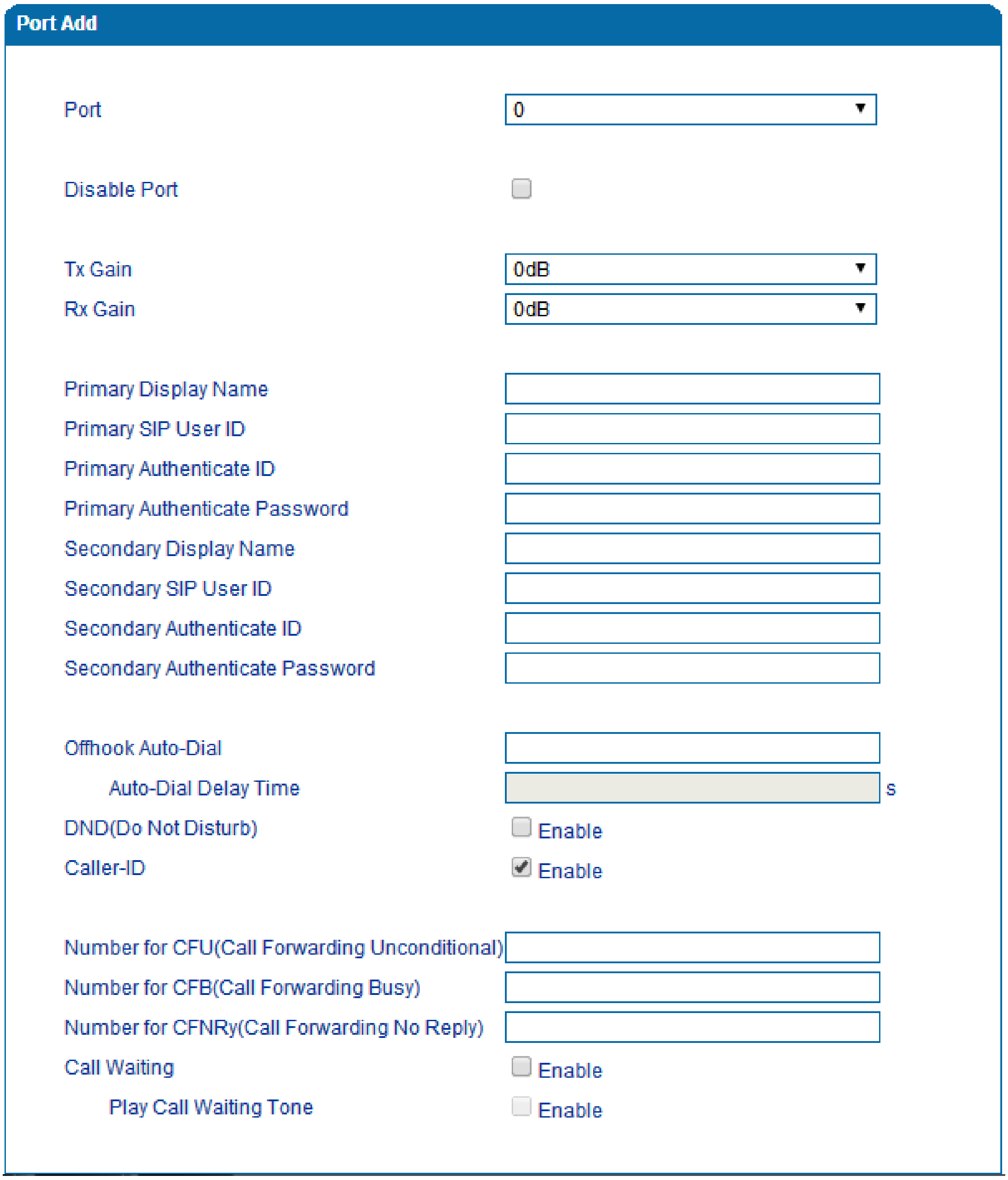
SIP parameter description:

Primary SIP Server Address	SIP Server IP address or Domain name provided by VoIP service provider.
Primary SIP Server port	Service port, default is 5060
Register Expires	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 address	Backup SIP Server's IP address or Domain name provided by VoIP service provider.
Secondary SIP Server port	Service port, default is 5060
Register Expires	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.
Outbound Proxy Address	Outbound proxy IP address or Domain name provided by VoIP service provider.
Outbound Proxy Port	Default outbound proxy SIP service port is 5060.
Retry Interval when Registration failed	The retry interval time after the registration failed last time
Registration times per second	Limit the gateway to send REGISTER messages per second
SIP Transport Type	The SIP transport type, can be UDP, TCP, Auto; default to UDP
Use Random Port	Random SIP service ports for gateway
SIP Local Port	Default SIP local service port is 5060.

Port Configuration

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



Port configuration interface

Port parameters introduce as follows:

Port	Port number,
Disable port	Disable port temporally
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

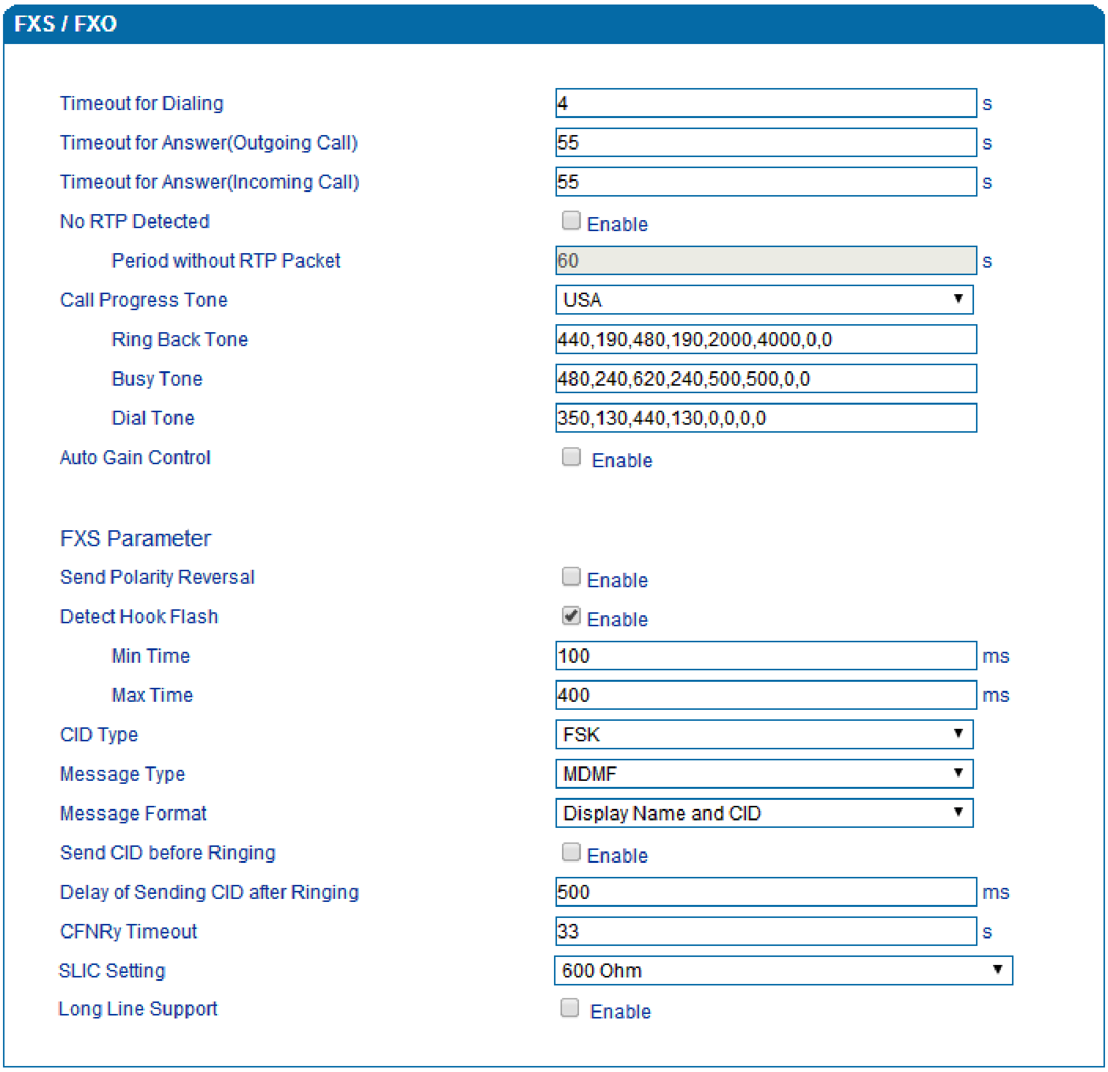
Rx Gain	It is use to control the volume of conversation, Adjust "RX gain" will affect the end users voice size, the default value is 0. Its value range from -10 – 10 dB
Primary /Secondary SIP Display Name	Primary /Secondary SIP account description, Its purpose is so you can identify the SIP account with 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.

Advanced

FXS/FXO Parameters

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



FXS Parameters Configuration Interface

FXS parameters description:

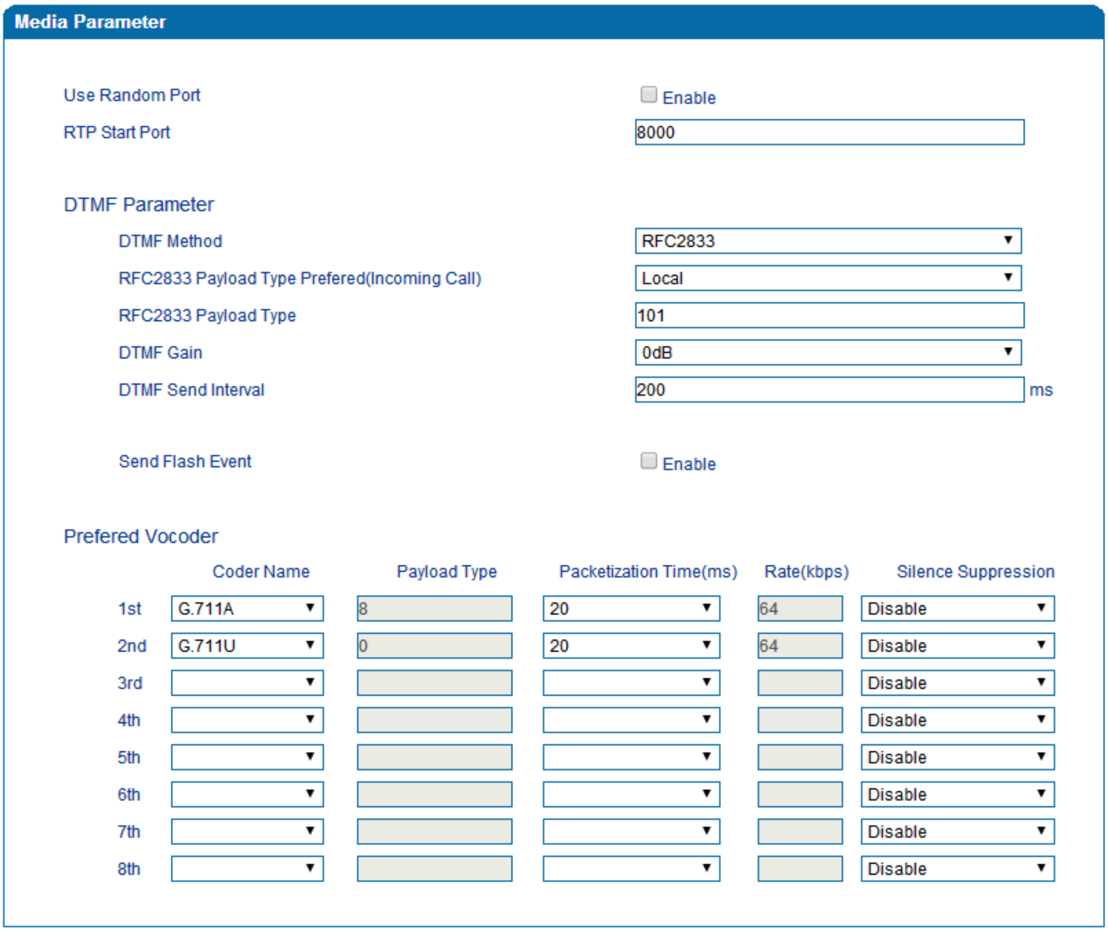
Timeout for dialing	With the help of dialing timeout, you can limit the time while users typing the digits from an extension. If the timeout expire while the

	user is typing in the extension then the GATEWAY 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 Detected	Detect when there's no RTP packet receive
Period without RTP Packet	The time interval of No RTP packet
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.
Auto Gain Control	Enable automatic gain control
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 types SDMF and MDMF, General for the default
Message Format	The call display format send to analog phone, can be “Display Name and CID”, “CID only”, or “Display Name only”; default to “Display Name and CID”

Send CID before Ringing	After enable this configuration, The THE GATEWAY 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
CFNRy Timeout	Timeout for call forward No Answer
SLIC Setting	Set the unit impedance
Long Line Support	Enable Long Analog extension line

Media Parameter

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

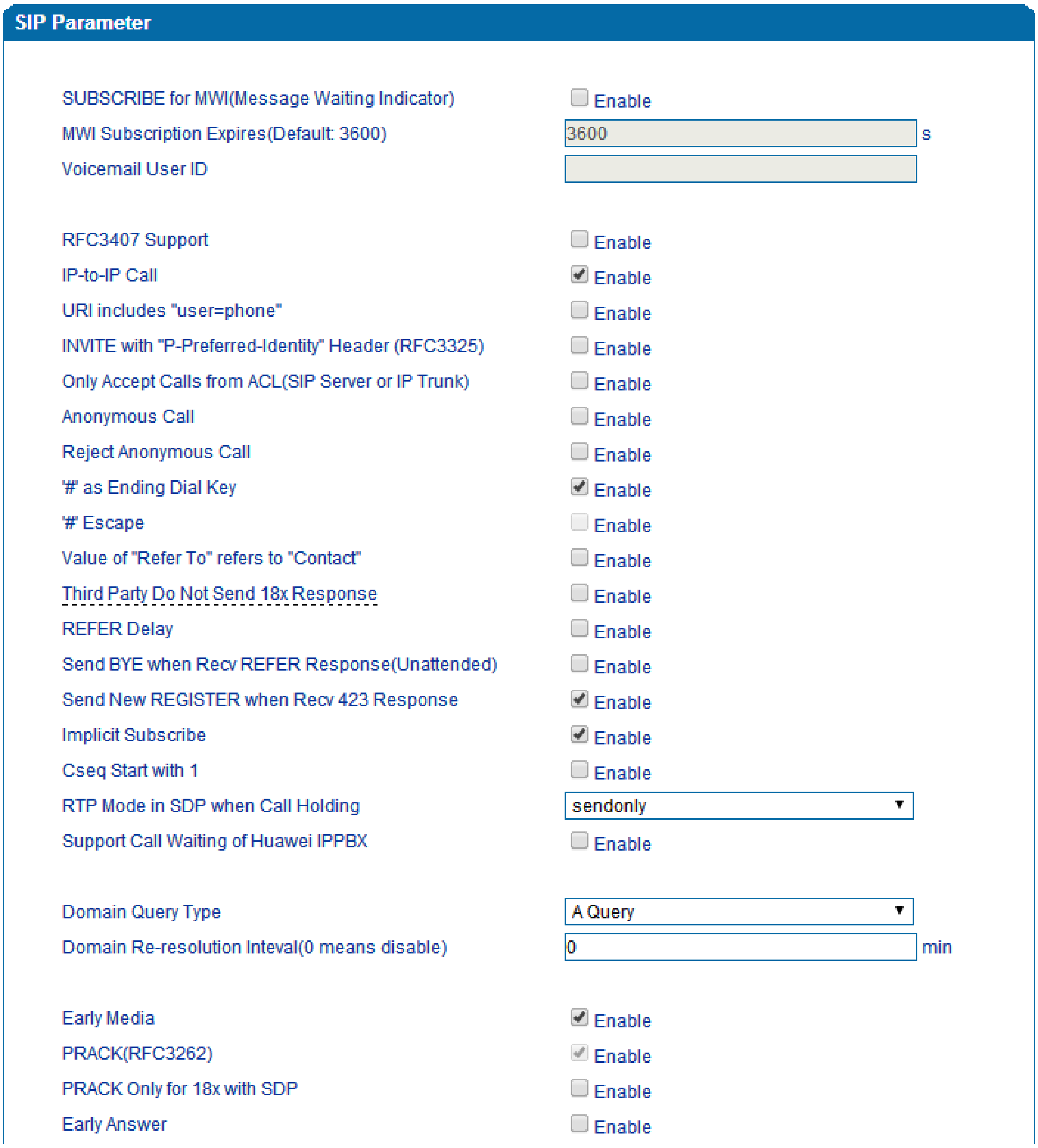


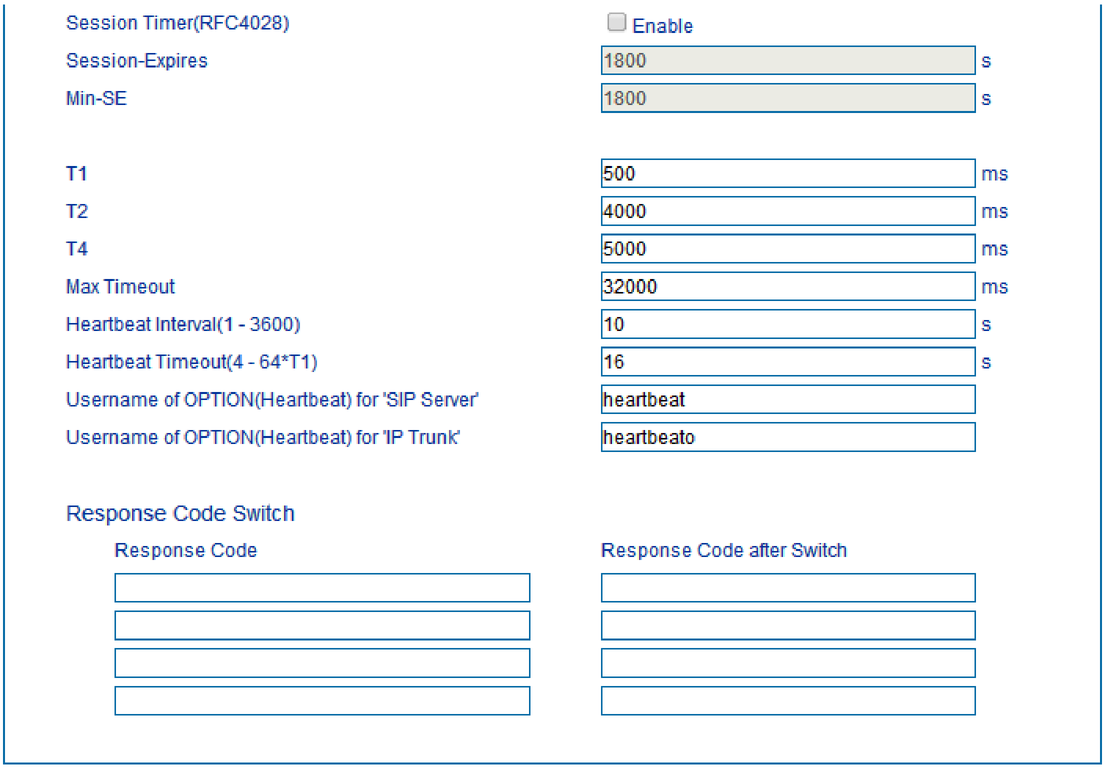
Media Parameter Configuration Interface

Media parameter description:

Use Random Port	Enable the gateway to use random RTP port
RTP Start Port	Default RTP port 8000
DTMF Method	SINGAL、INBAND、RFC2833
RFC2833 Payload Type	Payloadvalue, default is 101
DTMF Gain	Default is 0 DB
DTMF Send Interval	DTMF send signal interval, default is 200ms.
Send Flash Event	Enable gateway to send flash event to remotely instead of handling it locally
Coder Name	THE GATEWAY 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.

SIP Parameter





SIP Parameter Configuration Interface

SIP parameter description:

SUBSCRIBE for MWI	Voicemail message indicator, it is to be realized in the way of NOTIFY
MWI Subscription Expires	MWI subscription expires time, default to 3600
Voicemail User ID	Access code to voicemail box
RFC3407 Support	Enable support of RFC3407
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.
INVITE with"P-Preferred-Identity" Header (RFC3325)	Support RFC3325, add "P-Preferred-Identity" Header in INVITE message
Only Accept Call from ACL (SIP server or IP Trunk)	Default is no, it indicates the GATEWAY accept incoming call from SIP server only

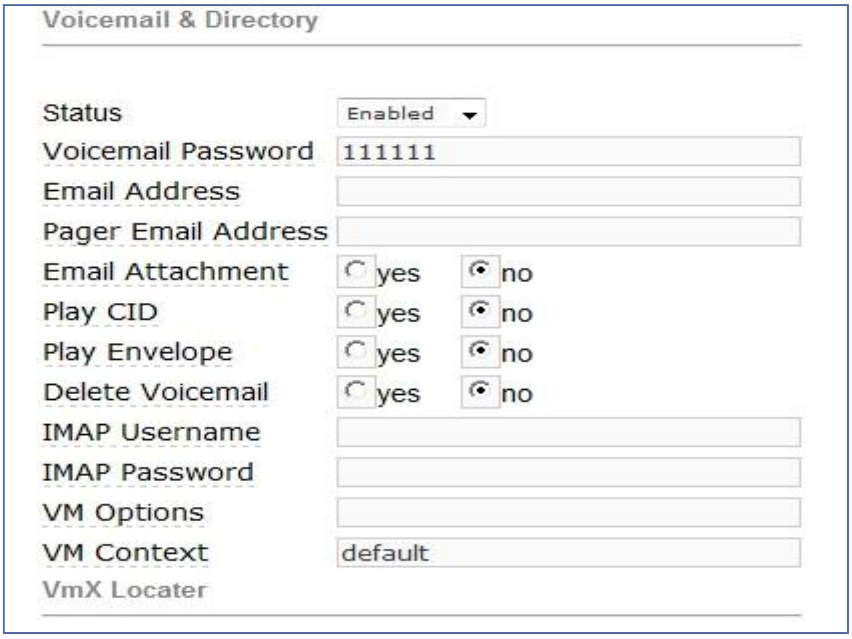
Anonymous Call	Enable anonymous call, “anonymous” will include in SIP message
Reject Anonymous Call	Enable this function, reject all anonymous call. Disable by default
# as ending Dial Key	Dial-up, use # as a end descriptor.
# Escape	Escape # key
Value of “Refer To“ refers to ”Contact”	Its function is 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”.
Third Party Do Not Send 18x Response	Send 18x response when acting as third party in a attended transfer
Send BYE when Recv REFER Response (unattended)	Send BYE to release session after receiving REFER when acting as
Send New REGISTER when Recv 423 Response	Update the value of expires header and re-send REGISTER when receive 423 response
Implicit Subscribe	Accept implicit subscription
CSeq Start with 1	Value of CSeq start with 1
Forbid Invilad m=line in reINVITE	Forbid invilad m=line in SDP of re-INVITE
RTP Mode in SDP when Call Holding	Use sendonly or inactive to hold the call
Support Call Waiting of Huawei IPPBX	Support call waiting of Huawei IPPBX
Accept Orphan 200 OK	Support different to-tag 200 OK in a INVITE session
Domain Query Type	There are two modes option: A QUERY and SRV QUERY. Default is A QUERY.

Domain Re-resolution Interval	Default 0: forbidden
DNS cache	Cache the DNS query result
Early Media	Support receive Early Media
PRACK(RFC3262)	Support reliable transmission of provisional response
PRACK Only for 18x with SDP	Send PRACK only when there's SDP in 18x response
Early Answer	Support contain SDP in 18x
Session Timer (RFC4028)	Enable session timer, default to no
Session-Expires	The Session-Expires header field conveys the session interval for a SIP session.
Min-SE	Min-SE header field indicates the minimum value for the session interval.
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.
Heartbeat Timeout	Default to 16s
Username of OPTION(Heartbeat) for "SIP Server"	The user ID part of OPTION SIP message in the heartbeat request for SIP server
Username of OPTION(Heartbeat) for "IP TRUNK"	The user ID part of OPTION SIP message in the heartbeat request for IP trunk

Voice mail instructions:

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

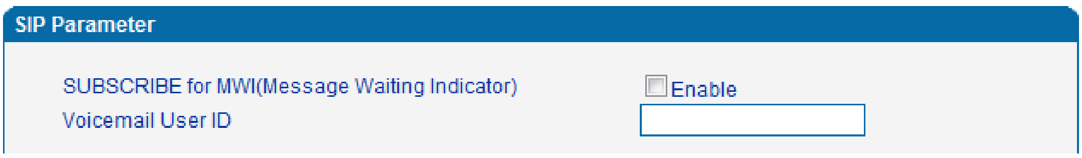
1）the GATEWAY register to Elastix server. Corresponding extension number enable voice mail function in Elastix and set password. As below：



Elastix Voicemail Configuration Interface

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

Elastix Voicemail Setting



VoiceMail Setting In SIP Parameter

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

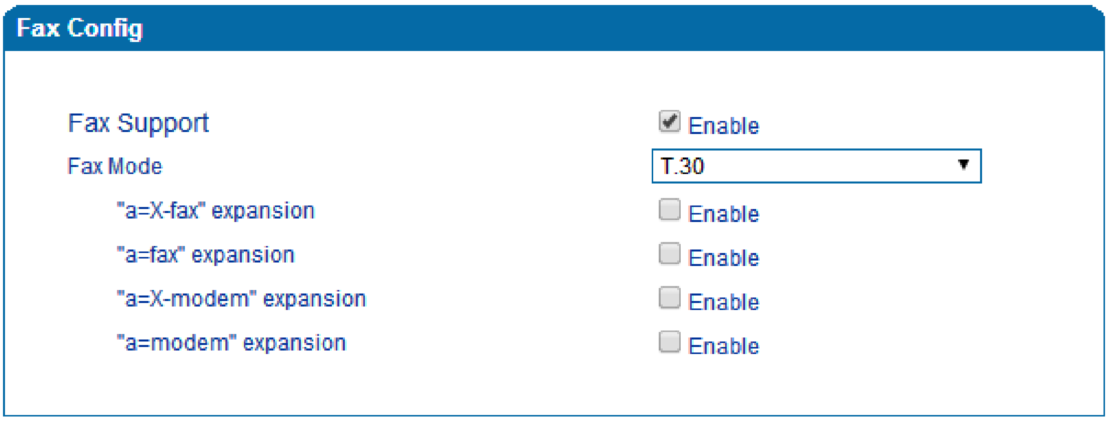
Voicemail Setting

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

Fax Parameter

Fax introduction：

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



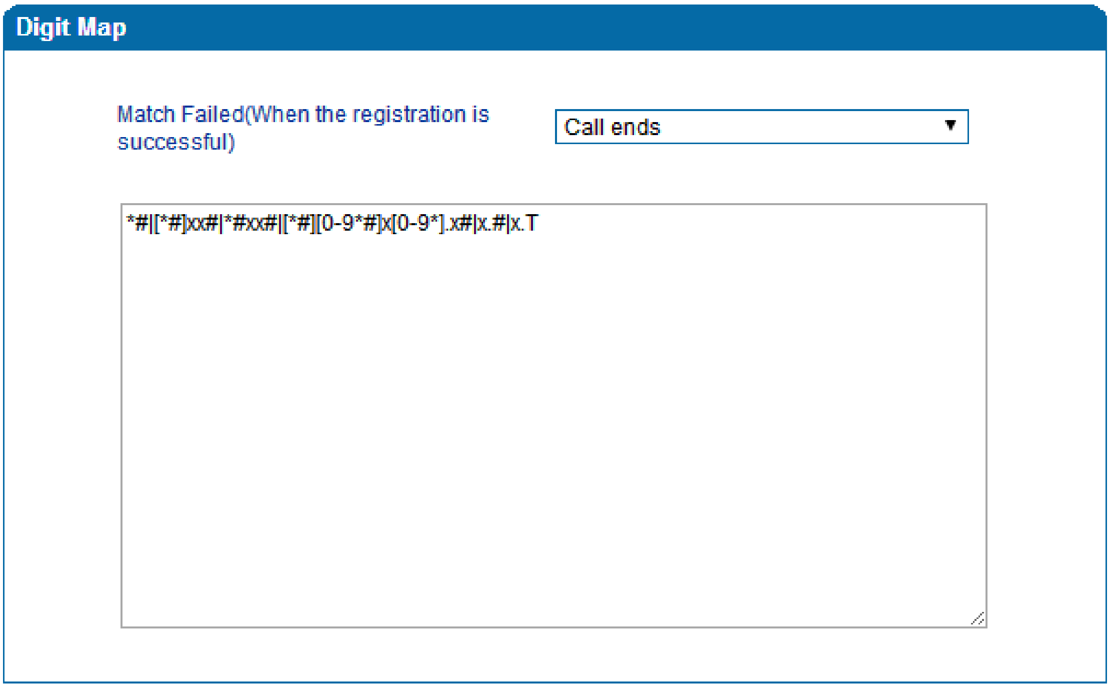
Fax Parameter Configure Interface

Fax parameter description:

Fax Support	Global switch for Fax support
Fax Mode	Fax mode support T.38, T.30(Pass-through),Modem, Adaptive.
Tone Detection by	Fax sound detection mode: Caller, Callee, Automatic.

“a=X-fax” expansion	Enable support of “a=X-fax” expansion
“a=fax” expansion	Enable support of “a=fax” expansion
“a=X-modem” expansion	Enable support of “a=X-modem” expansion
“a=modem” expansion	Enable support of “a=modem” expansion

Digit Map



Digit 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.

Feature Codes

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
Inquiry PortGroup Number	*115#	☑	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 by WAN in Route Mode	*160*	☑	Enable
Reset Basic Configuration	*165*	☑	Enable
Reset Factory Configuration	*166*	☑	Enable
Restart Device	*111#	☑	Enable
Call Function			
Call Holding	*#	☑	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
Call Forward Busy Deactivate	*91#	☑	Enable
Call Forward No Reply Activate	*92*	☑	Enable
Call Forward No Reply Deactivate	*93#	☑	Enable
Do Not Disturb Activate	*78#	☑	Enable
Do Not Disturb Deactivate	*79#	☑	Enable
Dial Voicemail	*200#	☑	Enable

Feature Code Configuration Interface

Inquiry LAN port IP address	Dial*158# to obtain device WAN port IP address

Inquiry WAN port IP address	Dial*159# to obtain device WAN port IP address
Inquiry Phone Number	Dial*114# to obtain port account
Inquiry PortGroup Number	Dial *115# to obtain port group number
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 Basic Configuration	Dial *165*000000# to restore default username/password and network configuration
Reset Factory Configuration	*166*000000#, reset factory
Restart Device	*111#, restart device
Call holding	During a call, 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

System Parameter

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

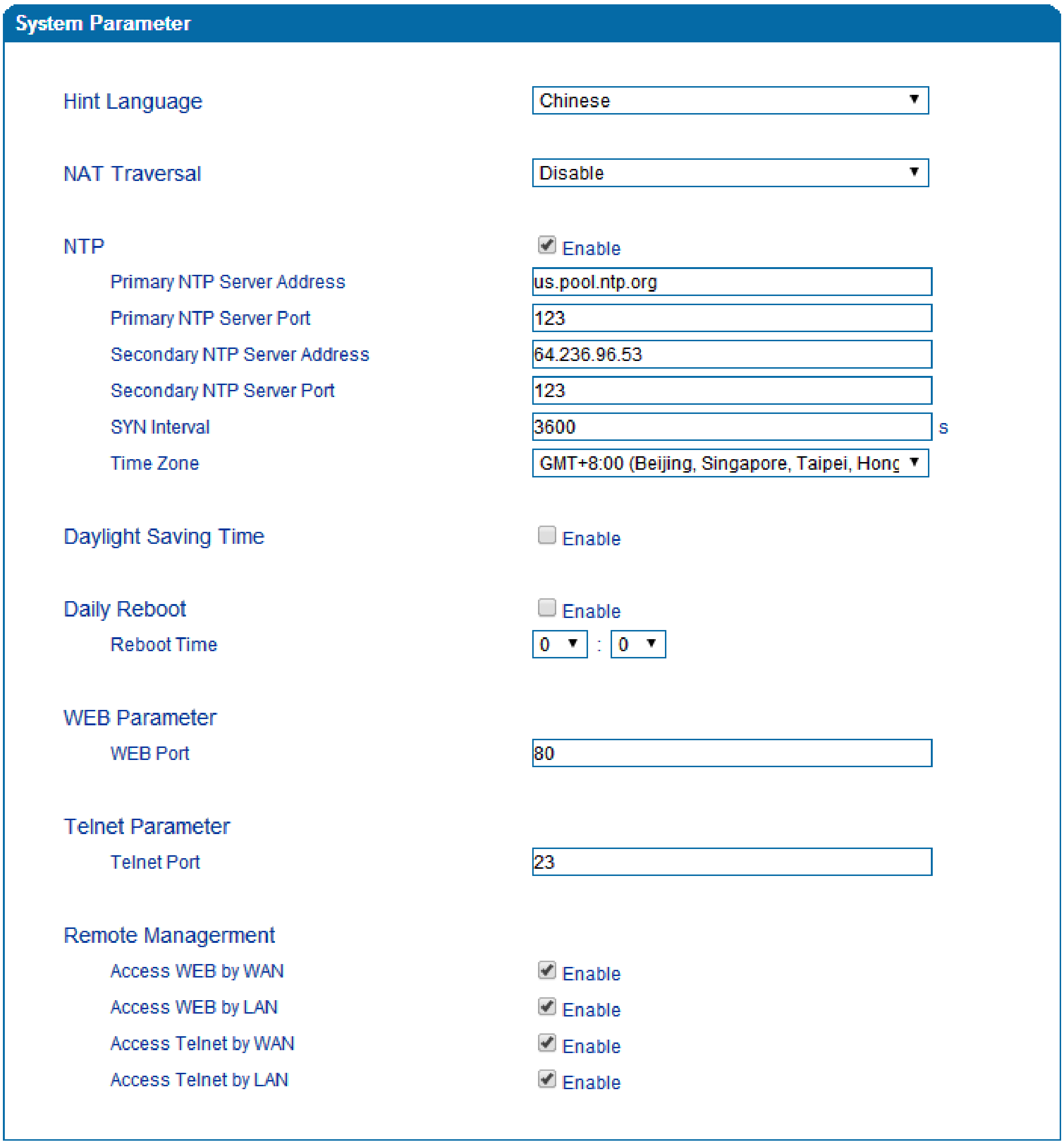
1）STUN：STUN（Simple Traversal of UDP over NATs）is a network protocol. It allows users back of NAT find their own public network address, NAT type and internet end port have been bound by NAT for a local port. Two back of NAT router devices established UDP communication through this information.

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

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

3）Provision：Auto Provisioning can be used to provide general and specific configuration parameters ("Settings") to the GATEWAYs and to manage firmware actualization.

System parameter configuration interface as follow:



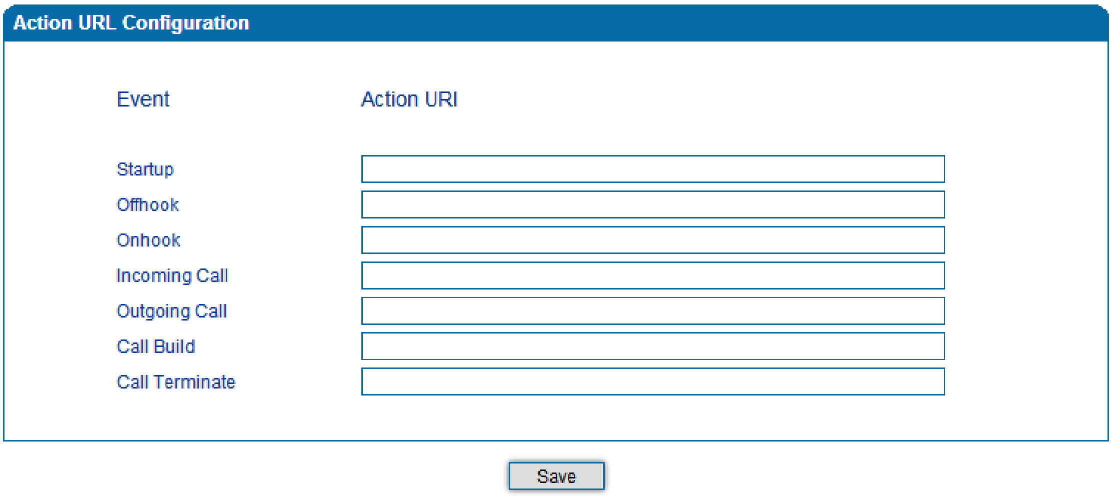
System Configuration Interface

Hint Language	IVR language
NAT Traversal	Disable, STUN, static NAT, dynamic NAT
Refresh interval	Default to 60
STUN Server Address	STUN server IP address or domain
STUN Server Port	STUN server port
NTP	Enable or disable NTP
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.
Daylight Saving Time	Enable or disable daylight saving time
Daily Reboot	Enable the gateway to reboot daily
Reboot time	Reboot time in 24H format
WEB Port	Gateway web port, default is 80
Telnet port	Listening port of telnet service, default to 23
Access WEB by WAN	Enable or disable Access web service from WAN
Access WEB by LAN	Enable or disable Access web service from LAN
Access Telnet by WAN	Enable or disable telnet web service from WAN
Access Telnet by LAN	Enable or disable telnet web service from LAN

Action URL

Action URL can be used as a means to allow the VoIP platform learn about the IAD's status. It transmits data by GET request over the HTTP protocol. The IAD is HTTP client. At HTTP server side, GET request must be processed, then cooperate with the VoIP platform. Thus, the purpose is achieved.



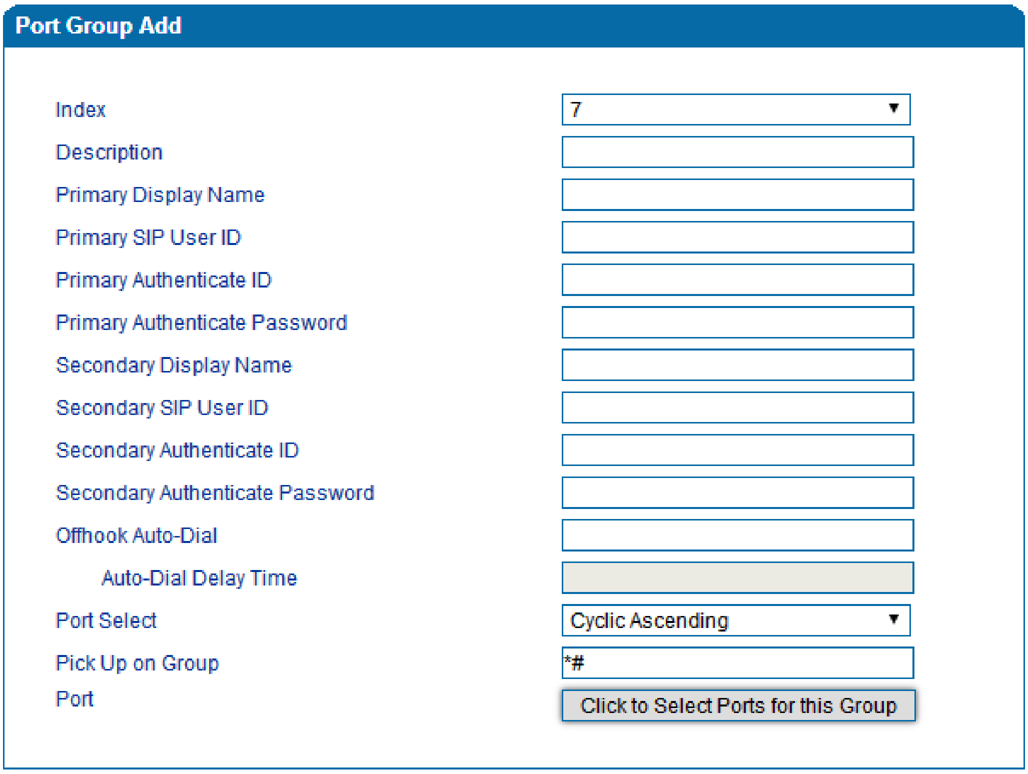
Action URL

Call & Routing

Wildcard Group

Port Group

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



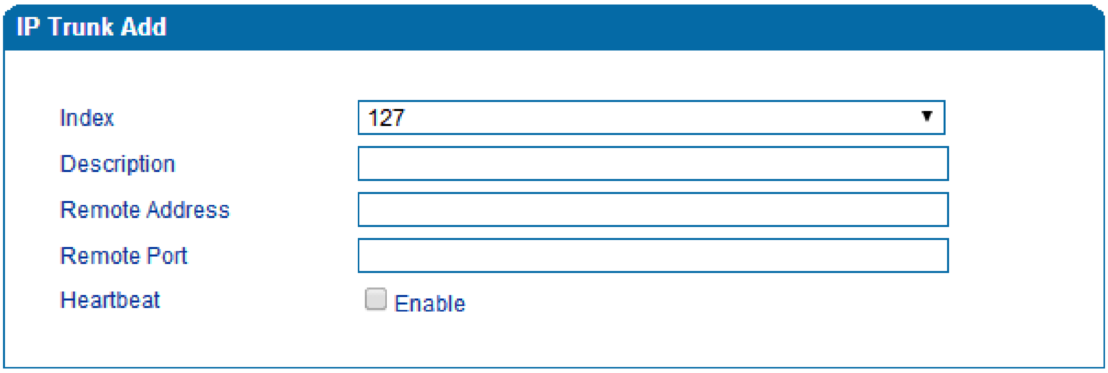
Port group configuration interface

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
Offhook Auto-Dial	Offhook auto-dial number
Auto-dial Delay time	Delay time before dialing
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
Pickup UP on group	When one of group port is ringing, other port can dial *# to pick up the call
Port	Add some ports to the same group

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 the GATEWAYs and also receiving incoming calls from other peer to peer gateway. IP trunk is help to the GATEWAYs establish peer-to-peer call between the GATEWAYs and other VoIP phones. IP trunk will be used in routing configuration.

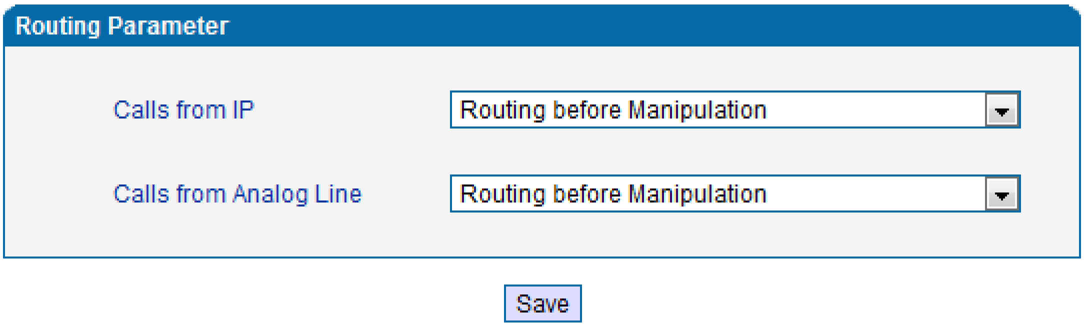


IP Trunk Configuration Interface

Index	IP trunk number, it is range from 0 to 127
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, THE GATEWAY will send "OPTION" to peer device

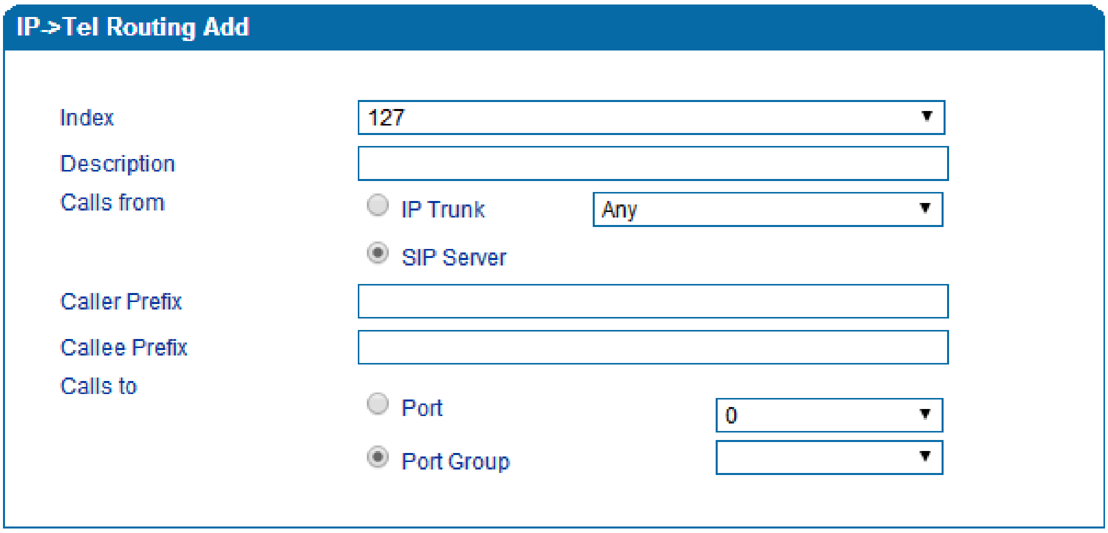
Routing Configuration



Routing Parameter Configuration Interface

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

IP-Tel Routing

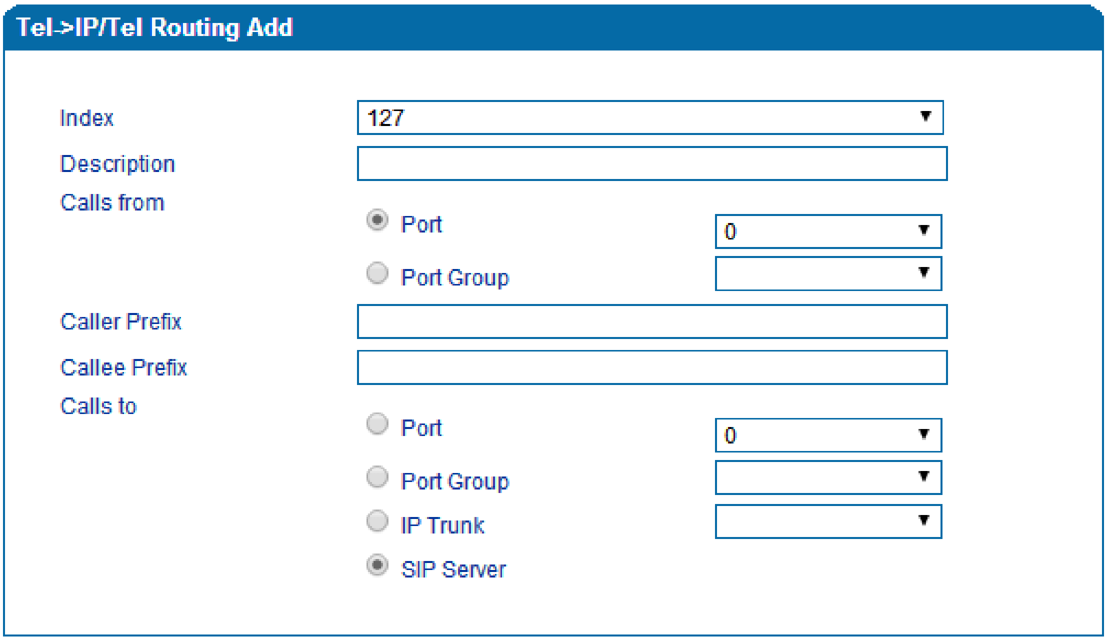


IP-Tel Routing Parameter

Index	Routing priority: 0-127, 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 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 or port group

Tel-IP/Tel Routing

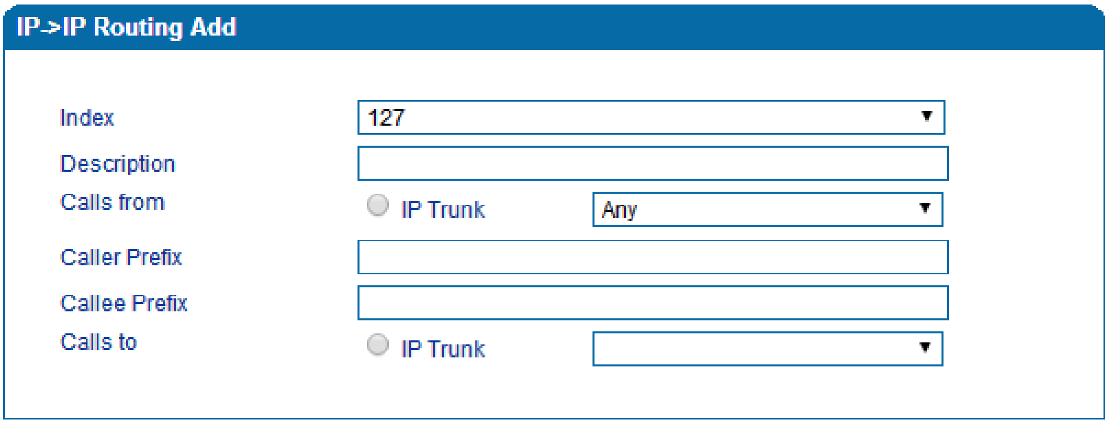


Tel-IP/Tel Parameters Configuration

Index	Routing priority :0-127, 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.

IP – IP Routing



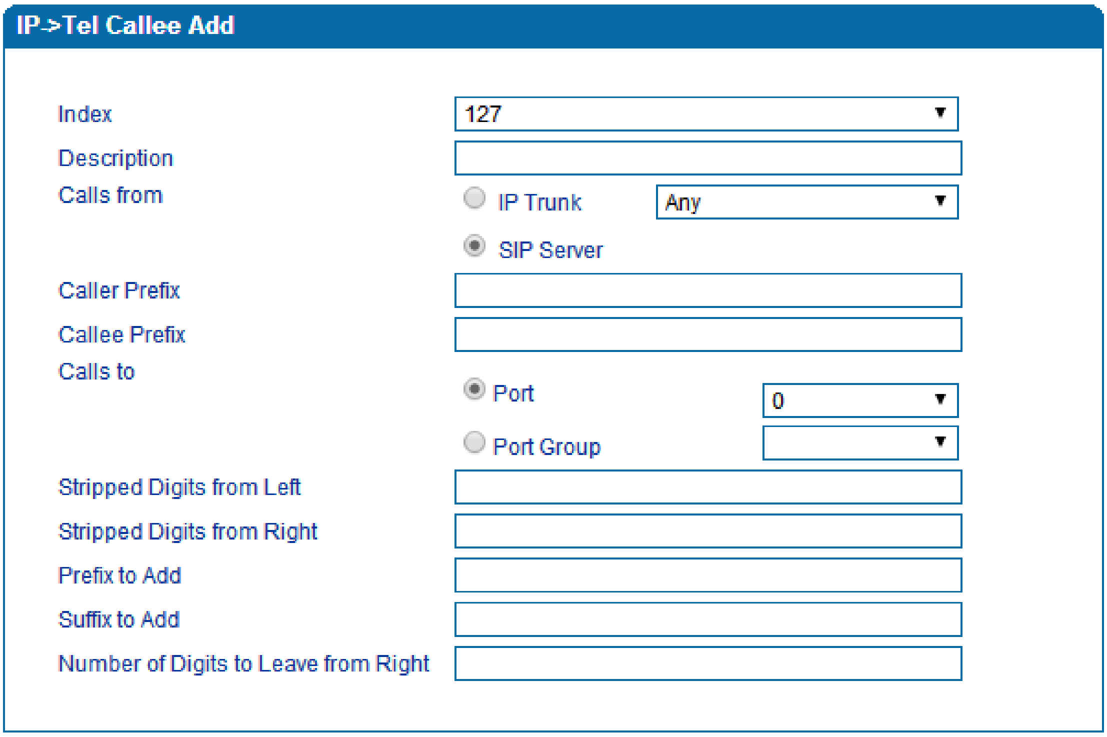
IP-IP routing Parameters Configuration

Index	Routing priority :0-127, 0 is the highest priority.
Description	its purpose is so you can identify the routing with a meaningful name
Calls From	IP-IP call select IP TRUNK
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 IP trunk

Manipulation Configuration

IP-Tel Callee

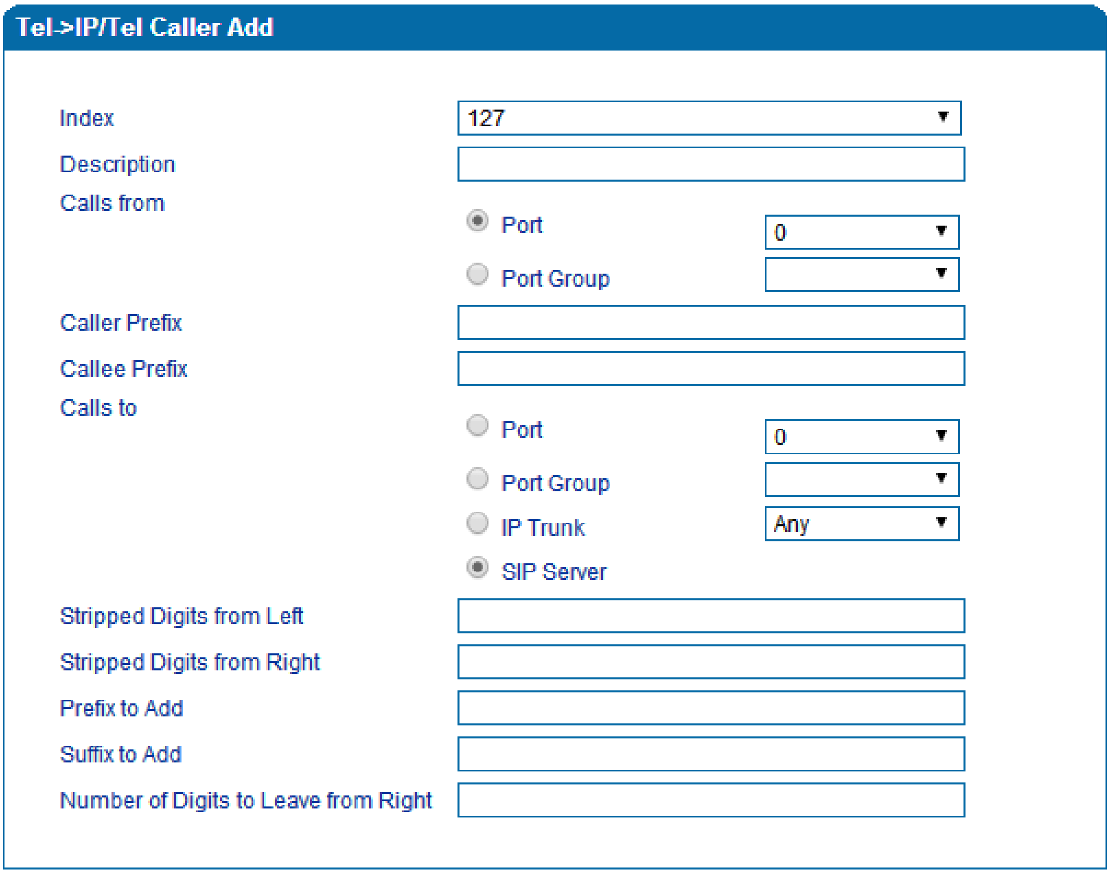


IP-Tel Callee number configuration

Description	IP-Tel manipulation name
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

Tel-IP/Tel Caller



Tel-IP Caller

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

Tel-IP/Tel Callee

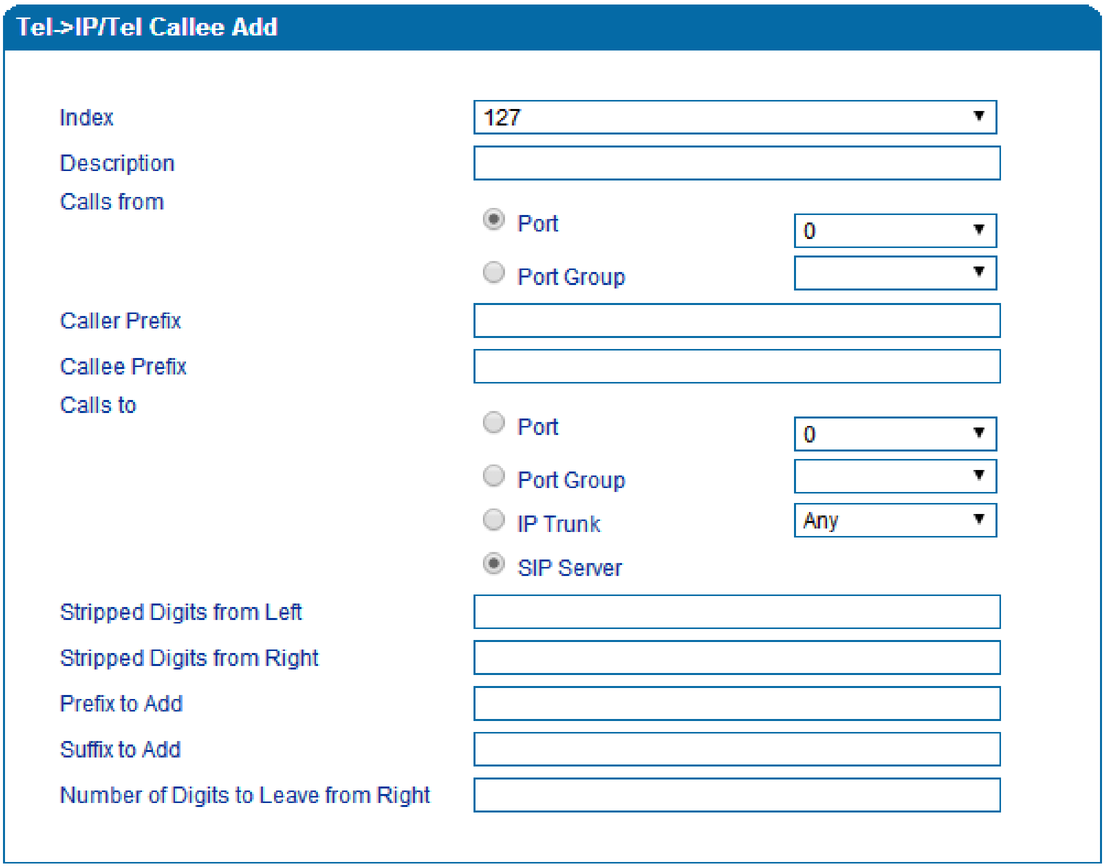


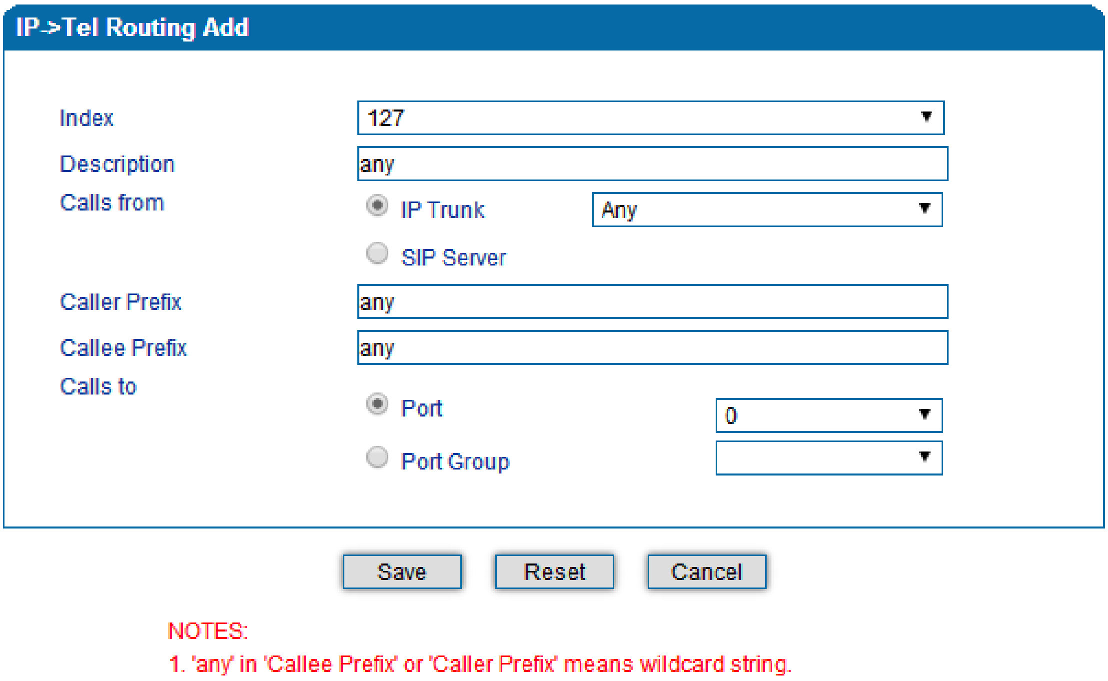
Figure 4.10-3 Tel-IP Callee

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

Routing rule examples

Route any calls from any IP to specific port

From web management access, Call & Routing -> IP-Tel Routing, click “Add” to create a new routing rule.

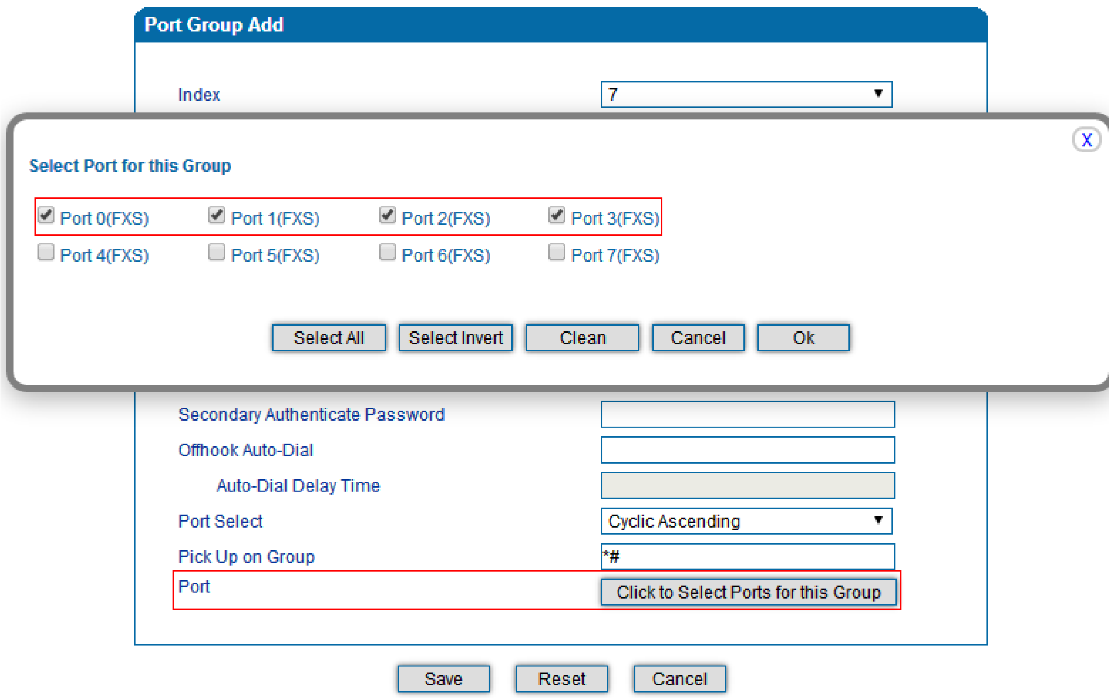


In the example above, all calls will be routed to port 0 when the routing rule is matched.

Route any calls from any IP to specified port group

- Create port group

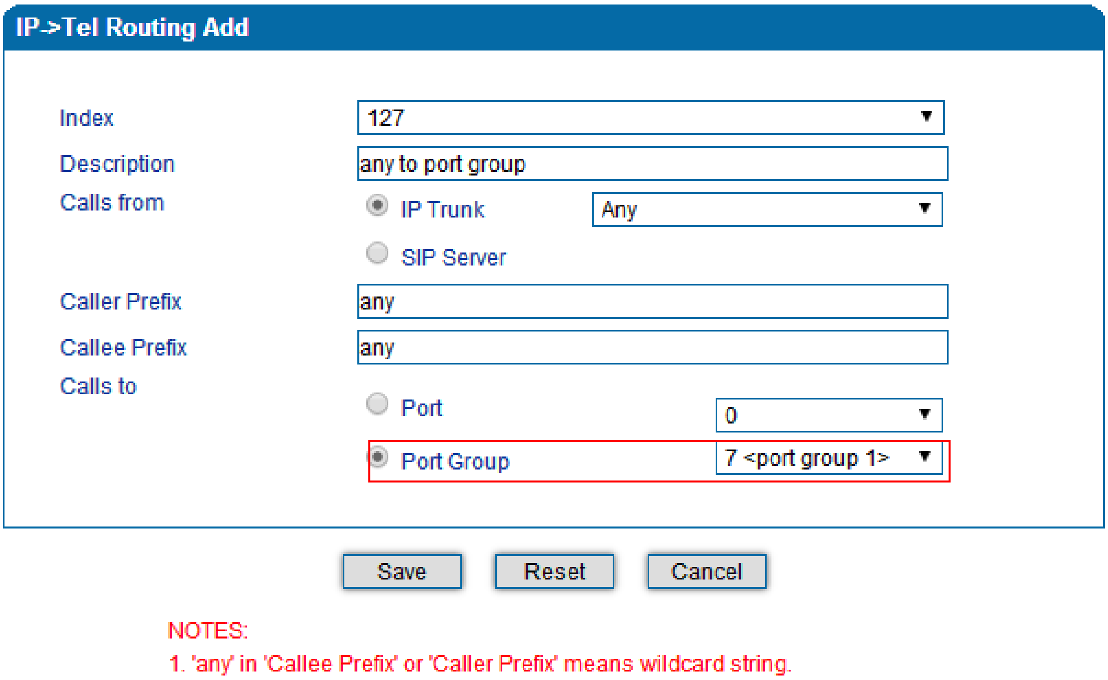
Before we can route calls to a port group, create the port group first as below. From Call & Routing -> Port Group, click “Add” to create a new port group.



Port 0 to port 4 are assigned to port group 7.

- Route any calls to port group

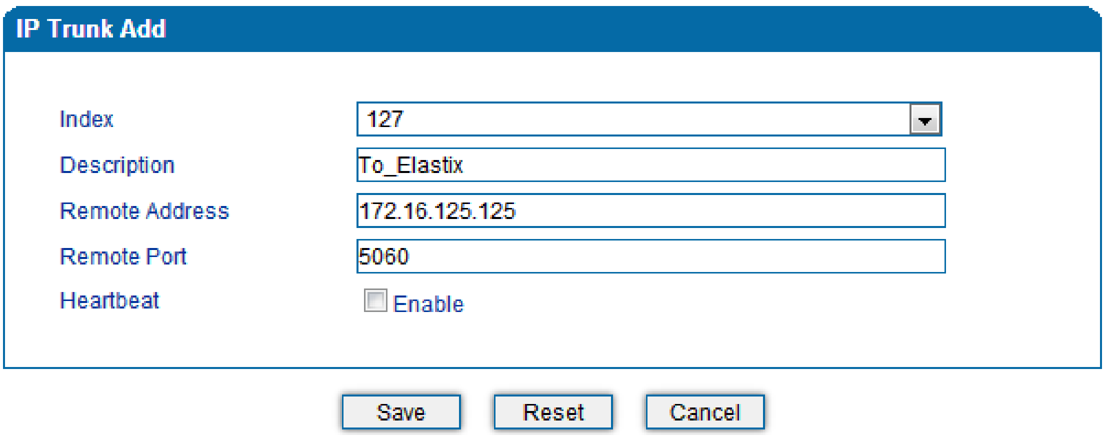
From Call & Routing -> IP-Tel Routing, click “Add” to create a new routing rule.



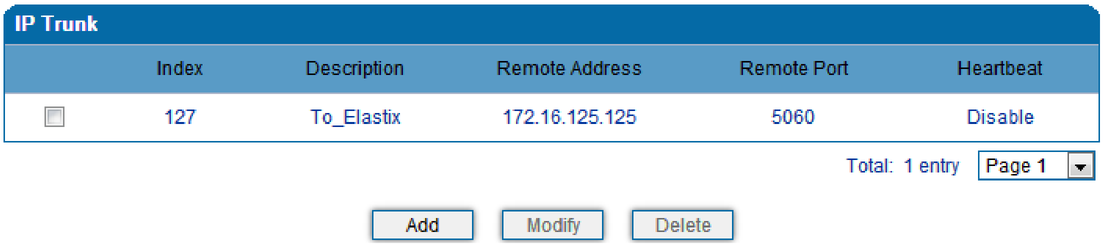
As above show, when this routing rule is matched, the call will be routed to port group 7.

Route any calls from any port to specific SIP IP trunk

Create SIP IP Trunk from Call & Routing -> IP Trunk, see as bellow:



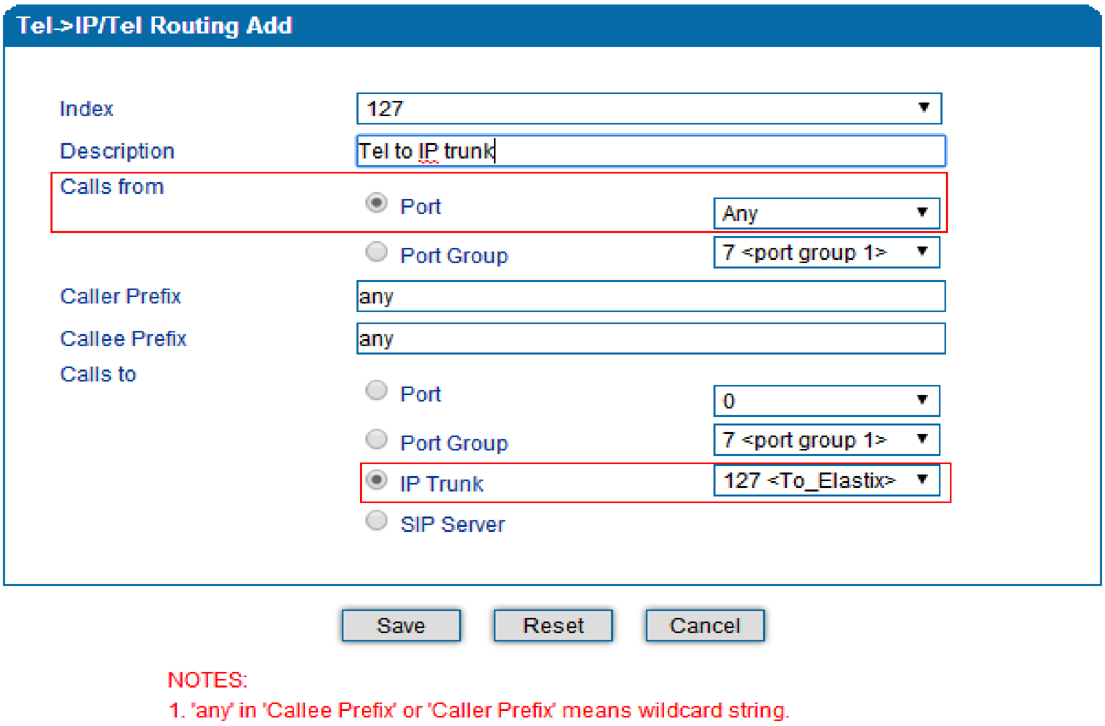
After SIP IP Trunk created, check the configuration:



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

Create Tel -> IP routing rule

From Call & Routing -> Tel-IP Routing, click “Add” to create a new Tel to IP routing rule.



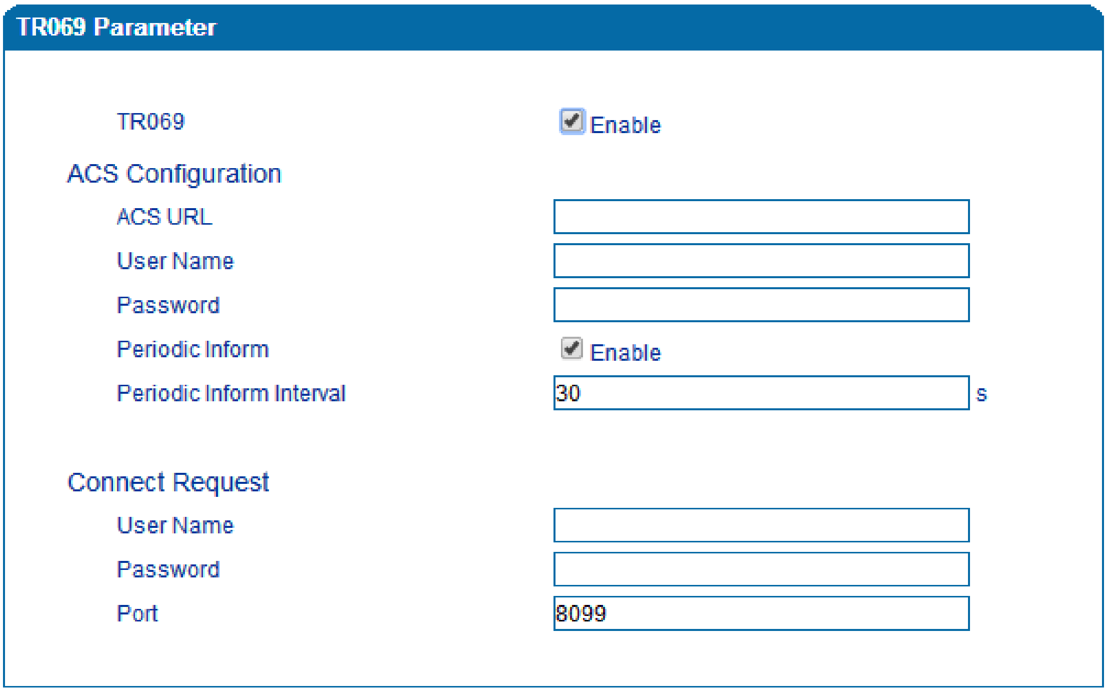
All call from any caller number to any called number will be routed to SIP IP trunk 127.

Maintenance

TR069

ACS URL: Type the Auto-Configuration Server URL Address provided by the provider. The ACS URL normally start with http:// or https://

Username/password: ACS authentication only if needed, e.g. device ID as username/password

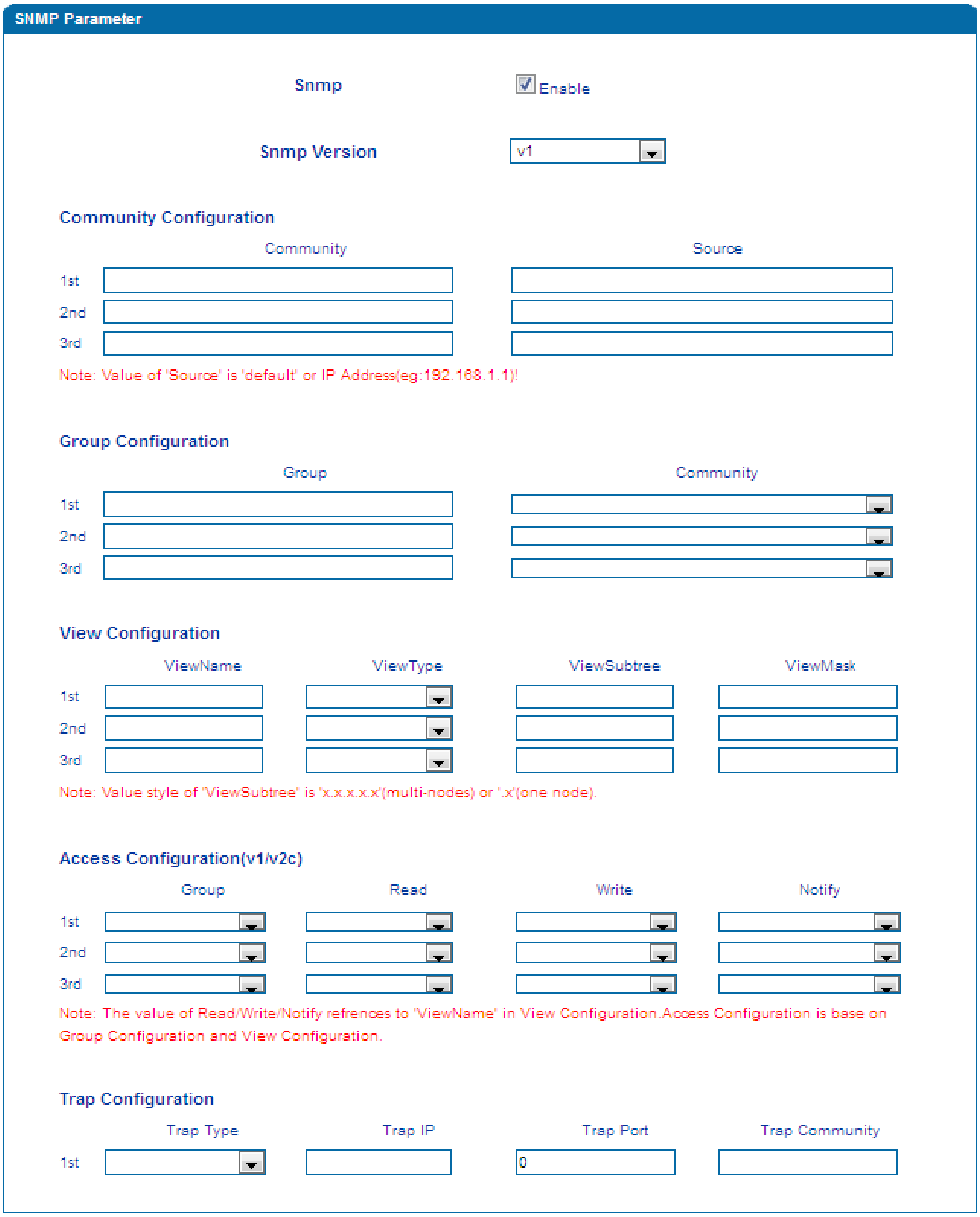


TR069 parameters

SNMP

SNMP Parameter

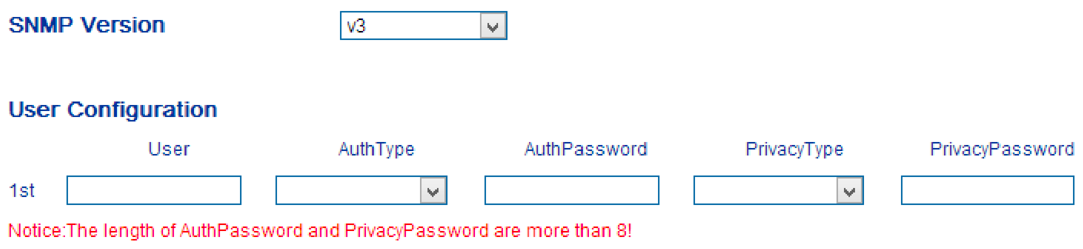
- SNMP enable: to disable or enable the SNMP feature
- SNMP version: the gateway support SNMP v1 and v2
- Community: the community name to read through SNMP protocol
- Source: the IP address of SNMP server



SNMP

User configuration

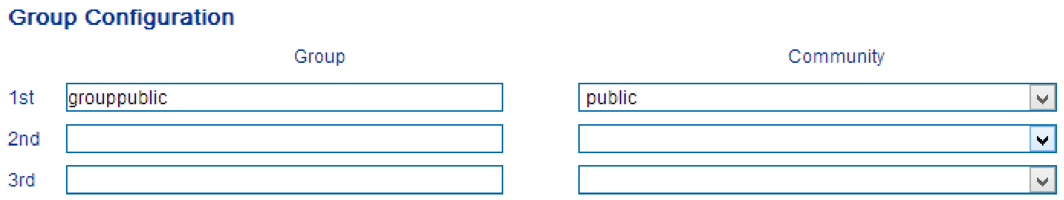
This configuration only available on SNMP v3.



Group configuration

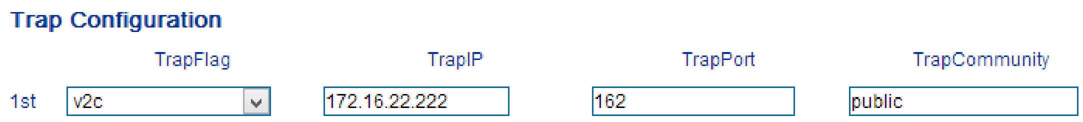
Group: community group name which consist of character string.

Community: let community join the community group which configured above



Trap configuration

Trap configuration enable to configure Trap server IP and port. This setting available for SNMP v2c and v1.



Syslog

Syslog is a standard for network device data logging. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices which would otherwise be unable to communicate a means to notify administrators of problems or performance. There are 5 levels of syslog, Including NONE, DEBUG, NOTICE, WARNING and ERROR.

The Signal Log is include following traces which defined in system by default

- *SD, hardware debug*
- *SIP, SIP signaling trace*
- *STUN, STUN logs*
- *ECC, detail information of call control module*

- *RE, the common communication module for SCP and SIM*
- *SCP, the communication protocol between gateway and cloud server*

The media log is include following traces which defined in system by default

- *RTP, RTP stream info collection*
- *SIM, to output traces between gateway and remote SIM cards*

The System Log is include following traces which mainly used by developer

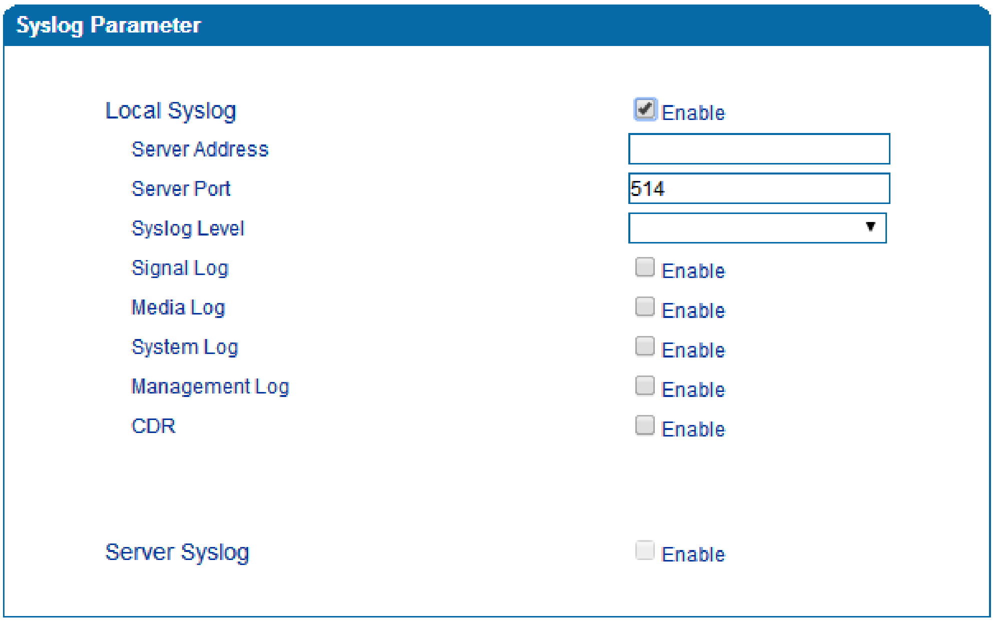
- *SYS, system log*
- *TIMER, system process*
- *TASK, system task process*
- *CFM, system process*
- *NTP*

The Management Log is include following traces which defined in system by default

- *CLI, command line*
- *TEL,*
- *LOAD, firmware upload*
- *SNMP*
- *WEBS, embedded web server*
- *PROV, provisioning*

Server Syslog:

When the gateway register to SIM Cloud server, the option will be changed to un-configurable and all logs to be storage on server.

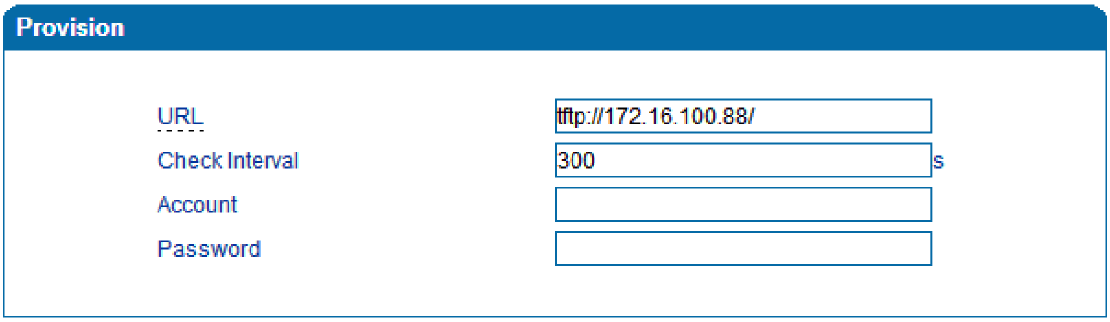


Syslog Parameter Configuration

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

Provision

Gateway can be managed by provisioning server for upgrading firmware, configuring parameters. For this purpose, provisioning server must be configured on the gateway.

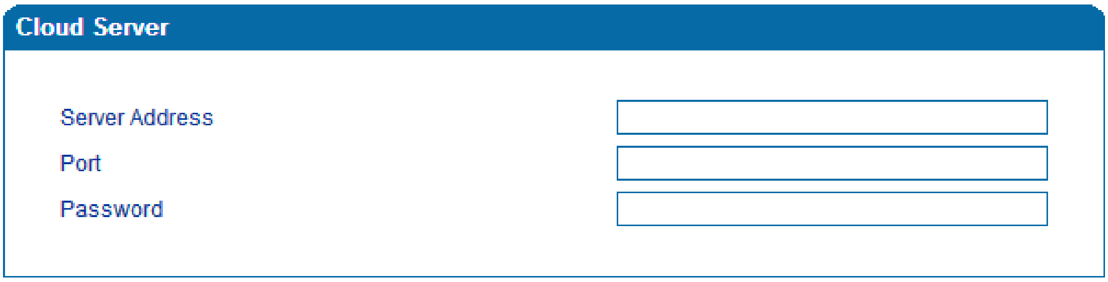


Provision

URL	Provisioning server URL, support HTTP, TFTP, FTP
Check Interval	The interval to check the changes on the provisioning server
Account	Account for login provisioning server
Password	Account for login provisioning server

Cloud server

Register the gateway with cloud server for being managed by cloud server.



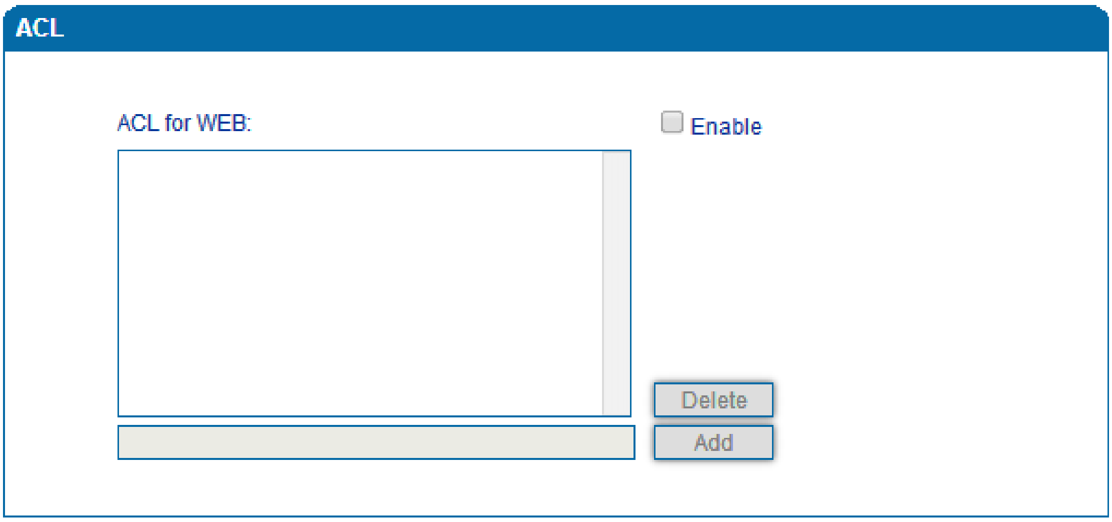
Cloud server

Server Address	The cloud server IP address or domain
port	Cloud server listening port
Password	Password for register with cloud server

Security

WEB ACL

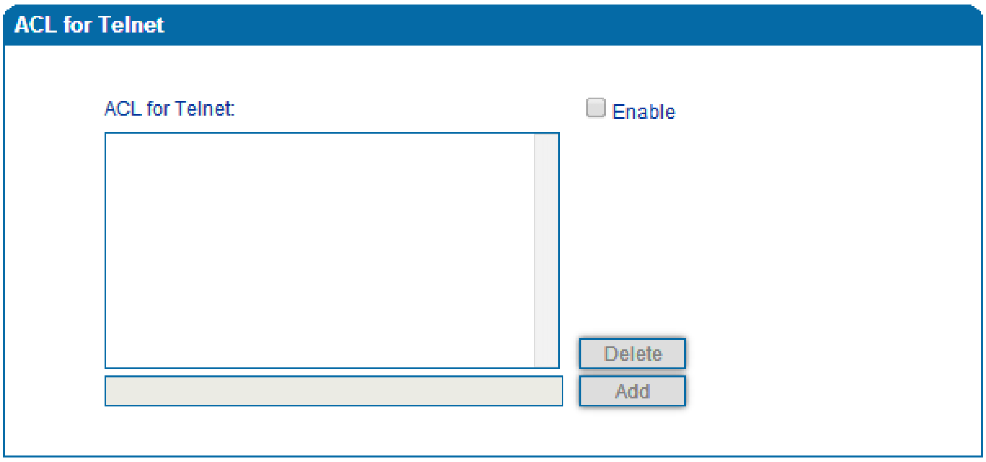
ACL for WEB enable you to configure IP list/users who allow to access the WEB page of device. IP lists can't be null once ACL enable.



ACL for WEB

Telnet ACL

ACL for telnet enable you to configure IP list/users who allow to access the telnet page of device. IP lists can’t be null once ACL enable.

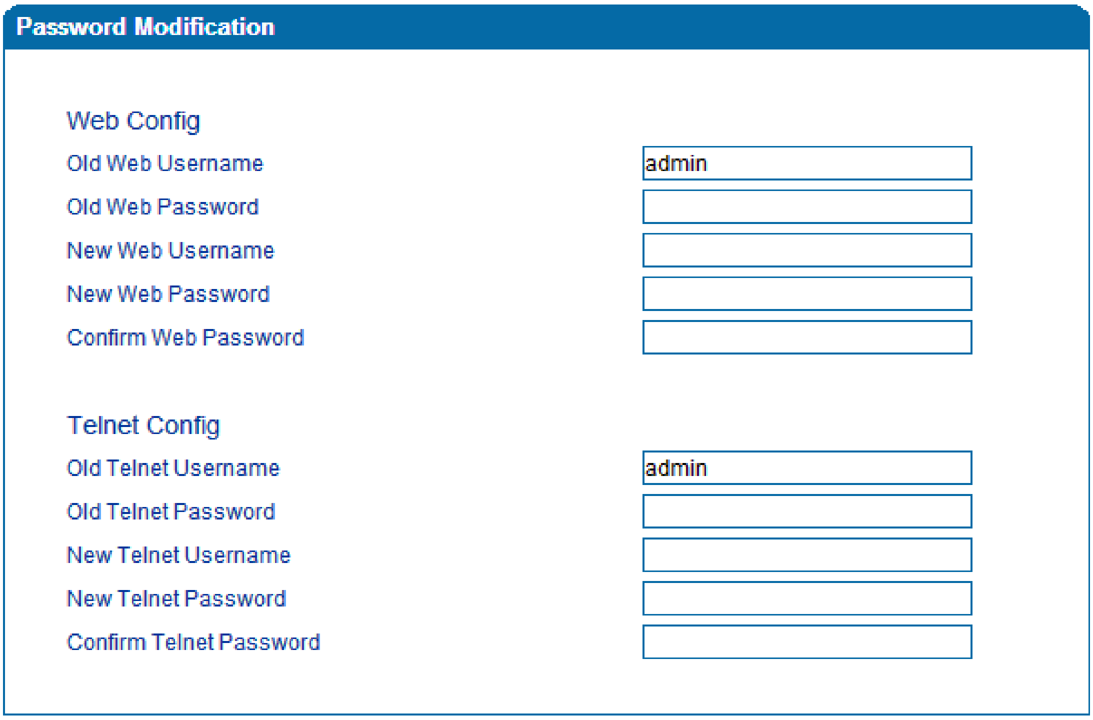


ACL for telnet

Passwords

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

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



Passwords configuration

Tools

Firmware upload

Firmware upload steps:

Step 1.

Check current running version on gateway, to get firmware version on web page ***System Information***

Current Software Version	DAG1000-8S 2.18.02.03 PCB 0 LOGIC 0 BIOS 1, 2013-11-16 16:39:57
Backup Software Version	DAG1000-8S 2.18.02.03 PCB 0 LOGIC 0 BIOS 1, 2013-11-16 16:39:57
U-BOOT Version	6.1
Kernel Version	10.1
FS Version	1.0.9.12 Sun, 30 Jun 2013 15:59:32 +0800
Hint Language	Chinese

Firmware version

Step 2.

Prepare firmware package. The most important is that the package must be match with existing version. Package version consist of several parts, as below:

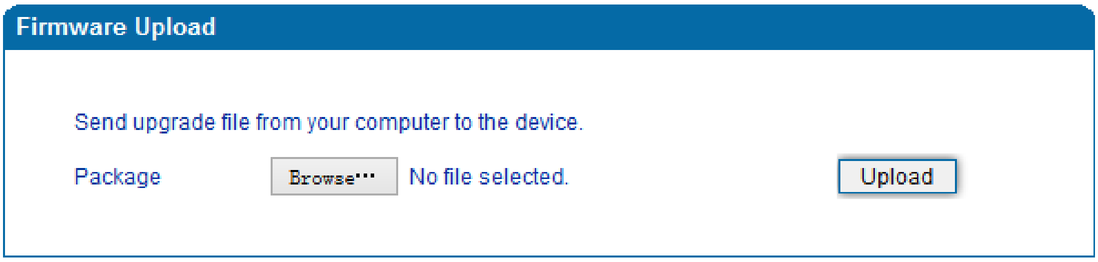
1.18.xx.xx

01/02 is vendor name

18 is hardware version, xx.xx is version number

Step 3.

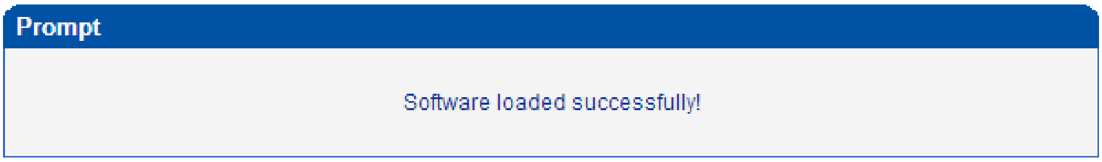
Upload firmware, select the package from specific folder on the computer and click ***Upload*** button.



Firmware upload

Step 4.

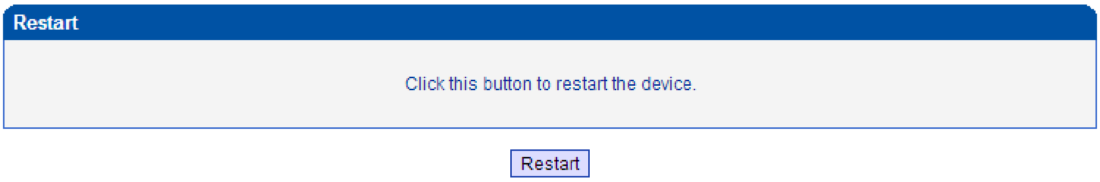
Keep waiting until it prompt 'Software loaded successfully!'



Firmware upload success

Step 5.

Reboot gateway. Refer to web page ***Maintenance-> Device Restart***



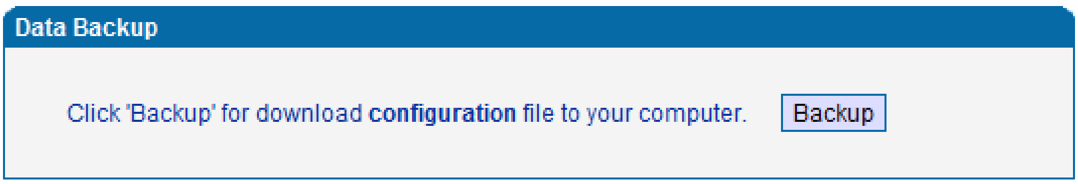
Restart gateway

Data Backup

The process data backup:

1) Click "Data Backup"

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

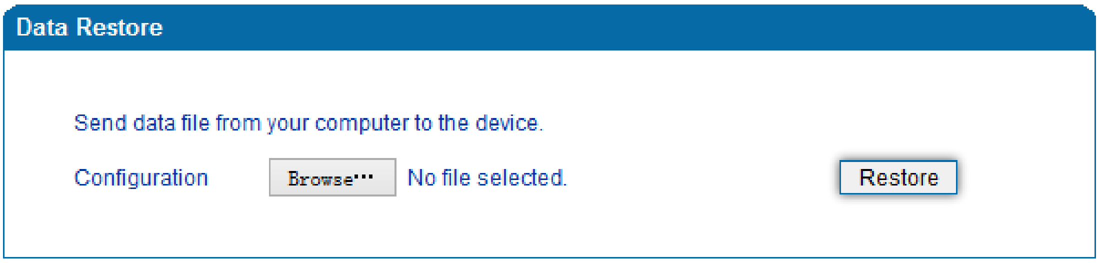


Data Backup

Data Restore

The processes of data restore:

- Click “Data Restore”
- Browse file, select data file.
- Click “Restore” and then import successfully, the device will restart automatically.



Data restore

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.

Ping instructions:

1) Click “ping test”

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

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

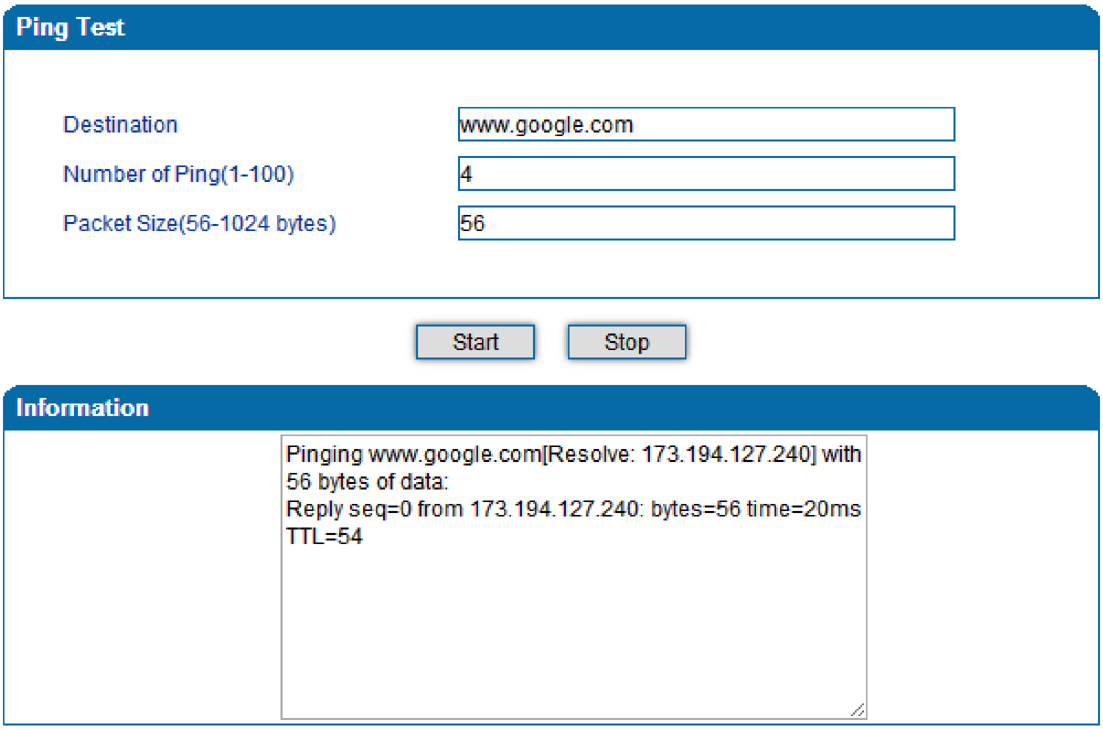


Figure 4.14.4 Ping Test

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：

- Click tracert test.
- Fill IP address or domain connected, click start.

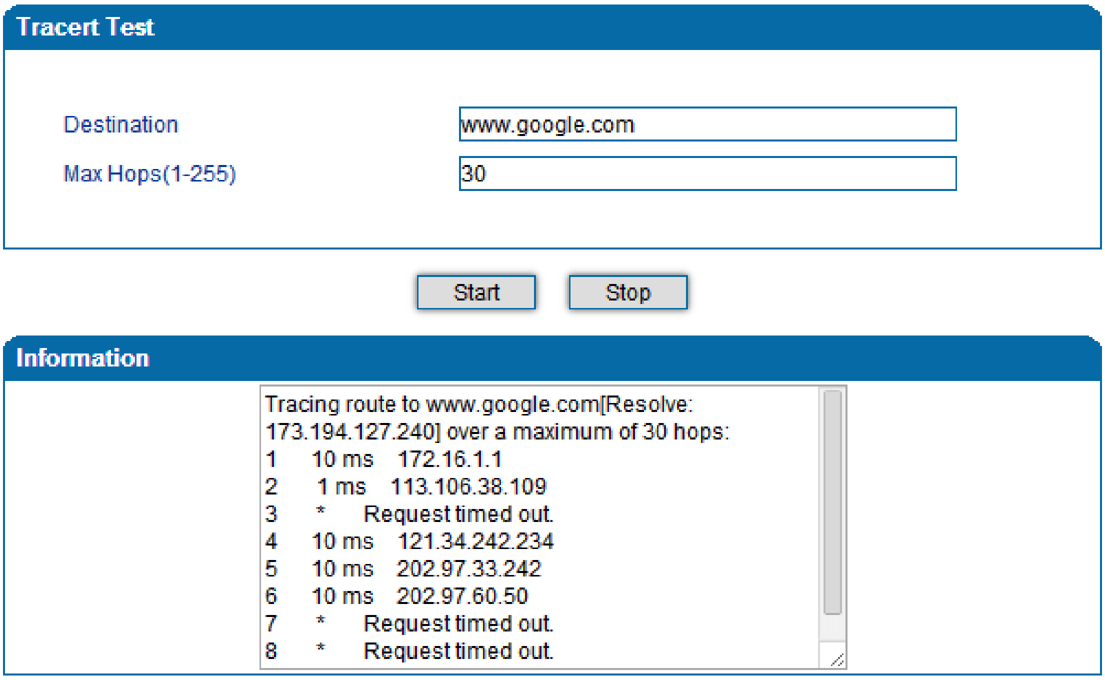


Figure 4.14.5 Tracert Test

Outward Test

Outward test enable you to diagnose the physical phone lines which follow GR909 standards. To start outward test, select the Ports to be tested and click start button. Testing will takes about few minutes.

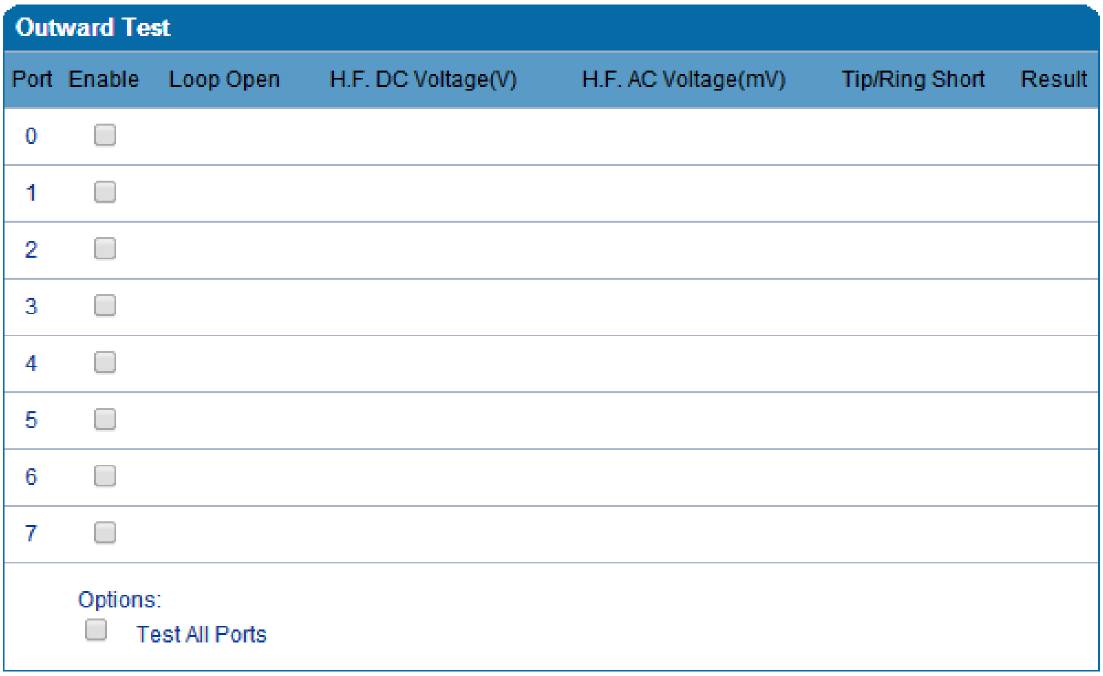


Figure 4.14.6 Outward Test

Test results

OK: the analog phone set and phone line are working well

FAIL: analog phone doesn't connect to FXS port or something wrong phone set

Network Capture

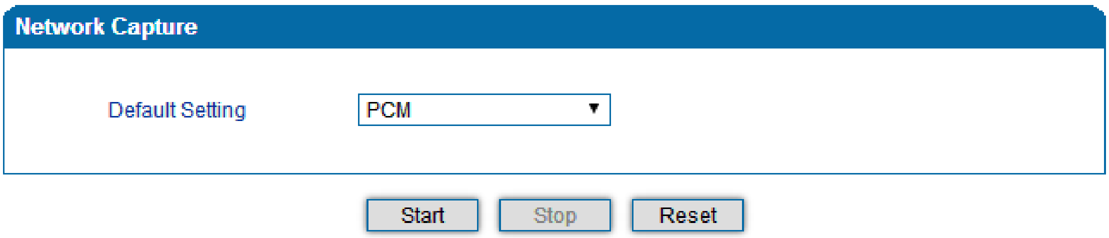
Network capture is a very important diagnostic tool for maintenance. This section is describes how to enable network capture.

- **Getting start to PCM capture**

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

  - **To enable PCM capture**

    - Select ‘PCM’ on Network Capture page



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

The capture is named to ‘capture(x).pcap’, x is serial number of capture and will be added 1 in next time. The sample of PCM capture as below:

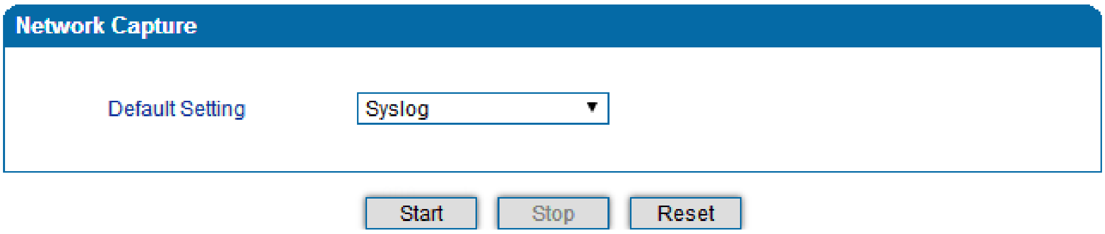
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0021 Ch: 0xFFFF, Seq: 8 (From Host)
2	0.000131	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
3	0.000245	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	44	--> 0x0021 Ch: 0xFFFF, Seq: 11 (From Host)
4	1.320893	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0e00 Ch: 0x0003, Seq: 0 (From Host)
5	1.321022	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
6	1.321129	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	--> 0x0e00 Ch: 0x0003, Seq: 1 (From Host)
7	1.329890	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0e01 Ch: 0x0003, Seq: 1 (From Host)
8	1.330010	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
9	1.330093	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	--> 0x0e01 Ch: 0x0003, Seq: 2 (From Host)
10	1.330472	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0802 Ch: 0x0003, Seq: 2 (From Host)
11	1.330566	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
12	1.330639	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	--> 0x0802 Ch: 0x0003, Seq: 3 (From Host)
13	1.330820	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0803 Ch: 0x0003, Seq: 3 (From Host)
14	1.330903	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
15	1.330989	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	--> 0x0803 Ch: 0x0003, Seq: 4 (From Host)
16	1.337791	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x9010 Ch: 0x0003, Seq: 4 (From Host)
17	1.337996	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
18	1.338033	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x9010 Ch: 0x0003, Seq: 5 (To Host)
19	1.338369	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x9000 Ch: 0x0003, Seq: 5 (From Host)
20	1.338460	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
21	1.338564	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x9000 Ch: 0x0003, Seq: 6 (To Host)
22	1.343521	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x8084 Ch: 0x0003, Seq: 6 (From Host)
23	1.343627	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
24	1.343725	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x8084 Ch: 0x0003, Seq: 7 (To Host)
25	1.344060	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x8001 Ch: 0x0003, Seq: 7 (From Host)

Getting start to Syslog capture

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

To enable syslog capture

- Select Syslog special only on Network Capture page



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

The capture is named to ‘capture(x).pcap’, x is serial number of capture and will be added 1 in next time. The sample of syslog capture as below:

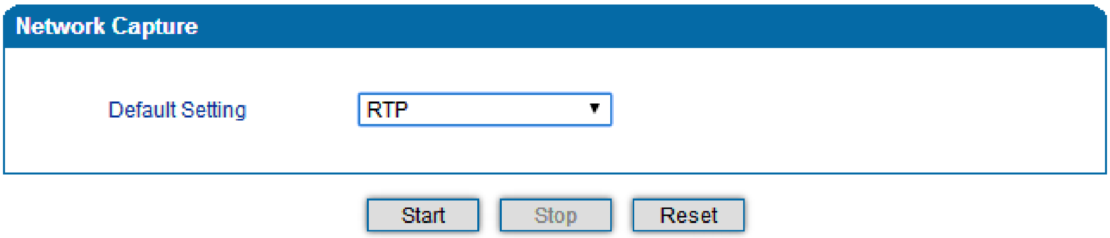
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.222.22	1.1.1.1	Syslog	172	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 0> [DEBUG] --->> to 172.16.222.22/5060 crypt:FALSE Phone
2	0.000344	172.16.222.22	1.1.1.1	Syslog	520	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 1> [DEBUG] OPTIONS sip:heartbeat@172.16.222.22 SIP/2.0\r\
3	0.013432	172.16.222.22	1.1.1.1	Syslog	595	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 2> [DEBUG] <<---*** message from 172.16.222.22/5060,crypt
4	0.013750	172.16.222.22	1.1.1.1	Syslog	176	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 3> [DEBUG] <<--- from 172.16.222.22/5060,crypt:FALSE, Phc
5	0.014036	172.16.222.22	1.1.1.1	Syslog	520	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 4> [DEBUG] OPTIONS sip:heartbeat@172.16.222.22 SIP/2.0\r\
6	0.014512	172.16.222.22	1.1.1.1	Syslog	172	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 5> [DEBUG] --->> to 172.16.222.22/5060 crypt:FALSE Phone
7	0.014806	172.16.222.22	1.1.1.1	Syslog	587	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 6> [DEBUG] SIP/2.0 200 OK\r\nVia: SIP/2.0/UDP 172.16.222.
8	0.028396	172.16.222.22	1.1.1.1	Syslog	662	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 7> [DEBUG] <<---*** message from 172.16.222.22/5060,crypt
9	0.028759	172.16.222.22	1.1.1.1	Syslog	176	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 8> [DEBUG] <<--- from 172.16.222.22/5060,crypt:FALSE, Phc
10	0.029052	172.16.222.22	1.1.1.1	Syslog	587	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 9> [DEBUG] SIP/2.0 200 OK\r\nVia: SIP/2.0/UDP 172.16.222.
11	0.030017	172.16.222.22	1.1.1.1	Syslog	233	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 10> [DEBUG] sip-->app: msgtype:ST_SIP_SERVER_CONN \r\n cal
12	0.331167	172.16.222.22	1.1.1.1	Syslog	983	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 11> [DEBUG] <<---*** message from 172.16.222.127/5060,cryp
13	0.331498	172.16.222.22	1.1.1.1	Syslog	177	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 12> [DEBUG] <<--- from 172.16.222.127/5060,crypt:FALSE, Ph
14	0.331959	172.16.222.22	1.1.1.1	Syslog	907	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 13> [DEBUG] INVITE sip:10086@172.16.222.22:5060 SIP/2.0\r\
15	0.332307	172.16.222.22	1.1.1.1	Syslog	122	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_ecc: < 14> [DEBUG] get route entry 31\r\n
16	0.332584	172.16.222.22	1.1.1.1	Syslog	111	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_ecc: < 15> [DEBUG] lPort:3\r\n
17	0.332848	172.16.222.22	1.1.1.1	Syslog	124	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_ecc: < 16> [DEBUG] get route, to port:3\r\n
18	0.333315	172.16.222.22	1.1.1.1	Syslog	526	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 17> [DEBUG] sip-->app: localindex:69, msgtype:SIP_CALL_INV
19	0.333603	172.16.222.22	1.1.1.1	Syslog	173	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 18> [DEBUG] --->> to 172.16.222.127/5060 crypt:FALSE Phone
20	0.333877	172.16.222.22	1.1.1.1	Syslog	386	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 19> [DEBUG] SIP/2.0 100 Trying\r\nVia: SIP/2.0/UDP 172.16.
21	0.346687	172.16.222.22	1.1.1.1	Syslog	131	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_ecc: < 20> [DEBUG] RTP: alg:0, pkt:20, band:-1\r\n
22	0.347453	172.16.222.22	1.1.1.1	Syslog	120	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_ecc: < 21> [DEBUG] dial tick:102433\r\n
23	7.232839	172.16.222.22	1.1.1.1	Syslog	533	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 22> [DEBUG] <<---*** message from 172.16.222.127/5060,cryp
24	7.233513	172.16.222.22	1.1.1.1	Syslog	177	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 23> [DEBUG] <<--- from 172.16.222.127/5060,crypt:FALSE, Ph
25	7.233959	172.16.222.22	1.1.1.1	Syslog	457	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 24> [DEBUG] CANCEL sip:10086@172.16.222.22:5060 SIP/2.0\r\
26	7.234596	172.16.222.22	1.1.1.1	Syslog	287	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 25> [DEBUG] sip-->app: localindex:69, msgtype:SIP_CALL_BYE

Getting start to RTP capture

PCM capture is help to analysis voice stream between gateway and remote IPPBX/SIP Server.

To enable RTP capture:

- Select RTP special on Network Capture page



- Click Start to enable RTP capture
- Dialing out through gateway, start talking a short while then hangup the call.
- Click Stop to disable RTP capture
- Save the capture to local computer

The capture is named to 'capture(x).pcap', x is serial number of capture and will be added 1 in next time. The sample of RTP capture as below:

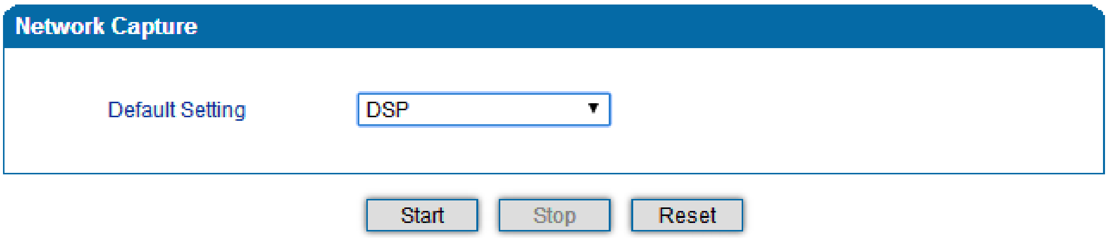
No.	Time	Source	Destination	Protocol	Length	Info
176	7.020000	172.16.221.228	116.204.105.50	SIP	565	Request: REGISTER sip:116.204.105.50 |
178	7.030000	116.204.105.50	172.16.221.228	SIP	411	Status: 200 OK (1 bindings) |
244	11.610000	172.16.221.228	58.56.64.101	SIP/SDP	814	Request: INVITE sip:201@58.56.64.101 |
248	11.710000	58.56.64.101	172.16.221.228	SIP	480	Status: 100 Trying |
249	11.710000	58.56.64.101	172.16.221.228	SIP/SDP	733	Status: 183 Session Progress |
250	11.710000	58.56.64.101	172.16.221.228	SIP/SDP	719	Status: 200 OK |
252	11.720000	172.16.221.228	58.56.64.101	RTP	66	Unknown RTP version 1
253	11.720000	172.16.221.228	58.56.64.101	RTP	66	Unknown RTP version 1
254	11.720000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1000, Time=160, Mark
255	11.720000	172.16.221.228	58.56.64.101	RTP	66	Unknown RTP version 1
256	11.730000	172.16.221.228	58.56.64.101	RTP	66	Unknown RTP version 1
257	11.730000	172.16.221.228	58.56.64.101	RTP	66	Unknown RTP version 1
258	11.740000	172.16.221.228	58.56.64.101	SIP	434	Request: ACK sip:201@58.56.64.101:5060 |
259	11.740000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1001, Time=320
261	11.770000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1002, Time=480
263	11.780000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1003, Time=640
264	11.810000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1004, Time=800
265	11.830000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1005, Time=960
266	11.840000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1006, Time=1120
267	11.870000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1007, Time=1280
268	11.890000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1008, Time=1440
270	11.900000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1009, Time=1600
271	11.930000	172.16.221.228	58.56.64.101	RTP	74	PT=ITU-T G.729, SSRC=0x43455AA6, Seq=31521, Time=1806312883
273	11.930000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1010, Time=1760
274	11.940000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1011, Time=1920
275	11.950000	172.16.221.228	58.56.64.101	RTP	74	PT=ITU-T G.729, SSRC=0x43455AA6, Seq=31522, Time=1806313043
277	11.970000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1012, Time=2080
278	11.970000	172.16.221.228	58.56.64.101	RTP	74	PT=ITU-T G.729, SSRC=0x43455AA6, Seq=31523, Time=1806313203

Getting start to DSP capture

DSP capture is help to analysis voice stream inside DSP chipset. The DSP chipset will handle RTP from IP network as well as voice stream from analog phone.

To enable DSP capture:

- Select DSP only on Network Capture page



- Click Start to enable DSP capture
- Dialing out through gateway, start talking a short while then hangup the call.
- Click Stop to disable DSP capture
- Save the capture to local computer

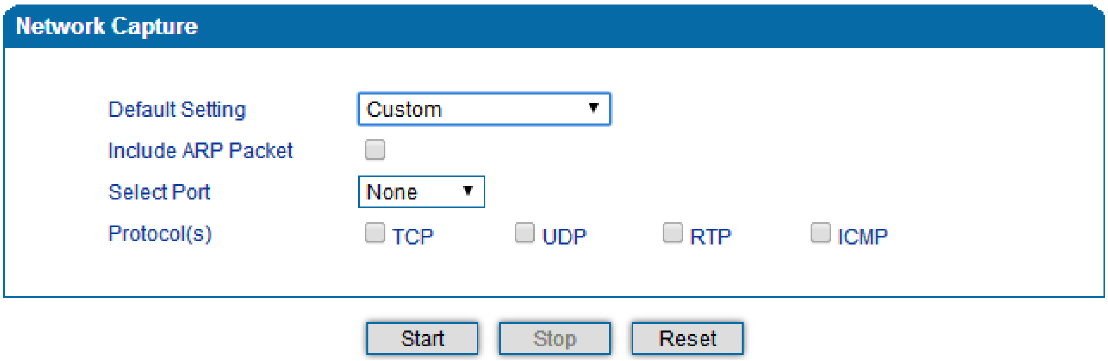
The capture is named to 'capture(x).pcap', x is serial number of capture and will be added 1 in next time. The sample of RTP capture as below:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0021 Ch: 0xFFFF, Seq: 2 (From Host)
2	0.007246	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
3	0.007260	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	44	--> 0x0021 Ch: 0xFFFF, Seq: 5 (From Host)
4	2.994581	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0021 Ch: 0xFFFF, Seq: 3 (From Host)
5	2.997308	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
6	2.997316	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	44	--> 0x0021 Ch: 0xFFFF, Seq: 6 (From Host)
7	5.992790	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0021 Ch: 0xFFFF, Seq: 4 (From Host)
8	5.997282	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
9	5.997290	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	44	--> 0x0021 Ch: 0xFFFF, Seq: 7 (From Host)
10	7.691428	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x9010 Ch: 0x0003, Seq: 3 (From Host)
11	7.691552	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
12	7.691715	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x9010 Ch: 0x0003, Seq: 1 (To Host)
13	7.701379	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x9000 Ch: 0x0003, Seq: 4 (From Host)
14	7.701494	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
15	7.701622	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x9000 Ch: 0x0003, Seq: 2 (To Host)
16	7.709662	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x8084 Ch: 0x0003, Seq: 5 (From Host)
17	7.709798	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
18	7.709902	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x8084 Ch: 0x0003, Seq: 3 (To Host)
19	7.710238	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x8001 Ch: 0x0003, Seq: 6 (From Host)
20	7.710328	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
21	7.710496	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x8001 Ch: 0x0003, Seq: 4 (To Host)
22	7.716241	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x8018 Ch: 0x0003, Seq: 7 (From Host)
23	7.716352	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
24	7.716465	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	30	<-- 0x8018 Ch: 0x0003, Seq: 5 (To Host)
25	7.716711	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x805b Ch: 0x0003, Seq: 8 (From Host)

Configurable capture options

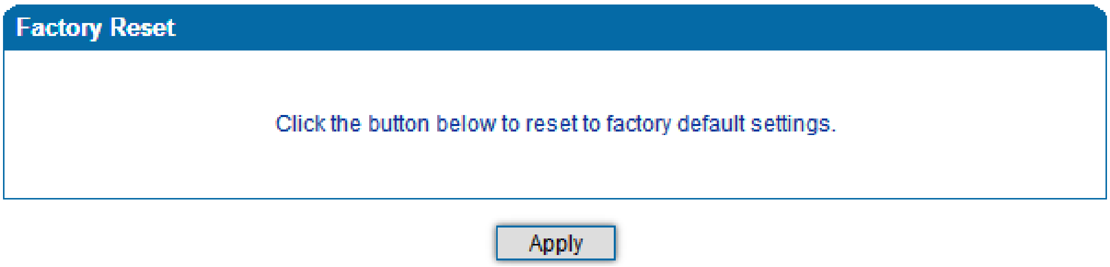
Getting start to custom capture

This menu provides more options to capture specific packets as actually needs.



Factory Reset

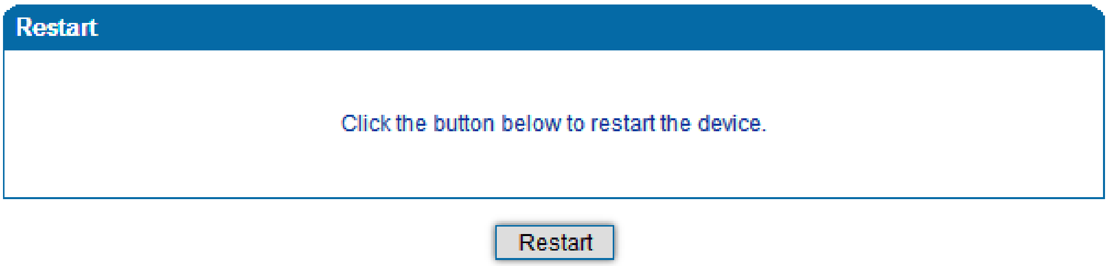
Click "Apply" to restore the factory settings.



Factory Reset

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.



Restart Gateway

Charpter5. 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：Address Resolution 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
- IMS: IP Multimedia Subsystem
- ACL: access rule list
- SNMP: Simple Network Management Protocol
- FXS: Foreign Exchange Station
- FXO: Foreign eXchange Office